Державний торговельно-економічний університет
Кафедра інженерії програмного забезпечення та кібербезпеки

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

**Збірник наукових статей студентів,
які здобувають освітній ступінь магістра
за спеціальностями 121 «Інженерія програмного забезпечення» та
125 «Кібербезпека та захист інформації»**

Київ 2023

Програмування та захист інформації : зб. наук. ст. студ. / відп. ред. – Київ : Держ. торг.-екон. ун-т, 2023. 654 с.

У збірнику наукових статей студентів висвітлені результати теоретичних та експериментальних досліджень в галузі інженерії програмного забезпечення й кібербезпеки та захисту інформації.

УДК

Відповідальна за випуск: О.В. Криворучко д-р техн. наук, проф.

Видається за рекомендацією вченої ради факультету інформаційних технологій ДТЕУ
(протокол №12 від 28 червня 2023 року).

ЗМІСТ

ВСТУП

На глобальному рівні відбуваються значні трансформації в сфері обробки та захисту інформації, що викликані інтенсивним ростом і впровадженням інформаційних технологій. Інформаційні технології, що ґрунтуються на комп'ютерних рішеннях, мають значний вплив на усі галузі життя та вимагають радикальних змін організаційних структур управління, його регламенту, кадрового потенціалу, системи документації, фіксування та передачі інформації.

Відчутно відзначається, що зростання значення інформаційних технологій створює нові виклики в контексті кібербезпеки та захисту інформації. Оскільки інформаційні технології стають не просто складовою частиною, але й активним каталізатором розвитку інформаційного суспільства, зростає необхідність в забезпеченні надійності та безпеки цих технологій та відповідної інформації.

В сучасному контексті однією з важливих пріоритетних задач є вивчення інформаційних процесів, що відбуваються в економіці, та ефективного управління ними в умовах інформаційного суспільства. При цьому неможливо обійти увагою аспекти кібербезпеки, які є необхідними відповідно до сучасного цифрового світу, де дані та системи стають вразливими перед кіберзагрозами.

В сучасному контексті важливою і актуальною є задачі розширення області інформаційної науки, зокрема зосередження на розвитку сучасних технологій програмування. Не менш вагомим є дослідження інформаційних процесів в економіці та розробка ефективних методів їх управління в умовах інформаційного суспільства. Важливо зазначити, що кіберзагрози стають все поширенішим явищем, тому дедалі більше уваги приділяється підготовці фахівців у галузі кібербезпеки та захисту інформації. Ці фахівці повинні бути компетентними у вирішенні практичних завдань, пов'язаних з розробкою, забезпеченням якості впровадження та супроводження програмних засобів, а також вміти знаходити раціональні методи та засоби їх розв'язання, включаючи складні ситуації. Додатково, вони грають важливу роль у підтримці сталого розвитку IT-компаній в аспекті якості процесів і результатів розробки програмного забезпечення.

Програма магістерської підготовка студентів спеціальностей «Інженерія програмного забезпечення» та «Кібербезпека та захист інформації» орієнтовані на формування у майбутніх фахівців відповідних компетентностей для роботи в галузі наукомістких технологій, педагогічної, науково дослідної роботи щодо вирішення актуальних прикладних, виробничих і народногосподарських задач.

У цьому збірнику наукових статей студентів, які здобувають освітній ступінь магістра за спеціальностями «Інженерія програмного забезпечення» та «Кібербезпека та захист інформації», представлені матеріали досліджень, отримані в рамках виконання їх випускних кваліфікаційних робіт.

RESTFUL API ЯК СТРАТЕГІЯ ПОЄДНАННЯ РОЗПОДІЛЕНИХ СИСТЕМ ТА ВПОРЯДКУВАННЯ БІЗНЕС-ПРОЦЕСІВ

АЛЕКСАНДРОВ А., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Стаття присвячена дослідженню REST API - архітектурного стилю, який забезпечує комунікацію між системами через Інтернет. У статті розглянуто компоненти RESTful архітектури, а також принципи та обмеження, на яких вони будуються задля забезпечення ефективної комунікації з акцентом на розподілених мікросервісних системах. Окрім цього, стаття досліджує питання безпеки REST API та рекомендації щодо захисту API від атак.

The article is devoted to the study of the REST API - an architectural style that enables communication between systems over the Internet. The article examines the components of a RESTful architecture, as well as the principles and constraints on which they are built in order to ensure effective communication focusing on distributed microservice systems. In addition, the article explores REST API security issues and recommendations regarding protecting APIs from attacks.

Актуальність. REST API (Representational State Transfer Application Programming Interface) є одним із найпоширеніших засобів взаємодії між програмними системами та їх компонентами в сучасному світі. Використання REST API має безліч переваг, що робить його дуже актуальним в сучасній програмній розробці, - гнучкість, легкість використання, масштабованість, безпека та інші.

В останні роки використання REST API стрімко зросло завдяки поширенню мобільних і вебзастосунків, цей підхід став кращим способом створення таких програмних засобів і використовується багатьма популярними вебсайтами та програмами, наприклад, Twitter, Amazon і Facebook.

Загалом, використання REST API є необхідною складовою сучасної веброзробки. Його здатність створювати масштабовані та гнучкі програми, які можна інтегрувати з іншими службами та технологіями, робить його важливим інструментом як для розробників, так і для компаній.

В контексті росту кількості програмних продуктів та сервісів, що потребують взаємодії між собою, REST API стає все більш потрібним для забезпечення безперебійної та ефективної комунікації між програмними системами.

Метою статті є розкриття основних компонентів та принципів архітектури REST.

Об'єктом дослідження є архітектура REST API, яка включає в себе різноманітні компоненти та принципи.

Предмет дослідження - основні компоненти REST API, їх функціонування та вплив на розробку вебзастосунків, а також можливість використання цієї технології для створення застосунків з покращеними функціональними можливостями.

Аналіз попередніх досліджень. Дослідженню розподілених систем, RESTful API, визначенню основних принципів та характеристик присвячені праці науковців: М. Массе [1], М. Фаулера [2], Л. Річардсона [3] та ін.

Виклад основного матеріалу. Стрімкий розвиток інформаційних технологій зумовлює ускладнення інформаційних систем. Розміри цілісних систем у минулому відповідають розмірам окремих модулів сучасних систем. Подібна архітектура привносить ряд проблем – обмежена масштабованість, потреба внесення змін у всю систему та необхідність повторного розгортання при найменших функціональних оновленнях, складність тестування та відлагодження через внутрішню зв'язність компонентів. Як результат, такі системи потенційно не стійкі та схильні до помилок, що виводять з ладу систему цілком.

Можливим шляхом вирішення проблем складності суцільної системи є її розподіл на менші частини, які можуть розглядатися як окремі системи, наділені власними характеристиками. Комп'ютерна система – це набір фізично розділених комп'ютерів, з'єднаних мережею, які комунікують та координують дії один одного для отримання результату. Програмна система – це набір незалежних компонентів, які працюють разом для надання ряду послуг або функціоналу.

У розподіленій системі користувацький інтерфейс та інші компоненти стають самостійними системами, які можуть комунікувати одна з одною, але не пов'язані напряму. Такий розподіл дозволяє ізолювати несправності окремих модулів, щоб інші могли залишатися працездатними, створити зручні умови для тестування, відлагодження, а також можливість швидких оновлень та розгортання (Рис.1).

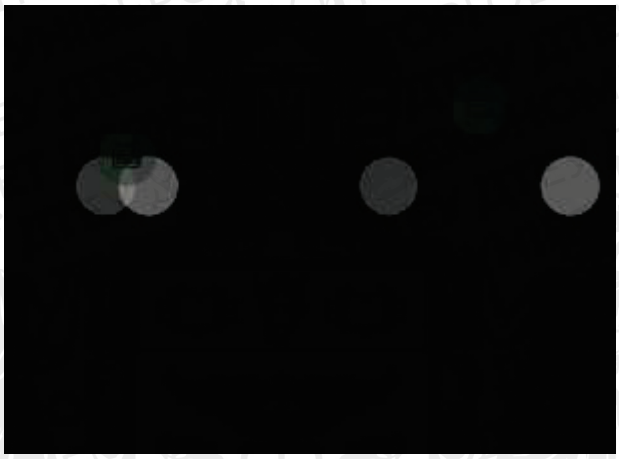


Рис. 1. Порівняння монолітної та розподіленої архітектури програмної системи

Одним з популярних підходів до реалізації розподілених систем є мікросервіси. Мікросервіси дозволяють розділити велику програму на менші незалежні частини, кожна з яких має свою сферу відповідальності. Щоб обслуговувати один запит користувача, програма на основі мікросервісів може звертатися до багатьох внутрішніх мікросервісів, щоб створити свою відповідь [4].

Проєктування та імплементація хорошої архітектури для програмного забезпечення є складною, комплексною задачею та передбачає розгляд таких аспектів, як функціональність, масштабованість, зручність обслуговування, продуктивність. Архітектура має бути достатньо надійною, щоб впоратися з різними сценаріями та непередбачуваними проблемами на етапах розробки чи розгортання.

Проєктування розподіленої архітектури значно складніше завдання та вимагає налаштування ефективної комунікації, забезпечення узгодженості та доступності даних у різних частинах системи, передбачає врахування потенційних проблем, пов'язаних із збоями та затримками в мережі. Дослідження архітектури програмного забезпечення включає методи визначення того, як найкраще розділити систему, як компоненти ідентифікують і взаємодіють один з одним, як передається інформація, як елементи системи можуть розвиватися незалежно, і як все вищезазначене можна описати за допомогою формальних і неформальних позначень [5, с. 16].

Серед переваг мікросервісної архітектури можна виділити наступні:

- відмовостійкість – виведення з ладу одного з сервісів не тотожно виведенню з ладу усієї системи;
- відсутність потреби використання однієї загальної технології чи мови програмування;
- зручні умови для командної розробки.

Чи не найбільшою проблемою розподіленої архітектури є забезпечення ефективної та стійкої комунікації між внутрішніми компонентами та створення уніфікованих інтерфейсів

для цього. Щоб полегшити інтеграцію різнорідних систем, які спочатку не були розроблені для спільної роботи, можна використовувати Web API.

Web API – це спосіб забезпечення зв'язку між різними системами через Інтернет, що дозволяє іншим програмам взаємодіяти з вебзастосунками, обмінюватися даними та виконувати різні операції. Вебінтерфейси API можуть бути реалізовані в різних форматах, включаючи REST API, SOAP, XML-RPC та інші. Кожен із цих форматів має свої переваги та недоліки, але REST API вважається одним із найпопулярніших і найбільш ефективних форматів для створення Web API.

REST API є простим та водночас дуже потужним інструментом для поєднання систем та інтеграції різних модулів в одну цілісну систему. Кожен з модулів виконує відведений набір функцій та взаємодіє з іншими модулями для забезпечення інтегрованої структури. Ефективність передачі даних між різними компонентами робить REST API незамінним інструментом в умовах розподіленої архітектури.

REST API – це архітектурний стиль, що став популярним у 2000-х роках завдяки стрімкому розвитку Інтернет-технологій та поширенню вебпрограмування. Цей стиль архітектури був розроблений Роєм Філдінгом, одним з авторів протоколу HTTP та співзасновником Apache Software Foundation. У своїй дисертації Рой Філдінг описав Representational State Transfer (REST) як стиль архітектури, що базується на створенні API для взаємодії між клієнтом та сервером та дозволяє отримувати доступ до ресурсів, які використовуються в різних контекстах.

RESTful API був розроблений з метою вирішення проблем, пов'язаних з існуючими підходами до взаємодії між клієнтом та сервером. Цей підхід робить взаємодію більш простою та ефективною, використовуючи вбудовані можливості протоколу HTTP – стандарту передачі даних в Інтернеті (Рис.2).

Рис. 2. Використання протоколу HTTP для комунікації в розподіленій системі

REST API заснований на ряді принципів, дотримання яких у повному обсязі забезпечує максимальну масштабованість та підтримуваність продуктів:

- Архітектура клієнт-сервер: клієнт та сервер можуть розвиватися незалежно один від одного і не залежать від реалізації один одного. Сервер надає ресурси, а клієнт запитує ці ресурси та маніпулює ними.
- Без збереження стану: сервер не зберігає жодного стану між запитами від клієнта. Кожен запит повинен містити всю необхідну інформації, щоб сервер міг зрозуміти його.
- Можливість кешування: відповіді на запити повинні бути чітко визначені як кешовані або некешовані, щоб дозволити клієнту оптимізувати майбутні запити.

- Багаторівнева система: сервер може складатися з кількох рівнів, кожен з яких виконує свою функцію. Клієнт не повинен мати змоги визначити, чи підключений він безпосередньо до сервера, чи до посередника.
- Уніфікований інтерфейс: ресурси однозначно ідентифікуються за URI (Uniform Resource Identifier) – уніфікованим ідентифікатором ресурсів.
- Повідомлення з описом: кожне повідомлення від клієнта до сервера та від сервера до клієнта повинно містити достатньо інформації, щоб описати, як обробити повідомлення.
- Гіпермедіа як механізм стану програми (HATEOAS): клієнти повинні мати можливість взаємодіяти з сервером виключно за допомогою гіперпосилань, наданих у представленнях.

Застосування принципів вимагає правильного використання компонентів та засобів, які складають архітектуру програмних інтерфейсів, серед яких:

- Ресурси – основний компонент REST API, може бути будь-яким об'єктом або набором об'єктів, доступних через Інтернет. Ресурси ідентифікуються унікальним іменем або URL-адресою.
- HTTP-методи – REST API підтримує методи HTTP, такі як GET, POST, PUT, DELETE, які дозволяють взаємодіяти з ресурсами та виконувати різні операції над ними – отримання, створення, оновлення існуючого та видалення ресурсів відповідно.
- Представлення даних – дані, які передаються через REST API, повинні мати певне представлення, серед них JSON - один з найпоширеніших форматів для передачі даних через REST API, також можуть передаватися у форматі XML, CSV, або будь-якому іншому форматі.
- Версіонування – використання різних URL-адрес для одних ресурсів, які можуть містити різні набори функції, це може допомогти із збереженням сумісності з попередніми версіями та дозволити користувачам за потреби обирати певну версію.

REST API є важливим інструментом у сучасному програмуванні, який дозволяє розробникам створити зручний та ефективний інтерфейс, доступний як з браузера, так і з будь-якої програми. Дотримання принципів REST сприяє створенню стандартизованої взаємодії між клієнтом і сервером, що спрощує розробку багатоплатформних застосунків.

Серед переваг REST API можна виділити наступні:

- Простота: REST API простий у використанні та розумінні, оскільки використовує стандартні HTTP методи (GET, POST, PUT, DELETE тощо) для взаємодії з ресурсами. Це дозволяє легко створювати вебсервіси, що працюють з більшістю браузерів та платформ.
- Гнучкість: REST API дає можливість розробникам використовувати будь-яку мову програмування, яка дозволяє взаємодіяти з протоколом HTTP, що робить його гнучким і масштабованим.
- Швидкість: REST API є дуже ефективним, оскільки використовує стандартні HTTP запити та відповіді, що дозволяє швидко передавати дані між клієнтом та сервером.
- Масштабованість: REST API дає можливість створювати вебсервіси, здатні працювати з великим обсягом даних та великою кількістю користувачів.
- Кешування: REST API підтримує кешування, що дозволяє зменшити навантаження на сервер та збільшити швидкість відповіді на запити.
- Сумісність: REST API може використовуватися на всіх платформах, де можна використовувати протокол HTTP.

Якщо програмне забезпечення відповідає архітектурному стилю REST, воно може вважатися RESTful. Однак не всі API, які претендують на RESTful, дотримуються всіх принципів, у деяких випадках API можуть реалізовувати лише підмножину принципів або можуть мати варіації чи розширення стандартних принципів. У цих випадках їх можна назвати

близькими до REST або REST-подібними. Проте і дотримання основних принципів REST може забезпечити значні переваги – масштабованість, гнучкість, простота впровадження та обслуговування.

REST API – потужний інструмент для комунікації між системами та обміну даними в розподілених середовищах. Однак, він надає доступ до ресурсів та даних за допомогою мережі Інтернет, тож безпека стає значною проблемою для розробників та адміністраторів подібних систем.

Основні проблеми безпеки, пов'язані з REST API, полягають у підвищенні ризику атаки на сервер, викрадення конфіденційної інформації, зміну чи видалення даних без дозволу власника, підробку запитів. Для запобігання цим проблемам, розробники REST API повинні дотримуватися низки заходів.

Один з найважливіших аспектів безпеки REST API – це аутентифікація та авторизація. Аутентифікація забезпечує ідентифікацію користувача та перевірку правильності облікових даних, тоді як авторизація визначає, які дії користувач має право виконувати в системі.

Крім того, розробники REST API повинні забезпечувати безпеку даних під час передачі їх по мережі. Для цього можуть використовуватися шифрування та підписи, що дозволяє переконатися, що отримувач отримує дані відправника та не були змінені в процесі передачі.

Також, розробники REST API повинні бути уважними при обробці вхідних даних та перевірці на вразливості. Наприклад, SQL-ін'єкції, атаки типу Cross-Site Scripting (XSS) та інші.

Висновки. Розподіл функціональності на менші компоненти є ключовою стратегією при розробці великих систем, це дозволяє знизити складність проєкту та забезпечити більш просту розробку, тестування та супровід. Важливим завдання розробників та архітекторів таких систем є забезпечення ефективної та стандартизованої комунікації, одним з можливих варіантів вирішення даної проблеми є використання RESTful API – одного з найбільш ефективних та поширених способів комунікації між компонентами системи. Використання RESTful API дозволяє стандартизувати та спростити інтерфейс взаємодії між компонентами системи, що забезпечує швидкість розробки та зниження витрат на розробку та підтримку коду, ефективної роботи системи в цілому.

Список використаних джерел

1. Masse M. Rest API Design Rulebook. O'Reilly Media, Incorporated, 2011.
2. Fowler M. Patterns of Enterprise Application Architecture. Pearsonn, 2012.
3. Richardson L., Ruby S., Amundsen M. RESTful Web APIs. O'Reilly Media, Incorporated, 2013.
4. Матеріали IT компанії “Google” \\ Режим доступу: https://cloud.google.com/learn/what-is-microservices-architecture / (останнє звернення 18.03.2023р.)
5. Fielding R. Architectural styles and the design of network-based software architectures : doctoral dissertation. Irvine, 2000. 162 с.
6. Masse M. Rest API Design Rulebook. O'Reilly Media, Incorporated, 2011.
7. Fowler M. Patterns of Enterprise Application Architecture. Pearsonn, 2012.
8. Richardson L., Ruby S., Amundsen M. RESTful Web APIs. O'Reilly Media, Incorporated, 2013.
9. Матеріали IT компанії “Google” \\ Режим доступу: https://cloud.google.com/learn/what-is-microservices-architecture / (останнє звернення 18.03.2023р.)
10. Fielding R. Architectural styles and the design of network-based software architectures : doctoral dissertation. Irvine, 2000. 162 с.

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н.О.

ОСНОВНІ ПРИНЦИПИ УСПІШНОЇ АРХІТЕКТУРИ САЙТУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

АРТАМОНОВ В., 2м курс ФІТ ДТЕУ,
спеціальність 121 «Інженерія програмного забезпечення»

У статті розглянуто основні принципи успішної архітектури сайту для електронної комерції з метою поліпшення користувацького досвіду та конверсії. В статті детально описано важливість ієрархії та структури інформації, види навігації та пошукові можливості, а також адаптивного дизайну для оптимізації мобільного досвіду. Також розглянуто взаємозв'язок архітектури сайту та оптимізації для пошукових систем, а також особливості архітектури ключових сторінок.

This article examines the basic principles of successful e-commerce site architecture to improve user experience and conversions. The article details the importance of hierarchy and structure of information, different types of navigation and search capabilities, as well as responsive design to optimize the mobile experience. The relationship between site architecture and search engine optimization, as well as the architectural features of key pages.

Актуальність. В статті висвітлено принципи успішної архітектури сайту для електронної комерції, що є актуальною темою в сучасному світі. За даними статистики, електронна комерція постійно зростає, а кількість інтернет-користувачів у світі швидко зростає з кожним роком. Це створює велику конкуренцію в онлайн-просторі, і успішність електронного бізнесу в значній мірі залежить від того, наскільки добре підібрана архітектура сайту. Правильна архітектура сайту може покращити користувацький досвід та зробити сайт більш зручним та доступним для відвідувачів, що може позитивно вплинути на конверсію та збільшення продажів. Також правильно розроблена архітектура сайту може покращити його видимість в пошукових системах, що є важливим фактором в успіху електронного бізнесу.

Мета. Метою даної статті є надання рекомендацій та інформації щодо того, як створити ефективну архітектуру сайту для онлайн-магазину. Стаття має на меті допомогти бізнес-власникам та розробникам зрозуміти основні принципи розробки ефективної архітектури для їхнього сайту електронної комерції.

Завдання. Основним завданням статті є надання читачам розуміння важливості ефективної архітектури сайту для досягнення успіху в електронній комерції. Стаття має на меті дати рекомендації щодо побудови архітектури сайту для забезпечення кращого користувацького досвіду, збільшення конверсії та покращення SEO-оптимізації для пошукових систем. Також стаття має за мету допомогти бізнесам розуміти, як використовувати архітектуру сайту для підвищення ефективності їхнього електронного магазину та забезпечення зростання прибутків.

Об'єкт. Об'єктом дослідження статті "Основні принципи успішної архітектури сайту для електронної комерції" є архітектура сайту для електронного магазину, що є ключовим елементом в успішній роботі електронної комерції. Стаття досліджує важливість створення ефективної архітектури сайту для забезпечення кращого користувацького досвіду та збільшення конверсії, що в свою чергу може призвести до зростання продажів та прибутків електронного магазину. Об'єктом статті є також взаємозв'язок архітектури сайту з оптимізацією для пошукових систем, що може забезпечити більш високу видимість сайту та збільшення трафіку на ньому.

Електронна комерція змінює спосіб ведення бізнесу на світовому ринку. Традиційні бізнес-практики замінюються онлайн-транзакціями та спілкуванням, завдяки чому компаніям стає легше, ніж будь-коли раніше, охопити глобальну аудиторію. Зростання електронної

комерції було експоненціальним, і це революціонізувало спосіб купівлі та продажу товарів і послуг. [1]

Основні принципи архітектури сайту електронної комерції: ієрархія інформації, зручність навігації, візуальний дизайн, адаптивність, швидкість завантаження.

У сучасному світі, де інформація є надзвичайно важливим ресурсом, є ключовим забезпечити її ефективне управління та організацію. Ієрархія та структура інформації є важливими інструментами для забезпечення управління та організації. Чітка ієрархія та структура інформації допомагає користувачам знайти потрібний товар або послугу, що робить процес пошуку більш швидким та ефективним.

Якщо ви не зрозуміло представите ієрархію ваших продуктів та послуг на своєму сайті, ви можете втратити відвідувачів, які хочуть знайти саме те, що їм потрібно. Чітка структура та ієрархія допоможуть відвідувачам швидко та ефективно знайти те, що вони шукають. [2]

Ефективна структура категорій та підкатегорій товарів на сайті має наступний вигляд:

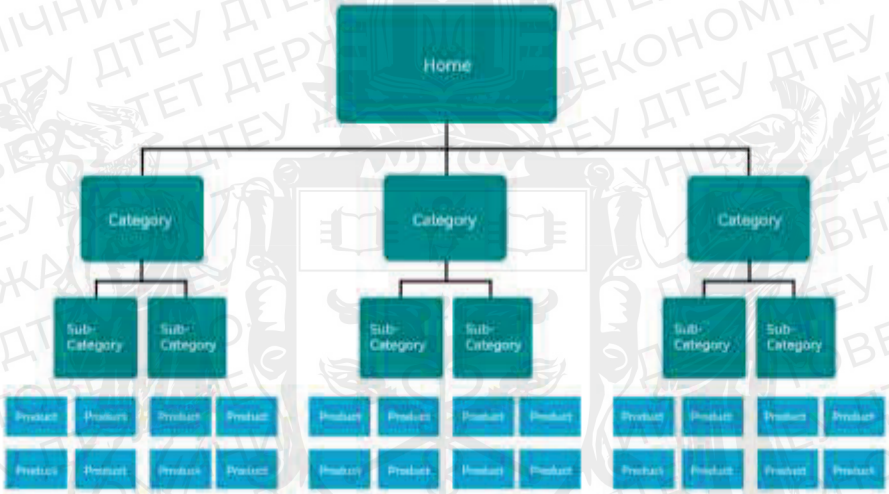


Рис.1. Ефективна структура даних на сайті електронної комерції [3]

Нижче наведено приклад моєї розробки використання даної структури на сайті магазину одягу (рис. 2).

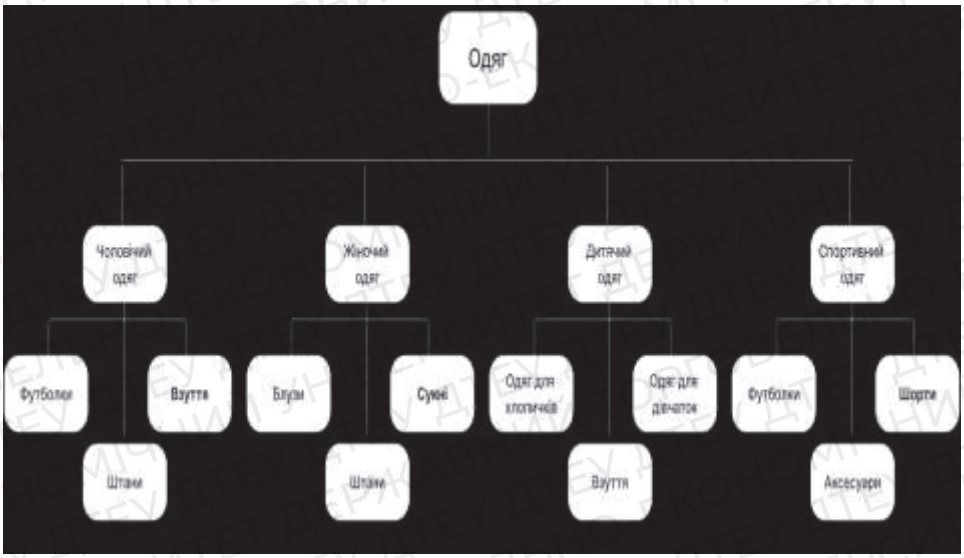


Рис.2. Приклад ефективної структури даних на сайті магазину одягу

Ця структура допомагає клієнтам швидко знайти потрібний товар, оскільки всі товари організовані в логічній послідовності.

Ефективна навігація є ключовим елементом успішної торгівлі в Інтернеті. Користувачам потрібно мати легкий доступ до того, що вони шукають, в ідеалі за кілька клацань мишкою або дотиків екрану [4].

Зв'язок між користувачем та веб-сайтом є важливою складовою, щоб забезпечити високу якість взаємодії. Навігація та пошук - це ключові елементи, які допомагають користувачам знайти необхідну інформацію на сайті. У цій статті будуть розглянуті різні види навігації та пошукові можливості, які полегшують знаходження товарів та інформації на сайті.

Головне меню зазвичай має випадаючі підменю, що дозволяє користувачам більш точно визначити свої потреби та перейти до необхідного розділу веб-сайту. Важливо, щоб головне меню було зрозумілим та легким у використанні.

Фільтри. Фільтри - це ще один вид навігації, який дозволяє користувачам вибирати та фільтрувати товари або інформацію за певними параметрами. Фільтри можуть бути розміщені на сторінках категорій товарів, пошукових сторінках та інших розділах сайту.

Breadcrumbs дозволяють користувачам зрозуміти, де вони знаходяться на веб-сайті та швидко повернутися до попередніх розділів. Вони також допомагають користувачам краще зорієнтуватися в структурі веб-сайту та розуміти, як вони можуть перейти до інших розділів.

Пошукові можливості. Пошук - це важливий елемент навігації на веб-сайті, який дозволяє користувачам швидко знаходити необхідну інформацію або товари. Сучасні веб-сайти зазвичай мають розширені пошукові функції, які дозволяють користувачам використовувати різні фільтри, сортування та інші опції.

Отже, навігація та пошук - це ключові елементи взаємодії між користувачами та веб-сайтом. Головне меню, фільтри та breadcrumbs дозволяють користувачам легко зорієнтуватися на веб-сайті та знайти необхідну інформацію. Розширені пошукові можливості дозволяють користувачам швидко та ефективно знаходити товари та інформацію за різними параметрами. Ці елементи навігації та пошукові можливості допомагають покращити користувацький досвід та забезпечують легкий доступ до інформації на веб-сайті.

Наш світ стає все більше мобільним, тому важливість оптимізації мобільного досвіду на сайті електронної комерції надзвичайно висока. Якщо ваш сайт не пристосований до мобільних пристроїв, ви втрачаєте велику кількість потенційних покупців. [5]

З огляду на зростання використання мобільних пристроїв, оптимізація мобільного досвіду є ключовою для успіху в електронній комерції. Адаптивний дизайн є одним з найважливіших аспектів оптимізації мобільного досвіду. Він забезпечує оптимальне відображення веб-сайту на будь-яких розмірах екрану, що дозволяє користувачам зручно переглядати контент та здійснювати покупки.

Додатково, для архітектури мобільних версій сайтів електронної комерції, наступні рекомендації можуть бути корисними:

Простота та зручність навігації. Важливо забезпечити зручну та легку навігацію мобільної версії веб-сайту, зокрема, головного меню та фільтри товарів. Кнопки навігації повинні бути відповідного розміру та розташування, щоб було зручно користуватися сайтом однією рукою.

Швидкість завантаження. Мобільні користувачі очікують, що веб-сайти будуть завантажуватися швидко. Важливо забезпечити оптимізовані зображення та мінімальний обсяг коду, щоб зменшити час завантаження мобільної версії веб-сайту.

Відповідність до формату мобільних пристроїв. Мобільні версії веб-сайтів повинні бути оптимізовані для роботи на різних типах мобільних пристроїв, включаючи планшети та смартфони з різними розмірами екранів. Рекомендується використовувати різні розміри шрифту та кнопок, щоб забезпечити зручне відображення контенту на будь-якому пристрої.

Простота оформлення замовлення та оплати. Мобільні версії веб-сайтів повинні забезпечувати легкий та зручний процес оформлення замовлення та оплати. Кнопки оплати повинні бути достатньо видимими та зрозумілими для користувачів.

Мобільні додатки можуть значно підвищити залучення, взаємодію та лояльність клієнтів. Клієнти, які завантажують мобільний додаток, частіше повертаються на сайт, проводять на ньому більше часу та роблять більше покупок, порівняно з тими, хто користується тільки мобільною версією сайту або десктопною версією. Крім того, мобільний додаток може забезпечити користувачам більш персоналізований досвід та бути корисним інструментом для збору даних про поведінку користувачів. [6]

Ефективна архітектура сайту може збільшити видимість сайту в пошукових системах та забезпечити краще ранжування, що приводить до більшого трафіку та прибутку. [7]

Архітектура сайту може визначати успіх в SEO. Власники сайтів повинні враховувати SEO, коли планують архітектуру сайту, і робити все можливе для забезпечення того, щоб їх сайт був легкодоступним для пошукових систем. Оптимізація для пошукових систем означає розробку та використання стратегій, які допоможуть підняти рейтинг вашого сайту в пошукових системах та забезпечать його високу позицію в результатах пошуку.

Основні аспекти оптимізації архітектури сайту включають:

Структуровані дані. Використання структурованих даних дозволяє пошуковим системам краще розуміти контент вашого сайту. Це може допомогти підняти рейтинг сайту, а також дозволяє відображати додаткову інформацію в результатах пошуку.

Ієрархія сторінок. Ієрархія сторінок на сайті повинна бути логічною та зрозумілою для користувачів та пошукових систем. Це допоможе зробити ваш сайт більш доступним для роботів пошукових систем.

Внутрішні посилання. Внутрішні посилання між сторінками вашого сайту можуть допомогти забезпечити легкий доступ для пошукових систем до різних сторінок сайту.

Оптимізація URL. URL-адреса сайту повинна бути легко зрозумілою та добре структурованою. Це зробить її більш зрозумілою для пошукових систем та користувачів.

Ось кілька рекомендацій щодо оптимізації URL:

Ключові слова в URL. Включення ключових слів в URL може покращити його SEO-показники. Ключові слова повинні бути релевантні тематиці сторінки та відображати зміст сторінки.

Короткі URL. Короткі URL краще, оскільки вони легше запам'ятати та поширювати. Якщо URL дуже довгий, то користувач може не зрозуміти, що він має вводити в адресний рядок браузера.

Структура URL. Хороша структура URL повинна бути логічною та легко зрозумілою для користувачів та пошукових роботів. Вона повинна відображати ієрархію сторінок на сайті.

Використання дефісів. Краще використовувати дефіси (-) у URL, а не знаки підкреслення (_). Пошукові роботи розглядають дефіс як роздільник між словами, а підкреслення - як частину слова.

Використання малих літер. URL повинні складатися з малих літер. Використання великих літер може призвести до проблем з SEO-показниками, оскільки пошукові роботи можуть розглядати різні URL як різні сторінки.

Нарешті, для досягнення високих показників SEO важливо враховувати аудиторію сайту та її потреби. Якщо архітектура сайту і контент не задовольняють потреб користувачів, то це може призвести до відсутності відвідувачів та негативно позначитися на показниках SEO. Отже, при проектуванні архітектури сайту необхідно зосередитися на забезпеченні зручного та корисного досвіду користувачів.

Оформлення замовлення - це критично важлива сторінка, оскільки вона забезпечує успішне завершення процесу покупки. Основна мета цієї сторінки полягає в тому, щоб забезпечити користувачам простий та зручний процес оформлення замовлення.

Під час розробки сторінки оформлення замовлення, важливо забезпечити, щоб користувачі мали можливість перевірити своє замовлення та всі відповідні деталі, такі як кількість товарів, ціни, вартість доставки та податки. Крім того, слід забезпечити можливість редагування замовлення до його підтвердження.

Один з ключових елементів сторінки оформлення замовлення - це форма оформлення замовлення. Вона має бути короткою та простою, але в той же час детальною. Крім основних елементів, таких як ім'я, адреса та спосіб оплати, можуть бути також додаткові поля для коментарів та питань.

Для підвищення конверсії на сторінці оформлення замовлення, рекомендується використовувати такі елементи, як гарантії повернення коштів та безкоштовну доставку при досягненні певної вартості замовлення. Крім того, важливо забезпечити можливість стеження за статусом замовлення та надсилання повідомлень про статус замовлення на електронну пошту або мобільний телефон.

Кошик є ключовим елементом електронної комерції, оскільки він є місцем, де покупець може зібрати разом свої покупки перед оформленням замовлення. Оскільки багато покупців відкладають свої покупки на пізніше, важливо мати чітку та просту у використанні систему кошика, щоб забезпечити, що вони можуть легко додавати та видаляти товари зі свого кошика, коли вони роблять свій вибір. [8]

Висновоки. Електронна комерція стає все більш популярною, і успішний онлайн-бізнес вимагає відповідної архітектури сайту для забезпечення високої конверсійності. Важливо ретельно продумати архітектуру свого сайту, включаючи розділи навігації та пошуку, адаптивний дизайн для мобільних пристроїв, оптимізацію для пошукових систем та ефективну архітектуру сторінок продукту, кошика та оформлення замовлення. Забезпечення зручного та простого користувацького досвіду може сприяти збільшенню кількості продажів та підвищенню лояльності клієнтів. Тому, при створенні сайту електронної комерції, важливо звернути увагу на кожну деталь та забезпечити максимальну зручність та простоту користування для кожного клієнта.

Список використаних джерел

1. Marketing in Hypermedia Computer-Mediated Environments / Donna L. Hoffman, Thomas P. Novak. 1995. С. 8-9; https://typeset.io/pdf/marketing-in-hypermedia-computer-mediated-environments-2ffhdnb9gv.pdf
2. A comprehensive review on e-commerce research / Vivian Khoo, Aidi Ahmi, and Ram Al-Jaffri Saad. 2016. С. 1-2; https://aip.scitation.org/doi/pdf/10.1063/1.5055471
3. Ecommerce SEO Guide: Ecommerce Marketing Strategies & SEO Tools. Електронний ресурс. URL: https://www.krishaweb.com/ultimate-ecommerce-seo-guide/
4. A Review Paper on E-Commerce / Dr. Shahid Amin, Prof. Keshav Kansana, Prof. Keshav Kansan. 2016. С 4-5; https://www.researchgate.net/publication/304703920_A_Review_Paper_on_E-Commerce
5. An Overview of Electronic Commerce (e-Commerce) / Vipin Jain, Bindoo Malviya, Satyendra Arya. 2021. С 5-7; https://www.researchgate.net/publication/351775073_An_Overview_of_Electronic_Commerce_e-Commerce
6. Katherine Taken Smith. Consumer perceptions regarding e-commerce and related risks. 2011. С 8-9; https://www.westga.edu/~bquest/2011/ecommerce11.pdf
7. Impact of e-commerce platform on consumer's mindset / Saani Solomon, Majji Lokesh, Jayaprakash Lamoriya. 2022. С 2-3; https://www.irjmets.com/uploadedfiles/paper/issue_3_march_2022/19668/final/fin_irjmets1646919637.pdf
8. A study on e-commerce trends in present scenario / Mrs. M.Vithya, Dr.Ti.M.Swaaminathan. 2022. С 6-7; https://ijcrt.org/papers/IJCRT2205354.pdf

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А.М.

ОСОБЛИВОСТІ ТА СУЧАСНІ ТЕНДЕНЦІЇ ПРОГРАМУВАННЯ НА МОВІ PYTHON

АФАНАСЬЄВ М., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто історію створення мови програмування Python. Проведено дослідження популярності даної мови програмування на основі особливостей даної мови. Проаналізовано та досліджено сучасні тенденції програмування на мові програмування Python.

The article discusses the history of the creation of the Python programming language. A study of the popularity of this programming language was conducted based on the features of this language. Modern programming trends in the Python programming language have been analyzed and researched.

Актуальність. Враховуючи тенденцію 22-23 року в сфері програмування, Python займає передові місця, про це свідчать дані індексу TIOBE, залишивши позаду Джава, Сі, C++ та інші не менш популярні мови, ставши лідером в рейтингу.

У зв'язку з чим саме з мови Python починається шлях майбутніх програмістів-початківців, а професіонали використовують цей інструмент для різного роду задач в різних сферах життя – це можуть бути як наукові дослідження чи навчальні програми, так і розробки в сфері штучного інтелекту чи машинного навчання.

В даній статті буде описано та розглянуто фактори популярності даної мови – її особливості, що передувало встановленню тенденціям програмування – на яких засадах базувалось створення даної мови програмування та коротка історія створення цього інструменту, котрий став одним з ключових в сфері розробки в наш час.

Метою статті є дослідження особливостей та тенденцій у сфері програмування з використанням мови програмування Python.

Об'єктом дослідження є особливості та тенденції програмування на мові Python в умовах розвитку мови програмування.

Предмет дослідження – мова програмування Python.

Аналіз попередніх досліджень. Дослідженню інформаційно-управляючих систем, визначенню структури, основних характерних рис присвячені праці вітчизняних та закордонних науковців: Ян Соммервіль, Стів МакКоннелл, Ерік Маттес, Дейв Томас, Енді Гант та ін.

Виклад основного матеріалу. В умовах сьогодення використання мови Пайтон в сфері інженерії програмного забезпечення можна представити наступним чином (Рис.1).

Python – це високорівнева та динамічно типізована мова програмування, що використовує інтерпретатор, в останні роки в сфері програмування став однією з ключових мов, що використовуються як початківцями так і професіоналами в різних напрямках, частина з них зображена на рисунку 1.

Рис. 1. Сфери використання мови Python

Проте популярним Python став набагато раніше. Проведемо дослідження історії створення. Історія мови Python розпочинається в кінці 1989 року – саме в цей момент Гвідо ван Россум – програміст з Нідерландів, почав розробку, маючи на меті створити зручний у використанні інструмент, що не мав би проблем з читабельністю коду, а також був би простим у використанні, що допомогло б новачкам швидше опанувати програмування та спростити розробку сценаріїв та автоматизацію задач.

В 90-х роках Python розвивався як альтернатива іншим мовам програмування, пропонуючи простий синтаксис та широкий набір функцій. Саме в цей час було реалізовано вбудовані типи даних, а також модулі та пакети – крім цього Python став доступним для багатьох платформ, що дозволило використання для вирішення ще більшої кількості задачі, окремо варто відмітити функціональні можливості такі як підтримка об'єктно-орієнтованого програмування та наявність інтерфейсів до баз даних та веб-розробки.

В 2000-х роках популярність Python продовжувала збільшуватись – саме в цей час було представлено версію мови 2.0, що мала ряд суттєвих переваг в порівнянні з минулими версіями. До переваг можна віднести покращення стандартної бібліотеки – з'явилась можливість додавати та змінювати наявні модулі.

Разом з розвитком мови збільшувалась й спільнота розробників – завдяки чому було створено велику кількість нових бібліотек, що застосовувались у таких сферах як навчання, бізнес, технології та інтернет, окремо варто відмітити сферу наукових досліджень – саме Python використовувався для симуляції та аналізу даних, інша сфера – це геймдев індустрія, в котрій Python використовувався для розробки ігр та інструментів для їх створення. Ще одним важливим кроком в покращенні мови стали підтримка багато поточності, мобільної та веб розробок.

В 2010-х роках популярність Python продовжувала збільшуватись. Цьому передувало декілька причин, одна з яких – це поява нових версій продукту, а саме версії 3, що збільшила кількість наявних функцій та покращила продуктивність. Крім цього стрімко збільшувалась кількість нових бібліотек – таких як NumPy чи Matplotlib – та доступних пакетів, окремо варто відмітити збільшення кількості доступних ресурсів для вивчення мови – таких як підручники та інформаційні форуми, що в свою чергу стало наслідком від розвитку спільноти програмістів Python.

Підсумовуючи, можна сказати що десятиліття роботи над мовою, функціями мови та інструментами й засобами використання внесли позитивний вклад в закріплення Python як однієї з найбільш широко використовуваної мови програмування в світі.

Розглянувши минуле мови програмування наступним кроком є аналіз популярності в даний час – для цього необхідно провести дослідження особливостей даної мови програмування. У зв'язку з багатою історією мови, наявністю двох основних гілок версій мови та щоденного впливу розробників та користувачів на наявні можливості мови програмування, виділимо ключові особливості, завдяки яким Python наразі є однією з найбільш популярних мов програмування. Відповідно до документації, філософії цієї мови, праць та статей іноземних та вітчизняних науковців, виділяють наступні особливості мови (див. рис. 2.):

- Простота вивчення та використання – Python має зрозумілий синтаксис, завдяки чому використання та вивчення є доволі простим процесом, що робить цю мову популярною серед новачків-програмістів або людей, котрі починають своє знайомство з програмуванням. Наявність стандартної бібліотеки з великою кількістю реалізованих функцій всередині також є ключовим фактором, що позбавляє програмістів зайвий раз писати код уже реалізованих функцій.
- Універсальність даної мови – це те, що робить мову Python тим, чим вона наразі є, можливість використання мови для веб-розробки, десктоп розробки, мобільної розробки, штучного інтелекту чи аналізу даних, наукових досліджень – це невелика частина широкого спектру сфер мови.
- Наявність великої спільноти розробників, котрі створюють нові більш актуальні інструменти та бібліотеки, завдяки яким відбувається розвиток мови. Внаслідок чого Python має велику базу інформаційних ресурсів та підтримку користувачів.
- Використання в науці – це окрема ключова особливість, завдяки використанню бібліотек для машинного навчання та аналізу великих даних, таких як NumPy чи Matplotlib. Завдяки цим бібліотекам складні завдання виконуються в рази швидше та дозволяють створювати візуалізацію отриманих даних. Сюди можна віднести також й використання мови інформаційними гігантами як Google чи Facebook, котрі використовують дану мову в своїх дослідженнях чи розробках.
- Наявність крос платформної підтримки – можливість використання Python на різних платформах дозволяє зосередитись саме на розробці програмного забезпечення, не переймаючись проблемою портативності на інші пристрої з іншими операційними системами.
- Наявність відкритого програмного коду – завдяки цьому розробники мають доступ до внутрішнього коду функцій та бібліотек, що дозволяє вносити правки в уже наявні програмні рішення, корегуючи функції під власні потреби – саме через це наявна така велика кількість користувацьких бібліотек та інструментів.

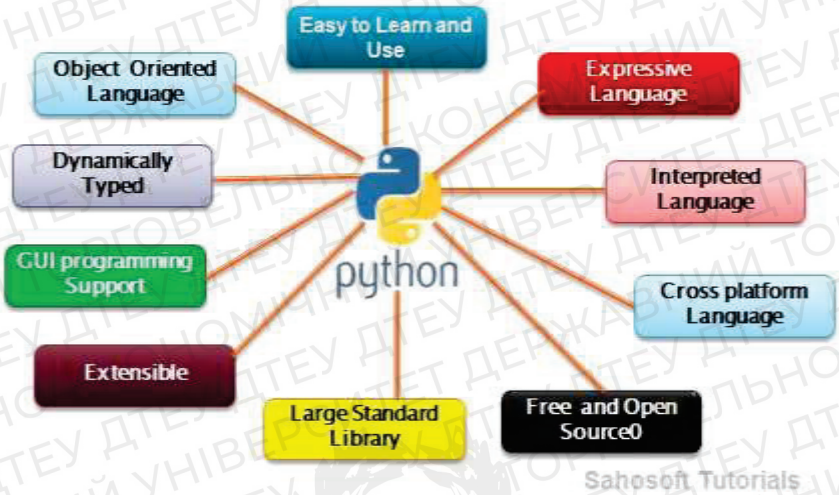


Рис. 2. Особливості мови програмування Python

Наступним кроком є аналіз сучасних тенденцій програмування на мові програмування Python. Для цього необхідно звернутись до статистичних даних, проаналізувавши варіанти використання даного інструменту [5].

Цей інструмент доволі популярний в сфері науки, а саме Data Science та Machine Learning, цьому є декілька причин. Одна з яких – це наявність великої спільноти користувачів, що створили багато інструментів для аналізу даних та проведення досліджень, а також для вирішення задач й проблем. Наступна причина – це простота використання та наявність й створення зрозумілого коду, адже синтаксис мови є простим та інтуїтивно зрозумілим, адже він схожий на англійську мову – це є ключовим фактором в сфері науки та даних, де необхідно концентрувати увагу на постановці й вирішенні задачі, а не створенню складного коду.

Крім цього Python має можливості, що дозволяють його використання для цього типу задач – підтримка ООП, паралельна обробка даних та розподілення обчислень – все це дозволяє вирішувати проблеми використання великих масивів даних. Також на це впливає й наявність бібліотек для машинного навчання – таких як TensorFlow, PyTorch, NLTK, завдяки наявним рішенням задач науковці-спеціалісти можуть без проблем використовувати необхідні методи для вирішення задач, не витрачаючи час на створення інструментів для досягнення мети.

Окремо варто відмітити сумісність Python з іншими мовами програмування, що дозволяє використовувати найбільш доцільні методи та інструменті; наявність великої кількості навчених моделей, доступних для використання та через які вже пройшли велика кількість даних, що дозволяє зекономити час та ресурси для навчання й створення вибірки даних; можливість взаємодії на різних рівнях – високому та низькому.

За останні роки Python став популярним й в сфері веб-розробки. Наявність фреймворків, таких як Django чи Flask дозволяють в короткий період часу створити веб-додаток, веб-сайт або інший веб-продукт, зосереджуючись на ідеї та меті продукту, пропонуючи готові рішення в тій чи іншій мірі.

Окремим пунктом варто відмітити популярність мови Python в сфері геймдеву. Завдяки сумісності на різних платформах можливе спрощення розробки та створенні портативних продуктів. Завдяки наявності абстракцій відбувається спрощення структури коду та його повторному використанні в різних проектах та управлінні складними системи всередині ігрових функцій. Наявність готових бібліотек для розробки ігр дозволяють прискорити процес створення продукту – бібліотеки такі як Pygame, Panda3D, Pyglet надають користувачеві доступ до готових класів та функцій щодо розробки ігр, що дозволяє використати зекономлений час на інших задачах. Швидке прототипування дозволяє переходити від абстракцій високого рівня до низькорівневої реалізації функції, що пришвидшує процес тестування та доробки. Оскільки дана мова займає провідні позиції в сфері програмування не

перший рік, наявна велика кількість спеціалістів, котрі шукають можливість застосування своїх знання та вмінь, зосереджуючись не лише на написанні коду, геймдев – це одне з таких місць.

Резюмуючи, Python – це універсальна мова програмування зі своїми особливостями, завдяки яким зараз знаходиться в перших списках рейтингу мов програмування, з тенденцією до використанню в різних сферах життя – в науці та дослідженнях, машинному навчанні, десктоп, мобільній та веб-розробці – завдяки наявній готовій базі бібліотек, інструментів та ресурсів, а також спільноті спеціалістів.

Крім цього наявне використання й в різних інших сферах технологій та програмування:

- штучний інтелект – у зв'язку з використанням бібліотек TensorFlow, Keras, PyTorch, Scikit-learn;
- веб-розробка – використовується для створення веб-серверів, сервісів та веб-додатків, можливе використання фреймворків Джанго та Фласк; дозволяє швидко створювати веб-сайти та інші веб-продукти, в тому числі й такі, що не потребують великої кількості обчислювальних ресурсів чи техніки;
- розробка додатків – Python був й залишається доволі популярним інструментов для створення десктоп та мобільних додатків; завдяки наявністю бібліотек та інструментів таких як PyInstaller та Py2Exe, можлива швидка розробка додатків на різні платформи;
- BigData та Data Science – широко використовується в сфері обробки великих масивів даних, завдяки наявністю бібліотек таких як Pandas, Numpy, Matplotlib. Можливе використання як для обробки, аналізу так і для візуалізації масивів даних. Використовується для розробки алгоритмів машинного навчання чи статичного аналізу.

Завдяки своїм особливостям та наявній базі ресурсів Python був та залишається одним з найбільш популярних мов програмування наразі та буде займати провідні позиції в майбутньому.

Висновки. Python – це універсальна мова програмування, історія якої почалась в кінці 90х років минулого століття, протягом часу розвивалась з власною спільнотою й наразі займає ключові місця в сфері програмування. В статті було розглянуто історію створення й розвитку мови програмування, розглянуто ключові особливості даної мови, розглянуто тенденції програмування з використанням мови програмування Python. Зроблено висновки щодо використання в подальшому й наразі.

Список використаних джерел

1. Ian Sommerville: Software Engineering, 10th edition, Person Education Ltd, 2015
2. Steve McConnell : Perfect Code / Steve McConnell – Los Santos, USA: GTA 806 с.
3. Matthes E. Python Crash Course (2nd Edition) : A Hands-On, Project-Based Introduction to Programming / Eric Matthes. – San Francisco, United States: No Starch Press, US, 9. – 544 с. – (2nd Edition).
4. Learn Python the Hard Way : A Very Simple Introduction to the Terrifyingly Beautiful World of Computers and Code – New Jersey, United States: Pearson Education (US), 2013. – 320 с.
5. Thomas D. The Pragmatic Programmer : your journey to mastery, 20th Anniversary Edition / D. Thomas, A. Hunt. – Boston, United States: Pearson Education (US), 2020. – 352 с.

Робота виконана під науковим керівництвом к.е.н., доц.
ТИЩЕНКА Д.О.

ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІЙНОГО ДОСТУПУ

БАРАНОВ О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті висвітлено питання важливості захисту інформації від несанкційного доступу зі сторони інформаційної безпеки держави. Проаналізовано основні види захисту та шляхи запобігання цілісності інформації з обмеженим доступом.

The article highlights the importance of protecting information from unauthorized access from the information security side of the state. The main types of protection and ways to prevent the integrity of information with limited access are analyzed.

Актуальність. Ефективність функціонування ринку інформаційних послуг та продуктів є комплексним процесом, який ґрунтується на численних аспектах, зокрема на забезпеченні належної законодавчої підтримки та відповідного правового захисту. Розвиток сучасної сфери інформації вимагає ретельного розгляду та вирішення широкого спектру взаємопов'язаних економічних, юридичних та технологічних аспектів на законодавчому рівні.

У сучасному інформаційному просторі, де зв'язок та обмін даними мають підвищений обсяг та швидкість, проблема захисту інформації набуває особливої актуальності. Ця проблема полягає не лише у захисті від зовнішніх загроз, але й у внутрішньому контролі та управлінні доступом до конфіденційних даних. Важливим аспектом стає виявлення та нейтралізація потенційних ризиків, пов'язаних зі зловживанням інформацією, порушенням прав доступу та можливими порушеннями конфіденційності.

Правове забезпечення інформаційної безпеки виступає ключовою складовою розвитку інформаційного суспільства. Це вимагає не лише прийняття відповідних законів і нормативів, але й ефективного контролю за їхнім виконанням. Забезпечення відповідного правового режиму для обігу інформації сприяє підвищенню довіри суб'єктів ринку, що, у свою чергу, стимулює розвиток інформаційних послуг та продуктів.

Недооцінка проблеми інформаційної безпеки може мати далекосяжні наслідки. Вона загрожує не лише нанесенням збитків окремим суб'єктам, але й функціонуванню всього інформаційного ринку в цілому. Недостатня захищеність даних може спричинити втрату конфіденційності, порушення відносин між бізнес-партнерами та споживачами, а також порушити довіру до електронних систем та онлайн-платформ.

Отже, ефективний розвиток ринку інформаційних послуг та продуктів потребує глибокого аналізу, розробки та впровадження відповідних законодавчих та правових механізмів для забезпечення надійності, конфіденційності та доступності інформації.

Мета статті. Аналіз механізмів захисту інформації та їх особливостей, які використовуються для захисту від несанкціонованого доступу.

Завдання дослідження полягають у: бґрунтуванні необхідності забезпечення захисту інформації з обмеженим доступом.

Результати дослідження. Відповідно до потенційних порушень функціонування інформаційних систем та загроз несанкціонованого доступу, види захисту інформації можуть бути класифіковані на різні групи, які включають морально-етичні, правові, адміністративні, організаційні, технічні або фізичні, а також програмні аспекти. Ця класифікація надає комплексний погляд на системний підхід до забезпечення надійності інформаційного середовища та ефективності її функціонування.

Морально-етичні аспекти відіграють важливу роль у визначенні етичних норм та стандартів поведінки користувачів, розробників інформаційних систем та технологій. Ця група заходів відображає значення засад порозуміння та поваги до інформаційної власності, конфіденційності та приватності.

Правові механізми захисту ґрунтуються на нормативно-правових актах, які встановлюють норми використання, розповсюдження та обміну інформацією. Вони включають правила відшкодування збитків у разі порушення авторських прав, а також регламентують питання щодо відповідальності за порушення законодавства у сфері інформаційних технологій.

Адміністративні та організаційні методи захисту передбачають встановлення внутрішніх правил та політик, спрямованих на забезпечення безпеки інформації. Це включає управління доступом до даних, регулярний аудит систем безпеки та навчання персоналу щодо обізнаності з потенційними загрозами.

Технічні та фізичні заходи захисту ґрунтуються на використанні технологій та фізичних бар'єрів для захисту інформації. Це включає шифрування даних, біометричну ідентифікацію, контроль доступу та інші технічні засоби.

Програмні аспекти захисту охоплюють розробку та застосування програмних засобів для виявлення, запобігання та нейтралізації загроз інформаційній безпеці. Ці засоби можуть включати антивіруси, фаєрволи, системи виявлення вторгнень та інші.

Сучасний напрям розвитку технологій полягає в поєднанні апаратних та програмних рішень для досягнення максимальної надійності та ефективності захисту інформації. Це можливо завдяки використанню новітніх технічних розробок та інтеграції програмних інструментів, що робить сучасну систему захисту більш адаптованою до викликів сучасного цифрового середовища. [1].

До групи морально-етичних засобів відносять стандарти поведінки, які сформувались чи формуються з поширенням ЕОМ, мереж та ін. Дані норми не затверджені на законодавчому рівні та є більше умовними, проте їх недотримання може призвести до зниження авторитету особи чи групи осіб, організації чи навіть цілої країни. Дані норми можуть бути як неписаними, так і оформленими у вигляді статуту. Прикладом може слугувати Кодекс професійної поведінки членів асоціації користувачів ЕОМ США.

У сфері правового регулювання належної охорони інформації відзначається, що належність до правових засобів захисту включає діючі укази, закони та інші нормативно-правові акти, які становлять основний стовп регулювання правил використання конкретної інформації. Відмітною рисою цих юридичних інструментів є їхнє жорстке формалізоване визначення, яке встановлює норми, обов'язки та відповідальність в разі порушення визначених правил.

Узагальнюючи вищевказане, варто підкреслити, що зазначені методи правового захисту мають важливе значення для забезпечення інтелектуальної власності та прав програмістів, оскільки вони надають гарантію протекції авторських прав на творчість у сфері ІТ. Це сприяє створенню рівних умов для розробників програмного забезпечення та інших інноваторів, що змушує ринок ІТ визнати та поважати їхню інтелектуальну власність.

Значущість нормативно-правових актів в сфері інформаційної безпеки та використання технологій не обмежується лише авторськими правами. Вони також визначають важливі аспекти використання інформації загалом, включаючи захист особистих даних, правила конфіденційності та відповідальність за порушення цих норм.

Таким чином, зазначені юридичні методи захисту належать до ключових інструментів впорядкування та контролю в галузі інформаційної безпеки та використання інформаційних технологій. Вони забезпечують не лише захист інтелектуальних прав суб'єктів, а й встановлюють засади відповідального та етичного використання інформації в сучасному цифровому світі. На даному етапі переходу до цифрового суспільства гостро постає питання покращення цивільного та карного законодавства й судочинства. Відповідні закони затверджуються та доповнюються в більшості розвинених країнах сучасного світу та різних міжнародних коаліціях. Їх порівняння майже неможливе, беручи до уваги той аспект, що кожен окремий закон має розглядатися в контексті законодавства кожної країни. Загально можна відслідкувати тенденцію зростання жорсткості кримінальних законів щодо інформаційних злочинів. На приклад, Гонконг встановив максимальне покарання за дані

злочини у вигляді 10 років позбавлення волі, якщо наслідком є пошкодження справності 1С або Web-сайту. В Україні, ж на противагу, протизаконне втручання в роботу комп'ютерних мереж несе за собою покарання у вигляді виправних робіт строком не більше двох років, штрафу до сімдесяти неоподаткованих мінімумів доходів злочинця чи позбавлення волі строком до двох років.

Щодо адміністративних або організаційних засобів захисту інформації, то вони покликані регламентувати процеси діяльності 1С, користування її ресурсами, функціонування діяльності персоналу та взаємодію користувачів із даною системою в такий спосіб, мінімізувати ризик порушення безпеки. Такі засоби включають (рис.1):

- заходи, що запроваджуються в процесі проектування, облаштування та будівництва об'єктів охорони, на приклад: протипожежна безпека, режим пропусків, охорона поміщення, таємний контроль роботи працівників та ін.;
- заходи, які впроваджують безпосередньо під час розробки, ремонту, та замінні обладнання або програмного забезпечення, до яких відносяться: процес сертифікації програмних та технічних засобів, стале санкціонування, затвердження усіх видів змін і тд.;
- заходи під час набору й підготовки персоналу, такі як: створення спеціальних умов, за яких унеможливлюється витік інформації, детальна перевірка потенційних працівників, обов'язкове ознайомлення співробітників із правилами конфіденційності та відповідальністю за їх недотримання;
- заходи щодо правил обробки й зберігання інформації та її захисту, а саме: зберігання, облік, використання, утилізація документів та носіїв інформації, що є конфіденційною, обмеження доступу до інформації за допомогою паролів, персональних профілів та створення видів покарань за порушення даних правил [2].

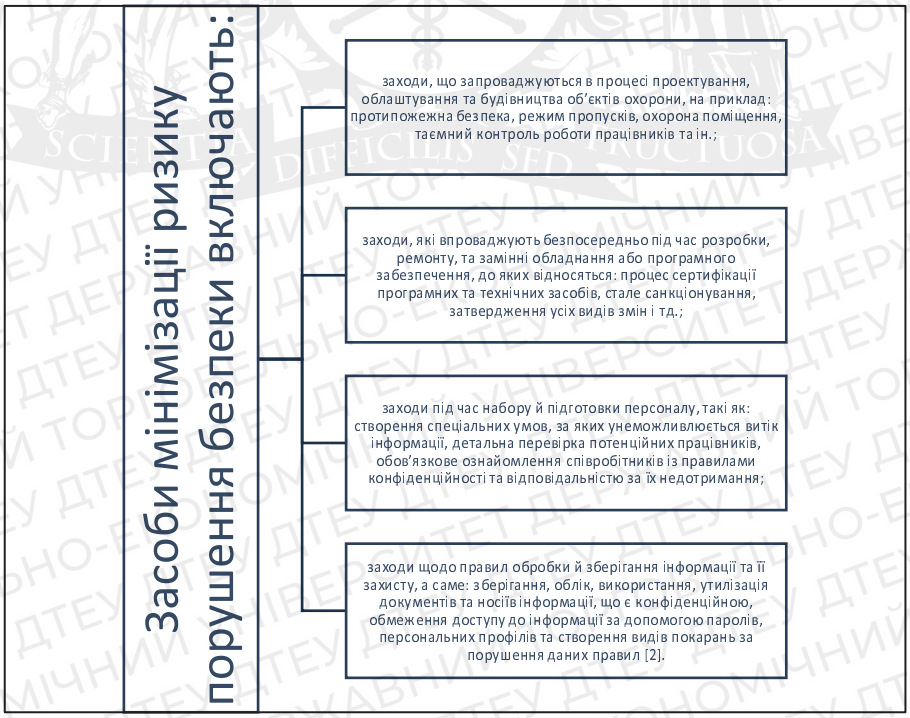


Рис. 1. Засоби мінімізації ризику порушення безпеки

Важливість адміністративних заходів зумовлюється їх здатністю в доповненні законодавчих норм, де це є необхідним, доступністю та можливістю застосування різних видів захисту (програмного, технічного). Проте, потрібно враховувати, зо надмірна кількість

таких заходів негативно впливає на персонал, обтяжуючи його та не являється достатньо ефективним методом протекції інформації, позаяк деякі інструкції часто просто ігноруються.

Засоби фізичного або технічного захисту – це різноманітні пристрої (механічні, електро-механічні, електронно-механічні) та матеріали й спорудження, призначенням яких є захист інформації від незаконного доступу, її викрадення та втрат в разі виведення з ладу компонентів 1С, диверсії, саботажу та і тд. До даних заходів відносяться:

- засоби щодо заходу систем електропостачання. Спираючись на аналіз американських досліджень, можна зробити висновок, що найефективнішою протидією втрати інформації у разі припинення постачання електроенергії до серверів або стрибків напруги являється облаштування в приміщеннях устаткування безперебійного живлення. Сучасні технології дозволяють вибрати найкраще устаткування відповідно до різних критеріїв;
- засоби, призначені для захисту кабельної системи. Щоб попередити збої кабельної системи, які є причиною багатьох відказів ЛОМ, слід облаштовувати структуровану кабельну систему, яка має однакові кабелі для датчиків протипожежної безпеки, передачі даних 1С, відео системи охорони, та локальної мережі телефонів. Структурована система має на увазі кабельну систему, яка поділяється на декілька рівнів в залежності від розміщення та її призначення. Для забезпечення ефективності роботи даної системи варто дотримуватись міжнародних стандартів;
- засоби, що захищають інформацію від відпливу на декількох фізичних полях, які з'являються під час роботи технічних засобів. До них належать пристрої, що призначенні виявляти прослуховувальну апаратуру, радіотехнічне маскування за допомогою широкосмугових генераторів шумів, екранування приміщень електромагнітними пристроями тощо.
- засоби для дублювання та архівації інформації – спеціалізовані сервери, які служать для архівації даних. Доцільно їх використовувати при наявності великих обсягів інформації та зберігати у спеціальних приміщеннях під охороною [4].

До цієї групи ще відносять матеріали по забезпеченню безпеки зберігання та транспортування носіїв інформації, а також захист від їх копіювання. Вони являють собою професійні тонкоплівкові матеріали з наявністю змінної кольорової гамми чи голографічних міток, які наносяьбся на предмети, елементи комп'ютерної техніки, документи з метою ідентифікації справжності об'єкта та контролю доступу до нього.

Як було заначено вище, в більшості випадків на практиці технічні засоби реалізовують в комбінації з програмними.

Програмні засоби захисту покликані забезпечувати ідентифікацію та аутентифікацію користувачів, відокремлення доступу до інформації відповідно до повноважень її користувачів, реєстр подій 1С, протекцію від комп'ютерних вірусів, криптографічний захист даних і тд.

Під час дослідження програмних засобів важливо приділити особливу увагу стеганографічним методам, які в свою чергу можуть бути визначені як методи "прихованого письма". Ця галузь криптографії вивчає способи приховування інформації в інших носіях, таких як зображення, звукові файли або текстові документи, з метою унеможливлення особам без відповідного доступу виявити наявність такої прихованої інформації.

Одним з ключових аспектів стеганографії є те, що вона прагне робити стеганографічний контент незамітним та непомітним для звичайного спостерігача. Це означає, що прихована інформація не повинна спричиняти підозрілих змін у вигляді основного носія (наприклад, зображення чи звуку). Завдяки цьому, стеганографія може бути ефективним засобом для передачі конфіденційних даних без виклику підозрілості.

Одним із прикладів використання стеганографічних методів в сучасності є використання комп'ютерних технологій для заховування інформації в текстових або графічних

документах. Наприклад, у контексті друкованих контрактів, можуть бути застосовані практики стеганографії, що передбачають невеликі та майже непомітні викривлення обрисів окремих символів. Ці незначні зміни в обрисах можуть містити зашифровану інформацію, пов'язану з умовами контракту або іншими конфіденційними деталями. Цей метод дозволяє створювати зовнішній вигляд документа, який виглядає звичайним, однак, містить додатковий рівень інформації, недоступний звичайному спостерігачу.У суті комп'ютерної стеганографії лежать два основні принципи. Перший полягає в тому, що відео-, аудіо- та файли з оцифрованими зображеннями можливо дещо змінювати, при цьому не втрачаючи їх функціональності. Другий принцип наголошує на обмежених можливостях вбачати невелику різницю у зміні кольору або звуку. Частіше за все стеганографія використовується при створенні цифрових водяних знаків, які можна наносити та помічати лише за допомогою використання спеціально призначеного програмного забезпечення. В таких випадках цифрові водяні знаки записуються у вигляді псевдовипадкових послідовних шумових сигналів, сформованих за допомогою секретних ключів. Такого роду знаки забезпечують недоторканість та автентичність документа, ідентифікацію власника та перевірку права користувача [3, 5-6].

При впровадженні засобів програмно-технічної протекції використовують такі основні способи як (рис.2):

- вбудований захист, а саме механізми, які реалізують як окремі компоненти 1С або розподілені за іншими компонентами системи;
- додатковий захист, що являє собою доповнення до основного переліку програмних та апаратних засобів комп'ютерної системи.

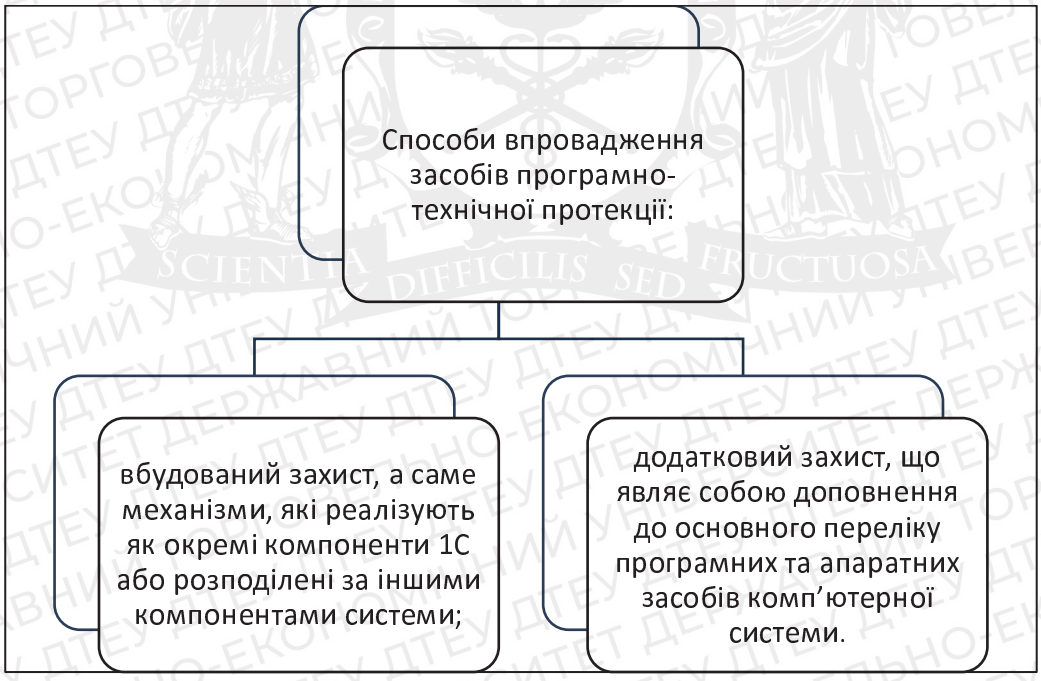


Рис. 2. Способи впровадження засобів програмно-технічної протекції

Останній спосіб є гнучкішим, даний механізм можливо залучати та вилучати за необхідності, проте під час його впровадження можуть виникнути проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом 1С. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

Висновки. Розробка та реалізація комплексної програми захисту інформації в сучасному бізнес-середовищі є невід'ємною складовою ефективного функціонування будь-якої організації. Ця програма, що об'єднує організаційні та програмно-технічні заходи, спрямована

на гармонійний баланс між доступністю інформації та її надійним захистом. Вона є каркасом, на основі якого будуються стратегії та тактики забезпечення інформаційної безпеки. Ця програма включає в себе широкий спектр дій та стратегій. Розмежування прав доступу до інформації є однією з найважливіших складових, оскільки воно дозволяє обмежити доступ до конфіденційної інформації лише тим особам, які мають відповідні повноваження. Це зменшує ризик несанкціонованого доступу та можливість витоку даних.

Оновлення програмного та технічного забезпечення є необхідною умовою забезпечення інформаційної безпеки. Швидкий розвиток технологій означає, що потенційні загрози також стають все більш складними та виразними. Захисна стратегія повинна враховувати цей аспект та постійно оновлювати заходи захисту, щоб відповідати сучасним стандартам безпеки.

Навчання персоналу відіграє ключову роль у забезпеченні успішної програми захисту інформації. Інсайдерські загрози, а також людський фактор загроз взагалі, є найскладнішими для контролю. Навчання персоналу щодо правил безпеки, розпізнавання фішингу та інших атак допомагає підвищити обізнаність та відповідальність кожного працівника.

Важливо зрозуміти, що створити абсолютно небезпечну інформаційну систему майже неможливо. Система безпеки завжди є компромісом між доступністю та захистом. Організації повинні постійно аналізувати та оцінювати потенційні ризики, вдосконалювати свої заходи безпеки та адаптувати їх до змінних умов.

Таким чином, розробка та впровадження комплексної програми захисту інформації є невід'ємною складовою успішної діяльності будь-якої сучасної організації. Ця програма допомагає забезпечити баланс між доступністю та безпекою інформації, мінімізувати ризики та зберегти довіру від клієнтів та партнерів.

Список використаних джерел

1. Зотова І.Г., Берестов Д.С. Підсистема захисту інформації від несанкційного доступу в ERP-системі. Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ. 2015. С. 38-42.
2. Шевченко В.Л. Несанкціонований доступ до інформаційних ресурсів ERP-системи / В.І. Кулажський, О.С. Кульчицький// ЦВСД НУО України, м.Київ, ЗНП ЦВСД НУО України, Вип. 1(50), 2014 р. С. 9.
3. Півень А.Г. Захист інформації та використання інформаційних технологій в інтелектуальній власності: монографія, 2011.
4. Lakhno, V. ., Maliukov, V. ., Komarova, L. ., Kasatkin, D. ., Osypova, T., & Chasnovskyi, Y. (2022). Оптимізація розміщення засобів захисту інформації на основі застосування генетичного алгоритму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 6–20. https://doi.org/10.28925/2663-4023.2022.17.620
5. Tyshyk, I. (2022). Тестування корпоративної мережі організації на несанкціонований доступ . Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 39–48. https://doi.org/10.28925/2663-4023.2022.18.3948
6. Shevchenko, S., Skladannyi, P., & Martseniuk, M. (2019). Аналіз та дослідження характеристик антивірусного програмного забезпечення, стандартизованого в україні. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(4), 62–71. https://doi.org/10.28925/2663-4023.2019.4.6271

Робота виконана під науковим керівництвом ст. викладача
БЕБЕШКА Б.Т.

ДОСТУПНІСТЬ ВЕБОРІЄНТОВАНИХ НАВЧАЛЬНИХ ПЛАТФОРМ

БІЛЬСЬКА А., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади впровадження, налаштування та покращення доступності. Зазначено актуальність впровадження доступності для онлайн-освітніх платформ. Розглянуто шлях розробки веобрієнтованої навчальної платформи з точки зору інтернет-доступності.

The article covers the basics of implementing, configuring, and improving web accessibility. The relevance of the implementation of accessibility for online educational platforms is indicated. The way to develop a web-oriented educational platform from the point of view of Internet accessibility is outlined.

Актуальність. У період з початку COVID-19 і до сьогодні, школярі, студенти та викладачі періодично вимушені навчатися у дистанційному або змішаному режимі у зв'язку із заходами безпеки. Це спричинило стрімкий зріст використання навчальних технологій та спеціальних освітніх онлайн-платформ таких як Всеукраїнська школа онлайн, Moodle, Microsoft Teams та Google Classroom. Все більше навчальних закладів оновлюють свої вебсайти та створюють власні освітні платформи, адже тепер вони відіграють провідну роль у освітньому процесі. Однак певна кількість вебсайтів та навчальних платформ минулого покоління все ще має проблеми із важливим аспектом їхнього використання – доступністю. Адже згідно з останніми дослідженнями Всесвітньої Організації охорони здоров'я якість зору серед дітей та дорослих продовжує падати, а отже, проблема доступності це тепер не лише додатковий бонус до просування вебсайту – це пряма необхідність.

Метою статті є дослідження доступності та її аспектів на прикладі навчальних веборінтованих платформ.

Об'єктом дослідження є розробка доступної веобрієнтованої навчальної платформи.

Предметом дослідження є вебдоступність в освіті.

Аналіз попередніх досліджень. Дослідженню вебдоступності, доступності освітніх платформ та розробки сучасних веборієнтованих платформ присвячені праці вітчизняних та іноземних науковців: Т. М. Винарчук, Л. Е. Гризун, Е. Дінк, І. І. Дончев, К. С.Куппусамі, М. Лі, А. М. Сущук, І. Ю Шахіна та ін.

Виклад основного матеріалу. Згідно з даними Всесвітньої Організації охорони здоров'я на 2022 рік, у всьому світі принаймні 2,2 мільярда людей мають порушення зору. [1] А журнал The Lancet Global Health передбачає, що до 2050 року кількість людей зі сліпотою в усьому світі зросте до 61 мільйона, якщо медичне суспільство не розробить нових методів лікування сліпоти [2]. З урахуванням всіх цих прогнозів ми повинні вже зараз замислитись, як полегшити життя людей з вадами зору. При цьому порушення зору – це безперечно лише один з багатьох типів порушень, що можуть ускладнювати життя, таких як вади слуху, м'язова атрофія та ін. Можливі шляхи вирішення цієї проблеми включають у себе покращення доступності різноманітних допоміжних технологій та технологічної доступності загалом, в тому числі в інтернеті.

До COVID-19 онлайн-доступність розвивалася, але повільно. Пандемія пришвидшила цей процес і значно діджиталізувала багатьох людей по всьому світу. Про це свідчить фінансова звітність компаній, що надають інтернет-послуги, наприклад, Zoom. Так, прибуток компанії у порівнянні із 2019 роком, зріс у 2020 році у майже 32 рази [3]. Такому стрімкому зросту прибутку сприяв повний або частковий перехід на дистанційне навчання та роботу у більшості країн світу. Відеозв'язок – це лише один із багатьох аспектів, який впровадився у звичайний навчальний та робочий процес. Також зросла популярність месенджерів, а сайти

організацій стали основним джерелом розповсюдження актуальної інформації, замінивши звичні дошки оголошень на робочому місці.

Тривала пандемія COVID-19 змусила школи відмовитись, від таких традиційних подій як дні відкритих дверей. Як результат, школи почали все більше звертатися до своїх вебсайтів та передових технологій, таких як віртуальні екскурсії, щоб безперервно надавати інформацію батькам, вчителям та учням. Ці інноваційні інструменти довели свою високу ефективність в залученні майбутніх школярів та батьків, незважаючи на виклики пандемії.

Крім цього Захін Мансурі, у своїй статті зазначає і декілька інших переваг наявності сучасного шкільного вебсайту:

1. Зручна взаємодія зі студентами – за допомогою веборієнтованої навчальної платформи, здобувачі освіти можуть легко увійти до свого облікового запису та перевірити успішність своєї навчальної діяльності.
2. Підтримка зв'язку з батьками та опікунами – батьки можуть бути в курсі оцінок своїх дітей, подій, розкладу, навчального плану та всього, що їх цікавить.
3. Покращення навчального досвіду – дозволяє навчатися та використовувати необхідні матеріали не лише у стінах навчального закладу, а й поза ними без ускладнень.
4. Полегшене оновлення навчальних матеріалів – викладачі можуть миттєво оновлювати навчальні матеріали до актуальних, легко повідомляти здобувачам освіти про зміни у навчальному плані, додавати необхідні до виконання завдання. Крім цього, навчальні платформи дають змогу школярам і студентам так само легко завантажувати свої домашні завдання та інші роботи.
5. Оптимізована передача інформації зі сторони шкільної адміністрації – за допомогою навчальних платформ, адміністрація завжди легко оновити актуальну інформацію про події у школі та проінформувати учнів та їхніх батьків [4].

На жаль, деякі вебзастосунки в Україні, в тому числі пов'язані з освітніми послугами, виявились неготовими до того, що тепер їхніми послугами будуть користуватися частіше в тому числі і люди з певними видами інвалідності. Разом з цим у дослідженні Центру Разумкова спільно з Фондом «Демократичні ініціативи» імені Ілька Кучеріва» виявилось, що відсутність необхідних гаджетів і низька якість інтернет з'єднання – були одними із найсерйозніших проблем в організації дистанційного навчання на початку пандемії COVID-19 в Україні [5].

Після початку повномасштабного вторгнення, українці знов були змушені стикнутися із необхідністю впровадження дистанційного навчання. А досвід попередньої діджиталізації остаточно закріпив у навчальному процесі використання вебтехнологій. Тож доступність виявляється все необхіднішою у сьогоденні, як серед здобувачів освіти та їхніх батьків, так і серед викладачів та іншого персоналу закладу освіти. Війна тим не менш обмежує використання тих чи інакших технологій та техніки.

Частина здобувачів освіти та викладачів втратили доступ до тих чи інакших технічних пристроїв, що використовували у навчанні – телефони, ноутбуки чи планшети. Запроваджені графіки відключень, так званий блекаут, поганий зв'язок спричинені військовою агресією Російською Федерацією по цивільній інфраструктурі, сприяли частковому або повному унеможливленню навчатися, використовуючи мережу інтернет. Та не всі навчальні веб-платформи України можуть працювати в умовах поганого інтернет-зв'язку та використання на мобільних пристроях. Таким чином питання веб-доступності ще ніколи не стояло так гостро для України та української освіти загалом.

Впровадження доступності на вебсайтах – це тривалий процес. Організація World Wide Web Consortium (W3C) створила так звані настанови з доступності вебвмісту (WCAG) 2.0 та 2.1, основною метою яких було створення рекомендацій по розробці більш доступного контенту для людей з інвалідністю та адаптації для людей з труднощами у навчанні та з когнітивними порушеннями на таких гаджетах як комп'ютери, ноутбуки, планшети та мобільні пристрої. При цьому у самій організації наголошують, що зробити контент повністю доступним для всіх людей – неможливо. Однак основні рекомендації та принципи, закладені

у Настановах з доступності вебвмісту 2.0 та 2.1, можуть допомогти зробити споживання вебвмісту доступнішим для ширшого кола людей [6].

Настанова базується на таких чотирьох принципах:

1. Сприйнятливість – зміст, а саме компоненти та інформація, інтерфейсу користувача має бути поданий таким чином, щоб користувачі могли вільно їх сприймати.
2. Керованість – забезпечення доступної навігації для усіх користувачів, в тому числі для користувачів, що користуються клавіатурою, комп'ютерною мишкою та іншими допоміжними технологіями.
3. Зрозумілість – кожен користувач має зрозуміти контент та дизайн, які впроваджені на веб-сайті.
4. Надійність – розробка вебзастосунку має передбачати, що його контент буде відображатися однаково якісно і надійно у всіх браузерах та пристроях, в тому числі при використанні допоміжних технологій [7].

WCAG – це не єдині настанови із рекомендаціями по поліпшенню доступності. Серединших відомих настанов і стандартів є також Настанова з розробки доступних мобільних інтерфейсів від Funka, Настанова з мобільної доступності від BBC та Настанови по розробці вебсайтів для мобільних пристроїв від Університету Остін. Та так чи інакше, всі перелічені вище рекомендації базуються або включають у себе настанови WCAG, тому ми базуємося у цій статті саме на них.

Консорціум Всесвітнього павутиння виділяє такі основні етапи впровадження веб доступності:

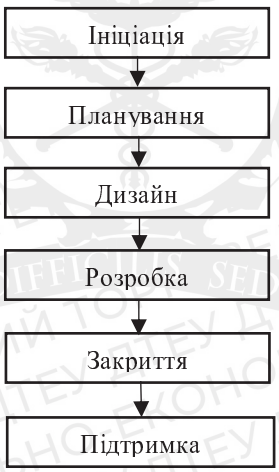


Рис. 1. Етапи впровадження доступності при створені проєкту

Використовуючи вище наведені етапи впровадження доступності, розберемо їх детальніше на прикладі створення веб-орієнтованої навчальної платформи.

Отже, перший пункт – ініціалізація проєкту. На цьому етапі, керівник відповідальний за успіх доступного веб-проекту, має впевнитись, що кожна із зацікавлених та виконавчих сторін розуміє свою роль та обов'язки на кожному з етапів розробки веб-застосунку. Крім цього саме на цьому етапі необхідно розглянути юридичні вимоги та політику щодо доступності, в нашому випадку в Україні. А також доцільно розробити внутрішню політику та план впровадження та проаналізувати рівень розуміння доступності всередині організації і надати можливість пройти навчання, якщо це необхідно.

В нашому випадку, візьмемо настанови WCAG як основу для розробки політики впровадження. Мінцифри України підтримало WCAG, про це свідчить офіційний переклад настанов на українську мову від 23 лютого 2023 року. На цьому етапі важливо також зрозуміти

проблеми, з якими можуть стикнутися учні, викладачі, батьки та адміністрація школи. За даними WebAIM найчастішими невідповідностями з нативами WCAG серед домашніх сторінок у 2022 році є:

- Низька контрастність тексту (83,9%)
- Відсутність альтернативного тексту (55,4%)
- «Пусті» посилання (50,1%)
- Відсутність підписів до форм (46,1%)
- «Пусті» кнопки (27,2%)
- Відсутність вказаної мови документа (22,3%)

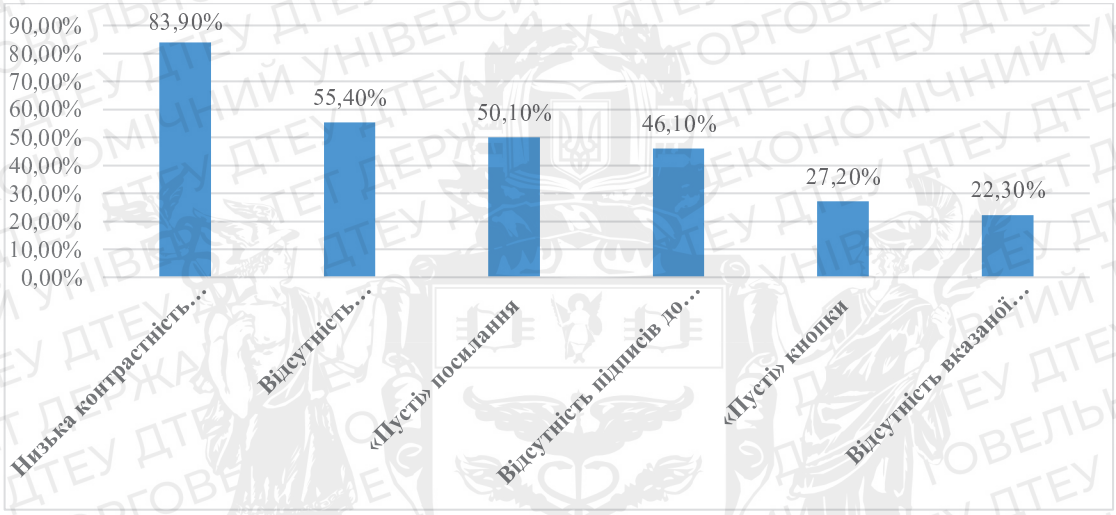


Рис. 2. Найчастіші невідповідності з нативами WCAG серед домашніх сторінок у 2022 р.

Окрім перелічених вище помилок, у звіті перелічені також такі часті невідповідності як порушена структура заголовків, відсутність ARIA-атрибутів, неоднозначний текст посилання, непрацюючі посилання «пропустити», недійсний тип документа [8].

Тож можемо зробити висновок, що в першу чергу, необхідно звернути увагу саме на ці проблеми при створенні дизайну та безпосередній розробці. Наприклад, проконтролювати, щоб контрастність тексту була достатньою або на сайті була додаткова кнопка для збільшення контрастності тексту. Кнопки та посилання працювали та були оснащені необхідними ARIA-атрибутами, такими як aria-label, до прикладу додати підпис «Натисніть, щоб повернутися на головну сторінку» для SVG-іконки з зображенням будинку. До того ж, необхідно буде впевнитися, що всі зображення на вебсайті містять альтернативний текст, наприклад «Шкільна ярмарка у головному холі школи – 2023 рік».

Крім цього, на даному етапі необхідно визначитись із приблизним переліком інструментів, які дозволять досліджувати рівень доступності під час створення вебзастосунку. Серед таких інстументів можуть бути Lighthouse у Google Developer Tools, ARIA від Equally AI та UserWay Tools.

Наступним етапом впровадження доступності є планування. На цьому етапі необхідно спланувати бюджет впровадження доступності. У бюджет мають входити витрати на платне програмне забезпечення для оцінки рівня доступності, тестування вебдоступності веборієнтованої навчальної платформи людьми з обмеженими можливостями, а також витрати на навчання розробників, дизайнерів та інших людей, залучених до створення проєкту. Наразі, існує доволі багато безкоштовних інструментів для оцінки рівня доступності та підняття

обізнаності про доступність загалом. В нашому випадку, основні витрати будуть складати із залучення людей з обмеженими можливостями до тестування. Бажано буде залучити до тестування на добровільній основі безпосередньо школярів та вчителів, які навчаються у школі та мають певні вади зору, слуху чи інше.

На цьому етапі також важливо запланувати проведення тестування на кожній стадії розробки проєкту, в тому числі людьми з обмеженими можливостями. Наприклад, тестування макету та кожної нової версії навчальної веб-платформи. Раннє заплановане тестування, допоможе ефективно управляти часом та бюджетом при розробці, а також постійно відслідковувати рівень якості та швидко помітити невідповідності із запланованою технічною специфікацією.

Наступний етап – дизайн. Дизайнери відповідають за графічний дизайн і дизайн інтерфейсу користувача веб-сторінок і програм. Включення доступності на початку створення технічних специфікацій є обов'язковим для того, щоб гарантувати, що кольори, розмір шрифту, дизайн інтерфейсу відповідають вимогам доступності. Вибір доступних технологій на самому початку розробки робить процес набагато ефективнішим. Оцінка ранніх прототипів дизайну допомагає визначити аспекти користувацького досвіду, які будуть добре працювати, і знайти потенційні бар'єри доступності.

У той же час слід звернути увагу на зміст. Зрозумілий і доступний для людей з обмеженими можливостями зміст є фундаментальним аспектом веб-доступності, і його слід враховувати при розробці проекту. Отже, контент має буде написаний таким чином, щоб охопити та бути зрозумілим всім користувачам, а його зовнішній вигляд має бути розроблений професійними дизайнерами з урахуванням вимог доступності. Крім цього, бажано, щоб інформація, особливо освітнього характеру, дублювалася у мінімум двох видах. До уроку має бути можливість прикріпити декілька матеріалів, наприклад, відеоурок і стаття до неї – таким чином, інформацію зможуть легко засвоїти одночасно і учні з вадами зору, і учні із вадами слуху, адже будуть задіяні аудіо-, відео- та текстова інформація.

В нашому випадку зміст і дизайн відіграють провідну роль у ефективному впровадженні доступності. Шкільним сайтом будуть користуватися діти різних вікових категорій, саме тому інформацію на сайті потрібно організувати таким чином, щоб всі користувачі, від наймолодших, до найстарших могли вільно зрозуміти структуру та зміст вебплатформи. Всі учні та вчителі повинні мати можливість легко і зручно ознайомлюватись з інформацією на сайті, знаходити необхідні розділи та мати розуміння того, як користуватися навчальною платформою загалом. Гарною практикою вважається додавання режиму підвищеною контрастності на сайті. А також можливість збільшувати або зменшувати шрифт. Крім цього Британська асоціація дислексії визначила, що найзручнішими для читання людям із дислексією, є шрифти sans serif, або ж ширфти без «засічок». А отже, при розробці шкільної платформи також варто звернути увагу на використання саме таких шрифтів [9].

Наступний етап – розробка. При розробці потрібно врахувати всі ті імовірні проблеми, з якими стикнуться користувачі з обмеженими можливостями. Саме на етапі розробки впроваджуються альтернативні тексти для фото, субтитри для відеоматеріалів, збільшення тексту. Та є деякі моменти, на які варто особливо звернути увагу саме на цьому етапі впровадження доступності. Наприклад, налаштування анімацій та автопрогравання. Часто в хедери навчальних платформ додають фото-слайдери, де зображені шкільні події. Це зроблено з метою покращення зовнішнього вигляду сайту та демонстрації навчальної діяльності. Однак не всі користувачі готові передивлятися анімації та об'єкти, що швидко змінюються. Таким

чином важливо додати можливість автоматичного вимкнення анімації, якщо користувач не відмітив у налаштуваннях браузера, що надає перевагу не передивлятися анімації. Це можна зробити за допомогою @media запитів у CSS. Потрібно також вимкнути автопрогравання для всіх медіа-матеріалів, таких як відео та аудіо, наприклад відеоуроки.

Також на етапі розробці важливо додати aria-label до інтерактивних елементів, сенс яких може бути не зрозумілим для скрін-рідерів. Припустимо, що на шкільній платформі буде кнопка, яка виконує функцію підняття з низу сайту догори, коли користувач прогортав основну інформацію. На таких кнопках частіше за все немає підписів, натомість використовується svg-зображення у якості демонстрації певної дії, наприклад, стрілка вгору. Для скрін-рідерів важко зрозуміти, яку функцію виконує ця кнопка. Aria-label дозволяє внести ясність, наприклад «щоб піднятись догори – клікніть». Ще однією практикою, яка вважається корисною, є додавання title-атрибутів до інтерактивних елементів. Наприклад, на нашій платформі у футері сайту будуть знаходитись іконки із зображенням телефону та поштового конверту. Розробник знає, що це посилання, які автоматично здійснюють виклик на відкривають електронну пошту. Однак для користувачів це може бути не настільки очевидно. Title допоможе прояснити функцію іконки «написати шкільній адміністрації» або «подзвонити у приймальну комісію». Звичайно, краще надати також пряме пояснення даним елементам.

Сайт також має бути доступним з девайсів всіх розмірів – від найменшого мобільного телефона, до великих екранів, таких як телевізори або інтерактивні дошки – щоб надати можливість викладачам демонструвати роботу сайту. Це важливо, щоб забезпечити здобувачам освіти на викладачам можливість продовжувати навчальний процес у будь-яких умовах. Варто також зауважити, що у мобільній версії тайтли не відображаються, тому, у деяких випадках, потрібно буде написати пояснення до інтерактивних елементів з неочевидною функцією прямо. Варто врахувати, що сайтом можуть користуватися люди з обмеженим інтернетом, тому розробку варто оптимізувати таким чином, щоб сайт міг швидко вантажитись навіть при поганій якості інтернету та зв'язку. Важливо налаштувати можливість зручно переміщатися по сайту не лише за допомогою комп'ютерної миші, а також тачпаду та клавіатури. Останнє доцільно зробити за допомогою правильної tab-індексації. І безперечно потрібно подбати про те, щоб веборієнтована навчальна платформа був кросбраузерною, тобто відображалася та працювала однаково якісно у всіх браузерах.

Передостанній етап – закриття проєкту. Консорціум Всесвітнього павутиння рекомендує відзначити впровадження доступності – як досягнення, а також задокументувати пройдені кроки задля подільної ефективної роботи над іншими проєктами. Однак, коли веборієнтована навчальна платформа повністю створена, важливо також розуміти, що стандарти веб-доступності поступово змінюються та потребують роботи та підтримки сайту.

З цього випливає останній пункт – підтримка проєкту. На самому початку існування інтернету, в нас не було можливість робити вебзастосунки такими інтерактивними, якими ми знаємо їх зараз. Технології невпинно розвиваються, а потреби користувачів постійно зростають разом із ними. Важливо проводити постійне тестування веб доступності із кожною зміною дизайну та додавання нового функціонала. Безперечно з кожним роком з'являються і все новіші методики викладання, змінюються рекомендації щодо проведення навчального процесу, умови в яких приходиться працювати вчителям та вчитися здобувачам освіти. Все це впливає на виникнення і нових вимог до вебдоступності, а також зміну старих.

Висновки. Отже, веб доступність є критично важливою для забезпечення доступу до вебресурсів для всіх користувачів, включаючи людей з обмеженими можливостями. Це особливо важливо для веборієнтованих навчальних платформ та шкільних вебсайтів, оскільки ці ресурси можуть забезпечити рівний доступ до освіти для усіх здобувачів освіти та можливості для робити для вчителів з обмеженими можливостями. Стандарти WCAG надають практичні настанови по розробці та дизайну вебсайтів, що дозволяють забезпечити вебдоступність на високому рівні. Основні аспекти веб-доступності включають забезпечення доступності для всіх типів користувачів, включаючи людей з обмеженнями, забезпечення сумісності з допоміжними технологіями та забезпечення доступності для різних типів пристроїв та платформ. Забезпечення веб-доступності є важливим кроком у забезпеченні рівних можливостей та доступу до освіти для всіх людей. І наразі однією з задач діджиталізації освіти має стояти і цей важливий аспект інклюзивності для всіх учнів, а також надання гідних умов праці для всіх працівників закладів освіти.

Список використаних джерел

1. World Health Organization, Blindness and vision impairment \\ Режим доступу: https://www.who.int/news-room/fact-sheets/detail/blindness-and-visual-impairment (останнє звернення 31.03.2023).
2. The Lancet Global Health, Trends in prevalence of blindness and distance and near vision impairment over 30 years: an analysis for the Global Burden of Disease Study \\ Режим доступу: https://www.thelancet.com/action/showPdf?pii=S2214-109X%2820%2930425-3 (останнє звернення 31.03.2023).
3. Mansoor Iqbal, Zoom Revenue and Usage Statistics (2023) \\ Режим доступу https://www.businessofapps.com/data/zoom-statistics/ (останнє звернення 31.03.2023)
4. Sahin Mansuri, Importance of An Educational Website Post Pandemic \\ Режим доступу: https://www.perceptionsystem.com/blog/benefits-of-educational-web-development/ (останнє звернення 31.03.2023)
5. Центру Разумкова, Фонд «Демократичні ініціативи» імені Ілька Кучеріва», освіта і пандемія: що українці думають про дистанційне навчання та як оцінюють ЗНО \\ Режим доступу: https://dif.org.ua/en/article/education-and-the-pandemic-the-attitudes-of-ukrainians-towards-distance-learning-and-external-independent-testing (останнє звернення 31.03.2023)
6. World Content Accessibility Guidelines, Настанови з доступності вебвмісту (WCAG) 2.1 \\ Режим доступу: https://www.w3.org/Translations/WCAG21-ua/ (останнє звернення 31.03.2023)
7. Міністерство цифрової трансформації України, Міжнародні практики щодо доступності мобільних застосунків державних органів влади \\ Режим доступу: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Accessibility_Goverment_UKR_final.pdf (останнє звернення 31.03.2023)
8. The WebAIM Million, The 2023 report on the accessibility of the top 1,000,000 home pages \\ Режим доступу: https://webaim.org/projects/million/ (останнє звернення 31.03.2023)
9. British Dyslexia Association, Dyslexia friendly style guide \\ Режим доступу: https://www.bdadyslexia.org.uk/advice/employers/creating-a-dyslexia-friendly-workplace/dyslexia-friendly-style-guide (останнє звернення 31.03.2023)

Робота виконана під науковим керівництвом кандидатки педагогічних наук, доцента КОТЕНКО Н. О.

ЕТАПИ МОДЕЛЮВАННЯ ВОРОНКИ ПРОДАЖІВ

БУР'ЯНОВ О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні етапи процесу моделювання воронки продаж, описи а аналіз програмного забезпечення інформаційних платформ воронки. Запропоновано та описано модель діаграми класів програмного забезпечення воронки продаж.

The article presents the main stages of the sales funnel modeling process, descriptions and analysis of the information platform software for the funnel. Model class diagrams for the sales funnel software are proposed and described.

Актуальність моделювання програмного забезпечення інформаційної платформи воронки продажів полягає в тому, що сучасні бізнес-процеси мають значну частину, яка пов'язана з продажами товарів/послуг та маркетингом. Воронка продажів є ефективним інструментом для підвищення продажів та оптимізації бізнес-процесів. Програмне забезпечення для інформаційної платформи воронки продажів завдяки керуванню процесами продажів, допомагає аналітику компанії відстежувати клієнтську базу, аналізувати дані та підвищувати ефективність продажів.

Метою статті є дослідження питань, пов'язаних з моделюванням програмного забезпечення для інформаційної платформи воронки продажів, а також розробка ефективної моделі класів програмного забезпечення, яка б відповідала потребам сучасного бізнесу.

Об'єктом дослідження є інформаційна платформа воронки продажів, яка включає в себе різні компоненти програмного забезпечення.

Предметом дослідження є моделювання програмного забезпечення для інформаційної платформи воронки продажів.

Аналіз попередніх досліджень. Дослідженню особливостей використання інформаційна платформи воронки продажів для управління маркетинговою діяльністю присвячені праці українських науковців В. В. Сірополко, Є. В. Галас, І. О. Жарська, О.Є. Воскресенська, В.В. Шукліна, І. Румник, С. Пижьянов.

Виклад основного матеріалу. Воронка продажу – це метод, який використовують компанії для просування товарів чи послуг на ринку, з метою підвищення кількості продажів. Цей метод здійснюється в послідовному перенесенні потенційних клієнтів через кілька етапів продажу з поверненням їх на реальних покупців.

Етапи моделювання воронки продажу можуть варіюватись у зв'язку з компанією та її продуктом, але загалом вони включають такі етапи:

1. Ознайомлення з продуктом/брендом – на цьому етапі покупець дізнається про продукт або бренд компанії, можливо, через рекламу, соціальні медіа, пошукову рекламу тощо.
2. Зацікавленість – якщо потенційний клієнт виявляє зацікавленість у продукції компанії, він переходить до цього етапу, де має змогу докладніше вивчити товари/послуги компанії.
3. Оцінка – потенційний клієнт оцінює продукти/послуги компанії, порівнює її з конкурентами, оцінюється про ціни, доставку та інші важливі параметри.
4. Рішення – на цьому етапі потенційний клієнт приймає рішення про купівлю продукту/послуги.
5. Придбання – потенційний клієнт стає реальним покупцем та безпосередньо виконує придбання товарів/послуг.
6. Післяпродажне обслуговування – компанія забезпечує післяпродажне обслуговування та підтримку клієнтів.

Воронка продажу може допомогти компанії зрозуміти, на якому етапі їхні клієнти застрягають та як можна покращити процес продажу. Використання воронки продажу компаніями знижує витрати на маркетинг та збільшує ефективність рекламної кампанії.

Існує багато програмних платформ, які допомагають моделювати та аналізувати воронку продажів. Ці платформи можуть створювати воронки продажу та відслідковувати кожен етап воронки, які допомагають компаніям аналізують та покращити продаж їхніх товарів/послуг.

Розглянемо детальнішу інформацію про наявні програмні платформи для моделювання воронки продажу.

Pipedrive – це платформа для управління продажами та контактами з клієнтами, яка надає інструменти для створення та аналізу воронки продажів, а також планування та відстеження продажів. Pipedrive пропонує різні плани з сервісними функціями для компаній різних розмірів.

На Pipedrive можна створити воронку продажу та відстежувати кожен етап, додавати контакти та створювати завдання для продавців. Також на платформі є інструменти для аналізу ефективності воронки продаж, планування продажів та відстеження досягнення цілей.

Переваги:

- простий та зручний інтерфейс, який дозволяє легко відстежувати воронку продажу;
- можливість настроювати та адаптувати інструмент під потреби конкретного бізнесу;
- можливість налаштувати електронні листи та автоматизовані кампанії.

Недоліки:

- обмежені можливості в аналізі даних та статистики;
- обмежені можливості в налаштуванні робочих процесів.

Zoho CRM – це інструмент для управління відносинами з клієнтами, який включає інструменти для створення та аналізу воронки продажу, а також автоматизації маркетингу та продажів. Zoho CRM пропонує різні плани з додатковими функціями, які підходять для різних бізнесів.

На Zoho CRM можна створити воронку продажу та відстежити кожен етап, відправити електронні листи та створити завдання для продавців. Також на платформі є інструмент для аналізу ефективності воронки продаж, збору та обробки даних про клієнтів, автоматизації маркетингу та багато іншого.

Переваги:

- широкий функціонал та можливості для управління продажами та воронкою продажів;
- можливість налаштувати додаткові інструменти та забезпечити інтеграцію з іншими платформами;
- широкі можливості в налаштуванні робочих процесів.

Недоліки:

- Складний інтерфейс, який можна забрати більше на час вивчення;
- Відносно висока вартість.

HubSpot – це платформа для маркетингу та продажів, яка надає інструменти для створення воронок продажів та аналізу їх ефективності. HubSpot пропонує безкоштовний план для початківців, а також платні плани зі швидкими функціями, які підходять для компаній різних розмірів.

На HubSpot можна створити воронку продажу та відстежувати кожен етап, створювати електронні листи та автоматизовані кампанії, відстежувати поведінку користувачів на сайті та забезпечувати їхнє задоволення після покупки. Також на платформі є інструменти для аналізу ефективності воронки продаж, збору та обробки даних про клієнтів, автоматизації продажів та багато іншого.

Переваги:

- безкоштовна версія з базовим функціоналом;

- широкі можливості для управління продажами та воронкою продаж;
- можливість використання різних інструментів для маркетингу та продажів на одній платформі.

Недоліки:

- обмежені можливості у безкоштовній версії;
- відносно висока вартість платних планів.

Salesflare – це платформа для управління продажами та CRM, яка надає інструменти для створення та аналізу продажів, автоматизації маркетингу та продажів, а також забезпечення задоволення клієнтів. Salesflare пропонує план із повними функціями для бізнесів різних розмірів.

У Salesforce можна створити воронку продажу та відслідковувати кожен етап, відправляти електронні листи та створювати завдання для продавців. Також на платформі є інструменти для аналізу ефективності воронки продажу, збору та обробки даних про клієнтів, аналізу поведінки користувачів та багато іншого.

Переваги:

- широкі можливості для управління продажами та воронкою продаж;
- можливість налаштувати інтеграцію з іншими платформами та додатками;
- великий вибір різних інструментів та додатків для роботи з даними.

Недоліки:

- висока вартість та складність інсталяції та налаштування платформи;
- складний інтерфейс, який можна забрати більше на час вивчення.

Bitrix24 - це платформа для управління бізнесом, яка надає різні інструменти для управління продажами та воронкою продажів. Бітрікс24 пропонує безкоштовні та платні плани з безкоштовними функціями для бізнесів різних розмірів.

Переваги:

- безкоштовна версія з базовим функціоналом;
- широкі можливості для управління продажами та воронкою продаж;
- широкі можливості в налаштуванні робочих процесів.

Недоліки:

- складний інтерфейс, який можна забрати більше на час вивчення;
- обмежені можливості в безкоштовній версії.

Google Analytics є єдиним із найпопулярніших та безкоштовних веб-аналітичних платформ, який дозволяє власникам веб-сайтів вимірювати та аналізувати трафік на своєму сайті, ефективність маркетингових запитів та поведінку користувачів.

Google Analytics працює за допомогою веб-аналітики встановлення на коді сайту, яка збирає дані про відвідувачів сайту та їх поведінку, наприклад кількість відвідувачів, час перебування на сайті, кількість переглядів сторінок, розташування відвідувачів, інформацію про використані пристрої та браузери, конверсії та багато іншого. інше.

Для аналізу цих даних Google Analytics пропонує широкий вибір різноманітних звітів та аналітики, які можна використовувати для оцінки ефективності веб-сайту та маркетингових проблем.

Google Analytics має можливості для створення воронки продажу та відстеження конверсій. Воронка продаж дозволяє програмувати етапи, які направляють відвідувача веб-сайту на шляху до покупки та знаходять доступні місця, де можна підвищити ефективність веб-сайту та збільшити конверсії.

Крім того, Google Analytics має можливість налаштування цілей та сегментів, які запобігають дослідженню поведінки користувачів на веб-сайті та підвищують ефективність маркетингових випадків.

Переваги:

- безкоштовна версія з базовим функціоналом;
- легка настройка та використання;
- великий вибір різноманітних звітів та аналітики;

- можливість налаштування цілей та воронки продаж;
- інтеграція з іншими продуктами Google.

Недоліки:

- обмежені можливості у безкоштовній версії;
- може вибрати багато часу на аналіз та вивчення інформації;
- не підходить для великих бізнесів, які потребують додаткових функцій та зберігання даних.

Загалом, кожна з перерахованих програмних платформ має свої переваги та недоліки, а вибір підходящої для конкретного бізнесу залежить від його потреб та можливостей. Однак, усі ці платформи мають спільний функціонал, який дозволяє ефективно управляти продажами та воронкою продажів, а також отримувати аналітику для подальшого розвитку бізнесу.

Модель воронки продажу для платформи HubSpot може включати такі етапи:

1. Потенційний клієнт: клієнт, який тільки ознайомився з інформацією про компанію або продукт / послугу.
2. Відвідувач: особа, яка відвідує сайт компанії або сторінку в соціальній мережі.
3. Лід (Lead): особа, яка залишає свої контактні дані на сайті компанії, наприклад, заповнює форму зворотного зв'язку або підписується на розсилку.
4. Перспектива (Prospect): лід, який проявляє інтерес у продукті або послузі компанії.
5. Кваліфікована перспектива (Qualified Prospect): перспектива, яка має велику ймовірність перетворитися на клієнта через показники, такі як бюджет, терміни, інтереси тощо.
6. Клієнт: особа, яка купує продукт або замовляє послугу компанії.
7. Пост-продаж: етап, на якому здійснюється підтримка клієнтів та розширення продажу через збір зворотного зв'язку та рекомендації.

Ця модель показує принципи продажу воронки для платформи HubSpot і може бути корисною при створенні маркетингових завдань та управлінні продажами на цій платформі. Але перед тим, як створювати програмне забезпечення воронки продажів, необхідно розробити модель класів (подано на рисунку 1), що описує взаємодію класів між собою та послуговує основою для створення програмного коду.

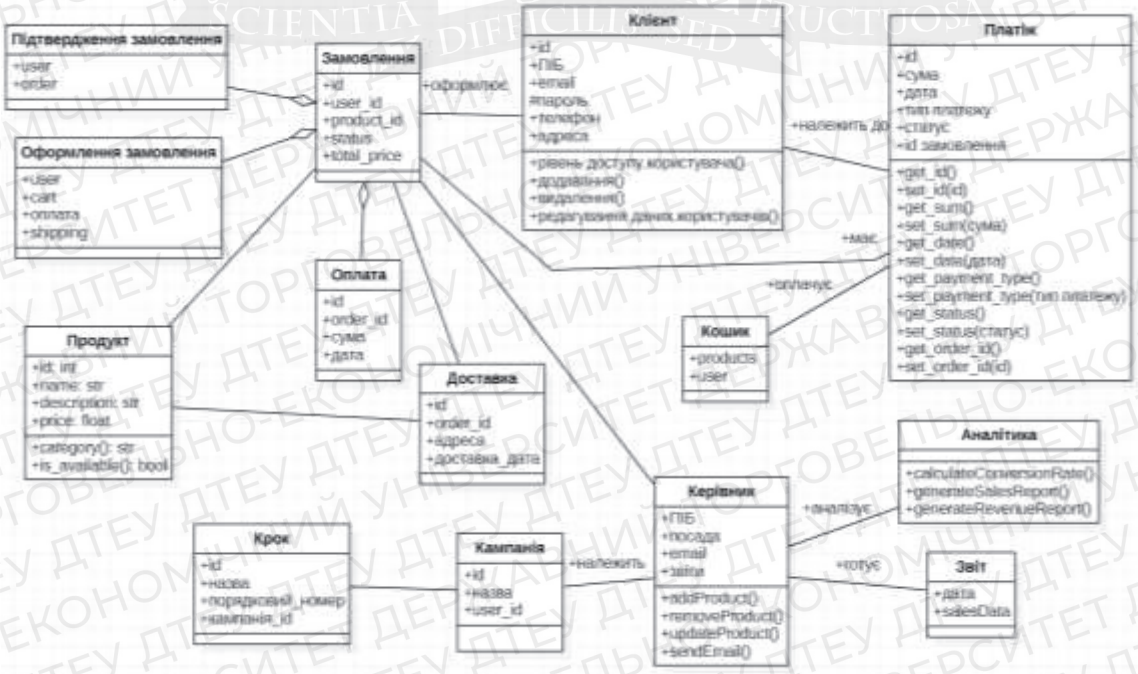


Рис. 1. Модель класів програмного забезпечення воронки продажів

Клас «Клієнт»: цей клас представляє користувачів платформи. Він має наступні атрибути:

- id (int): унікальний ідентифікатор користувача;
- ім'я (строка): ім'я користувача;
- email (строка): email-адреса користувача;
- пароль (строка): пароль користувача;
- телефон: номер телефону користувача;
- адреса: адреса користувача

Властивість:

- access_level: int - рівень доступу користувача

Клас має методи для додавання, видалення та редагування даних користувачів.

Клас «Кампанія»: цей клас представляє кампанії, які створені користувачами на платформі. Клас має наступні атрибути:

- id (int): унікальний ідентифікатор кампанії;
- назва (строка): назва кампанії;
- user_id (int): ідентифікатор користувача, який створив щось.

Клас «Крок»: цей клас представляє продаж кроків воронки для кожної кампанії. Клас має наступні атрибути:

- id (int): унікальний ідентифікатор кроку;
- назва (строка): назва кроку;
- порядковий_номер (int): порядковий номер кроку в рамках кампанії;
- кампанія_id (int): ідентифікатор кампанії, до якої належить крок.

Клас «Замовлення». Цей клас відповідає для збереження даних про замовлення користувача. Він містить наступні атрибути:

- id: унікальний ідентифікатор замовлення;
- user_id: ідентифікатор користувача, який зробив замовлення;
- product_id: ідентифікатор продукту, який був замовлений;
- status: поточний статус замовлення (наприклад, "в очікуванні", "виконується", "завершено");
- total_price: загальна вартість замовлення.

Клас «Оформлення замовлення». Цей клас представляє процес оформлення замовлення користувачем. У нього є наступні атрибути:

- user (типу User): користувач, який робить замовлення;
- cart (типу Cart): кошик, який відображає вміст замовлення;
- оплата (типу Payment): інформація про спосіб оплати;
- shipping (типу Shipping): інформація про доставку.

Клас «Підтвердження замовлення»: цей клас виводиться підтвердження замовлення користувачем. У нього є наступні атрибути:

- user (типу User): користувач, який підтверджує замовлення;
- order (типу Order): замовлення, яке підтверджується.

Клас «Оплата»: цей клас відповідає оплаті замовлення. Він містить наступні атрибути:

- id: унікальний ідентифікатор оплати;
- order_id: ідентифікатор замовлення, яке було сплачено;
- сума: сума оплати;
- дата: дата оплати.

Клас «Доставка»: цей клас відповідає для доставки замовлення. Він містить наступні атрибути:

- id: унікальний ідентифікатор доставки;
- order_id: ідентифікатор замовлення, яке було доставлене;
- адреса: адреса доставки;
- доставка_дата: дата доставки.

Клас «Продукт»: цей клас відповідає для зберігання даних про продукцію. Він містить наступні атрибути:

- id: int - унікальний ідентифікатор продукту;

- name: str - назва продукту;
- description: str - опис продукту;
- price: float - ціна продукту.

Властивості класу:

- category: str - категорія продукту;
- is_available: bool - наявність продукту на складі.

Клас «Платіж» містить такі атрибути:

- id: унікальний ідентифікатор платежу;
- сума: сума, яка була сплачена;
- дата: дата платежу;
- тип платежу: тип платежу, наприклад, оплата кредитною карткою або готівкою;
- статус: статус платежу, наприклад, оплачено або неоплачено;
- id замовлення: унікальний ідентифікатор замовлення, для якого був зроблений платіж.

Клас «Платіж» має методи:

- get_id(): повертає ідентифікатор платежу;
- set_id(id): задає ідентифікатор платежу;
- get_sum(): повертає суму платежу;
- set_sum(сума): задає суму платежу;
- get_date(): повертає дату платежу;
- set_date(дата): задає дату платежу;
- get_payment_type(): повертає тип платежу;
- set_payment_type(тип платежу): задає тип платежу;
- get_status(): повертає статус платежу;
- set_status(статус): задає статус платежу;
- get_order_id(): повертає ідентифікатор замовлення, для якого був зроблений платіж;
- set_order_id(id): задає ідентифікатор замовлення.

Клас «Платіж» пов'язаний з класами «Клієнт», «Замовлення» та «Кошик» через асоціації. Кожен об'єкт класу «Платіж» пов'язаний з об'єктом класу «Клієнт» через асоціацію «належить до» (belongs to). Кожен об'єкт класу «Платіж» пов'язаний з об'єктом класу «Замовлення» через асоціацію «має» (has). Кожен об'єкт класу «Платіж» пов'язаний з об'єктом класу «Кошик» через асоціацію «оплачує» (pays for).

Клас «Кошик»: цей клас відображає вміст кошика користувача. У нього є наступні атрибути:

- products (типу List <Product>): список продуктів, які знаходяться в кошику;
- user (типу User): користувач, який має цей кошик.

Клас «Аналітика» (Analytics) - відповідає для аналізу даних та побудови звітів про воронку продаж. Має наступні методи:

- calculateConversionRate(): обчислює конверсію на кожному етапі воронки та повертає результат у вікні словника з ключами - назвами етапів та значеннями - конверсією на цьому етапі
- generateSalesReport(): формує звіт про продажі на платформі та повертає його у вигляді документа у форматі PDF
- generateRevenueReport(): формує звіт про доходи на платформі та повертає його у вигляді документа у форматі PDF

Клас «Керівник» відображає керівника, який має доступ до звітів та статистичних даних. У нього є наступні атрибути:

- name (типу String): ім'я керівника;
- посада (типу String): посада керівника;
- email (типу String): електронна адреса керівника;
- звіти (типу List <Report>): список звітів, доступних для перегляду цьому керівнику.

«Керівник» (Manager) - відповідає керівній платформі та надає підтримку користувачам. Має наступні методи:

- addProduct(): додавання нового продукту на платформу;
- removeProduct(): видалення продукту з платформи;
- updateProduct(): оновлення даних про продукт на платформі;
- sendEmail(): відправлення електронного листа користувачам.

Клас «Звіт»: цей клас представляє звіти, які генеруються зі статистичних даних про продажі. У нього є наступні атрибути:

- дата (типу Date): дані звіту;
- salesData (типу List <SalesData>): дані про продажі, на основі яких формується звіт.

Висновок. Важливість програмного забезпечення воронки продаж для бізнесу відбувається у збільшенні ефективності продажів та зниженні витрат на маркетинг. Ось декілька важливих причин, чому програмне забезпечення продажу воронки є необхідним для бізнесу:

1. Оптимізація продажів: програмне забезпечення воронки продаж допомагає виявити слабкі місця в процесі продажу та оптимізувати його для забезпечення максимальної ефективності.
2. Збільшення конверсії: за допомогою воронки продажу можна виявити та виправити проблеми, які призводять до втрат клієнтів на кожному етапі процесу продажу. Це збільшити конверсію та збільшить кількість постійних клієнтів.
3. Оптимізація маркетингу: програмне забезпечення воронки продажів допоможе виявити, які канали маркетингу працюють найкраще. Це зменшити витрати на маркетинг збільшити ефективність користувачів.
4. Аналітика: програмне забезпечення воронки продажу забезпечує детальну аналітику процесу продажу, що дозволяє побачити всі етапи просування та продажу товарів, з подальшим аналізом про їх ефективність.

Крім того, програмне забезпечення для воронки продажів надає компаніям цінні дані та інформацію про процеси продажів. Відстежуючи поведінку клієнтів на кожному етапі воронки, компанії можуть визначати сфери, які потрібно вдосконалити, і відповідно коригувати свої стратегії. Цей підхід на основі даних допомагає компаніям приймати обґрунтовані рішення та оптимізувати процеси продажів для досягнення максимальної ефективності. А це, свою чергу, призводить до підвищення продуктивності, швидшого коефіцієнта конверсії потенційних клієнтів і, зрештою, збільшення доходу.

Загалом програмне забезпечення для воронки продажів є важливим інструментом для підприємств, які прагнуть покращити процеси продажів, підвищити ефективність і збільшити дохід. Вибравши правильне програмне забезпечення та використовуючи його можливості, підприємства можуть отримати конкурентну перевагу у своїх галузях і досягти довгострокового успіху.

Список використаних джерел

1. Румик І., Пижьянов, С. (2022). Економічні підходи до функціонування системи маркетингу на промислових підприємствах. // Вчені записки Університету «КРОК», (4(68), С. 9–19. https://doi.org/10.31732/2663-2209-2022-68-9-19
2. Воскресенська О.Є., Шукліна В.В. Формування маркетингової інформаційної системи підприємства // ВІСНИК ХНТУ № 4(71), 2019 р – С.141–147. https://doi.org/10.35546/kntu2078-4481.2019.4.16
3. Ways to Protect Your Company From a CRM Data Breach [Електронний ресурс]. – Режим доступу: https://www.nimble.com/blog/crm-data-breach-protection/

Робота виконана під науковим керівництвом к.т.н., доцента
РЗАЄВОЇ С.Л.

СТАН ЦИФРОВІЗАЦІЇ ЛІСОВОЇ ГАЛУЗІ УКРАЇНИ У 2022 РОЦІ

ВАСЕЧКО А., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглядається сутність та ключові досягнення процесу цифровізації лісової галузі України у 2022 році. Зазначені переваги та необхідність впровадження сучасних інформаційних платформ. Викладено результати реалізованих у 2022 році цифрових проєктів у лісовій галузі України та визначено подальші напрямки їх розвитку.

In this article considers the essence and the key achievements of the process of digitalization of the forestry sector of Ukraine in 2022. The advantages and necessity of introducing modern information platforms are indicated. The results of the digital projects implemented in 2022 in the forestry industry of Ukraine are presented and further directions of their development are determined.

Актуальність. В наш час цифровізація стає головною тенденцією розвитку світової економіки. Цифрові технології, що з'являються протягом останніх десятиліть, допомагають віднайти джерела підвищення ефективності та стрімкого конкурентного розвитку як окремих підприємств, так і галузі в цілому.

Одним із інструментів інтеграції України до ЄС та її виходу на світовий ринок є розвиток цифрової економіки та формування електронного середовища економічних відносин.

В Україні щороку видається більше 40 000 лісорубних квитків і 110 000 сертифікатів про походження лісоматеріалів [1]. Для цих бізнес-процесів притаманні 2 речі: супроводження документацією у паперовому форматі та застарілі дозвільні процедури. Перехід цих потоків документів у цифровий формат не тільки полегшить роботу всім суб'єктам господарювання у лісовому господарстві, а і забезпечить прозорість на всіх етапах документообігу та унеможливить операції із «сірою» деревиною.

Метою статті є дослідження процесу цифровізації лісової галузі України у 2022 році з метою створення сучасних інформаційних платформ, уніфікації процесів функціонування галузі, спрощення механізмів взаємодії з громадянами та учасниками ринку, забезпечення прозорості та безпеки даних і процесів, а також залучення міжнародних партнерів та інвесторів до лісового ринку України.

Об'єктом дослідження є лісова галузь України.

Предмет дослідження – стан цифровізації лісової галузі України у 2022 році.

Аналіз попередніх досліджень. Питанням розвитку та реформування лісової галузі України присвятили свої праці такі вітчизняні дослідники, як Фурдичко О.І., Бобко А.М., Дребот О.І., Дзюбенко О.М., Карпук А.І. та ін. Чимало зарубіжних теоретиків та практиків присвятили свої дослідження розвитку цифрової економіки загалом, серед них можна виділити Б. Гейтса, С. Гантінгтона, Е.Тоффлера, А. Томпсона та ін.

Виклад основного матеріалу. Термін «цифровізація» визначений на державному рівні і трактується Кабінетом Міністрів України як насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір [2].

Для забезпечення функціонування ефективних механізмів взаємодії з суспільством, бізнесом та міжнародними партнерами Державне лісове агентство України (далі – Держлісагенство) проводить цифрову трансформацію лісової галузі України. Цифрова трансформація галузі передбачає комплексний підхід і створення фундаментальних рішень для обслуговування реальних потреб. Провідне місце у цифровізації галузі має зайняти єдина геоінформаційно-аналітична система управління лісовою галуззю - «Лісовий Портал», як

уніфіковане рішення керування процесами, послугами, реєстрами та даними про лісове господарство України.

Метою проєкту є створення сприятливих передумов, середовища та інфраструктури для розвитку лісової галузі, покращення бізнес-клімату та експортних можливостей, залучення міжнародних учасників ринку та інвесторів за рахунок digital-трансформації системи управління на основі впровадження єдиної геоінформаційно-аналітичної системи, що забезпечить створення і зберігання та оприлюднення інформації у сфері лісового господарства України.

Завдання проєкту:

- розробка методології управління галуззю за допомогою цифрових інструментів врядування на основі кращих світових практик, залучення експертних та фінансових ресурсів до науково-дослідної діяльності;
- аналіз та надання пропозицій для внесення змін до законодавства України щодо використання цифрових систем та послуг в лісовій галузі;
- розробка технічних вимог (ТВ), технічного завдання (ТЗ) та техніко-економічного обґрунтування проєкту «Лісовий портал»;
- проведення комунікацій та маркетингових заходів на національному та міжнародному рівнях для інформування та просування ідей інвестування в науково-технічний комплекс України, зокрема проєкт «Лісовий портал»;
- поетапна розробка та впровадження Єдиної геоінформаційно-аналітичної системи «Лісовий портал», приведення бізнес-процесів, даних, електронного документообороту до вимог системи. Спрощення пошуку, надання та обміну інформацією, оформлення дозвільних документів тощо;

Для упорядкування всієї інформації та функціональних можливостей «Лісового порталу» він має складатися із логічних модулей, що будуть реалізовуватись та вводитись в дослідну експлуатацію поетапно (рис.1).

Рис.1 Структура «Лісового порталу»

Серед таких модулей варто відмітити наступні:

- отримання всіх дозвільних документів для лісової та мисливської галузі в електронному вигляді, таких як лісорубний квиток, сертифікат, посвідчення мисливця, контрольна картка, ліцензія, паспорти тварин, лісовий квиток;
- прозорі механізми контролю за рухом деревини (Електронний Облік Деревини 2.0);
- особисті кабінети лісокористувачів та учасників ринку;

- моніторинг лісових пожеж у режимі реального часу. Система повинна складатися з пожежних вишок з обладнанням та відповідним програмним забезпеченням з побудовою нейронних зв'язків для самостійного навчання виявлення вогню чи диму;

- єдина система реєстрів (лісорубні квитки, сертифікати походження, ТТН, електронні чіпи, інформація із земельних кадастрів, матеріали таксації, реєстри мисливської галузі);

- функціонал для проведення онлайн-торгів деревиною;

- система електронного документообігу між суб'єктами господарювання;

- інтерактивна карта озеленення країни. Окремий проєкт дистанційного зондування Землі за допомогою технології LIDAR (Light Identification, Detection and Ranging) для проведення інвентаризації кількісних та якісних характеристик українських лісів. Технологія дозволить вперше в історії України отримати максимально точні дані про запас деревини, площу лісів України та їхні кількісні та якісні характеристики, а також створити 3D карту українських лісів;

- мережа стандартизованих внутрішньо-галузевих веб-сайтів державних підприємств;

- система аналітики та фінансового аудиту для оцінки діяльності суб'єктів господарювання;

- доступ громадськості до відкритих даних.

Розглянемо більш детально ключові модулі «Лісового порталу», які були реалізовані у 2022 році.

Інтерактивна карта озеленення країни. Необхідність у наявності актуальної, регулярно оновлюваної, змістовно однотипної, картографічно представленої інформації про поширення лісів на всій території України є очевидною для багатьох сфер наукової та практичної діяльності. Незважаючи на тривалий за часом і значний за обсягом отриманої інформації досвід вивчення лісів, в Україні це питання досі не є повністю вирішеним. Востаннє державний облік лісів України проводився ще в 2010 році [3]. Він носив переважно статистичний характер і не супроводжувався картографічними матеріалами. В свою чергу це викликає наступні проблеми:

- відсутність оцифрованих даних про кількісні та якісні характеристики українських лісів, що дозволяє зловживати та маніпулювати даними;

- застарілі методи інвентаризації лісів з впливом людського фактору, який дає похибку при прорахунку до 20%;

- відсутність достатнього контролю за незаконними рубками;

- відсутність єдиного офіційного картографічного модуля по лісах;

- відсутність точних даних дуже ускладнює прогнозувати та планувати розвиток лісів України.

Таким чином, в Україні залишається нагальною потреба в створенні актуальної маски лісів, яка б охоплювала всю територію України, була створена за єдиною методологією, постійно та оперативно оновлювалася і уточнювалася, по можливості максимально інтегрувала інші джерела інформації про просторовий розподіл лісового покриву, була доступною для широкого використання в практичних і наукових цілях. Основою для створення такої маски лісів мають бути дані дистанційного зондування Землі.

Тому в Держлісагенстві ініціювали роботу з дешифрування космічних знімків з метою створення актуальної карти лісів України на основі наявних доступних даних дистанційного зондування Землі за допомогою лазерних імпульсів *(LIDAR)*. Результат роботи дасть можливість визначити дійсні площі, які вкриті лісовою рослинністю в Україні, незалежно від того, в чиєму підпорядкуванню та власності вони знаходяться (в тому числі й ті лісові ділянки, власники яких не встановлені).

В якості вихідних матеріалів для створення маски лісів були використані знімки супутника Sentinel-2 Level 2A. Перевагою цих знімків є одні з найкращих показників просторового розрізнення знімків серед безкоштовних даних.

На сьогоднішній момент дешифровано та створено маску лісів станом на 2020 рік (для періоду з 01.04.2020 по 31.10.2020) (рис.2).

Рис.2 Маска лісів України станом на 2020 рік

Створення маски лісів проводилося з використанням сезонних безхмарних мозаїк – вегетаційний період (квітень – жовтень). При формуванні сезонних мозаїк обиралися знімки у відповідних часових діапазонах з хмарністю не більше 30% та на всіх знімках застосовувалась маска хмар на основі продукту Sentinel-2: Cloud Probability.

За просторову основу для формування навчальної вибірки була взята розроблена вибіркова мережа для проведення Національної інвентаризації лісів [4]. Це в перспективі дозволить краще поєднати матеріали Національної інвентаризації лісів з матеріалами дистанційного зондування Землі. Дешифрування навчальних ділянок відбувалося переважно за допомогою відкритих знімків високого просторового розрізнення, наявних в Google Earth Pro, з використанням програмного забезпечення OpenForis Collect Earth. Додатковим джерелом для дешифрування навчальних ділянок були знімки високого просторового розрізнення SuperView, наявні для окремих областей України.

В результаті дешифрування встановлено, що площа ділянок, вкритих деревною рослинністю, зросла з 9,6 млн га до 11,3 млн га (приблизно на 18%). В цю різницю входять самосійні ліси за межами лісового фонду, лісосмуги, зелені насадження в населених пунктах, захисні насадження та інші категорії деревних насаджень, які були не враховані під час обліку лісів 2010 р (рис.3).

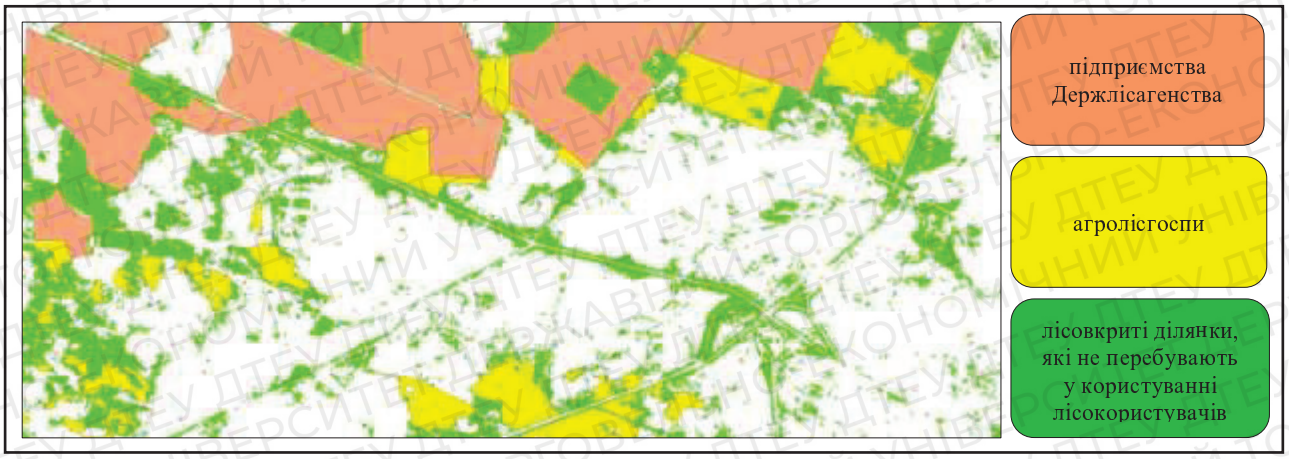


Рис.3 Встановлення актуальної площі лісів в межах лісокористувасів

Похибка дешифрування становить ±7% в цілому для всіх ділянок, дешифрованих як вкриті деревною рослинністю, та ±2% – для суцільних лісових масивів.

В результаті створення маски лісів визначено лісистість України та окремих регіонів. В більшості областей показник лісистості вийшов більший за офіційні дані 2010 р. В цілому для території України лісистість за офіційними даними становить 15,9%, а за результатами дешифрування – 18,7%.

За останні 20-30 років в Україні виникла значна кількість самосійних лісів на землях сільськогосподарського призначення, які не віднесені до лісового фонду та не обліковані (рис.4).

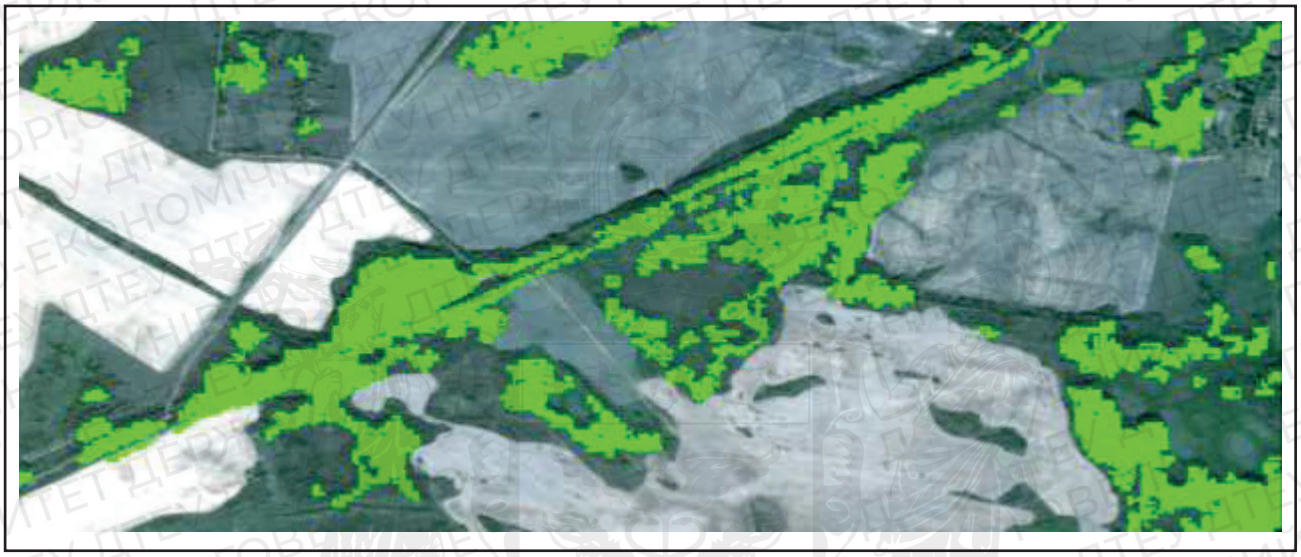


Рис. 4 Ідентифікація самосійних лісів

Створена маска лісів дає можливість після накладання шару лісокористувачів, знаходити такі ділянки та у співпраці з органами Держгеокадастру визначати власника земельних ділянок.

Подальшими напрямки діяльності у створенні інтерактивної карти озеленення України можна визначити наступні:

- уточнення та деталізація отриманих результатів з використанням інших наявних даних дистанційного зондування Землі (зокрема, доступних знімків високого просторового розрізнення; даних Sentinel-1 та інших даних дистанційного зондування Землі, отриманих за технологією SAR), а також польових даних (зокрема, матеріалів Національної інвентантаризації лісів);
- створення масок лісів для інших років (зокрема, для 2021 і 2022 рр.), формування просторово-часової маски лісів та вивчення на її основі змін лісового покриву за відповідний часовий період;
- визначення та аналіз інших характеристик лісів (зокрема, породного складу, висоти деревостанів, запасів біомаси, стану лісів тощо);
- деталізація отриманої маски лісів за лісокористувачами і категоріями лісів, виявлення лісів, які не мають офіційно визначених користувачів (зокрема, самосійних лісів).

Ще одним ключовим досягненням діджиталізації лісової галузі України у 2022 році стала цифрова трансформація одного з найголовніших бізнес-процесів лісової галузі – подачі документів на отримання і видачу лісорубного квитка. Кабінет Міністрів України визначає лісорубний квиток як основний документ, на основі якого здійснюється спеціальне використання лісових ресурсів, ведеться облік дозволених до відпуску запасів деревини та інших продуктів лісу, встановлюються строки здійснення лісових користувань та вивезення заготовленої продукції, строки і способи очищення лісосік від порубкових решток, ведеться

облік природного поновлення лісу, що підлягає збереженню, а також ведеться облік плати, нарахованої за використання лісових ресурсів [5].

Основною метою створення електронного лісорубного квитка є створення єдиного електронного реєстру лісорубних квитків з високим рівнем захисту, забезпечення ефективної і якісної автоматизації процесів внесення і обробки даних. Завданням впровадження е-лісорубного квитка є систематизація процесів обробки даних, які супроводжують створення дозвільних документів лісорубного квитка, з подальшою їх візуалізацією на мапі, що передує внесенню їх до Єдиного державного реєстру.

Основні функції е-лісорубного квитка [6]:

- забезпечення стабільної роботи всіх користувачів в режимі «онлайн» на основі Web-технології та забезпечення доступу до інформації даного продукту усім інформаційно зацікавленим особам;
- створення електронного лісорубного квитка;
- занесення даних лісорубного квитка в єдину електронну базу;
- перевірка внесених даних електронного лісорубного квитка;
- видача електронного лісорубного квитка;
- візуалізація на мапі даних щодо дозвільних документів.

У табл.1 показані ключові зміни, які відбулися в процесі трансформація лісорубного квитка в електронний вигляд.

Таблиця 1

Трансформація паперового лісорубного квитка у електронний лісорубний квиток

№ пор	Паперовий лісорубний квиток	Електронний лісорубний квиток
1	Багато ділянок в одному лісорубному квитку	Один лісорубний квиток – одна ділянка
2	Розрізненні бази (фізичні, електронні) всіх виданих електронних квитків	Єдина публічна електронна база всіх лісорубних квитків
3	Децентралізовані бази зберігання інформації	Єдина база збереження інформації про лісорубний квиток із можливістю інтеграцій до будь-яких сервісів
4	Фізичний візит з пакетом документів до територіального органу Державного агентства лісових ресурсів та центру надання адміністративних послуг за місцем провадження діяльності (далі - ЦНАП) та повторний візит для отримання виписаних документів	Онлайн заповнення заявки та отримання документів з можливістю самостійно роздрукувати при необхідності
5	Статус розгляду заявки - рекомандований лист або фізичний візит до ЦНАП/обласного управління	Статус розгляду заявки - онлайн сповіщення на e-mail та перегляд статусу заявки в особистому кабінеті.
6	Безліч розрізнених застарілих інструментів для роботи з матеріально-грошовою оцінкою	Єдиний інструмент для розрахунку матеріально-грошової оцінки
7	Термін надання послуг - 30 днів	Термін надання послуг - 10 днів
8	Тільки паперовий документ	Електронний документ із QR-кодом та можливістю друку

Закінчення табл. 1

9	Відсутній чіткий перелік необхідних документів для подачі разом із заявкою щодо отримання лісорубного квитка	Юридично зафіксований перелік всіх необхідних документів з урахуванням залежностей від виду робіт

Станом на кінець 2022 року можна виділити основні досягнення в процесі цифровізації електронного лісорубного квитка:

- запущено онлайн-платформу із доступом 24/7;
- створено єдиний електронний архів всіх лісорубних квитків;
- інтегровано державну систему електронної ідентифікації та автентифікації користувачів ID.GOV.UA;
- застосовано єдиний формат подання заявки для отримання, анулювання або відстрочення лісорубного квитка;
- пришвидшено процес обробки заявок;
- реалізовано автоматичне внесення інформації до електронного обліку деревини.

Висновки. Узагальнюючи аналіз стану цифровізації лісової галузі України у 2022 році, можна зробити висновок, що на незважаючи на воєнний стан в Україні та масову хакерську атаку у 2022 році, Держлісагенство у співпраці з Міністерством довкілля і Міністерством цифрової трансформації продовжує створювати прозоре та комфортне цифрове середовище у лісовій галузі, що буде ефективно працювати для держави та піклуватись про людей. Продовжує створювати ефективні механізми та для забезпечення розвитку потенціалу України в сучасних умовах, а також впроваджувати транспарентні цифрові послуги та процеси в цій галузі.

Лісова галузь України має величезний потенціал, тому потрібно її розвивати, щоб побудувати нову економіку, яка базуватиметься на можливостях сучасного світу.

Список використаних джерел

1. Матеріали Північного міжрегіонального управління лісового та мисливського господарства [Електронний ресурс]. – Режим доступу: https://n.forest.gov.ua/rozpochato-protses-tsifrovoji-transformatsiji-ta-tsifrovizatsiji-lisovoji-galuzi/
2. Розпорядження Кабінета Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text
3. Матеріали Рахункової палати України [Електронний ресурс]. – Режим доступу: http://www.rp.gov.ua/PressCenter/News/?id=798
4. Сторожук В. Ф. Науково-практичні аспекти проектування національної інвентаризації лісів України // Обладнання і інструмент для професіоналів. Деревообробка. – 2019 – №1. – с. 18-23.
5. Порядок видачі спеціальних дозволів на використання лісових ресурсів, затверджений постановою Кабінету Міністрів від 23 травня 2007 р. № 761 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/761-2007-%D0%BF#Text
6. Дані Державного лісового агентства України [Електронний ресурс]. – Режим доступу: https://forest.gov.ua/

Робота виконана під науковим керівництвом канд. пед. наук, доцент
КОТЕНКО Н.О.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ У ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖАХ

ВОЛЧАТОВ І., 2м курс ФІТ ДТЕУ
спеціальність «Кібербезпека та захист інформації»

У даній статті розглядаються методи авторизації користувачів у мережах VPN та описуються їх принципи роботи. Розглянуто технології, які використовуються для забезпечення безпеки та захисту інформації в мережах VPN, зокрема протоколи авторизації користувачів TACACS+, RADIUS та DIAMETER, кожен з яких має свої особливості, переваги і недоліки та може бути застосований для різних типів мереж та потреб користувачів.

This article discusses methods of user authorization in VPN networks and describes their principles of operation. The technologies used to ensure the security and protection of information in VPN networks are considered, in particular, the user authorization protocols TACACS+, RADIUS and DIAMETER, each of which has its own characteristics, advantages and disadvantages and can be applied to different types of networks and user needs.

Актуальність. У сучасному світі віртуальні приватні мережі (VPN) відіграють вирішальну роль у забезпеченні безпечного зв'язку та доступу до корпоративних ресурсів. VPN дозволяють віддаленим користувачам підключатися до приватної мережі через публічну мережу, таку як Інтернет, зберігаючи при цьому конфіденційність, цілісність і доступність даних. Однак забезпечення автентичності та авторизації користувачів VPN є критично важливим завданням. Саме тут в гру вступають такі протоколи, як TACACS+ (TACACS Plus), RADIUS (Remote Authentication Dial-In User Service) і Diameter. Ці протоколи забезпечують автентифікацію, авторизацію та облік (AAA) користувачів VPN, гарантуючи, що тільки авторизовані користувачі можуть отримати доступ до мережі та її ресурсів.

Метою статті є дослідження технологій авторизації користувачів у мережах VPN та опис принципів роботи протоколів TACACS+, RADIUS та DIAMETER з метою надання детального розуміння технологій, що використовуються для забезпечення безпеки та захисту інформації в мережах VPN.

Об'єктом дослідження є протоколи TACACS+, RADIUS та Diameter, що відповідають за авторизацію користувачів у VPN-мережах.

Предмет дослідження – технології авторизаціїї користувачів у віртуальних приватних мережах.

Аналіз попередніх досліджень. Дослідженню технології захисту інформації у віртуальних приватних мережах присвячені праці закордонних вчених: Пет Р. Калхун, Глен Зорн, Наман Мехта, В. Фахардо, Дж.

Виклад основного матеріалу. Технології захисту інформації в мережах VPN є комплексом методів та протоколів, які забезпечують захист конфіденційності, цілісності та доступності даних під час їх передачі між віддаленими користувачами та центральною мережею. Ці технології дозволяють встановлювати безпечне з'єднання між віддаленими користувачами та центральною мережею з використанням шифрування, аутентифікації та авторизації. Шифрування забезпечує конфіденційність даних, аутентифікація визначає ідентичність користувачів та перевіряє їх права на доступ до мережі, а авторизація контролює доступ користувачів до різних ресурсів мережі.

Для реалізації цих цілей в мережах VPN використовують різні протоколи, такі як TACACS+, RADIUS та Diameter. Ці протоколи забезпечують механізми аутентифікації та авторизації користувачів в мережі, а також дозволяють контролювати доступ до різних ресурсів мережі.

TACACS+, що розшифровується як Terminal Access Controller Access Control Server - це протокол безпеки, який використовується в структурі AAA для забезпечення централізованої автентифікації користувачів, які хочуть отримати доступ до мережі. Автентифікацію TACACS+ надає центральний сервер, на якому можна дозволити або заборонити доступ до комутаторів та інших пристроїв з підтримкою TACACS у мережі. TACACS використовує центральну базу даних, яка створює кілька унікальних наборів імен користувачів і паролів з відповідними рівнями привілеїв. Доступ до цієї центральної бази даних можна отримати через комутатор з консольного порту або через Telnet [1].

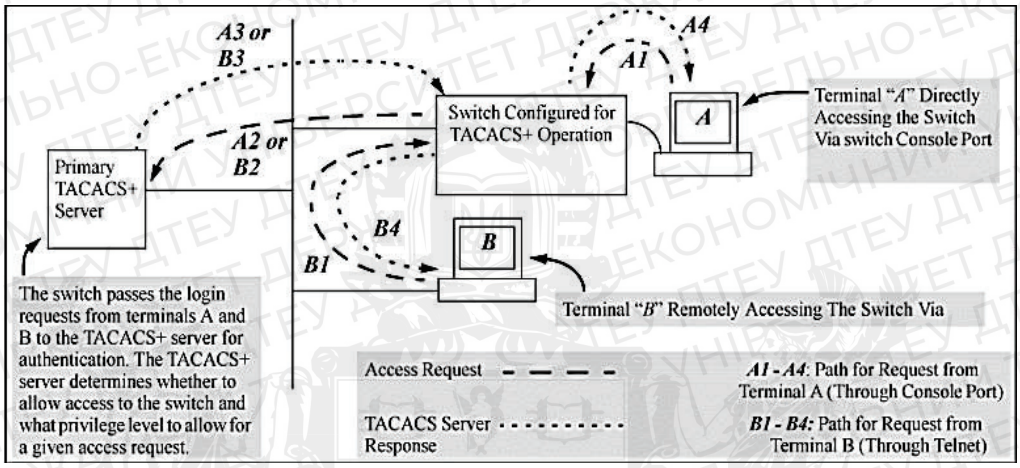


Рис. 1. Приклад роботи TACACS+

TACACS+ використовує ієрархію автентифікації, яка включає віддалені паролі, призначені на сервері TACACS+, і локальні паролі, налаштовані на комутаторі. За допомогою TACACS+ сервер може налаштувати автентифікацію для входу з правами на читання/запис або тільки читання, а також керувати спробами входу через консольний порт або Telnet. У разі збою з'єднання TACACS+ за замовчуванням використовує локально призначені паролі для контролю автентифікації.

Клієнт TACACS+ називається пристрій мережевого доступу (Nad) або сервер мережевого доступу (NAS). Пристрій мережевого доступу зв'язується з сервером TACACS+ для отримання запиту на введення імені користувача через повідомлення CONTINUE. Користувач вводить ім'я користувача, і пристрій мережевого доступу знову зв'язується з сервером TACACS+ для отримання запиту на введення пароля, який відображає запит на введення пароля користувачеві, користувач вводить пароль, після чого пароль надсилається на сервер TACACS+.

Сервер може відповісти одним з наступних повідомлень:

- Якщо введені облікові дані дійсні, сервер TACACS+ відповість повідомленням «ACCEPT».
- Якщо введені облікові дані не дійсні, сервер TACACS+ відповість повідомленням «REJECT».
- Якщо зв'язок між сервером TACACS+ та мережевим сховищем або сервером TACACS+ не працює належним чином, сервер TACACS+ відповість повідомленням «ERROR».
- Якщо потрібна авторизація TACACS+, сервер TACACS+ знову отримує запит на контакт і повертає відповідь про авторизацію «ACCEPT» або «REJECT». Якщо повертається повідомлення «ACCEPT», воно містить атрибути, які використовуються для визначення послуг, що дозволені користувачеві [2].

Для обліку клієнт надсилає серверу TACACS+ повідомлення «REQUEST», на яке сервер відповідає повідомленням «RESPONSE», в якому зазначається, що запис отримано.

Особливості протоколу TACACS+:

- Cisco розробили протокол для фреймворку AAA, тобто його можна використовувати між пристроєм Cisco та сервером Cisco ACS.
- Він використовує TCP як протокол передачі.
- Він використовує порт TCP номер 49.
- Якщо пристрій і сервер ACS використовують TACACS+, то всі пакети AAA, якими вони обмінюються, шифруються.
- Це розділяє AAA на окремі елементи, тобто автентифікацію, авторизацію та облік розділено.
- Він забезпечує більш детальний контроль ніж RADIUS, оскільки можна вказати команди, які дозволено використовувати користувачеві.
- Забезпечує підтримку обліку, але менш широку, ніж RADIUS.

Переваги:

- Забезпечує більш детальний контроль, ніж RADIUS.TACACS+ дозволяє мережевому адміністратору визначати, які команди може виконувати користувач.
- Всі пакети AAA зашифровані, а не тільки паролі, як у випадку з RADIUS.
- TACACS+ використовує TCP замість UDP. TCP гарантує зв'язок між клієнтом і сервером.

Недоліки:

- Оскільки він є власністю Cisco, тому може використовуватися тільки між пристроями Cisco. TACAS+ − відкритий стандарт RFC8907
- Менш широка підтримка обліку, ніж у RADIUS.

RADIUS − це протокол клієнт/сервер, який використовується у розподіленому режимі для захисту мереж від несанкціонованого доступу. Він зазвичай реалізується в мережах, які вимагають суворої безпеки і контролюють доступ віддалених користувачів. Протокол описує формат і механізм передачі RADIUS-пакетів, які передаються через протокол UDP по портам 1812 і 1813 для аутентифікації та обліку відповідно.

Спочатку RADIUS слугував як протокол AAA виключно для користувачів комутованого доступу. Однак, коли режими доступу користувачів розширилися, включивши в себе доступ до Ethernet та інші, RADIUS був адаптований для роботи з цими режимами доступу. За допомогою аутентифікації та авторизації RADIUS надає послуги доступу і веде облік використання мережевих ресурсів за допомогою обліку.

RADIUS має наступні характеристики:

- Модель клієнт/сервер
- Безпечний механізм обміну повідомленнями
- Хороша масштабованість [3].

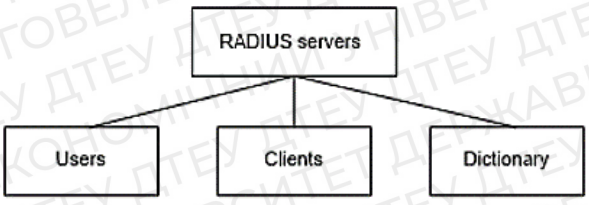


Рис. 2. Бази даних, що підтримуються RADIUS-сервером

Звичайна конфігурація RADIUS передбачає, що мережеве сховище виконує роль клієнта RADIUS, а демон-процес, запущений на комп'ютері з UNIX або Windows NT, − роль сервера RADIUS. За такої конфігурації клієнт передає дані користувача певному серверу RADIUS, а потім відповідно реагує на відповідь сервера. Коли користувач ініціює з'єднання, сервери RADIUS автентифікують користувача і надають деталі конфігурації, необхідні клієнту для надання послуг користувачеві. Крім того, RADIUS-сервер може слугувати проксі-клієнтом для інших RADIUS-серверів або різних серверів автентифікації. Зазвичай сервер RADIUS повинен підтримувати три бази даних (Рис.2).

База даних користувачів містить дані, пов'язані з користувачами, такі як імена користувачів, паролі, протоколи та IP-адреси.

На противагу цьому, база даних клієнтів зберігає інформацію про клієнтів RADIUS, таку як їхні спільні ключі та IP-адреси. Нарешті, база даних словників містить інформацію про атрибути та їхні відповідні описи значень у протоколі RADIUS.

Клієнти та сервери RADIUS використовують спільний ключ для автентифікації повідомлень, якими вони обмінюються. Цей ключ являє собою рядок символів, який є спільним для обох сторін і передається поза смугою пропускання, усуваючи необхідність незалежної передачі через мережу.

Поле автентифікатора в RADIUS-пакеті містить дані цифрового підпису для всього пакета і займає 16 октетів. Ці дані підпису генеруються за допомогою алгоритму MD5 і спільного ключа. При отриманні, приймач пакетів RADIUS перевіряє точність підпису і відкидає пакет, якщо підпис невірний. Цей механізм значно підвищує безпеку обміну повідомленнями між клієнтами і серверами RADIUS. Крім того, паролі користувачів шифруються за допомогою спільних ключів у пакетах RADIUS перед передачею, щоб запобігти крадіжці паролів у незахищених мережах. Приклад пакету RADIUS (Рис.3).

Крім того, задля підвищеної безпеки, RADIUS підтримує тонку масштабованість. Протокол залишається незмінним, навіть коли до пакетів RADIUS додаються нові атрибути. Пакети RADIUS складаються з заголовка пакета і певної кількості атрибутів, а сам протокол базується на протоколі UDP.

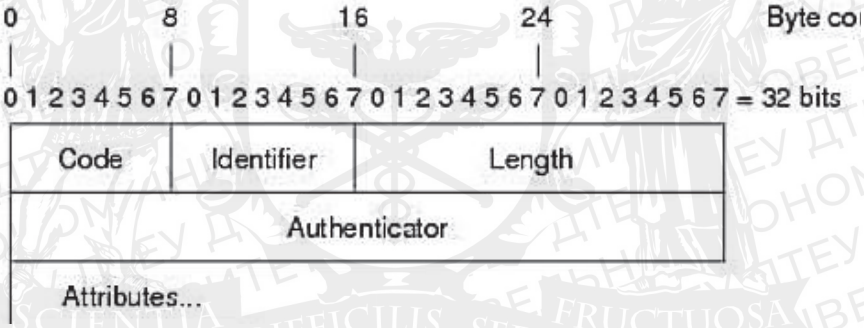


Рис. 3. Формат пакету RADIUS

Кожен RADIUS-пакет містить наступну інформацію:

- Код − поле коду складається з одного октету. Значення поля Code змінюється в залежності від типу RADIUS-пакету.
- Ідентифікатор − поле ідентифікатора складається з одного октету; воно допомагає RADIUS-серверу зіставляти запити і відповіді та виявляти дублікати запитів. Після того, як клієнт надсилає пакет-запит, сервер надсилає пакет-відповідь з тим самим значенням ідентифікатора, що й у пакеті-запиті.
- Довжина − поле довжини складається з двох октетів; воно визначає довжину всього пакета. Октети, що виходять за межі діапазону поля Length, повинні розглядатися як пробіли і ігноруватися при отриманні. Якщо довжина пакета менша за поле Length, він має бути мовчки відкинутий
- Автентифікатор − поле автентифікатора складається з 16 октетів. Першим передається старший октет; він використовується для автентифікації відповіді від сервера RADIUS. Існує два типи автентифікаторів:
  - Запит-автентифікація: Доступний у пакетах «Access-Request» та «Accounting-Request»
  - Автентифікатор відповіді: Доступний у пакетах «Access-Accept», «Access-Reject», «Access-Challenge» та «Accounting-Response» [4]

Пристрій, який функціонує як клієнт RADIUS, збирає інформацію про користувача, включаючи ім'я користувача та пароль, і надсилає цю інформацію на сервер RADIUS. Потім

RADIUS-сервер аутентифікує користувачів відповідно до отриманої інформації, після чого виконує авторизацію та облік користувачів (Рис. 4).

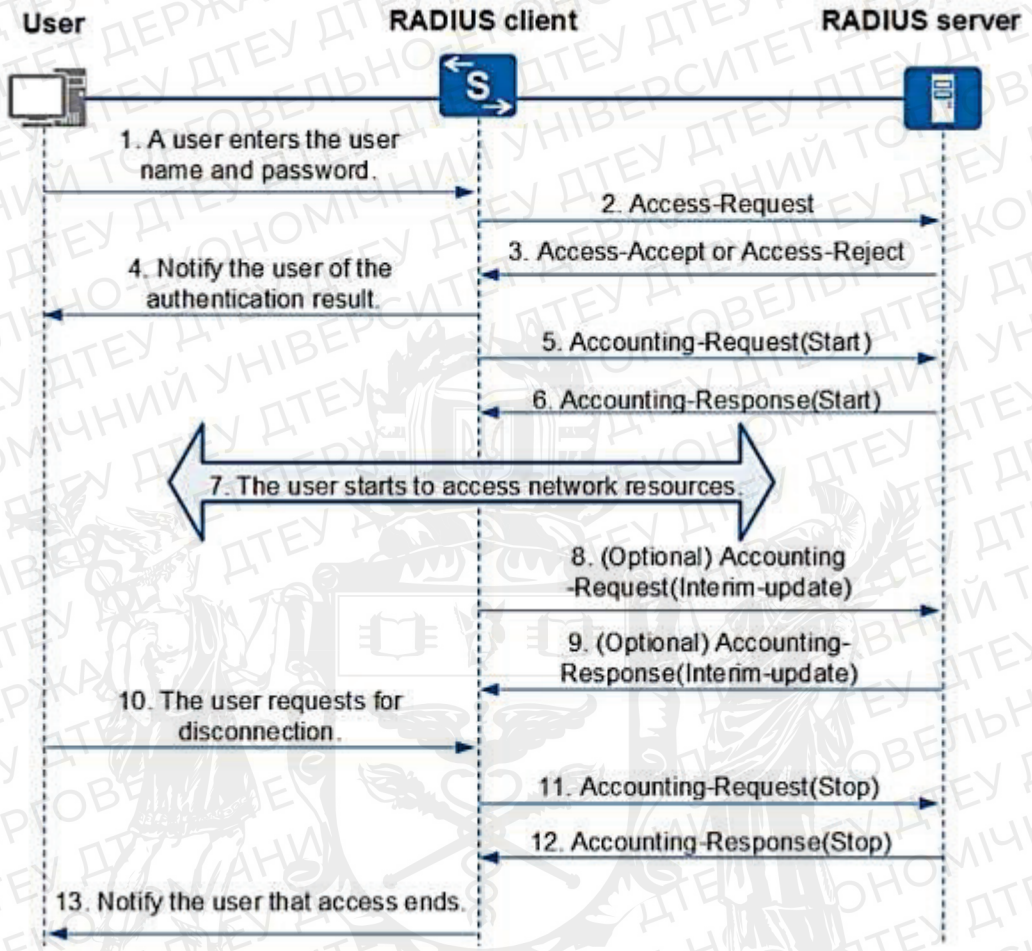


Рис. 4. Процес автентифікації, авторизації та обліку RADIUS

Переваги:

- Масштабованість: RADIUS − це масштабований протокол, який може працювати з великою кількістю користувачів і пристроїв.
- Централізована аутентифікація: RADIUS забезпечує централізований механізм аутентифікації, що полегшує управління доступом користувачів до різних мережевих пристроїв.
- Розширюваність: RADIUS є розширюваним протоколом, що означає, що його можна налаштувати для підтримки додаткових методів автентифікації, таких як одноразові паролі або біометрія.
- Інтеграція з іншими системами: RADIUS може інтегруватися з іншими системами, такими як LDAP або Active Directory, щоб забезпечити комплексне рішення для автентифікації та авторизації.

Недоліки:

- Обмежене шифрування: RADIUS не забезпечує наскрізне шифрування, а це означає, що облікові дані користувачів та інші конфіденційні дані можуть бути вразливими до перехоплення і прослуховування.
- Складна конфігурація: налаштування та конфігурація серверів і клієнтів RADIUS може бути складним і трудомістким процесом, що вимагає хорошого розуміння мережевих технологій і концепцій безпеки.
- Вразливості: RADIUS не застрахований від вразливостей безпеки, і в минулому повідомлялося про кілька випадків експлойтів і атак на сервери та клієнти RADIUS.

- Єдина точка відмови: RADIUS покладається на єдину точку відмови, що означає, що якщо сервер RADIUS вийде з ладу, користувачі можуть бути не в змозі пройти автентифікацію та отримати доступ до мережевих ресурсів.
- Обмежена функціональність: RADIUS в першу чергу призначений для аутентифікації та авторизації, і не надає додаткових функцій безпеки, таких як шифрування або виявлення вторгнень.

Diameter − це протокол, який використовується для автентифікації, авторизації та обліку в базових вузлах мереж архітектур 3G і LTE. Він є розвитком протоколу RADIUS з додатковими функціями. Протокол Diameter визначений IETF і називається Diameter Base Protocol (RFC 6733). Він забезпечує структуру для таких додатків, як доступ до мережі та IP-мобільність. Додатки Diameter розширюють базовий протокол Diameter, додаючи нові AVP (Attribute-Value Pairs) і команди для забезпечення розширених можливостей.

Вважається, що Diameter Application − це програмне забезпечення, яке забезпечує необхідну функціональність. Однак насправді це протокол, заснований на протоколі Diameter Base, визначеному в RFC 6733. Протокол Diameter base дозволяє Diameter додатку визначати свій власний ідентифікатор додатку і нові коди команд, разом з обов'язковими/необов'язковими наборами AVP, для виконання необхідної поведінки. Приклади Diameter додатків (Рис. 5).

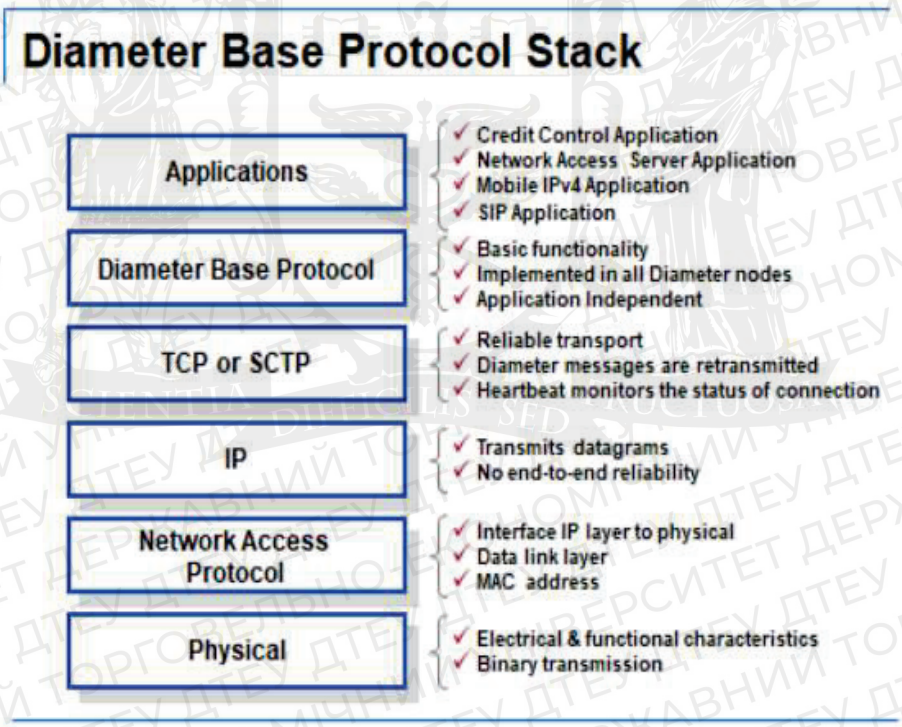


Рис. 5. Стек базових протоколів діаметру

Diameter визначається в термінах базового протоколу AAA та набору додатків. Базовий протокол забезпечує основні механізми для надійного транспортування, доставки повідомлень та обробки помилок. Він повинен використовуватися разом з додатком Diameter, який використовує послуги базового протоколу для підтримки певного типу доступу до мережі.

Протокол Diameter працює як розмова, де одна сторона задає питання («Запит»), а інша сторона відповідає («Відповідь»). Приклад обміну запитами і відповідями в протоколі Diameter (Рис. 6).

Протокол Diameter використовує модель клієнт/сервер для зв'язку між вузлами мережі. Кожного разу, коли надсилається повідомлення-запит, завжди буде отримано повідомлення-відповідь. Пакет протоколу Diameter містить заголовок повідомлення Diameter і змінну кількість пар атрибут-значення AVP (Рис. 7). Дані повідомлення зберігаються у вигляді AVP.

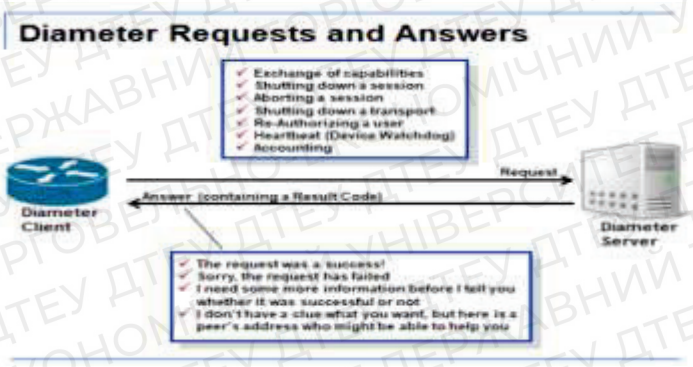


Рис. 6. Запити і відповіді Diameter

Опис різних полів формату Diameter Message Packet Format (Рис. 7):

- Version − 1 байт, версія базового протоколу Diameter Base Protocol. Значення має бути "1".
- Length − 3 байти, довжина повідомлення Diameter, включаючи всі AVP та заголовні байти.
- Flags − 1 байт, значення призначається порозрядно.
- Command-Code − 3 байти, ідентифікує кожну команду Diameter. Парі повідомлень «Запит»/ «Відповідь» присвоюється унікальний код, відомий як код команди. Значення 0-255 зарезервовано для зворотної сумісності з протоколом RADIUS.
- Application-ID − 4 байти, ідентифікує програму діаметра, для якої застосовується це повідомлення.
- Hop-by-Hop Identifier − 4 байти, використовується для зіставлення запитів з відповідями. У випадку ретрансляцій та проксі-агентів, його значення зберігається і замінюється на інший унікальний номер.
- End-to-End Identifier − 4 байти, використовується для виявлення дублікатів повідомлень. Цей ідентифікатор повинен залишатися локально унікальним протягом щонайменше 4 хвилин, навіть після перезавантажень [5, с.15–16].

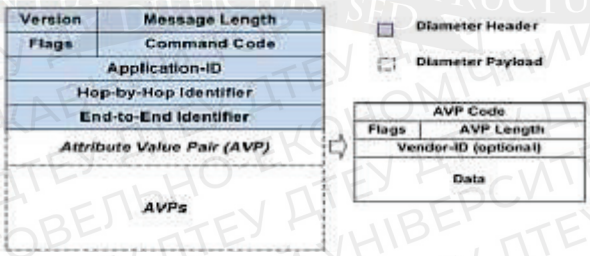


Рис. 7. Формат пакету протоколу Diameter

Переваги:

- Покращений транспорт: протокол Diameter використовує надійний транспортний рівень, такий як TCP або SCTP, який забезпечує повторну передачу втрачених пакетів на кожному кроці. Постійне з'єднання з пульсовим повідомленням на рівні програми (Watchdog-повідомлення) підтримує своєчасне обхід відмови. TCP і SCTP можуть адаптуватися до перевантаження мережі, роблячи зв'язок більш ефективним.
- Покращене проксіювання: покрокове виявлення транспортних збоїв у протоколі Diameter дозволяє здійснювати обхід відмов у потрібному місці. Проксі-сервери можуть локально обходити відмову на альтернативний наступний вузол. Після обходу відмови проксі-сервер автоматично ретранслює всі очікувані повідомлення запитів. AVP, що визначає кінцевий пункт призначення, дозволяє спрямовувати кілька транзакцій для певного сеансу на один і той самий домашній сервер.

- Покращений контроль сеансів: управління сеансами не залежить від обліку, а облікова інформація може бути перенаправлена на інший сервер, ніж повідомлення про автентифікацію/авторизацію. Завершення сеансу передається спеціальним повідомленням про завершення сеансу, а не повідомленням про зупинку обліку. Сервер може ініціювати повідомлення із запитом на завершення сеансу або повторну автентифікацію/авторизацію користувача.
- Покращена безпека: протокол Diameter забезпечує наскрізний захист за допомогою IPsec або TLS. Наскрізний захист захищає цілісність та/або конфіденційність важливих AVP через проміжні проксі-сервери.

Недоліки:

- Протокол Diameter може бути складнішим у впровадженні та налаштуванні порівняно з RADIUS через його додаткову функціональність та функції безпеки.
- Повідомлення протоколу Diameter можуть бути більшими за розміром, ніж повідомлення RADIUS, що потенційно може призвести до збільшення мережевого трафіку та зниження продуктивності.
- Протокол Diameter може бути більш ресурсоємним, ніж RADIUS, через підвищені вимоги до обробки.
- Протокол Diameter не так широко підтримується, як RADIUS, що може обмежувати його сумісність з певними мережевими пристроями та програмами.

Висновки. Аналізуючи методи авторизації користувачів у віртуальних приватних мережах (VPN), можна зробити висновок, що вибір протоколу авторизації залежить від конкретних потреб та умов використання. При виборі протоколу для захисту інформації в віртуальних приватних мережах, важливо враховувати вимоги до безпеки, масштабованості та ефективності використання ресурсів. Розглянуті протоколи авторизації користувачів, мають свої переваги та недоліки. Наприклад, TACACS+ забезпечує більш високий рівень безпеки, але потребує більше ресурсів, ніж RADIUS, що забезпечує більшу масштабованість. DIAMETER використовується в більш розподілених мережах, де масштабованість та надійність є ключовими факторами. Отже, при виборі протоколу авторизації для віртуальної приватної мережі, необхідно враховувати потреби користувачів та вимоги до безпеки, масштабованості та ефективності використання ресурсів.

Список використаних джерел

1. TACACS+ Authentication and Accounting \\ Режим доступу: https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/16-02/5200-1648_K_ASG/content/ch09.html (Останнє звернення 20.03.2023р.)
2. Configuring TACACS+ \\ Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg/configuring_tacacs_.pdf (Останнє звернення 20.03.2023)
3. How Does RADIUS Work \\ Режим доступу: https://support.huawei.com/enterprise/en/doc/EDOC1100086516#:~:text=RADIUS%20has%20the%20following%20characteristics%3A (Останнє звернення 20.03.2023)
4. RADIUS Attributes Overview and RADIUS IETF Attributes \\ Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_radatt/configuration/15-s/sec-usr-radatt-15-s-book/sec-rad-ov-ietf-attr.pdf (Останнє звернення 20.03.2023)
5. Hannes Tschofenig, Sebastien Decugis, Jean Mahoney, Jouni Korhonen, Diameter: New Generation AAA Protocol - Design, Practice, and Applications. – 2019. – с. 15 – 16.

Робота виконана під науковим керівництвом старшого викладача
КОСТЮК Ю.В.

КОНЦЕПЦІЯ МОДЕЛІ КЛІЄНТ-СЕРВЕРНОГО ДОДАТКУ ДЛЯ ПІДПРИЄМСТВА ЛОГІСТИКИ

ГАВРИЛЕНКО Г., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови модель клієнт-серверного додатку для підприємства логістики: розробку API, веб-додаток, мобільний додаток, базу даних, алгоритми оптимізації, безпеку даних, масштабованість та використання сучасних технологій.

The article discusses the basic principles of building a client-server application model for a logistics enterprise: API development, web application, mobile application, database, optimization algorithms, data security, scalability and use of modern technologies.

Актуальність. Мікросервісна архітектура стала найбільш популярною архітектурою для побудови програмних систем, В роботі розкрита важливість розробки ефективного клієнт-серверного додатку для підприємства логістики з врахуванням вимог забезпечення безпеки, оптимізації ресурсів, масштабованості та використання сучасних технологій.

Метою статті є дослідження особливостей побудови модель клієнт-серверного додатку для підприємства логістики.

Об'єктом дослідження є аспекти побудови модель клієнт-серверного додатку для підприємства логістики в розрізі розробки API, веб-додатоку, мобільного додатку, бази даних, алгоритмів оптимізації, безпеки даних, масштабованості та використання сучасних технологій.

Предмет дослідження: модель клієнт-серверного додатку для підприємства логістики.

*Виклад основного матеріалу***:** Впродовж останніх років спостерігається безперервний ріст складності логістичних процесів, посилення конкуренції на ринку та зміни клієнтських вимог. Відповідно до сучасних наукових досліджень, інформаційні технології дозволяють підвищити ефективність логістичних систем та забезпечити краще управління ресурсами [1].

Очевидним є необхідність автоматизації логістичних процесів, підвищення продуктивності, забезпечення оперативного реагування на зміни та підтримки ефективного спілкування між усіма учасниками логістичної мережі [2]. Крім того, клієнт-серверні додатки надають можливість інтеграції з різними інформаційними системами, IoT-пристроями та аналітичними інструментами для отримання оптимальних результатів у логістичних процесах та підтримки прийняття обґрунтованих управлінських рішень.

У світлі цих досліджень, створення клієнт-серверного додатку для підприємства логістики є актуальним кроком, спрямованим на підвищення конкурентоспроможності та оптимізацію бізнес-процесів.

Існує безліч підходів та моделей побудови різноманітного програмного забезпечення. Модель клієнт-серверного додатку для підприємства логістики повинна включати розробку системи, яка взаємодіє між клієнтами та сервером для ефективного управління логістичними операціями. Відповідно можливо виділити основні компоненти такої моделі:

1. Серверна частина (backend) - частина що виконується на серверах системи та не має прямої взаємодії з кінцевим користувачем. В свою чергу серверна частина має охоплювати реалізацію наступних компонентів:

- База даних - відповідальна за зберігання всіх даних про товари, склади, замовлення, маршрути, транспортні засоби, водіїв та інші логістичні ресурси. База даних є ключовим компонентом логістичної системи, оскільки вона забезпечує централізоване зберігання, управління та доступ до даних, які стосуються всіх аспектів логістичних операцій. Ефективна база даних повинна бути оптимізована для швидкого та безпечного обміну даними, підтримки

одночасного доступу до інформації для різних користувачів та гарантування консистентності даних. Сучасні технології баз даних, такі як реляційні, NoSQL та графові бази даних, пропонують різні архітектурні підходи та можливості, що можуть бути використані для досягнення цих цілей. Для підприємства логістики база даних повинна бути здатна ефективно обробляти великі обсяги структурованих та неструктурованих даних, що стосуються товарів, складів, замовлень, маршрутів, транспортних засобів, водіїв та інших логістичних ресурсів. Оптимальне проектування бази даних передбачає врахування факторів, таких як нормалізація даних, вибір відповідних індексів та використання оптимізованих запитів для забезпечення високої продуктивності та надійності системи. Застосування розподілених технологій баз даних та хмарних рішень може допомогти забезпечити масштабованість та доступність бази даних відповідно до зростаючих потреб підприємства. Інтеграція з іншими системами та джерелами даних є ще одним важливим аспектом бази даних для підприємства логістики. Наприклад, база даних може бути інтегрована з системами управління складом (WMS), системами управління транспортом (TMS) та іншими внутрішніми та зовнішніми джерелами даних, що можуть надавати актуальну інформацію про стан ресурсів, маршрути, відправлення та інші логістичні операції [3]. Це вимагає розробки ефективних механізмів обміну даними та інтеграції на рівні інтерфейсів програмування додатків (API), що дозволяє забезпечити сумісність та гнучкість інтеграційних процесів.

- API (Application Programming Interface) - інтерфейс для обміну даними між клієнтськими додатками та сервером, який дозволяє отримувати, створювати, оновлювати та видаляти інформацію про ресурси. API є ключовим компонентом для створення модульних та гнучких логістичних систем. Він дозволяє клієнтським додаткам, таким як веб-додатки, мобільні додатки та інші програмні системи, спілкуватися та обмінюватися даними з сервером та базою даних. API відіграє важливу роль у забезпеченні прозорості, інтеграції та автоматизації логістичних процесів, спрощуючи доступ до інформації та управління ресурсами для користувачів та розробників. При розробці API для логістичної системи необхідно враховувати ряд факторів, щоб забезпечити його надійність, продуктивність та безпеку. Серед цих факторів - розробка чіткої та зрозумілої специфікації API, використання стандартних протоколів обміну даними (наприклад, REST або GraphQL), оптимізація запитів та відгуків та реалізація механізмів аутентифікації та авторизації для захисту даних від несанкціонованого доступу. Крім того, підтримка гнучкості та масштабованості API є важливим аспектом для забезпечення стійкості системи до змін та росту підприємства.
- Алгоритми оптимізації - відіграють важливу роль в логістиці, оскільки вони допомагають підприємствам планувати маршрути, оптимізувати ресурси та підвищувати ефективність логістичних операцій. Відповідно до сучасних наукових досліджень, одними з найвідоміших алгоритмів оптимізації маршрутів є метод розв'язання задачі комівояжера (TSP) та методи маршрутизації з доставкою та збором (VRP) [4]. Ці алгоритми допомагають розробляти оптимальні маршрути для транспортних засобів, мінімізуючи відстань, час та витрати палива, що сприяє економії ресурсів та зменшенню негативного впливу на навколишнє середовище.

2. Клієнтська частина (frontend):

- Веб-додаток - забезпечує ефективну взаємодію між користувачами та API, що дозволяє обробляти дані логістичних систем [5]. Веб-додаток включає інтерфейс, який дозволяє персоналу компанії та клієнтам відстежувати замовлення, управляти ресурсами та переглядати статистику. Це полегшує доступ до інформації, сприяє більшій прозорості логістичних процесів та сприяє прийняттю обґрунтованих рішень. Наукові дослідження підкреслюють важливість розробки користувацького інтерфейсу, який є інтуїтивно зрозумілим та легко використовується для різних груп користувачів [6]. В запропонованій моделі рекомендовано використання сучасних технологій, таких як реактивне програмування, односторінкові додатки (SPA) та фреймворки розробки, такі як Angular та React, що дозволяють створювати високоякісні веб-додатки, які забезпечують швидкість, надійність та

безпеку інформації. Використання веб-додатків у логістичних системах стає все більш поширеним у зв'язку з перевагами, які вони надають для ефективності та роботи з клієнтами.

- Мобільний додаток - є важливим компонентом сучасних логістичних систем, оскільки він забезпечує ефективну взаємодію між водіями, іншим персоналом на місцях та центральною системою [7]. Інтерфейс мобільного додатку дозволяє швидко отримувати інформацію про замовлення, маршрути, зміни розкладів тощо, що полегшує комунікацію та роботу на різних етапах логістичного процесу. Використання мобільних додатків сприяє підвищенню ефективності та оперативності роботи персоналу, а також забезпечує можливість адаптації до змінних умов ринку та вимог клієнтів. Наукові дослідження вказують на важливість розробки мобільних додатків, які враховують потреби та вимоги різних груп користувачів, таких як водії, складський персонал, менеджери та клієнти [8]. Сучасні технології розробки мобільних додатків, такі як React Native, Flutter та Xamarin, дозволяють створювати високоякісні, кросплатформені мобільні додатки, які забезпечують швидкість, надійність та зручність використання. Інтеграція мобільних додатків у логістичні системи допомагає підприємствам підвищити рівень обслуговування, а також забезпечити гнучкість та адаптивність логістичних процесів.
- Інтеграція зі сторонніми системами: Можливість обміну даними та взаємодії з іншими системами (наприклад, системами відстеження, сервісами доставки, системами електронної комерції тощо).

Для реалізації клієнт-серверної моделі логістичного додатку важливо використовувати сучасні технології та методи, які відповідають вимогам і потребам логістичної компанії [9]. Вибір правильних технологій впливає на швидкість реалізації проекту, надійність, масштабованість та безпеку рішення. Розглянемо деякі з них:

1. Серверна частина (backend):

- Мови програмування: Python, Java, Node.js, C#, Ruby, Go - відомі мови програмування, які підходять для розробки серверних додатків.
- Фреймворки: Django, Flask, Spring Boot, Express.js, ASP.NET Core, Ruby on Rails, Gin - популярні фреймворки для розробки серверних додатків з різними можливостями та рівнем складності.
- Бази даних: PostgreSQL, MySQL, Oracle, MongoDB, Microsoft SQL Server - різні типи баз даних (реляційні, NoSQL) залежно від потреб компанії.

2. Клієнтська частина (frontend):

- Мови програмування: JavaScript, TypeScript - основні мови програмування для розробки веб-додатків та мобільних додатків (за допомогою React Native, Ionic або Flutter).
- Фреймворки: React, Angular, Vue.js, Svelte - сучасні фреймворки для створення інтерактивних веб-інтерфейсів.
- CSS-фреймворки: Bootstrap, Tailwind CSS, Material-UI, Bulma - засоби для швидкого створення гарного та зручного інтерфейсу.

При розробці клієнт-серверного додатку для підприємства логістики існує ряд аспектів, що потребують особливої уваги та врахування.

Безпека даних є одним з ключових аспектів розробки та впровадження клієнт-серверного додатку для підприємства логістики, оскільки надійність і конфіденційність інформації мають вирішальне значення для успішної роботи системи [10].

Забезпечення захисту даних клієнтів та підприємства від несанкціонованого доступу, витоку інформації та зловживань вимагає використання сучасних технологій та методів кібербезпеки, а також розробки ефективних політик та процедур управління безпекою. Наукові дослідження підкреслюють важливість розробки гнучких та адаптивних механізмів захисту даних, які можуть відповідати змінам у загрозах та вимогах ринку [11].

Основні напрямки забезпечення безпеки даних в клієнт-серверних додатках для підприємств логістики включають захист комунікацій між клієнтами та серверами за допомогою протоколів шифрування, таких як SSL/TLS, реалізацію автентифікації та авторизації користувачів на основі ролей, використання брандмауерів та інших систем захисту

мережі, а також застосування методів моніторингу та аудиту для виявлення і відстеження зловживань та атак.

Розробка та впровадження ефективних рішень з кібербезпеки в логістичних системах допомагає підприємствам забезпечити конфіденційність, цілісність та доступність даних та ресурсів, що підвищує довіру клієнентів та сприяє забезпеченню стійкості бізнесу в умовах постійно розвиваючихся кіберзагроз.

Наступним важливим аспектом при розробці клієнт-серверного додатку для підприємства логістики є масштабованість, оскільки забезпечення можливості легкого розширення системи з ростом бізнесу, навантаження та потреб користувачів є критичним фактором для успіху та стабільності підприємства.

Сучасні наукові дослідження підкреслюють важливість використання гнучких архітектурних рішень та принципів проектування, що сприяють масштабованості, таких як мікросервіси, віртуалізація, контейнеризація та розподілені системи.

Одним з основних напрямів розробки масштабованих клієнт-серверних додатків для підприємств логістики є застосування віртуалізації, контейнеризації та хмарних технологій для створення гнучких інфраструктур, які можуть адаптуватися до зміни навантаження та ресурсів. Це дозволяє компаніям динамічно змінювати розмір своїх серверних ресурсів, оптимізувати використання апаратного забезпечення та забезпечувати високу доступність та продуктивність системи.

Також, важливим аспектом масштабованості є розробка модульної архітектури додатку, яка дозволяє легко додавати та оновлювати функціональність, розширювати можливості системи та забезпечувати інтеграцію з іншими підсистемами та сервісами.

Другим елементом масштабованості є оптимізація роботи бази даних, яка включає в себе застосування розподілених баз даних, кешування та інших технік, що дозволяють забезпечити високу продуктивність та доступність даних.

Розподілені бази даних можуть бути використані для забезпечення надійного зберігання та доступу до даних, забезпечуючи реплікацію та автоматичне розподілення навантаження між різними серверами. Кешування може бути використано для зменшення часу відповіді системи та зниження навантаження на базу даних шляхом зберігання та повторного використання часто запитуваних даних.

Висновки. В даній роботі було розглянуто модель клієнт-серверного додатку для підприємства логістики. Основні аспекти, що були розглянуті, включають: розробку API, веб-додаток, мобільний додаток, базу даних, алгоритми оптимізації, безпеку даних, масштабованість та використання сучасних технологій. У ході розгляду цих аспектів було виявлено, що розробка такої системи вимагає врахування ряду важливих факторів, що можуть вплинути на її успішність та стабільність. Зокрема, розробка API має передбачати взаємодію між різними компонентами системи, підтримку різних форматів даних та безпечне обмін даними між клієнтами та серверами. Веб-додаток та мобільний додаток повинні забезпечувати інтуїтивний інтерфейс для користувачів, що дозволяє їм ефективно виконувати свої функції та контролювати логістичні процеси. Розробка бази даних має передбачати надійне зберігання та доступ до даних, оптимізацію роботи з даними, а також захист від несанкціонованого доступу та витоку інформації. Використання алгоритмів оптимізації для планування маршрутів, оптимізації ресурсів та підвищення ефективності логістичних операцій є важливим елементом розробки системи. Безпека даних має бути врахована на всіх рівнях розробки, починаючи від проектування архітектури системи та закінчуючи реалізацією механізмів авторизації та аутентифікації для користувачів. Важливо впроваджувати регулярні оновлення безпеки та проводити аудити системи з метою запобігання можливих загроз та зловживань. Масштабованість є критичним фактором для успіху та стабільності підприємства логістики. Розробка системи, яка здатна легко масштабуватися з ростом підприємства, навантаження та потреб користувачів, вимагає використання гнучких архітектурних рішень та принципів проектування, таких як мікросервіси, віртуалізація, контейнеризація та розподілені системи. Використання сучасних технологій та методів проектування допомагає досягти мети

стабільності та успіху підприємства на довготривалій перспективі. Зокрема, розробка модульної архітектури додатку, оптимізація роботи з базами даних, застосування віртуалізації та хмарних технологій для створення гнучких інфраструктур та інтеграція з іншими підсистемами та сервісами є важливими аспектами розробки масштабованого клієнт-серверного додатку для підприємства логістики. У висновку, дане дослідження підкреслює важливість розробки ефективного клієнт-серверного додатку для підприємства логістики з врахуванням вимог забезпечення безпеки, оптимізації ресурсів, масштабованості та використання сучасних технологій.

Список використаних джерел

1. Asgari, N., Farahani, R. Z., & Goh, M. (2021). Supply chain management: developments, issues, and trends. Annals of Operations Research, 293(1), 1-9.
2. Rushton, A., Croucher, P., & Baker, P. (2017). The handbook of logistics and distribution management: Understanding the supply chain. Kogan Page Publishers.
3. Aysegul Sarac, Nabil Absi, Stéphane Dauzère-Pérès, A literature review on the impact of RFID technologies on supply chain management, International Journal of Production Economics, Volume 128, Issue 1, 2010, Pages 77-95, ISSN 0925-5273, https://doi.org/10.1016/j.ijpe.2010.07.039.
4. Toth, P., & Vigo, D. (2014). Vehicle routing: problems, methods, and applications. SIAM
5. Wang, X., & Li, H. (2019). Design and implementation of a logistics information management system based on the Web. Journal of Physics: Conference Series, 1229(1), 012043.
6. Forsgren, N., Humble, J., & Kim, G. (2018). Accelerate: The science of lean software and DevOps: Building and scaling high performing technology organizations. IT Revolution.
7. Evans, J. R., Grubaugh, S., & Navaro, D. (2018). Implementing a mobile application for a trucking company. Journal of Management & Engineering Integration, 11(1), 33-42.
8. Zhang, M., Yu, S., Li, M., & Feng, X. (2020). Design and implementation of a logistics mobile application system based on Android. Journal of Physics: Conference Series, 1550(4), 042027.
9. Fosso Wamba, S., & Akter, S. (2021). The rise of artificial intelligence-enabled logistics 4.0: key technologies, applications, and research issues. The International Journal of Logistics Management.
10. Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press
11. Zhang, X., Zheng, X., Chen, W., & Zhang, Z. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122-129
12. TACACS+ Authentication and Accounting \\ Режим доступу: https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/16-02/5200-1648_K_ASG/content/ch09.html (Останнє звернення 20.03.2023р.)
13. Configuring TACACS+ \\ Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg/configuring_tacacs_.pdf (Останнє звернення 20.03.2023)

Робота виконана під науковим керівництвом PhD, доцентом
ДЕСЯТКО А.М.

ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ ДАНИХ У МОБІЛЬНИХ ЗАСТОСУНКАХ

ГАЛУШКО М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні засоби впровадження та застосування систем захисту у мобільних додатках. Відзначено переваги використання криптографічних систем захисту та методів автентифікації в мобільних застосунках. Розглянуто приклад програмного коду впровадження захисту мобільного додатку.

The article discusses the main means of implementing and using security systems in mobile applications. The advantages of using cryptographic security systems and authentication methods in mobile applications are noted. An example of a program code for implementing mobile application security is considered.

Актуальність. В наші дні популярність мобільних додатків настільки велика, що перенасичує ринок мобільних продуктів як і ліцензійними, так і сумнівними розробниками, що встановлення таких додатків стало звичайною справою для користувачів мобільних пристроїв не підозрюючи про можливий ризик. Кожна людина в розвинутій країні має десяток додатків на своєму смартфоні та на інших портативних пристроях, які потенційні додатки можуть бути зламані, а отже є ризик викрадення власних персональних даних зловмисниками. Тому забезпечення безпеки мобільних застосунків, захист персональних даних є важливим та пріоритетним завданням сьогодення з застосуванням криптографічних методів та механізмів автентифікації.

Згідно даним IDS за минулі роки, було розвантажено близько 1205.5 мільйонів одиниць смартфонів різних світових виробників, а за даними Statista на січень 2022 року, кількість мобільних застосунків для IOS в Apple Store становила близько 2,9 мільйонів, в той час як кількість додатків для Android в Google Play складає близько 3,8 мільйонів застосунків.

Таблиця 1

Топ-5 компаній світових поставок смартфонів, річний обсяг у 2022 та 2021 роках (млн одиниць).

Компанія	Обсяги 2022	Ринок 2022	Обсяги 2021	Ринок 2021	Зміна з року в рік
Samsung	260.9	21.6%	272.1	20%	-4.1%
Apple	226.4	18.8%	235.8	17.3%	-4.0%
Xiaomi	153.1	12.7%	191.0	14.0%	-19.8%
OPPO	103.3	8.6%	133.6	9.8%	-22.7%
Vivo	99.0	8.2%	128.3	9.4%	-22.8%
Інші	362.7	30.1%	399.1	29.3%	-9.1%
Всього	1205.5	100%	1359.8	100%	-11.3%

Ключові слова: мобільний застосунок\додаток, захист даних, криптографія, автентифікація, безпека даних.

Метою статті є дослідження впровадження та особливостей систем захисту мобільних застосунків з використанням криптографічних засобів та методів автентифікації з метою підвищення безпеки збереження конфіденційних даних для обізнаності користувачів та розробників.

Об'єктом дослідження є системи захисту даних у мобільних застосунках.

Предмет дослідження – мобільні застосунки.

Аналіз технологій та методів захисту даних у мобільних застосунках.

В даній статті у межах дослідження розглянуто основні найголовніші технології та методи захисту у мобільних застосунках.

Криптографія. Використання криптографічних методів в мобільних застосунках може надати надійний захист даних користувачів від викрадення як особистих, так і конфіденційних даних користувача. Криптографією називають науку про методи захисту, шифрування інформації від несанкціонованого доступу.

Найпоширеніший метод криптографії визначають шифрування даних, що використовується у мобільних застосунках. Шифруванням являється процес кодування звичайного тексту різними алгоритмами перетворюючи його на нерозбірливий текст або код, розшифрувавши який можливо тільки при наявності ключа, що забезпечує конфіденційність та цілісність даних від несанкціонованого доступу. Це означає, що навіть якщо дані будуть викрадені, злочинці не зможуть їх прочитати і використати не за призначенням. Ви можете зрозуміти силу шифрування, коли такі організації, як ФБР і АНБ, просять дозволу на доступ до iPhone і розшифровку повідомлень WhatsApp. Якщо вони не можуть зламати шифрування навмисно, то хакери точно не зможуть.

Керування ключами має вирішальне значення для того, щоб зусилля з шифрування окупилися. Розробникам не потрібно кодувати ключі, оскільки імовірність такого ключа написаного розробником, полегшує викрадення ключів зловмисниками. Дані ключі потрібно зберігати в безпечних контейнерах від несанкціонованого доступу та ніколи не зберігати їх на локальних на пристроях. Деякі загальноприйняті криптографічні протоколи, такі як MD5 і SHA1, виявилися недостатніми за сучасними стандартами безпеки. Лібше використовувати найновіші, найбільш надійні API, такі як 256-бітове шифрування AES з SHA-256 для хешування.

Також визначають один зі головних методів криптографії у мобільних застосунках, це хешування. Хешуванням являється процес перетворення будь-який набір даних в унікальний набір символів для перевірки цілісності даних. Такий метод шифрування ще називають хеш-функціями, що використовують для перевірки цифрового підпису та забезпечення цілісності даних.

Розробка системи захисту для мобільного застосунку має на меті забезпечити безпеку даних користувачів та запобігти несанкціонованому доступу до цих даних. Для розробки системи захисту можна використовувати різні технології та методи, що були наведені вище.

Помилки та вразливості в коді - це відправна точка для більшості зловмисників, які намагаються зламати додаток. Вони намагатимуться переробити ваш код і втрутитися в нього, і все, що їм для цього потрібно, - це публічна копія вашого додатку. Дослідження показують, що шкідливий код впливає на понад 11,6 мільйона мобільних пристроїв у будь-який момент часу. Пам'ятайте про безпеку вашого коду з першого дня і зміцнюйте його, щоб його було складно зламати. Заплутуйте та мінімізуйте свій код, щоб його неможливо було зламати. Проводьте багаторазове тестування та виправляйте помилки одразу після їх виявлення. Створюйте код так, щоб його було легко оновлювати та виправляти. Переконайтесь, що підтримується гнучкість вашого коду, щоб його можна було оновити після того, як користувач повідомить про порушення. Використовуйте зміцнення коду та підписання коду.

Безпека Android. Основою операційної системи Android є ядро Linux з деякими змінами, внесеними розробниками Google. Програми для операційної системи Android розробляються на Java або на досить нових мовах Scala і Kotlin. Починаючи з Android версії 1.5, було представлено Android NDK Toolkit. Це дозволяє розробляти модулі програми на C і C++ і компілювати їх у машинний код. Програми постачаються у вигляді спеціальних файлів у форматі APK, який є ZIP-архівом з певним каталогом і файловою структурою.

APK-файл містить:

- DEX-файл;

- Скомпільовані в машиний код код бібліотеки .so;
- Маніфест.

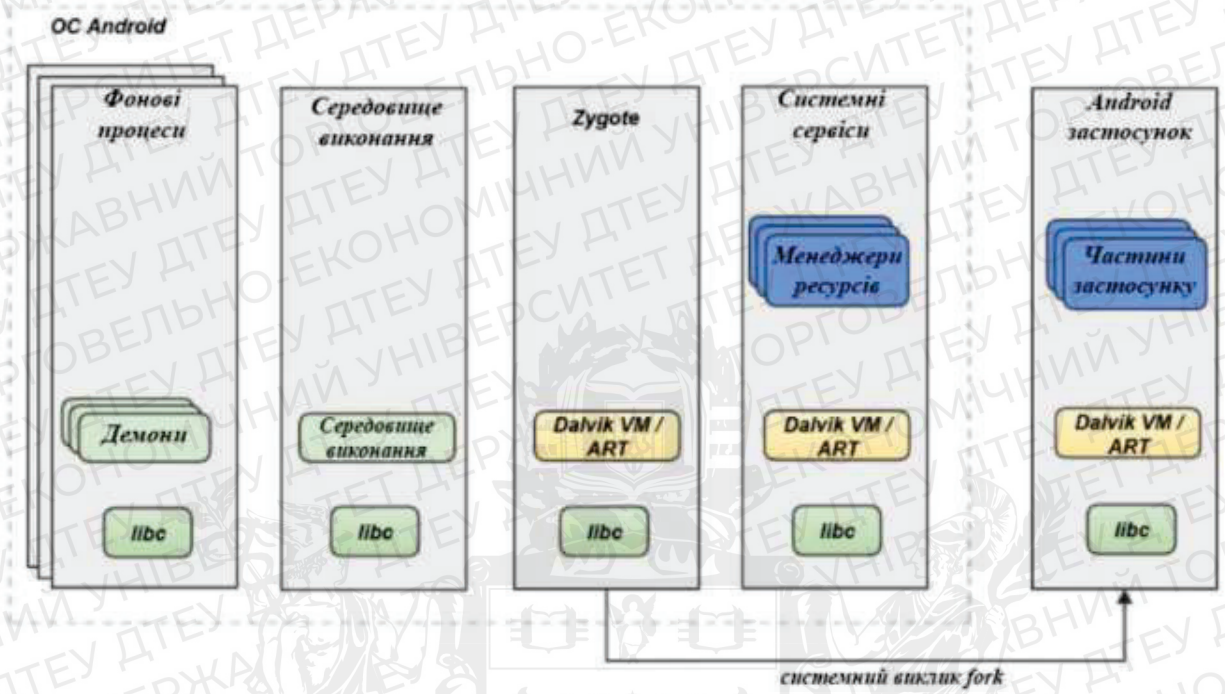


Рис.1. Схема роботи операційної системи Android із застосунками

Батьківським процесом усіх програм операційної системи Android є процес Zygote. Представлений процес є скелетом програми для Android зі вже завантаженими всіма бібліотеками, необхідними для середовища Android, але відсутній сам код програми. Запуск програми Android з точки зору операційної системи відбувається таким чином:

- Спочатку відбувається системний виклик fork для створення нащадка від процесу Zygote;
- У новоствореному процесі відкривається файл програми який ви запускаєте (системний виклик open).
- Відбувається читання інформації про файлах класів (classes.dex) і ресурсів з файлу програми. Відбувається відкриття сокетів для IPC;
- Виконується системний виклик mmap для транспортування файлів програми в пам'ять;
- Середовище виконання робить налаштування необхідного оточення виконує застосунок (інтерпретує байт-код Dalvik або передає управління функціям в виконуваному коді в разі ART).

Безпека IOS. Мобільна операційна система Apple під назвою IOS (IPhone Operating System) є найбезпечнішою з усіх мобільних систем. Нові розробки підвищують безпеку особистих даних на мобільних пристроях, роблячи можливі бекдори в Інтернеті рідким сенсаційним явищем на відміну від Android.

Безпека IOS розбита на такі модулі, як:

- Модуль Ідентифікація та автентифікація відповідає за перевірку ідентичності користувачів і запитів на автентифікацію. Цей модуль містить Touch ID і Face ID і підтримує створення складних паролів і двофакторну автентифікацію.
- Механізм шифрування відповідає за захист даних на вашому пристрої за допомогою шифрування. iOS використовує 256-бітне шифрування AES для захисту даних на вашому пристрої.

- Механізм безпеки додатків відповідає за захист додатків від зловмисних атак і ізоляції додатків один від одного. Кожна програма має власний простір пам'яті для роботи та власний доступ до файлів і ресурсів пристрою.

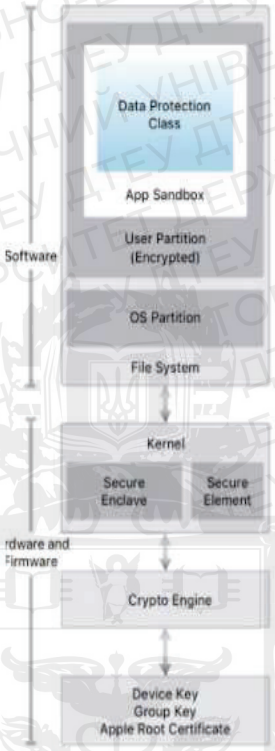


Рис. 2. Архітектура безпеки операційної системи IOS

- Модуль безпеки мережі відповідає за захист даних, які надсилаються через мережу. Зокрема, він захищає підключення до Wi-Fi і стільникових мереж.
- Модуль безпеки системи захищає саму операційну систему від зловмисних атак і забезпечує безпеку під час виконання системних процесів і взаємодії з апаратними компонентами.
- Модуль обробки інформації користувача відповідає за захист особистої інформації користувача, такої як контакти, календарі, фотографії та музика. Доступ до цих даних може бути обмежений та отриманий за певних умов, як перевірка дозволу користувача або використання Face ID або Touch ID. Цей модуль також шифрує дані, що зберігаються на пристрої, і захищає їх від несанкціонованого доступу програм і зовнішніх пристроїв. Крім того, цей модуль забезпечує безпеку процесу входу в систему та захист від вірусів і шкідливих програм.

Бібліотеки. Використовуючи сторонні бібліотеки при написані коду для свого додатку, будьте вдвічі обережнішими і ретельно тестуйте код, перш ніж використовувати його у своєму додатку. Незважаючи на їхню корисність, деякі бібліотеки можуть бути вкрай небезпечними для вашого додатку. Наприклад, бібліотека GNU C мала вразливість, яка дозволяла зловмисникам віддалено виконувати шкідливий код і виводити систему з ладу. І ця вразливість залишалася невиявленою понад сім років. Щоб захистити свої програми від вразливостей у бібліотеках, розробники повинні використовувати контрольовані внутрішні репозиторії та здійснювати політичний контроль під час їх придбання.

Використовуйте лише авторизовані API. Неавторизовані API зі слабким кодом можуть ненавмисно надати хакеру привілеї, які можуть бути використані зловмисниками для серйозних зловживань. Наприклад, локальне кешування інформації про авторизацію

допомагає програмістам легко повторно використовувати цю інформацію під час виклику API. Крім того, це полегшує життя програмістам, спрощуючи використання API. Однак це також дає зловмисникам шпаринку, через яку вони можуть викрасти привілеї. Експерти рекомендують авторизувати API централізовано для забезпечення максимальної безпеки.

Автентифікація користувачів. Одним з елементів системи захисту є автентифікація користувачів. Для цього можна використовувати різні методи, такі як логін та пароль, біометричні дані, двухфакторна автентифікація.

У зв'язку з тим, що деякі з найбільших порушень безпеки трапляються через слабку автентифікацію, стає все більш важливим використовувати більш надійну автентифікацію. Простіше кажучи, автентифікація стосується паролів та інших особистих ідентифікаторів, які діють як бар'єри для входу. Насправді, значна частина цього залежить від кінцевих користувачів додатку, але розробник має заохотити своїх користувачів бути більш чутливими до автентифікації. Мобільні додатки мають бути розроблені так, щоб вони приймали лише надійні алфавітно-цифрові паролі, які потрібно оновлювати кожні три або шість місяців. Все більшої популярності набуває багатофакторна автентифікація, яка передбачає поєднання статичного пароля та динамічного. У випадку надто чутливих додатків можна також використовувати біометричну автентифікацію, наприклад, сканування сітківки ока або відбитки пальців.

Захист даних. Окрім захисту мережі та автентифікації користувачів, система захисту повинна забезпечувати захист даних. Для цього можна використовувати такі методи як захист від шкідливих програм, шкідливого коду, резервне копіювання та виявлення несанкціонованого доступу.

Резервне копіювання даних. Резервне копіювання даних забезпечує можливість відновити дані у разі їх втрати або дефектування. Для цього можна використовувати різні методи, такі як регулярне копіювання даних на зовнішній носій, збереження даних на хмарному сервері та інші.

Розгортання технологій виявлення несанкціонованого доступу. Існують технології, що дозволяють сповіщати про спроби втручання у код або вбудовування шкідливого коду. Активне виявлення несанкціонованого доступу можна розгорнути, щоб переконатися, що код взагалі не буде функціонувати, якщо його буде змінено.

Принцип найменших привілеїв. Принцип найменших привілеїв передбачає, що код повинен працювати лише з тими дозволами, які йому абсолютно необхідні, і не більше. Додаток не повинен запитувати більше привілеїв, ніж мінімально необхідні для його роботи. Наприклад, якщо розробнику не потрібен доступ до контактів користувача, не надсилайте запит на надання доступу цих контактів. Не встановлюйте зайвих мережевих з'єднань. Все значною мірою залежить від специфіки додатку, тому постійно потрібно моделювати загрози під час оновлення коду.

Сесії. "Сесії" на мобільних пристроях тривають набагато довше, ніж на персональних комп’ютерах або лептопах. Це ускладнює обробку сесій для сервера. Потрібно використовувати токени замість ідентифікаторів пристроїв для ідентифікації сесії. Токени можуть бути відкликані в будь-який час, що робить їх більш безпечними у випадку втрати або крадіжки пристроїв. Застосуйте можливість віддаленого стирання даних із загубленого або вкраденого пристрою, а також можливість віддаленого виходу з системи.

Тестування. Захист додатку - це процес, який ніколи не закінчується. З'являються нові загрози і потрібні нові рішення. Потрібно проводити ругулярне тестування на проникнення, моделювання загроз та емулятори, щоб постійно перевіряти свої додатки на вразливості. Проводження виправлень вразливостей з кожним оновленням та випуск патчів, коли це необхідно. Знакові витоки даних 2017 року, такі як WannaCry і NotPetya, безумовно, змусили більшість звернути увагу на важливість кібербезпеки, і в найближчі роки організації та споживачів - будуть ставитися до безпеки серйозніше, ніж будь-коли. Безпека стане більшим диференціатором успіху додатків поруч зі зручністю використання та естетична привабливість.

Висновки. Розробка системи захисту для мобільного застосунку є актуальною задачею у сучасному світі, де все більше користувачів використовують мобільні пристрої для роботи та особистого використання. Для забезпечення безпеки мобільного застосунку необхідно використовувати комплексний підхід, який включає захист мережі, автентифікацію користувачів та захист даних. Також при розробці системи захисту для мобільного застосунку необхідно враховувати особливості мобільних пристроїв, такі як обмежені ресурси, низьку швидкість передачі даних та можливість втрати зв'язку. Також необхідно забезпечити можливість постійного оновлення системи захисту та регулярно проводити аудит безпеки системи.

Однак, у зв'язку зі зростанням кількості користувачів мобільних пристроїв та збільшенням ризику кібератак на них, розробка системи захисту є надзвичайно важливою для забезпечення безпеки користувачів та захисту їх приватності та даних.

У майбутньому очікується подальше розвиток технологій захисту мобільних застосунків. Одним із напрямків є використання штучного інтелекту та машинного навчання для виявлення та блокування загроз. Також очікується подальший розвиток технологій шифрування даних та автентифікації користувачів.

Список використаних джерел

1. Mobile Application Security: Who, How and Why – OWASP (Open Web Application Security Project) \\ Режим доступу: https://owasp.org/www-project-mobile-app-security/ (останнє звернення 03.20.2023р.)
2.Mobile App Security: 10 Best Practices for App Developers – Business News Daily \\ Режим доступу: https://www.tripwire.com/state-of-security/top-mobile-app-security-best-practices-developers (останнє звернення 03.20.2023р.)
3. Build a secure and private mobile app experience – IBM \\ Режим доступу: https://developer.ibm.com/articles/building-a-secure-and-private-mobile-app-experience/ (останнє 03.20.2023р.)
4.Mobile App Security Best Practices: A Checklist – PreEmptive Solutions \\ Режим доступу: https://www.preemptive.com/top-10-app-protection-practices/ (останнє звернення 03.25.2023р.)
5. Avoid Mobile Application Security Pitfalls – Knovation \\ Режим доступу: https://knovation.co.za/wp-content/uploads/2022/05/Avoid-Mobile-Application-Security-Pitfalls.pdf (останнє звернення 03.25.2023р.)
6. Android Security: Guide to Android OS– Veracode \\ Режим доступу: https://www.veracode.com/security/android-security (останнє звернення 03.25.2023р.)
7. Application Protection: Achieve application protection with cloud-based testing tools – Veracode \\ Режим доступу: https://www.veracode.com/security/application-protection (останнє звернення 03.31.2023р.)
8. Mobile App Security Testing: Resolve vulnerabilities with mobile app security testing – Veracode \\ Режим доступу: https://www.veracode.com/security/mobile-app-security-testing (останнє звернення 03.31.2023р.)
9. Захист мобільних застосунків на основі систем з нульовим знанням \\ Режим доступу: https://core.ac.uk/download/pdf/323525655.pdf (останнє звернення 04.01.2023р.)
10. Smartphone Market Share \\ Режим доступу: https://www.idc.com/promo/smartphone-market-share (останнє звернення 04.01.2023р.)
11. Number of apps available in leading app stores as of 3rd quarter 2022 \\ Режим доступу: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (останнє звернення 04.01.2023р.)

Робота виконана під науковим керівництвом ст. викладача,
ШЕСТАКА Я.І.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ПІДПРИЄМСТВА ЗАСОБАМИ ХЕШУВАННЯ

ГЕРМАН В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглядається поняття хеш-функцій та їх використання у захисті даних. В статті увага приділена понятійному апарату хеш-функцій, принципам їх роботи, і прикладам їх використання в програмуванні та криптографії.

Також в роботі розглядається важливість хеш-функцій для безпеки даних, зокрема, для захисту від зловмисного доступу до конфіденційної інформації. Наводяться приклади того, як хеш-функції використовуються для перевірки цілісності даних.

The article discusses the concept of hash functions and their use in data protection. The article focuses on the conceptual apparatus of hash functions, the principles of their operation, and examples of their use in programming and cryptography.

The work also considers the importance of hash functions for data security, in particular, for protection against malicious access to confidential information. Examples of how hash functions are used to verify data integrity are provided

Актуальність. Хеш-функції є потужним інструментом для перевірки цілісності файлів. Коли файл обробляється хеш-функцією, вона створює унікальний хеш-код, який можна використовувати для перевірки, чи було внесено будь-які зміни в файл. Якщо навіть один біт в файлі було змінено, хеш-код буде змінено і перевірка цілісності не буде успішною.

Хеш-функції є особливо важливими для перевірки цілісності файлів в інтернеті. Наприклад, коли ви завантажуєте програмне забезпечення з Інтернету, використання хеш-функцій може допомогти вам перевірити, що завантажений файл є тим самим файлом, який був викладений розробником програми, і що він не був змінений або пошкоджений під час завантаження.

Хеш-функція - це спеціальна функція, що відноситься до математичних функції, яка трансформує дані на вході у дані фіксованої довжини на виході. Це забезпечує легкість при роботі з перевіркою на цілісність файлів.

Хеш-функції також допомагають підвищити безпеку даних. Вони можуть використовуватися для захисту паролів та інших конфіденційних даних, щоб забезпечити, що ніхто не може отримати доступ до цих даних, навіть якщо вони стануть доступні для зловмисників.

Отже, використання хеш-функцій для перевірки цілісності файлів є дуже важливим кроком для забезпечення безпеки та цілісності даних.

Метою статті є дослідження особливостей використання актуальних хеш-функцій для забезпечення безпеки та цілісності файлів.

Об’єктом дослідження є розробка програмного продукту для перевірки на цілісність файлів на основі хеш-алгоритмів сімейства SHA.

Предмет дослідження – програмний продукт Hash my Data.

Аналіз попередніх досліджень. Дослідженню використання хеш-функцій для перевірки цілісності файлів присвячено праці закордонних науковців: William Stallings (Уильям Сталлингс), Lawrence Peter "Lawrie" Brown (Лорі Браун), Kazumaro Aoki (Кадзумаро Аокі), Farhana Sheikh (Фархана Шейх), Leonel Sousa (Леонель Соуза), Keith Martin (Кейт Мартін), Mike Burmester (Майк Бурместер), Gene Tsudik (Джин Цудік), Spyros S. Magliveras (Спірос С. Магліверас), Edem Swathi, G. Vivek, G. Sandhya Rani та ін.

Виклад основного матеріалу. .

На сьогоднішній день, люди використовують криптографію щодня, не усвідомлюючи (наприклад, банківські транзакції, вхід на вебсайти, спілкування в соціальних мережах тощо), щоб забезпечити та захистити свою конфіденційність. Раніше криптографія стосувалася виключно конфіденційності повідомлень, тобто шифрування.

Шифрування — це процес перетворення звичайного тексту (форма, яку можна прочитати) у зашифрований текст (форма, яку не можна прочитати, «абракадабра»). Дешифрування — це процес перетворення зашифрованого тексту назад у звичайний текст [1]. Графічно шифрування можна представити наступним чином, рисунок 1.

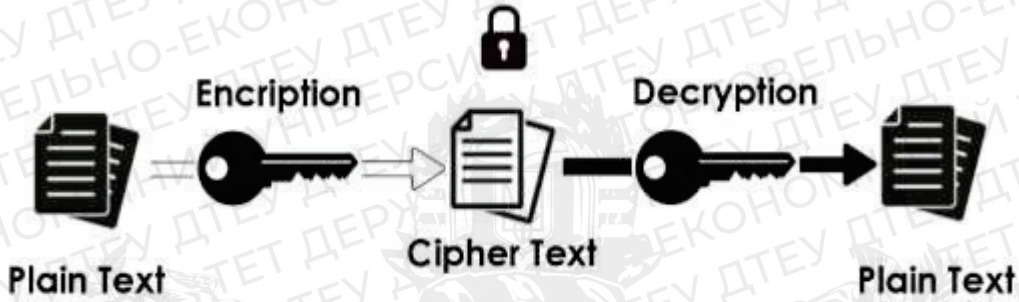


Рис. 1. Приклад роботи шифрування

Хеш-функція (геш-функція) — це функція, яка призначена для відображення даних будь-якого (довільного) розміру на дані строго визначеного (фіксованого) розміру. Значення, які повертає хеш-функція, називаються хеш-значеннями, хеш-кодами, хеш-сумами або просто хешами. Хеш-функції в основному використовуються в хеш-таблицях. Хеш-таблиця — це набір елементів даних, які зберігаються таким чином, щоб їх було легко знайти пізніше. Кожна позиція хеш-таблиці називається слотом. Слот може містити елемент даних і йому присвоюється ціле число, починаючи з 0. Слот ідентифікується ключем. Елемент даних, що зберігається в слоті, називається значенням [2]. Приклад роботи будь-якої хеш-функції зображено на рисунку 2.

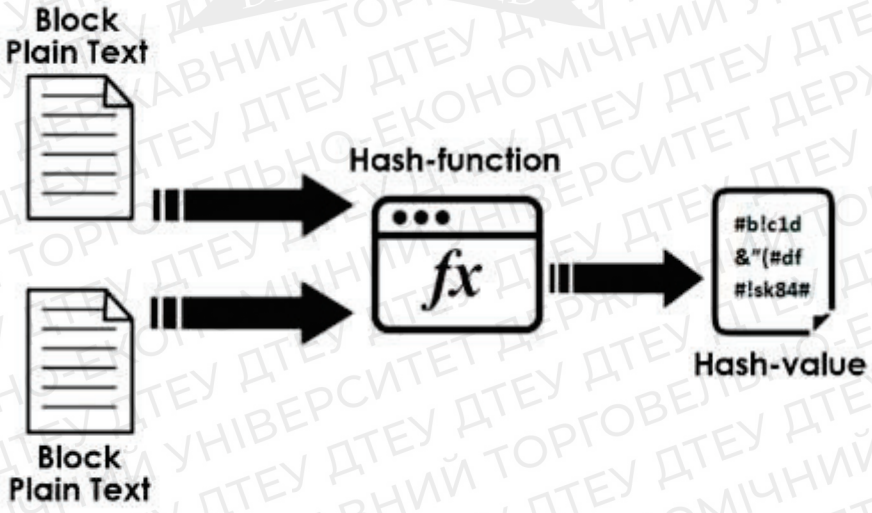


Рис. 2. Приклад роботи будь-якої хеш-функції

Як і блоковий шифр, алгоритм хешування включає раунди вищезазначеної хеш-функції (рисунок 2). Але на кожному раунді хеш-функція приймає вхідні дані фіксованого розміру, як правило, це складає комбінацію останніх блоків повідомлень і вихідних даних останнього раунду.

Цей процес повторюється n-раундів в залежності від того, скільки потрібно для хешування всього повідомлення. Схема алгоритму хешування зображено на рисунку 3.

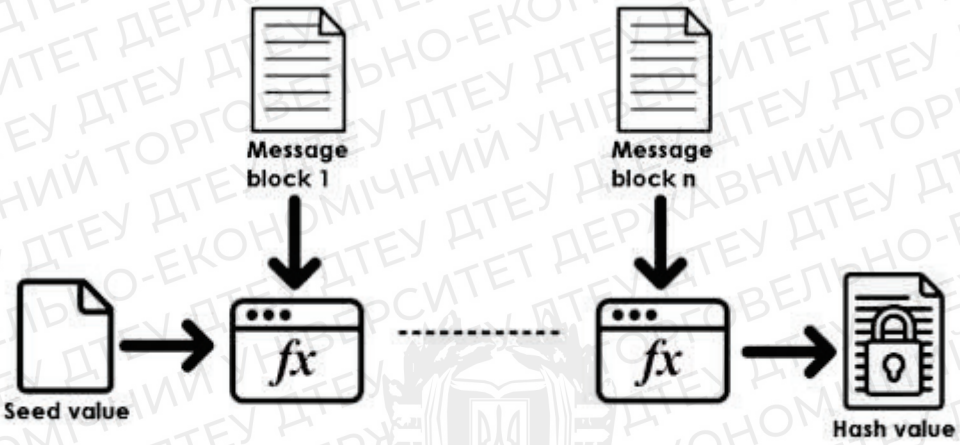


Рис. 3. Схема алгоритму хешування

Оскільки хеш-значення першого блоку повідомлення стає вхідним елементом для другої хеш-операції, а вихідний результат другої змінює результат третьої операції, і так далі. Цей ефект також відомий як лавинний ефект хешування. Ефект лавини призводить до суттєво різних хеш-значень для двох повідомлень, які відрізняються навіть одним бітом даних.

Саме тому необхідно розуміти різницю між хеш-функцією та алгоритмом. Хеш-функція генерує хеш-код, оперуючи двома блоками двійкових даних фіксованої довжини. А алгоритм хешування – це спеціальний процес використання хеш-функції, який визначає як саме вхідне повідомлення розбивається на блоки, та як результати з попередніх блоків вхідного повідомлення об'єднуються разом [3].

До основних вимог, що покладаються на хеш-функцію є:

- Collision resistant (стійкість до зіткнень). Тобто, будь-яка хеш-функція H є стійкою до зіткнень за умови, що для неї важко знайти такі два вхідні повідомлення, для яких на виході будуть мати однакові хеш-значення (рисунок 4).

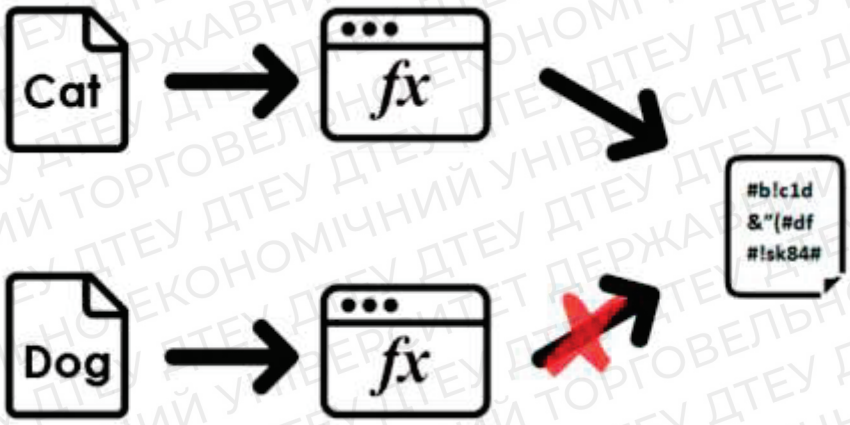


Рис. 4. Collision resistant

- Pre-image resistance (стійкість до прообразу). Це властивість, яка забезпечує хеш-функції неможливість отримання початкового повідомлення, знаючи хеш-значення (рисунок 5).

Рис. 5. Pre-image resistance

- Second pre-image resistance (стійкість до другого прообразу). Неможливо знайти друге вхідне повідомлення для хеш-значення, яке було отримано для першого повідомлення (рисунок 6).

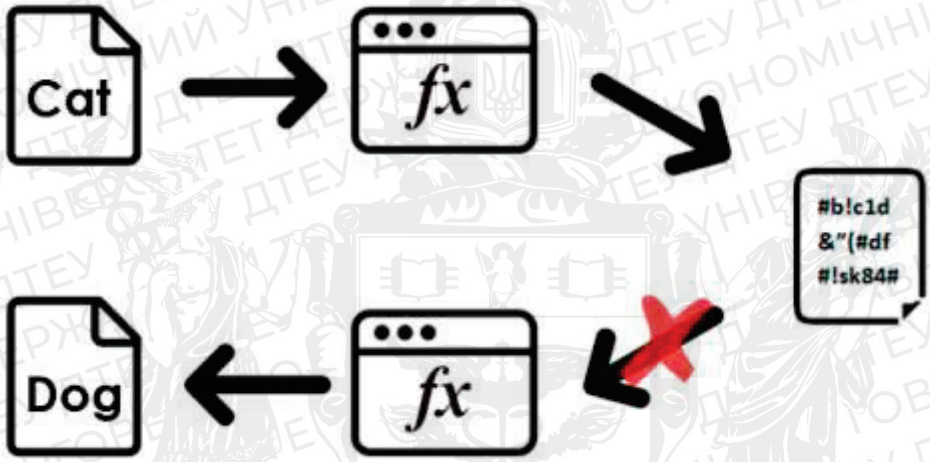


Рис. 6. Second pre-image resistance

- Large output space. Вихідні хеш-значення хеш-функції зазвичай представляються великими цілими числами, які представлені у двійковій формі, як біти (інколи для представлення хеш-значень використовується шістнадцяткова система числення). Так, наприклад, для хеш-функції SHA-256 довжина результату становитиме 256 біт, що в свою чергу становить 2^{256} = 1, 1579209*10^{77} загальна кількість можливих результатів. Тому при використанні методу грубої сили для такої кількості виходів займе десятки років для обчислення. Дана властивість робить даних підхід неефективний, а хеш-функцію більш надійною, стійкою до застосування грубої сили.
- Deterministic.Це означає, що для певного початкового повідомлення буде завжди обчислюватися одне й те саме хеш-значення.
- Avalanche effect (ефект лавини). При зміні хоча б одного символу в повідомленні чи біту, в результаті буде отримано зовсім інше хеш-значення на виході.
- Fixed-length mapping. Вихідний розмір хеш-функції завжди є фіксованим і ніяким чином не залежить від розміру вхідного повідомлення.
- Efficiency of operation (швидкість обчислення). Оскільки хеш-функція розроблюється для хешування тексту великої довжини, то стає дуже важливим питанням до швидкості роботи хеш-функції. Зазвичай, будь-яка хеш-функція обчислюється набагато швидше на відмінну від алгоритмів шифрування [4].

Спираючись на вищеописані вимоги порівняємо сучасні хеш-функції на колізії та першого та другого прообразів. Порівняльна характеристика подана в табл. 1.

Таблиця 1

Порівняльна характеристика хеш-функцій сімейства SHA

Функція	Вихідний розмір	Рівень захисту в бітах		
		Колізія	Прообраз	Другий прообраз
SHA-1	160	<80	160	160 - L(M)
SHA-224	224	112	224	min(224, 256 – L(M))
SHA-512/224	224	112	224	224
SHA-256	256	128	256	256 - L(M)
SHA-512/256	256	128	256	256
SHA-384	384	192	384	384
SHA-512	512	256	512	512 – L(M)
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	156	512	512
SHAKE128	d	min(d/2, 128)	≥min(d, 128)	min(d, 128)
SHAKE256	d	min(d/2, 256)	≥min(d, 256)	min(d, 256)

Раніше SHA-1 широко використовувався в протоколах TLS та SSL, але через низький рівень безпеки був замінений на більш безпечне сімейство хеш-функцій SHA-2. Низький рівень безпеки SHA-1 пов'язаний з високим рівнем зіткнень (показано в дослідженні 2019 року Гаетана Лерана та Томаса Пейрена (Gaëtan Leurent and Thomas Peyrin)) та вразливий до атак (перша успішна атака була проведена в 2017 році та мала назву SHAttered). На відмінну від SHA-1, SHA-256 ще жодного разу не був зламаний.

Також, варто порівняти швидкість обчислення хеш-значення, оскільки швидкість являється однією з ключових вимог до будь-якої хеш-функції. Так, самою швидкою хеш-функцією сімейства SHA є SHA-1. Після неї слідує SHA-256 та SHA-512, в залежності від довжини вхідного повідомлення. Так, SHA-256 працює швидше, ніж SHA-512, лише якщо хешуються невеликі рядки [5][6].

Цілісність даних гарантує, що дані зберігаються однаково під час будь-якої операції з ними, наприклад під час передавання, зберігання чи пошуку.

Під час передачі даних, дані, що передаються між програмами в загальнодоступному мережевому середовищі, можуть проходити через будь-яку кількість вузлів або мереж. Кожна з цих мереж може бачити передані дані. Використання криптографії гарантує, що хоча ці вузли можуть бачити дані, але вони не зможуть їх зрозуміти. Але оскільки дані можуть перетікати через вузли, які не контролюються відправником, існує ризик того, що вузол у мережі змінить дані до того, як вони досягнуть місця призначення. Звичайно, вузол може змінити

зашифровані дані навмання і це не призведе до витоку інформації, але це призведе до порушення в роботі програми.

Хоча користувач не може запобігти зміні даних кимось у мережі, приймаючий вузол повинен мати можливість виявити, чи були дані змінені, і, якщо так, не передавати пошкоджені дані програмі. Для цієї мети використовується дайджест повідомлення (message digest). Іншими словами, дайджест повідомлення – це відбиток даних. Якщо дані змінюються, відбиток (дайджест повідомлення або хеш) змінюється таким чином, що це неможливо передбачити (лавинний ефект) [7].

Однією з безкоштовних програм для перевірки файлів на цілісність за допомогою хеш-функцій для Windows – OpenHashTab (рисунок 7).

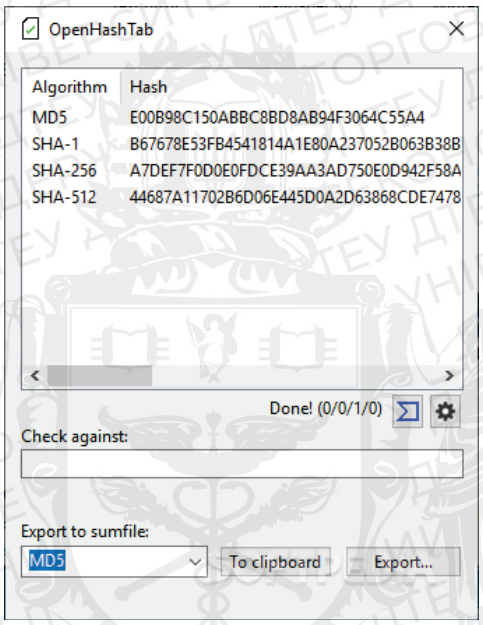


Рис. 7. Головне вікно програми OpenHashTab

Даний програмний продукт дає можливість обраховувати хеші для файлів на основі популярних хеш-функцій, таких як SHA-1, SHA-2, SHA-3, MD5 та ін. Загалом в програмі представлено підтримку для 28 алгоритмів. Для обрахування хеш-значення необхідно на головному вікні натиснути праву кнопку миші та перейти до налаштувань. Після цього буде відкрито відповідне вікно, в якому відбувається налаштування хеш-функції (рисунок 8).

Рис. 8. Вікно налаштувань для хеш-функції

Висновки. Існує декілька варіантів використання хеш-функцій, одна з яких – перевірка файлів на цілісність даних. Оскільки лише дайджести повідомлень забезпечують часткову цілісність даних, захищаючи від випадкового пошкодження даних. Однак, при використанні із зашифрованими даними дайджести повідомлень захищають від навмисних спроб пошкоджень з іншого боку. У випадку, якщо дані представлені у незашифрованому вигляді, зловмисник може змінити дані на необхідні йому, обчислити дайджест для нього значення та зберегти його замість старого. В результаті користувач не буде знати, що дані були змінені. Оскільки збережений дайджест для цього повідомлення буде відповідати дайджесту, який буде обраховуватися під час використання. Тому, навіть використання хеш-функції не гарантують цілісність та можливість запобіганню модифікації даних. Цей ризик можливо зменшити при умові використання шифрування даних.

Список використаних джерел

1. Comparison of Hash Function Algorithms Against Attacks: A Review \\ Режим доступу: https://pdfs.semanticscholar.org/6ed2/50d11a5c80f550bd8efcc673606c3cae34b7.pdfb (останнє звернення 01.03.2023р.)
2. Universal classes of hash functions (Extended Abstract) \\ Режим доступу: https://dl.acm.org/doi/abs/10.1145/800105.803400 (останнє звернення 01.03.2023р.)
3. Analysis and improvement of a chaos-based Hash function construction \\ Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1007570409003426 (останнє звернення 02.03.2023р.)
4. Cryptographic Hash Functions: A Review \\ Режим доступу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=85abc4805adb741b0f8c962794d2ab4dac975c5f (останнє звернення 03.03.2023р.)
5. An efficient implementation of hash function processor for ipsec \\ Режим доступу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4ad55cff822563aafb31a1533eaa60afbeec37aa (останнє звернення 05.03.2023р.)
6. A Novel Improvement with an Effective Expansion to Enhance the MD5 Hash Function for Verification of a Secure E-Document \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/9072400 (останнє звернення 05.03.2023р.)
7. Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms \\ Режим доступу: https://link.springer.com/chapter/10.1007/978-3-540-85174-5_9 (останнє звернення 05.03.2023р.)
8. How Does RADIUS Work \\ Режим доступу: https://support.huawei.com/enterprise/en/doc/EDOC1100086516#:~:text=RADIUS%20has%20the%20following%20characteristics%3A (Останнє звернення 20.03.2023)
9. RADIUS Attributes Overview and RADIUS IETF Attributes \\ Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_radatt/configuration/15-s/sec-usr-radatt-15-s-book/sec-rad-ov-ietf-attr.pdf (Останнє звернення 20.03.2023)
10. Hannes Tschofenig, Sebastien Decugis, Jean Mahoney, Jouni Korhonen, Diameter: New Generation AAA Protocol - Design, Practice, and Applications. – 2019. – с. 15 – 16.

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

ВИКОРИСТАННЯ ПРОТОКОЛУ SSHV2 ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

ГИРИЧ В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні способи захисту комп'ютерних мереж підприємства з використанням протоколу SSHv2. Зазначено основні переваги застосування протоколу SSHv2, який є одним з найбільш ефективних способів захисту каналу передачі даних в мережі. Розглянуто топологію, архітектуру та комунікаційні пристрої комп'ютерної мережі підприємства, способи керування мережею, питання надійності системи та інформаційної безпеки мережі.

The article discusses the basic principles of protecting enterprise computer networks using the SSHv2 protocol. The main advantages of using the SSHv2 protocol, which is one of the most effective ways to protect the data transmission channel in the network, are indicated. Topology, architecture and communication devices of the company's computer network, network management methods, issues of system reliability and information security of the network are considered.

Актуальність. Майже всі комп'ютери світу сьогодні підключені до інтернету, а робота в мережі здійснюється за допомогою мережевих протоколів. Мережевий протокол − це комплекс установок, завдяки яким визначається і регулюється процес інформаційного обміну між комп'ютерами, підключеними до інтернету. Протокол в певному сенсі вважається мовою, необхідною машинам для взаємодії. Серед його ключових особливостей − структурованість і стандартизація.

Протокол SSH (Secure Shell) реалізований на рівні додатків і призначений для того, щоб дистанційно керувати системою за допомогою захищеного каналу. Даний варіант застосовується в роботі багатьох технологій. Підключення по протоколу SSH включають такі особливості: шифрування − характерна властивість SSH; авторизацію по ключу, тобто відбувається кодування всього трафіку, в тому числі паролів, за допомогою різних алгоритмів; безпеку − властивість випливає з попереднього, так як завдяки шифруванню збільшується надійність віддаленої роботи; можливість стиснення − така особливість актуальна при передачі інформації.

Копіювання файлів по протоколу SSH дозволяє підвищити рівень захисту при передачі інформації. Secure Shell вважається протоколом прикладного рівня, і його пряме призначення − забезпечення віддаленого захищеного доступу. Зараз відомо дві версій − 1 і 2. Проте версія 1 зупинена, оскільки наприкінці 90-х років у ній було знайдено багато вразливостей, деякі з яких досі накладають серйозні обмеження на її використання, тому перспективною і найбезпечнішою є версія 2.

Метою статті є дослідження особливостей захищеної комп'ютерної мережі підприємства з використанням протоколу SSHv2.

Об'єктом дослідження є розробка комп'ютерної мережі з використанням мережевого протоколу SSHv2, який є одним з найбільш ефективних способів захисту каналу передачі даних в мережі.

Предмет дослідження є захищена комп'ютерна мережа.

Аналіз попередніх досліджень. Дослідженню комп'ютерних мереж та протоколів захисту присвячені праці вітчизняних та закордонних науковців: В.А. Світличного, Ю.М. Онищенко, Б.М. Корнієнка, Л. Щербака, В. М. Богуша, О. К. Юдіна та ін.

Виклад основного матеріалу. Майже всі комп'ютери світу сьогодні підключені до інтернету, робота в мережі здійснюється за допомогою мережевих протоколів.

Комп'ютерні мережі – це сукупність персональних комп’ютерів, розподілених на території і з’єднаних для спільного використання деяких ресурсів. Головна мета об'єднання у мережу обчислювальних пристроїв це надання доступу до різних інформаційних ресурсів багатьом користувачам, розподіленим по цих комп'ютерах, і їх спільного використання. Широта території впливу – важлива характеристика для усіх комп'ютерних мереж. Широта охоплення визначається взаємною віддаленістю комп'ютерів, що складають мережу, і, отже, впливає на технологічні рішення, обрані при побудові мережі. Комп'ютерні мережі доступу це результат революції на інформаційному полі, це основний засіб комунікації. По всьому світу йде об'єднання комп'ютерів у спільну мережу, що обґрунтовано такими причинами, як прискорення передачі інформації та повідомлень, швидкий обмін інформацією між серверами, обробка і передача повідомлень, безпосередньо на робочому місця, а також миттєвий доступ до будь-якої інформації незалежно від розташування, обмін інформацією між серверами різних підприємств-виробників, використовуючи різне програмне забезпечення. Одною з важливих відмінностей між мережами доступу є їх топологія. Під топологією розуміють взаємне розташування вузлів мережі відносно один одного. Комп'ютери, комутатори, концентратори, маршрутизатори та точки доступу відносяться до вузлів мережі [1, 2].

Топологія – це комутація фізичних з’єднань між вузлами мережі. Від типу топології, яку використовує провайдер, залежать характеристики мережі. Вибір топології може впливати:

1) на модель мережевого обладнання, яке необхідно у цьому випадку;
2) на технологічні можливості мережевого обладнання;
3) на резервування пропускної здатності для розширення мережі;
4) на засоби управління мережею.

Існують наступні види топологій: кільце, шина, зірка. Існують інші комбінації цих топологій: змішані або гібридні. У порівнянні з основними видами топологій, змішана топологія має більшу надійність. Доцільно використовувати змішану топологію через поєднання переваг надійності та економічності використання.

Під структурою мережі розуміють спосіб поділу мережі на частини (сегменти), а також спосіб з'єднання цих сегментів між собою. Мережа підприємства може включати в себе робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. Для об'єднання частин мережі можуть використовуватися повторювачі, концентратори, комутатори, мости та маршрутизатори. Причому в ряді випадків вартість цього обладнання може навіть перевищити вартість комп'ютерів, мережевих адаптерів і кабелю, тому вибір структури мережі дуже важливий [3]. В ідеалі, структура мережі повинна відповідати структурі будівлі або комплексу будівель підприємства. Робочі місця групи співробітників, які займаються одним завданням (наприклад, бухгалтерія, відділ продажів, інженерна група), повинні розміщуватися в одній або поруч розташованих кімнатах. Тоді можна комп'ютери цих співробітників об'єднати в один сегмент, в єдину робочу групу і встановити поблизу їх кімнат сервер, з яким вони працюватимуть, а також концентратор або комутатор, що зв'язує всі їхні машини.

Специфікація 100Base-T4 була розроблена для того, щоб можна було використовувати для високошвидкісного Ethernet наявну проводку на кручений парі категорії 3. Ця специфікація дозволяє підвищити загальну пропускну здатність за рахунок одночасної передачі потоків біт по всім 4 парам кабелю [3]. Специфікація 100Base-T4 з'явилася пізніше інших специфікацій фізичного рівня Fast Ethernet. Розробники цієї технології в першу чергу хотіли створити фізичні специфікації, найбільш близькі до специфікацій 10Base-T і 10Base-F, що працювали на двох лініях передачі даних: двох парах чи двох волокнах. Для реалізації роботи з двох кручених пар довелося перейти на більш якісний кабель категорії 5 [1].

На Рис. 1 показано з'єднання порту MDI мережного адаптера 100Base-T4 з портом MDI-X концентратора (приставка X говорить про те, що в цього роз'єму приймача і передавача міняються парами кабелю в порівнянні з роз'ємами мережного адаптера, що дозволяє простіше з'єднувати пари проводів у кабелі − без перехрещування). Пари 1-2 завжди потрібні для

передачі даних від порту MDI до порту MDI-X, пари 3-6 для прийому даних портом MDI від порту MDI-X, а пари 4-5 і 7-8 є двонаправленими і використовуються як для прийому, так і для передачі, в залежності від потреби [1].

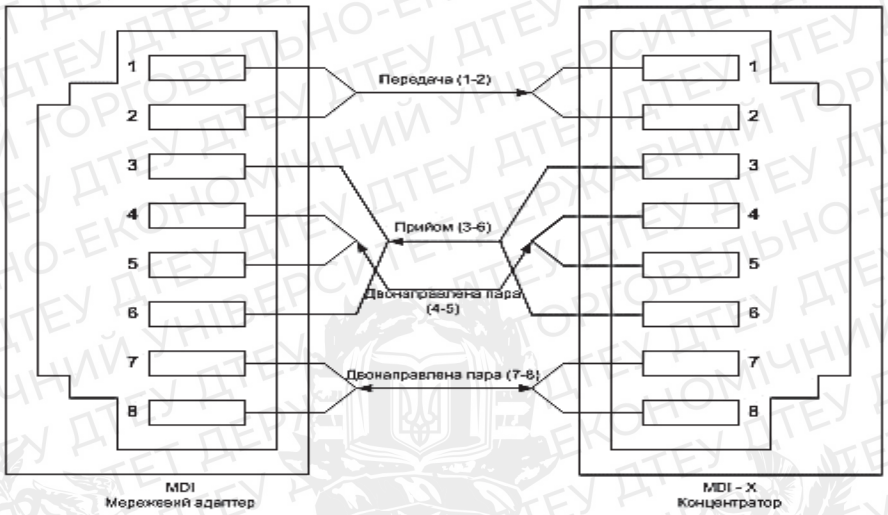


Рис.1. З'єднання порту MDI мережного адаптера 100Base-T4 з портом MDI-X концентратора.

Ні для кого не секрет, що в наш час дуже важливим є забезпечення максимальної безпеки даних, особливо якщо вони стосуються особистого життя або комерційної діяльності. Адже сьогодні вже сформувалася ціла індустрія з перехоплення інформації, злому акаунтів тощо.

Тому, якщо потрібно передати на сервер особливо важливі файли, або скористатися віддаленим доступом до операційної системи, то цілком логічним буде подбати про безпеку передачі даних. Сьогодні, одним з найбільш поширених способів захисту конфіденційних даних, є використання мережевого протоколу SSH (Secure Shell).

Серед характеристик протоколу SSHv2 слід виділити стійкість до атак прослуховування – «man-in-middle»; атак, що здійснюються «шляхом приєднання посередині» – «session hijacking»; атак – «DNS spoffing».

Необхідність використання таких засобів захисту обумовлена двома факторами:

1. У більшості випадків, в мережі інтернет, дані передаються у відкритому вигляді, і відповідно будь-який бажаючий зможе без особливих зусиль перехопити їх. Особливо варто відзначити, що в цьому випадку можуть бути перехоплені і паролі;
2. Авторизація, за допомогою паролів або IP-адрес, також дуже вразлива.

Ще в середині 70-х років двадцятого століття був створений алгоритм шифрування RSA, який використовують для створення «публічних ключів». В основі роботи цього алгоритму лежить використання двох криптоключів – один з них використовується для дешифрування, а другий для шифрування. «Публічним», називають ключ, який використовується для шифрування даних, «секретним» – ключ, який використовується для дешифрування, оскільки повноцінний доступ до даних може отримати тільки його власник.

Мережевий протокол SSH, розшифровується як Secure Shell, або якщо говорити українською мовою – «безпечна оболонка». Безпека передачі даних забезпечується за допомогою шифрування трафіку з його можливою компресією. Крім того, цей мережевий протокол часто використовується для створення захищених каналів, що дозволяють безпечно передавати дані через небезпечну середу (зокрема інтернет). Також він, непогано себе показує з переадресації портів або віддалених клієнтів. Завдяки цьому, даний мережевий протокол на сьогоднішній день являє собою перевірений стандартний протокол і активно використовується для адміністративної роботи з серверами в віддаленому режимі.

Доступ по протоколу SSH, можна отримати за допомогою одного з трьох типів аутентифікації:

- Аутентифікація за допомогою пари ключів. У цій ситуації генерується пара з закритого (на ПК, з якого здійснюється підключення), і відкритого (на пристрої, до якого підключаються) ключів. Система автоматично перевіряє наявність ключів без передачі цих файлів;
- Стандартна аутентифікація за допомогою пароля. В цьому випадку в кожному підключенні створюється свій ключ для шифрування трафіку, за аналогією з HTTPS;
- Аутентифікація за допомогою IP-адреси. Використовується досить рідко, оскільки це найменш безпечний з трьох варіантів.

На сьогоднішній день, існує два варіанти мережевого протоколу SSH:

1. OpenSSH – версія з відкритим вихідним кодом, яку можна використовувати безкоштовно для комерційних і некомерційних проєктів. Реалізація Open SSH є на всіх операційних системах Unix. OpenSSH є провідним інструментом підключення для віддаленого входу за допомогою протоколу SSH. Він шифрує весь трафік, щоб виключити підслуховування, викрадення з'єднання та інші атаки. Крім того, Open SSH пропонує багатий набір функцій безпечного тунелювання, кілька методів аутентифікації та складні параметри конфігурації;
2. Комерційний варіант, який розробляється SSH Communications Security. Цю версію теж можна використовувати безкоштовно, але тільки для некомерційних проєктів.

Зрозуміло, найбільшою популярністю користується саме безкоштовна версія. Але заради справедливості, треба сказати, що більшості програмістам вона подобається саме через наявність відкритого вихідного коду, оскільки це дозволяє модифікувати версію для своїх потреб.

Основними задачами, для вирішення яких застосовується SSH-клієнт, крім підключення до сервера, є:

- Робота з архівами, файлами і папками;
- Перегляд і редагування даних;
- Вивчення робочих процесів;
- Використання баз даних.

Особливо важливим є те, що завдяки можливості стиснення даних, при передачі через протокол SSH, який дозволяє швидко обробляти файли великих розмірів, наприклад відео.

Перша версія, яка отримала назву SSHv1, була створена в далекому 1995-му році, автором є Тату Улен. Основним завданням цієї версії, було забезпечення більш високого рівня конфіденційності, в порівнянні з протоколами RSH, TELNET I RLOGIN, які використовувалися в той час [1, 4].

Головною перевагою першої версії, перед своїми конкурентами, була стійкість до прослуховування трафіку («сніфінг»), проте даний протокол все ще був вразливий для атак, принцип яких базується на тому, що зловмисник стає посередником між двома сторонами обміну даними, і може ретранслювати їх або змінювати.

Саме тому в 1996-му, був розроблений протокол SSHv2, який і використовується в наш час. Дана версія передбачає використання спеціальної авторизації при підключенні до сервера, що не дає можливості третім особам підключитися до потоку даних. На сьогоднішній день використовується виключно друга версія.

Для роботи по протоколу SSH потрібен SSH-сервер і SSH-клієнт. Сервер прослуховує з'єднання від клієнтських машин і при встановленні зв'язку створює аутентифікацію, після чого починає обслуговування клієнта. Клієнт використовується для входу на віддалену машину і виконання команд. Для з'єднання сервер і клієнт повинні створити пари ключів – відкритих і закритих – і обмінятися відкритими ключами. Зазвичай використовується також і пароль.

На сьогоднішній день використання мережевого протоколу SSH v2, є одним з найбільш ефективних способів захисту каналу передачі даних. Його головною перевагою є

використання відкритого і закритого ключа при з'єднанні клієнта з сервером, що дозволяє звести до мінімуму ймовірність того, що до каналу підключиться хтось третій.

Коли використовують протокол SSHv2, істотно підвищують безпеку з'єднання, тому рекомендовано виконувати наступні дії:

- Заборонити відключення входу по паролю або підключення з порожнім паролем;
- Заборонити віддалений root-доступ;
- Обмежити список IP-адрес, для яких буде дозволений доступ;
- Вибрати нестандартні системні логіни і порт.

Також варто регулярно переглядати повідомлення про помилки аутентифікації. Ще одним важливим моментом, який дозволяє суттєво збільшити безпеку з'єднання, є використання довгих ключів для SSHv2. Вважається, що довгий ключ містить більше 2048 біт. Взагалі, надійною вважається система шифрування, якщо довжина ключа дорівнює як мінімум 1024 біт, або більше [1, 2].

Додатково покращити захист з'єднання допоможе використання пасток, які імітують SSH-сервіс, технологія Port knocking та система виявлення вторгнень (IDS).

На сьогоднішній день комп'ютерна мережа є не тільки звичним засобом комунікації, а також інструментом обміну інформацією. У зв'язку з розвитком та створенням великої кількості комп'ютерних мереж виникає ціла низка взаємопов'язаних проблем захисту інформації, що зберігається в комп'ютерах або серверах комп'ютерної мережі. Сучасні мережеві операційні системи, які вже повністю захищені від атак та загроз, також представляють собою потужні засоби захисту від несанкціонованого доступу до мережевих ресурсів. Однак виникають випадки, коли навіть такий захист стає вразливим і не спрацьовують програмні продукти для захисту інформації [3].

При створенні великомасштабних комп'ютерних мереж виникає проблема забезпечення взаємодії великої кількості комп'ютерів, серверів, підмереж та мереж, тобто проблема пошуку та вибору оптимальної топології стає головним завданням. Найважливішим компонентом локальних та корпоративних мереж є їхня системна топологія, яка визначається архітектурою міжкомп'ютерних зв'язків. З погляду безпеки комп'ютерні мережі мають наступні недоліки:

1. Недостатній контроль над клієнтськими комп'ютерами;
2. Відсутність механізму доступу кількох користувачів до різних ресурсів на одному комп'ютері;
3. Необхідність підготовки користувача до різних адміністративних заходів - оновлення антивірусної бази, архівування даних, визначення механізмів доступу до ресурсів, що роздаються;
4. Поділ ресурсів та завантаження розподіляються по різних вузлах мережі.

До апаратних засобів захисту відносяться різні брандмауери, мережеві екрани, фільтри, антивірусні програми, пристрої шифрування протоколу та інше. До програмних засобів захисту відносять: стеження мережевих підключень (моніторинг мережі); засоби архівації даних; антивірусні програми; криптографічні засоби; засоби ідентифікації та аутентифікації користувачів; засоби управління доступом; протоколювання та аудит. Як приклади комбінацій таких заходів можна навести [2]: захист баз даних; захист інформації при роботі в комп'ютерних мережах.

На основі аналізу загроз безпеці комп'ютерних мереж можна зробити висновки про властивості та функції, які повинна мати система забезпечення безпеки локальних та корпоративних мереж (КМ) [2]:

1. Ідентифікація ресурсів;
2. Аутентифікація ресурсів;
3. Застосування парольного захисту ресурсів у всіх частинах комп'ютерної мережі;
4. Реєстрація всіх дій: вхід користувача в мережу, вихід з мережі, порушення прав доступу до ресурсів, які захищаються;

5. Забезпечення захисту інформації при проведенні сканування мережі від шкідливих програм і ремонтно-профілактичних робіт.

Під загрозою безпеки інформації в КМ розуміється подія або дія, що може викликати зміну функціонування КМ, пов'язана з порушенням захищеності інформації, що в ній обробляється. Вразливість інформації – це можливість виникнення такого стану, при якому створюються умови для реалізації загроз безпеці інформації.

Атака на КМ пов’язана з дією, яка виконується порушником і полягає в пошуку та використанні тієї або іншої вразливості. Інакше кажучи, атака на КМ є реалізацією загрози безпеці інформації в ній.

Одним із найнебезпечніших способів проведення атак є впровадження в системи, що атакуються, шкідливого програмного забезпечення (ШПЗ). Виділяють наступні аспекти ШПЗ: шкідлива функція; спосіб поширення; зовнішнє представлення.

В сучасному світі проблема захисту інформації в КМ досить актуальна, тому вимагає постійного аналізу нових або вже існуючих систем захисту. В результаті проведення аналізу загроз безпеці інформації в КМ, аналізують основні загрози, визначають причини їх виникнення та наслідки, до яких приводить їх діяльність.

По механізму поширення розрізняють: віруси – код, що володіє здатністю до поширення (можливо, зі змінами) шляхом впровадження в інші програми; «мережеві хробаки» – код, здатний самостійно, тобто без впровадження в інші програми, викликати поширення своїх копій по мережі і їх виконання (для активації вірусу потрібен запуск зараженої програми).

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

- перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;
- модифікація інформації – вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;
- підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може послати лист від чужого імені або веб-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

Специфіка КМ, з точки зору їх вразливості, пов'язана в основному з наявністю інтенсивної інформаційної взаємодії між територіально рознесеними і різнорідними (різнотипними) елементами.

Вразливими є буквально всі основні структурно-функціональні елементи КМ: робочі станції, сервери (Host-машини), міжмережеві мости (шлюзи, центри комутації), канали зв'язку тощо. Загрози класифікуються за можливістю нанесення шкоди суб'єкту відносин при порушенні цілей безпеки. Збиток може бути заподіяний будь-яким суб'єктом (злочин, вина або недбалість), а також стати наслідком, незалежних від суб'єкта проявів. При забезпеченні конфіденційності інформації, це може бути розкрадання (копіювання) інформації і засобів її обробки, а також її втрата (ненавмисна втрата, витік). При забезпеченні цілісності інформації список загроз такий: модифікація (спотворення) інформації; заперечення автентичності інформації; нав'язування неправдивої інформації. При забезпеченні доступності інформації можливе її блокування, або знищення самої інформації та засобів її обробки.

Класифікація можливостей реалізації загроз (атак), являє собою сукупність можливих варіантів дій джерела загроз певними методами реалізації з використанням вразливостей, які призводять до реалізації цілей атаки. Мета атаки може не збігатися з метою реалізації загроз і може бути спрямована на отримання проміжного результату, необхідного для досягнення подальшої реалізації загрози. У разі такого неспівпадання атака розглядається як етап підготовки до вчинення дій, спрямованих на реалізацію загрози, тобто як «підготовка до вчинення» протиправної дії.

Вихідними даними для проведення оцінки та аналізу загроз безпеки при роботі в мережі служать результати анкетування суб'єктів відносин, спрямовані на з'ясування спрямованості їх діяльності, передбачуваних пріоритетів цілей безпеки, завдань, що вирішуються в мережі і умов розташування та експлуатації мережі [2].

Найчастішими і найнебезпечнішими (з погляду розміру збитку) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують комп'ютерну мережу.

Іноді такі помилки і є власне загрозами (неправильно введені дані або помилка в програмі, яка викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (зазвичай помилки адміністрування). За деякими даними, до 65% втрат – наслідок ненавмисних помилок [3]. Очевидно, найрадикальніший спосіб боротьби з ненавмисними помилками – максимальна автоматизація і суворий контроль.

Для виведення систем зі штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок. Як засіб виведення мережі зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). Згідно розташування джерела загрози таке споживання підрозділяється на локальне та віддалене.

При помилках в конфігурації системи локальна програма здатна практично монополізувати процесор та фізичну пам'ять та зводить швидкість виконання інших програм до нуля [2]. Віддалене споживання ресурсів останнім часом проявляється в особливо небезпечній формі – скоординовані розподілені атаки, коли на сервер з великої кількості різних адрес з максимальною швидкістю спрямовуються цілком легальні запити на з'єднання та обслуговування. Якщо мають місце архітектурні помилки у вигляді розбалансованості між пропускною спроможністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність вкрай важко.

Висновки. На сьогоднішній день, використання мережевого протоколу SSHv2, є одним з найбільш ефективних способів захисту каналу передачі даних. Його головною перевагою, є використання відкритого і закритого ключа при з’єднанні клієнта з сервером, що дозволяє звести до мінімуму ймовірність того, що до каналу підключиться хтось третій. Дуже важливим моментом можна назвати те, що клієнт і сервер для протоколу SSHv2, вимагають спеціального налаштування, яке далеко не завжди під силу людині, що не володіє певними знаннями. Саме тому багато провайдерів пропонують своїм клієнтам послуги зі створення та налаштування захищеного з’єднання.

Список використаних джерел

1. Корнієнко Б. Я., Щербак Л. М. Захист інформації в комп`ютерних системах та мережах, частина 2 (модульні технології навчання). Навчально-методичне видання, Київ: НАУ. – 2015, 139 с.
2. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
3. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах. – К., 2013. – 435 с.
4. Кучернюк В. П. Методи і технології захисту комп’ютерних мереж (фізичний та канальний рівні). Мікросистеми, електроніка та акустика. 2017. № 6. Том 22. С. 64-70.

Робота виконана під науковим керівництвом к.п.н., доцента
ЧУБАЄВСЬКОГО В.І.

АНАЛІЗ ТЕХНОЛОГІЙ FRONT-END РОЗРОБКИ

ГЛАВАЦЬКА Д., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто технології, що використовуються для front-end розробки. Аналіз технології front-end є важливим напрямом дослідження. Попередні дослідження в цій сфері були спрямовані на порівняння різних фреймворків та бібліотек для front-end, вивчення впливу технологій та інструментів на користувацький досвід та продуктивність, а також на виявлення впливу нових технологій на front-end. В результаті таких досліджень було визначено найкращі підходи до front-end розробки, оптимальні інструменти та технології, що покращують продуктивність та користувацький досвід. Аналіз технології front-end допомагає розробникам бути в курсі останніх тенденцій та використовувати нові технології для покращення своїх продуктів.

The article considers Technologies used for front-end development. Analysis of front-end development technology is a research area in the field of web development. Previous research in this area has focused on comparing different frameworks and libraries for front-end development, studying the impact of technologies and tools on user experience and performance, and identifying the impact of new technologies on front-end development. As a result of such research, the best approaches to front-end development, optimal tools and technologies that improve productivity and user experience have been determined. Analysis of front-end development technologies is ready for developers to stay abreast of the latest trends and use new technologies to improve their products.

Актуальність. У віковій епосі цифрового прогресу, коли користувачі вимагають більше функціональності та естетичності з програм та веб-сайтів, роль фронтенд розробки стає надзвичайно важливою. Від інтерфейсу користувача до взаємодії з платформою, технології фронтенду стали основою успіху в сфері розробки програмного забезпечення. У даній статті ми розглянемо глибокий аналіз найсучасніших технологій фронтенд розробки, розкриючи їх переваги, недоліки та сфери застосування. Вивчення цих технологій дозволить нам краще зрозуміти, як забезпечити найвищу якість користувацького досвіду та досягти успіху у вимогливому цифровому світі.

Сфера front-end розробка – це процес створення веб додатків або сайтів, що охоплює розробку імовірної частини клієнтського інтерфейсу. З моменту народження веб-розробки, front-end технології зазнавали численних змін та вдосконалень. Сьогодні front-end -розробка є дуже важливою для розробки сучасних веб-додатків та мобільних додатків.

Однією з головних причин актуальності front-end розробки є постійна зміна технологій та тенденцій. Кожен рік виходять нові фреймворки, бібліотеки та інструменти для front-end розробки. Це ставить перед front-end розробниками виклик, оскільки вони повинні встигати за новими технологіями та уміти працювати з ними.

Крім того, з появою мобільних пристроїв та технології responsive design, важливість front-end розробки зросла ще більше. Клієнти очікують, що веб-сайти та додатки будуть працювати на різних пристроях з різними розмірами екрану та забезпечувати зручний користувацький досвід на всіх пристроях.

Крім того, front-end розробка є важливою складовою для забезпечення SEO оптимізації та збільшення конверсії веб сайтів та додатків. Відправна точка взаємодії між користувачем

та веб сайтом або додатком знаходиться саме на front-end, тому дизайн та функціональність фронтенду має вирішальне значення для привернення та утримання відвідувачів.

Метою статті є розгляд технології та інструментів, які використовуються для front-end. Наприклад, ECMAScript & JavaScript, HTML5, CSS3 & Sass, JQuery, JSON, AJAX. А також практичне застосування технологій та навичок, необхідних для front-end розробки, таких як робота зі змінними, компонентою архітектурою, обробкою подій тощо.

Об'єктом дослідження є фреймворки, бібліотеки та інші інструменти front-end розробки. Наприклад, технології, пов'язані з дизайном та верстkою, такі як HTML, CSS та JavaScript, які використовуються для створення користувацького інтерфейсу.

Предмет дослідження – аналіз технологій та інструментів, що використовуються для front-end розробки. Це охоплює вивчення найбільш популярних фреймворків та бібліотек, а також інших інструментів, які допомагають у розробці.

Аналіз попередніх досліджень. Попередні дослідження у галузі front-end розробки були спрямовані на вивчення різних аспектів цієї галузі та її впливу на веб розробку в цілому.

Одним з найбільш популярних напрямів досліджень є порівняння різних фреймворків та бібліотек для front-end розробки. У таких дослідженнях порівнюються переваги та недоліки кожного інструменту, що допомагає розробникам вибрати найбільш підходящий для їх потреб.

Інші дослідження у галузі front-end розробки спрямовані на розуміння впливу технологій та інструментів на користувацький досвід та продуктивність. Такі дослідження допомагають виявити найкращі підходи до front-end розробки, які забезпечують оптимальну продуктивність та задоволення користувачів.

У сфері front-end розробки вивчається вплив нових технологій, таких як Progressive Web Apps (PWA), WebAssembly, Web Components та інші. Дослідження в цій області допомагають розробникам бути в курсі останніх тенденцій та використовувати нові технології для покращення своїх продуктів. Узагальнюючи, попередні дослідження підтверджують важливість front-end -розробки для успішної веб-розробки та показують шляхи для покращення цієї галузі, такі як використання нових технологій та оптимізація продуктивності та користувацького досвіду.

Виклад основного матеріалу. Технології, що використовуються для front-end розробки можна розділити на категорії, що представлені нижче.

ECMAScript & JavaScript.

ECMAScript – стандарт мови програмування, затверджений міжнародною організацією *ECMA* згідно зі специфікацією *ECMA*-262.

JavaScript (JS) – реалізація стандарту *ECMAScript*. Це прототипно-орієнтована динамічна мова, що має декілька парадигм та підтримує об'єктно-орієнтований, імперативний та декларативний (тобто функціональне програмування) стилі. *JavaScript* код інтерпретується або компілюється під час виконання. Хоча *JavaScript* насамперед відома як скриптова мова для веб-сторінок, вона також використовується у багатьох небраузерних середовищах: *node.js, Apache CouchDB* та *Adobe Acrobat*.

HTML5.

HTML – це простий код, що інтерпретується веб браузером (таким як *Chrome, Firefox* чи *Safari*) для відображення веб сторінки для користувача. *HTML* не є мовою програмування. Це форма збереження даних.

HTML розшифровується як "Мова розмітки гіпертексту". Гіпертекст означає тип тексту, який підтримує гіперпосилання між сторінками. Розмітка (*markup*) означає, що ми отримали документ із зміщеним кодом для того, щоб повідомити браузеру як треба інтерпретувати сторінку. *HTML* код побудований за допомогою тегів, кожен з яких починається із < і закінчується на >. Теги представляють елементи розмітки. *HTML5* є найновішим стандартом *HTML*. Це новий виток у розвитку інтернет-простору, який ще не до кінця сформувався, але можливості якого вже в більшості випадків використовують багато браузерів.

Технологія *HTML5* дозволяє: спростити розмітку сторінок, зменшивши їх розмір; істотно полегшити завдання для творців макетів сторінок сайтів. У *HTML5* введено безліч нових можливостей, які в розмітці коду сторінок можуть використовувати дизайнери, наприклад, нові елементи форм, мультимедіа, *API* та інше. І не дивлячись на те, що при побудові сайтів зараз далеко не всі можливості *HTML5* можуть бути використані, багато пошукових систем дуже лояльно ставляться до таких сайтів, в розмітці яких використовуються переваги HTML5.

CSS3 & Sass.

CSS (абревіатура від *Cascading Style Sheets*, що в перекладі означає каскадні таблиці стилів) – технологія опису зовнішнього вигляду документа, написаного мовою розмітки. Найчастіше *CSS* використовується для документів, котрі розмічені мовою *HTML*, *XHTML* та *XML*.

CSS використовується розробниками веб сторінок для завдання кольорів, шрифтів, розташування і інших аспектів представлення документа. Основною метою розробки *CSS* було розділення вмісту (написаного на *HTML* або іншій мові розмітки) від представлення стилю документа. Це розділення може збільшити доступність документа, надати велику гнучкість і можливість управління його виглядом, а також зменшити складність і повторюваність в структурному вмісті. Крім того, *CSS* дозволяє представляти один і той же документ в різних стилях.

Стандарт *CSS* визначає пріоритети, у порядку яких застосовуються правила стилів, якщо для якогось елементу підходять деякі правила одночасно. Це називається "каскадом", в якому для правил розраховуються пріоритети або "ваги", що робить результати передбаченими. Таблиця стилів складається з набору правил. Кожне правило, у свою чергу, складається з одного або декількох селекторів, розділених комами, а також блоку визначень.

*CSS*3 – це новий стандарт оформлення *HTML* документів значно розширюючий можливості попереднього стандарту *CSS*2.1. Багато можливостей, які були важкодоступні в *CSS*2.1, тобто вимагали використання додаткових зовнішніх програм (таких як *Adobe Photoshop*), скриптів (таких як *JavaScript*) або спеціальних "хитрощів" можуть легко досягатися в *CSS*3 за рахунок використання нових властивостей оформлення.

Sass (*Syntactically Awesome Stylesheets*) – це *CSS*-препроцессор, який надає додатковий набір функцій, призначених для підвищення рівня абстракції коду та спрощення файлів *CSS*.

Скриптова мова *Sass* має два синтаксиси:

- *sass* (оригінальний) – відрізняється відсутністю фігурних дужок, в ньому вкладені елементи реалізовані за допомогою відступів, а правила відокремлюються переведенням рядка;
- *scss* (новий) – використовує фігурні дужки (подібно до *CSS*).

Файли *sass*-синтаксису мають розширення *.sass*, *scss*-синтаксису – *.scss*.

Sass розширює *CSS*, надаючи кілька механізмів, доступних в більш традиційних мовах програмування, зокрема об'єктно-орієнтованих мовах, але недоступних для *CSS*. Інтерпретатор *Sass* транслює *SassScript* у блоки правил *CSS*.

JQuery.

jQuery – це фреймворк розроблений на мові *JavaScript* з метою спрощення написання об'ємного коду. Бібліотека *jQuery* містить в собі велику кількість вже прописаних функцій, що дозволяють швидко та якісно створювати інтерактивні сторінки веб-сайту. Використовують *jQuery* як в програмуванні елементів веб-сторінок так і в створенні різного типу додатків.

JSON.

JavaScript Object Notation (*JSON*, об'єктний запис *JavaScript*) – це формат обміну даними. Не зважаючи на те, що *JSON* не є строгою підмножиною *JavaScript*, він нагадує його синтаксис. Хоча багато мов програмування підтримують *JSON*, та він є особливо корисним для використання у програмах, що базуються на *JavaScript*, таких, як веб-сайти чи розширення браузерів.

JSON може представляти числа, булеві значення, строки, *null*, масиви (впорядковані послідовності значень) та об'єкти (пари ключ-значення), що включають у себе ці значення, чи інші об’єкти та масиви. *JSON* не підтримує представлення більш складних даних, таких як функції, регулярні вирази, дати та інше. (Об'єкти *Date* за замовчуванням серіалізуються у строку, що містить дату у форматі *ISO*, отже інформація не є остаточно втраченою).

AJAX.

AJAX (*Asynchronous JavaScript And XML*) – підхід до побудови користувацьких інтерфейсів веб-застосунків, у якому веб-сторінка, не перезавантажуючись, у фоновому режимі надсилає запити на сервер і сама звідти завантажує потрібні користувачу дані.

AJAX – один з компонентів концепції *DHTML* (*Dynamic HTML*).

Ключовим моментом *AJAX*-запиту є об'єкт *XMLHttpRequest* – *API*-запит веб-клієнта (браузера) до веб-сервера за протоколом *HTTP* у фоновому режимі, для мов програмування *JavaScript*, *JScript*, *VBScript* і подібних.

Використовується для синхронного або асинхронного обміну інформацією в довільному текстовому форматі (наприклад *XML*, *JSON*, *HTML*).

Механізм роботи: через запит до сервера генерується сторінка, яку буде бачити користувач. Запити користувача будуть звертатися до *AJAX*-модулю, який забезпечує роботу з сервером через динамічні звернення. Інформація з бази даних зберігається в *XML*-файлі, який формується динамічно і виводить інформацію на сторінку сайту. *AJAX* передбачає асинхронний зв’язок. Це означає, що події не наступають негайно після певної дії, а може пройти достатньо часу, перш ніж буде отримано відповідь. На деякі запити відповідь взагалі можна і не отримати (рис. 1).

Рис. 1. Робота AJAX-запиту до бази даних

Переваги *AJAX*: підвищення інтерактивності і динамічності веб-сторінок за рахунок зменшення об’єму інформації, що завантажується; зменшення навантаження на сервер, що важливо, враховуючи постійне зростання потоків інформації в мережі Інтернет. Також *AJAX* забезпечує покращення функціональності сайту.

До недоліків *AJAX* слід віднести: безпеку (можливість прочитати вихідний код у браузері), неможливість реєстрації браузерами історії відвідування сторінок (не працюватиме кнопка «Backward»), проблеми індексації пошуковими системами (динамічно завантажений контент недоступний для пошукових ботів). Тому доцільно використовувати *AJAX* тільки для окремих частин контенту сайту.

- Система управління *WordPress* швидка, проста для замінювання коду та достатньо гнучка.
- Оновлення *WordPress* плагінів, тем та системи відбувається автоматично.
- У середовищі *WordPress* легко налаштовуються віджети (блоки) та меню, а також є редактор *HTML* сторінок.
- Розробниками *WordPress* передбачено ретранслювання тегів з кирилиці у латиницю для правильної індексації сторінок у пошукових системах.

Висновки. Аналіз технології front-end розробки є важливим напрямом дослідження у галузі веб-розробки, оскільки front-end розробка є важливою складовою створення веб-додатків та сайтів. У ході досліджень було виявлено, що використання фреймворків та бібліотек допомагає значно скоротити час розробки та покращити продуктивність. Також було визначено, що використання новітніх технологій, таких як HTML5 та CSS3, дозволяє створювати більш інтерактивні та привабливі інтерфейси. Окрім того, було виявлено, що впровадження підходів до розробки з використанням Agile та DevOps допомагає зменшити час розробки та поліпшити якість продукту.

У підсумку аналізу сучасних технологій фронтенд розробки відкривається вражаюче поле можливостей для створення інноваційних та захоплюючих веб-додатків. Швидкий розвиток інтернету вимагає від розробників не тільки вміння володіти інструментами, але й глибокого розуміння потреб користувачів та трендів сучасного веб-світу.

Вибір технологій залежить від конкретних вимог проекту: від простоти та ефективності чистого HTML/CSS/Javascript до потужності фреймворків, таких як React, Vue та Angular. Кожен із цих виборів має свої плюси та мінуси, і їхня вірна імплементація залежатиме від завдання, яке потрібно вирішити.

Технології розробки фронтенду постійно еволюціонують, і важливо залишатись на чолі інновацій. Розуміння не тільки технічних аспектів, але й дизайну, взаємодії з користувачем та відповідності сучасним стандартам безпеки є критичними для створення високоякісних та конкурентоспроможних продуктів.

Усі ці аспекти свідчать про те, що фронтенд розробка є більше, ніж просто технічний процес. Це мистецтво створення гармонійного та зручного веб-досвіду для користувачів, яке вимагає глибокого розуміння взаємодії між технологіями, дизайном та прагненням задовольнити потреби сучасної аудиторії.

Отже, вивчення, аналіз та впровадження сучасних технологій фронтенд розробки є ключем до творення інноваційних веб-продуктів, які не лише задовольняють потреби користувачів, але й сприяють розвитку інтернет-середовища загалом.

Висновки з цього дослідження допоможуть розробникам зрозуміти, які технології та інструменти можна використовувати для покращення продуктивності та якості front-end розробки. Крім того, розробники зможуть використовувати рекомендації з цього дослідження для вибору оптимального набору технологій та інструментів для своїх проектів.

Отже, аналіз технології front-end розробки є важливим кроком у розробці веб-додатків та сайтів, оскільки дозволяє виявити оптимальний підхід до розробки, вибрати найкращі інструменти та технології, що покращують продуктивність та користувацький досвід, та зрозуміти, які нові тенденції відбуваються в цій галузі.

Список використаних джерел

1. Сайт для перевірки швидкості завантаження веб порталів URL: https://tools.pingdom.com/
2. Smashing Magazine URL: https://www.smashingmagazine.com/
3. CSS-Tricks URL: https://css-tricks.com/
4. A List Apart URL: https://alistapart.com/
5. SitePoint URL: https://www.sitepoint.com/
6. JavaScript Weekly URL: https://javascriptweekly.com/
7. Front-End Front URL: https://frontendfront.com/
8. CSS Grid - https://cssgrid.io/

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н.О.

ДОСЛІДЖЕННЯ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ДЛЯ АВТОМАТИЗОВАНИХ СИСТЕМ ЗБОРУ, АНАЛІЗУ ТА ЗБЕРІГАННЯ МАРКЕТИНГОВИХ ДАНИХ З СОЦІАЛЬНИХ МЕРЕЖ

ГОЛУБ Ю., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглядається дослідження інструментальних засобів для автоматизованих систем збору, аналізу та зберігання маркетингових даних з соціальних мереж. Детально описано актуальність, мету, об'єкт та предмет дослідження, а також викладено основний матеріал, що стосується різних інструментів, які дозволяють ефективно використовувати соціальні медіа-платформи для маркетингової діяльності.

The article explores the research of instrumental tools for automated systems of collecting, analyzing and storing marketing data from social media. The relevance, purpose, object, and subject of the research are described in detail, and the main material related to different tools that allow efficient use of social media platforms for marketing activities is presented.

Дана стаття присвячена дослідженню інструментальних засобів для автоматизованих систем збору, аналізу та зберігання маркетингових даних з соціальних мереж.

Актуальність дослідження. Під час цифрової епохи соціальні медіа-платформи є одними з найбільш важливих каналів маркетингової комунікації. Кількість користувачів соціальних мереж постійно зростає, а отже, вони стають все більш привабливими для маркетологів, які можуть зібрати велику кількість цінної інформації про своїх клієнтів.

Однак, збір, аналіз та зберігання цієї інформації може бути вкрай складним завданням через велику кількість даних та їх розпорошеність по різних платформах. Тому, розробка інструментальних засобів для автоматизованого збору, аналізу та зберігання маркетингових даних з соціальних мереж є актуальною проблемою для сучасних маркетологів та дослідників. Використання таких інструментів може значно полегшити процес збору та аналізу даних, дозволяючи більш ефективно використовувати їх для підвищення ефективності маркетингових стратегій та збільшення продажів. Отже, дослідження інструментальних засобів для автоматизованих систем збору, аналізу та зберігання маркетингових даних соціальних мереж є важливою темою для науковців та практиків у галузі маркетингу.

Основною метою дослідження є встановлення ефективних інструментальних засобів для автоматизованої збірки, аналізу та зберігання маркетингових даних з соціальних мереж, що дозволить оптимізувати процеси збору та аналізу даних, забезпечити їх достовірність та зручний доступ до них.

Проведення дослідження актуально в контексті активного використання соціальних мереж в маркетингу, де велика кількість інформації про цільову аудиторію може бути зібрана, проаналізована та використана для оптимізації рекламних кампаній.

Основна мета дослідження полягає у визначенні найбільш ефективних інструментальних засобів для збору та аналізу даних з соціальних мереж, таких як засоби збору даних, засоби візуалізації та аналізу даних, засоби зберігання та обробки даних. Важливим етапом дослідження є порівняння різних програмних рішень та встановлення їх переваг та недоліків в контексті використання їх для автоматизованої збірки, аналізу та зберігання маркетингових даних з соціальних мереж.

Об'єктом дослідження є інструментальні засоби, призначені для автоматизованого збору, аналізу та зберігання маркетингових даних з соціальних мереж. Дослідження спрямоване на визначення ефективних методів та інструментів збору та аналізу маркетингової інформації з соціальних мереж з метою покращення стратегій маркетингу та продажів,

збільшення прибутків підприємства та підвищення рівня конкурентоспроможності. Дослідження також має на меті виявлення недоліків та проблем, що виникають під час використання інструментів для збору та аналізу маркетингової інформації з соціальних мереж, та розробки рекомендацій щодо їх усунення.

Предметом дослідження статті є інструментальні засоби, які використовуються для автоматизованої збірки, аналізу та зберігання маркетингових даних з соціальних мереж. Дослідження охоплює широкий спектр інструментів, таких як соціальний моніторинг, аналітику соціальних мереж, інструменти автоматизації маркетингових кампаній та інші. Основна увага зосереджена на вивченні можливостей та ефективності використання цих інструментів для збору та аналізу маркетингових даних з соціальних мереж.

Виклад основного матеріалу. У сучасному світі зі зростанням кількості інформації та змін в способах її споживання, маркетологам необхідно швидко та ефективно збирати, аналізувати та зберігати дані, щоб приймати обґрунтовані рішення щодо стратегій реклами та продажів. Одним з джерел таких даних є соціальні мережі, які вже давно стали невід'ємною частиною нашого життя та ділового середовища. Це створює потребу в автоматизованих системах збору, аналізу та зберігання маркетингових даних з соціальних мереж.

Соціальні мережі є важливим джерелом маркетингових даних для бізнесу. Інформація, яку користувачі діляться у соціальних мережах, може бути використана для розуміння поведінки та потреб споживачів, а також для покращення взаємодії з ними та збільшення продажів.

Однак, збір та аналіз маркетингових даних з соціальних мереж може бути викликанням для бізнесу. Він вимагає багато часу та зусиль для збору даних, аналізу та зберігання. Для того, щоб підприємство могло використовувати соціальні мережі як ефективний інструмент маркетингу, воно повинно мати доступ до інструментальних засобів для автоматизованої системи збору, аналізу та зберігання маркетингових даних з соціальних мереж.

Один із таких інструментальних засобів - соціально-медіа моніторингові системи, які дозволяють бізнесу правильно вести аналіз та зберігання маркетингових даних.

У сучасному світі соціальні мережі стали невід'ємною частиною життя людей та бізнесу. Вони є потужним інструментом для залучення та збереження клієнтів, вивчення їхніх потреб та побажань, а також для підвищення свідомості про бренд. Автоматизовані системи збору, аналізу та зберігання маркетингових даних з соціальних мереж допомагають підвищити ефективність маркетингу та забезпечують швидкий доступ до важливої інформації [1].

Один з основних інструментів для автоматизації збору маркетингових даних з соціальних мереж - це програмні інтерфейси додатків (API). Вони дозволяють отримувати доступ до даних, що публікуються користувачами у соціальних мережах, і дозволяють збирати та аналізувати ці дані. Іншим інструментом є програми-аналізатори, які дозволяють проводити різноманітний аналіз даних з соціальних мереж. Вони можуть допомогти виявити тенденції та поведінку споживачів, що допомагає бізнесу адаптуватися до їхніх потреб та бажань.

Інший інструмент для автоматизованої системи збору та аналізу маркетингових даних з соціальних мереж – це системи управління відносинами з клієнтами (CRM). Вони дозволяють збирати та організовувати дані про клієнтів, що дозволяє бізнесу бути більш ефективним у взаєминах з ними. Більшість CRM-систем мають інтеграцію з соціальними мережами, що дозволяє збирати дані про клієнтів з різних джерел і зберігати їх в одному місці. Це дозволяє бізнесу легко відстежувати поведінку клієнтів та проводити аналіз їхніх дій на різних платформах.

Крім того, інструментарій для автоматизованої системи збору, аналізу та зберігання маркетингових даних з соціальних мереж включає також веб-скрапінг. Це процес автоматичного збору даних з різних веб-сайтів, включаючи соціальні мережі. Веб-скрапінг дозволяє збирати інформацію з різних джерел та зберігати її у зручному форматі.

Дослідження цих даних може надати цінну інформацію про потенційних клієнтів, їхні вподобання та поведінку, що дозволить бізнесу покращити свої продукти та послуги та збільшити прибуток. У цій статті ми розглянемо найпопулярніші інструментальні засоби для

автоматизованої системи збору, аналізу та зберігання маркетингових даних з соціальних мереж.

Brandwatch – це інструмент, який дозволяє збирати та аналізувати дані з більш ніж 85 мереж соціальних мереж, включаючи Twitter, Facebook, Instagram, YouTube та інші. Brandwatch надає можливість відстежувати репутацію бренду в реальному часі, аналізувати думки та відгуки клієнтів, визначати тенденції та знайомитися з новими ідеями для розвитку бізнесу.

Hootsuite – це платформа для управління соціальними мережами, яка дозволяє планувати та публікувати контент в соціальних мережах, а також відстежувати та аналізувати реакції клієнтів на публікації. Hootsuite також надає можливість створювати звіти та аналізувати дані про залученість та ефективність контенту.

Sprout Social – це інструмент, який дозволяє управляти всіма аспектами соціальних мереж, включаючи публікацію контенту, взаємодію з клієнтами та аналіз реакцій на контент. Сервіс надає можливість відстежувати діяльність конкурентів, визначати тенденції та виявляти можливості для розвитку бізнесу.

Mention – це інструмент, який дозволяє відстежувати згадки про бренд в соціальних мережах, блогах та новинах. Сервіс надає можливість відстежувати репутацію бренду, аналізувати теми, які найбільше цікавлять користувачів, та виявляти можливості для розвитку бізнесу.

Semrush – це інструмент для аналізу та планування маркетингових кампаній в інтернеті, включаючи соціальні мережі. Semrush надає можливість аналізувати ключові слова, конкурентів та розкривати нові можливості для розвитку бізнесу [2].

Загалом, автоматизована система збору, аналізу та зберігання маркетингових даних з соціальних мереж допомагає бізнесу зекономити час та зусилля, які потрібні для збору та аналізу даних вручну. Вона дозволяє збирати більш точну та повну інформацію про клієнтів, що допомагає бізнесу підвищити ефективність маркетингу та забезпечує більш точне прогнозування ринку. Крім того, автоматизована система збору та аналізу маркетингових даних з соціальних мереж дозволяє бізнесу бути більш адаптивним до змін у потребах та бажаннях клієнтів та підвищує шанси на успіх у конкурентному середовищі.

Функціональність рішень даного програмного продукту передбачає:

- Збір даних з різних соціальних мереж, таких як Facebook, Twitter, LinkedIn, Instagram, YouTube тощо.
- Можливість моніторингу та аналізу поведінки користувачів в соціальних мережах, включаючи їхні інтереси, попередні покупки, поведінку в онлайн-середовищі тощо.
- Фільтрація та сегментація даних для подальшого використання в маркетингових кампаніях.
- Можливість інтеграції з іншими інструментами для збору даних, такими як Google Analytics, Adobe Analytics, SEMrush тощо.
- Можливість створення звітів та графіків для відображення результатів аналізу даних.
- Захист даних користувачів та дотримання стандартів безпеки даних.
- Надання рекомендацій для поліпшення маркетингових стратегій на основі аналізу зібраних даних з соціальних мереж.

Одним з головних факторів впливу соціальних мереж на маркетингові стратегії підприємств є залучення цільової аудиторії. Завдяки соціальним мережам, підприємства мають можливість налаштовувати свої рекламні кампанії таким чином, щоб вони були спрямовані на конкретну групу користувачів, яка має інтерес до їхніх товарів та послуг. Це дозволяє підприємствам ефективно використовувати свої рекламні бюджети та забезпечувати високу конверсію рекламних оголошень.

Також важливою складовою успішної маркетингової стратегії на соціальних мережах є взаємодія зі спільнотою. Підприємства, які активно взаємодіють зі своїми клієнтами на соціальних мережах, мають більше шансів залучити нових клієнтів та зберегти існуючу базу.

Для цього вони використовують різні інструменти, такі як створення спеціальних груп або чатів, проведення конкурсів та акцій, відповіді на питання та коментарі.

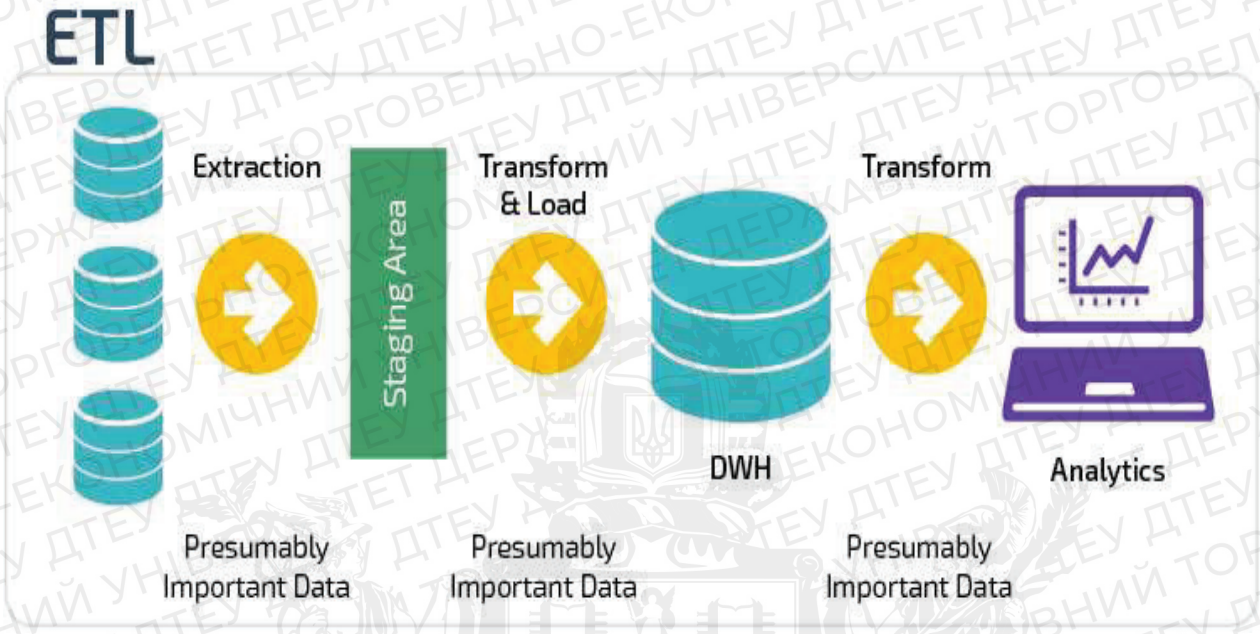


Рис. 1. Приклад концепції збору, обробки та зберігання даних.

Збір, аналіз та зберігання маркетингових даних з соціальних мереж - це важливий етап в розвитку ефективної маркетингової стратегії. Завдяки розробленим інструментам збору, аналізу та зберігання даних, компанії мають можливість збирати інформацію про споживачів та їх поведінку в соціальних мережах. Це дозволяє зробити маркетингові кампанії більш ефективними та націленими на конкретних споживачів.

Перший етап передбачає визначення метрик та цілей, що дозволяють оцінювати ефективність маркетингових кампаній в соціальних мережах. До основних метрик можна віднести кількість переглядів, лайків, коментарів, репостів та конверсію.

Другий етап передбачає вибір інструментів збору даних з соціальних мереж. До таких інструментів можна віднести соціальні моніторингові системи, які забезпечують моніторинг та аналіз відгуків про бренд, продукти та послуги на основних платформах соціальних мереж.

Після вибору інструментів необхідно зібрати дані з соціальних мереж. Для збору даних можна використовувати API (Application Programming Interface) соціальних мереж, які дозволяють отримувати різні дані, такі як профілі користувачів, повідомлення, лайки, коментарі тощо.

Після збору даних необхідно їх обробити та підготувати до аналізу. Це включає в себе чистку даних від спаму та непотрібної інформації, їх структурування та підготовку для подальшого аналізу.

Після підготовки даних до аналізу, необхідно визначити головні напрямки дослідження та виконати аналіз даних. Наприклад, можна досліджувати поведінку користувачів у соціальних мережах, їх інтереси та переваги, а також вплив маркетингових кампаній на їх поведінку.

Після аналізу даних необхідно зберегти їх для подальшого використання. Для зберігання можна використовувати бази даних, в яких зберігається інформація про користувачів, їхні повідомлення, лайки, коментарі тощо.

Важливим аспектом зберігання даних є їх безпека та конфіденційність. Компанії повинні забезпечувати захист даних від несанкціонованого доступу та зловживань. Для цього можна використовувати різні інструменти, такі як шифрування даних, двофакторна аутентифікація, моніторинг доступу до даних тощо [3].

Узагальнюючи, збір, аналіз та зберігання маркетингових даних з соціальних мереж - це складний процес, що вимагає від компаній знань та досвіду в галузі маркетингу та аналітики. Однак, завдяки розробленим інструментам збору, аналізу та зберігання даних, компанії мають можливість зробити маркетингові кампанії більш ефективними та націленими на конкретних споживачів, що сприяє покращенню їхньої прибутковості та конкурентоспроможності на ринку.

Висновки. Можна сказати, що інструментальні засоби для автоматизованих систем збору, аналізу та зберігання маркетингових даних з соціальних мереж мають великий потенціал для використання в сучасному маркетингу. Ці інструменти можуть допомогти компаніям отримати цінну інформацію про своїх клієнтів та конкурентів, а також про тенденції ринку та споживацьку поведінку.

Інструменти збору даних можуть включати такі функції, як моніторинг соціальних мереж, збір даних про клієнтів та конкурентів, аналіз настроїв та поведінки споживачів, відстеження ефективності маркетингових кампаній та багато іншого. Ці засоби можуть допомогти компаніям більш ефективно налаштувати свої маркетингові кампанії та забезпечити більшу конкурентоспроможність.

Однак, слід пам'ятати, що використання інструментів для збору та аналізу даних з соціальних мереж може також стати об'єктом критики, особливо відносно питань приватності та безпеки даних. Тому компанії повинні дотримуватися етичних принципів використання цих інструментів та забезпечувати захист даних своїх клієнтів.

Загалом, збір та аналіз маркетингових даних з соціальних мереж є надзвичайно важливим для сучасного маркетингу, тому компанії повинні використовувати інструменти для автоматизованого збору, аналізу та зберігання даних для того, щоб забезпечити більшу ефективність своїх маркетингових стратегій.

Список використаних джерел

1. Філ Барден. — Злам маркетингу. Наука про те, чому ми купуємо. — 2020р. Україна.
2. Modeling and Analysis of A Modeling and Analysis of Automated St omated Storage and Retrie age and Retrievals System. 2015 p. URL: https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1076&context=etd
3. Analysis and improvement of a chaos-based Hash function construction \\ Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1007570409003426 (останнє звернення 02.03.2023р.)
4. Cryptographic Hash Functions: A Review \\ Режим доступу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=85abc4805adb741b0f8c962794d2ab4dac975c5f (останнє звернення 03.03.2023р.)
5. An efficient implementation of hash function processor for ipsec \\ Режим доступу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4ad55cff822563aafb31a1533eaa60afbeec37aa (останнє звернення 05.03.2023р.)
6. A Novel Improvement with an Effective Expansion to Enhance the MD5 Hash Function for Verification of a Secure E-Document \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/9072400 (останнє звернення 05.03.2023р.)
7. Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms \\ Режим доступу: https://link.springer.com/chapter/10.1007/978-3-540-85174-5_9 (останнє звернення 05.03.2023р.)
8. Big data storage and analytics. 2013y. URL: https://www.techtarget.com/searchstorage/feature/Big-data-storage-and-analytics

Робота виконана під науковим керівництвом к.пед.н., доцента
ЖИРОВОЇ Т.О.

ТЕХНОЛОГІЯ БЛОКЧЕЙН: РЕВОЛЮЦІЯ В ЗАХИСТІ ІНФОРМАЦІЇ

ГОЛУБЧУК І., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

В останні роки технологія блокчейн стала однією з найперспективніших інновацій у світі цифрових транзакцій. Спочатку розроблений як базова технологія для криптовалюти біткойн, блокчейн згодом перетворився на універсальний інструмент для широкого спектру застосувань, від безпечних фінансових транзакцій до управління ланцюгом поставок тощо.

In recent years, blockchain technology has emerged as one of the most promising innovations in the world of digital transactions. Originally developed as the underlying technology for the cryptocurrency Bitcoin, blockchain has since evolved to become a versatile tool for a wide range of applications, from secure financial transactions to supply chain management and more.

Актуальність. Одним із найбільш помітних застосувань технології блокчейн є сфера криптовалют. Біткойн, перша і найвідоміша криптовалюта, використовує технологію блокчейн для безпечного запису та перевірки транзакцій між користувачами. Замість того, щоб покладатися на централізований орган, такий як банк чи уряд, транзакції біткойн перевіряються та записуються мережею комп'ютерів по всьому світу. Це робить систему набагато безпечнішою та стійкішою до шахрайства, оскільки немає єдиної точки збою чи вразливості.

За своєю суттю блокчейн — це децентралізована цифрова книга, яка записує транзакції або дані в мережі комп'ютерів. Кожен блок даних у блокчейні містить криптографічний хеш попереднього блоку, створюючи ланцюжок блоків, який надзвичайно важко підробити. Оскільки блокчейн підтримується мережею комп'ютерів, а не одним органом, він також дуже стійкий до шахрайства та злому.

Крім криптовалют, технологія блокчейн має широкий спектр інших потенційних застосувань. Наприклад, блокчейн можна використовувати для створення безпечних, захищених від підробок записів транзакцій або даних, що робить його ідеальним для додатків, таких як керування ланцюгом поставок, де важливо відстежувати переміщення товарів з одного місця в інше. Подібним чином блокчейн можна використовувати для створення безпечних цифрових ідентифікацій, стійких до шахрайства та злому. Ще одним перспективним застосуванням технології блокчейн є сфера смарт-контрактів. Смарт-контракт — це самовиконуваний контракт, який зберігається в блокчейні та автоматично виконується, коли виконуються певні умови. Наприклад, смарт-контракт можна використовувати для автоматичної передачі права власності на майно, коли покупець і продавець виконали свої відповідні зобов'язання.

Незважаючи на численні потенційні застосування, технологія блокчейн все ще є відносно новою, і перед її широким впровадженням необхідно вирішити багато проблем. Наприклад, масштабованість та енергоефективність блокчейн-мереж все ще є основними проблемами, які потребують вирішення.

Метою статті є дослідження основних методів захисту за допомогою технології Blockchain.

Об'єктом дослідження є розробка програмного забезпечення на основі технології Blockchain.

Предмет дослідження – Blockchain.

Аналіз попередніх досліджень. Дослідженню технології blockchain присвячені праці наступних науковців: Dylan Yaga(Ділан Яга), Peter Mell(Пітер Мелл), Qiang Wang(Цян Ван), Min Su(Мін Су), Nik Roby(Нік Робі), Karen Scarfone(Карен Скарфонета) та інші.

Виклад основного матеріалу. На сьогоднішній день необхідно знати принцип роботи блокчейну. Дані про роботу системи показані на рисунку 1

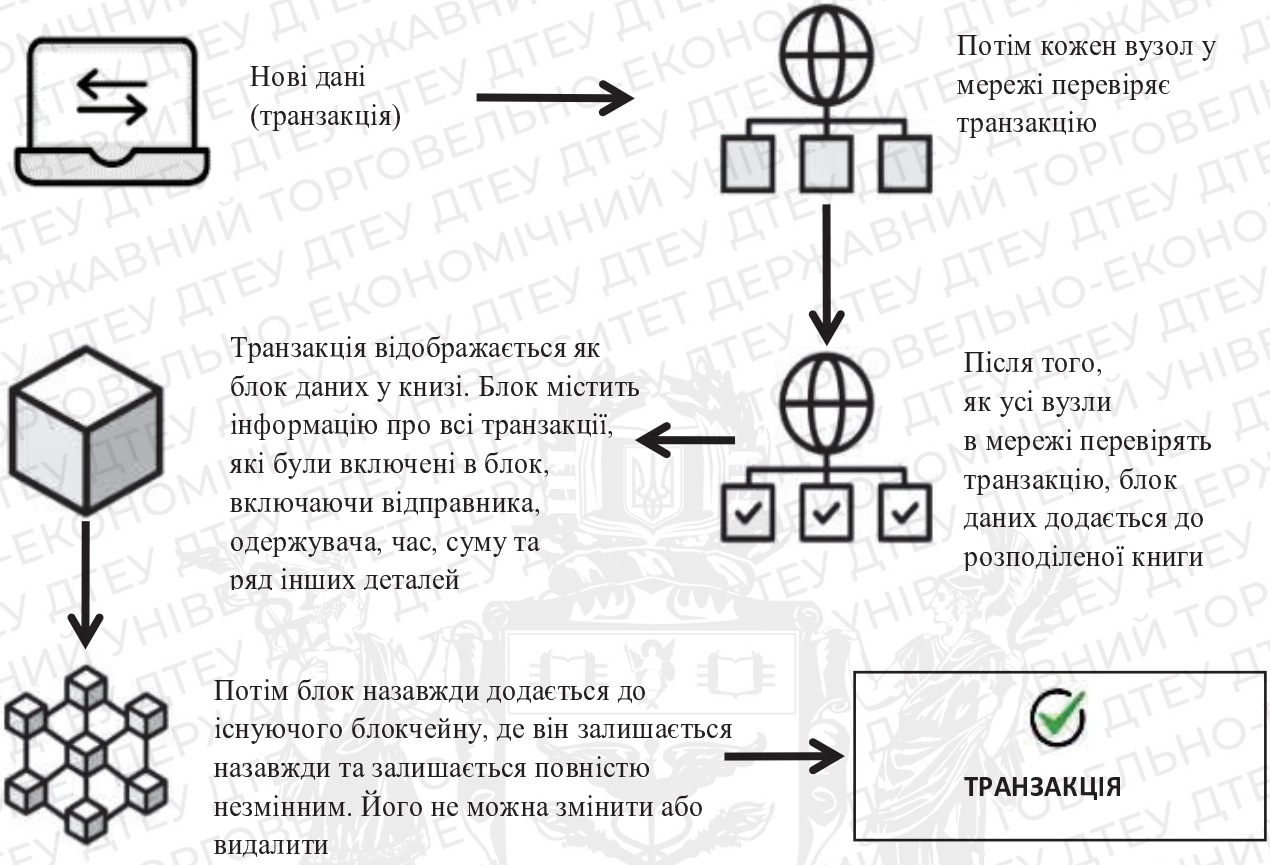


Рис. 1. Принцип роботи технології blockchain

Блокчейн — це прозора та децентралізована база даних (так звана розподілена книга), яка відстежує кожну однорангову транзакцію в режимі реального часу. Прозорий у тому сенсі, що будь-хто може переглядати загальнодоступний блокчейн . Децентралізовано в тому, що всі користувачі володіють ідентичними копіями цього блокчейну, і жодна особа чи орган не має керівної влади над цим блокчейном або його використанням.

Кожна транзакція реєструється та зберігається як блок інформації. Кожен блок визначається номером блоку та зберігає дані транзакції, включаючи суму транзакції та запис про те, між якими гаманцями транзакція відбулася. Кожен дійсний обмін даними призводить до ідентифікатора транзакції – унікального коду для кожної транзакції. Безпечно володіючи «приватним ключем» або паролем, користувачі можуть гарантувати, що їхні кошти або цифрові елементи доступні виключно для них самих.

Кожен блок «видобувається» або, точніше, криптографічно перевіряється, щоб автентифікувати та підтверджувати транзакції, що відбуваються в цьому блоці. Результатом цього процесу є «незмінна» (нередагована) база даних, яка завжди доступна (децентралізована) з усіма користувачами, які впевнені, що всі вони мають ту саму перевірену правильну інформацію, що й усі інші користувачі.[1]

Але постає питання, у чому сенс блокчейн технології?

Підприємствам, організаціям і приватним особам блокчейн:

- Усуває потребу в центральних точках надійності даних
- Усуває використання непотрібних посередників або «посередників»
- Дозволяє «ненадійну» поведінку та транзакції

Вище ми розібрали принцип роботи технології блокчейн, але необхідно розуміти, що у даній технології є багато типів та принципів роботи. У таблиці 1 продемонстрована порівняльна характеристика основних видів блокчейну.

Таблиця 1

Типи блокчейнів

Особливості	Консорціум	Приватний	Громадський	Гібрид
Використання	Фінанси, ланцюг поставок і дослідницька робота	Ланцюжок поставок, нерухомість та власність на активи	Перевірка документів і операції IoT	Сектор нерухомості та охорони здоров'я
Доступ	Контрольований доступ та охорона	Повністю контрольований доступ	Незалежний за своєю природою з повною прозорістю та довірою	Контрольований доступ і висока масштабованість
Прозорість/ можливість перевірки/ безпека	Відсутність прозорості	Відсутність ревізійності	Відсутність безпеки	Відсутність прозорості

У зв'язку з тим, що компанії та стартапи все частіше інтегрують блокчейн у системи своїх організацій, децентралізовану технологію було класифіковано на чотири основні типи на основі випадків її використання:

1. Громадський блокчейн.

Громадський блокчейн — це блокчейн-мережа з відкритим кодом. Вони дозволяють кожному бути частиною мережі як користувачам, розробникам, учасникам мережі та майнерам. Публічні блокчейни відкриті для рівноправної участі всіх учасників без будь-яких обмежень. Транзакції, що обробляються в загальнодоступному блокчейні, є повністю прозорими та доступними для всіх учасників мережі для вивчення їх деталей.

Загальнодоступний блокчейн є повністю децентралізованим за своєю природою, без центральної влади. Приватний блокчейн.

2. Приватний блокчейн

Приватні блокчейни — це дозволені блокчейни. Людям потрібен дозвіл, щоб приєднатися до цих блокчейнів. Транзакції в приватних блокчейнах є приватними за своєю природою і доступні лише учасникам мережі, які мають дозвіл працювати в приватному блокчейні.

Ці блокчейни важливі для підприємств, які співпрацюють і діляться своїми даними, але вони не хочуть вдаватися до своїх конфіденційних бізнес-даних у процесах у загальнодоступному блокчейні. Приватний блокчейн є набагато більш централізованим за своєю природою, оскільки різні об'єкти мережі керують ланцюгом, таким чином маючи рівний контроль над різними учасниками та структурами управління.

3. Гібридний блокчейн.

Гібридний блокчейн має екосистему з об'єднаними функціями загальнодоступної та приватної мережі блокчейнів. Це пояснює, що гібридний блокчейн містить конфіденційність і безпеку приватного блокчейну разом із прозорістю публічного блокчейну. Таким чином, гібридний блокчейн забезпечує гнучкість бізнес-операцій, забезпечуючи конфіденційність і вибір публічного розміщення будь-яких даних відповідно до їх зручності.

Гібридна екосистема можлива завдяки запатентованій міжланцюговій функції. Ця функція дозволяє ланцюжку з'єднуватися з іншими протоколами блокчейну. За допомогою гібридного механізму легко можливе формування багатоланцюгової мережі.

4. Блокчейн консорціуму.

Блокчейни консорціуму також відомі як федеративні блокчейни. Вони дозволяють будь-якому новому учаснику блоку підключати встановлену структуру та обмінюватися даними замість того, щоб починати з самого початку. За допомогою блокчейнів консорціуму організації зручно отримують рішення, щоб захистити свій час і витрати на розробку.

Існують різні переваги блокчейну консорціуму, такі як перевірка, контроль, безпека, економічна доцільність, гнучкість та енергія[2].

Очікується, що протягом наступних кількох років використання технології блокчейн значно зросте. Ця революційна технологія вважається інноваційною та руйнівною, оскільки блокчейн змінить існуючі бізнес-процеси за рахунок оптимізації ефективності та безпеки.

Технологія блокчейн забезпечує конкретні переваги для бізнесу, які допомагають компаніям у такі способи:

- встановлює довіру між сторонами, які ведуть спільний бізнес, пропонуючи надійні спільні дані;
- усуває виділені дані шляхом інтеграції даних в одну систему через розподілену книгу, спільну в мережі, доступ до якої мають сторони з відповідним дозволом;
- забезпечує високий рівень безпеки даних;
- зменшує потребу в сторонніх посередниках;
- створює записи в режимі реального часу, захищені від підробки, якими можна поділитися між усіма учасниками;
- дозволяє учасникам переконатися в автентичності та цілісності продуктів, розміщених у потоці торгівлі;
- забезпечує безперебійне відстеження та відстеження товарів і послуг у всьому ланцюжку постачання;

Блокчейн, безумовно, вигідний для організацій, але він має значні недоліки через певні проблеми безпеки.

Ось 5 головних проблем безпеки блокчейну та їх вирішення.

1. Напад Sybil

Під час атаки Sybil хакери створюють різноманітні підроблені мережеві вузли. використовуючи ці вузли, хакер досягне консенсусу більшості та порушить транзакції ланцюжка. Як наслідок, широкомасштабний напад Sybil – це не що інше, як атака 51%.

Щоб запобігти атакам Sybil:

- Використовуйте прийнятні алгоритми консенсусу.
- Відстежуйте поведінку альтернативних вузлів і перевіряйте вузли, які вимірюють блоки пересилання виключно від одного користувача.

Хоча ці алгоритми можуть не повністю запобігти цим атакам, вони створюють багато перешкод, і для хакерів майже неможливо здійснити атаки.

2. Вразливості кінцевих точок

Уразливість кінцевих точок блокчейну є ще однією важливою проблемою безпеки блокчейну.

Кінець мережі блокчейн знаходиться там, де користувачі діють за допомогою блокчейну: на електронних пристроях, таких як комп'ютери та мобільні телефони. Хакери спостерігатимуть за поведінкою користувачів і націлюватимуться на пристрої, щоб викрасти ключ користувача. Це може бути однією з найпомітніших проблем безпеки блокчейну.

Щоб запобігти кінцевій вразливості:

- Не зберігайте блокчейн-ключі на своєму ноутбуці чи мобільному телефоні як текстові файли.
- Передайте та встановіть пакети антивірусного програмного забезпечення для своїх електронних пристроїв.
- Часто перевіряйте систему, відстежуючи час, місцезнаходження та доступ до пристрою.

3. Атака 51%.

Атака 51% відбувається, коли одна особа або організація (зловмисні хакери) збирає 1/2 хеш-рейту та захоплює контроль над усією системою, що може мати катастрофічні наслідки. Хакери можуть змінити порядок транзакцій і запобігти їх підтвердженню.

Щоб запобігти атакам 51%:

- Переконайтеся, що хешрейт вищий.
- Покращте моніторинг пулу майнінгу.

4. Фішингові атаки

Метою хакера під час фішингової атаки є викрадення облікових даних користувача. вони надсилатимуть легітимні електронні листи власнику ключа гаманця. Від користувача вимагається ввести дані для входу через вкладене підроблене гіперпосилання. Доступ до облікових даних користувача та іншої конфіденційної інформації може призвести до збитків як для користувача, так і для мережі блокчейн. вони також схильні до наступних атак.

Щоб запобігти фішинговим атакам:

- Повторно зверніться до служби підтримки або партнера, якщо ви отримаєте електронний лист із запитом на дані для входу щодо проблеми.
- Не натискайте на посилання, доки ви їх ретельно не переглянете. Замість того, щоб натискати на посилання, введіть адресу в приватній вкладці вашого браузера.
- Уникайте мереж Wi-Fi відкритих або громадських кафе.
- Переконайтеся, що ваша система та програмне забезпечення оновлені.

5. Маршрутизація атак

Хакери можуть використовувати анонімність облікового запису для перехоплення даних, оскільки вони передаються постачальникам послуг Інтернету.

У разі атаки маршрутизації учасники блокчейну зазвичай не знають про загрозу, оскільки передача даних і операції відбуваються, як це було звичайно. Небезпека полягає в тому, що ці атаки часто відкривають конфіденційні дані або витягують валюту без відома користувача.

Щоб запобігти атакам маршрутизації:

- Використовуйте шифрування.
- Впровадити безпечні протоколи маршрутизації (із сертифікатами).
- Навчіть себе та своїх працівників про ризики, пов’язані з інформаційною безпекою [3].

Висновки. Технології блокчейну та штучного інтелекту вдосконалюються швидкими темпами та створюють можливості для обміну та об’єднання даних у спосіб, який раніше не передбачався.

Передача персональних даних створює головоломку для компаній і окремих осіб, що може принести цінні переваги, але також може створити великі ризики та витрати як для особи, так і для організацій, з якими надаються особисті дані. Blockchain надає нові механізми, такі як децентралізовані ідентифікатори та підтвердження з нульовим знанням, які дозволяють обмінюватися даними таким чином, щоб зберегти конфіденційність особи та дозволити користувачам зберігати контроль над своїми даними. Ці досягнення можуть забезпечити як підвищену кібербезпеку, так і більш практичне використання персональних даних.

Список використаних джерел

1. Research on information security technology based on blockchain \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/8386546 (останнє звернення 27.02.2023р.)
2. A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation \\ Режим доступу: https://dl.acm.org/doi/abs/10.1145/3287921.3287978 (останнє звернення 27.02.2023р.)
3. The benefits and threats of blockchain technology \\ Режим доступу: https://www.sciencedirect.com/science/article/pii/S138650562030154433 (останнє звернення 01.03.2023р.)

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

МЕХАНІЗМИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇХ РЕАЛІЗАЦІЯ ПРИ СТВОРЕННІ СИСТЕМИ СУПРОВОДУ ВСТУПНОЇ КАМПАНІЇ ЗВО

ГОРДЄЄВА І., 2м курс ФІТ ДТЕУ,
спеціальність «Кібребезпека та захист інформації»

У статті досліджено існуючі механізми політики інформаційної безпеки. Розкрито поняття інформаційної безпеки системи супроводу вступної компанії, запропоновано шляхи реалізації механізмів політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО.

The article examines the existing mechanisms of information security policy. The concept of information security of the admission company support system is revealed, ways of implementing information security policy mechanisms in the creation of the admission company support system of higher education institutions are proposed..

Актуальність. Суворі виклики сьогодення: нестабільна політична та соціально-економічна ситуація в країні, подолання наслідків пандемії короновірусу, повномасштабна агресія Російської Федерації проти України, акцентують ключові пріоритети національної безпеки, а саме питання інформаційної безпеки.

Інформаційна безпека характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і таке інше) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи. Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави.

Одним із складників забезпечення інформаційної безпеки виступає забезпечення інформаційної безпеки в системі супроводу вступної кампанії ЗВО. Своєчасна та об'єктивна інформація є важливим фактором механізму вступної кампанії, який можна розглядати крізь призму механізму політики інформаційної безпеки. Нові реалії функціонування системи освіти, виокреслили такі питання, які до сьогодні ніхто не вирішував.

Питання реалізації інформаційної безпеки при вступній кампанії ЗВО є питанням майбутнього країни. Адже, забезпечення інформаційної безпеки обумовлно не тільки інтересами держави, але й інтересами вступника – громадянина країни, на плечі якого покладено відродження та відбудова країни, залежить розвиток країни та формування світового іміджу.

Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність та достовірність. Інформаційна безпека містить в собі не тільки нормативно-правову та політичну складову, але також інституційну сферу, що передбачає діяльність органів, які її забезпечують, а також використання програмно-технічних засобів. З метою забезпечення інформаційної безпеки в Україні Указом Президента України від 25.02.2017 р. була затверджена «Доктрина інформаційної безпеки України» [1]. В сучасних умовах війни 18.03.2022 р. прийнято рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки» [2]. Наразі в Україні функціонує також Центр протидії дезінформації при РНБО України, на сайті якого

можна ознайомитись з актуальною інформацією та подіями в цій сфері.

Використання особливих форм і методів державного управління при забезпеченні інформаційної безпеки пояснюється необхідністю своєчасного реагування на виникаючі загрози політичного, економічного та військового характеру, оскільки в таких умовах використання звичайних традиційних правових механізмів не завжди призводить до очікуваного результату.

З огляду на це випливає, що одним із важливих напрямів інформаційної безпеки є реалізація механізму політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО.

Метою статті є вивчення теоретичних засад формування механізмів політики інформаційної безпеки та їх реалізації при створенні системи супроводу вступної кампанії ЗВО.

Об'єктом дослідження є процес реалізації механізмів політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО.

Предмет дослідження є теоретико-методологічні засади та практичні аспекти реалізації механізмів політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО.

Аналіз попередніх досліджень. Серед вітчизняних авторів, які приділяли у своїх роботах значну увагу аспектам інформаційної безпеки, можна виділити М.А. Бендікова, Я.Д. Вишнякова, Л.П. Гончаренко, В.П. Шеломенцева, Г.Б. Клейнера, Л.Г. Окорокова, Е.А. Олейникова, В.Л. Тамбовцева, О.О. Барабаш, В. Мунтіян, С.А. Харченко, В.П. Бочарникова й ряд інших. Водночас варто зазначити, що сьогодні в Україні проблематика реалізація механізму політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО практично не розглянуто в наукових працях, що зумовлює актуальність її дослідження.

Виклад основного матеріалу. Першочерговою та важливою складовою діяльності будь якого закладу вищої освіти є організація вступної кампанії. Відповідно до законодавчих та нормативних вимог вступна кампанія за умови рівності та прозорості повинна сприяти реалізації права на здобуття вищої освіти майбутніми студентам та водночас забезпечити заклад вищої освіти (ЗВО) набором здобувачів вищої освіти. Це складна система взаємозв'язаних та взаємозумовлених елементів, до яких можна віднести профорієнтаційну підготовку, нормативно-правовий супровід, організаційні дії, рекламно-інформаційне забезпечення, що формуються відповідно до цілей та стратегій ЗВО [3].

Питання інформаційної безпеки та її реалізації при створенні системи супроводу вступної кампанії ЗВО в умовах війни є актуальним питанням яке впливає на виживання людини, суспільства і держави. Адже забезпечення інформаційної безпеки обумовлено не тільки інтересами держави, але і інтересами людини в контексті забезпечення її прав та свобод. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність та достовірність.

Кризові явища, що характеризують розвиток національної економіки, зумовили визначення внутрішніх загроз для економічної безпеки держави як такі, що значно перевищують небезпеку зовнішніх та можуть призвести до соціального вибуху, загальнонаціональних техногенних та екологічних катастроф, істотного обмеження можливостей керівництва держави вирішувати внутрішні проблем та діяти на міжнародній арені [4, с. 47]

Сучасна система супроводу вступної кампанії повинна базуватися на повній інформаційній підтримці в прийняті рішень абітурієнтами. Відповідно до особливостей вступної кампанії як процесу, основні задачі, що потребують розв'язання, це вибір спеціальності та оцінка шансів вступу.

Особливості вступної кампанії свідчать про актуальність впровадження інформаційної системи безпеки, основною ціллю якої є підтримка прийняття рішень абітурієнтів.

Відповідно до механізму політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО, як процесу, основними задачами, що потребують розв'язання є:

1. Опрацювання даних повинно здійснюватися відповідно до актуальних нормативно-правових вимог щодо правил прийому поточного року, а також до правил, встановлених конкретним ЗВО та переліку його освітніх пропозицій.

2. Результатом роботи інформаційної системи повинно бути розв'язання таких задач: підвищення усвідомленості вибору спеціальності для вступу, підвищення точності оцінки абітурієнтом своїх шансів на вступ, вдосконалення існуючих інформаційно-пошукових системи освітніх пропозицій;

3. Гнучкість до змін у відповідності до змін умов вступу, орієнтація на взаємодію з потенційними абітурієнтами ЗВО;

4. Адаптивність до модернізації за умови незначних змін правил прийому.

5. Надійність, якість, контроль результатів, наявність каналів внесення та виведення інформації.

Саме тому запровадження механізму політики інформаційної безпеки та їх реалізації при створенні системи супроводу вступної кампанії ЗВО є важливим комплексом заходів або напрямків державної політики щодо попередження виникнення та ліквідації наслідків впливу загроз на економічну безпеку та потребує певних зусиль і відповідної нормативно-правової й наукової бази [5].

На наш погляд, що таких кроків можна віднести:

1. Вдосконалення існуючої нормативно-правової бази, зокрема в частині посилення захисту економічної та інформаційної безпеки. Проте в нових нормативно-правових актах необхідно звертати не тільки на актуальні загрози, а й на потенційні, спрогнозувати можливі ситуації при яких виникають загрози та методи їх попередження.
2. Радикальне переосмислення концепції реагування та управління загрозами.
3. Розбудова розвиненої інституціональної ринкової інфраструктури, в тому числі побудова ефективного господарського механізму з підготовкою відповідної нормативно-правової бази.
4. Ефективна реалізація регіональна соціально-економічних програм.
5. Пошук і активна розробка альтернативних джерел енергоресурсів.
6. Побудова ефективного воєнно-промислового комплексу.
7. Забезпечення умов для розвитку й збереження науково-технічного потенціалу країни.
8. Підвищення зайнятості населення та стимулювання офіційного працевлаштування громадянами.
9. Створення ефективної системи захисту інформаційної безпеки з метою попередження інформаційних атак з боку РФ.

Механізми політики інформаційної безпеки системи супроводу вступної кампанії ЗВО – це процес реалізації уповноваженими органами державної влади, ЗВО та іншими суб'єктами економічної безпеки держави системи заходів, спрямованої на протидію поширенню загроз з метою запобігання їхнього негативного впливу на права вступників, діяльність ЗВО та національну економіку вцілому. Відповідно до такого концептуального підходу забезпечення повинно відбуватися в рамках стратегії економічної безпеки держави й передбачає формування й впровадження комплексу заходів з упередження потенційних загроз, спрямованого на розв'язання суперечностей, які виникають в процесі реалізації національних економічних інтересів та вступної кампанії.

Механізм політики інформаційної безпеки системи супроводу вступної кампанії ЗВО повинен включати в себе мету, принципи, функції, аналітичне забезпечення, організаційну систему упередження загроз, формування пріоритетних напрямів забезпечення економічної

безпеки, методи, важелі, інструменти державного регулювання процесу упередження загроз інформаційній безпеці вступної кампанії.

Оперативне нівелювання загроз і принцип превентивності передбачають раннє виявлення загроз із використанням внутрішнього і зовнішнього інформаційного середовища системи супроводу вступної кампанії ЗВО, їх завчасне упередження за допомогою економічних, організаційних, нормативно-правових, адміністративних та інституційних важелів, з використанням декількох прогнозних сценаріїв забезпечення інформаційної безпеки.

До складу запропонованого механізму включається блок аналітичного забезпечення інформаційної безпеки системи супроводу вступної кампанії ЗВО, призначений для постійного збору інформації, розрахунку поточного рівня інформаційної безпеки вступної кампанії, оцінювання виявлених тенденцій, ідентифікації та моделювання загроз, оцінювання їх впливу на рівень інформаційної безпеки системи супроводу вступної кампанії ЗВО та прогнозування можливих наслідків для діяльності ЗВО та економічної системи держави.

Ключовими завданнями формування механізму політики інформаційної безпеки системи супроводу вступної кампанії ЗВО є наступні: формування комплексу оптимальних умов для забезпечення життєдіяльності й розвитку індивіда, фізичних і юридичних осіб; підтримка соціально-економічної й військово-політичної стабільності українського суспільства; збереження цілісності та державності України; протидія впливу загроз зовнішнього й внутрішнього походження.

Отже, пріоритетними напрямами формування механізму політики інформаційної безпеки системи супроводу вступної кампанії ЗВО в умовах воєнного стану є:

– розроблення та здійснення заходів у рамках забезпечення безперебійного функціонування інформаційно-аналітичної системи супроводу вступної кампанії;

– розроблення та здійснення заходів спрямованих на збереження системи освітньої статистики, адміністративної інформації, звітності з урахуванням викликів, спричинених війною;

– розроблення та здійснення заходів у рамках використання інформаційно-аналітичної системи, націлених на підтримку безперебійного функціонування ресурсних центрів, забезпечення безперервності та якості освіти для осіб з особливими потребами, підтримки інклюзивної освіти в період дії воєнного стану;

– створення, упровадження й технічна підтримка баз оперативних даних, забезпечення захисту та збереження інформації в умовах широкомасштабної військової агресії рф, зокрема постійних кібератак із боку ворога;

– розвиток системи електронного діловодство в закладах освіти, створення відповідної нормативно-правової бази;

– створення сучасних електронних опитувальників з автоматизованим збором інформації для оцінювання чисельності переміщених майбутнії учасників освітнього процесу.

Висновки. Таким чином, механізми політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО є важливим напрямом діяльності будь якого ЗВО. Результати вступної кампанії мають прямий вплив як на діяльність, існування та розвиток освітнього закладу, так і на життєву траєкторію студента, майбутнього фахівця держави. В умовах цифровізації послуг та стрімкого розвитку інформаційного середовища стає критично необхідним застосування механізму політики інформаційної безпеки системи супроводу вступної кампанії ЗВО, що вцілому є складовою захисту інформації та необхідною умовою ефективної вступної кампанії. Виклики системі освіти України в період дії воєнного стану сприяють та акцентують необхідність реалізації дієвого механізму політики інформаційної безпеки при створенні системи супроводу вступної кампанії ЗВО.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017 // Режим доступу: https://zakon.rada.gov.ua/go/47/2017 (останнє звернення 04.04.2023р.)
2. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022 // Режим доступу: https://zakon.rada.gov.ua/go/152/2022 (останнє звернення 04.04.2023р.)
3. Коломієць М.Б, Мирний Р.Ф. Вступна кампанія закладу вищої освіти як система / М.Б. Коломієць, Р.Ф. Мирний // Вісник Глухівського національного педагогічного університету імені Олександра Довженка, серія Педагогічні науки. – 2017. – № 3. – С. 105 – 111.
4. Економічна безпека держави: оцінювання та стратегічні орієнтири забезпечення : [монографія] / О. В. Комеліна, С. В. Онищенко, А. В. Матковський, О. А. Пугач. // Полтава : ПолтНТУ. – 2013. – С. 202.
5. Цвігун Т. В. Економічна безпека в системі національної безпеки України / Т.В, Цвігун // Економіка та суспільство. Вип. 11. К. – 2017. – С. 150–156.
6. Рейтинг закладів вищої освіти у сфері управління МОН, які фінансуються за формулою, за оцінкою зайнятості та показником працевлаштування їх випускників. // Режим доступу: https://mon.gov.ua/storage/app/media/news/2022/02/03/01/Zvit.z.monitorynhu.pratsevlashtuvannya-2022-02-03.pdf (останнє звернення 04.04.2023р.)
7. Про затвердження Методичних рекомендації з проведення моніторингу працевлаштування випускників закладів вищої та фахової передвищої освіти і визначення показника працевлаштування для Формули розподілу видатків державного бюджету на вищу освіту між закладами вищої освіти : наказ Міністерства освіти і науки України від 02.02.2022 № 101. // Режим доступу: https://mon.gov.ua/ua/npa/pro-zatverdzhennya-metodichnih-rekomendacij-zprovedennya-monitoringu-zajnyatosti-vipusknikiv-zakladiv-vishoyi-ta-fahovoyi-peredvishoyi-osviti-i-viznachennyapokaznika-pracevlashtuvannya-dlya-formuli-rozpodilu-vidatkiv-derzhavnogo-byudzhetu. (останнє звернення 04.04.2023р.)
8. Звіт з моніторингу працевлаштування випускників закладів вищої та фахової передвищої освіти / М-во освіти і науки України. С. 3. // Режим доступу: https://mon.gov.ua/storage/app/media/news/2022/02/03/01/Zvit.z.monitorynhu.pratsevlashtuvannya-2022-02-03.pdf. (останнє звернення 04.04.2023р.)
9. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII (зі змінами та доповненнями). // Режим доступу: https://zakon.rada.gov.ua/laws/show/389-19#Text. (останнє звернення 04.04.2023р.)
10. Про введення воєнного стану в Україні : указ Президента України від 24.02.2022 № 64/2022. // Режим доступу: https://www.president.gov.ua/documents/642022-41397. (останнє звернення 04.04.2023р.)
11. Порядок прийому на навчання для здобуття вищої освіти в 2022 році : затв. наказом Міністерства освіти і науки України від 27.04.2022 № 392. // Режим доступу: https://mon.gov.ua/storage/app/media/vishcha-osvita/vstup-2022/05.05.2022/Poryadok.pryyomu.VO.392-400.05.05.2022.pdf. (останнє звернення 04.04.2023р.)

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

ТЕХНОЛОГІЇ ДЛЯ НАЛАГОДЖЕННЯ КОМУНІАЦІЇ ТА СПІВПРАЦІ В КОМАНДІ СТАРТАПУ

ГУРСЬКИЙ Б. 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто використання сучасних технологій для покращення комунікації та співпраці в команді стартапу. Детально розглядаються такі інструменти, як онлайн-конференції, чат-боти, системи управління проектами та інші. Стаття описує, як ці технології можуть сприяти підвищенню продуктивності та ефективності роботи команди стартапу. Зокрема, вона надає поради щодо вибору правильних інструментів для конкретних завдань, а також щодо того, як правильно використовувати ці інструменти для досягнення максимального результату.

The article discusses the use of modern technologies to improve communication and collaboration in a startup team. The article discusses in detail such tools as online conferences, chatbots, project management systems, and others. The article describes how these technologies can contribute to the productivity and efficiency of a startup team. In particular, it provides tips on choosing the right tools for specific tasks, as well as how to use these tools correctly to achieve maximum results.

Актуальність. Розвиток та глобалізація технологій призвели до появи багатьох нових можливостей для комунікації та співпраці між людьми з різних куточків світу. Зокрема, стартап-команди, що складаються з розробників, маркетологів, дизайнерів та інших спеціалістів, нерідко працюють з використанням віддалених комунікаційних технологій. Завдяки цьому, збільшується швидкість та ефективність вирішення завдань, зменшується час на узгодження проектів, забезпечується постійний зв'язок між командою.

У сучасному динамічному світі стартапів, де співпраця, ефективна комунікація та швидке реагування на зміни є ключовими складовими успіху, використання технологій для налагодження комунікації та співпраці в команді стає невід'ємною частиною стратегічного планування. Колективність, обмін ідеями та координація – ці аспекти визначають можливість стартапу досягти поставлених цілей та перетворити інноваційні концепції на реальні продукти чи послуги.

Стартап-команди зазвичай працюють в умовах швидких змін та нестабільності. Ключовим фактором успіху для таких них є ефективна комунікація та співпраця. З цією метою, створення та використання відповідних технологій є надзвичайно важливим для досягнення успіху в діяльності стартапу.

Мета. Метою статті є розгляд технологій, які можуть допомогти налагодити комунікацію та співпрацю в стартап-команді. Вона присвячена вивченню інструментів, які дозволяють забезпечити ефективну взаємодію між учасниками, зручний доступ до спільних документів, моніторинг прогресу проекту та інше.

Об'єктом статті є стартап-команда та її потреби в ефективній комунікації та співпраці

Предметом статті є технології, які можуть бути використані для налагодження комунікації та співпраці в стартап-команді. Серед них можуть бути засоби відеозв'язку, спільні робочі простори в Інтернеті, системи для обміну повідомленнями.

Виклад основного матеріалу. В сучасному світі, де бізнес-процеси постійно змінюються і ефективна комунікація є ключовим фактором успіху, технології стають все більш важливими для налагодження комунікації та співпраці в команді. Застосування

відповідних технологій та підходів може значно полегшити роботу, сприяти більш ефективній комунікації та зменшенню витрат на час та кошти.

Технології також допомагають забезпечити ефективну комунікацію між членами команди. Один з важливих елементів комунікації - це спільний доступ до проектів та завдань, що відповідають конкретним цілям бізнесу. Для цього використовуються спеціальні інструменти, такі як проектні менеджери та системи управління завданнями, які дозволяють команді легко відстежувати процес виконання завдань та бачити, хто відповідає за яку частину проекту.

Наприклад дослідження Edmondson (2012)[1] було зосереджене на впливі новітніх технологій на командну роботу та співпрацю. Автор дослідження провів аналіз декількох компаній, які успішно використовують нові технології для покращення командної роботи. Дослідження показало, що використання спільних платформ, засобів електронного зв'язку та інтерактивних додатків може допомогти зменшити ризики, пов'язані з комунікацією в команді, та забезпечити ефективну співпрацю між різними співробітниками.

Дослідження також підкреслює, що використання новітніх технологій може допомогти підвищити рівень задоволеності членів команди, забезпечивши їм більш гнучкі умови для роботи та спілкування. Зокрема, використання технологій може сприяти зменшенню кількості зустрічей та робочих нарад, що дозволить членам команди більш ефективно розподіляти свій час та зосередитися на важливих завданнях.

Щоб забезпечити ефективну комунікацію та співпрацю в команді, необхідно враховувати специфіку проекту та потреби учасників. Кожен стартап може використовувати різні технології. Наприклад, для команд, які працюють дистанційно, може бути корисним використовувати відеоконференції та спільні онлайн-документи, щоб забезпечити зручний доступ до інформації та підтримати колективну роботу над проектом. Для команд, які працюють в офісі, можуть бути корисні інтерактивні дошки та програмні засоби для ведення проектів.

Цифрові інструменти можуть допомогти зменшити час, який потрібно на збір інформації та розподіл завдань, тим самим забезпечивши більш ефективну роботу команди та швидше досягнення мети проекту.

Приклади інструментів та технологій які допоможуть налагодити взаємодію членів команди:

1. Комунікаційні платформи: для зручного та ефективного спілкування учасників команди можна використовувати спеціальні платформи, такі як Slack, Microsoft Teams, Trello тощо. Вони дозволяють створювати чати, обмінюватися документами та інформацією, планувати зустрічі та завдання.
2. Проєктувальні інструменти: для спільної роботи над проектом та вирішення задач команда може використовувати проектувальні інструменти, такі як Figma, Sketch, InVision тощо. Вони дозволяють створювати та редагувати дизайн, робити анімацію, проводити тестування.
3. Відеоконференції: для зборів та зустрічей команда може використовувати відеоконференції, такі як Zoom, GoogleMeet, Skype тощо. Вони дозволяють зустрічатися з колегами з будь-якої точки світу, проводити онлайн-презентації та демонстрації.
4. Календарі: для планування зустрічей та завдань можна використовувати спільні календарі, такі як Google Calendar, Apple Calendar тощо. Вони дозволяють створювати спільні події та ділитися ними з іншими учасниками команди.
5. Інструменти для спільної роботи над документами: для редагування та спільної роботи над документами команда може використовувати Google Docs, Microsoft Office 365, DropboxPaper тощо. Вони дозволяють працювати над документами в режимі реального часу та забезпечують зручний доступ до даних з будь-якого пристрою.
6. Системи контролю версій: для спільної роботи над кодом програмного забезпечення команда може використовувати системи контролю версій, такі як Git, GitHub, Bitbucket

тощо. Вони дозволяють зберігати копії коду та його зміни, контролювати версії та спільно працювати над проектом.

7. Соціальні мережі та форуми: для спілкування з потенційними клієнтами та партнерами стартап може використовувати соціальні мережі та форуми. Наприклад, Twitter, LinkedIn, Reddit тощо. Ці інструменти дозволяють ширити інформацію про проект, спілкуватися з зацікавленими особами та знаходити нові можливості для розвитку стартапу.

Одним з основних завдань таких технологій є забезпечення доступу до необхідної інформації, яка є ключовою для розвитку бізнесу. На сьогоднішній день, висока швидкість інтернету та зростаюча кількість хмарних сервісів, дозволяють команді забезпечити швидкий та безперебійний доступ до всієї необхідної інформації, що становить велику перевагу в порівнянні з традиційними методами комунікації.

Розглянемо деякі технології які використовуються для налагодження комунікації в сучасних організаціях.

Slack - це платформа, яка дозволяє створювати та управляти комунікацією в команді чи в організації. Основна ідея Slack полягає в тому, щоб замінити електронну пошту та інші різні засоби комунікації, зосередивши всі зв'язки в одному місці.

Основні можливості Slack включають:

- організацію чатів та каналів для комунікації між колегами;
- відправку повідомлень в режимі реального часу;
- організацію відеозв'язку та аудіодзвінків між користувачами;
- інтеграцію з різними сервісами, такими як Google Drive, Trello, GitHub та інші.

Переваги використання Slack включають:

- зменшення кількості електронних листів, що приходять на пошту;
- збільшення ефективності комунікації та співпраці між колегами;
- організація робочих процесів, що вимагають співпраці між різними відділами;
- зручність доступу до інформації та історії комунікації в майбутньому;

ClickUp - це онлайн-інструмент управління проектами та задачами, який дозволяє користувачам організовувати свої завдання, проекти та команди. ClickUp заснований на принципі "все в одному місці", що дозволяє об'єднати усі необхідні інструменти в одному місці, такі як список завдань, календар, трекер часу, дошка Kanban та інше.

Основні можливості ClickUp включають:

- список завдань зі статусами, пріоритетами та дедлайнами;
- дошка Kanban для візуалізації процесу роботи над проектом;
- календар для планування завдань та проектів;
- трекер часу для відстеження часу, витраченого на роботу над завданням;
- функції спільної роботи, такі як коментарі, згадки та обговорення завдань;
- вбудовані інтеграції з іншими популярними інструментами, такими як Google Drive, Dropbox, Trello, Slack та інші.

Переваги ClickUp перед іншими подібними програмами включають:

- все в одному місці: ClickUp дозволяє об'єднати усі інструменти управління проектами в одному місці, що зменшує необхідність використовувати декілька різних програм для управління проектами;
- гнучкість: ClickUp дозволяє настроювати різні вигляди для завдань, такі як списки, дошки та календарі, що дозволяє користувачам працювати з інтерфейсом, який найбільше підходить для їх потреб;
- інтеграції: ClickUp має вбудовані інтеграції з популярними інструментами, такими як Google Drive, Dropbox, Trello, Slack та інші, що зменшує необхідність переходити між різними програмами для виконання різних завдань і підвищує ефективність роботи;

- підтримка різних методів управління проектами: ClickUp підтримує різні методи управління проектами, такі як Scrum, Kanban та інші, що дозволяє користувачам працювати з тим методом, який найбільше підходить для їх проекту.

Загалом, ClickUp - це потужний інструмент управління проектами та задачами, який дозволяє користувачам працювати зі своїми проектами та командами більш ефективно та продуктивно. Завдяки своїм унікальним можливостям та перевагам, ClickUp може стати ідеальним вибором для бізнесу будь-якого розміру, команди розробників та інших користувачів, які шукають потужний та зручний інструмент для управління своїми проектами та завданнями.

Google Meet є однією з популярних програм для відеоконференцій, розроблених компанією Google. Він дозволяє користувачам взаємодіяти один з одним в режимі реального часу, використовуючи аудіо та відео, відправляти повідомлення в чаті, робити екранні демонстрації та спільно працювати над документами.

Основні можливості Google Meet включають:

- відеоконференції з можливістю додавати до 250 учасників;
- відеострім на YouTube, що дозволяє передавати відео на живому екрані;
- відправка повідомлень у приватний чат або в загальний чат;
- створення віртуальних кімнат для дискусій;
- спільна робота над документами та редактори Google Docs, Sheets і Slides;
- запис відеоконференцій та збереження їх на Google Drive.

Перевагами Google Meet є:

- легкий доступ: Google Meet працює на будь-якому комп'ютері або мобільному пристрої з веб-браузером і доступом до Інтернету;
- висока якість звуку та відео: програма забезпечує якість звуку та відео, що робить відеоконференції більш реалістичними;
- легка інтеграція: Google Meet інтегрується з іншими програмами Google, такими як Google Calendar, Gmail, Google Drive і Google Classroom.

Загалом, GoogleMeet є потужним інструментом для відеоконференцій та спільної роботи над документами. Він має багато функцій, що роблять його відмінним від інших програм для відеоконференцій, і дозволяє користувачам ефективно спілкуватися та працювати з командою незалежно від географічного розташування. Більшість функцій є безкоштовними, що робить його доступним для користувачів з усього світу. Крім того, GoogleMeet може бути використаний для різноманітних цілей, таких як вебінари, онлайн-курси, віддалені зустрічі з клієнтами та співробітниками.

Одним з досліджень, що підтверджує ефективність використання технологій у команді, є дослідження, проведене компанією Slack, яка є провідним постачальником комунікаційних платформ для бізнесу. У цьому дослідженні було виявлено, що використання комунікаційних інструментів, таких як Slack, дозволяє зменшити час, витрачений на комунікацію між співробітниками, на 32%, а кількість електронних листів на 48%. Крім того, співробітники, які використовують Slack, мають більш позитивну думку про робоче оточення та відчувають більшу налагодженість у співпраці зі своїми колегами[2].

З іншого боку, необхідно пам'ятати, що технології не замінять необхідності взаємодії та спілкування, тому важливо забезпечити баланс між використанням технологій та міжособистісної взаємодії в команді

Ще одним важливим аспектом для ефективної комунікації та співпраці в команді є використання процесів та методологій, таких як Agile та Scrum. Ці методики орієнтовані на роботу в команді та взаємодію між її учасниками, забезпечуючи швидку та ефективну розробку продукту.

Agile та Scrum - це методології управління проектами, які дозволяють ефективно виконувати проекти в умовах невизначеності та швидких змін. Основні принципи Agile та Scrum включають наступне:

Принципи Agile:

1. Люди та співпраця важливіші за процеси та інструменти: важливо створювати ефективні команди, де кожен учасник знаходиться у комфортному для себе середовищі та взаємодіє з іншими учасниками.
2. Робота програмного забезпечення важливіша за вичерпну документацію: важливо зосередитися на розробці програмного забезпечення та створенні функціональності для користувачів, а не на вичерпній документації.
3. Співпраця з клієнтом важливіша за умови договору: важливо взаємодіяти з клієнтом та долучати його до процесу розробки для забезпечення максимальної задоволеності від результатів роботи.
4. Реагування на зміни важливіше за виконання плану: важливо бути готовим до швидких змін та реагувати на них у найбільш ефективний спосіб.

Принципи Scrum:

1. Команди повинні бути самоорганізованими та мультидисциплінарними: важливо, щоб кожен учасник команди був готовий виконувати різноманітні завдання та самостійно приймати рішення.
2. Робота повинна відбуватися у складі ітерацій: проект повинен бути розбитий на короткі ітерації (спринти), кожна з яких має чітко визначені цілі та завдання.
3. Кожен спринт повинен мати відповідність результатам: під час кожного спринту має бути створена певна кількість робочого продукту (шаблонів, коду, тестів тощо), який можна демонструвати клієнту та отримувати його зворотний зв'язок. 4. Щоденні зустрічі (daily scrum): кожен учасник команди повинен зустрічатися з іншими щодня, обговорювати свої завдання та проблеми, щоб забезпечити максимальну ефективність команди.
4. Регулярні огляди та ретроспективи: після кожного спринту команда повинна проводити огляд результатів та ретроспективу, щоб оцінити свою роботу та знайти способи для її поліпшення.

Основними ролями в методології Scrum є:

- ScrumMaster: відповідає за виконання методології Scrum та забезпечення її ефективного впровадження в проекті;
- ProductOwner: відповідає за формулювання вимог до продукту та визначення пріоритетів;
- Розробник (Developer): відповідає за розробку програмного продукту та його тестування.

Узагальнюючи, Agile та Scrum - це гнучкі методології управління проектами, які дозволяють ефективно виконувати проекти у швидкозмінних умовах та забезпечувати високу якість продукту за допомогою самоорганізованих та мультидисциплінарних команд.

Таким чином, використання сучасних технологій та методологій є важливим елементом успішної роботи команди. Відкрита та ефективна комунікація, використання Agile та Scrum, а також використання онлайн-інструментів для спільної роботи дозволяють збільшити ефективність роботи та покращити якість розробки продукту.

Список використаних джерел

1. Edmondson,A.(2012).Teaming, creativity, and collaboration: How new technologies can help organizations improve teaming. Journal of Leadership & Organizational Studies, 19(2), 137-151.

2. Slack.(2018). Trust, tools and teamwork: what workers want. https://slack.com/intl/en-gb/blog/transformation/trust-tools-and-teamwork-what-workers-want

Робота виконана під науковим керівництвом к.т.н., доцента
КОТЕНКО Н.О.

СИСТЕМА ОЦІНКИ РИЗИКІВ ТА ЇЇ ВПЛИВ НА ЗБІЛЬШЕННЯ ПРИБУТКОВОСТІ ПІДПРИЄМСТВА

ДАВИДОВА Т., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто вплив процесу впровадження системи оцінки ризиків по відношенню до загроз активам підприємства. Описано, як система оцінки ризиків може допомогти підприємствам ідентифікувати потенційні загрози та визначати шляхи їх управління. Визначена методика та основні принципи реалізації зазначеної системи. Розглянуто зразок оцінки ризиків та процес управління ними.

The article examines the impact of implementing a risk assessment system on threats to a company's assets. It describes how a risk assessment system can help companies identify potential threats and determine ways to manage them. The methodology and key principles of implementing such a system are defined. An example of risk assessment and its management process is also discussed.

Актуальність. В сучасних умовах бізнес-середовище постійно змінюється, що призводить до зростання ризиків для підприємств. Відсутність ефективного управління ризиками може призвести до фінансових втрат та негативного впливу на репутацію компанії. В таких умовах важливо мати систему оцінки ризиків, яка допоможе ідентифікувати потенційні загрози та визначати шляхи їх управління. Впровадження ефективної системи оцінки ризиків може значно зменшити витрати та збільшити прибутковість підприємства.

В ході своєї діяльності будь-яке підприємство має на меті генерування доходів. Відповідно до чого будь-які втрати як то фінансові так і репутаційні невідворотно несуть за собою зниження дохідності, і як факт – рентабельності і можливості конкурувати на ринку.

Враховуючи це, невід'ємною частиною операційної діяльності підприємства є коректне управління активами, а саме: виявлення джерел загроз, класифікація загроз, оцінка та управління ризиками. Впровадження системи оцінки ризиків надасть можливість менеджменту підприємства вчасно реагувати на загрози активам і нівелювати їх вплив, а також сформує методику та основні принципи впровадження системи оцінки ризиків, а також пропонує приклади успішної реалізації на різних підприємствах. Ця інформація може бути корисною для менеджерів та власників підприємств, які бажають зменшити ризики та підвищити ефективність своєї діяльності.

Метою статті є дослідження впливу від впровадження системи оцінки ризиків на підприємстві.

Об'єктом дослідження є розробка і впровадження системи оцінки ризиків на підприємстві.

Предмет дослідження – система оцінки ризиків.

Аналіз попередніх досліджень. Аналіз попередніх досліджень в області систем оцінки ризиків та їх впливу на прибутковість підприємств показує, що такі системи є необхідним елементом ефективного управління ризиками. Дослідження з питань систем оцінки ризиків та їх впливу на збільшення прибутковості підприємств проводили вчені з різних галузей і країн: Маріо Салерно, Джон Сандерленд, Елізабет Фултон, Реймонд Зімбарді, Майкл Плас.

Дослідження, проведені в галузі фінансів та управління ризиками, доводять, що ефективна система оцінки ризиків допомагає зменшити витрати та підвищити прибутковість підприємства. Одним з ключових факторів успіху в цій області є правильне визначення потенційних ризиків та вчасне прийняття заходів щодо їх управління.

Крім того, дослідження показують, що реалізація системи оцінки ризиків на підприємстві може позитивно впливати на репутацію компанії та забезпечити відповідність законодавчим та регуляторним вимогам. Також було встановлено, що ефективність системи оцінки ризиків залежить від якості використовуваних методів та засобів оцінки ризиків, а також від професійної кваліфікації менеджменту та ступеню взаємодії між різними підрозділами компанії.

Таким чином, аналіз попередніх досліджень підтверджує значення впровадження системи оцінки ризиків для забезпечення успішної та стійкої діяльності підприємств в сучасних умовах.

Виклад основного матеріалу. У сучасних умовах бізнесу питання управління ризиками є надзвичайно важливим для забезпечення успішності діяльності підприємства. Система оцінки ризиків (СОР) є ефективним інструментом для ідентифікації, аналізу та управління ризиками, що можуть впливати на фінансові результати та прибутковість підприємства. Дослідження показують, що впровадження системи оцінки ризиків може допомогти підприємствам зменшити кількість випадків негативних наслідків від ризиків, що можуть призвести до збитків. Крім того, СОР може допомогти підприємствам зменшити витрати на страхування, а також забезпечити більш точне планування бюджету та фінансових ресурсів.

Система оцінки ризиків є важливим інструментом для забезпечення успішної діяльності підприємства. Вона дозволяє ідентифікувати потенційні загрози та визначати шляхи їх управління, що сприяє збільшенню прибутковості підприємства. Одним з найважливіших етапів впровадження СОР є ідентифікація загроз, які можуть вплинути на активи підприємства [1, 2]. Для цього використовуються різні методики, які забезпечують якісну та кількісну оцінку ризиків. Окрім ідентифікації ризиків, СОР дозволяє розробити та впровадити плани управління ризиками. Це допомагає підприємству ефективно управляти потенційними ризиками та забезпечувати безпеку своїх активів. Отже, СОР є необхідним інструментом для успішної діяльності підприємства, який дозволяє ідентифікувати та управляти ризиками, що сприяє збільшенню прибутковості та зменшенню можливих збитків.

Застосування СОР на підприємстві може забезпечити наступні переваги [2, 3]:

- Мінімізація можливих втрат та шкідливих наслідків в результаті ризиків, що впливають на підприємство.
- Збільшення ефективності прийнятих рішень та виконання стратегії розвитку, зокрема зменшення витрат та підвищення якості продукції.
- Підвищення рівня довіри соціального середовища до підприємства та його іміджу, який є ключовим для успішного розвитку.
- Забезпечення відповідності законодавству та регулюванням у сфері бізнесу, що сприяє запобіганню фінансових санкцій та покращенню взаємодії з органами державної влади.

Таким чином, СОР допомагає підприємствам досягати стійкості та стабільності, зменшує можливі втрати та ризики, а також забезпечує підвищення ефективності роботи та збільшення прибутковості бізнесу. Отже, СОР є важливим інструментом управління ризиками, що можуть впливати на прибутковість підприємства. Впровадження такої системи може позитивно позначитись на фінансових результатів підприємства, зменшити кількість негативних наслідків від ризиків та забезпечити більш точне планування бюджету [1, 3].

Реалізація системи оцінки ризиків передбачає виконання декількох етапів, включаючи:

1. Ідентифікацію ризиків: перелік потенційних ризиків, які можуть впливати на діяльність підприємства, та їх кваліфіковану оцінку.

2. Оцінку ризиків: визначення імовірності виникнення ризиків та їх впливу на підприємство.

3. Розробку стратегії управління ризиками: визначення оптимального способу управління кожним з ризиків (уникнення, зменшення, передача, прийняття ризику).

4. Реалізацію стратегії: введення запланованих заходів з управління ризиками в дію.

5. Моніторинг та оновлення: постійний контроль за ризиками та оновлення стратегій управління ними відповідно до змін у діловому середовищі.

Основними принципами реалізації СОР є [2, 3]:

- Систематичний підхід − оцінка ризиків повинна бути проведена систематично, охоплюючи всі аспекти діяльності підприємства.
- Інтеграція − СОР повинна бути інтегрована в управлінський процес підприємства, щоб забезпечити найбільш ефективне управління ризиками.
- Співпраця − робота з СОР повинна здійснюватися в тісній співпраці з різними підрозділами підприємства, щоб забезпечити повну інформацію про ризики та ефективність заходів по їх управлінню.
- Об'єктивність − оцінка ризиків повинна бути об'єктивною та неупередженою, ґрунтуватися на достовірних даних та аналізі.
- Пріоритетність − ризики повинні оцінюватися за їх важливістю та пріоритетністю для підприємства, щоб забезпечити оптимальне використання ресурсів при їх управлінні.
- Неперервність − СОР повинна бути неперервною та регулярно оновлюватися з метою виявлення нових ризиків та змін у вже ідентифікованих.
- Керованість − ризики повинні бути керовані та управлятися за допомогою ефективних заходів з мінімізації наслідків їх реалізації.

Зразок оцінки ризиків та процес управління ними можуть включати наступні етапи [3]:

1. Ідентифікація ризиків − визначаються потенційні загрози, які можуть вплинути на діяльність підприємства. Для цього можуть використовуватися різні методи, такі як SWOT-аналіз, аналіз ризиків згідно з індустрійними стандартами тощо. Ідентифікація ризиків допомагає підприємству передбачити можливі негативні наслідки своєї діяльності та прийняти заходи для зменшення ризиків. Для проведення ідентифікації ризиків необхідно: визначити область діяльності, яку необхідно проаналізувати на наявність ризиків; описати процес діяльності та визначити основні етапи; визначити потенційні загрози або небезпеки, які можуть виникнути на кожному етапі діяльності; оцінити ймовірність виникнення небезпеки та її вплив; визначити заходи для зменшення ризиків та підвищення безпеки діяльності підприємства. Ідентифікація ризиків дозволяє виявити потенційні небезпеки та прийняти заходи для їх зменшення, що допомагає зберегти ресурси та забезпечити безпеку діяльності [2].
2. Оцінка ризиків − проводиться оцінка ймовірності та наслідків потенційної загрози. Це може включати визначення ймовірності настання ризику, ступеня впливу на діяльність підприємства та можливих наслідків.
3. Розробка плану управління ризиками − визначаються заходи, які допоможуть зменшити вплив ризиків на діяльність підприємства. Це може включати розробку планів невідкладних заходів у разі виникнення ризику, розробку процедур управління ризиками та визначення відповідальних осіб за їх виконання.
4. Реалізація плану управління ризиками − виконуються заходи, які були визначені на попередньому етапі. Це може включати здійснення профілактичних заходів, проведення навчань та тренувань з управління ризиками тощо.
5. Моніторинг та оновлення СОР. Система оцінки ризиків повинна постійно оновлюватися та вдосконалюватися на основі нових даних про ризики та їх вплив на діяльність підприємства. Також важливо проводити періодичний моніторинг стану системи.

Опираючись на кращі практики в сфері та регламентуючі стандарти, такі як сімейство міжнародних стандартів ISO 27001-27002, першим етапом впровадження системи оцінки ризиків (далі – СОР) є визначення менеджментом підприємства поняття активів та їх цінності, тобто їх описом.

Під поняттям «актив» в даному випадку варто розуміти все, що має цінність для підприємства. Залежно від сфери застосування ризик-менеджменту необхідно вибрати певну категорію активів. Якщо розглядати категорію інформаційних активів, достатньо обмежитися тільки інформаційними системи та персоналом, які зберігають, отримують чи передають та обробляють інформацію. Зазначені системи та персонал і будуть визначені як інформаційні активи. Окрім того, слід зазначити, що активами являються не тільки матеріальні об'єкти, які дотичні до процесів роботи з інформацією, а й сама інформація, що міститься у вище описаних системах та доступна персоналу.

Визначившись з поняттям «активу» та описавши їх, наступним кроком є створення реєстру активів. Даний реєстр систематизує та визначить пріоритизацію роботи з активами та їх власників, тобто осіб (підрозділів) відповідальних за їх безпеку [1].

З метою більш наочної демонстрації впливу СОР на бізнес-процеси, розглянемо умовне підприємство «Україна» та створимо реєстр активів даного підприємства різноманітних категорій, використовуючи такі атрибути: найменування активу, власник активу та категорія активу (Таблиця 1).

Таблиця 1.

Реєстр активів підприємства «Україна»

№	Актив	Власник активу	Категорія активу
1	План розвитку підприємства	Керівник підприємства	Конфіденційна інформація
2	База даних клієнтів	Відділ продажів	Електронний документ
3	Податкова звітність	Відділ бухгалтерії	Паперовий документ
4	Система відеоспостереження	Відділ безпеки	Допоміжне обладнання
5	Сервер обміну інформацією	Відділ інформаційних технологій	Комп'ютерна техніка
6	Керівник відділу постачання	Відділ постачання	Персонал

Визначені активи приймемо як такі, що критично впливають на бізнес-процеси підприємства і порушення основних властивостей інформації щодо них (цілісності, конфіденційності та доступності) нестиме невідворотні збитки для підприємства «Україна».

Визначивши активи підприємства, необхідно описати ймовірні ризики по відношенню до них, реалізація яких знизить прибутковість підприємства. Для цього створимо так званий профіль ризику (Таблиця 2).

Використовуючи метод статистичних досліджень та метод експертних оцінок проведемо оцінку ризиків по відношенню до активів наведених у Таблиці 1. Для цього використаємо систему СОР по відношенню до довільних активів з реєстру – «База даних клієнтів» . та «Керівник відділу постачання».

Приймемо наступну методику оцінки ризиків (далі – ОР): рівень ризику визначається перемноженням вірогідності реалізації загрози на максимальне значення реалізації загрози з результатів оцінки властивостей інформації (цілісності, конфіденційності, доступності). Дані оцінки базуються на основі рівня наслідків реалізації вразливостей з градацією 1 – 5 балів залежно від степені збитків (приймемо як такі, що 1 – прийнятні, 5 – критичні).

Таблиця 2.

Профіль ризику

№	Категорія	Характеристики
1	Актив	Тип активу (основний або допоміжний, інформація або бізнес-процес, ПО або апаратний засіб тощо). Цінність активу.
2	Загроза	Властивості загрози (внутрішня або зовнішня, випадкова або навмисна, минулі інциденти, нові розробки і тенденції). Вірогідність реалізації загрози (низька, середня, висока).
3	Вразливість	Опис вразливості. Критичність вразливості.
4	Ризик	Значення ризику обчислюється виходячи з таких даних: • Цінність активу • Вірогідність реалізації загрози • Критичність вразливості

В свою чергу загальний рівень ризику для бізнес-процесу, персоналу, фізичного середовища тощо дорівнює максимальній величині з усіх ризиків за кожною вразливістю.

Кожен ризик визначається на підставі кількості балів загального рівня ризику:

- низький ризик - 1 – 6;
- середній ризик - 7 – 14;
- високий ризик - 15 – 25.

Проведемо ОР для активу «База даних клієнтів».

Таблиця 3.

Визначення загального рівня ризику активу «База даних клієнтів»

Загроза	Вразливість	Вірогідність загрози	Оцінка цілісності	Оцінка конфіденційності	Оцінка доступності	Рівень ризику
1	2	3	4	5	6	7
Викрадення	Підкуп персоналу	3	2	5	1	15
Некоректне використання	Помилка програмного забезпечення	2	3	1	3	6
Недоступність	Відсутність живлення серверу БД	4	1	1	5	20
Внесення недостовірних даних	Помилка персоналу	2	5	1	1	10
Загальний ризик бізнес-процесу:						20

Проведемо ОР для активу «Керівник відділу постачання».

Як видно з Таблиць 3 та 4 ОР, загальний рівень ризиків для активу «База даних клієнтів» має 20 балів та відноситься до високого рівня ризику та потребує його обробки, в свою чергу ОР активу «Керівник відділу постачання» має 6 балів та відноситься до низького степеню ризиків, які можуть бути прийняті.

Таблиця 4.

Визначення загального рівня ризику активу «Керівник відділу постачання»

Загроза	Вразливість	Вірогідність загрози	Оцінка цілісності	Оцінка конфіденційності	Оцінка доступності	Рівень ризику
1	2	3	4	5	6	7
Несвоєчасне внесення інформації щодо постачання комплектуючих до інформаційної системи	Хвороба	2	1	1	1	2
Викрадення конфіденційної інформації	Підкуп персоналу	1	3	5	1	5
Саботаж	Підкуп персоналу	2	3	2	3	6
Внесення недостовірних даних	Помилка персоналу	1	5	1	1	5
Загальний ризик бізнес-процесу:						6

Приймемо, що актив має матеріальну цінність в розмірі 1 000 000 грн та репутаційну цінність, як таку, втрата якого приведе до повної зупинки роботи підприємства «Україна» і відповідно генерацію доходів в розмірі 10 000 000 грн. Виходячи з цього, менеджментом підприємства проведені наступні заходи щодо зниження ризику, а саме:

Таблиця 5.

Визначення рівня затрат щодо обробки загальних ризиків

№	Вразливість	Захід протидії	Розмір витрат, грн
1	Викрадення	Підвищення заробітної плати персоналу на 5 000 грн	120 000, 00
2	Некоректне використання	Доопрацювання програмного забезпечення розробником	100 000, 00
3	Недоступність	Встановлення альтернативного джерела живлення	150 000, 00
4	Внесення недостовірних даних	Курси підвищення кваліфікації для персоналу.	20 000, 00
		ВСЬОГО:	390 000, 00

Після чого було проведено повторну ОР

Таблиця 6.

Оцінка загального рівня ризику після процесу обробки ризиків

Загроза	Вразливість	Вірогідність загрози	Оцінка цілісності	Оцінка конфіденційності	Оцінка доступності	Рівень ризику
1	2	3	4	5	6	7
Викрадення	Підкуп персоналу	1	2	5	1	5
Некоректне використання	Помилка програмного забезпечення	1	3	1	3	3
Недоступність	Відсутність живлення серверу БД	1	1	1	5	5
Внесення недостовірних даних	Помилка персоналу	1	5	1	1	5
Загальний ризик бізнес-процесу:						5

Як результат наявне зниження рівня загального ризику до прийнятного. Окрім того, витрати на обробку рівня ризику більш ніж у 2,5 рази нижчі ніж ймовірні збитки від реалізації виявлених загроз. Більш того, вчасно виявлені вразливості значно знизили ймовірність зупинки підприємства, та в свою чергу надали можливість і надалі конкурувати на ринку. Впровадження СОР на підприємстві може бути досить складним процесом. Впровадження системи оцінки ризиків на підприємстві може бути складним процесом, але він має велику кількість переваг, які допоможуть підприємству зменшити ризики і покращити ефективність діяльності.

Одним з можливих викликів під час впровадження СОР може бути затримка у роботі, пов'язана з необхідністю проведення аналізу ризиків. Однак, ця затримка може бути компенсована підвищенням ефективності прийняття рішень та зменшенням загальних витрат на управління ризиками. Окрім того, для успішного впровадження СОР необхідно, щоб на керівному рівні підприємства була належна підтримка та зобов'язання щодо реалізації системи [4]. Відповідно, маючи впроваджену систему ризиків, керівництво підприємства здатне своєчасно виявляти та реагувати на загрози бізнес-процесам, матиме достатньо ресурсів для їх оптимізації та в свою чергу підвищення рентабельності підприємства.

Висновки. Результати даного дослідження надають глибоке розуміння важливості системи оцінки ризиків для підприємств і її впливу на збільшення прибутковості. Вивчення різноманітних аспектів цієї теми вказує на те, що в сучасному бізнес-середовищі врахування можливих ризиків є необхідним елементом ефективного управління та стратегічного планування.

Висновок, що можна зробити, полягає в тому, що система оцінки ризиків впливає на прибутковість підприємства через низку механізмів. Вчасне виявлення та аналіз можливих негативних впливів дозволяє підприємствам приймати обґрунтовані рішення для зменшення можливих втрат. Крім того, це сприяє збереженню ресурсів та покращенню керованості процесів в організації, що в свою чергу має позитивний вплив на її фінансову стійкість та здатність досягати більш високого рівня рентабельності.

Другий висновок стосується необхідності інтеграції системи оцінки ризиків у всі аспекти діяльності підприємства. Відділення оцінки ризиків від стратегічного та оперативного управління може призвести до неефективного реагування на зміни в зовнішньому середовищі

та внутрішніх процесах. Інтеграція ж дозволяє враховувати потенційні ризики при прийнятті рішень на всіх рівнях управління, що сприяє збільшенню внутрішньої взаємодії та забезпечує більш гармонійний розвиток організації.

Третій висновок стосується важливості використання сучасних методів та інструментів для оцінки ризиків. Технологічний розвиток надає підприємствам можливість використовувати аналітичні системи, штучний інтелект, великі дані та інші інноваційні засоби для більш точного та прогнозованого аналізу ризиків. Це дозволяє підприємствам зробити краще обгрунтовані рішення та підвищити ефективність своєї діяльності.

Отже, результати цього дослідження підтверджують, що система оцінки ризиків має вагомий вплив на збільшення прибутковості підприємства. Впровадження ефективної системи оцінки ризиків є ключовим елементом стратегічного управління, що допомагає забезпечити стабільність, конкурентоспроможність та стійкий розвиток підприємства в умовах невизначеності та змін у бізнес-середовищі.

Запровадження СОР позитивно впливає на бізнес-процеси підприємства: систематизує активи, виявляє загрози щодо активів та вразливості щодо їх реалізації, надає змогу правильно оцінити менеджментом підприємства ефективність свої дій. Регулярне проведення ОР та обробки виявлених ризиків дозволяє підприємству вдосконалити бізнес-процеси, підвищити навченість персоналу і тим самим підвищити дохідність. Отже, СОР є важливим інструментом для підприємства, що дозволяє зменшувати ризики та підвищувати ефективність його діяльності. Впровадження системи може бути складним процесом, але це інвестиція, яка може принести значну користь в майбутньому.

Список використаних джерел

1. International Organization for Standardization. (2013, Oct. 01). ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.. Режим доступу: https://www.iso.org/standard/54534.html (останнє зверення 31.03.2023р.)
2. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного компанії України:\\ Режим доступу: http://zakon5.rada.gov.ua/laws/show/v0365500-11 (останнє зверення 31.03.2023р.)
3. Верба В.А. Інформаційне забезпечення управління розвитком компанії / В.А. Верба // Формування ринкової економіки: зб. наук. праць ДВНЗ "КНЕУ імені В.Гетьмана". – 2009. – № 22. – С. 145 – 154.
4. Економічна безпека держави: оцінювання та стратегічні орієнтири забезпечення : [монографія] / О. В. Комеліна, С. В. Онищенко, А. В. Матковський, О. А. Пугач. // Полтава : ПолтНТУ. – 2013. – С. 202.
5. Цвігун Т. В. Економічна безпека в системі національної безпеки України / Т.В, Цвігун // Економіка та суспільство. Вип. 11. К. – 2017. – С. 150–156.
6. Рейтинг закладів вищої освіти у сфері управління МОН, які фінансуються за формулою, за оцінкою зайнятості та показником працевлаштування їх випускників. // Режим доступу: https://mon.gov.ua/storage/app/media/news/2022/02/03/01/Zvit.z.monitorynhu.pratsevlashtuvannya-2022-02-03.pdf (останнє звернення 04.04.2023р.)
7. International Organization for Standardization. (2018, Febr. 15). ISO 31000. Risk management. Guidelines. Режим доступу: https://www.iso.org/standard/65694.html. (останнє зверення 31.03.2023р.).

Робота виконана під науковим керівництвом к.т.н., доцента
ЗВЄРЄВА В.П.

АНАЛІЗ СУЧАСНИХ ВИМОГ ДО ІНФОРМАЦІЙНИХ СИСТЕМ ОСВІТНІХ ЗАКЛАДІВ

ДАВИДЧУК І., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Розглянуто характеристики традиційних інформаційних систем закладів освіти. Виявлено особливості застосування характеристик моделі якості ISO/IEC 25022, що підлягають оцінюванню в сучасних закладах освіти. Розглянуто вимоги, що встановлює вищезазначений стандарт стосовно реалізації функцій кожного окремого програмного модуля інформаційної системи освітнього закладу.

The characteristics traditional information systems in educational institutions are considered. Features of the ISO/IEC 25022 quality model application characteristics in modern educational institutions have been revealed. The implementation requirements of each separate software module functions of the educational institution information system have been considered.

Актуальність дослідження. Інтернаціоналізація освіти призвела до того, що різні освітні заклади надають свої послуги, що дозволяє революціонізувати доступ до знань і нових контекстів і викликів освіти. Це змусило їх переосмислити та змінити свої форми управління та адміністрування, щоб вижити та конкурувати в сучасному капіталістичному світі з новими механізмами інтеграції суспільства-знань.

Щоб подолати ці нові виклики, необхідно покращити свої процеси прийняття рішень, інтегруючи та аналізуючи всю доступну інформацію, щоб оптимізувати ресурси, надати якісні послуги та підвищити актуальність використання своїх програм. Таким чином, необхідно впроваджувати інформаційні системи, які надають широкий спектр даних з інформацією, спрямованою на всі групи користувачів. Інформаційна система повинна, перш за все, дозволяти оцінювати, аналізувати та вирішувати різні проблеми, а також наслідки внутрішніх освітніх дій на суспільство[3, с. 308].

Наразі концепція інформаційних систем у різних освітніх закладах змінилася, враховуючи те, що сьогодні вони використовуються більше як інструмент підтримки у прийнятті рішень, ніж як простий запис історичних даних. На це вказують різні маркетингові документи щодо апаратного та програмного забезпечення: «інформаційні системи поступово переходять до кімнат прямої взаємодії на керівних рівнях». Інформація та технології, що використовуються для підтримки їх отримання, обробки, зберігання, відновлення та розповсюдження набули стратегічного значення в усіх типах організацій, а також в закладах освіти на всіх рівнях системи, державних чи приватних. Все вищезазначене і визначає актуальність обраної тематики.

Метою статті є проведення аналізу вимог до інформаційних систем сучасних освітніх закладів. Для виконання мети необхідно розглянути наступні завдання:

- розглянути характеристики традиційних інформаційних систем закладів освіти;
- виявити особливості застосування характеристик моделі якості ISO/IEC 25022, що підлягають оцінюванню в сучасних закладах освіти;
- розглянути вимоги, що встановлюють вищезазначений стандарт стосовно реалізації функцій кожного окремого програмного модуля інформаційної системи освітнього закладу.

Об`єктом дослідження є інформаційні системи сучасних освітніх закладів.

Предметом дослідження є вимоги до впровадження інформаційних систем в сучасних освітніх закладах.

Аналіз результатів дослідження. Інформаційні системи, які зазвичай використовуються в освітньому секторі, зосереджені на отриманні основної інформації для здійснення управління закладами освіти. Інформація, що зберігається, не аналізувалася б і в більшості випадків є відсталою, невпорядкованою, повторюваною та ненадійною чи повною. Це – головний недолік поточних систем – ненадання інформації для прийняття рішень освітнім закладом.

До характеристик традиційних інформаційних систем належать:

- підготовка персоналу, який користується освітньою системою, не відповідає потребам посади та зв`язку з іншими інституційними процесами;
- загальна відсутність системного аналізу процесів управління та центральних служб, а також недостатній рівень уваги приділено питанням користувачів, які потребують інформації для щоденної роботи та здійснення прийняття управлінських рішень;
- відсутність вертикальної та горизонтальної координації в інформаційних системах освітніх закладів.

Інноваційні моделі управління освітою повинні бути розроблені та впроваджені відповідно до потреб інформаційних систем, які допомагають зміцнити позиції закладів освіти. Система освіти повинна дозволяти приймати управлінські рішення. Таким чином, це дозволяє оцінювати процес освіти як постійний і безперервний процес, який поступово розвивається до аналітичного, стратегічного, розширеного та інноваційного рівнів.

Інформаційна система, яка відповідає поточній динаміці розвитку закладів освіти, повинна включати, серед іншого:

- інтеграцію баз даних, що дозволяє взаємопов`язати змінні системи;
- дозволяє сформувати традиційні елементи організаційної системи: людські, фінансові, технологічні, матеріальні ресурси, засоби підтримки даних або архівів, засоби обробки інформації;
- підготовку динамічного звіту: для рішень різних рівнів, які складають освітній заклад;
- виявити можливості еволюції системи освіти, тобто збільшити їх аналітичну здатність [7, с. 930].

Інформаційна система складається з компонентів, які виконують такі функції, як збирання, збору даних, класифікації, стиснення, зберігання або архівування, адміністрування, обробку або перетворення, передачу та відновлення, показу або представлення інформації. Метою освітньої системи є надання інформації для прийняття рішень і сприяння координації між різними видами діяльності. Інформаційні системи, у вузькому сенсі, включають всю запрограмовану обробку інформації, але в широкому сенсі вони включають всі людські та механічні компоненти, залучені до координації та прийняття управлінських рішень.

Щоб інформація була ефективною, вона повинна відповідати низці вимог, щоб корисність, яку вона надає, виправдовувала використання ресурсів, які були застосовані для її створення. Зокрема, має бути дотримана вимога щодо тимчасової довідковості інформації, щоб ця інформація була справді оперативною.

Характеристикою систем для закладів освіти є індикатори управління. Індикатор визначається як спостережуваний прояв функції або характеристики однієї чи кількох змінних, що представляють інтерес, піддається оцінці, який надає кількісну інформацію та/або якісну характеристику. Систему індикаторів можна визначити як структурований і узгоджений набір індикаторів, об`єднаних чи ні, відповідно до системи змінних і категорій, які представляють управління або функціонування підрозділу аналізу щодо конкретної функції [4, с. 101].

Розробка та використання індикаторів як критеріїв для формулювання політики, планування та прийняття рішень у закладах освіти пов`язуються з дуже важливою зміною в методології, яка традиційно використовується для управління, моніторингу та контролю інформації. Всі вони призначаються для представлення ситуації суб`єкта в певний період часу.

Концепція освітньої автономії означає, що навчальні заклади вважаються автономними організаціями з точки зору планування, управління та контролю. Таким чином, керівники цих організацій володіють автономією приймати рішення, які вони вважали доречними, беручи до уваги рішення своїх колегіальних органів і чинних нормативних актів, які визначають діяльність закладу освіти, як державних положень (багато з них залежать від європейських нормативних актів), таких як нормативні акти автономного співтовариства, де знаходиться сам заклад освіти, так і нормативні акти, видані самими закладами освіти.

Отже, обов`язковою умовою є те, що інформаційна система, з якою мають працювати всі відділи освітніх закладів, має бути комплексною та диверсифікованою, щоб інформаційні потоки не накладалися та доповнювали один одного, і, таким чином, можна було використовувати переваги великої кількості користувачів у межах суб`єктів.

Інформаційна система закладу освіти дозволяє установі перейти від системи звітності на тактичному та транзакційному рівнях до системи, яка дозволяє аналізувати інформацію в режимі реального часу з використанням аналітичних інструментів, прогнозного моделювання, створення вітрин даних, які гарантують, що установа на всіх своїх ієрархічних рівнях планує, контролює та управляє на стратегічному рівні [1, с. 209].

Нова інформаційна система може викликати всередині установ різні реакції, серед яких є відмова від змін. Значна кількість проектів розробки та впровадження інформаційних систем, як правило, закінчуються невдачею через опір змінам, головним чином, через страхи та боязнь невідомого, невдачі, втрати влади, навчання новим навичкам, залучати нові людські таланти, бути заміненим або ставити під сумнів збільшення чи зменшення рівня навантаження.

Будь-яка зміна несе з собою невизначеність, тому дуже важливо, щоб працівники закладу освіти сприяли її зниженню, надаючи інформацію про проект і вплив, який він матиме на спосіб роботи, залучаючи персонал, щоб він міг знати всі переваги, які забезпечать як продуктивність роботи, так і професійний розвиток спільно з освітнім закладом. Управління змінами є життєво важливим компонентом розробки інформаційних систем і проектів впровадження, і, крім того, управління ризиками та впровадження відповідних методологій, що збільшують шанси на успіх проекту [8, с. 135].

У випадку вимірювання якості системи освіти, що використовується, модель якості ISO/IEC 25022 визначає характеристики, що підлягають оцінюванню:

- ефективність – здатність програмного забезпечення досягати цілей користувача, використовуючи мінімальні ресурси;
- задоволеність – здатність програмного забезпечення задовольняти мінімальні потреби користувачів під час його використання;
- вільність від ризику – здатність програмного забезпечення зменшувати потенційний ризик, пов`язаний з економікою, життям людей, здоров`ям або навколишнім середовищем;
- охоплення контексту – здатність програмного забезпечення використовуватися з ефективністю, результативністю, свободою ризику та задоволенням у сфері використання, для якої було визначено придбання програмного забезпечення.

Вищезазначений стандарт надає показники для вимірювання якості використання програмного забезпечення. Користувачі можуть використовувати стандартизовані метрики вимог, а також змінювати або додавати нові, вказуючи, як метрика пов`язується з моделлю якості ISO/IEC 25010. Отже, необхідно обрати характеристики та підхарактеристики якості, які потрібно оцінити, і визначити показники, які більш підходять для цього, а потім об`єктивно інтерпретувати результати, виконуючи вимірювання в реальному середовищі, де працює освітній заклад [5, с. 4].

Вищезазначений стандарт встановлює вимоги до реалізації функцій кожного окремого програмного модуля інформаційної системи освітнього закладу:

- модуль закупівель має дозволяти централізовано або розподілено реєструвати вимоги до елементів або послуг для кожної із залежностей центрів витрат, безпосередньо

контролюючи бюджетні асигнування для кожної позиції та консолідуючи вимоги для отримання відмінних переговорів з постачальником освітніх послуг;

- модуль «Основні засоби» має отримувати від складського модуля необхідну інформацію для здійснення ефективного контролю елементів, призначених кожному відповідальному працівнику, дозволяючи вносити доповнення, записуючи історію кожного основного або переданого засобу; крім того, модуль основних засобів має щомісяця реєструвати всю надану інформацію про амортизацію та перерахування в модулі бухгалтерського обліку та бюджету;
- модуль «Склад і постачання» надає можливість контролювати постачання, які здійснює постачальник, автоматично реєструючи ціни та кількість наданої техніки, узгоджені в замовленні на закупівлю, щоб уникнути можливих помилок у процесі введення вимог; він має дозволити динамічно визначати дані транзакцій, як вхідні, так і вихідні дані;
- модуль управління фінансами має відповідати за отримання прибутку освітнього закладу, керування збором написів або запропонованих замовлень, надання можливостей вибору найкращої форми оплати або рівня необхідного фінансування;
- бюджетний модуль має здійснити контроль документів, що підлягають скасуванню, або витрат, руху модулів дебіторської заборгованості та рахунків, а також доходів від продажу послуг або матеріальних товарів;
- модуль облікової заборгованості має бути інструментом для забезпечення більшого рівня контролю над освітньою системою, оскільки з цього моменту посадова особа може автоматично отримувати реєстрацію зобов`язань щодо витрат, зроблених у модулі;
- модуль бухгалтерського обліку має функціонувати як сховище всієї фінансової інформації системи, де визначаються робочі параметри інших модулів, такі як кошти, джерела, функції, план рахунків і процедури контролю, які необхідно здійснювати над цими елементами;
- модуль нарахування заробітної плати має виконувати повний процес ліквідації та виплати заробітної плати, допомоги та внесків роботодавця кожного працівника закладу освіти, а також здійснення управління режимом соціального, фіскального та парафіскального забезпечення, соціальними виплатами тощо [6, с. 872].

Основними вимогами до інформації є її повнота та достовірність. Під повнотою слід розуміти, що інформація повинна бути повна і не містити пропущених деталей. Достовірність означає, що інформація повинна бути точною і відповідати дійсності. Все це дозволяє уникнути помилок та неправильних висновків, які можуть виникнути при прийнятті рішень.

Варто, також зазначити, що Верховною Радою України визначено вимоги щодо використання інформаційних систем в управлінні освітою. До них належать:

- Обов’язкове використання інформаційних систем для збору та обробки даних про стан освіти в країні, регіоні, місті або окрузі.
- Створення єдиного інформаційного простору, що об’єднує всі рівні освіти (починаючи з дошкільної освіти і закінчуючи вищою освітою), та забезпечення його постійної актуалізації.
- Встановлення стандартів щодо формування та обміну даними між різними інформаційними системами.
- Забезпечення безпеки та конфіденційності даних, що обробляються в інформаційних системах.
- Підвищення кваліфікації працівників освітніх установ щодо використання інформаційних систем в управлінні освітою.

Законодавство повинно визначити основні типи користувачів, їх основні функції, повноваження та відповідальність, а також механізми їх взаємодії. Основними функціями інформаційної системи управління освітою можуть бути збір та обробка даних про навчальні заклади та їх діяльність, введення обліку студентів та вчителів, формування звітності, встановлення та контроль за виконанням державних стандартів та інших нормативно-

правових актів у сфері освіти. При цьому, механізм взаємодії повинен забезпечувати взаємодію між різними рівнями управління освітою, зокрема між загальнодержавними, регіональними та місцевими системами управління освітою. Окрім цього, система повинна бути забезпечена необхідним програмним забезпеченням, обладнанням та інфраструктурою для забезпечення її роботи та забезпечення безпеки зберігання та обробки даних.

Аналіз сучасних вимог до інформаційних систем освітніх закладів дозволяє визначити ключові тенденції та вимоги, які визначають ефективну організацію навчального процесу в цифровій епохі. Висновки з даного аналізу підкреслюють значущі аспекти, які впливають на підвищення якості освіти та оптимізацію управління навчальними закладами.

Інформаційні системи освітніх закладів мають відповідати вимогам масштабної цифровізації. Це означає, що платформи повинні бути гнучкими та масштабованими, здатними адаптуватися до зростаючих потреб користувачів та забезпечувати швидкий доступ до інформації. Сучасні інформаційні системи повинні гарантувати захист конфіденційної інформації студентів, викладачів та адміністраторів. Це стає особливо важливим в умовах збільшення кількості онлайн-курсів та дистанційного навчання.

Висновки. Ефективне використання інформаційних систем управління освітою потребує розроблення та впровадження нових стандартів та принципів їх створення та використання, які забезпечать їх відповідність сучасним вимогам. Також важливо забезпечити партнерство між усіма учасниками освітнього процесу та визначити їх ролі, повноваження та механізми взаємодії. Важливою складовою успішного функціонування інформаційних систем управління освітою є забезпечення безпеки та конфіденційності даних, що обробляються в інформаційних системах. Відкритість даних та автоматизована обробка інформації є важливими, хоча і не достатніми умовами забезпечення їх достовірності. Доступність даних ще не є гарантією їх використання при прийнятті рішень. Потрібно ще й сформувати розуміння необхідності аналізу цих даних та вміння і бажання їх опрацьовувати. Вищезазначені вимоги мають бути у повній мірі відтворені на практиці, щоб забезпечити високий рівень ефективності управління сучасними закладами освіти.

Список використаних джерел

1. Angonese R., Lavarda R. Analysis of the Factors Affecting Resistance to Changes in Management Accounting Systems. *ContableFinance*. 2014. No 66. P. 214–227.
2. CramW., Brohman M.K.,Gallupe R. Information Systems Control: A Review and Framework for Emerging Information. *Systems Processes*. 2016. No 17. P. 216–266.
3. GürdürD., Kaynak O., Sait S. Rethinking engineering education at the age of industry 5.0. J. *Inferent Integration*. 2022. No 25.P. 303–311.
4. LokanathM., Tushar G., Abha S. Online teaching-learning in higher education during lockdown period of COVID-19 pandemic.*Inferent Integration*.2020. No 1. P. 100–102.
5. O`Leary D. Evolving Information Systems and Technology. Research Issues for COVID-19 and Other Pandemics.*Computer Electron Commer*. 2020. No 30. P. 1–8.
6. Pereira J.L. Process-based Information Systems: Technological Infrastructure and Development Issues. *Procedia Computer Science*. 2016. No 100. P. 872–877.
7. SaideS., Sheng M. L. Knowledge exploration-exploitation and information technology: Crisis management of teaching-learningscenario in the COVID-19 outbreak. *Technological AnaliticalStrategicManagement*. 2021. No 33. P. 927–942.
8. YuhanaU. L.,Saptarini I., Rochimah S. Portability characteristic evaluation Academic information System assessment module using AIS Quality Instrument. *Information Technology, Computer, and Electrical Engineering*. 2015. No 7.P. 133–137.

Робота виконана під науковим керівництвом кандидата педагогічних наук, доцента ЖРОВОЇ Т.О.

РОЛЬ ПРОГРАМНИХ ПЛАТФОРМ ERP-СИСТЕМ В АНАЛІЗІ ТА ПРОГНОЗУВАННІ ПРОДАЖІВ ТОВАРІВ

ДОВГАЙ В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто особливості та можливості використання програмних платформ ERP-систем, як важливі інструменти ефективного управління діяльністю підприємства в розрізі аналізу та прогнозування продажів товарів.

The article examines the features and possibilities of using software platforms of ERP systems as important tools for effective management of enterprise activities in terms of analysis and forecasting of sales of goods.

Актуальність. На сьогоднішній день в умовах бізнес-середовища збільшується конкуренція між підприємствами, що змушує їх постійно вдосконалювати свої процеси та стратегії. Одним з важливих аспектів успішної діяльності компанії є ефективне управління продажами, яке передбачає аналіз та прогнозування змін в попиті на продукцію.

У сучасному бізнесі дуже важливо мати ефективну систему управління діяльністю підприємства. Однією з ключових складових такої системи є ERP-системи та програмні засоби для аналізу та прогнозування продажів товарів. Ці засоби забезпечують точніше прогнозування продажів та ефективне управління запасами, що дозволяє знизити витрати підприємства та збільшити його прибуток, а також вони дозволяють підприємствам максимально ефективно використовувати наявну інформацію про клієнтів, продукцію та ринок, а також швидко реагувати на зміни в зовнішньому середовищі.

ERP-системи та програмні засоби дозволяють зібрати та аналізувати великі обсяги даних про продажі, запаси та виробництво. За допомогою цих засобів можна побачити, які товари продаються найкраще, які найменш популярні та в якому розмірі потрібно зберігати запаси. Це дозволяє підприємству знизити витрати на запаси, уникнути необхідності зберігати надмірну кількість товарів та збільшити швидкість обігу запасів.

Крім того, ERP-системи та програмні засоби дозволяють прогнозувати попит на товари та планувати виробництво. За допомогою цих засобів можна побачити, як змінюється попит на товари в різні періоди часу та які фактори впливають на цей попит. Це дозволяє підприємству планувати виробництво з урахуванням попиту на товари та уникнути необхідності зберігати надмірну кількість товарів на складі.

Загалом, ERP-системи та програмні засоби є важливими інструментами управління діяльністю підприємства, які дозволяють знизити витрати та збільшити прибуток. Детальне розглядання ERP-систем та програмних засобів з програмної точки зору дозволяє краще зрозуміти їхню роль та переваги управління діяльністю підприємств. Такі дослідження можуть стати основою для розробки нових програмних засобів та покращення вже існуючих ERP-систем, що дозволить підприємствам ще ефективніше управляти своєю діяльністю та забезпечити більш високий рівень конкурентоспроможності на ринку.

Метою статті є дослідження можливостей використання ERP-систем та програмних засобів для аналізу та прогнозування продажів товарів.

Об'єктом дослідження є ERP-системи та програмні засоби, які використовуються для аналізу та прогнозування продажів товарів.

Предмет дослідження - методи та алгоритми, що використовуються у ERP-системах та програмних засобах для аналізу та продажу товарів з метою покращення їх ефективності та точності.

Аналіз попередніх досліджень. Дослідження, проведене в 2018 році в журналі International Journal of Engineering Research & Technology, показало, що використання ERP-

систем може допомогти зменшити запаси на складі та збільшити точність прогнозування попиту.

Дослідження, опубліковане в журналі International Journal of Supply Chain Management у 2019 році : використання програмних засобів для прогнозування попиту та планування запасів. Дослідження показало, що використання програмних засобів може допомогти забезпечити точне прогнозування попиту та ефективне планування запасів.

Дослідження, проведене в 2020 році в журналі International Journal of Advanced Science and Technology : можливості використання ERP-систем для аналізу продажів та попиту. Дослідження показало, що використання ERP-систем може допомогти забезпечити точний та своєчасний аналіз продажів та попиту, що в свою чергу допоможе управляти запасами та планувати виробництво.

Усі дослідження підкреслюють важливість використання ERP-систем та програмних засобів для ефективного управління запасами та прогнозування попиту

Виклад основного матеріалу. У сучасному світі, де бізнес є динамічним і конкурентним, важливо мати належну стратегію для забезпечення ефективного управління запасами та передбачення попиту на товари та продукцію. Зміни модних тенденцій та сезонність можуть значно впливати на попит товарів.

На сьогоднішній день, де величезна кількість споживачів здійснює покупки онлайн, надзвичайно важливо мати ERP-системи та програмні засоби для аналізу та прогнозування продажу товарів. Це дає змогу розуміти потреби клієнтів та відповідно планувати виробництво, викладати ціни та рекламувати товар. Програмні засоби для аналізу та прогнозування продажів товарів :

- *системи Business Intelligence (BI)* - один із засобів для збору та аналізу даних, які дозволяють збирати, зберігати та аналізувати великі обсяги даних. BI-системи надають змогу працювати з різноманітними джерелами даних, такими як бази даних, електронні таблиці, звіти тощо. Вони дозволяють проводити різноманітні аналітичні операції, включаючи статистичний аналіз, регресійний аналіз, аналіз тенденцій тощо.

Рис. 1. Концепція систем Business Intelligence

- *ERP (Enterprise Resource Planning) системи* забезпечують цілеспрямоване управління бізнес-процесами, включаючи планування виробництва, управління запасами та контроль витрат. Аналіз даних, які збираються цими системами, дає змогу планувати виробництво товарів на основі попиту.

Рис. 2. Концепція ERP систем

- *системи прогнозування* дають змогу визначати попит на товари на основі аналізу історії попиту та інших факторів, які можуть впливати на продажі. Вони використовують різноманітні алгоритми для прогнозування попиту, такі як регресійна модель, ARIMA-модель та інші. За допомогою цих систем можна розробляти стратегії продажу та планувати виробництво відповідно до прогнозів.
- *інструменти машинного навчання (Machine Learning)* є дуже потужним інструментом для аналізу та прогнозування продажів товарів. Вони дозволяють розробляти моделі на основі великої кількості даних, що забезпечує більш точні прогнози. Наприклад, можна розробити модель, яка буде прогнозувати попит на товари в різних регіонах залежно від сезону, погодних умов, культурних подій та інших факторів.

Огляд ERP-систем та програмних засобів для аналізу та прогнозування продажів товарів демонструє, що сучасні технології дозволяють збирати та аналізувати великі обсяги даних, розробляти прогнози та стратегії продажу на основі цих даних. Використання цих інструментів дозволяє виробникам товарів забезпечити попит на свій товар та збільшити прибуток.

Однією з найбільш популярних BI систем є QlikView, яка базується на концепції "інтерактивного аналізу даних". QlikView забезпечує зручний та інтуїтивно зрозумілий інтерфейс для користувачів, що дозволяє швидко та ефективно відображати, фільтрувати та візуалізувати дані з різних джерел.

Функціональність рішень програмного продукту QlikView :

- З'єднання з джерелами даних, такими як бази даних, ексель файли, текстові файли, веб-сервіси та інші, щоб забезпечити зручний доступ до даних.
- Візуалізація даних у різних форматах, таких як графіки, таблиці, діаграми, кругові діаграми та інші, для швидкого та зручного аналізу даних.
- Інтерактивний аналіз даних: можливість взаємодії з даними та створення "інтерактивних дерев", що дозволяє переходити між гілками дерева та відображати вибрані дані у вигляді таблиць, графіків та інших візуальних елементів.
- Пошук та фільтрація даних: QlikView дозволяє швидко та ефективно знаходити необхідні дані з використанням різних фільтрів та пошукових запитів.

- Створення різних аналітичних звітів та дашбордів з використанням візуалізації даних, що допомагає швидко та зручно аналізувати дані та приймати управлінські рішення.
- Підтримка мобільних пристроїв: можливість отримувати доступ до даних та звітів з мобільних пристроїв, що забезпечує зручний та швидкий доступ до даних навіть в дорозі.
- Спільна робота над проектами та даними з допомогою спільних робочих просторів та можливості ділитися даними та звітами з колегами. Крім того, QlikView підтримує інтеграцію зі сторонніми інструментами та системами управління даними, що дозволяє легко і ефективно інтегрувати QlikView з іншими рішеннями в бізнесі.

Основним принципом дії QlikView є побудова "інтерактивних дерев". При створенні зв'язків між джерелами даних, програма створює дерево відносин між елементами даних. Користувачі можуть взаємодіяти з даними, переходити між гілками дерева та відображати вибрані дані у вигляді таблиць, графіків та інших візуальних елементів.

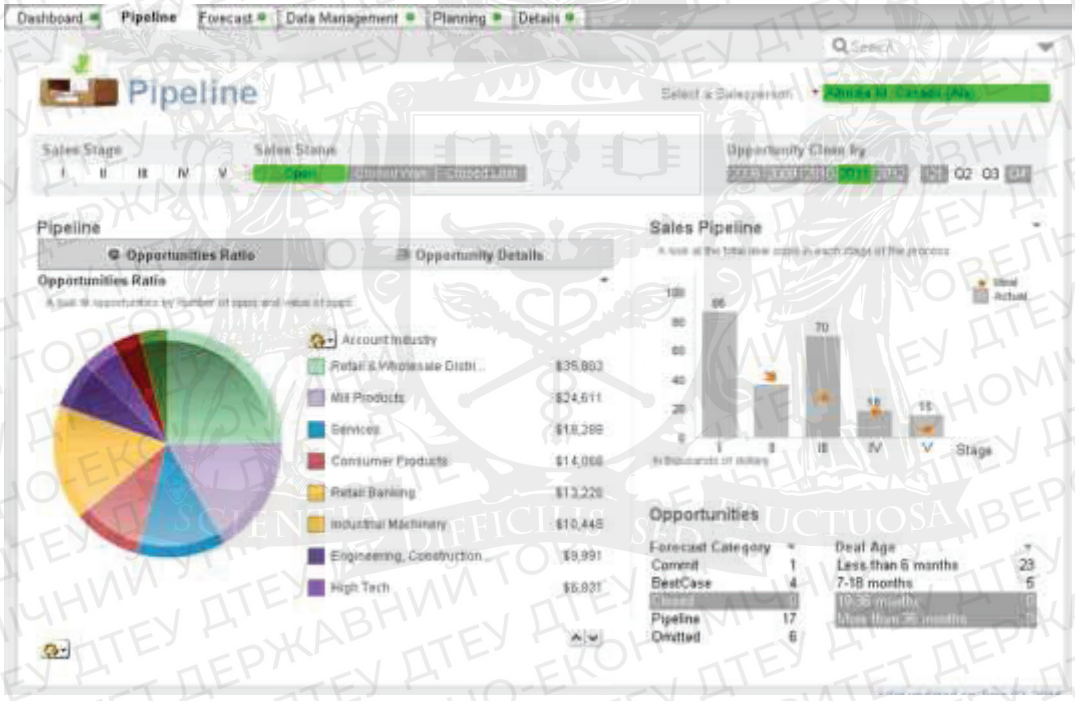


Рис. 3. Перегляд інформаційної панелі даних по продажам

Процес створення BI звіту в QlikView починається з завантаження даних з різних джерел. Далі, користувачі створюють "сценарії" (scripts) для обробки та очищення даних, а також для створення зв'язків між джерелами даних. Після цього, користувачі можуть створювати різні візуалізації даних та звіти з використанням зручного інтерфейсу QlikView.

Однією з ключових переваг цієї системи є швидкість та ефективність обробки великих обсягів даних. Вона використовує вбудовану технологію "інтерактивної пам'яті" (in-memory technology), що дозволяє зберігати та обробляти дані в оперативній пам'яті, замість зберігання на диску. Це робить можливим швидкий доступ до даних та швидке створення звітів та аналізів.

Ще однією перевагою QlikView є його можливість автоматично підлаштовуватися під потреби користувачів. Користувачі можуть вибирати дані, які їм необхідні, фільтрувати дані за певними параметрами та вибирати спосіб відображення даних.

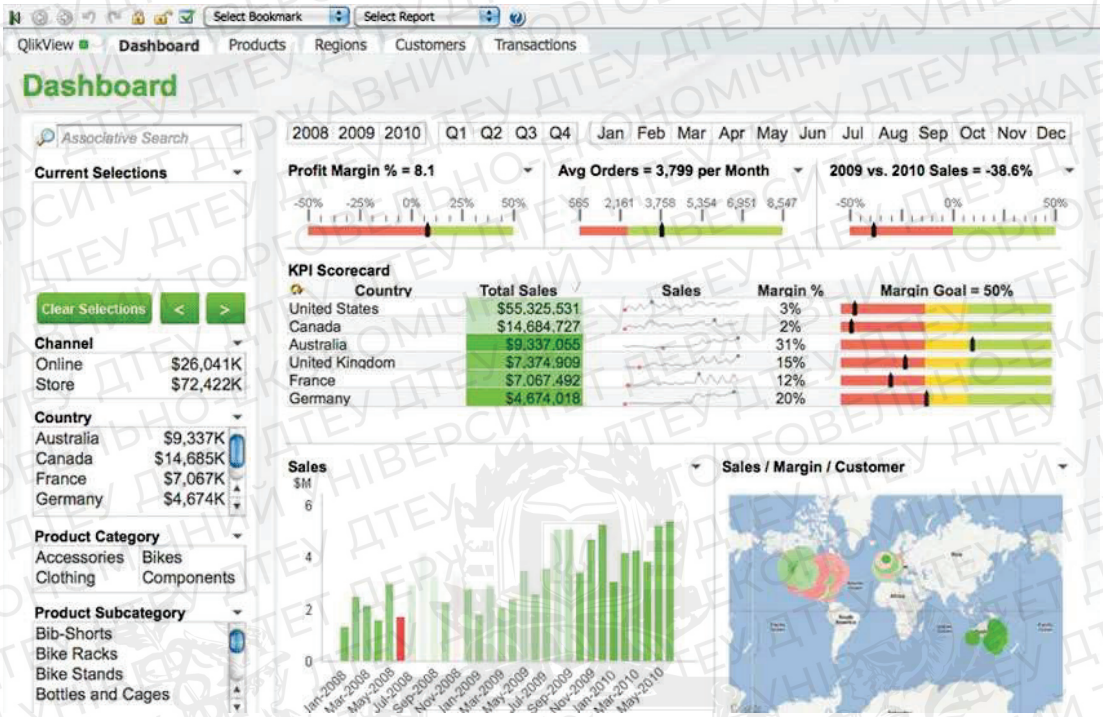


Рис. 4. Перегляд панелі інструментів

У QlikView також є можливість розширення функціональності за допомогою додаткових плагінів та розширень. Користувачі можуть створювати власні додатки та розширювати функціональність QlikView для вирішення конкретних завдань.

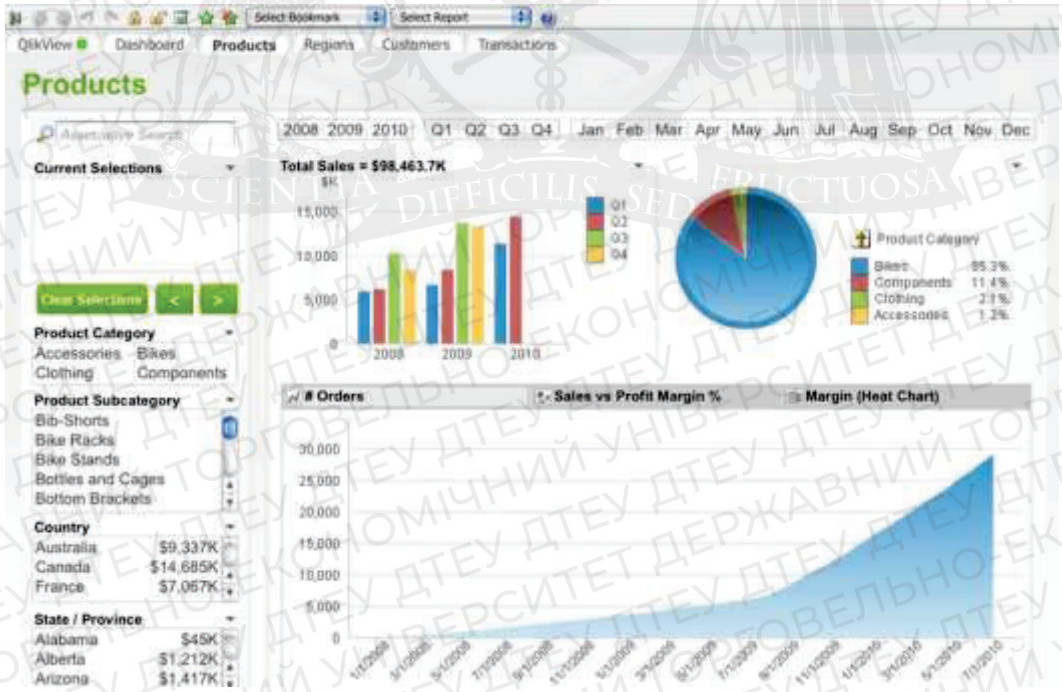


Рис. 5. Аналіз товарної інформації

Усі ці переваги роблять BI систему QlikView популярним рішенням для аналізу даних в бізнесі. Використання QlikView дозволяє користувачам швидко та ефективно аналізувати дані, забезпечувати краще управління бізнесом, створювати індивідуальні аналітичні інструменти та приймати обгрунтовані рішення.

ERP система SAP S/4HANA є програмним комплексом для інтегрованого управління ресурсами підприємства. Вона включає в себе різноманітні функції та процеси, необхідні для

ефективного управління бізнесом, які забезпечують потреби користувачів у точній та надійній інформації, стандартизації та автоматизації бізнес-процесів, а також підвищення якості прийняття рішень.

Концепція SAP S/4HANA полягає в тому, щоб забезпечити інтеграцію усіх бізнес-процесів підприємства в єдину систему, що дозволяє отримати єдину версію даних про бізнес та створити спільну платформу для управління діяльністю підприємства. SAP S/4HANA дозволяє об'єднати фінансовий облік, логістику, управління персоналом, продажі та маркетинг в єдину систему. Вона забезпечує можливість побудови індивідуальних конфігурацій для кожного підприємства та інтегрується з іншими системами.

Система SAP S/4HANA використовує відкриту архітектуру, що дозволяє підключати додаткові рішення та забезпечує зручний інтерфейс для користувачів. Вона базується на інтернет-технологіях та може працювати як в хмарі, так і на локальному сервері.

Рис. 6. Інтерфейс програми SAP S/4HANA

Основним принципом дії системи SAP S/4HANA є взаємодія між всіма модулями системи, що дозволяє забезпечити інтегровану обробку даних та швидкий доступ до необхідної інформації. Система використовує технології обробки даних в реальному часі, що дозволяє отримувати швидкий доступ до даних та швидко реагувати на зміни в бізнес-процесах.

Процеси в системі SAP S/4HANA охоплюють всі галузі діяльності підприємства, включаючи фінанси, логістику, управління персоналом, продажі та маркетинг. Система дозволяє планувати та керувати виробництвом, складською логістикою та доставкою продукції, а також відстежувати її рух від постачальника до клієнта.

Функціональність системи SAP S/4HANA включає в себе такі можливості, як управління проектами, аналітику даних, планування ресурсів підприємства, управління звітністю та бізнес-аналіз. Система також дозволяє автоматизувати процеси обліку та оплати рахунків, управління розрахунками з клієнтами та постачальниками, управління замовленнями та продажами.

Рис. 7. Моделювання плану потужності

В загальному, система SAP S/4HANA дозволяє підприємствам отримати комплексне управління своєю діяльністю та забезпечити оптимальний рівень ефективності та прибутковості. Вона є потужним інструментом для автоматизації бізнес-процесів та створення єдиного джерела даних для прийняття рішень на всіх рівнях підприємства.

Система прогнозування Streamline - це програмне забезпечення для автоматизованого прогнозування та аналізу даних в режимі реального часу. Streamline базується на технології машинного навчання та штучного інтелекту, що дозволяє отримувати точні прогнози з високою швидкістю та ефективністю.

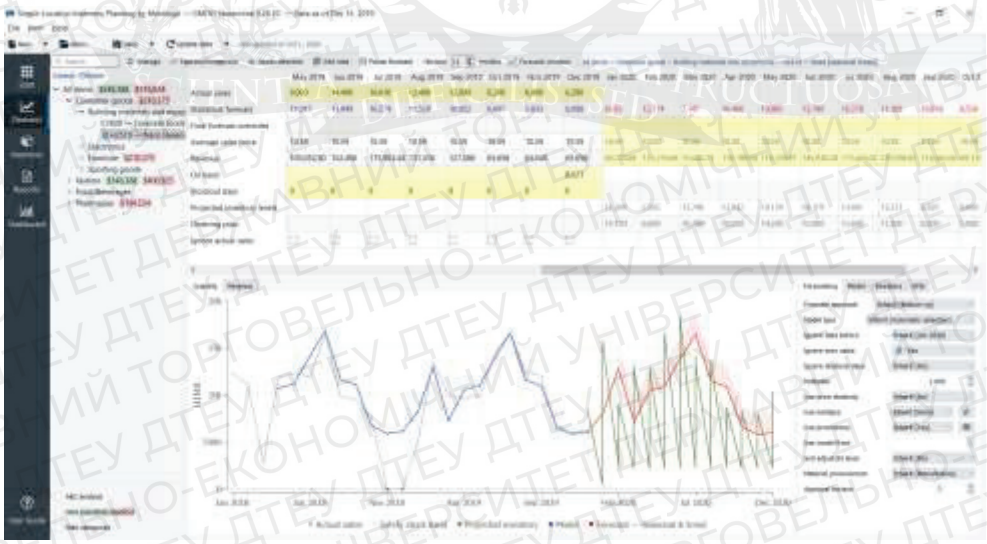


Рис. 8. Інтерфейс системи прогнозування Streamline з використанням машинного навчання

Архітектура Streamline є сучасною технологією для аналізу та прогнозування даних в реальному часі. Вона складається з трьох основних компонентів: компоненту збору даних, компоненту обробки даних та компоненту прогнозування.

Компонент збору даних відповідає за збір даних з різних джерел, таких як бази даних, сенсори та інші джерела даних. Цей компонент забезпечує можливість збирати великі обсяги даних у режимі реального часу, що дозволяє підприємствам миттєво реагувати на зміни в

зовнішньому середовищі та швидко приймати рішення. Для забезпечення швидкості та ефективності збору даних використовуються технології, такі як Apache Kafka та Apache Storm.

Компонент обробки даних забезпечує аналіз та обробку даних, які були зібрані компонентом збору даних. Цей компонент включає в себе різноманітні алгоритми та методи аналізу даних, що дозволяє використовувати дані для прогнозування тенденцій та побудови стратегій управління бізнесом. Для обробки даних використовуються технології, такі як Apache Spark та Apache Flink.

Компонент прогнозування відповідає за проведення прогнозування на основі оброблених даних та виведення результатів прогнозування. Для прогнозування використовуються різні моделі машинного навчання, такі як нейронні мережі, дерева рішень та інші.

Усі компоненти архітектури Streamline працюють разом та забезпечують швидке та ефективне аналізування даних в реальному часі. Використання цієї технології дозволяє підприємствам отримувати корисну інформацію про свій бізнес швидко та ефективно, що допомагає в прийнятті важливих рішень та побудові ефективних стратегій управління бізнесом. Таким чином, архітектура Streamline є потужним інструментом для аналізу та прогнозування даних, який може допомогти підприємствам вдосконалити свої процеси та збільшити ефективність своєї діяльності.

Основною функціональністю Streamline є прогнозування різних параметрів в режимі реального часу, таких як продажі, виробництво, трафік та інші. Система також дозволяє аналізувати дані та відстежувати зміни у даних з часом.

Концепція Streamline полягає в тому, щоб забезпечити швидку та точну обробку даних та прогнозування в режимі реального часу, щоб дозволити користувачам оперативно реагувати на зміни в даних та приймати ефективні рішення.

Основним принципом дії системи є використання технологій машинного навчання та штучного інтелекту для прогнозування та аналізу даних в режимі реального часу. Система використовує навчальні дані для тренування моделей машинного навчання та підтримує їхню актуальність з часом за допомогою постійного збору та обробки даних.

Процеси в системі прогнозування Streamline включають збір та обробку даних, тренування моделей машинного навчання, прогнозування на основі даних та виведення результатів прогнозування. Для кожного процесу використовуються відповідні технології, що дозволяють забезпечити швидку та ефективну роботу системи.

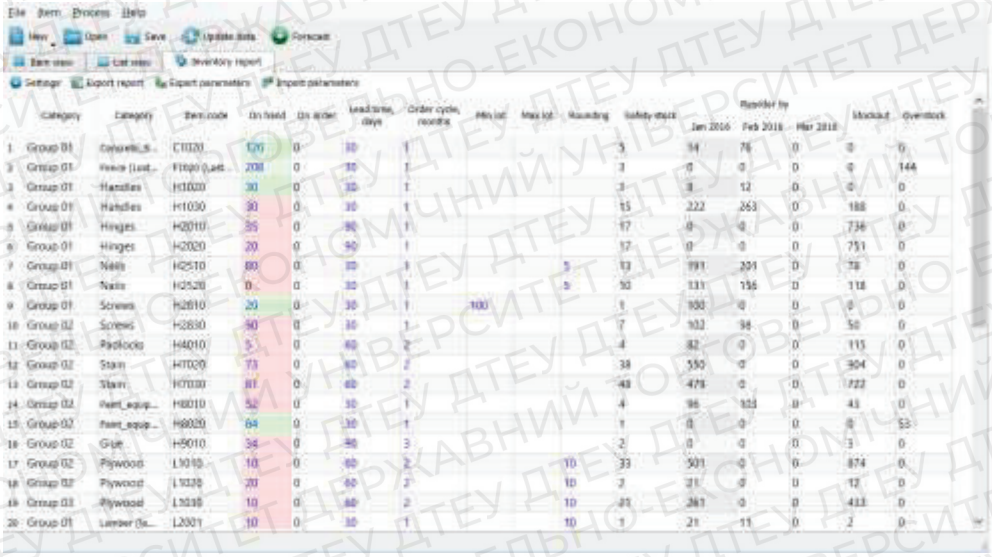


Рис. 9. Звіт інвентарю

Загалом, система прогнозування Streamline є потужним інструментом для прогнозування та аналізу даних в режимі реального часу. Використання технологій

машинного навчання та штучного інтелекту дозволяє отримувати точні прогнози з високою швидкістю та ефективністю, що дозволяє користувачам оперативно реагувати на зміни в даних та приймати ефективні рішення.

Висновки. У статті розглянуто важливість використання ERP-систем та програмних засобів для аналізу та прогнозування продажів товарів. Це дозволяє компаніям забезпечувати більш точне прогнозування продажів, що підвищує ефективність управління запасами та покращує стосунки зі споживачами.

ERP-системи, такі як SAP S/4HANA, дозволяють зібрати та обробляти дані з різних джерел, зокрема з магазинів, складів та інтернет-магазинів. За допомогою таких систем, компанії можуть отримувати доступ до актуальної інформації про обсяги продажів та попит на товари в різних регіонах та каналах збуту. Це дозволяє компаніям планувати виробництво та поставки продукції з урахуванням попиту.

Програмний засіб QlikView дозволяє аналізувати дані та візуалізувати їх у зручному для сприйняття форматі. Це допомагає компаніям швидко виявляти тенденції та зміни в попиті, а також прогнозувати майбутні продажі.

Streamline є іншим програмним засобом для аналізу продажів, який дозволяє отримувати детальну інформацію про продажі товарів за різними параметрами, такими як регіон, канал збуту, тип товару тощо. Це дозволяє компаніям точно визначати найбільш прибуткові канали збуту та товари, що дозволяє зосередити увагу на них та підвищити прибутковість.

Узагальнюючи, використання ERP-систем та програмних засобів, таких як QlikView, SAP S/4HANA та Streamline, дозволяє компаніям точно прогнозувати та аналізувати продажі товарів, що підвищує їх ефективність та дозволяє зосередитися на найбільш прибуткових каналах збуту та товарах. Це також допомагає знизити ризики пов'язані зі зайвими запасами та недостатньою кількістю товарів на складі.

Використання таких систем дозволяє компаніям не тільки бути більш гнучкими та адаптивними до змін в попиті та на ринку загалом, але й оптимізувати процеси, зменшувати витрати та збільшувати прибуток, бути більш конкурентоспроможними.

Список використаних джерел

1. Мельничук, А. А. Використання ERP-системи для оптимізації управління підприємством / А. А. Мельничук, В. М. Євтушенко // Економічні науки. – 2018. – № 2 (27). – С. 38-43.
2. Офіційний сайт QlikView // Режим доступу : https://www.qlik.com/us/products/qlikview (дата звернення 29.03.2023р.)
3. Краснокутська, О. А. Аналіз можливостей використання ERP-систем у підприємницькій діяльності / О. А. Краснокутська // Міжнародний науковий журнал "Інтернаука". – 2019. – № 3 (10). – С. 90-93.
4. Микитюк, А. А. Використання програмного забезпечення для аналізу продажів товарів / А. А. Микитюк, А. В. Ткаченко // Економічні науки. – 2017. – № 2 (22). – С. 43-48.
5. Офіційний сайт SAP S/4HANA // Режим доступу : https://www.sap.com/ukraine/products/erp/s4hana.html (дата звернення 31.03.2023р.)
6. Ковальова, А. М. Аналіз програмних засобів для прогнозування продажів товарів / А. М. Ковальова, Ю. В. Сідлецький // Науковий вісник Херсонського державного університету. Серія: Економічні науки. – 2018. – Вип. 29, т. 2. – С. 26-30.
7. Офіційний сайт Streamline // Режим доступу : https://gmdhsoftware.com/ua/ (дата звернення 02.04.2023р.)

Робота виконана під науковим керівництвом к.т.н., доцента
РЗАЄВОЇ С.Л.

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДОКУМЕНТАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

ЄГУНОВ П., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У даній статті було розглянуто технології, які використовуються для забезпечення безпеки документів у системах електронного документообігу. Основні завдання та принципи для яких застосовується система електронного документообігу, що дозволяє зрозуміти та оцінити основні місця ураження електронних та програмних частин цих систем.

This article discusses the technologies used to ensure document security in electronic document management systems. The main tasks and principles for which the electronic document management system is used, which allows to understand and evaluate the main places of defeat of electronic and software parts of these systems.

Актуальність. Системи електронного документообігу (СЕД) стали дуже популярними серед підприємств, організацій та установ в сучасному світі. Вони змінили спосіб, яким ми зберігаємо та керуємо документами, надаючи численні переваги, такі як зручність, доступність та економію. СЕД є надійним та швидким засобом обміну інформацією, що дозволяє прискорити бізнес-процеси та знизити витрати на друк та доставлення паперових документів. Однак, необхідно враховувати ризики, пов'язані зі зберіганням та передачею конфіденційної інформації через ці системи. Захист даних є важливою задачею для будь-якої компанії, організації чи установи, що працює з електронними документами. Втрата або розголошення конфіденційної інформації може призвести до серйозних наслідків, таких як втрата довіри клієнтів та партнерів, штрафні санкції та втрата конкурентоспроможності на ринку. У цій статті розглянуті основні засоби захисту даних в системах електронного документообігу. Одна з відмінностей від звичайних паперових носіїв полягає у тому, що всі дані представлені в електронному вигляді. Процеси роботи з електронними документами аналогічні процесам з паперовими: вони створюються; обробляються; відправляються в середині та за межами компанії; надходять адресатам; використовуються; зберігаються; знищуються. Від впровадження електронного документообігу очікується більш ефективне управління підприємством шляхом автоматичного контролю виконання, прозорості діяльності установи на всіх рівнях; підтримка ефективного накопичення, управління і доступу до інформації і знань; забезпечення кадрової гнучкості внаслідок більшої формалізації діяльності кожного співробітника і можливості збереження всієї історії його діяльності; усунення дублювання і багаторазового перетворення інформації; протоколювання діяльності установи в цілому (внутрішні службові розслідування, аналіз діяльності підрозділів, виявлення "гарячих точок"); оптимізація управлінських процесів, автоматизація механізму їх виконання і контролю; виключення або максимально можливе скорочення обігу паперових документів; заощадження ресурсів за рахунок скорочення витрат на управління потоками ЕД в організації; виключення необхідності чи істотне спрощення і здешевлення збереження паперових документів внаслідок наявності оперативного електронного архіву [1].

Також у статті зазначається, що для успішного впровадження систем електронного документообігу, потрібно забезпечити грамотне планування процесів та розробку відповідних стратегій безпеки.

У цілому, системи електронного документообігу можуть значно полегшити роботу підприємств, організацій та установ, прискорити бізнес-процеси та знизити витрати, проте важливо бути уважними та дотримуватись заходів безпеки, щоб уникнути можливих ризиків, пов'язаних зі зберіганням та передачею конфіденційної інформації.

Основними загрозами безпеки СЕД є:

– Загроза цілісності інформації може включати також внесення змін до даних з метою викривлення інформації або введення неправдивої інформації. Також, може бути загрозою цілісності інформації наслідок навмисного введення інформації некомпетентними або недоброчесними користувачами. Для захисту цілісності інформації, компанії можуть застосовувати технології контролю цілісності даних та перевірку доступу до них, а також політики та процедури щодо захисту від неправомірного впливу на інформацію [2].

– Загроза конфіденційності - це можливість втрати, викрадення або порушення конфіденційності важливої інформації. Це може статися через крадіжку, перехоплення, витік даних або навіть зміну маршруту доставки. Для зменшення ризику загрози конфіденційності, організації можуть використовувати захисні технології, такі як шифрування, фірмові мережі, мультифакторна аутентифікація і так далі. Крім того, важливо мати політику безпеки, яка визначає, які заходи повинні бути прийняті для забезпечення конфіденційності даних, і яка враховує різноманітні види загроз, що можуть виникнути [2].

– Загроза роботі системи — ця загроза може бути настільки серйозною, що призведе до зупинки всієї діяльності компанії, що використовує СЕД. Наприклад, атака з використанням шкідливого програмного забезпечення може заблокувати доступ користувачів до СЕД, що зробить неможливим обробку документів та зв'язок між співробітниками компанії.

– Загроза доступності — здійснення дій, які унеможливлюють чи ускладнюють доступ до СЕД, зокрема, створення таких умов, при яких доступ до послуги чи інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших цілей. Такі дії можуть бути здійснені зловмисниками з метою зниження продуктивності бізнесу, шантажу або просто задоволення вандалів. Для попередження цієї загрози, необхідно розробляти та впроваджувати заходи захисту, такі як резервне копіювання даних, захист від DDOS-атак і так далі [2].

Джерела загроз:

– *Користувач системи електронного документообігу*

У системі електронного документообігу користувач може бути потенційним загрозливим фактором, особливо якщо він необачний або має недобрі наміри. Не тільки внутрішні, але й легальні користувачі можуть становити ризик, наприклад, захопивши апаратну частину системи або крадучи дані для власної користі. Таким чином, широкий спектр можливих загроз від користувачів необхідно враховувати при захисті даних в системі електронного документообігу.

– *Персонал IT-служби підприємства*

Особлива увага повинна бути приділена персоналу IT-служби підприємства, який є одною з основних груп ризику. Ці фахівці зазвичай мають широкі та нерідко необмежені повноваження, доступ до сховищ даних і володіють всіма необхідними знаннями для цільового враження. Крім того, вони є найбільш кваліфікованими у питаннях безпеки та інформаційних можливостей. За результатами численних досліджень, майже 80% втрат документів та інформації пов'язані зі злочинними діями «внутрішнього ворога».

– *Зовнішні Зловмисники*

Зазвичай конкурентні компанії, або хакери які діють по цільвим компаніям, з метою дестабілізувати компанію, завдати їй фінансових та репутаційних втрат. Зовнішні зловмисники можуть бути різного рівня підготовки та застосовувати чисельні методи знайти вразливе місце та заподіяти шкоди компанії.

Технології для електронних обмінів документів мають відповідати сертифікованим стандартам, і ця відповідність має контролюватися. На різних етапах процесу обміну інформацією беруть участь оператори (користувачі) та інформаційні технології — технічні (персональні комп'ютери, сервери) і програмні (операційні системи, програми виведення препроцесорів). Інформація створюється людьми, потім перетворюється на дані, а потім

вводиться в автоматизовані системи у вигляді електронних документів, які разом з іншими такими документами представляють інформаційні ресурси. Комп'ютери обмінюються даними по каналах зв'язку. Під час роботи автоматизованих систем відбувається перетворення даних (електронних документів) відповідно до інформаційних технологій, що застосовуються. Системи електронного документообігу є важливою складовою електронної бізнес-інфраструктури, тому забезпечення їх технічної безпеки є критичним завданням, для цього можуть бути використані компоненти зображені на рис.1.

Рис.1. Компоненти технічної безпеки

У системах електронного документообігу виникає потреба захистити дані від несанкціонованого доступу, втрати, порушення конфіденційності та цілісності. Для цього існують різні засоби захисту даних.

Одним з основних засобів є криптографічні методи, які забезпечують конфіденційність, цілісність та автентичність електронних документів. Для цього використовуються шифрування, електронний підпис та інші методи.

Контроль доступу є ще одним компонентом технічної безпеки. Він обмежує доступ до електронних документів на основі рівня доступу, встановленого адміністратором системи. Це забезпечує безпеку документообігу та захищає конфіденційну інформацію.

Системи виявлення вторгнень (IDS) є програмним забезпеченням, яке відслідковує мережеві активності та сповіщає про можливі вторгнення. IDS дозволяють вчасно виявляти та запобігати атакам на систему документообігу.

Аудит є системою відстеження та аналізування дій користувачів в системі документообігу, що дозволяє виявляти потенційні загрози та проводити розслідування інцидентів безпеки.

Засоби бекапу дозволяють зберігати резервні копії електронних документів та іншої важливої інформації, що дозволяє відновлювати їх у разі втрати.

Системи управління безпекою інформації (ISMS) забезпечують системний підхід до управління безпекою інформації та допомагають забезпечувати відповідність з різними стандартами та нормативними документами.

Основні засоби захисту даних в системах електронного документообігу

1. Шифрування – це процес, який перетворює відкритий текст на зашифрований текст, який неможливо прочитати без секретного ключа чи пароля. Шифрування є важливою технологією для забезпечення безпеки документів у системах електронних документів. Шифрування можна застосовувати до документів у дорозі та в стані спокою. Для документів,

що передаються, можна застосувати шифрування за допомогою таких протоколів, як Transport Layer Security (TLS) або Secure Sockets Layer (SSL). Для документів, що перебувають у стані спокою, шифрування можна застосувати до самого файлу або пристрою чи сервера, де зберігається документ. Найпоширенішими алгоритмами шифрування, які використовуються для захисту документів, є Advanced Encryption Standard (AES) і Rivest-Shamir-Adleman (RSA).

2. Цифрові підписи – це електронні підписи, які використовують криптографію для перевірки автентичності та цілісності документа. Цифровий підпис створюється за допомогою закритого ключа для шифрування хешу документа, який можна перевірити за допомогою відповідного відкритого ключа. Цифрові підписи гарантують, що документ не було підроблено та що підписувач є тим, за кого себе видає. Цифрові підписи можна реалізувати за допомогою різних стандартів, таких як інфраструктура відкритих ключів (PKI) або проста інфраструктура відкритих ключів (SPKI).

3. Контроль доступу гарантує, що лише авторизований персонал має доступ до документів. Контроль доступу можна реалізувати за допомогою різних методів автентифікації, таких як паролі, біометрія, смарт-карти або токени. Контроль доступу також може бути реалізований на різних рівнях, таких як рівень документа, рівень папки або рівень системи. Контроль доступу на основі ролей (RBAC) – це поширений метод керування доступом, який призначає різні рівні доступу для різних ролей в організації. Контроль доступу є критично важливим для безпеки документів, оскільки вони обмежують ризик неавторизованого доступу до документів.

4. Журнали аудиту – це записи всіх дій, виконаних з документом, у тому числі хто мав до нього доступ, коли до нього був доступ і які зміни були внесені. Журнали аудиту забезпечують підзвітність і прозорість, полегшуючи виявлення будь-якого несанкціонованого доступу або змін до документів. Журнали аудиту можуть бути реалізовані за допомогою різних методів, таких як файли журналів, інструменти моніторингу системи або інструменти аудиту бази даних. Журнали аудиту необхідні для дотримання нормативних вимог, таких як HIPAA або GDPR.

5. Рішення для резервного копіювання та відновлення гарантують, що документи не будуть втрачені через системні збої або катастрофи. Резервне копіювання та відновлення можна реалізувати за допомогою різних методів, таких як резервне копіювання на стрічку, хмарне резервне копіювання або дзеркальне відображення сервера. Рішення для резервного копіювання та відновлення мають вирішальне значення для безпеки документів, оскільки вони гарантують доступність документів у разі потреби та можливість їх відновлення у разі аварії.

6. Водяні знаки – це техніка, яка вбудовує в документ унікальний ідентифікатор, щоб зробити його відстежуваним. Водяні знаки можуть бути видимими або невидимими, і їх можна застосовувати на різних рівнях деталізації, наприклад на рівні документа, сторінки або зображення. Водяні знаки використовуються для різних цілей, наприклад для захисту авторських прав, відстеження розповсюдження документів або виявлення підробки документів.

7. Управління цифровими правами (DRM) – це технологія, яка контролює доступ до цифрового вмісту, його копіювання та розповсюдження. DRM використовується для захисту інтелектуальної власності та забезпечення дотримання ліцензійних угод. DRM можна реалізувати за допомогою різних методів, таких як шифрування, контроль доступу або цифрові водяні знаки. DRM зазвичай використовується для документів, які містять чутливу або конфіденційну інформацію.

8. Брандмауер – це пристрій безпеки мережі, який забезпечує захист від небажаного мережевого трафіку, називається брандмауером. Брандмауер можна реалізувати за допомогою різних методів, таких як апаратне забезпечення, програмне забезпечення або хмарні рішення. Використання брандмауера може допомогти захистити СЕД від різних кіберзагроз, зокрема від шкідливих програм, хакерських атак і несанкціонованого доступу. Для ефективної роботи брандмауера необхідно регулярно оновлювати його програмне забезпечення та налагоджувати правила контролю мережевого трафіку.

Програмне забезпечення для захисту від зловмисного програмного забезпечення – це тип програмного забезпечення, призначеного для виявлення та видалення зловмисного програмного забезпечення з комп'ютерної системи. Зловмисне програмне забезпечення включає віруси, троянські програми, хробаки та інші види шкідливого програмного забезпечення. Програмне забезпечення для захисту від шкідливих програм може допомогти захистити системи електронних документів від зараження зловмисним програмним забезпеченням, яке може поставити під загрозу безпеку документів.

9. Запобігання втраті даних (DLP). DLP – це технологія, яка допомагає запобігти втраті конфіденційної інформації шляхом моніторингу та контролю доступу та передачі даних. DLP можна реалізувати за допомогою різних методів, таких як моніторинг мережі, захист кінцевих точок або хмарні рішення. DLP може допомогти запобігти витоку чи викраденню конфіденційних документів інсайдерами чи зовнішніми зловмисниками.

10. Багатофакторна автентифікація (MFA) – це техніка безпеки, яка вимагає від користувачів надання двох або більше факторів автентифікації для доступу до системи чи програми. Факторами автентифікації можуть бути те, що користувач знає (наприклад, пароль), те, що користувач має (наприклад, смарт-карта чи маркер), або те, чим користувач є (наприклад, біометричний ідентифікатор). MFA може допомогти запобігти несанкціонованому доступу до систем електронних документів, вимагаючи додаткової автентифікації, окрім пароля.

11. Шифрування на основі ролей – це техніка, яка шифрує документи на основі ролі користувача в організації. Рольове шифрування може гарантувати, що доступ до документів матиме лише авторизований персонал. Шифрування на основі ролей можна реалізувати за допомогою різних методів, наприклад шифрування на основі політики, шифрування на основі атрибутів або систем керування ключами.

Висновки. Для забезпечення безпеки документів у системах електронного документообігу можна використовувати різноманітні технології, такі як криптографічні протоколи, електронні підписи, системи контролю доступу та багато інших. Комбінація цих технологій допоможе забезпечити максимальний рівень безпеки конфіденційної інформації, що обробляється в системі електронного документообігу.

Проте важливо мати на увазі, що використання технологій само по собі не гарантує безпеку. Організації повинні розробити та впровадити політику та процедури забезпечення безпеки, які дозволять ефективно використовувати ці технології. Наприклад, важливо забезпечити належний контроль доступу до системи, здійснювати періодичну оцінку ризиків та проводити навчання персоналу з питань безпеки. Такі заходи допоможуть ефективно використовувати технології забезпечення безпеки та знизити ризик можливих загроз.

Список використаних джерел

1. Державне управління. Том 2: http:/e-pidruchniki.com/content/2157_164_Elektronnii_dokymentoobig_ta_zahist_informacii.html
2. Захист систем електронного документообігу: юридичні й технічні моменти https://www.kadrovik.ua/content/zahyst-system-elektronnogo-dokumentoobigu-yurydychni-j-tehnichni-momenty
3. «What is encryption?»: www.techtarget.com/searchsecurity/definition/encryption
4. Закон України Про електронні документи та електронний документообіг https://zakon.rada.gov.ua/laws/show/851-15#Text

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКО Б.Т.

АНАЛІТИЧНИЙ ОГЛЯД ІСНУЮЧИХ СИСТЕМ ПІДБОРУ СПІВРОБІТНИКІВ

ЖИЛА Я., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті проаналізовано сучасні системи підбору персоналу, зокрема онлайн-платформи, з технічної точки зору. Розглянуто ключові аспекти функціонування та переваги таких систем. Досліджено їх вплив на ефективність підбору кандидатів і взаємодію з роботодавцями. Основний висновок полягає в тому, що технологічні рішення у сфері підбору персоналу сприяють покращенню процесу та відкривають нові можливості для роботодавців та працівників.

The article analyzes modern personnel selection systems, particularly online platforms, from a technical perspective. Key aspects of their functioning and advantages are discussed. Their impact on the effectiveness of candidate selection and interaction with employers is examined. The main conclusion is that technological solutions in the field of personnel selection contribute to improving the process and open up new opportunities for employers and workers.

Актуальність. У сучасному світі, який характеризується стрімким розвитком технологій та постійною зміною ринку праці, актуальність теми підбору персоналу за допомогою сучасних систем та онлайн-платформ не викликає сумнівів. Ефективний підбір кадрів є ключовим фактором успіху для будь-якої організації, оскільки правильно підібрані співробітники забезпечують високу продуктивність, інноваційність та конкурентоспроможність підприємства.

Аналіз попередніх досліджень. Відомі українські та зарубіжні науковці, такі як Бондаренко В.В. [5], Демченко О.М .[6], Ковальчук Т.І [7]., та Cappelli P. [8], Keller J.R. [9], Pfeffer J [10], активно вивчають питання підбору персоналу та впровадження сучасних технологій у цей процес. У своїх роботах вони розглядають проблеми підбору та адаптації персоналу, а також досліджують можливості застосування сучасних технологій, таких як алгоритми машинного навчання та інтелектуальний аналіз даних для підбору співробітників.

Метою статті є аналітичний огляд існуючих систем підбору персоналу з акцентом на технічний аспект їх функціонування та вплив на ефективність процесу підбору.

Об'єктом даного дослідження є системи підбору персоналу, зокрема онлайн-платформи та інші технологічні інструменти, що використовуються для підбору співробітників.

Предметом дослідження є технічні аспекти функціонування систем підбору персоналу, а також їх вплив на ефективність процесу відбору кандидатів та взаємодію між роботодавцями та претендентами.

Завдання. Для досягнення поставленої мети, сформульовано такі завдання:

– виявити основні типи систем підбору персоналу та їх характеристики.

– проаналізувати технічні аспекти функціонування різних платформ підбору персоналу.

– визначити переваги та недоліки існуючих систем та оцінити їх вплив на ефективність підбору кандидатів.

– висвітлити можливості щодо вдосконалення систем підбору персоналу з урахуванням сучасних технологічних рішень.

Виклад основного матеріалу. В сучасному світі, де роль технологій у бізнесі набуває все більшого значення, успіх компанії в значній мірі залежить від якості її персоналу. Завдяки розвитку новітніх технологій та аналітичних методів, системи підбору персоналу стають все більш потужними інструментами для відбору талановитих фахівців та забезпечення

ефективності рекрутингових процесів. Враховуючи стрімкі зміни на ринку праці, постійне зростання кількості нових професій та вимог до навичок, важливо зрозуміти особливості та можливості сучасних систем підбору персоналу [1].

Системи підбору персоналу можуть бути класифіковані на кілька типів (Рис.1).

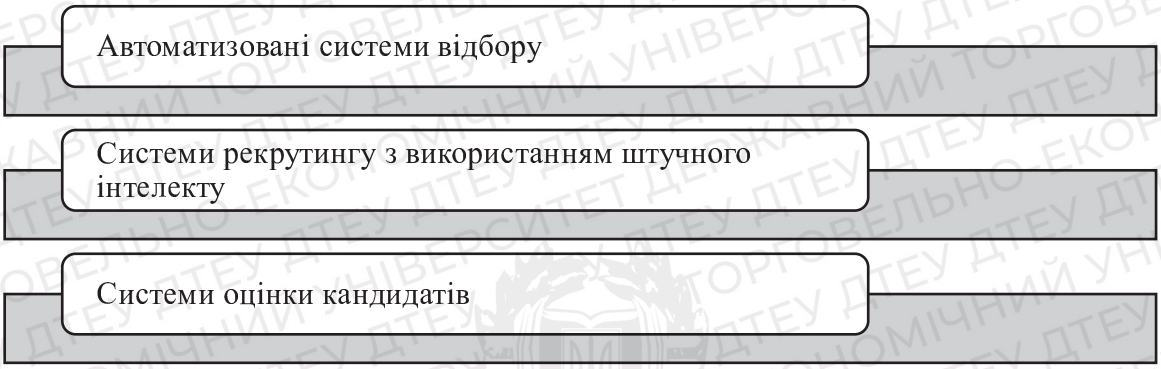


Рис. 1. Класифікація систем підбору персоналу

Автоматизовані системи відбору (Applicant Tracking Systems, ATS) – це програмні рішення, які допомагають автоматизувати процес відбору кандидатів, відслідковувати їх статус, аналізувати резюме та оцінювати їх відповідність вимогам посади. Приклади таких систем: Workday, Taleo, Greenhouse, Jobvite.

Автоматизовані системи відбору (ATS) стали неодмінним інструментом у сучасному світі рекрутингу, оскільки вони спрощують і прискорюють процес пошуку та найму кандидатів. Вони дають ряд переваг для роботодавців та рекрутерів, зокрема:

– Ефективність: ATS дозволяють автоматично відсіювати резюме, які не відповідають вимогам посади, що допомагає зменшити час, витрачений на ручну обробку резюме. Це дозволяє рекрутерам зосередитися на відібраних кандидатах, які мають найбільше шансів на успішне працевлаштування.

– Організація даних: ATS структурують і зберігають інформацію про кандидатів, створюючи єдину базу даних, яка може бути легко оновлена і аналізована. Це допомагає уникнути втрати важливої інформації та полегшує пошук потрібних даних.

– Забезпечення об'єктивності: Автоматизовані системи відбору використовують алгоритми для аналізу резюме та оцінки відповідності кандидатів вимогам посади. Це забезпечує більш об'єктивний та стандартизований підхід до відбору кандидатів, що зменшує вплив особистих уподобань рекрутера на процес.

– Звітність та аналітика: ATS можуть збирати дані про ефективність процесу відбору та найму, що допомагає рекрутерам і менеджерам визначати, які методи працюють найкраще, та виявляти можливі проблеми. Це може сприяти постійному вдосконаленню процесів найму та відбору.

Системи рекрутингу з використанням штучного інтелекту (AI Recruiting) – ці системи здійснюють відбір кандидатів на основі аналізу великих масивів даних та алгоритмів машинного навчання. Вони можуть оцінювати кандидатів на основі їх досвіду, навичок, особистісних рис, а також прогнозувати їх успішність на певній посаді. Приклади таких систем: Pymetrics, HireVue, XOR, Ideal.

Системи рекрутингу з використанням штучного інтелекту (AI Recruiting) стали новим поколінням інструментів у сфері найму та відбору кандидатів, пропонуючи ряд переваг порівняно з традиційними методами:

– Більш точна оцінка: AI Recruiting аналізує великі масиви даних та використовує алгоритми машинного навчання для виявлення закономірностей і візерунків, які можуть вказувати на успішність кандидатів на певній посаді. Це дозволяє рекрутерам краще визначити

потенціал кандидата на основі набору різноманітних факторів, таких як досвід, навички, особистісні риси та інше.

– Швидкість та ефективність: AI Recruiting може автоматично оцінювати кандидатів та прискорювати процес відбору, зменшуючи час, потрібний для ручного аналізу та оцінки резюме. Це допомагає рекрутерам ефективніше витрачати свій час та ресурси на кандидатів з найбільшим потенціалом.

– Зменшення упередженості: Використання алгоритмів машинного навчання може допомогти зменшити вплив людської упередженості на процес відбору, оскільки AI Recruiting здійснює оцінку на основі об'єктивних критеріїв, відображених у великих масивах даних.

– Краще зрозуміння кандидатів: AI Recruiting може аналізувати значно більше даних про кандидатів, ніж традиційні методи, що дозволяє рекрутерам глибше оцінити кандидатів та краще розуміти, як вони можуть вписатися в компанію та виконувати свої обов'язки.

Системи оцінки кандидатів (Assessment Systems) – ці системи можуть включати в себе психометричні тести, віртуальні співбесіди, відеоінтерв'ю та інші інструменти для оцінки кандидатів за різними параметрами. Приклади таких систем: SHL, Criteria Corp, Plum, HackerRank.

Системи оцінки кандидатів (Assessment Systems) є сучасними та ефективними інструментами, які використовуються в процесі рекрутингу для отримання додаткової інформації про кандидатів та їх потенціал. Вони пропонують ряд переваг, таких як:

– Більш об'єктивна оцінка: Використання різноманітних інструментів оцінки, таких як психометричні тести та відеоінтерв'ю, дозволяє рекрутерам краще розуміти здібності, навички та особистісні риси кандидатів. Це сприяє більш об'єктивному підходу до відбору та найму персоналу.

– Ефективність: Системи оцінки кандидатів дозволяють проводити оцінку одночасно для великої кількості кандидатів, що значно зменшує час, потрібний для відбору та найму. Вони також допомагають автоматизувати процес оцінки, полегшуючи роботу рекрутерів.

– Забезпечення порівнянності: Різні інструменти оцінки забезпечують стандартизовані результати, які можуть бути легко порівняні між кандидатами. Це допомагає рекрутерам приймати обґрунтовані рішення щодо відбору.

– Краще зрозуміння потреб компанії: Використання систем оцінки кандидатів допомагає рекрутерам краще зрозуміти, які кандидати можуть вписатися в культуру компанії та які з них найбільше відповідають вимогам посади. Це дозволяє компанії забезпечити підбір персоналу, який максимально відповідає її потребам.

На основі аналізу наведених прикладів систем можна виділити наступні технічні аспекти функціонування платформ підбору персоналу [2]:

1. Інтерфейси користувача: Веб-інтерфейси, мобільні додатки, віджети для інтеграції з іншими системами.
2. Бази даних: Системи підбору персоналу використовують реляційні або NoSQL бази даних для зберігання інформації про кандидатів, вакансії та інші деталі. Це дозволяє забезпечити швидкий доступ до даних та гнучкість у керуванні структурою даних.
3. Модулі аналітики: Використання алгоритмів машинного навчання, статистичного аналізу, текстової аналітики та інших методів для аналізу даних та оцінки кандидатів.
4. Інтеграція з іншими системами: Системи підбору персоналу часто інтегруються з системами управління персоналом (HRIS), системами електронної пошти, соціальними мережами та іншими інструментами для спрощення процесів рекрутингу та комунікації з кандидатами.

Технологічна сторона таких систем має значний вплив на їх можливості та ефективність у підборі кандидатів. Основоположним є вибір адекватних технічних рішень для специфічних потреб компанії та галузі, в якій вона працює.

Враховуючи значення технічних аспектів, необхідно також оцінити переваги та недоліки існуючих систем підбору персоналу. Переваги та недоліки існуючих систем та оцінки їх впливу на ефективність підбору кандидатів розглянемо в таблиці 1.

Таблиця 1

Переваги та недоліки існуючих систем

Переваги	**Недоліки**
Швидкість обробки даних та відбору кандидатів	Можливість помилок через неправильну інтерпретацію даних
Зменшення впливу людського фактора та упереджень	Відсутність емпатії та глибокого розуміння особистості кандидата
Автоматизація рутинних задач та зниження навантаження на рекрутерів	Витрати на впровадження та підтримку системи
Можливість аналізу великих масивів даних	Обмеження у зв'язку з відсутністю даних про нові навички та технології

За результатом таблиці, можно зробити висновок, існують як позитивні сторони, так і обмеження використання цих систем. З одного боку, системи підбору персоналу сприяють швидкості, автоматизації та аналізу великих масивів даних; з іншого - можуть приводити до помилок у відборі та обмежень, пов'язаних з відсутністю даних про нові навички та технології [3].

Враховуючи ці результати, розглянемо можливості щодо вдосконалення систем підбору персоналу з урахуванням сучасних технологічних рішень. Це допоможе визначити напрямки розвитку та впровадження новітніх технологій, які можуть підвищити ефективність підбору кандидатів та забезпечити компаніям конкурентні переваги на ринку праці.

Напрямки вдосконалення систем підбору персоналу [4]:

1. Глибше використання алгоритмів машинного навчання та штучного інтелекту для аналізу даних про кандидатів, що дозволить точніше прогнозувати успішність кандидата на певній посаді.
2. Використання технологій Big Data для збору та аналізу великих масивів даних про ринок праці, нові навички та технології, а також тренди у сфері рекрутингу.
3. Розвиток інтеграції з іншими системами та сервісами, які можуть покращити ефективність підбору кандидатів, такими як системи управління персоналом, соціальні мережі, професійні спільноти, системи онлайн-навчання та інше.
4. Розробка більш інтуїтивних та зручних інтерфейсів користувача, що сприятимуть швидкому та ефективному використанню системи рекрутерами та кандидатами.
5. Застосування етичних підходів у використанні технологій аналітики та штучного інтелекту для підбору персоналу, що допоможе уникнути дискримінації та порушення приватності кандидатів.

В цілому, сучасні системи підбору персоналу вже надають значні переваги для роботодавців та кандидатів, автоматизуючи рутинні задачі та впроваджуючи новітні технології аналітики. Однак, є ще багато можливостей для вдосконалення цих систем, які можуть значно покращити ефективність підбору кандидатів та сприяти створенню більш продуктивних та успішних команд.

Висновки. У даній статті ми розглянули основні типи систем підбору персоналу та їх характеристики. Виявлено, що сучасні системи можуть бути класифіковані за різними критеріями, такими як рівень автоматизації, використання алгоритмів машинного навчання та штучного інтелекту, а також залежно від сфери застосування. Вивчення цих типів систем допомагає роботодавцям та кандидатам зрозуміти, які методи найбільш ефективні для їх потреб.

Було проаналізовано технічні аспекти функціонування різних платформ підбору персоналу. Особливу увагу було приділено архітектурі систем, базам даних, модулям аналітики та інтеграції з іншими системами. Усвідомлення технічних особливостей дозволяє компаніям краще адаптуватися до сучасних технологій та вибрати найбільш підходящі системи для своїх потреб.

Розглянуто основні переваги та недоліки існуючих систем підбору персоналу та їх вплив на ефективність підбору кандидатів. Було виявлено, що сучасні системи пропонують ряд переваг, таких як швидкість, автоматизація та аналіз великих масивів даних. Проте, існують і обмеження, такі як можливість помилок у відборі та відсутність даних про нові навички та технології.

У підсумку, дана стаття пропонує комплексний аналіз різних систем підбору персоналу та розкриває їх основні характеристики, технічні аспекти, переваги та недоліки. Оцінка існуючих систем та їх потенційного вдосконалення дозволяє роботодавцям раціонально вибирати та інтегрувати найбільш ефективні технологічні рішення для підбору та управління персоналом.

Список використаних джерел

1. Коваленко, В. М. Сучасні системи підбору персоналу: теоретичні аспекти та класифікація / В. М. Коваленко // Управління персоналом. – 2019. – № 2. – С. 20–28.
2. Мельник, Л. Г. Технічні аспекти функціонування різних платформ підбору персоналу / Л. Г. Мельник // Інформаційні технології в управлінні персоналом. – 2020. – № 4. – С. 35–43.
3. Гончаренко, І. В. Аналіз переваг та недоліків існуючих систем підбору персоналу / І. В. Гончаренко // Вісник соціально-економічних досліджень. – 2018. – № 3. – С. 50–58.
4. Білоус, О. В. Інноваційні технології в системах підбору персоналу / О. В. Білоус // Науковий вісник. – 2017. – № 1. – С. 115–120.
5. Бондаренко В.В. (2018). Сучасні підходи до підбору персоналу в організаціях. Вісник економіки та управління, № 1, с. 24-31.
6. Демченко О.М. (2019). Адаптація персоналу як складова стратегії управління персоналом підприємства. Економічний часопис-XXI, № 179, с. 35-39.
7. Ковальчук Т.І. (2020). Використання технологій машинного навчання в процесі підбору та адаптації персоналу. Наукові праці Донецького національного технічного університету. Серія: економічна, № 1, с. 123-130.
8. Cappelli P. (2015). Skill Gaps, Skill Shortages, and Skill Mismatches: Evidence and Arguments for the United States. ILR Review, 68(2), 251-290.
9. Keller J.R., & Cappelli P. (2014). An Assessment of the State of Human Resources Analytics: A Review and Research Agenda. Journal of Organizational Effectiveness: People and Performance, 1(3), 219-233.
10. Pfeffer J., & Sutton R.I. (2016). Hard Facts, Dangerous Half-Truths, and Total Nonsense: Profiting from Evidence-Based Management. Harvard Business Review Press.

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н.О.

КЛАСИФІКАЦІЯ ЗАГРОЗ ДЛЯ WEB-САЙТІВ ТА СПОСОБИ ЇХ ВИРІШЕННЯ

ЖМЕНЯ Є., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті описані основні види загроз для web-сайтів: шкідливе програмне забезпечення, крадіжка пароля, перехоплення трафіку, фішингова атака, DDoS атака, міжсайтова атака, експлойти нульового дня, SQL ін'єкція, атака MITM, криптоджекінг, внутрішня загроза, ботнет, розширена постійна загроза, троянський вірус. Описані методи їх виявлення та способи їх вирішення.

The article describes the main types of threats to websites: malware, password theft, traffic interception, phishing attack, DDoS attack, cross-site attack, zero-day exploits, SQL injection, MITM attack, cryptojacking, insider threat, botnet, advanced persistent threat attack, Trojan virus. The methods of their detection and ways of solving them are described.

Актуальність. У сучасному світі одним із найважливіших напрямків інформаційної безпеки є захист веб-ресурсів. У зв'язку з широким розповсюдженням новітніх технологій та їх залежністю від інтернет-з'єднання зростає ринок зловмисного програмного забезпечення. З моменту створення Інтернету різноманітні загрози безпеці приходили та зникали. Їх серйозність коливається від незначних незручностей до руйнівних економічних наслідків. У зв'язку зі зростанням терористичних загроз, поширенням гібридних війн та пандемією, вразливість веб-ресурсів до атак отримала також політичний простір.

Отже, актуальною науковою проблемою залишається вдосконалення методів і систем захисту веб-ресурсів від атак, особливо з урахуванням їх постійного вдосконалення та збільшення інструментів атак. Формування повної класифікації загроз та способів їх вирішення є важливою практичною задачею внаслідок зростаючих політико-економічних та соціальних наслідків від зловмисних дій.

Метою статті є дослідження і розробка класифікації загроз для web-сайтів та формування способів їх вирішення з метою підвищення рівня оцінки захищеності web-ресурсів, за рахунок удосконалення методів та засобів виявлення потенційних загроз.

Об'єктом дослідження є потенційні загрози для web-сайтів та способи їх вирішення.

Предмет дослідження – найпоширеніші загрози для web-сайтів.

Аналіз попередніх досліджень. Досліджено статті про інформаційні технології, запобігання втраті даних, керування мережею та ERP Лінди Розензранце, дані сайту Executech – провайдера IT-послуг, кібербезпеки, хмарних сервісів та статистика Website Security Statistics Report

Виклад основного матеріалу. Загрози безпеці веб-сайтів – це кібератаки, спрямовані на вразливі місця в інфраструктурі та веб-додатках задля отримання доступу до цінних даних і облікових даних.

Кількість організацій, які застосовують веб-технології для підвищення продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. До таких організацій належать, як комерційні компанії різних форм власності, так і органи державної влади і місцевого самоуправління. Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз. Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері, або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Основною причиною більшості зламів у веб-додатках є написаний розробниками програмний код. Розробники можуть допускати помилки при написанні коду або не

усвідомлювати всю важливість використання прийомів безпечного програмування – все це призводить до появи вразливостей в додатках.

Для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (Framework), в якому вбудовані механізми перевірки, шифрування та валідації. Найкращим методом захисту від атак на мережеві служби, наприклад, DoS та DDoS є використання хмарних технологій і перевірених конфігурацій серверів.

Як свідчать статистичні результати [3] та запропоновані методи, які орієнтовані на захист від конкретного типу атаки, зловмисна дія на веб-ресурс відбувається, як правило, із використанням відразу декількох різних типів атак. Тому задачею системи менеджменту інформаційної безпеки є розробка ефективної стратегії протидії атакам зловмисників за умови, що вони використовують комбіновані типи атак. Розробка такої стратегії захисту веб-ресурсу є нетривіальною задачею.

У світі налічується дуже велика кількість загроз для web-сайтів і їх кількість постійно зростає. В статті виокремлено 15 найбільш поширених ризиків кібербезпеки та способи їх уникнення.

1 – Шкідливе програмне забезпечення.

Почнемо з найпоширенішої загрози безпеці: шкідливого програмного забезпечення. Ця форма загрози існує з моменту появи Інтернету та продовжує залишатися постійною проблемою. Зловмисне програмне забезпечення – це небажана частина програми або програмного забезпечення, що встановлюється в цільову систему, викликаючи незвичайну поведінку. Наслідки такого втручання в систему варіюються від заборони доступу до програм, видалення файлів, викрадення інформації до поширення на інші системи. Сюди можна віднести і такий підвид цієї атаки як шкідлива реклама. Цю техніку використовують кіберзлочинці для введення шкідливого коду в законні мережі онлайн-реклами та веб-сторінки. Цей код зазвичай перенаправляє користувачів на шкідливі веб-сайти або встановлює зловмисне програмне забезпечення на їхні комп'ютери чи мобільні пристрої. Комп'ютери користувачів можуть заразитися, навіть якщо вони не почали завантаження шкідливої програми. Кіберзлочинці можуть використовувати зловмисну рекламу для розгортання різноманітних зловмисних програм, які заробляють гроші, зокрема сценаріїв для майнінгу криптовалют, програм-вимагачів і банківських троянів.

Деякі веб-сайти відомих компаній, зокрема Spotify, The New York Times і Лондонська фондова біржа, ненавмисно показували шкідливу рекламу, піддаючи користувачів ризику [1].

Профілактика:

- По-перше, користувачі та організації повинні мати найновіші програми захисту від шкідливих програм. Також важливо розпізнавати підозрілі посилання, файли або веб-сайти, які є ефективними способами впровадження зловмисного програмного забезпечення. Часто поєднання обережності та антивірусу достатньо, щоб запобігти більшості проблем зі зловмисним програмним забезпеченням.
- Щоб запобігти зловмисній рекламі, рекламні мережі повинні додати перевірку. Це зменшує ймовірність того, що користувач може бути скомпрометований. Перевірка може включати: перевірку потенційних клієнтів шляхом вимагання юридичних документів для бізнесу, двофакторна аутентифікація, сканування потенційних оголошень на наявність шкідливого вмісту перед публікацією оголошення, перетворення Flash-оголошень на анімовані gif-файли чи інший тип вмісту.
- Задля пом'якшення атаки зловмисної реклами, веб-хостинги повинні періодично перевіряти свої веб-сайти з невиправленої системи та контролювати цю систему, щоб виявити будь-яку зловмисну активність. Веб-хостингу слід вимкнути будь-яку шкідливу рекламу.

- Щоб зменшити ризик атак зловмисної реклами, команди корпоративної безпеки повинні постійно оновлювати програмне забезпечення та виправлення, а також встановлювати мережеві засоби захисту від зловмисного програмного забезпечення.

2 – Password attacks.

Крадіжка пароля – це метод, який використовують хакери для зловмисної автентифікації та викрадення даних. Як правило, ці атаки здійснюються шляхом використання вразливостей у системі та використання програмного забезпечення для прискорення процесу злому паролів.

Запобігання:

- Є кілька причин втрати пароля. Зловмисники можуть вгадати пароль або використати програми «грубої сили», щоб виконати тисячі потенційних спроб. Вони також можуть викрасти його з небезпечного місця або використовувати соціальну інженерію, щоб обманом змусити користувача віддати його. Двофакторна автентифікація є надійним методом захисту, оскільки для завершення входу потрібен додатковий пристрій. Крім того, використання складних логінів запобігає спробам грубої сили [2].

3 – Перехоплення трафіку.

Також відоме як «прослуховування», перехоплення трафіку відбувається, коли третя сторона «прослуховує» інформацію, що надсилається між користувачем і хостом. Тип викраденої інформації залежить від трафіку, але часто використовується для входу в обліковий запис або цінних даних.

Запобігання:

- Уникнення скомпрометованих веб-сайтів (наприклад, тих, які не використовують HTML5) є чудовим проактивним захистом.
- Шифрування мережевого трафіку, наприклад через VPN, є ще одним профілактичним методом.

4 – Фішингові атаки.

Фішингові атаки – це тип загроз інформаційній безпеці, який використовує соціальну інженерію, щоб обманом змусити користувачів порушити звичайні методи безпеки та надати конфіденційну інформацію, зокрема імена, адреси, облікові дані для входу, номери соціального страхування, дані кредитних карток та іншу фінансову інформацію.

У більшості випадків хакери надсилають підроблені електронні листи, які виглядають так, ніби вони надходять із законних джерел, таких як фінансові установи, eBay, PayPal, і навіть друзів і колег [1].

Під час фішингових атак хакери намагаються змусити користувачів виконати певні рекомендовані дії, наприклад натиснути посилання в електронних листах, які спрямовують їх на шахрайські веб-сайти, що запитують особисту інформацію або встановлюють шкідливе програмне забезпечення на їхні пристрої. Відкриття вкладень у електронних листах також може встановлювати на пристрої користувачів зловмисне програмне забезпечення, призначене для збору конфіденційної інформації, надсилання електронних листів їхнім контактам або надання віддаленого доступу до їхніх пристроїв.

Як запобігти фішинговим атакам:

- Ефективні засоби захисту електронної пошти можуть допомогти зменшити ймовірність отримання таких електронних листів, але вони не є ефективними на 100%. Тому навчання користувачів бути обережними та виявляти ознаки спроби фішингу є найкращим способом боротьби з цією загрозою.

5 – DDoS атака.

У розподіленій атаці типу «відмова в обслуговуванні» (DDoS) кілька скомпрометованих машин атакують ціль, наприклад сервер, веб-сайт або інший мережевий

ресурс, що робить ціль повністю непрацездатною. Потік запитів на з'єднання, вхідних повідомлень або неправильно сформованих пакетів змушує цільову систему сповільнюватися або виходити з ладу та вимикатися, відмовляючи в обслуговуванні законним користувачам або системам.

Щоб запобігти DDoS-атакам, компаніям слід вжити таких заходів:

- Впровадити технологію та інструменти для візуального моніторингу мереж і знати, яку пропускну здатність у середньому використовує сайт. DDoS-атаки пропонують візуальні підказки, тож адміністратори, які розуміють нормальну поведінку своїх мереж, зможуть краще відловлювати ці атаки.
- Переконатися, що сервери мають здатність обробляти інтенсивні стрибки трафіку та необхідні інструменти пом'якшення, необхідні для вирішення проблем безпеки.
- Своєчасно оновлювати та виправляти брандмауери та програми безпеки мережі.
- Налаштувати протоколи, що описують кроки, які необхідно виконати у разі виникнення DDoS-атаки.

6 – Міжсайтова атака.

Цей вид називається XSS-атакою. У цьому випадку третя сторона націлиться на вразливий веб-сайт, зазвичай без шифрування. Далі небезпечний код завантажується на сайт. Коли звичайний користувач отримує доступ до зазначеного веб-сайту, цей код доставляється або в його систему, або в браузер, викликаючи небажану поведінку. Мета полягає в тому, щоб порушити стандартні послуги або викрасти інформацію користувача.

Запобігання:

- На стороні хоста потрібно встановити шифрування. Крім того, надання можливості вимкнення сценаріїв сторінок є важливим для запобігання активації зловмисного завантаження.
- Користувачі також можуть установити додатки для блокування сценаріїв у свій браузер, якщо вони віддають перевагу додатковому контролю перегляду.

7 – Експлойти нульового дня.

Експлойт, що виникає після виявлення «вразливості нульового дня», є цілеспрямованою атакою на систему, мережу або програмне забезпечення. Ця атака використовує проблему безпеки, яку не помічають, намагаючись спричинити незвичну поведінку, пошкодити дані та викрасти інформацію.

Запобігання:

- Зупинити експлойти складно, оскільки це залежить від того чи виявить постачальник проблему та запустить програму її виправлення. У деяких випадках уразливість нульового дня може існувати протягом тривалого періоду, перш ніж її виявлять.

8 – SQL ін'єкція.

Structured Query Language або SQL-атака – маніпулювання даними, реалізоване для доступу до інформації, яка не повинна бути доступною. По суті, зловмисники маніпулюють «запитами» SQL (типовий рядок запиту коду, який надсилається до служби або сервера), щоб отримати конфіденційну інформацію.

Запобігання:

- Впровадження розумних брандмауерів є одним із методів запобігання втручанню, брандмауери програм можуть виявляти та фільтрувати небажані запити.
- Найефективнішим способом – є розробка коду, який ідентифікує незаконні введення користувачами.

9 – Атака MITM.

Атака Man-in-the-Middle («людина посередині») відбувається, коли третя сторона захоплює сеанс між клієнтом і хостом, коли відвідувач використовує незахищену публічну мережу Wi-Fi. Зазвичай хакер маскує себе за допомогою підробленої IP-адреси, відключає

клієнта та запитує інформацію від клієнта. Наприклад, спроба входу в банківський сеанс дозволить атаці MITM викрасти інформацію користувача, пов'язану з їхнім банківським рахунком.

Запобігання:

- Рекомендується шифрування та використання HTML5.

10 – Програми-вимагачі.

Програми-вимагачі встановлюються в систему або мережу користувача та блокують доступ до функціональних можливостей (частково чи повністю), доки третім особам не буде сплачено «викуп».

Запобігання:

- Видалити після встановлення складно. Оновлення антивірусної програми та уникнення шкідливих посилань є найкращими методами профілактики.
- Поточні резервні копії та реплікації є ключовими для того, щоб атаки програм-вимагачів не стали катастрофічними.

11 – Cryptojacking.

Криптоджекінг – це спроба встановити зловмисне програмне забезпечення, яке змушує інфіковану систему виконувати «криптомайнінг», популярну форму отримання криптовалюти. Цей, як і інші віруси, може вражати незахищені системи. Видобування криптовалюти, як правило, потребує надзвичайно високої активності процесора, що спричиняє негативний ефект, наприклад: зниження продуктивності пристроїв, збільшення споживання енергії, підозрілий мережевий трафік.

Запобігання:

- Щоб запобігти криптоджекінгу потрібно постійно оновлювати всі додатки та програмне забезпечення безпеки та переконатися, що мікропрограмне забезпечення на смарт-пристроях також використовує останню версію. Cryptojacking може заразити більшість незахищених систем [2].

12 – Внутрішні загрози.

Внутрішня загроза виникає, коли особи, близькі до організації, що мають дозвіл на доступ до її мережі, навмисно чи ненавмисно зловживають цим доступом, щоб негативно вплинути на критично важливі дані або системи організації.

Недбалі працівники, які не дотримуються бізнес-правил і політики своєї організації, спричиняють внутрішні загрози. Наприклад, вони можуть ненавмисно надсилати електронною поштою дані клієнтів стороннім особам, натискати фішингові посилання в електронних листах або ділитися своєю реєстраційною інформацією з іншими. Підрядники, ділові партнери та сторонні постачальники є джерелом інших внутрішніх загроз.

Деякі інсайдери навмисно обходять заходи безпеки через зручність або необдумані спроби підвищити продуктивність. Зловмисники навмисно ухиляються від протоколів кібербезпеки, щоб видалити дані, викрасти дані для подальшого продажу чи використання, порушити роботу чи іншим чином завдати шкоди бізнесу.

Перелік речей, які організації можуть зробити, щоб мінімізувати ризики, пов'язані з внутрішніми загрозами, включає наступне:

- Обмежити доступ співробітників лише до певних ресурсів.
- Навчити нових співробітників і підрядників знанням безпеки, перш ніж дозволити їм доступ до мережі. Включити інформацію про ненавмисні та зловмисні внутрішні загрози в регулярні тренінги з безпеки.
- Створити для підрядників та інших фрілансерів тимчасові облікові записи, термін дії яких закінчується в певні дати, наприклад, дати закінчення їхніх контрактів.
- Реалізувати двофакторну автентифікацію, яка вимагає від кожного користувача надання другої ідентифікаційної інформації на додаток до пароля.

- Встановити програмне забезпечення для моніторингу співробітників, щоб зменшити ризик витоку даних і викрадення інтелектуальної власності шляхом виявлення необережних, незадоволених або зловмисних інсайдерів.

13 – Ботнети.

Ботнет – це набір пристроїв, підключених до Інтернету, включаючи ПК, мобільні пристрої та сервери, які заражені та дистанційно керовані звичайним типом зловмисного програмного забезпечення. Як правило, зловмисне програмне забезпечення ботнету шукає вразливі пристрої в Інтернеті. Метою зловмисника, який створює ботнет, є зараження якомога більшої кількості підключених пристроїв, використовуючи обчислювальну потужність і ресурси цих пристроїв для автоматизованих завдань, які зазвичай залишаються прихованими для користувачів пристроїв. Зловмисники, часто кіберзлочинці, які контролюють ці бот-мережі, використовують їх для надсилання спаму електронною поштою, участі в кампаніях шахрайства з кліками та створення зловмисного трафіку для розподілених атак на відмову в обслуговуванні.

Організації мають кілька способів запобігти зараженню ботнетами:

- Відстежувати продуктивність і активність мережі, щоб виявити будь-яку нерегулярну поведінку мережі.
- Тримати операційну систему в актуальному стані.
- Підтримувати все програмне забезпечення в актуальному стані та встановлювати всі необхідні патчі безпеки.
- Навчати користувачів не брати участь у будь-якій діяльності, яка створює для них ризик зараження ботами чи іншим зловмисним програмним забезпеченням, зокрема відкривати електронні листи чи повідомлення, завантажувати вкладені файли чи натискати посилання з незнайомих джерел.
- Впроваджувати антиботнет-інструменти, які знаходять і блокують віруси-ботів. Крім того, більшість брандмауерів і антивірусного програмного забезпечення містять базові інструменти для виявлення, запобігання та видалення ботнетів [1].

14 – Advanced persistent threat attacks.

Розширена постійна загроза (APT) – це цілеспрямована кібератака, під час якої неавторизований зловмисник проникає в мережу та залишається непоміченим протягом тривалого періоду часу. Замість того, щоб завдати шкоди системі чи мережі, ціллю APT-атаки є моніторинг мережевої активності та викрадення інформації для отримання доступу, включаючи набори експлойтів і зловмисне програмне забезпечення. Кіберзлочинці зазвичай використовують APT-атаки, щоб націлитися на цільові цілі, такі як великі підприємства та національні держави, крадучи дані протягом тривалого періоду.

Виявлення аномалій у вихідних даних може бути найкращим способом для системних адміністраторів визначити, чи їхні мережі були ціллю.

Показники APT включають наступне:

- Широке використання зловмисного програмного забезпечення троянського програмного забезпечення, що дозволяє APT підтримувати доступ.
- Дивна діяльність бази даних, наприклад раптове збільшення операцій бази даних, що включають величезні обсяги даних.
- Наявність незвичайних файлів даних, що, можливо, вказує на те, що дані були зібрані у файли для допомоги в процесі вилучення.
- Для боротьби з цим типом загроз інформаційній безпеці організація також повинна розгорнути програмне забезпечення, апаратне забезпечення або хмарний брандмауер для захисту від атак APT. Організації також можуть використовувати брандмауер веб-додатків для виявлення та запобігання атакам, що надходять із веб-додатків, перевіряючи трафік HTTP.

15 – Троянський вірус.

Зловмисне троянське програмне забезпечення намагається завантажити свої файли, маскуючись під законне програмне забезпечення. Одним із використаних методів було «сповіщення» про те, що систему користувача скомпрометовано зловмисним програмним забезпеченням, із рекомендацією сканування, за допомогою якого сканування фактично доставляло шкідливе програмне забезпечення. На сьогоднішній день троянський вірус є найпоширенішою категорією шкідливих програм, яку використовують для відкриття бекдорів, контролю інфікованого пристрою, видалення даних користувача та передачі їх зловмисникам, завантаження та запуску інших шкідливих програм у певній системі та інших цілей.

Запобігання:

- Уникати завантаження програм або файлів від невідомих постачальників або тих, які намагаються попередити користувача про серйозну проблему.
- Для зменшення кількості вразливостей користувачам рекомендується регулярно встановлювати оновлення та виправлення не лише для операційної системи, а для всього програмного забезпечення.

Висновки. В статті було проаналізовано існуючі та запропоновано власну класифікацію найпоширеніших загроз для web-сайтів та сформульовано способи їх вирішення. Підприємствам необхідно вжити багато кроків, щоб забезпечити належну IT-безпеку та ефективний захист різних аспектів цифрової інфраструктури. Сьогодні IT-фахівці застосовують цілісний підхід до кібербезпеки, гарантуючи, що їхні компанії захищені на всіх рівнях, щоб виявляти та пом'якшувати загрози до їх виникнення. Підсумувавши все вищесказане, можна виділити основне програмне забезпечення, необхідне для кібербезпеки:

- Рішення для моніторингу безпеки мережі: створені для виявлення та аналізу потенційно зловмисної активності у вашій мережі.
- Інструменти шифрування: шифрує дані та файли для захисту конфіденційної інформації.
- Антивірусне програмне забезпечення: запобігає, виявляє та видаляє зловмисне програмне забезпечення з пристроїв користувачів.
- Програмне забезпечення брандмауера: відстежує та фільтрує трафік в мережі.
- Інструменти тестування на проникнення: використовуються для оцінки безпеки мережі та виявлення будь-яких вразливостей.
- Інструменти сканування веб-вразливостей: автоматизовані інструменти, розроблені для сканування та виявлення загроз безпеки в програмах веб-сайтів.

Список використаних джерел

1. Матеріали сайту Techtarget. – URL: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams
2. Матеріали сайту Executech – провайдера IT-послуг, кібербезпеки, хмарних сервісів. – URL: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams
3. Website Security Statistics Report: 2015. – WhiteHat Security, 2015. – 30 p. – URL: https://info.whitehatsec.com/Website-StatsReport-2015.html

Робота виконана під науковим керівництвом к.т.н., доцента
САВЧЕНКО Т.В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ У ПРОВЕДЕННІ ТЕСТУВАНЬ ТА ОПИТУВАНЬ

ЗАГУРА О., 2мз курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади для проведення тестів та опитувань у закладах освіти. Зазначено переваги застосування програмних продуктів в університетах, коледжах тощо. Розглянуто як зразок інформаційно-управляючої системи Quizlet, Kahoot та Plickers.

The article discusses the basic principles for conducting tests and surveys in educational institutions. The advantages of using software products in universities, colleges, etc. are noted. Quizlet, Kahoot and Plickers are considered as an example of an information management system.

Актуальність. Найважливішим аспектом будь-якої освітньої діяльності є система контролю якості знань. Активне використання навчальними закладами засобів інформатизації забезпечило передумови до створення й використання автоматизованих тестів для контролю знань учнів (студентів) на всіх етапах навчання. Такі системи використовуються не тільки для визначення рівня підготовленості, але й для проведення моніторингу навчального процесу, для організації адаптивного навчання, дистанційного утворення. Актуальність тестового методу обумовлена його перевагами перед іншими педагогічними методами: наукова обґрунтованість тесту, що дає об'єктивну оцінку; технологічність тестових методів; точність визначень; наявність однакових вимог для всіх випробуваних; сумісність тестових технологій з іншими сучасними освітніми технологіями.

Метою статті є дослідження особливостей використання програмного забезпечення в закладах освіти для перевірки контролю знань.

Об'єктом дослідження є розробка програмного забезпечення для проведення тестів та опитувань в закладах освіти.

Предмет дослідження є програмне забезпечення.

Аналіз попередніх досліджень. Розглядаючи наявні програмні засоби для проведення тестового контролю, необхідно зазначити, що будь-який програмний засіб, що використовується у навчальному процесі, повинен відповідати загальним вимогам педагогічних програмних засобів, зокрема: інтерфейс програми повинен бути виконаний рідною мовою студента; програмне забезпечення повинно бути ліцензійним, тобто законно придбаним.

Виклад основного матеріалу. Контроль знань та вмінь учнів/студентів є важливим аспектом навчального процесу. Під час контролю реалізується «зворотній зв`язок», інформація, яка надходить від студента викладачу і характеризує процес навчання: досягнення студентів, труднощі на певному етапі опанування знань.

Контроль в загальному вигляді визначається як операція зіставлення запланованого результату з наявними вимогами та стандартами. Процес контролю можна представити у формулі (1):

$$\boldsymbol{K = B + B_M + O_W} \quad (1)$$

де: **K** – контроль, **B** – виявлення, $\boldsymbol{B_M}$ – вимірювання, $\boldsymbol{O_W}$- оцінювання.

Контроль складається з декількох етапів:

– розпізнавання та виявлення навчального матеріалу;

– вимірювання засвоєного навчального матеріалу: за рівнями засвоєння, за повнотою, за усвідомленням, тощо;

– оцінювання результатів учнів/студентів за визначеною школою.

Слово «тест» (англ. – test) означає іспит, проба. У педагогічних вимірювань тести використовують для діагностування різних сторін розвитку особистості учня/студента. Розрізняють:

- тести засвоювання знань та умінь (тести успішності);
- тести розумової обдарованості (тести інтелекту);
- тести інтересів;
- тести спеціальних здібностей;
- тести характерологічні (особистісні тести).
- тести визначення окремих психічних функцій (пам'яті, уваги та ін.)

При розробці тестів слід враховувати що є репродуктивне та продуктивне засвоювання. При *репродуктивному* учень/студент відтворює раніше засвоєну інформацію і застосовує її ж для виконання типових дій у майже незмінному вигляді. При *продуктивному* учень/студент не тільки використовує засвоєну інформацію, а також й перетворює її для використання в нетипових умовах [1].

Тест складається із завдання та еталону відповіді – зразка повного та правильного виконання дій.

Тест без еталону – це контрольне завдання. Оцінювання тесту без порівняння з еталоном перетворює об'єктивну процедуру контролю на суб'єктивну з усіма властивими для останньої недоліками.

Зіставлення відповіді учня з еталоном робить тестування якості знань об'єктивним.

За еталоном визначається кількість суттєвих операцій, необхідних для вирішення тесту. При тестуванні *операцією* називають нерозподілену дію учня, яку він виконує відповідно до завдання. *Суттєві операції* – це операції, що відображають засвоєння знань та умінь.

Порівняння відповіді учня з еталоном зі кількістю правильно виконаних завдань тесту дає можливість визначити *коефіцієнт засвоєння (2)*:

$$\boldsymbol{K\,\alpha = n/p} \qquad (2)$$

де **n** – кількість правильно виконаних завдань тесту, **p** – загальна кількість завдань у тесті.

За допомогою коефіцієнта засвоєння вимірюється кількість засвоєних знань.

Враховуючи специфіку тестового контролю, програмні засоби мають задовольняти такі вимоги: можливість використання кількох типів питань; можливість створення питань і відповідей, що можуть містити формули, малюнки, схеми; можливість вибору наступного питання випадковим чином з наявної сукупності тестових завдань; відображення варіантів відповідей у випадковому порядку для кожного тестуючого; збереження результатів тестування після завершення виконання тесту; збереження усіх відповідей для забезпечення зворотного зв'язку із тестуючим; можливість проведення аналізу тестових завдань, загалом усього тесту й аналізу відповідей кожного тестуючого зокрема; можливість експорту результатів тестування в інші програмні засоби для більш детального аналізу результатів тестування [2].

Як правило, сучасні системи комп'ютерного тестування складаються з кількох функціональних модулів, які можуть бути об'єднані в єдине ціле і інсталюватись на комп'ютери або існувати окремо у вигляді виконуваних файлів. Найчастіше до складу стандартної системи тестування входять:

- редактор тестів (модуль, призначений для створення тестів);
- модуль тестування;
- модуль для обробки результатів тестування;
- довідкова система;
- модуль, за допомогою якого можна здійснювати мережеве тестування.

Найбільш оптимально освітні можливості контролю здійснюють автоматизовані навчальні системи високого рівня, комп'ютерні освітні середовища, частиною яких є засоби діагностики та контролю знань. Для реалізації функцій, принципів, форм, видів та прийомів педагогічного контролю, проектування та програмування тестової програми-оболонки повинні базуватися на загальних педагогічних засадах розробки навчально-контролюючих програм. Програмний комплекс підтримки навчання та контролю повинен ґрунтуватися на двох, практично незалежних, програмних підсистем: проектування та інтерпретації. Проектувальник та інтерпретатор взаємодіють на основі низки архітектурних структур та бази навчальних елементів, схема якої моделюється відповідно до робочої програми автоматизованого курсу. Користувачем проектувальника вважається викладач, інтерпретатора – той що навчається.

В інструментальній системі має бути прийнятий підхід, що дозволяє викладачеві-проектувальнику уникнути «будь-якого програмування». Потрібні лише початкові навички роботи з комп'ютером та знання автоматизованої предметної галузі.

Інструментальна система для реалізації алгоритму має втілити обрану теоретичну концепцію, дизайн, навігацію, враховувати індивідуально-психологічні особливості учнів та вимоги ергономіки. Водночас вона має надавати досить широкий вибір методів та засобів аналізу відповідей, зручні та наочні еталони відповіді, потужну статистику, достатню для забезпечення коригування курсу.

Інструментальне середовище має бути спроможним адаптуватися до вимог автора, не бути «нав'язливою» і допускати реалізацію внутрішньо закладених методів тільки з дозволу автора-проектувальника. Основне завдання програмної реалізації проектування бачиться як найбільш адекватне відображення у навчальній програмі положень та методів, розроблених у сценарії.

При програмній реалізації доцільно використати метод діалогового автоматизованого проектування на основі набору спеціальних, що налаштовуються фрагментів-модулів. Він базується на конструюванні контролюючої програми з розроблених типових заготовок сценарію, здатних змінювати не лише своє змістовне наповнення, а й структуру.

Інструментальне середовище має підтримувати:

– мережеву технологію (стосовно локальної та глобальної мережі) з метою економії ресурсів та зручності формування статистики;

– технологію MultiMedia, що реалізує комбіноване застосування у тесті тексту, звуку, анімації, відео фрагментів тощо.

– створення продукту а) у режимі діалогу користувача з комп'ютером (с можливістю експортування завдань, структурно-логічної схеми, параметрів файлу ініціалізації в текстовий процесор та їх роздруківки), частина тестових завдань створюється автоматично, лише за вказівкою користувача, що призводить до економії часу, витраченого на створення тесту та/або б) формування вихідної інформації в текстовому файлі (як файлу завдань так і файлу ініціалізації, що задає параметри налаштування: кількість обраних завдань з бланку завдань, час тестування, кількість спроб відповіді, встановлення важливості завдання та ін.);

– створення довільної кількості тестових завдань (питань);

– створення довільної кількості елементів тестового завдання (відповідей);

– конструювання всіх основних чотирьох форм тестових завдань (закритої, відкритої, на відповідність та встановлення правильної послідовності), а також, можливості їх варіацій (наприклад, не два стовпці /списку, множини/ привести в відповідність, а матрицю; вписати не слово чи словосполучення у відкритій формі, а вільно конструйована відповідь до 1/3 сторінки тощо);

– виставлення оцінки за шкалою (абсолютною або відносною), визначеною розробниками тесту, як традиційної диференційованої (2-5 або 0-10), бінарної (залік/незалік), більш гнучкою (20, 100, 1000 бальної), і оцінки у відсотковому співвідношенні;

– встановлення вибору послідовності подачі завдань (за ступенем зростання проблеми, у випадковому порядку, у спеціальному порядку, у блоковому порядку, у порядку, що поєднує випадковий та спеціальний підбір);

– опціоне встановлення вибору кількості тестових завдань із загального бланку завдань;

– встановлення тимчасового відрізка, необхідного для проходження як тесту в цілому, так і кожного завдання зокрема;

– основні методи введення та аналізу відповіді:

1. Альтернативний. Постановка питання передбачає один із двох можливих відповідей: «ТАК» чи «НІ». Для організації аналізу відповіді.

2. Вибірковий. Видається питання та перелік можливих відповідей або тверджень, з яких потрібно вибрати правильний. В ідеалі зазначаються номери правильних відповідей.

3. Переставний. Видається питання та перелік дій чи тверджень. Необхідно впорядкувати їх у певній послідовності за допомогою номерів тверджень (в еталоні вказується необхідна послідовність).

4. Класифікаційний. У питаннях цього типу перевіряється, чи може студент/учень встановити відповідність між об'єктами та їх властивостями. З цією метою видається перелік об'єктів та перелік їх властивостей, а в еталоні відповіді задається список пар (об'єкт-властивість), зафіксованих під номером об'єкта. Потрібно вказати кожному з об'єктів його властивості.

5. Інжекторний. На екран видається завдання з пропущеними символами або словами. Місця перепусток позначаються деяким обумовленим способом, наприклад, символом підкреслення, а еталоні вказуються ключові слова, розставлені у потрібній послідовності. Керуючи курсором, необхідно заповнити перепустки. Інжекторний метод аналізу призначений для тестових завдань відкритої форми.

Отже, можливі наступні три режими проектування тесту:

1. Коли розробник повністю покладається на керуючу програму (формується так званий сценарій «за умовчанням», зрозуміло, за наявності наповненої змістовними навчальними елементами бази даних). Тут достатньо лише вказати тему, обрану для контролю.

2. Для переходу в другий режим достатньо виявити деяку «керуючу ініціативу», наприклад, звернутися до опцій меню інтерфейсу системи, що проектує. У цьому випадку викладачеві передається ініціатива управління. Він може керувати значеннями параметрів, послідовністю видачі тем, формуванням кадрів та інших атрибути сценарію. Тут необхідно мати деякий досвід роботи з проектувальником та знанням його архітектури.

3. Третій режим проектування призначений для досвідчених розробників сценарію. Він дає викладачеві повний контроль над створюваним середовищем. Можна змінити настройки навчання, вид майбутнього додатка, задати іншу форму, розмальовку, розташування тих чи інших полів введення, керуючих панелей і т. п., формуючи, таким чином, свій власний дизайн та структуру майбутнього навчально-контролюючого продукту.

Окремо слід зупинитися на такій групі параметрів, як комфортність роботи, яка характеризується наявністю невербальної підтримки, можливістю впровадження об'єктів мультимедіа (використання відео/аудіо об'єктів робить навчання (режим «тренінг») більш наочним і дозволяє забезпечити справжню інтерактивність, а також занурення що навчається у пізнавальний процес за рахунок активного включення різних каналів сприйняття інформації), візуалізацією роботи (як поточної, так і підсумкової) та ін.

Розглянемо на прикладі дві системи комп'ютерного тестування, які широко використовуються сьогодні в навчальному процесі – Quizlet, Kahoot та Plickers.

У монологічною формою навчання платформа Quizlet може застосовуватися для вивчення різних предметів і оцінки рівня знань студентів. Перед тим як користуватися Quizlet, викладач на сторінці онлайн-проекту вибирає з власних карт або розроблених іншими розробниками необхідний навчальний матеріал. Можна скопіювати набір карток в свій обліковий запис, а потім відредагувати і адаптувати їх до поточної теми занять або створювати

їх з нуля і ділитися з іншими. Програма має функцію озвучення, доступну для серії карт флеш-пам'яті, і завантаження набору карток з документа Word.

Існують декілька способів вивчення інформації: віртуальні картки, введення відповідей на письмові або звукові підказки. Користуючись панеллю запитань обираємо питання з однією відповіддю, з багатьма відповідями, текстового, описового характеру та на встановлення відповідності. Тест дозволяє вставляти картинки, відео та створювати по ним відповідні питання. Можна сказати що програма Quizlet має досить широкий функціонал, але і має певні недоліки, які ускладнюють створення тесту для визначення точного рівня знань тестуючих [3].

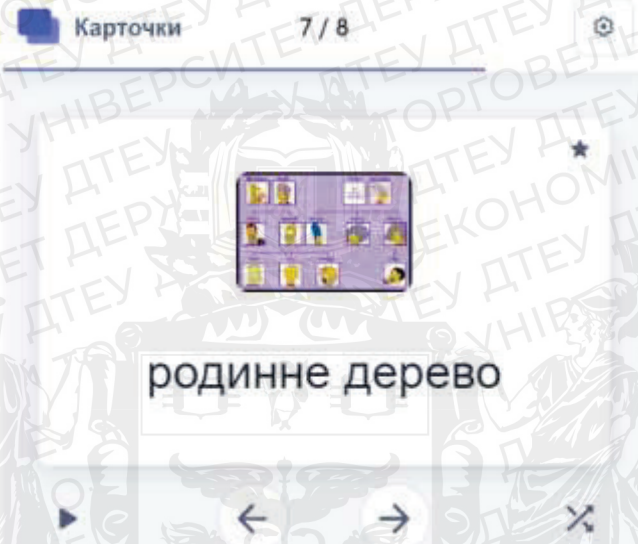


Рис. 1. Приклад тесту в програмі Quizlet

Kahoot! - онлайн сервіс для створення інтерактивних завдань. Дозволяє створювати тести, опитування, вікторини. Платформу можна використовувати під час роботи з будь-якими віковими категоріями. В даній програмі є всього два вида теста:

- Квіз (Quiz). Для кожного питання 4 варіанти відповіді, одна з яких правильна.
- Тест (True or False). До кожного питання 2 варіанти відповіді, правильна одна.

Також уже великим мінусом є те, що Kahoot! не підтримує українську мову, тому всі кнопки, елементи та новини англійською. Для створення нового тесту Kahoot! краще одразу продумати структуру та відповіді. Для тестів можна використовувати фото та відео, у питаннях писати формули. Самі питання та відповіді Kahoot! можна писати будь-якою мовою. Вікно конструктора, у якому створюються тести Kahoot!, має декілька головних частин:

1. Поле для введення тексту запитання або опису завдання
2. Поле, куди можна додавати фото чи відео
3. Поле, де можна виставити таймер для відповіді на одне запитання (Time limit) та кількість балів, які отримує учасник за кожну правильну відповідь
4. Поля для створення варіантів відповідей
5. Поле, де відображаються вже створені питання. За допомогою кнопки "Add question" додаються нові запитання.
6. Поле для введення назви нового кахуту та опису тесту.
7. "Preview" - попередній перегляд створеного тесту [4].

Сервіс Plickers дозволяє проводити мобільні голосування і фронтальні опитування під час навчального заняття з вивченого або поточного матеріалу в тестовій формі. Робота з мобільним додатком забирає не більше кількох хвилин. Отримання результатів опитування відбувається на занятті без тривалої перевірки та миттєво виводиться на екран комп'ютера (телевізора, проектора), під'єднаного до Інтернету. Наявність смартфонів або комп'ютерів не потрібна: тільки смартфон учителя з доступом до Інтернету.

Для користування електронним ресурсом потрібно зареєструватися. Ресурс англомовний, але якщо, наприклад, користуватися опцією браузера **Google Chrome**, то з'являється можливість автоматичного перекладу.

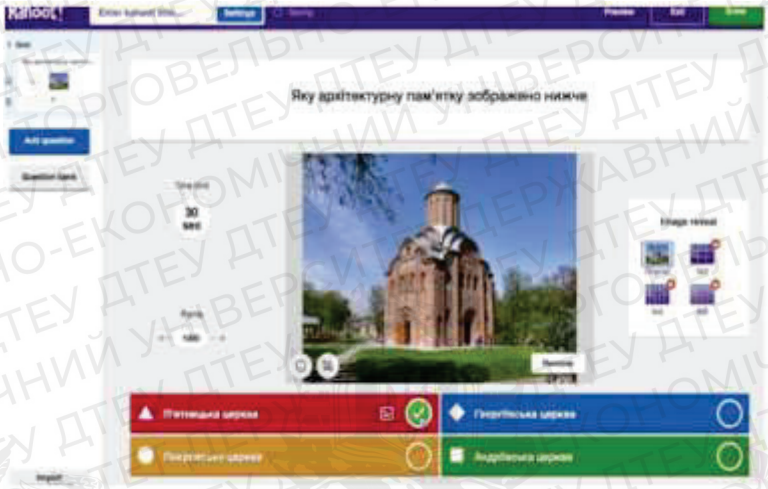


Рис. 2. Приклад тесту в програмі Kahoot!

Роздрукувати картки з QR-кодом. Для безкоштовного скачування з офіційного сайту є 5 наборів карток:

- Standard (стандартний з 40 карток), на одному аркуші А4 по 2 картки.
- Expanded (розширений з 63 карток), на одному аркуші А4 по 2 картки.
- Large Font (великий шрифт варіантів відповідей A, B, C, D) для маленьких дітей.
- Large Cards (40 великих карток), на одному аркуші А4 по 1 картці.
- Large Cards Expanded (розширений набір з 63 великих карток).

Один комплект карток можна використовувати для різних класів. У кожному класі номер картки буде відповідати окремому учню (згідно зі списком). Для тривалого використання їх можна роздрукувати на білому картоні.

Створити тестові завдання. Для полегшення пошуку необхідних тестів можна створити папки з предметів та зробити в них папки за темами. Можливі два варіанти тестів:

- з чотирма варіантами відповідей
- опитування ТАК/НІ. Є варіант множинних правильних відповідей.

Щоб скласти питання тесту, потрібно натиснути кнопку **New Question** (Нове питання). Форма питання містить поле для тексту, поля для чотирьох варіантів відповіді. Правильна відповідь або відповіді відзначено галочкою. До питання можна додати зображення.

Створити облікові записи учнів — «класи». Необхідно ввести назву класу, можна вибирати рік навчання і навчальний предмет. Кожен клас можна позначити певним кольором. Після заповнення форми потрібно натиснути кнопку **Save** (Зберегти).

Номер картки відповідатиме номеру учня в класі.

Список учнів можна скопіювати та вставити в поле, натиснувши кнопку **Add Roster** (Додати реєстр). Кожне нове прізвище слід починати з нового рядка.

Після того як класи сформовані та підготовлені питання тесту, потрібно створити чергу (послідовність питань, які ставлять обраному класу) для кожного класу. Одне і те саме питання можна використовувати кілька разів. Вже поставлене і видалене з черги питання можна знову додати в чергу.

На уроці відкрити програму на комп'ютері. Відкрити пряму трансляцію Live view. Це режим показу питань у реальному часі для синхронізації роботи смартфона (планшета) і комп'ютера, яким можна керувати з мобільного пристрою в будь-якому місці класу. Відкрити додаток Plickers на своєму телефоні (смартфоні). Обрати клас та необхідне питання з черги

питань. Обране на мобільному пристрої питання автоматично відображається з допомогою проектора через режим Live view.

За допомогою камери сканувати відповіді учнів — картки потрібно повернути так, щоб літера правильної відповіді була розташована вгорі. Кольорове виділення допомагає швидко зорієнтуватися, наскільки правильно учні відповідають на питання: сірим кольором позначені учні, що ще не відповіли, червоним кольором — неправильні відповіді учнів, зеленим кольором — відповіді правильні.

Після завершення тесту натиснути кнопку **Reports** (Звіти, результати) в головному верхньому меню веб-сайту Plickers. Це надасть можливість вивести на екран правильну відповідь і гістограму результатів в списку учнів класу. Також можна показати учням правильні відповіді.

Можна проаналізувати роботу над тестом, за потреби — роздрукувати результати [5].

Рис. 3. Приклад тесту в програмі Plickers

Висновки. В розглянутих системах не завжди доступні характеристики, які є ключовими для розробки продукту. Найчастіше відсутній статистичний пакет, позбавляючи педагога можливості провести перевірку основних характеристик тесту: складність, надійність, валідність тощо. Незважаючи на те, що сучасні програмні засоби дозволяють розробляти діагностичний інструментарій, максимально наближений до перерахованих вище вимог, на даний момент середовищ такого рівня не існує. Тому для розробки нашої платформи оберемо середовище Microsoft Visual Studio (Visual Studio) і спробуємо максимально наблизитись то виконання всіх вимог.

Список використаних джерел

1. В. Вікторук «Використання тестових технологій для контролю знань та умінь учнів». \\ Режим доступу: https://naurok.com.ua/vikoristannya-testovih-tehnologiy-dlya-kontrolyu-znan-ta-umin-uchniv-155709.html (останнє звернення 09.03.2023р.)

2. В. Бойко «Програмні засоби для проведення тестового контролю знань». \\ Режим доступу: http://oldconf.neasmo.org.ua/node/1821 (останнє звернення 09.03.2023р.)

3. О. Корж «Додаток Quizlet ». \\ Режим доступу: https://what.com.ua/dodatok-quizlet-iak-koristyva/ (останнє звернення 13.03.2023р.)

4. О. Тиркалова «Що таке Kahoot! І чому його варто спробувати для організації дистанційного навчання». \\ Режим доступу: https://buki.com.ua/news/shcho-take-kahoot-i-chomu-yoho-varto-sprobuvaty-dlya-orhanizatsiyi-dystantsiynoho-navchannya/ (останнє звернення 13.03.2023р.)

5. «Plickers». \\ Режим доступу: https://sites.google.com/view/it-teachers/plickers (останнє звернення 26.03.2023р.)

Робота виконана під науковим керівництвом д.пед.н., доцента
ЖИРОВОЇ Т.О.

СТАНДАРТ ERC-20. ВИКОРИСТАННЯ API ДЛЯ РОЗГОРТАННЯ ERC-20 ТОКЕНІВ

ЗАДОРОЖНА А., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто інформацію про блокчейн загалом, про Ethereum та технічний стандарт ERC-20. Зазначено переваги та недоліки ERC-20 токенів. Розглянуто також інші популярні токени, такі як ERC-721, ERC-1155, Stellar, NEP-5, TRC-20, BEP-20. *Досліджено переваги та недоліки використання API для розгортання ERC-20 токенів.*

The article discusses information about the blockchain in general, about Ethereum, and the ERC-20 technical standard. The advantages and disadvantages of ERC-20 tokens are indicated. Other popular tokens such as ERC-721, ERC-1155, Stellar, NEP-5, TRC-20, BEP-20 *are also considered. The advantages and disadvantages of using an API for deploying ERC-20 tokens are explored.*

Актуальність. Тематика ERC-20 токенів є досить актуальною, оскільки вона стосується блокчейн - технологій та криптовалют, а це з кожним днем набирає більших обертів. ERC-20 є стандартом, який визначає правила, якими керуються токени, які працюють на блокчейні Ethereum. Тому створення та розгортання ERC-20 токенів є важливою задачею для розвитку різноманітних проектів на основі Ethereum.

API для автоматичної генерації та розгортання ERC-20 токенів може бути корисним інструментом для розробників, які хочуть створити свій власний токен на основі Ethereum, забезпечуючи зручний та швидкий спосіб створення токена з мінімальними зусиллями.

Метою є опис та пояснення стандарту ERC-20, який є одним з найбільш популярних стандартів для створення токенів на блокчейні Ethereum, та аналіз використання API для розгортання ERC-20 токенів.

Об'єкт дослідження. Ethereum як платформа, ERC-20 токени, блокчейн - технології та API для розгортання ERC-20 токенів.

Предмет дослідження. ERC-20 токени та API для їх розгортання.

Виклад основного матеріалу. Блокчейн - це технологія розподіленого реєстру, що забезпечує безпечну, надійну та безперервну обробку транзакцій між користувачами без необхідності в посередниках, таких як банки чи інші фінансові установи. Блокчейн запобігає можливості зміни чи фальсифікації даних та забезпечує високу ступінь безпеки і конфіденційності.

Блокчейн Ethereum - це розподілена платформа для створення децентралізованих додатків та контрактів. Ethereum використовує технологію блокчейн для збереження інформації про транзакції, стану контрактів та інших даних. Ethereum дозволяє розробникам створювати різноманітні децентралізовані додатки, включаючи криптовалютні гаманці, онлайн-ігри та соціальні мережі.

На платформі Ethereum можна створювати власні токени на основі стандарту ERC-20(Ethereum Request for Comment 20), що дозволяє розробникам створювати свої власні токени та використовувати їх у додатках, що побудовані на Ethereum.

ERC-20 - це технічний стандарт для токенів на блокчейні Ethereum, створені токени можуть взаємодіяти з будь-якими іншими токенами, що відповідають стандарту ERC-20. Це означає, що ERC-20 токени можуть бути легко обмінюватись між різними додатками та сервісами, що працюють на базі блокчейну Ethereum.

Стандарт ERC-20 включає в себе ряд функцій, які дозволяють розробникам створювати токени з різними функціональними можливостями. Наприклад, розробники можуть

створювати токени з фіксованою або змінною кількістю в обігу, токени з можливістю виплати дивідендів, токени з можливістю використання у голосуванні та багато іншого.

Токени ERC-20 повинні мати певну структуру та функціональність, а саме:

–назва та символ: кожен токен повинен мати унікальну назву та символ;

–баланси: кожен адрес, що утримує erc-20 токени, має свій власний баланс;

–функції передачі: токени можна передавати з одного адресу на інший. у стандарті erc-20 передбачені дві функції передачі - transfer() та transferfrom();

–approve(address spender, uint256 value) - надання дозволу на пересилання токенів іншому користувачеві;

–функції отримання даних: токени повинні мати функції, які дозволяють отримати інформацію про баланси та інші дані;

–перевірка стану: функції, що дозволяють перевірити стан токенів та перевірити, чи вони належать власникам;

–totalsupply - загальна кількість токенів у циркуляції;

–функції контролю доступу: erc-20 токени можуть мати функції контролю доступу, які дозволяють встановлювати обмеження на передачу токенів;

–стандартні події: erc-20 токени можуть викликати стандартні події, такі як передача токенів, додавання нових токенів та інші. ці події можуть бути використані для сповіщення про транзакції та звітів про стан токенів

–віртуальні гаманці мають підтримувати стандартний інтерфейс для взаємодії з токенами;

–токени мають бути передавані з віртуального гаманця на віртуальний гаманець через стандартний механізм передачі;

–кількість токенів має зберігатись відкрито та бути доступною для перевірки;

–токени повинні бути доступними для покупки та продажу на різних біржах;

–історія транзакцій повинна бути доступна для перегляду;

–токени повинні мати захист від шахрайства та неправомірних дій [1].

Загальний обсяг токенів, що випускається відповідно до стандарту ERC-20, є фіксованим, а це означає, що кількість токенів, які можуть бути створені, буде визначена при створенні контракту.

Оскільки ERC-20 є стандартом, він дозволяє токенам, що відповідають цьому стандарту, взаємодіяти між собою та з різними сервісами та додатками на Ethereum. Це і зробило ERC-20 одним з найпопулярніших стандартів для створення токенів на платформі Ethereum.

Переваги ERC-20 токенів:

– Широке поширення: ERC-20 є одним з найбільш поширених стандартів для випуску токенів на Ethereum, що забезпечує зручність у використанні та інтеграції.

– Стандартизація: Стандарт ERC-20 надає єдиний набір правил, що робить токени ERC-20 взаємозамінними між різними додатками та платформами, що підтримують Ethereum.

– Зручність: ERC-20 токени дозволяють зручно та безпечно виконувати операції зі зберіганням та передачею токенів, що робить їх більш популярними в середині блокчейну.

– Розширюваність: ERC-20 токени можуть бути легко збільшені або зменшені в майбутньому, якщо їх власникам потрібно зробити зміни.

– Автоматизованість: Стандарт ERC-20 може бути програмно забезпечений, що дозволяє розробникам автоматизувати процеси пов'язані з розповсюдженням токенів, створенням контрактів та іншими операціями.

Незважаючи на багато переваг, ERC-20 токени також мають деякі недоліки:

– Обмеженість функцій: ERC-20 токени можуть бути досить обмеженими в тому, що вони можуть робити. Наприклад, вони не можуть безпосередньо взаємодіяти з іншими блокчейнами, що може бути недостатньо для певних додатків.

– Неповна сумісність з іншими стандартами: Інші блокчейн - платформи можуть використовувати різні стандарти, що може призвести до проблем зі сумісністю між різними типами токенів.

– Висока вартість транзакцій: Транзакції з ERC-20 токенами можуть бути відносно дорогими через високі комісії мережі Ethereum, що може становити проблему для користувачів з обмеженим бюджетом.

– Вразливість до помилок: Як і будь-який програмний код, ERC-20 контракти можуть містити помилки, що можуть призвести до втрати токенів або інших проблем.

– Потребує знань: Розуміння ERC-20 стандарту та програмування контрактів на мові Solidity може вимагати значних знань і навичок, що може бути неприйнятним для більшої частини користувачів.

Основною ціллю токенів ERC-20 є забезпечення стандартизованого та сумісного інтерфейсу для створення та управління токенами на блокчейні Ethereum. Це дозволяє розробникам створювати токени, які можуть взаємодіяти з іншими токенами, що відповідають стандарту ERC-20, та легко інтегрувати їх в додатки та сервіси на блокчейні.

Токени ERC-20 також можуть використовуватись як засіб фінансування проектів. В цьому випадку токени можуть бути продані інвесторам з метою залучення коштів на розвиток проекту або інші цілі.

Окрім того, токени ERC-20 можуть використовуватись як засіб платежів та передачі значних сум грошей через блокчейн. Такі токени можуть бути використані в додатках, що працюють на блокчейні Ethereum, для забезпечення безпечних та швидких операцій з переказу токенів[2].

Багато криптовалютних проектів використовують токени ERC-20 для збору коштів та фінансування своїх проектів, так як вони можуть швидко та легко створювати власний токен на основі стандарту ERC-20. Однак, важливо зазначити, що не всі криптовалюти є токенами ERC-20, а ERC-20 токени є лише одним з багатьох видів криптовалют та токенів, що існують на ринку криптовалют.

Використання токенів ERC-20 також пов'язане з ризиками, пов'язаними зі зберіганням і пересиланням токенів. Наприклад, якщо користувач втратить приватний ключ до свого гаманця, він не зможе отримати доступ до своїх токенів. Крім того, відомі випадки крадіжок токенів через підробку гаманців або розсилання шахрайських посилань на гаманці.

Та не дивлячись на ризики, токени ERC-20 здобули широку популярність серед розробників блокчейн - додатків та інвесторів.

Однак, існують інші типи токенів, які можна порівняти з ERC-20 токенами за деякими параметрами. Деякі з них:

– ERC-721 токени: Ці токени відрізняються від ERC-20 токенів тим, що вони не є взаємозамінними. Кожен ERC-721 токен має унікальний ідентифікатор, який відрізняє його від інших токенів. Ці токени частіше використовуються для представлення цифрових активів, таких як мистецькі твори, нерухомість та інші.

– ERC-1155 токени: Це більш новий стандарт, який поєднує в собі можливості як ERC-20, так і ERC-721 токенів. ERC-1155 токени можуть бути взаємозамінними, але вони також можуть мати унікальний ідентифікатор, який надає їм індивідуальність. Цей стандарт широко використовується в ігровій індустрії для створення віртуальних предметів, які можуть бути продані та обмінені між гравцями.

– Stellar токени: Stellar є іншою популярною платформою для створення токенів. Токени на Stellar мають деякі переваги перед ERC-20 токенами, включаючи більш низькі комісії та більш швидкі транзакції. Однак, Stellar має менший розмір спільноти та менше розвинуту інфраструктуру, ніж Ethereum.

– NEP-5 токени: NEP-5 токени є стандартом токенів на платформі NEO, яка є конкурентом Ethereum. Ці токени також використовуються для створення цифрових активів, таких як криптовалюти та інші. Хоча NEP-5 токени є сумісними з ERC-20 токенами та мають

схожі можливості, вони мають деякі відмінності, наприклад, у NEP-5 токенів є можливість додаткового захисту, що дозволяє зменшити ймовірність втрати токенів внаслідок помилкових транзакцій.

– TRC-20 токени: TRC-20 є стандартом токенів на блокчейні TRON. Ці токени можуть використовуватись для створення криптовалют на TRON, а також для створення інших цифрових активів, які можуть бути обмінюваними на TRON. TRC-20 токени мають деякі схожі можливості з ERC-20 токенами, але вони працюють на іншій платформі.

– BEP-20 токени: BEP-20 є стандартом токенів на блокчейні Binance Smart Chain. Ці токени можуть бути використані для створення криптовалют та інших цифрових активів, які можуть бути обмінюваними на Binance Smart Chain. BEP-20 токени також мають схожі можливості з ERC-20 токенами, але вони працюють на іншій платформі.

Хоча кожен з цих типів токенів має свої особливості, всі вони мають деякі спільні риси з ERC-20 токенами, такі як можливість створення власних цифрових активів та їх обмін на різних біржах.

Після проведення порівняльного аналізу можна зробити висновки, що хоч всі ці токени мають спільні риси, вони мають відмінності в стандартах та використанні, які можуть бути важливими для різних проектів та використання. Отже, перед створенням токенів, варто обрати платформу та стандарт, що найкраще відповідає конкретним потребам проекту.

Якщо розробник хоче створити свій власний ERC-20 токен, для цього йому потрібно мати розуміння того, які кроки потрібно зробити для його створення та розгортання. Хоча процес розгортання ERC-20 токенів може здатися складним, насправді для цього існують спеціальні API, які спрощують цей процес.

API - це інтерфейс програмування застосунків, який дозволяє розробникам взаємодіяти зі складовими програмного забезпечення, такими як сервери, бази даних, бібліотеки, фреймворки та інші. Для розгортання ERC-20 токенів розробники можуть використовувати спеціальні API, які забезпечують швидке та просте створення та розгортання токенів, або створити своє API, якщо для цього є достатні можливості і знання [3].

Переваги API для розгортання ERC-20 токенів:

– Швидкість розгортання. Використання API дозволяє значно зменшити час, необхідний для розгортання ERC-20 токенів на Ethereum. API надає можливість автоматизувати процес розгортання токенів, що дозволяє збільшити швидкість та ефективність цього процесу.

– Зручність використання. Використання API дозволяє значно спростити процес розгортання ERC-20 токенів на Ethereum. Замість того, щоб вручну вводити всі необхідні параметри, можна використовувати API, що надає готові інтерфейси для взаємодії з Ethereum - блокчейном. Це зменшує ризик помилок, пов'язаних з неправильним введенням параметрів та збільшує ефективність процесу.

– Більш висока точність та надійність. Використання API дозволяє забезпечити більш високу точність та надійність процесу розгортання ERC-20 токенів на Ethereum. Це пов'язано з тим, що API використовує стандартні параметри та протоколи, що забезпечує сумісність токенів з будь-яким Ethereum - гаманцем, що підтримує ERC-20.

– Більш простий доступ до Ethereum - блокчейну. Використання API дозволяє значно спростити доступ до Ethereum - блокчейну для розгортання ERC-20 токенів. Замість того, щоб створювати власний вузол Ethereum - блокчейну та налаштовувати його, можна використовувати API, яке забезпечує доступ до Ethereum - блокчейну з максимально спрощеною процедурою.

– Менші витрати. Використання API для розгортання ERC-20 токенів на Ethereum дозволяє зменшити витрати на інфраструктуру, необхідну для створення власного вузла Ethereum - блокчейну. Крім того, витрати на оплату газу, необхідного для транзакцій на Ethereum - блокчейні, можуть бути значно зменшені за допомогою використання API, яке забезпечує оптимізацію витрат на транзакції.

– Більш висока безпека. Використання API для розгортання ERC-20 токенів на Ethereum забезпечує більш високу безпеку, оскільки API використовує відповідні протоколи та захист, що забезпечують захист від можливих атак та зламів. Крім того, використання API дозволяє забезпечити більш високу безпеку управління токенами, оскільки API забезпечує автоматичний контроль доступу до токенів та автоматичне відслідковування транзакцій.

– Підтримка стандартів та протоколів. Використання API для розгортання ERC-20 токенів на Ethereum забезпечує підтримку стандартів та протоколів, що необхідні для розгортання токенів на Ethereum - блокчейні. API надає можливість використовувати стандартні параметри та протоколи, що забезпечують сумісність токенів з будь-яким Ethereum - гаманцем, що підтримує ERC-20.

– Підтримка аудиту безпеки. Використання API для розгортання ERC-20 токенів на Ethereum забезпечує можливість підтримки аудиту безпеки токенів. API надає можливість відслідковувати транзакції токенів та забезпечує автоматичне відслідковування потенційних проблем безпеки.

– У всього є недоліки, і API для розгортання ERC-20 токенів не виключення, але їх кількість значно менша за переваги. API мають такі недоліки:

– Сумісність: Деякі API можуть бути несумісні з іншими блокчейн - платформами або стандартами, що може призвести до проблем зі сумісністю між різними типами токенів.

– Витратність: Якщо використовувати вже готові API, то сервіси можуть стягувати високі комісії за використання їхнього API.

– Складність: Використання API може вимагати значних знань програмування та блокчейн технологій, що може бути неприйнятним для більшої частини користувачів [4].

При розгляді API для розгортання ERC-20 токенів варто враховувати як переваги, так і недоліки цього рішення. Розробники повинні детально вивчити можливості, обмеження та ризики, пов'язані з використанням API для розгортання ERC-20 токенів, перш ніж вирішувати, чи цей варіант підходить для їх потреб.

Висновки. Стандарт ERC-20 є одним з найбільш популярних стандартів для створення токенів на блокчейні Ethereum. Він забезпечує стандартизацію токенів, що дозволяє їх використовувати на різних біржах і у гаманцях, а також сприяє прозорості і безпеці управління токенами. Для ефективного розгортання ERC-20 токенів, необхідне API, яке забезпечує зручний та безпечний спосіб створення, керування та взаємодії з токенами. Це дозволяє створювати токени з мінімальними зусиллями, забезпечуючи при цьому високий рівень безпеки та надійності. Тематика автоматичної генерації та розгортання Erc-20 токенів є актуальною для розробників, бізнесу та тих, хто цікавиться блокчейн-технологіями та криптовалютами.

Список використаних джерел

1. What Are ERC-20 Tokens on the Ethereum Network? \\ Режим доступу: https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/
2. ERC-20 token standard. \\ Режим доступу: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
3. How to Create an ERC20 Token the Simple Way \\ Режим доступу: https://www.toptal.com/ethereum/create-erc20-token-tutorial
4. Exploring the Ultimate ERC20 Token API \\ Режим доступу: https://moralis.io/exploring-the-ultimate-erc20-token-api/

Робота виконана під науковим керівництвом к.пед.н., доцента
ЖИРОВОЇ Т.О.

ВПЛИВ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ НА ЕФЕКТИВНІСТЬ РОБОТИ АВТОТРАНСПОРТНОГО ПІДПРИЄМСТВА

ЗАПОРОЖЕЦЬ Б., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Ця наукова стаття присвячена дослідженню впливу автоматизованих систем управління на ефективність роботи автотранспортного підприємства, в ній розглядаються основні переваги використання автоматизованих систем управління, таких як зменшення ризику помилок та підвищення продуктивності працівників.

This research article is devoted to the study of the impact of automated control systems on the efficiency of a road transport enterprise, and it examines the main advantages of using automated control systems, such as reducing the risk of errors and increasing employee productivity.

Актуальність. В сучасному світі автотранспортні підприємства стикаються з рядом складних викликів, таких як зменшення прибутковості, підвищення витрат на паливо та обслуговування автопарку, а також потребу в ефективній організації та керуванні транспортними потоками.

Використання автоматизованих систем управління може допомогти компаніям ефективно керувати транспортними потоками та забезпечити оптимальне використання ресурсів, що може призвести до зниження витрат та підвищення продуктивності.

Метою статті є дослідження впливу автоматизованих систем управління на ефективність роботи автотранспортного підприємства.

Об'єктом дослідження є автотранспортне підприємство, яке займається перевезенням вантажів та/або пасажирів.

Предмет дослідження – автоматизовані системи управління, що використовуються для керування автотранспортними потоками та забезпечення ефективної роботи підприємства.

Аналіз попередніх досліджень. Розвиток автоматизації виробництва можна умовно поділити на три етапи. Перший етап автоматизації охоплює період часу з початку XVIII до кінця XIX століття. Потрібно зазначити, що розвиток автоматизації виробництва в цей період часу базувався на принципах і методах класичної механіки. Другий етап розвитку автоматизації виробництва охоплює кінець XIX середини XX століття. Цей етап пов'язаний із розвитком електротехніки та практичним використанням електроенергії у засобах автоматизації. Переходом до третього етапу розвитку автоматизації послужили нові можливості ЧПУ, які базуються на застосуванні мікропроцесорної техніки, що дозволило створювати принципово нову систему машин, в якій би поєднувалась висока продуктивність автоматичних ліній з вимогами гнучкості виробничого процесу. Сучасні мікроелектроніка та ЕОМ дозволяють досягти вищого рівня автоматизації. [1]

Виклад основного матеріалу. За останні роки автоматизовані системи управління (АСУ) почали активно впроваджуватись в різні сфери людської діяльності, оскільки вони дають змогу зменшити використання людських ресурсів, здатні працювати 24 години на добу, аналізувати та опрацьовувати великі обсяги даних за невеликий час та багато інших аспектів, в яких машина перемагає у людини. Автотранспортні підприємства (АТП) не є виключенням, адже в сучасному світі їх діяльність може не обмежуватись одним населеним пунктом чи країною, при цьому кількість замовлень може перевищувати кількість наявних ресурсів, які використовуються на підприємстві, що в свою чергу знижує його дохідність, в гіршому випадку, призводить до втрати клієнтів. [2]

Процес впровадження автоматизованих систем управління на підприємство включає декілька етапів: детальний аналіз, вибір системи, планування проекту, впровадження, тестування та налагодження, операційну підтримку, навчання персоналу та оцінку результатів.

Починаючи з аналізу потреб та вимог підприємства, визначаються пріоритетні напрямки автоматизації та формуються функціональні вимоги до системи. Відповідно до аналізу, обирається найкраща система, яка задовольняє вимоги підприємства. Розробляється детальний план проекту, який визначає ресурси, терміни та витрати на реалізацію. Впровадження системи передбачає збір, обробку та міграцію даних, налаштування та встановлення програмного забезпечення. Після цього проводяться тестування та налагодження системи. Забезпечується операційна підтримка та навчання персоналу для ефективного використання нової системи. Оцінка результатів дозволяє визначити ефективність, продуктивність та інші ключові показники проекту. На основі цих даних приймаються рішення щодо подальшої оптимізації та розвитку системи. Основні проблеми, які можуть виникнути під час впровадження, включають високі витрати, суперечливість з існуючими процесами, недостатню підготовку персоналу, технічні питання, неправильний вибір системи, безпеку та конфіденційність. Успішне впровадження системи вимагає уважного аналізу, планування, операційної підтримки та навчання персоналу. Після оцінки результатів та вирішення можливих проблем, підприємство може почати повноцінно використовувати автоматизовану систему управління для покращення ефективності та продуктивності. Важливо продовжувати моніторинг роботи системи, виявляти і усувати нові проблеми та недоліки. Також корисно забезпечити регулярні оновлення системи, адаптацію до змін у законодавстві, індустріальних стандартах та ринкових вимогах. Система повинна постійно розвиватися і вдосконалюватися, щоб підтримувати конкурентоспроможність підприємства. Залучення зовнішніх експертів і консультантів може допомогти у впровадженні та підтримці автоматизованих систем управління. Вони можуть надати цінні поради, рекомендації та допомогу у вирішенні складних питань. Отже, успішне впровадження автоматизованих систем управління на автотранспортне підприємство вимагає відповідного планування, аналізу, реалізації та операційної підтримки. Важливо забезпечити навчання та адаптацію персоналу, а також постійно оцінювати результати та вдосконалювати систему. Це допоможе підприємству покращити свою ефективність та конкурентоспроможність, а також адаптуватися до змін у ринкових умовах.

Аналіз сучасних тенденцій у використанні автоматизованих систем управління на автотранспортних підприємствах показує, що вони стають все більш популярними та необхідними для забезпечення ефективної та безпечної роботи підприємств. Зокрема, можна виділити такі тенденції та напрямки розвитку:

- Використання хмарних технологій – автотранспортні підприємства все частіше використовують хмарні технології для зберігання та обробки даних. Це дозволяє забезпечити доступ до інформації з будь-якого місця та прискорити роботу з даними.
- Використання інтернету речей – використання сенсорів та інших пристроїв для збору даних про роботу транспортних засобів та їхнє місцезнаходження дозволяє автоматизувати процеси управління та підвищити ефективність роботи підприємства.
- Використання штучного інтелекту та машинного навчання – ці технології дозволяють автоматизувати процеси прийняття рішень та оптимізувати роботу підприємства. Наприклад, використання алгоритмів машинного навчання для прогнозування попиту на послуги транспортного підприємства дозволяє підприємству планувати свої ресурси та роботу більш ефективно.
- Розвиток систем моніторингу та керування – сучасні системи моніторингу дозволяють в режимі реального часу контролювати роботу транспортних засобів, їх місцезнаходження та стан. Це дозволяє оперативно реагувати на зміни та прогнозувати проблеми, що можуть виникнути під час експлуатації транспорту.
- Використання системи геолокації – система геолокації дозволяє точно визначити місцезнаходження транспортного засобу, що є корисним для планування маршрутів та вибору оптимального маршруту для доставки вантажів. Також ця система може допомогти в забезпеченні безпеки транспорту та підвищенні якості обслуговування.

- Використання систем бронювання – системи бронювання дозволяють замовляти транспортні послуги в режимі онлайн та оплачувати їх через інтернет. Це дозволяє зменшити витрати на обслуговування та забезпечити більш зручний та швидкий процес бронювання послуг.
- Розвиток систем аналітики даних – збільшення обсягів даних та їх складність потребують використання спеціалізованих систем аналітики даних. Ці системи дозволяють виявляти тенденції, розуміти потреби клієнтів та забезпечувати високу ефективність роботи транспортного підприємства.
- Розробка мобільних додатків – мобільні додатки дозволяють замовляти транспортні послуги, відстежувати місцезнаходження транспорту та отримувати інформацію про розклади руху. Це дозволяє забезпечити більш зручний та швидкий процес замовлення транспорту та забезпечити задоволеність клієнтів.

Існують готові рішення автоматизованих систем управління для автотранспортних підприємств, які можуть бути використані без необхідності розробки власної програми. Головними представниками, які вже закріпилися на ринку є Wialon, FleetComplete, GPSWOX та TransICS - це програмні продукти, призначені для керування автопарками та транспортними потоками на автотранспортних підприємствах. Хоча вони мають схожі функції, кожен з цих продуктів має свої особливості, які роблять його унікальним.

Порівняльна характеристика цих програмних продуктів: [2-5]

- Wialon – це потужна система керування автопарком, яка дозволяє відслідковувати рух транспорту в режимі реального часу, контролювати витрати на паливо та зберігання, а також підтримує безкоштовний мобільний додаток для Android та iOS. Wialon також має гнучку систему налаштувань, яка дозволяє налаштовувати функціональність системи під конкретні потреби підприємства.
- FleetComplete – це програмне забезпечення, яке надає повну інформацію про рух транспорту, стан палива, витрати та інші параметри, що дозволяє керувати автопарком на більш ефективному рівні. FleetComplete також має функції моніторингу водіїв та виконання маршрутів, що дозволяє підприємствам забезпечити своїм клієнтам найкращий сервіс.
- GPSWOX – це проста у використанні система керування автопарком, яка дозволяє відслідковувати рух транспорту в режимі реального часу, контролювати рівень палива та інші параметри, а також отримувати сповіщення про відхилення від заданого маршруту та інші події. GPSWOX також має зручний інтерфейс та доступний ціновий пакет.
- TransICS – це програмний продукт, що дозволяє керувати автопарком в режимі реального часу, контролювати витрати на паливо та зберігання, а також підтримує моніторинг поведінки водіїв. Однією з ключових переваг TransICS є його інтеграція з системами електронних довірчих послуг, що дозволяє автоматизувати процеси звітності та документообігу.

Загалом, кожен з цих програмних продуктів має свої переваги та може бути корисним для різних типів автотранспортних підприємств. Wialon та FleetComplete мають більше функціональних можливостей, що робить їх ідеальними для великих підприємств, які потребують більш гнучкої настройки системи. GPSWOX та TransICS, з іншого боку, можуть бути корисними для менших підприємств, які шукають прості та доступні рішення для керування автопарком.

При виборі програмного продукту для керування автопарком необхідно враховувати розмір та тип підприємства, а також його потреби та бюджет. Крім того, важливо бути впевненим у тому, що програмний продукт відповідає всім необхідним вимогам та має потрібний рівень надійності та безпеки.

Існують деякі недоліки використання готових рішень для керування автотранспортними підприємствами. Один з них – обмежена функціональність. Готові рішення можуть мати обмежену функціональність, що не відповідає специфічним потребам

підприємства, в такому випадку використання готового рішення може бути неефективним. Інший недолік - відсутність гнучкості. Готові рішення можуть бути недостатньо гнучкими для настройки на конкретні потреби підприємства. Це може призвести до того, що підприємство буде витрачати гроші на функціонал, який не потрібен, або не зможе отримати функціонал, який потрібен. Третій недолік - проблеми з безпекою. Готові рішення можуть бути вразливими до кібератак та інших видів злому. Якщо рішення не має достатнього рівня захисту, то це може призвести до втрати даних та порушення безпеки підприємства.

Окрім цього, використання готових рішень може обмежувати можливості розвитку та інновацій підприємства. Тому, перед вибором готового рішення, потрібно ретельно проаналізувати всі його переваги та недоліки та визначити, яке найкраще відповідає потребам конкретного підприємства. Крім того, можна розглянути можливість залучення фахівців для розробки власної системи управління, що дозволить повністю врахувати всі специфічні потреби підприємства.

Використання готових рішень має свої плюси та мінуси. Врахування всіх переваг та недоліків, а також конкретних потреб підприємства, дозволить зробити найбільш ефективний вибір.

Автоматизована система управління забезпечує зручне та швидке управління автотранспортним підприємством. Вона дає можливість контролювати використання транспортних засобів, їхній технічний стан, склад та рух вантажів. Завдяки автоматизованій системі управління можна точно контролювати витрати на паливо, зарплату персоналу.

Одним з головних позитивних ефектів автоматизованої системи управління є економія часу. Автоматизована система управління дозволяє швидко та точно вести облік всіх дій, пов'язаних з перевезенням вантажів, тому менше часу витрачається на аналіз даних та прийняття рішень. Більше часу можна відвести на розвиток бізнесу та роботу з клієнтами.

Іншим важливим ефектом є зниження витрат. Автоматизована система управління дозволяє точно контролювати витрати на паливо, зарплату водіїв та іншого персоналу. Завдяки цьому можна зменшити витрати на оплату праці та паливо, що в свою чергу призведе до зниження вартості перевезень та збільшення прибутку.

Крім цього, автоматизована система управління допомагає уникнути людських помилок, що можуть призвести до неправильних рішень та втрати часу та коштів. Вона також дозволяє вести статистику та аналізувати дані, що допомагає визначати слабкі місця в роботі підприємства та шукати шляхи їх вдосконалення.

Іншим важливим ефектом є покращення безпеки та якості роботи. Автоматизована система управління дозволяє вести контроль за технічним станом транспортних засобів та їхньою експлуатацією. Це дозволяє знизити ризик аварій та непередбачуваних ситуацій, що можуть призвести до збитків та втрати репутації підприємства.

Крім того, автоматизована система управління дозволяє ефективніше взаємодіяти з клієнтами та партнерами, що в свою чергу може призвести до збільшення прибутку та розширення бізнесу.

Серед представників українського сектору автотранспортних підприємств, які впроваджують та вдосконалюють свої автоматизовані системи, можна виділити такі як “Нова Пошта”, “Київпастранс”.

"Нова Пошта" – це одна з найбільших і найпопулярніших логістичних компаній в Україні, яка займається доставкою різних видів вантажів та поштових відправлень. Вона використовує в своїй роботі систему GPS-трекінгу та надає своїм клієнтам доступ до цієї інформації, що дає можливість в режимі реального часу відслідковувати посилки клієнтів. [7] Також це підприємство автоматизовувало свої системи в сферах фінансового обліку, оподаткування та логістики. [8-10]

"Київпастранс" – це комунальне підприємство, яке забезпечує пасажирський транспорт у місті Києві. Головним впровадженням стало використання системи GPS-трекінгу, котра надає можливість відслідковувати маршрутні транспортні засоби в режимі реального часу.

[11] Крім цього на підприємстві впроваджені автоматизована система контролю використання палива, автоматизовані АЗС, а також система електронного квитка. [12]

Висновки. Отже, можна стверджувати, що автоматизована система управління має великий вплив на ефективність роботи автотранспортного підприємства. Вона дозволяє знизити витрати, покращити безпеку та якість роботи, збільшити ефективність взаємодії з клієнтами та партнерами та забезпечити економію часу.

Автоматизована система управління є необхідною складовою успішного функціонування автотранспортного підприємства та дозволяє підвищити його конкурентоспроможність на ринку. Водночас, необхідно враховувати витрати на впровадження та підтримку автоматизованої системи управління та підготувати персонал до роботи з нею. Крім того, необхідно провести дослідження та аналіз ринку, вибрати систему, яка найкраще відповідає потребам підприємства та забезпечити підтримку та навчання персоналу.

Також важливо пам'ятати, що не завжди готові рішення є ідеальним варіантом для підприємства, оскільки вони можуть мати певні обмеження та недоліки. Тому, необхідно проводити обґрунтований аналіз та оцінку ризиків при виборі та впровадженні автоматизованої системи управління на автотранспортному підприємстві.

Список використаних джерел

1. Єфремов, М. Ф., Єфремов, В. М., & Єфремов, Ю. М. (2015). АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ ПІДПРИЄМСТВОМ SAB 3000. Вісник ЖДТУ. Серія "Технічні науки", (2(61), 80–85.
2. Єфремов, М. Ф., Єфремов, Ю. М., & Єфремов, В. М. (2017). Проблеми і вимоги до АСУ автотранспортного підприємства. Вісник ЖДТУ. Серія "Технічні науки", 1(2(80), 135–138.
3. Wialon – система моніторинга транспорту // Режим доступу: https://gurtam.com/en/wialon (Останнє звернення 04.04.2023)
4. Fleet Complete - провідний світовий постачальник рішень Інтернету речей у сфері підключених комерційних транспортних засобів // Режим доступу: https://www.fleetcomplete.com/ (Останнє звернення 04.04.2023)
5. GPSWOX — онлайн-програмне забезпечення для відстеження GPS і система керування автопарком // Режим доступу: https://www.gpswox.com/ (Останнє звернення 04.04.2023)
6. TransISC - програмне рішення для автоматизації управління автотранспортним підприємством // Режим доступу: https://www.zf.com/products/en/cv/home/cv.html/ (Останнє звернення 04.04.2023)
7. Нова Пошта - трекінг посилки // Режим доступу: https://novaposhtaglobal.ua/track/ (Останнє звернення 05.04.2023)
8. Автоматизація відділень Нової Пошти // Режим доступу: https://systemgroup.com.ua/uk/project/avtomatyzaciya-viddilen-novoyi-poshty (Останнє звернення 05.04.2023)
9. Новий термінал для Нова Пошта // Режим доступу https://konsort.com.ua/novyj-terminal-dlya-nova-poshta/ (Останнє звернення 05.04.2023)
10. Впровадження Microsoft Dynamics AX2012 R3 для “Нової пошти” // Режим доступу: https://ontargit.com/ua/case-study/nova-poshta-story/ (Останнє звернення 05.04.2023)
11. Київпастранс - транспорт online // Режим доступу: https://kpt.kyiv.ua/online (Останнє звернення 05.04.2023)
12. Київпастранс - річниця та звіт по виконаній роботі. // Режим доступу: https://kpt.kyiv.ua/kyivpastransformation/anniversary_18 (Останнє звернення 05.04.2023)

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н.О.

ЗАХИСТ ТА ЛІЦЕНЗУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ІГНАТОВ М., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні методи та принципи захисту програмного забезпечення. Зазначено переваги та недоліки застосування готових програмних продуктів для забезпечення ліцензійного управління програмним забезпеченням. Розглянуто "License4J" як зразок програми для забезпечення ліцензійного управління своїм програмним забезпеченням.

The article discusses the main methods and principles of software protection. The advantages and disadvantages of using ready-made software products to ensure software license management are indicated. Considered "License4J" as a sample program for providing license management of your software.

Актуальність. В сучасному світі програмне забезпечення використовується практично в усіх галузях, починаючи від медицини та закінчуючи фінансами та технологіями. Захист програмного забезпечення стає все важливішим, оскільки його вразливість може призвести до серйозних наслідків, таких як виток конфіденційної інформації, крадіжка особистих даних або керуванням програмами зловмисниками.

Всі ці вразливості є давно відомими, проте в час коли цифрова інформаційна діяльність поширюється на нові сфери та набігає нових масштабів, ці загрози повстають вже не тільки перед звичайним користувачем, проте стають серйозною загрозою для економічної та національної безпеки держави.

Ось кілька факторів, які підкреслюють актуальність цих питань:

1. Захист інтелектуальної власності: Програмне забезпечення є одним з ключових елементів інтелектуальної власності, і його захист має важливе значення для розробників та компаній, які вкладають ресурси в його створення. Зловживання програмним забезпеченням, таке як незаконне копіювання, розповсюдження або використання без ліцензії, може призвести до втрати прибутків та порушення прав розробників. Захист інтелектуальної власності в програмному забезпеченні є важливим економічним фактором, що сприяє стимулюванню інновацій та розвитку високотехнологічного сектору, яким є ІТ-галузь в Україні.
2. Контроль за використанням програмного забезпечення: Це може бути важливим фактором національної безпеки, оскільки використання нелицензійного або піратського програмного забезпечення може ставити під загрозу безпеку державних систем та інфраструктури. Нелегальне використання програмного забезпечення також може викликати ризик порушення правил використання та витоків даних, що може мати серйозні наслідки для державної безпеки.
3. Забезпечення якості та безпеки програмного забезпечення: Ліцензування може також включати вимоги щодо якості та безпеки програмного забезпечення, забезпечуючи виконання відповідних стандартів та правил розробки. Це може бути важливим фактором національної безпеки, оскільки ненадійне або небезпечне програмне забезпечення може викликати ризик для захисту даних, конфіденційності та цілісності інформації, включаючи державну інформацію.

Отже, захист та ліцензування програмного забезпечення в Україні є актуальними факторами економічної та національної безпеки держави з ряду причин. Вони сприяють захисту інтелектуальної власності, розкриттю економічного потенціалу, забезпеченню конкурентоспроможності національної ІТ-галузі, забезпеченню якості та безпеки програмного забезпечення, а також виконанню міжнародних зобов'язань.

Метою статті є висвітлення проблематики захисту та ліцензування програмного забезпечення, огляд наявних методів, які дозволяють розробникам забезпечувати ліцензійне управління своїм програмним забезпеченням. Дослідження зосереджене на аналізі різних типів ліцензій та технологій, які використовуються для захисту ПЗ.

Об'єктом дослідження є розробка безпечної системи ліцензування.

Предмет дослідження – інформаційні системи ліцензування.

Аналіз попередніх досліджень. Захист та ліцензування програмного забезпечення є важливим фактором захисту інтелектуальної власності, економічної та національної безпеки. Дослідники з різних галузей, такі як право, бізнес, техніка та етика, досліджували цю проблематику з різних перспектив. Деякі з відомих дослідників, які присвятили свої роботи цій проблемі, включають:

- Річард Столлман - відомий американський програміст і активіст, засновник Free Software Foundation. У своїх роботах, включаючи статтю «Чому програмне забезпечення має бути безкоштовним», Столлман обговорює важливість захисту вільної ліцензії для захисту прав користувачів і розробників.
- Брюс Шнайер — відомий американський криптограф і експерт з кібербезпеки. У таких роботах, як «Секрети та брехня: цифрова безпека в мережевому світі», Шнайер розглядає різні аспекти захисту програмного забезпечення та ліцензування з точки зору криптографії та технічної безпеки.
- Лоуренс Лессіг - відомий американський юрист і активіст, автор теорії «кодексу і закону» (code is law), яка стосується взаємодії правового регулювання і технологій, зокрема програмного забезпечення. У таких роботах, як «Код: версія 2.0», Лессіг аналізує вплив ліцензування та правових аспектів на розповсюдження та використання програмного забезпечення.

Джон Ф. Шерман і Томас Дж. Малнайт у своїх роботах «Захист прав інтелектуальної власності на програмне забезпечення» та «Управління інноваціями в новій економіці: стратегії інтелектуальної власності та практика ліцензування програмного забезпечення» розглянули аспекти захисту та ліцензування програмного забезпечення з точки зору бізнесу. Вони визначили важливість правового захисту програмного забезпечення, включаючи авторські права, патенти та умови ліцензії, для забезпечення права власності та контролю над розповсюдженням і використанням програмного забезпечення. Вони також вказали на труднощі досягнення балансу між захистом прав розробників і користувачів, просуванням інновацій і відкритої співпраці, забезпеченням безпеки та захистом конфіденційності під час ліцензування програмного забезпечення.

Інші дослідники, такі як Роберт А. Ганц у своїй роботі «Піратство програмного забезпечення та злочинність: глобальна проблема з економічними, соціальними та культурними наслідками» досліджували економічні наслідки незаконного копіювання та використання незаконних копій програмного забезпечення. Він підкреслив, що незаконне використання програмного забезпечення може мати серйозні наслідки для економіки, суспільства та культури, включаючи втрату доходу для розробників, порушення прав інтелектуальної власності та незаконну конкуренцію.

Тому захист і ліцензування програмного забезпечення є важливими аспектами забезпечення інтелектуальної власності, економічної та національної безпеки. Враховуючи різноманітні проблеми та проблеми, пов'язані із захистом програмного забезпечення та ліцензуванням, можна зробити наступні висновки:

- Питання захисту та ліцензування програмного забезпечення має багато аспектів, включаючи технічні, правові, етичні та соціальні аспекти.
- Ефективний захист програмного забезпечення та ліцензування є важливим фактором захисту прав інтелектуальної власності розробників. Це може сприяти інноваціям, оскільки стимулює розробників і компанії інвестувати ресурси в дослідження та розробку нових продуктів, гарантуючи, що їхні творчі права захищені та винагороджені відповідно.

- Незаконне використання програмного забезпечення може призвести до втрати прибутків розробниками та виробниками, порушення їх прав інтелектуальної власності, а також може мати негативні наслідки для національної економіки.
- Використання різних методів захисту, таких як шифрування, цифрові підписи, ліцензійні угоди та інші технічні та юридичні заходи, може бути ефективним способом захисту програмного забезпечення від незаконного використання.
- Захист програмного забезпечення та ліцензування також мають важливий аспект національної безпеки, оскільки вони можуть впливати на захист конфіденційної інформації та захист критично важливих систем і мереж від можливих кібератак.

Виклад основного матеріалу. Огляд різних методів захисту програмного забезпечення є важливим аспектом в розробці програм, оскільки це дозволяє забезпечити захист від несанкціонованого доступу, копіювання, підробки та зміни програмного коду. Для досягнення цієї мети використовуються різноманітні методи, такі як криптографічні методи, методи обфускації та віртуалізації, а також методи, що базуються на аналізі поведінки програм, разом з різноманітними методами ліцензування.

Один з ефективних методів захисту програмного забезпечення - це криптографічні методи, які забезпечують захист даних та коду шляхом шифрування і підписування [1]. Криптографічні методи можуть використовуватись для захисту ліцензійного ключа, валідації програмного забезпечення та забезпечення цілісності та конфіденційності даних, які використовуються програмою.

Методи обфускації та віртуалізації також використовуються для захисту програмного забезпечення [2]. Обфускація полягає в унеможливленні зрозуміння коду програми шляхом зміни його структури та логіки, тоді як віртуалізація передбачає виконання програми в ізольованому середовищі, що робить важким аналіз та зрозуміння її роботи.

Методи, що базуються на аналізі поведінки програм, також використовуються для виявлення та захисту від потенційно шкідливої активності. Ці методи передбачають відстеження дій програми під час виконання та виявлення ненормальної активності, такої як відправка незвичних мережевих запитів або зміна внутрішнього стану програми, що може свідчити про можливість атаки або незаконної діяльності [3].

Огляд наявних технічних методів ліцензування програмного забезпечення може включати різні технологічні рішення, які допомагають контролювати використання програмного забезпечення та захищати інтелектуальну власність розробника. Деякі з таких технічних рішень включають:

1. Ключі активації: Це метод ліцензування, при якому розробник надає спеціальні ключі активації, які користувач повинен ввести під час встановлення або активації програмного забезпечення. Ключ активації може бути зв'язаний з певним обладнанням або залежати від кількості користувачів, які мають доступ до програми.
2. Хешування апаратного забезпечення: Це метод ліцензування, при якому програмне забезпечення перевіряє хеш-код апаратного забезпечення, на якому воно встановлене, і порівнює його зі збереженим значенням. Це дозволяє розробнику обмежувати використання програмного забезпечення лише на певних комп'ютерах або пристроях.
3. Контроль доступу: Це метод ліцензування, при якому розробник встановлює механізми контролю доступу до програмного забезпечення, такі як паролі, рівні доступу або автентифікація, що дозволяють обмежувати доступ до програми лише певним користувачам або групам користувачів.
4. Шифрування: Це метод ліцензування, при якому програмне забезпечення шифрується, що робить його незрозумілим або недоступним без відповідного розшифрування або ключа. Це дозволяє розробникам захистити своє програмне забезпечення від несанкціонованого використання або копіювання.
5. Віддалене управління: Це метод ліцензування, при якому розробник може віддалено керувати використанням свого програмного забезпечення. Наприклад, розробник може використовувати хмарні сервіси для моніторингу та контролю використання своєї

програми на різних пристроях, включаючи вимкнення доступу до програми в разі порушення ліцензійних умов.

6. Цифрові підписи: Це метод ліцензування, при якому програмне забезпечення підписується цифровим ключем розробника, що дозволяє перевіряти автентичність та цілісність програми. Це допомагає відслідковувати та запобігати змінам або модифікаціям програми без дозволу розробника.

7. Ліцензійні сервери: Це метод ліцензування, при якому розробник використовує централізований сервер для контролю доступу до свого програмного забезпечення. Користувачі повинні зв'язуватися з цим сервером для отримання ліцензії або активації програми.

8. Використання апаратних токенів або донглів: Це метод ліцензування, при якому розробник використовує спеціальні апаратні токени або донгли для фізичного контролю доступу до програми. Ці токени можуть містити ключі, сертифікати або іншу інформацію, необхідну для ліцензування програмного забезпечення [4].

Ці технічні методи ліцензування можуть бути використані окремо або в комбінації, залежно від потреб розробника та вимог ринку.

Захист та ліцензування програмного забезпечення можуть бути здійснені за допомогою різних технічних методів, кожен з яких має свої переваги та недоліки. Ось декілька загальних прикладів:

1. Апаратний ключ (dongle):
   Переваги:
   - Висока рівень захисту: апаратний ключ має фізичну форму, тому його важко скопіювати або зламати.
   - Зручність в управлінні: ліцензійна інформація зберігається на апаратному ключі, що дозволяє зручно керувати ліцензіями та встановлювати контроль над використанням програмного забезпечення.
   - Можливість фізично відключити доступ до програмного забезпечення: у разі порушення ліцензійних умов, апаратний ключ можна відключити, що дозволяє заборонити використання програмного забезпечення.

   Недоліки:
   - Вартість: придбання апаратних ключів та їх обслуговування може бути вартісним, особливо в випадку великих масштабів використання програмного забезпечення.
   - Можливість втрати або пошкодження: якщо апаратний ключ втрачений або пошкоджений, це може призвести до втрати доступу до програмного забезпечення.
   - Обмеження використання на різних платформах: апаратний ключ зазвичай прив'язаний до конкретної платформи, що може обмежити його використання на різних пристроях або платформах.
2. Ліцензійний файл:
   Переваги:
   - Зручність в розповсюдженні: ліцензійний файл може бути відправлений електронно або включений в саму програму, що дозволяє зручно розповсюджувати програмне забезпечення та ліцензії.
   - Гнучкість в управлінні: ліцензійний файл може містити різні параметри ліцензування, такі як термін дії, кількість користувачів, функціональні обмеження тощо, що дозволяє гнучко налаштовувати ліцензії для різних клієнтів.

   Недоліки:

- Можливість копіювання або передачі ліцензійного файлу: ліцензійний файл може бути скопійований або переданий іншим користувачам, що може призвести до незаконного використання програмного забезпечення.
- Вразливість до копіювання або редагування: ліцензійний файл може бути вразливим до копіювання або редагування, що може призвести до нелегального використання програмного забезпечення.
- Важкість контролю за використанням: залежно від реалізації, контроль за використанням ліцензійного файлу може бути важким, особливо в випадку розповсюдження програмного забезпечення на багатьох пристроях або платформах.

3. Мережевий ліцензування:
   Переваги:
   - Контроль за використанням через мережу: мережевий ліцензійний сервер дозволяє контролювати використання програмного забезпечення на різних комп'ютерах в мережі, що дозволяє забезпечити високий рівень захисту ліцензій та управляти ліцензіями централізовано.
   - Гнучкість в управлінні: мережевий ліцензійний сервер може надавати різні параметри ліцензування для різних користувачів, такі як кількість одночасних використань, обмеження функціональності тощо, що дозволяє гнучко налаштовувати ліцензії відповідно до потреб клієнтів.
   - Легка активація та деактивація: користувачі можуть легко активувати та деактивувати ліцензії на різних комп'ютерах через мережевий ліцензійний сервер, що дозволяє ефективно управляти ліцензіями в разі зміни обладнання або потреби в зміні кількості використань.

   Недоліки:
   - Вимагає налаштування мережевого ліцензійного сервера: мережевий ліцензійний сервер потребує налаштування та управління, що може бути складним завданням для деяких організацій.
   - Залежність від мережі: використання мережевого ліцензування передбачає наявність функціонуючої мережі, що може бути обмеженням в деяких випадках, наприклад, при використанні програмного забезпечення в офлайн-режимі або на віддалених робочих місцях.
4. Хмарне ліцензування:
   Переваги:
   - Зручність у використанні: користувачі можуть легко активувати ліцензії через хмарний сервіс без необхідності встановлення та налаштування ліцензійних серверів.
   - Можливість віддаленого доступу: хмарне ліцензування дозволяє користувачам мати доступ до програмного забезпечення з різних пристроїв та місць, що забезпечує високий рівень мобільності.
   - Оновлення та підтримка: хмарні сервіси можуть забезпечувати автоматичні оновлення та підтримку програмного забезпечення, що дозволяє користувачам завжди мати останні версії та захищені відновлені від помилок.

   Недоліки:
   - Залежність від Інтернет-з'єднання: для використання хмарного ліцензування потрібне стабільне Інтернет-з'єднання, що може бути обмеженням в умовах зі слабким Інтернетом або відсутності доступу до Інтернету.
   - Конфіденційність даних: використання хмарного ліцензування передбачає зберігання даних ліцензій та використання програмного забезпечення на хмарних серверах, що може викликати обмеження з точки зору конфіденційності даних.

- Вартість: хмарне ліцензування може мати вищу вартість порівняно з іншими методами, особливо при великій кількості користувачів або великому обсязі використання [5].

Порівняльна характеристика локального, мережевого та хмарного методів:

- Активація та деактивація: всі три методи дозволяють активувати та деактивувати ліцензії відповідно до потреб користувачів, але мережеве та хмарне ліцензування можуть бути більш зручними, оскільки не вимагають налаштування ліцензійних серверів.
- Управління ліцензіями: мережеве та хмарне ліцензування надають більшу гнучкість та контроль над управлінням ліцензіями, оскільки дозволяють централізовано керувати ліцензіями на різних комп'ютерах або пристроях.
- Залежність від мережі: мережеве та хмарне ліцензування потребують наявності функціонуючої мережі, що може бути обмеженням в деяких випадках, тоді як локальне ліцензування нема таких обмежень і може бути використане в офлайн-режимі.
- Конфіденційність даних: локальне ліцензування зазвичай забезпечує вищий рівень конфіденційності даних, оскільки ліцензійні ключі та інформація про ліцензії зберігаються на локальних комп'ютерах або пристроях, тоді як мережеве та хмарне ліцензування вимагає передачі цих даних через мережу та зберігання їх на серверах, що може бути менш безпечним.
- Вартість: локальне ліцензування може бути більш економічним, оскільки не вимагає додаткових витрат на налаштування ліцензійних серверів або підписку на хмарні послуги. Мережеве та хмарне ліцензування можуть бути дорожчими, особливо при великому обсязі використання або багатокористувацькому середовищі.
- Доступність: локальне ліцензування може бути більш доступним в умовах з обмеженим або нестабільним Інтернет-з'єднанням, оскільки не вимагає постійного з'єднання з Інтернетом. Мережеве та хмарне ліцензування можуть бути менш доступними в таких умовах, оскільки вимагають стабільного Інтернет-з'єднання.

Узагальнюючи, локальне ліцензування може бути більш підходящим для офлайн-роботи, забезпечувати вищий рівень конфіденційності даних та бути економічно вигіднішим. Мережеве та хмарне ліцензування можуть бути більш зручними для управління ліцензіями та забезпечення централізованого контролю, але можуть мати деякі обмеження в доступності та безпеці даних. Остаточний вибір між різними методами ліцензування повинен враховувати конкретні потреби організації, включаючи розмір компанії, тип діяльності, доступність Інтернету, бюджет та безпекові вимоги.

Ось кілька прикладів програм, які дозволяють розробникам забезпечувати ліцензійне управління своїм програмним забезпеченням:

- License4J
- Thales Sentinel Licensing Development Kit (LDK)
- SafeNet Sentinel

Ці програми та рішення допомагають розробникам захистити своє програмне забезпечення від несанкціонованого копіювання, розповсюдження та використання, а також керувати ліцензіями та відстежувати використання своїх продуктів. Вони надають розробникам різноманітні можливості для налаштування ліцензійних моделей, активації, деактивації та відстеження ліцензій, а також захищають програмне забезпечення від зловживань та несанкціонованого використання.

License4J є одним з популярних програмних застосунків, який дозволяє розробникам забезпечувати захист та ліцензування свого програмного забезпечення. Він надає розробникам зручні та потужні інструменти для створення, керування та відстеження ліцензій для їх додатків.

Основні можливості License4J включають:

1. Створення ліцензій: License4J дозволяє розробникам створювати різні типи ліцензій, включаючи часові обмеження, кількість користувачів, обмеження функціональності та інші варіанти ліцензування.
2. Керування ліцензіями: Програма надає інструменти для керування ліцензіями, такі як генерація ліцензійних ключів, активація, деактивація, відновлення, скасування та перевірка статусу ліцензій.
3. Захист від копіювання: License4J використовує різні методи захисту від копіювання, такі як шифрування, підписи, хеш-коди та інші техніки, для запобігання несанкціонованого копіювання та розповсюдження програм.
4. Відстеження використання: Програма дозволяє розробникам відстежувати використання їх програм, включаючи кількість активацій, користувачів, дати та інші дані, для відслідковування ліцензій та контролю використання продуктів.
5. Кастомізація: License4J дозволяє налаштовувати вигляд та поведінку ліцензійних вікон, повідомлень про помилки, інтерфейсу користувача та інших аспектів програми.
6. Інтеграція: Програма надає API для інтеграції з програмним забезпеченням розробників, що дозволяє автоматизувати процеси створення, активації та відстеження ліцензій безпосередньо з програмного забезпечення.
7. Підтримка різних платформ: License4J підтримує різні платформи, включаючи Java, Android, .NET, C/C++ та інші, що робить його відповідним для розробників різних типів програмного забезпечення.
8. Локальна та серверна ліцензія: License4J дозволяє використовувати як локальну, так і серверну ліцензію для забезпечення захисту та управління ліцензіями на різних рівнях.
9. Підтримка різних видів ліцензування: License4J дозволяє використовувати різні види ліцензування, включаючи одноразову ліцензію, періодичну ліцензію, ліцензію з обмеженням функціональності та інші варіанти.

Загалом, License4J є потужним програмним засобом для захисту та ліцензування програмного забезпечення, який надає розробникам багато можливостей для створення та управління ліцензіями своїх додатків. Він має велику кількість функцій, гнучкість налаштувань та підтримку різних платформ, що робить його популярним вибором для розробників, які шукають ефективний спосіб захистити своє програмне забезпечення від несанкціонованого використання [6].

Хоча License4J має багато переваг, включаючи багатий набір функцій та підтримку різних платформ, він також має кілька недоліків. Деякі з них включають:

1. Вартість: License4J є комерційним програмним забезпеченням, що може бути високим за вартістю, особливо для невеликих розробників або стартапів з обмеженим бюджетом.
2. Складність налаштування: Налаштування License4J може бути складним процесом, особливо для новачків, які не мають досвіду у роботі з ліцензуванням програмного забезпечення.
3. Залежність від стороннього рішення

Використання License4J або іншого готового програмного застосунку для ліцензування означає, що розробник стає залежним від стороннього рішення та підтримки від постачальника програмного забезпечення.

Обмежені можливості налаштування: Готові програмні застосунки для ліцензування можуть мати обмежені можливості налаштування, що може бути неприйнятним для деяких розробників, які вимагають високого рівня налаштування та кастомізації відповідно до їхніх вимог.

Відсутність повного контролю: Використання готових програмних застосунків може обмежити розробника в можливостях повного контролю над ліцензійним управлінням своїм програмним забезпеченням. Це може бути проблемою, особливо для розробників, які мають специфічні потреби або вимоги щодо ліцензування.

Можливість взлому: Жодне програмне забезпечення не може гарантувати 100% захист від взлому. Готові програмні застосунки для ліцензування також можуть бути піддані ризику взлому, особливо якщо не вжиті додаткові заходи безпеки.

Оновлення та підтримка: Готові програмні застосунки для ліцензування можуть вимагати постійного оновлення та підтримки від постачальника програмного забезпечення. Це може бути витратним та вимагати додаткових зусиль від розробника.

Відсутність гнучкості: Готові програмні застосунки можуть бути менш гнучкими в порівнянні з власним рішенням ліцензування, оскільки вони можуть мати встановлені обмеження та правила, які не завжди відповідають потребам конкретного розробника.

Висновки. Отже, перед використанням License4J або іншого готового програмного застосунку для ліцензування, розробник повинен ретельно зважити на переваги та недоліки такого рішення, врахувати свої вимоги та потреби, а також оцінити ризики та витрати, пов'язані з використанням готового програмного забезпечення. Можливо, в деяки их випадках розробникам варто розглянути альтернативні варіанти, такі як розробка власного рішення ліцензування з нуля або використання інших рішень з відкритим вихідним кодом, які можуть забезпечити більший рівень гнучкості та контролю.

Крім того, важливо пам'ятати, що ефективне ліцензування програмного забезпечення потребує комплексного підходу, включаючи не тільки технічні засоби, такі як License4J або інші готові програмні застосунки, але й правильну стратегію ліцензування, відповідний юридичний контекст та заходи безпеки. Розробникам слід ретельно проаналізувати всі аспекти ліцензування свого програмного забезпечення перед вибором відповідного рішення.

Загалом, готові програмні застосунки для ліцензування, такі як License4J, можуть бути корисними рішеннями для деяких розробників, які шукають швидкий та простий спосіб реалізації ліцензійного управління. Однак, вони також мають свої недоліки, такі як обмежена гнучкість, можливість взлому та залежність від підтримки постачальника програмного забезпечення. Розробникам слід ретельно розглянути ці фактори перед вибором рішення для ліцензування свого програмного забезпечення. Загальний висновок щодо захисту та ліцензування програмного забезпечення полягає в тому, що немає універсального рішення, яке б відповідало всім випадкам. Ефективність різних методів захисту та ліцензування залежить від рівня загроз, яким піддається програмний продукт, та потреб розробника та користувачів.

Список використаних джерел

11. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC press.
12. Collberg, C., & Nagra, J. (2009). Surreptitious software: Obfuscation, watermarking, and tamperproofing for software protection. Addison-Wesley.
13. Chandra, P., & Arora, R. (2018). A Comprehensive Survey on Software Protection and Licensing Techniques. International Journal of Computer Applications, 181(47), 8-15.
14. Zhou, L., Deng, H., & Varadharajan, V. (2015). Software protection and licensing: A survey. Journal of Systems and Software, 107, 166-185.
15. Balasubramanian, S., & Bhowmik, S. (2019). A survey on software protection techniques: from traditional to modern approaches. International Journal of Information Technology, 11(1), 87-96.
16. License4J \\ Режим доступу: https://www.license4j.com/ (останнє звернення 29.03.2023р.)

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ПАЛАГУТИ К.О.

МОВА DART ТА ФРЕЙМВОРК FLUTTER, ЯК ІНСТРУМЕНТ РОЗРОБКИ МОБІЛЬНИХ ДОДАТКІВ

КАС'ЯН Д., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Стаття присвячена вивченню мови Dart та фреймворку Flutter як інструменту для розробки мобільних додатків. У статті представлені основні характеристики мови та фреймворку, їх переваги та недоліки, а також результати порівняння з іншими інструментами розробки. Наведено приклади відомих мобільних додатків, які використовують Dart та Flutter. Висновки, зроблені на основі досліджень, підтверджують, що мова Dart та фреймворк Flutter є потужним та зручним інструментом для розробки мобільних додатків.

The article explores the use of Dart language and Flutter framework for mobile app development. The history and main characteristics of Dart and Flutter are described, as well as the advantages and disadvantages of using them in mobile app development. The article also includes a comparison of Dart and Flutter with other mobile app development tools and showcases examples of popular mobile apps developed using this language and framework. Overall, this article aims to provide a comprehensive understanding of Dart and Flutter as powerful tools for mobile app development.

Актуальність статті полягає в тому, що розробка мобільних додатків стала надзвичайно популярною в останні роки, і з'явилася потреба в ефективному та зручному інструменті для їх створення. Мова Dart та фреймворк Flutter використовуються в широкому колі проектів, оскільки забезпечують швидкість розробки, ефективність та зручність у використанні. Ця стаття присвячена дослідженню можливостей, переваг та недоліків мови та фреймворку для розробки мобільних додатків.

Метою статті є розгляд мови програмування Dart та фреймворку Flutter, як інструментів розробки мобільних додатків. Опис основних характеристик мови та фреймворку, їх переваги та недоліки. Аналіз досліджень з використанням Dart та Flutter у розробці мобільних додатків.

Завданнями статті є:

- Дослідження історії розвитку мови Dart та фреймворку Flutter.
- Опис основних характеристик мови та фреймворку, що використовуються для розробки мобільних додатків.
- Аналіз переваг та недоліків використання мови та фреймворку для розробки мобільних додатків.
- Опис основних елементів Flutter, що використовуються для розробки мобільних додатків.
- Порівняння мови та фреймворку з іншими інструментами розробки мобільних додатків.
- Дослідження використання мови Dart та фреймворку Flutter у відомих мобільних додатках.
- Формулювання висновків про ефективність використання мови Dart та фреймворку Flutter для розробки мобільних додатків.

Об'єктом статті є мова програмування Dart та фреймворк Flutter, як інструменти для розробки мобільних додатків, їх основні характеристики та переваги та недоліки використання.

Результатом статті є деталізоване пояснення принципів використання мови Dart та фреймворку Flutter як інструменту для розробки мобільних додатків.

Виклад основного матеріалу.

Розвиток мови Dart та фреймворку Flutter.

Мова Dart була розроблена компанією Google у 2011 році як заміна JavaScript для веб-розробки. Її основні принципи - ефективність, швидкість, надійність, простота та гнучкість. Ці принципи дозволяють розробникам швидко створювати високоякісні програми, забезпечуючи зручність та надійність.

Flutter, фреймворк для розробки мобільних додатків, був анонсований Google у 2017 році. Він базується на мові Dart і відразу здобув популярність серед розробників мобільних додатків. Flutter дозволяє створювати привабливі та динамічні інтерфейси користувача та має багато інструментів для розробки мобільних додатків.

Згодом Flutter було розширено на платформи веб-розробки, настільні та вбудовані операційні системи , тим самим збільшив можливості користувачів. У 2019 році Google оголосив про те, що Flutter став стабільним та готовим для продакшн-рівня.

Зараз Dart та Flutter є загальнодоступними інструментами, які підтримує Google та широко використовуються в індустрії розробки мобільних додатків та веб-додатків.

Мова Dart та фреймворк Flutter мають свої унікальні характеристики та переваги, які роблять їх популярними серед розробників додатків.

Основні характеристики мови Dart:

- *Швидкість та ефективність*: Dart має високу швидкість роботи, що дозволяє створювати високоякісні та ефективні програми.
- *Простота*: Dart має чіткий та простий синтаксис, що робить його легким для вивчення та розуміння.
- *Надійність*: Dart має розгалужену типізацію, що дозволяє виявляти помилки під час компіляції.
- *Асинхронне програмування*: Dart має вбудовану підтримку асинхронного програмування, що дозволяє ефективно використовувати мережеві запити та інші операції, які потребують часу.
- *JIT та AOT компіляція*: Dart підтримує як компіляцію в Just-In-Time (JIT) режимі для швидкого розвитку та відлагодження коду, так і Ahead-Of-Time (AOT) компіляцію для ефективної роботи в продукції.
- *Підтримка null-безпеки*: Dart має вбудовану підтримку null-безпеки, що дозволяє запобігати помилкам, пов'язаним з нульовими значеннями.

Основні характеристики фреймворку Flutter:

- *Гнучкість*: Flutter дозволяє компілювати код однаково просто на будь-яку платформу незалежно від розмірів та типів пристроїв.
- *Кросплатформеність*: Фреймворк Flutter має можливість одночасного вибору декількох платформ, та адаптує весь код для всіх платформ у реальному часі.
- *Відкритий код*: Flutter є відкритим проектом, що дозволяє розробникам робити внески для його розвитку та підтримки.
- *Widget-орієнтованість*: Flutter базується на концепції віджетів (widgets), що дозволяє створювати складні та динамічні інтерфейси користувача.
- *Привабливий дизайн та анімації*: Flutter має вбудовану підтримку створення ефектних дизайнів та анімацій, що дозволяє створювати додатки з високоякісним користувацьким інтерфейсом.

Переваги та недоліки використання мови та фреймворку для розробки мобільних додатків

Переваги використання мови Dart:

- *Швидкість розробки*: Dart має простий та зрозумілий синтаксис, що дозволяє розробникам швидко створювати нові функції та модулі.

- *Ефективність розробки*: Dart має вбудовану підтримку асинхронного програмування та компіляцію в JIT режимі, що дозволяє розробникам швидко відлагоджувати та тестувати код.
- *Інтероперабельність з JavaScript*: Dart має можливість взаємодіяти з кодом JavaScript, що дозволяє використовувати його в змішаному середовищі зі стандартними веб-технологіями.

Переваги використання фреймворку Flutter:

- *Швидкість розробки*: Flutter дозволяє швидко створювати складні та динамічні інтерфейси користувача завдяки використанню концепції віджетів.
- *Ефективність розробки*: Flutter має вбудовану підтримку привабливих дизайнів та анімацій, що дозволяє розробникам створювати додатки з високоякісним користувацьким інтерфейсом.
- *Гнучкість*: Flutter має вбудовану підтримку різних платформ, що дозволяє розробляти мобільні додатки для різних операційних систем, а також веб-додатки та додатки для настільних операційних систем.

Недоліки використання мови Dart та фреймворку Flutter:

- *Розмір додатку*: збільшений розмір додатку, порівняно з додатками, написаними з використанням нативних інструментів розробки.
- *Нестабільність*: деякі розробники відмічають проблеми зі стабільністю Flutter-додатків, особливо під час взаємодії зі сторонніми бібліотеками.
- *Швидкість розробки*: хоча Flutter дозволяє розробляти додатки для різних платформ з використанням одного коду, це може бути менш ефективним для простих додатків, де швидкість розробки є більш важливою, ніж кросплатформеність.
- *Обмежена підтримка*: Flutter підтримується Google, але існує шанс того, що додаток не отримає підтримки в майбутніх версіях фреймворку.
- *Відсутність інтеграції з деякими сервісами*: Flutter має обмежену підтримку деяких сервісів, таких як Apple Pay та Google Maps.
- *Невелика кількість розробників*: Flutter ще не такий популярний, як деякі інші фреймворки, такі як React Native або Xamarin. Це може призвести до того, що знайти досвідченого розробника може бути складно.
- *Обмеження використання деяких стандартних бібліотек*: Flutter має свої власні бібліотеки та інструменти, які можуть бути обмежені в порівнянні зі стандартними бібліотеками. Це може призвести до того, що деякі функції можуть бути складніші для реалізації.

Опис основних елементів Flutter для розробки мобільних додатків. Flutter – це фреймворк від Google для розробки кросплатформених мобільних додатків. Основною метою Flutter є забезпечення швидкої та ефективної розробки мобільних додатків з високоякісним користувацьким інтерфейсом. Ось деякі з основних елементів Flutter для розробки мобільних додатків:

- Widgets: Всі елементи UI у Flutter є widgets. Widgets можуть бути розташовані один в одному, щоб створювати більш складний користувацький інтерфейс. Є два види widgets: StatelessWidget та StatefulWidget. StatelessWidget - це безстаний віджет, що не може змінювати свій стан. StatefulWidget - це віджет, що може змінювати свій стан.
- Layouts: Layouts використовуються для організації widgets на екрані. Flutter надає різноманітні layouts, такі як Column, Row, Stack, та інші, які можна використовувати для створення складніших користувацьких інтерфейсів.
- Themes: Flutter надає можливість змінювати тему додатку, щоб він мав однаковий дизайн на різних платформах.

- Animations: Flutter надає потужні інструменти для створення анімацій та ефектів. Це допомагає зробити користувацький інтерфейс більш привабливим та динамічним.
- Packages: Flutter має велику кількість packages, які можуть допомогти у вирішенні різноманітних задач. Наприклад, є пакети для роботи з базами даних, роботи з графікою, мережевого з'єднання та інших.

Окрім відомих елементів, таких як текстові поля, кнопки та вікна, Flutter також має багато інших елементів, які роблять розробку мобільних додатків зручною та ефективною. Наприклад, Flutter має багато видів списків, які дозволяють легко відображати велику кількість даних на екрані без нагромадження інтерфейсу користувача.

Крім того, Flutter має можливості для розробки анімацій та переходів, що дозволяє створювати більш динамічний та привабливий інтерфейс користувача. Наприклад, з допомогою Flutter можна створити анімацію, яка з'являється при відкритті нової сторінки додатку, або створити анімацію для плавного відкриття випадаючого меню.

Загалом, Flutter має багато елементів, які дозволяють розробникам швидко створювати ефективні мобільні додатки зі зручним та привабливим інтерфейсом користувача. Flutter є одним з популярних мультиплатформних фреймворків для розробки мобільних додатків.

Цей фреймворк відрізняється від інших мультиплатформних рішень таких як React Native, Xamarin та Ionic, принциповою відмінністю, яка полягає в тому, що Flutter складається зі своєї власної віртуальної машини Flutter Engine, а не використовує вбудовані компоненти мобільних операційних систем.

Ось деякі порівняння Flutter з іншими мультиплатформними фреймворками:

React Native: React Native використовує JavaScript для написання додатків, тоді як Flutter використовує Dart. Flutter надає більшу швидкість розробки і більш високу продуктивність, оскільки він має вбудовану віртуальну машину.

Xamarin: Xamarin використовує мову програмування C# для написання додатків. Flutter пропонує більше готових компонентів та ширший вибір сторонніх бібліотек, що дозволяє розробникам більш ефективно працювати.

Ionic: Ionic використовує HTML, CSS та JavaScript для розробки додатків. Flutter забезпечує кращу продуктивність і швидкість розробки, оскільки він не потребує використання веб-технологій та забезпечує більшу швидкість виконання коду.

Всі ці переваги роблять Flutter одним з найбільш привабливих мультиплатформних фреймворків для розробки мобільних додатків.

Використання мови Dart та фреймворку Flutter у відомих мобільних додатках

Dart та Flutter стали популярними серед розробників мобільних додатків завдяки своїй ефективності та простоті використання. Ці інструменти успішно використовуються в розробці відомих мобільних додатків, наприклад:

- *Alibaba* використовує Flutter для створення мобільних додатків для своїх клієнтів. Flutter дозволяє створювати красиві та ефективні інтерфейси користувача, що є важливим критерієм для успіху бізнесу.
- *Google Ads* також використовує Flutter для розробки своєї мобільної платформи, яка використовується мільйонами користувачів по всьому світу. За словами команди розробників Google Ads, використання Flutter дозволяє значно прискорити розробку мобільної платформи та зменшити кількість помилок в коді.
- *Reflectly* - це популярний додаток для медитації та розмірковувань, який також був розроблений з використанням Flutter. Додаток отримав високі оцінки в магазинах додатків та став дуже популярним завдяки своєму ефективному та простому інтерфейсу.
- *Hookle* - соціальна медіа-платформа для підприємців, що дозволяє керувати кількома соціальними мережами в одному місці.
- *Coach Yourself* - додаток для саморозвитку та досягнення особистих цілей.

Таким чином, використання мови Dart та фреймворку Flutter стає все більш популярним у розробці мобільних додатків

Висновки. Зазначена вище аналітика доводить, що мова Dart та фреймворк Flutter - це ефективні інструменти для розробки мобільних додатків. Основні переваги включають в себе швидкість розробки, платформно-незалежний підхід, відмінну документацію та підтримку від розробників Google.

Хоча використання мови та фреймворку має свої недоліки, які включають в себе більший обсяг пам'яті та час розгортання, ці проблеми можуть бути легко вирішені за допомогою оптимізації та інших підходів.

Порівняння з іншими інструментами розробки підтверджує, що Dart та Flutter відрізняються швидкістю та універсальністю, які відображаються в успішних додатках.

Отже, можна зробити висновок, що Dart та Flutter - це відмінні інструменти розробки мобільних додатків, які можуть бути використані для створення високоякісних та ефективних додатків для різних платформ.

Список використаних джерел

1. Statista. (2022). Number of smartphone users worldwide from 2016 to 2021. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
2. Pratik, R. (2019). What is Mobile Application Development? Benefits, Types, Frameworks & More. Retrieved from https://www.upgrad.com/blog/what-is-mobile-application-development/
3. Flutter. (2022). Why Flutter? Retrieved from https://flutter.dev/why-flutter/
4. Savan, V. (2020). Flutter Vs React Native: Which One Should You Choose for Mobile App Development? Retrieved from https://www.imaginovation.net/blog/flutter-vs-react-native-which-one-should-you-choose-for-mobile-app-development/
5. Flutter. (2022). Widgets. Retrieved from https://flutter.dev/docs/development/ui/widgets
6. Flutter. (2022). Material design widgets. Retrieved from https://flutter.dev/docs/development/ui/widgets/material
7. Flutter. (2022). Cupertino (iOS-style) widgets. Retrieved from https://flutter.dev/docs/development/ui/widgets/cupertino
8. Savan, V. (2020). Flutter Vs React Native: Which One Should You Choose for Mobile App Development? Retrieved from https://www.imaginovation.net/blog/flutter-vs-react-native-which-one-should-you-choose-for-mobile-app-development/
9. Dremio. (2018). Dart vs. Java: A Comparison for Server-Side Development. Retrieved from https://www.dremio.com/dart-vs-java-a-comparison-for-server-side-development/
10. Team Flutter. (2020). Flutter for Web: A Complete Guide to Create & Run Web Apps. Retrieved from https://www.simform.com/flutter-for-web-development/.
11. Flutter. (2022). Flutter Showcase. Retrieved from https://flutter.dev/showcase
12. React Native vs Flutter: що обрати для кросплатформної розробки? (2022) Retrieved from https://wezom.com.ua/ua/blog/react-native-vs-flutter-chto-vybrat-dlja-krossplatformennoj-razrabotki
13. Порівняння Ionic і Flutter для розробки мобільних і прогресивних додатків (2022) Retrived from https://senior.ua/articles/porvnyannya-ionic--flutter-dlya-rozrobki-moblnih--progresivnih-dodatkv

Робота виконана під науковим керівництвом к.пед.н, доцента
КОТЕНКО Н. О.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ОНЛАЙН-ГАМАНЦЯ

КАТКОВ Н., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

На теперішній час онлайн-платежі стали дуже поширеними і досить складно уявити день без них. І для цього люди використовують різні способи оплати, такі як дебетова або кредитна картка, електронний гаманець, онлайн банкінг, тощо. Але таке поширене використання не гарантує велику безпеку. Саме тому у даній статті розглядається система захисту інформації для онлайн-гаманця, поширені методики захисту, безпека даних, вирішення проблем безпеки пов'язані з онлайн-платежами.

Nowadays, online payments have become very common and it is quite difficult to imagine a day without them. And for this, people use various payment methods, such as debit or credit card, e-wallet, online banking, etc. But such widespread use does not guarantee much security. That is why this article discusses the information protection system for an online wallet, common protection methods, data security, and solutions to security problems related to online payments.

Актуальність. Система захисту інформації онлайн-гаманця є критично важливою для забезпечення безпеки коштів користувачів. Саме тому вона повинна включати наступні методи забезпечення захисту, такі як шифрування даних, багаторівневий доступ, захист від шахрайства, автоматичні оповіщення, аудит, можливість резервного копіювання.

Але навіть і це не може повністю гарантувати безпеку даних при використанні онлайн-гаманця, оскільки також існують ризики, що пов'язані з діями користувачами.

Тому для забезпечення надійного захисту інформації користувачів та уникненню втрат коштів внаслідок крадіжок або інших злочинних дій необхідно заздалегідь розробити вимоги на стороні системи та користувача.

Метою статті є дослідження основних загроз безпеки інформації, які несуть загрозу для онлайн-гаманця.

Об'єктом дослідження є розробка основних вимог для забезпечення безпеки інформації онлайн-гаманця.

Предмет дослідження – вимоги для забезпечення безпеки інформації.

Аналіз попередніх досліджень. Дослідженню розробки безпеки інформації онлайн-гаманця присвячено праці закордонних науковців: Sameer Saxena (Самір Саксена), Sonali Vyas (Соналі В'яс), B. Suresh Kumar (Б. Суреш Кумар), Shaurya Gupta (Шаурья Гупта), Tracey Caldwell (Трейсі Колдвелл), Noe Elisa (Ное Еліза), Longzhi Yang (Лунжи Ян), Fei Chao (Фей Чао), Yi Cao (І Цао) та ін.

Виклад основного матеріалу. Онлайн-гаманець, також відомий як цифровий гаманець або електронний гаманець, є наступним рівнем зручності для споживачів, яким потрібні простіші та швидші способи оплати. Електронні гаманці фактично використовуються вже багато років, особливо в Європі, де цифрові гаманці є дуже сильно поширеними. У Сполучених Штатах популярність електронного гаманця експоненціально зросла через пандемію, що пов'язана з COVID-19. Саме тоді, стала необхідність споживачами проводити покупки без фізичного контакту з картками та платіжними терміналами [1].

Але так само, як онлайн-гаманці пропонують зручність, вони також пропонують ще одну приховану можливість для кмітливих хакерів і кіберзлочинців спробувати викрасти ваші конфіденційні, фінансові дані. Тож постає питання: чи безпечно використовувати онлайн-гаманці чи просто не варто ризикувати? Відповідь залежить від того, як вирішується питання захисту інформації для онлайн-гаманців [2].

Є багато речей за допомогою яких відбувається покращення безпеки для онлайн-гаманця, від здорового глузду до використання програмного забезпечення онлайн-безпеки.

До основних вимог із забезпечення безпеки системи захисту інформації онлайн-банкінгу можна віднести:

- Конфіденційність. Це властивість інформації, яка означає, що доступ до неї обмежений лише тими особами, які мають на це дозвіл. Це означає, що конфіденційна інформація не повинна розголошуватися або передаватися третім особам без згоди власника цієї інформації. Конфіденційність є важливою для багатьох сфер життя, таких як бізнес, медицина, право та інформаційна безпека. Наприклад, компанії зберігають конфіденційну інформацію про своїх клієнтів, включаючи особисті дані, номер телефону, картки, договору, фінансову інформацію та іншу конфіденційну інформацію. Збереження конфіденційної інформації має бути забезпечено шляхом використання різних методів захисту, таких як шифрування даних, контроль доступу та інші методи захисту.
- Доступність. Доступність означає, що інформація або система повинні бути доступні користувачам, які мають на це дозвіл, та повинні функціонувати вірно та швидко. Наприклад, якщо відбувається відмова в обслуговуванні (Denial of Service - DoS) на веб-сайті, то це означає, що сайт стає недоступним для користувачів, що може призвести до втрати бізнесу та негативного впливу на репутацію компанії. Тому, забезпечення доступності є важливою складовою безпеки інформації,.
- Цілісність. Цілісність означає, що інформація повинна зберігатися в тому ж стані, в якому вона була збережена, та не повинна бути підроблена або змінена без належного дозволу. Наприклад, у банківській сфері, де зберігається велика кількість конфіденційної інформації, щоб забезпечити цілісність даних можуть використовуватися методи цифрової безпеки. Захищеність інформації за тріадою CIA зображено на рисунку 1 [3].

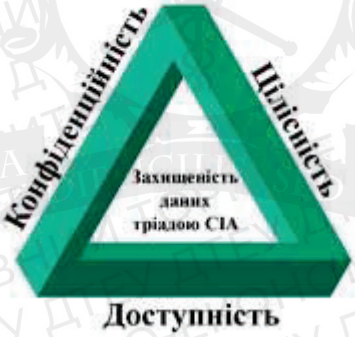


Рис. 1. Тріада CIA

- Шифрування даних: Всі дані, які передаються між клієнтом та сервером, повинні бути зашифровані. Для забезпечення шифрування зазвичай використовують протоколи шифрування, такі як SSL (Secure Socket Layer) або TLS (Transport Layer Security). Приклад забезпечення шифрування інформації онлайн-гаманця зображено на рисунку 2.
- Багаторівневий доступ: Доступ до гаманця повинен бути обмеженим за допомогою паролів, PIN-кодів, біометричних даних, таких як відбиток пальця або розпізнавання обличчя. Додатково можна встановлювати додаткові перевірки, такі як одноразові коди підтвердження (OTP).
- Захист від шахрайства: Система захисту повинна вміти виявляти аномальну поведінку системи та блокувати небезпечні дії, такі як спроби викрадення аккаунту, фішингові атаки та інші види шахрайства.
- Автоматичні оповіщення: Система повинна надсилати сповіщення користувачам про будь-які незвичні дії, такі як видалення коштів, зміна пароля або інших важливих налаштувань.

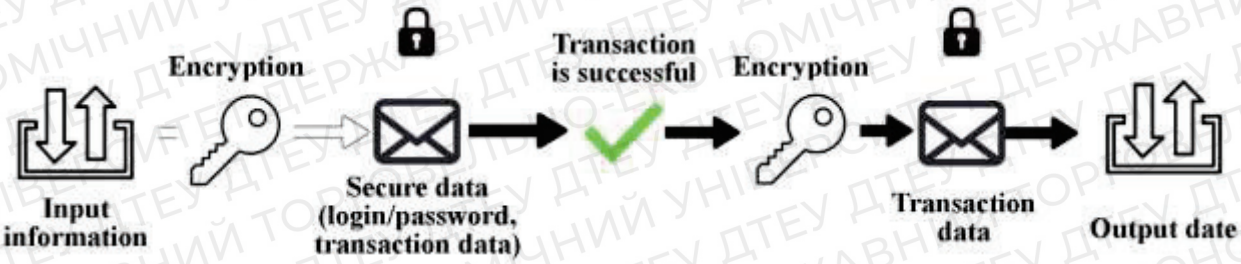


Рис. 2. Приклад шифрування інформації онлайн-гаманця

- Аудит: Система повинна вести журнал дій, які виконуються користувачами та адміністраторами. Це дозволить відстежувати події та реагувати на можливі проблеми. Також, при наявності аудиту в системі сильно спрощується пошук причин взлому, несанкціонованого доступу, тощо.
- Резервне копіювання: Система повинна мати можливість резервного копіювання, щоб у випадку втрати даних користувачів можна було відновити їх[4].

Вище було наведено приклад захисту системи онлайн-банкінгу. Але не варто забувати про безпеку з боку користувача, до якої відносяться:

- Завжди тримати пристрій заблокованим та захищеним графічним ключем/паролем/біометричними даними.
- Використовувати для захисту доступу до онлайн-банкінгу паролю з мінімальною кількість символів – вісім або десять. Також пароль має складатися з літер (верхнього та нижнього регістру), цифр та символів.
- Не використовувати систему онлайн-банкінгу при використанні загальнодоступної мережі.
- Використання додаткового програмного забезпечення для захисту даних. До таких програмних продуктів можна віднести додаткову двофакторну автентифікацію[5].

Модель загроз мобільної платіжної програми повинна враховувати загрози, які спрямовані проти основних компонентів екосистеми мобільних додатків, що підкреслює «межі довіри» (на рисунку зображено червоним пунктиром) та де найбільше загроз відбувається [6]. Загальна модель загроз зображена на рисунку 3.

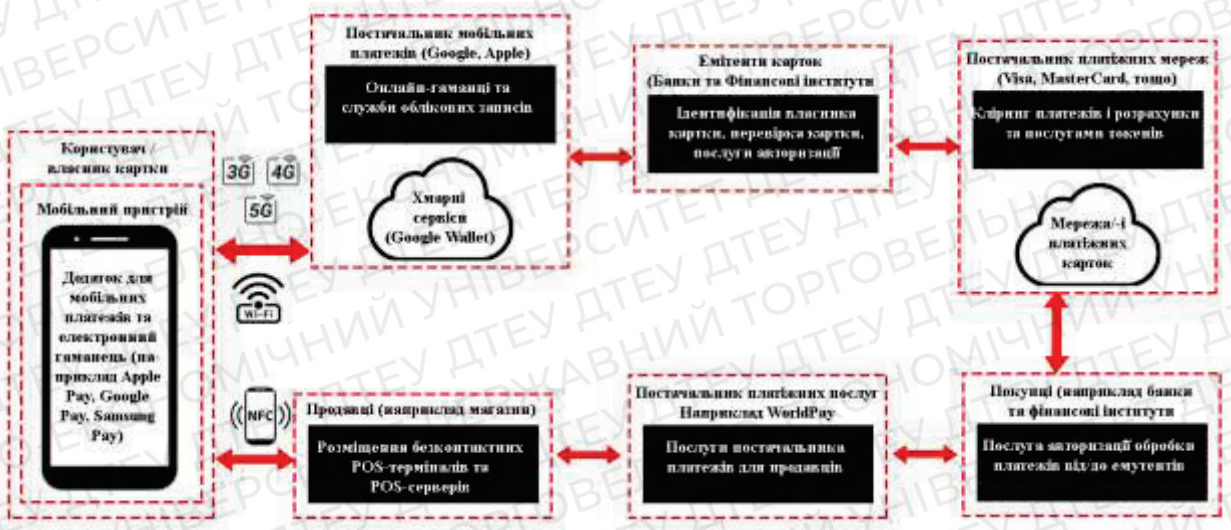


Рис. 3. Модель загроз

Згідно рисунку 3 проаналізуємо загрози та вектор атак на основні компоненти платіжних систем (табл. 1).

Таблиця 1

Загрози та вектор атак на основні компоненти платіжних систем

Компонент	Загроза та вектор атаки	Опис
Користувач/ власник гаманця	Фішинг та соціальна інженерія.	Ці атаки спрямовані на користувача за допомогою фішингових електронних листів і соціальної інженерії з використанням різних комунікаційних каналів (наприклад, телефон, електронна пошта, SMS).
	Встановлення шкідливого ПЗ.	Зазвичай маскується під легитивним ПЗ.
Пристрої	Несанкціонований доступ до втраченого або вкраденого пристрою.	Внаслідок необачного користування пристроєм можлива втрата конфіденційної інформації.
	Встановлення шкідливого ПЗ.	Зазвичай маскується під легитивним ПЗ.
Системи платежів та онлайн-гаманці	Зворотне проектування вихідного коду програми.	Зазвичай це перший метод, що використовується зловмисниками для вивчення цілі.
	Втручання в мобільну платіжну програму.	Зазвичай супроводжується несанкціонованим доступ, в разі якого порушується робота системи.
	Експлуатація вразливостей програми мобільних платежів.	Після вивчення цілі відбувається використання вразливостей для втручання в роботу системи.
	Встановлення руткітів/шкідливих програм.	Зазвичай являється фінальним етапом для приховування слідів втручання.

Продовження табл. 1

	Права доступу до мобільної операційної системи.	Використовується для зміни роботи системи, або отримання даних, що не відповідають правам доступу.
Торговці	Завантаження шкідливих програм POS на термінал безконтактної оплати POS	Встановлення шкідливого ПЗ для відслідковування за діями.
	Атаки MiTM на безконтактний POS-термінал і підключення до POS-сервера	Спеціальний тип атаки, що спрямований на термінали і подальше його зараження.
	Естафетні атаки на безконтактний термінал POS із підтримкою NFC	Після зламу першого терміналу, відбувається почергово злам усіх наступних терміналів.
Постачальники платіжних послуг	Компрометація платіжних систем	Націлено на шлюзи PSP.
	Компрометація підключення даних	Зловмисники можуть спробувати використати незахищені з'єднання (наприклад, відсутність примусового забезпечення безпечних з'єднань (SSL/TLS, VPN) для проведення таких атак, як MiTM, для підробки конфіденційних даних під час передачі даних від продавця.
Постачальники хмарних сервісів	Злам конфіденційних даних власника картки.	Викрадення облікових даних.
	Компрометація даних токен-сервісів	Унеможливлення шифрування та дешифрування даних.
	DDoS-атаки	Блокування доступу.

Проаналізуємо темп зростання кількості транзакцій з року в рік. Так, згідно з прогнозами цифрового ринку, до 2027 року за таких темпів ринок може зрости до 1 трильйонів доларів США, що порівняно з 2022 роком становить 130% (рисунок 4) [7].

Рис. 4. Загальний обсяг мобільних платежів

Висновки. Отже, в даній статті розглянуто важливість захисту інформації систем онлайн-гаманця. Захист інформації онлайн-гаманця є критично важливою задачею, оскільки він містить фінансову інформацію та приватні дані користувача, які можуть бути скомпрометовані або використані неправомірно. Це пов'язано як з недостатньою захищеністю онлайн-гаманців на стороні сервера, так і з діями користувачів через недостатню обізнаність в сфері захисту інформації.

Список використаних джерел

17. Survey on Online Electronic Paymentss Security \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/8701353/authors#authors (останнє звернення 19.03.2023р.)
18. A framework of blockchain-based secure and privacy-preserving E-government system \\ Режим доступу: https://link.springer.com/article/10.1007/s11276-018-1883-0 (останнє звернення 19.03.2023р.)
19. Основи інформаційної безпеки\\ Режим доступу: https://naurok.com.ua/informaciyna-bezpeka-247508.html (останнє звернення 19.03.2023р.)
20. How to Secure Your Digital Wallet \\ Режим доступу: https://www.mcafee.com/blogs/internet-security/how-to-secure-your-digital-wallet/ (останнє звернення 20.03.2023р.)
21. How safe are eWallets? How to Protect Your eWallet\\ Режим доступу: https://www.kaspersky.com/resource-center/threats/is-your-ewallet-safe (останнє звернення 20.03.2023р.)
22. Security of Mobile Payments and Digital Wallets \\ Режим доступу: https://www.mobeyforum.org/wp-content/uploads/2017/01/WP2016-3-1-4-Mobile-Payments-Security-002.pdf (останнє звернення 20.03.2023р.)
23. How to Build a Mobile Wallet App: CHI Software's Advice \\ Режим доступу: https://chisw.com/blog/how-to-make-a-digital-e-wallet-app/ (останнє звернення 20.03.2023р.)

Робота виконана під науковим керівництвом д.е.н., процесора
ТОКАРЯ В.В.

ДОСЛІДЖЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АДМІНІСТРУВАННЯ РОЗДРІБНОЇ ТОРГІВЛІ

КОЗИРЄВ Д., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови та функціонування інформаційно-управляючої системи роздрібної торгівлі. Проаналізовано плюси та мінуси різних підходів. А також проведено аналіз вимог до додатку з точки зору розробника

The article considers the basic principles of building and functioning of the information and management system of retail trade. Pros and cons of different approaches are analyzed. An analysis of the application requirements from the developer's point of view was also carried out

Актуальність. Роздрібна торгівля є важливою складовою економіки, а програмне забезпечення є невід'ємною частиною її функціонування. З розвитком технологій та збільшенням конкуренції на ринку, більше та більше роздрібних підприємств розглядають можливість використання програмного забезпечення для автоматизації своїх процесів та покращення управління бізнесом. Стаття пропонує детальний аналіз різних видів програмного забезпечення для адміністрування роздрібної торгівлі та надає читачам можливість підібрати найкращий варіант для свого бізнесу. У статті проаналізовані переваги та недоліки різних програмних продуктів, що дозволяє читачам зробити обґрунтований вибір. Крім того, стаття враховує специфіку роздрібної торгівлі в Україні та за кордоном, що робить її цінним джерелом інформації для представників бізнесу та фахівців з програмного забезпечення.

Одним з авторитетних джерел на цю тему є стаття «Retail Management Software: An Overview» авторів Nupur Biswas та Sanjib Kumar Biswas, опублікована в журналі International Journal of Advanced Research in Computer Science and Software Engineering в грудні 2014 року. У цій статті автори висвітлюють важливість програмного забезпечення для роздрібної торгівлі і проводять аналіз різних типів програмного забезпечення, що використовуються для управління роздрібною торгівлею. Одним з ключових висновків тієї статті є те, що ефективне програмне забезпечення може значно поліпшити продуктивність та прибутковість бізнесу в галузі роздрібної торгівлі.

Nupur Biswas зазначає, що ефективне програмне забезпечення для управління роздрібною торгівлею є ключовим інструментом для роздрібних продавців, які прагнуть підвищити ефективність і прибутковість свого бізнесу. За допомогою правильного програмного забезпечення роздрібні торговці можуть керувати всім, починаючи від інвентаризації та транзакцій у торгових точках до даних про клієнтів і маркетингових кампаній. Автоматизуючи багато з цих завдань, програмне забезпечення для управління роздрібною торгівлею може допомогти підприємствам заощадити час, зменшити кількість помилок і підвищити загальну продуктивніст ь[1].

Метою статті є проведення аналізу програмного забезпечення, яке використовується для адміністрування роздрібної торгівлі, з метою визначення його можливостей та ефективності в управлінні бізнесом. Крім того, стаття спрямована на висвітлення ключових функцій та характеристик програмного забезпечення, яке допомагає роздрібним торговим підприємствам управляти своїм бізнесом більш ефективно та знижувати витрати.

Об'єктом дослідження є програмне забезпечення, яке використовується для адміністрування роздрібної торгівлі. Конкретніше, стаття досліджує різні типи програмного забезпечення, їх функції та можливості, переваги та недоліки, а також ключові фактори, які слід враховувати при виборі програмного забезпечення для управління роздрібною торгівлею.

Предметом дослідження є роздрібна торгівля, яка потребує програмного забезпечення для оптимізації управління її бізнес-процесами.

Виклад основного матеріалу. В сучасному світі програмне забезпечення є невід'ємною частиною бізнесу, особливо у сфері роздрібної торгівлі. Адміністрування роздрібної торгівлі вимагає використання різноманітних програмних рішень для забезпечення ефективного та безпечного функціонування магазинів. В цій статті ми розглянемо аналіз програмного забезпечення для адміністрування роздрібної торгівлі та основні функції, які він повинен виконувати.

Рис 1. Основні функції які виконує додаток для управління роздрібної торгівлі

З точки зору розробника, аналіз програмного забезпечення для адміністрування роздрібної торгівлі має бути детальним та систематичним. Найперше, слід визначити мету програмного забезпечення та його функціональні вимоги. Наприклад, програмне забезпечення для адміністрування роздрібної торгівлі повинно забезпечувати ефективне керування запасами, управління продажами, лояльністю та маркетингом, а також швидкий та зручний доступ до інформації про продукти та їх характеристики.

Після визначення функціональних вимог, Розробник повинен оцінити наявні програмні продукти, які можуть виконувати ці вимоги. Важливо звернути увагу на технології, які використовуються в програмному забезпеченні, такі як бази даних, мови програмування, фреймворки та інші технології.

Наступним кроком є дослідження архітектури програмного забезпечення та оцінка його масштабуваності та розширюваності. Важливо забезпечити, що програмне забезпечення може зростати разом з бізнесом та забезпечити підтримку нових функцій та можливостей у майбутньому.

Також, розробник повинен дослідити стійкість програмного забезпечення до помилок та вразливостей, та забезпечити, що програмне забезпечення відповідає стандартам безпеки та захисту даних.

Нарешті, потрібно дослідити доступні інструменти для підтримки та розробки програмного забезпечення. Важливо забезпечити відповідну документацію, високу якість коду та належний рівень підтримки та оновлення програмного

Для забезпечення ефективної підтримки та розробки програмного забезпечення для адміністрування роздрібної торгівлі, Розробник повинен також дослідити можливості

інтеграції з іншими системами та протоколами обміну даними, такими як REST або SOAP. Це забезпечить можливість обміну даними з іншими системами, такими як системи управління запасами та фінансові системи.

Рис 2. Принцип роботи протоколу REST

Для забезпечення ефективної розробки та підтримки програмного забезпечення, Розробник повинен використовувати сучасні підходи до розробки програмного забезпечення, такі як Agile та DevOps, та використовувати відкриті стандарти та розробляти з використанням відкритого програмного забезпечення.

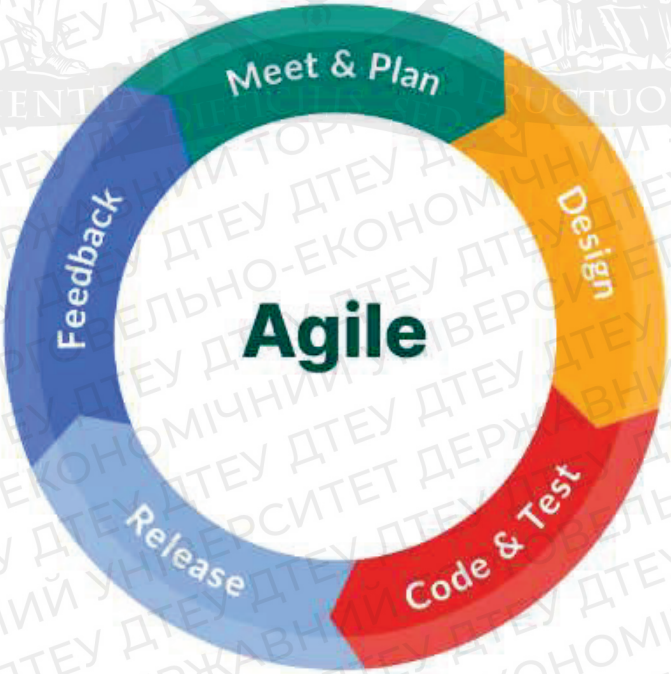


Рис 3. Підходи методології Agile

Загалом, аналіз програмного забезпечення для адміністрування роздрібної торгівлі з точки зору розробника має бути комплексним та систематичним.

Потрібно забезпечити відповідну документацію, високу якість коду та належний рівень підтримки та оновлення програмного забезпечення. Важливо звернути увагу на технології, які використовуються в програмному забезпеченні, а також на архітектуру та масштабуваність програмного забезпечення. Дослідження доступних інструментів для підтримки та розробки програмного забезпечення, також має бути частиною аналізу програмного забезпечення для адміністрування роздрібної торгівлі.

Також важливо звернути увагу на безпеку програмного забезпечення та захист від зловмисників. Потрібно забезпечити захист бази даних та конфіденційну інформацію користувачів, а також розглянути можливість застосування шифрування та механізмів аутентифікації.

При розробці програмного забезпечення для адміністрування роздрібної торгівлі необхідно використовувати сучасні технології та інструменти, що дозволяють швидко та ефективно створювати програмне забезпечення. До таких інструментів можна віднести фреймворки, такі як React, Angular, Vue.js, або бібліотеки, такі як jQuery, Bootstrap та інші.

Усі вищезгадані питання має враховувати розробник при аналізі програмного забезпечення для адміністрування роздрібної торгівлі. Тільки систематичний та всебічний підхід до розробки програмного забезпечення дозволить створити продукт, що задовольняє потреби користувачів та відповідає всім вимогам роздрібної торгівлі.

Крім того, важливо пам'ятати про безпеку програмного забезпечення для адміністрування роздрібної торгівлі. Потрібно забезпечити належну захищеність баз даних, де зберігаються конфіденційні дані про клієнтів та операції з товаром. Також потрібно використовувати захист від вразливостей програмного забезпечення та забезпечити валідацію та фільтрацію вхідних даних, щоб уникнути атак типу SQL Injection та Cross-Site Scripting (XSS).

До розробки програмного забезпечення для адміністрування роздрібної торгівлі також можуть бути задіяні інші спеціалісти, такі як дизайнери, аналітики, тестувальники та інші. Тому важливо забезпечити належну комунікацію та співпрацю між всіма учасниками проекту.

Для розробки програмного забезпечення для адміністрування роздрібної торгівлі можна використовувати такі інструменти та технології:

1. Java або C# для розробки серверної частини програмного забезпечення.
2. HTML, CSS, та JavaScript для розробки клієнтської частини програмного забезпечення.
3. База даних SQL для збереження та управління даними про клієнтів та операціями з товаром.
4. Фреймворки та бібліотеки, такі як Spring або ASP.NET Core, для прискорення розробки та забезпечення безпеки програмного забезпечення.
5. Система контролю версій, така як Git, для спільної роботи та відстеження змін у коді.

Також можна використовувати Agile методології розробки програмного забезпечення, такі як Scrum або Kanban, для ефективної співпраці та швидкого впровадження змін.

У процесі розробки програмного забезпечення важливо забезпечити належну документацію та тестування. Потрібно створити документацію з вимог та функціональності програмного забезпечення, а також забезпечити тестування програмного забезпечення для виявлення помилок та відлагодження коду.

На ринку програмного забезпечення для адміністрування роздрібної торгівлі існує велика кількість різних продуктів. Розглянемо деякі з них:

1. Retail Pro є одним з найбільш популярних програмних продуктів для управління роздрібною торгівлею. Продукт має багатий функціонал, який включає управління запасами, продажі, замовлення та інше. Retail Pro також має можливості для налаштування згідно з потребами конкретного бізнесу.

2. Microsoft Dynamics 365 Commerce. є програмним продуктом, який надає повний набір інструментів для управління торговим процесом, включаючи управління запасами,

продажі, замовлення та інше. Продукт має інтеграцію з Microsoft Power BI, що дозволяє користувачам створювати звіти та аналізувати дані.

3. Lightspeed Retail є програмним продуктом для роздрібної торгівлі, який дозволяє керувати всіма аспектами торгового процесу, включаючи продажі, управління запасами та замовлення. Продукт також має можливості для налаштування згідно з потребами конкретного бізнесу

4. Square for Retail є програмним продуктом, розробленим для роздрібної торгівлі та функціонує на основі хмарних технологій. Продукт має можливості для управління запасами, продажами, клієнтами та іншими процесами. Крім того, продукт дозволяє приймати оплату за допомогою карток та мобільних платежів.

5. Vend є програмним продуктом для роздрібної торгівлі, який дозволяє керувати продажами, управління запасами та замовленнями. Продукт має можливості для налаштування згідно з потребами конкретного бізнесу. Крім того, Vend має інтеграцію з багатьма іншими програмними продуктами, що дозволяє підвищити ефективність роботи.

Висновки. Аналіз програмного забезпечення для адміністрування роздрібної торгівлі є важливим етапом у розробці програмного забезпечення. Для розробника важливо мати розуміння вимог клієнта, використовувати сучасні технології та інструменти розробки, забезпечувати захист від вразливостей та використовувати засоби для тестування та відлагодження коду. У статті було проведено аналіз вимог до програмного забезпечення для роздрібної торгівлі та розглянуто деякі популярні програмні продукти на ринку.

Для розробки програмного забезпечення для адміністрування роздрібної торгівлі можна використовувати Java або C# для розробки серверної частини програмного забезпечення, HTML, CSS та JavaScript для розробки клієнтської частини програмного забезпечення, базу даних SQL для збереження даних та фреймворки та бібліотеки для прискорення розробки та забезпечення безпеки.

Для ефективної співпраці та швидкого впровадження змін можна використовувати Agile методології розробки програмного забезпечення, такі як Scrum або Kanban. Належна документація та тестування також є важливими елементами розробки програмного забезпечення.

Загальний аналіз потреб та вимог клієнта дозволить розробити програмне забезпечення, яке буде відповідати їх потребам та допоможе підвищити ефективність та якість роботи роздрібної торгівлі. Компетентний аналіз та розробка програмного забезпечення забезпечить успішне функціонування бізнесу та задоволення потреб клієнтів.

Список використаних джерел

1. TechnologyAdvice. (2021). Best Retail Management Software. https://technologyadvice.com/retail-management/
2. Software Advice. (2021). Top Retail Management Software - 2021 Reviews, Pricing & Demos. https://www.softwareadvice.com/retail/.
3. Міністерство розвитку економіки, торгівлі та сільського господарства України. (2017). Діяльність роздрібної торгівлі в Україні: стан та перспективи розвитку. http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=0f870d6e-94d8-4296-96c6-0d0fd85b6dd8&title=DiyalnistRozdribnoiTorgivliUVkrainiStanTaPerspektiviRozvitku.
4. https://www.softwareadvice.com/retail/small-business-retail-pos-comparison/
5. https://www.business.com/articles/the-benefits-of-retail-management-software/

Робота виконана під науковим керівництвом к.пед.н, доцента
ЖИРОВОЇ Т.О

НАТИВНИЙ МОБІЛЬНИЙ ДОДАТОК: ІНТЕРАКТИВНА ТЕХНОЛОГІЯ ОСВІТНЬОГО ПРОЦЕСУ

КОЛЕСНИК Д., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Стаття присвячена опису розробки нативного мобільного додатка для підтримки інтерактивної технології освітнього процесу. В статті описані необхідні кроки для створення такого додатка, які включають аналіз вимог користувачів, проектування та розробку архітектури додатка. Нативний мобільний додаток є потужним інструментом для підтримки інтерактивної технології освітнього процесу. Він дозволяє студентам та викладачам більш ефективно спілкуватися, обмінюватися інформацією та ділитися результатами.

The article describes the development of a native mobile application to support interactive technology in the educational process. The necessary steps for creating such an application are outlined, including user requirements analysis, application architecture design, and development. A native mobile application is a powerful tool for supporting interactive technology in education, enabling more effective communication, information exchange, and result sharing between students and teachers.

Актуальність. Актуальність теми дослідження «Нативний мобільний додаток: інтерактивна технологія освітнього процесу» виявляється тим, що з появою смартфонів та планшетів стали доступні нові можливості в галузі освіти. Розробка нативних мобільних додатків, які спеціально адаптовані під мобільні пристрої, може покращити якість навчання та забезпечити більш ефективний та цікавий навчальний процес. Для студентів мобільні пристрої є невід'ємною частиною їхнього життя, тому використання нативних мобільних додатків у навчальному процесі може сприяти підвищенню сучасної мотивації до навчання, покращенню засвоєння матеріалу та зниженню навчальної втоми. Крім того, нативні мобільні добавки можуть забезпечити доступ до навчального матеріалу з будь-якого місця та в будь-який час, що покращує доступність навчання та забезпечує гнучкість у навчальному процесі.

Метою є вивчення та опис використання нативних мобільних додатків у навчальному процесі, опис технології розробки таких додатків, а також дослідження інтерактивних функцій та інтерфейсу мобільних додатків для забезпечення більш ефективного та зрозумілого сприйняття навчального матеріалу студентами.

Об'єктом дослідження є нативний мобільний додаток, призначений для використання в освітньому процесі, з його структурою, інтерфейсом, функціоналом та можливостями.

Предмет дослідження є технологія розробки нативних мобільних додатків для освіти, їх функціональні можливості та інтерактивні функції, вплив на ефективність та результативність навчання.

Аналіз попередніх досліджень. Дослідження в галузі використання мобільних технологій у навчальному процесі здійснюється вже кілька десятиліть. Багато досліджень підтверджують ефективність використання мобільних технологій, зокрема нативних мобільних додатків, у навчальному процесі. Один із досліджень, проведених в Університеті штату Іллінойс, показав, що студенти, які використовують мобільні добавки для навчання, мають вищі результати засвоєння матеріалу та більшу мотивацію до навчання разом зі студентами, які не використовують мобільні добавки. Інше дослідження, проведене в Університеті Бруклін, досліджувало вплив використання мобільних додатків на мотивацію студентів до навчання. Результати показали, що використання мобільних додатків для навчання сприяє мотивації студентів до навчання, зокрема через можливість більшого залучення до навчального процесу та більшої інтерактивності з матеріалом. Інші дослідження

досліджували використання мобільних додатків у конкретних галузях, наприклад, у медичній освіті чи навчанні мов. Результати таких досліджень також підтверджують ефективність використання мобільних додатків у навчальному процесі. У своїй статті «Опитування мобільного навчання» автор Кумар С. обговорює поняття мобільного навчання та його переваги. Крім того, дослідник наводить приклади застосування мобільних додатків для освіти та ділиться досвідом впровадження мобільного навчання в різних країнах світу. Автори Го, Ю., Чжан, Д. (2017) в статті «Мобільне навчання в освіті: огляд останніх досліджень» розглядають дослідження мобільного навчання та його застосування в освітній практиці. Вони аналізують ефективність мобільного навчання, досліджують його вплив на навчальні досягнення студентів, а також досліджують використання мобільних додатків для навчання різних предметів.Аль-Фрейхат, Д., Джой, М., Сінклер, Дж. оцінюють використання та вплив гейміфікованого мобільного додатку для покращення навичок словникового запасу під час вивчення другої мови. Вони використовують мобільний додаток для вивчення англійської мови та досліджують, як гейміфікація краще покращить словниковий запас студентів. У своїй статті «Мобільні програми в класі: Огляд сучасного стану» автор Алсоват, Х. проводить огляд використання мобільних додатків у навчальному процесі. Отже, попередні аналізуючи дослідження дозволяють зробити висновок про те, що використання мобільних додатків, зокрема нативних мобільних додатків, у навчальному процесі є ефективним та може сприяти підвищенню якості навчання.

*Виклад основного матеріалу***.** Інтеграція технологій в освітній процес відкриває нові горизонти можливостей для підвищення ефективності навчання та забезпечення більшої взаємодії між усіма учасниками освітнього процесу. Один із ключових напрямів інновацій в освіті полягає в розробці нативних мобільних додатків, які можуть стати потужним інструментом для вчителів, студентів та батьків, сприяючи ефективному навчанню та взаємодії між усіма зацікавленими сторонами. Метою цієї статті є дослідження потенціалу та можливостей нативних мобільних додатків у інформатизації освітнього процесу. Особлива увага зосереджуються на аналізі ключових аспектів розробки, впровадження та використання таких додатків у різних освітніх контекстах, враховуючи специфіку потреб користувачів та особливості сучасних педагогічних підходів. У цій статті розглядаються основні складові ефективного нативного мобільного додатка для інформатизації освітнього процесу, включаючи систему авторизації та аутентифікації, управління профілями користувачів, доступ до навчальних матеріалів, комунікацію та співпрацю, оцінювання та звітність, а також адаптивність та персоналізацію навчального досвіду. У результаті дослідження очікується отримати рекомендації щодо оптимальних підходів до розробки та впровадження нативних мобільних додатків для інформатизації освітнього процесу, враховуючи потреби різних груп користувачів та специфіку освітнього середовища. Ми сподіваємося, що отримані результати допоможуть розробникам, учителям, адміністраторам та іншим зацікавленим сторонам краще зрозуміти потенціал та можливості використання нативних мобільних додатків для підвищення ефективності та якості навчання.

У сучасному цифровому світі мобільні технології докорінно змінили підхід до навчання та освіти. Завдяки високій доступності смартфонів та планшетів, навчальний процес стає більш гнучким, персоналізованим та ефективним. Водночас, на фоні цієї еволюції виникла потреба у нових підходах та інструментах для покращення освітнього процесу.

Один із найзначущіших розвитків цього напрямку – це народження та розвиток нативних мобільних додатків для освітньої сфери. Ці додатки стали потужним інструментом, що відкриває безмежні можливості для інтерактивності та особистісно орієнтованого навчання. Вони надають змогу створювати динамічні, цікаві та змістовні заняття, які сприяють поглибленому засвоєнню матеріалу та розвитку критичного мислення.

У статті ми розглянемо концепцію нативних мобільних додатків для освіти та їхню важливу роль у трансформації навчального процесу. Ми дослідимо переваги цих додатків у порівнянні з традиційними методами навчання, звернемо увагу на можливості інтерактивності

та адаптації до індивідуальних потреб студентів. Крім того, ми розглянемо приклади успішних нативних додатків для освіти та їхній вплив на підвищення ефективності навчання.

Нативні мобільні додатки для інформатизації освітнього процесу мають значний потенціал для покращення якості навчання та співпраці між вчителями, студентами та батьками. Ці додатки забезпечують доступ до навчальних ресурсів, інструментів комунікації та співпраці, а також можуть допомогти в отриманні зворотного зв'язку та оцінюванні навчальних досягнень. Отже, серед усіх можливостей слід виділити основні:

1. Розклад занять: Можливість перегляду, створення та редагування розкладу занять для студентів та вчителів.
2. Електронний журнал: Зберігання інформації про оцінки, відвідування та успішність студентів.
3. Завдання та контрольні роботи: Створення, надсилання та оцінювання завдань та контрольних робіт для студентів.
4. Комунікація: Чат-функція для спілкування між студентами, вчителями та батьками.
5. Ресурси для навчання: Доступ до підручників, відео, презентацій та інших матеріалів для навчання.
6. Календар подій: Організація та координація заходів, таких як зустрічі, семінари та конференції.
7. Система сповіщень: Автоматичне сповіщення про нові завдання, оцінки та інші важливі події.
8. Адаптивне навчання: Рекомендації щодо індивідуальних навчальних планів, враховуючи сильні та слабкі сторони кожного студента.
9. Аналітика та звіти: Статистика та аналіз успішності студентів для вчителів та батьків.
10. Інтеграція з іншими системами: Можливість синхронізації даних з існуючими освітніми системами, такими як електронні журнали, навчальні платформи тощо.

З технічної точки зору, розробка нативного мобільного додатку інформатизації освітнього процесу може бути розділена на наступні етапи:

1. Вибір архітектурної моделі: визначення моделі. яка найкраще підходить для додатка. Найпоширенішими моделями є клієнт-серверна (де додаток спілкується з сервером для отримання даних) та розподілена (де додаток працює безпосередньо з базою даних на пристрої).
2. Вибір технологій та фреймворків: обрання мови програмування та фреймворки, які будуть використані для розробки додатка. Для Android-розробки популярними є Java та Kotlin, для iOS - Swift та Objective-C. Також можна розглянути використання кросплатформних фреймворків, таких як React Native або Flutter, що дозволяють створювати додатки для обох платформ одночасно.
3. Розробка серверної частини (якщо необхідно): розробка серверної частини для забезпечення комунікації між додатком та базою даних, обробки запитів від клієнтів та передачі даних. Виберіть відповідну мову програмування, таку як Python, Ruby, PHP або Node.js, та базу даних, наприклад, MySQL, PostgreSQL або MongoDB.
4. Розробка клієнтської частини: створення інтерфейсу користувача та реалізуйте логіку додатка, використовуючи обрані мови програмування та фреймворки. Врахування адаптивності дизайну та коректну роботу на різних типах пристроїв та роздільних здатностях екранів.
5. Тестування та налагодження: проведення регулярного тестування додатка на різних пристроях, операційних системах та версіях, щоб забезпечити коректну роботу та стабільність додатка. Використовуйте ручне тестування, автоматизовані тести та тести продуктивності для виявлення та усунення помилок та проблем.
6. Забезпечення безпеки: розробка та впровадження заходів безпеки, щоб захистити дані користувачів та запобігти несанкціонованому доступу до системи. Включаючи

авторизацію, аутентифікацію, шифрування даних та інші рекомендації щодо інформаційної безпеки.

7. Оптимізація продуктивності та ресурсів: оптимізація додатка, щоб забезпечити швидкість, стабільність та ефективне використання ресурсів пристрою, таких як пам'ять, процесор та батарея.

8. Реалізація аналітики та звітів: впровадження інструментів аналітики, такі як Google Analytics або Firebase Analytics, для збору даних про користувачів, їхню активність та взаємодію з додатком. Використання цих даних для покращення додатка та розуміння потреб користувачів.

9. Маркетинг та просування: розробка стратегії маркетингу та просування вашого додатка, щоб залучити користувачів, збільшити встановлення та популярність. Використовуйте різні канали, такі як соціальні медіа, рекламні кампанії та співпрацю з освітніми закладами.

10. Оновлення та підтримка: Після запуску додатка, підтримка, оновлення, вдосконаленнями та виправленнями помилок. Регулярно збирайте відгуки від користувачів та аналізуйте дані про їхню активність, щоб забезпечити найкращий можливий досвід використання додатка. Також не забувайте про технічну підтримку користувачів, щоб допомогти їм у вирішенні проблем та відповісти на запитання.

11. Масштабування: У міру зростання кількості користувачів та розширення додатка, можливо, знадобиться масштабувати серверну інфраструктуру та базу даних, щоб підтримувати збільшення навантаження та запобігти проблемам із продуктивністю.

12. Сумісність з майбутніми версіями: перевірка сумісність додатка з майбутніми версіями операційних систем та пристроїв, щоб запобігти проблемам, які можуть виникнути через оновлення ПЗ або зміни у апаратному забезпеченні.

13. Інтеграція з іншими сервісами: можливість інтеграції вашого додатка з іншими освітніми сервісами, платформами або інструментами, що використовуються у вашій цільовій аудиторії, для підвищення ефективності та зручності використання додатка.

Важливо врахувати, що успішність мобільного додатку залежить від його здатності задовольнити потреби цільової аудиторії та реагувати на їх відгуки та вимоги. Тому на етапі розробки додатка слід зосередитись на забезпеченні високої якості та зручності використання всіх компонентів моделі.

Останнім кроком у розробці мобільного додатку інформатизації освітнього процесу буде його тестування та оптимізація. Це передбачає проведення ретельних тестів щодо продуктивності, безпеки, сумісності, а також отримання відгуків від користувачів та внесення відповідних змін для покращення досвіду використання.

У результаті розробки та впровадження ефективного мобільного додатку інформатизації освітнього процесу можна досягти підвищення якості освіти, забезпечення доступу до ресурсів для всіх студентів, полегшення роботи викладачів та підтримки керівництва освітніх установ.

Перед початком розробки мобільного додатку, необхідно запроектувати модель класів, яка буде враховувати особливості інтерактивної технології освітнього процесу, яка базується на взаємодії студентів та викладачів через мобільний додаток. Також варто ретельно продумати всі можливі взаємодії між класами та їх атрибути та методи, щоб забезпечити якісну та ефективну роботу системи освіти.

Основними класами, які необхідно врахувати в моделі, є «Студент», «Викладач», «Курс», «Завдання», «Вікторина», «Питання», «Тест», «Результат», «Матеріал» та «Ресурси для навчання». Вони повинні бути взаємозв'язані, щоб забезпечити ефективну взаємодію між учасниками навчального процесу.

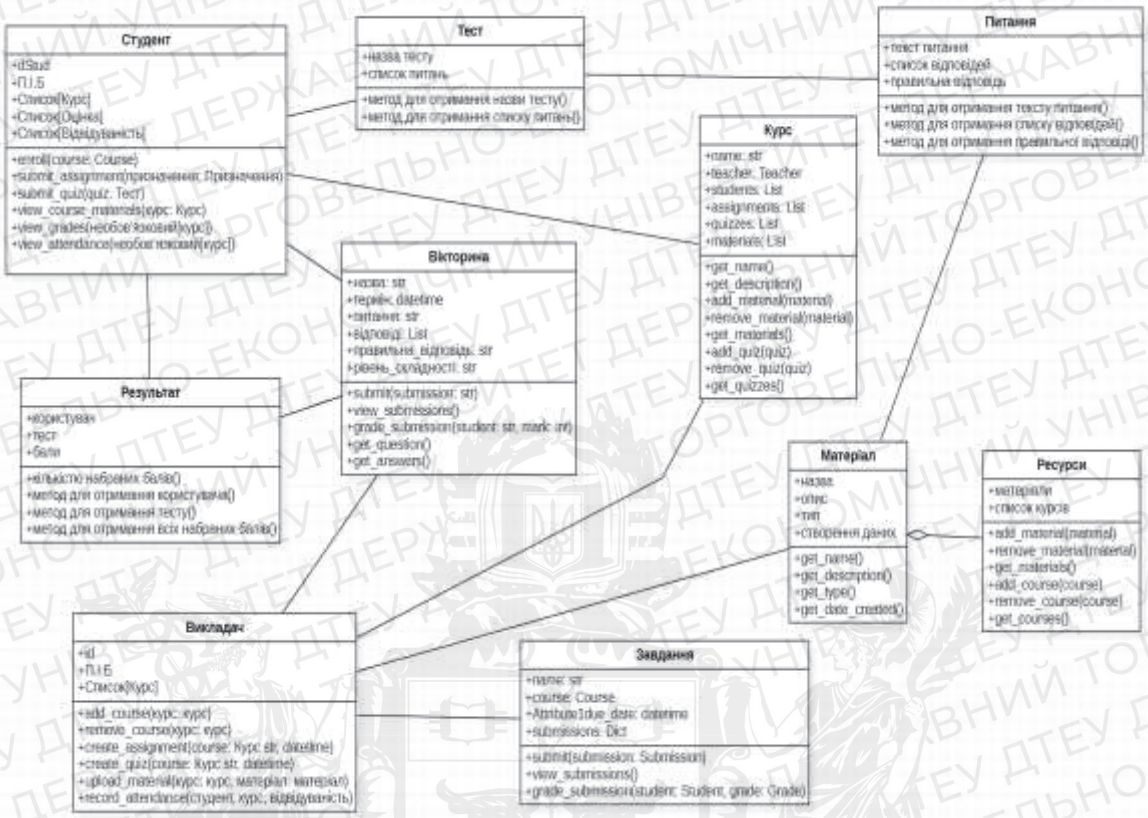


Рис. 1. Модель класів нативного мобільного додатку

Клас «Студент»: студенти повинні мати можливість зареєструватися на курс, після чого вони можуть брати участь у вікторинах та тестах. Також варто враховувати, що студенти можуть бути у різних станах (наприклад, активний, пасивний, заблокований), тому потрібно створити відповідний атрибут в класі «Студент»

Атрибути класу: name: str; id: int; courses: List[Course]; grades: Dict[Course, List[Grade]];attendance: Dict[Course, List[Attendance]]

Операції/Методи класу:

- enroll(course: Course) -> None
- submit_assignment(assignment: Assignment) -> None
- submit_quiz(quiz: Quiz) -> None
- view_course_materials(course: Course) -> List[Material]
- view_grades(course: Optional[Course] = None) -> Dict[Course, List[Grade]]
- view_attendance(course: Optional[Course] = None) -> Dict[Course, List[Attendance]]

Клас «Викладач»: викладачі повинні мати можливість створювати тести та вікторини, призначати завдання та оцінювати подання студентів.

Атрибути: name: str; id: int; courses: List[Course]

Операції/Методи класу:

- add_course(course: Course) -> None
- remove_course(course: Course) -> None
- create_assignment(course: Course, name: str, due_date: datetime) -> Assignment
- create_quiz(course: Course, name: str, due_date: datetime) -> Quiz
- upload_material(course: Course, material: Material) -> None
- record_grade(student: Student, course: Course, grade: Grade) -> None

- record_attendance(student: Student, course: Course, attendance: Attendance) -> None

Клас «Курс». Курси повинні мати набір матеріалів та ресурсів для навчання, які студенти можуть використовувати для підготовки до вікторин та тестів.

Атрибути класу: name: str; teacher: Teacher; students: List[Student]; assignments: List[Assignment]; quizzes: List[Quiz]; materials: List[Material].

Операції/Методи:

- get_name(): повертає назву курсу.
- get_description(): повертає опис курсу.
- add_material(material): додає матеріал до списку матеріалів курсу.
- remove_material(material): видаляє матеріал зі списку матеріалів курсу.
- get_materials(): повертає список матеріалів курсу.
- add_quiz(quiz): додає вікторину до списку вікторін курсу.
- remove_quiz(quiz): видає вікторину зі списку вікторін курсу.
- get_quizzes(): повертає список вікторін курсу.

Клас «Завдання» має такі атрибути: name: str; course: Course; due_date: datetime; submissions: Dict[Student, Submission].

Операції/Методи:

- submit(submission: Submission) -> None
- view_submissions() -> Dict[Student, Submission]
- grade_submission(student: Student, grade: Grade) -> None

Клас «Вікторина»: вікторина повина мати список подань та їх стан (прийнято, відхиллено, в очікуванні). Атрибути даного класу : назва: str; курс: str; термін: datetime; питання: str; відповіді: List[str]; правильна_відповідь: str; рівень_складності: str

Операції/методи:

- submit(submission: Dict[str, str]) -> None
- view_submissions() -> Dict[str, str]
- grade_submission(student: str, mark: int) -> None
- get_question() -> str
- get_answers() -> List[str]

Пояснення: submit(submission: Dict[str, str]) – додає подання (відповідь студента) в словник подань. Ключ – ім'я студента, значення – їх відповідь.

Клас «Питання» має наступні атрибути: текст питання; список відповідей;; правильна відповідь.

Методи: конструктор, який створює об'єкт питання із заданим текстом, списком відповідей та правильною відповіддю; метод для отримання тексту питання; метод для отримання списку відповідей; метод для отримання правильної відповіді.

Клас «Тест» містить такі атрибути: назва тесту; список питань.

Методи класу: конструктор, який створює об'єкт тесту із заданою назвою та списком питань; метод для отримання назви тесту; метод для отримання списку питань.

Клас «Результат» вміщує атрибути: користувач; тест; бали.

Методи: конструктор, який створює об'єкт результату із заданим користувачем, тестом та кількістю набраних балів; метод для отримання користувача; метод для отримання тесту; метод для отримання всіх набраних балів.

Клас «Матеріал». Атрибути класу: назва, опис, тип (відео, текст, зображення тощо), створення даних.

Операції/методи класу:

- get_name(): повертає назву матеріалу.
- get_description(): повертає опис матеріалу.
- get_type(): повертає тип матеріалу.
- get_date_created(): повертає дату створення матеріалу.

Клас «Ресурси для навчання». Атрибути: матеріали, список курсів.
Операції/методи:

- add_material(material): додає матеріал до списку доступних матеріалів.
- remove_material(material): видаляє матеріал зі списку доступних матеріалів.
- get_materials(): повертає список доступних матеріалів.
- add_course(course): додає курс до списку доступних курсів.
- remove_course(course): видає курс зі списком доступних курсів.
- get_courses(): повертає список доступних курсів.

Зв'язки між класами можуть бути наступними: клас «Студент» має взаємозв'язок з класами «Курс», «Вікторина», «Тест» та «Результат», оскільки студент може бути зареєстрований на курс, складати вікторини та тести, та отримувати результати відповідей. Клас «Курс» має взаємозв'язок з класами «Вікторина», «Тест», «Завдання» та «Матеріал», оскільки курс містить ці елементи навчання та може мати з ними взаємозв'язок. Клас «Завдання» має взаємозв'язок з класами «Вікторина», «Тест» та «Матеріал», оскільки завдання можуть містити питання для вікторин та тестів, а також матеріали для навчання.

Клас "Тест" має взаємозв'язок з класом "Питання", оскільки тест містить питання для відповідей. Клас "Результат" має взаємозв'язок з класами "Студент", "Вікторина" та "Тест", оскільки результати зберігаються для відповідної вікторини або тесту, що був складений студентом.

Висновки. Нативний мобільний додаток є достатньо перспективним для використання в освітньому процесі. Він дозволяє студентам ефективніше та інтерактивніше навчатися, забезпечуючи доступ до навчальних матеріалів, тестів, вікторин та інших додаткових ресурсів. Розробка такого додатка дає можливість забезпечити інтерактивність та цікавість у навчальному процесі, що дозволяє підвищити якість засвоєння знань та розширити можливості для розвитку креативності та самостійності студентів.

Додаток, описаний у статті є прикладом вдалого поєднання технологій та освіти. Розробка такого додатку дає можливість забезпечити інтерактивність та цікавість у навчальному процесі, що дозволяє підвищити якість засвоєння знань та розширити можливості для розвитку креативності та самостійності учнів.

Однією з ключових особливостей даного додатку є те, що він є нативним для мобільних пристроїв. Це означає, що додаток розроблений спеціально для операційних систем мобільних пристроїв (Android та iOS) і максимально пристосований до їхніх особливостей та можливостей. Такий підхід дозволяє забезпечити максимальний комфорт та зручність користування додатком, що є важливим чинником для ефективної навчальної діяльності.

Список використаних джерел

1. Asgari, N., Farahani, R. Z., & Goh, M. (2021). Supply chain management: developments, issues, and trends. Annals of Operations Research, 293(1), 1-9.
2. Beşoluk, Ş., & Büyüköztürk, Ş. (2018). Mobile learning in higher education: A meta-analysis of empirical research. International Journal of Educational Technology in Higher Education, 15(1), 1-27. https://doi.org/10.1186/s41239-018-0099-9
3. Chao, T. C., & Lo, H. C. (2019). Exploring the intention to use mobile learning among college students. Education and Information Technologies, 24(1), 77-92. https://doi.org/10.1007/s10639-018-9764-8
4. Chinnery, G. M. (2018). Emerging technologies–going to the MALL. Language Learning & Technology, 22(1), 1-4. https://doi.org/10125/44458

Робота виконана під науковим керівництвом PhD, доцентом
ДЕСЯТКО А.М.

AR В БІЗНЕСІ НА ПРИКЛАДІ КВЕСТ-КІМНАТИ

КОНДРАШЕВ С., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто використання доповненої реальності в різних сферах життя. Зазначено перспективи та переваги використання AR у бізнесі квест-кімнат, як безпосередньо всередині квестів для побудови механізмів і антуражу так і в бізнесі в цілому, для маркетинга.

The article discusses the use of augmented reality in various spheres of life. The prospects and advantages of using AR in the business of quest rooms are indicated, both directly inside quests for building mechanisms and entourage, and in business as a whole, for marketing.

Актуальність. Додатки з доповненою реальністю (AR) набувають все більшої популярності серед бізнес-користувачів через їх потенційну користь у різних галузях. Дана технологія може бути корисна у медицині, навчанні, туризмі, промисловості, дизайні, бізнесі. Актуальною вона є і для квест-кімнат котрі набрали свою популярність в останні декілька років.

Стрімкий розвиток бізнесу в сфері кімнат-кімнат призвів до великої конкуренції і відповідно до зростання складності і якості антуражу та механізмів у квестах. Технологія доповненої реальності здатна скоротити витрати часу та коштів на побудову квест-кімнат в декілька разів.

AR корисна для квестів в реальному житті не тільки як інструмент для створення кімнат, а і для реклами бізнесу для клієнтів та продажу франшизи.

Метою статті є дослідження особливостей використання доповненої реальності в квест-кімнат з метою зменшення витрати часу та зниження вартості побудови квестів.

Об'єктом дослідження є розробка AR додатку для квест-кімнати.

Предмет дослідження – доповнена реальність.

Аналіз попередніх досліджень. Технологіям доповненої реальності та їх використання для бізнесу присвячені праці зарубіжних науковців Рональда Т. Азума, Йосіо Маекава та Бріттані Сошнік, Бориса Кардіффа, Вернера Горліцера та Мартіна Оттербаха, Марка Лівро та Тобі Мейр.

Виклад основного матеріалу. Якщо казати технічною мовою, Доповнена реальність (AR) - технологія додавання в фізичний світ цифрових елементів в режимі реального часу, за допомогою смартфонів і інших комп'ютерних пристроїв, з метою доповнення відомостей про нього і поліпшення сприйняття інформації [1].

Використання доповненої реальності (AR) в бізнесі, зокрема на прикладі квест-кімнати, відкриває нові горизонти для підвищення залученості клієнтів та створення незабутніх вражень. Результати аналізу свідчать про те, що AR вносить значний внесок у підвищення інтерактивності та реалізму, що здатно підсилити взаємодію між брендом та споживачем.

Квест-кімната, поєднуючи в собі елементи реального та віртуального світу, надає можливість клієнтам брати участь у захоплюючій та інноваційній діяльності, забезпечуючи їм високий рівень залученості.

Другий важливий аспект полягає у тому, що AR підвищує конкурентоспроможність бізнесу через створення унікальної пропозиції. В основі квест-кімнати лежить ідея надати клієнтам відчуття новизни та непередбачуваності. Це може значно збільшити привабливість бренду, особливо в умовах збільшеного конкурентного середовища.

Не менш важливим є те, що AR сприяє взаємодії та соціальному взаємодії клієнтів. Квест-кімната, як яскравий приклад, дозволяє групам спільно розв'язувати завдання,

сприяючи обміну думками та спільній побудові стратегії. Це може зміцнити комунікацію та зв'язки між учасниками та відчуття належності до бренду.

Зазначені аспекти вказують на потужний потенціал AR у бізнесі та можливості, які воно відкриває. Проте, важливо розуміти, що успіх впровадження AR вимагає збалансованого підходу, звернення до інновацій та дбайливого ставлення до потреб та очікувань клієнтів. Однак, результати аналізу надають переконання, що AR може дійсно внести суттєвий внесок у підвищення привабливості бренду, залучення клієнтів та створення вражень, що залишаться у пам'яті на довгий час.

AR використовує камеру та сенсори смартфона, планшета або іншого пристрою для відстеження рухів та положення користувача, а потім проектує цифрові об'єкти на екран пристрою, додавши їх до реального оточення. Застосовувати цю технологію можна в багатьох різних галузях, для розваг, навчання, продажів, досліджень і це далеко не весь перелік сфер її застосування. AR технологія відображає віртуальні об'єкти у реальному часі та просторі, це дає змогу користувачам взаємодіяти з ними та отримувати додаткову інформацію про реальний світ навколо них. Доповнена реальність дозволяє візуалізувати цифрову інформацію в реальному світі, що дає більш реалістичне відчуття і взаємодію з цифровими об'єктами.
Бізнесу можуть бути корисні технології доповненої та віртуальної реальності. На це є дві головні причини:

- Сучасний споживач – це імерсивний споживач. Він хоче взаємодії з продуктом, хоче занурюватися в продукт. Йому вже недостатньо просто подивитися на товар на картинці в інтернет-магазині, щоб прийняти остаточне рішення про покупку. Він хоче спробувати цю пральну машину у себе вдома в реальному розмірі та реальній формі у два кліки за 30 секунд. Йому вже недостатньо просто уявити, якою буде його майбутня квартира, дивлячись на план-схему. Йому більше подобається одягнути окуляри віртуальної реальності та опинитися у цій квартирі – побачити якість стін, підлоги та помилуватися видом з вікна на 360 градусів.
- Інтеграція імерсивних технологій у маркетингові активності для брендів одразу не буде вимірюватись інвестиціями в сотні тисяч доларів, що є позитивним в умовах сучасного спаду у зв’язку з війною. Відповідно, роль імерсивних технологій у вигляді доповненої, віртуальної реальності та 3D може стати вагомим стимулом для бізнесу у контексті післявоєнної відбудови виробничих та маркетингових стратегій.[3]

Сфери застосування AR:

- Маркетинг і реклама: AR може використовуватися для створення інтерактивних рекламних кампаній, які дозволяють клієнтам взаємодіяти з продуктом чи брендом. Наприклад, компанія IKEA створила додаток, що дозволяє клієнтам розміщувати меблі в їхньому власному інтер'єрі
- Освіта: AR може допомогти вчителям і студентам зрозуміти складні концепції за допомогою візуальних елементів. Наприклад, додаток Anatomy 4D дозволяє користувачам роздивитися внутрішню будову тіла людини у 3D
- Медицина: AR може допомогти лікарям під час операцій та процедур. Додаток AccuVein використовує AR для візуалізації вен та артерій під шкірою, що допомагає медикам знайти кращий доступ до них
- Розваги: AR може бути використана для створення ігор та інтерактивних досвідів. Pokemon Go - це один з прикладів гри, що використовує AR для взаємодії з довколишнім світом
- Дизайн та архітектура: AR може бути використана для візуалізації дизайну будівлі чи інтер'єру в реальному часі. Додаток SketchAR дозволяє художникам намалювати свій ескіз на папері, дивлячись на нього через екран смартфона

- Туризм та подорожі: AR може бути використана для покращення туристичного досвіду, показуючи віртуальні об'єкти та інформацію про пам'ятки та визначні місця. Наприклад, додаток Wikitude дозволяє користувачам переглядати віртуальні об'єкти та отримувати інформацію про них у режимі реального часу
- Промисловість та виробництво: AR може бути використана для навчання працівників та поліпшення ефективності виробництва. Наприклад, AR може використовуватися для показування технічної інформації на екрані мобільного пристрою під час ремонту або налаштування обладнання
- Спорт: AR може бути використана для покращення тренувань та змагань. Наприклад, AR може використовуватися для створення віртуальних стежок для бігу або велосипедного спорту, що дозволить спортсменам тренуватися у реальних умовах
- Автомобільна промисловість: AR може бути використана для візуалізації інформації про швидкість, маршрут та інші параметри автомобіля на вітровому склі. Наприклад, додаток HUDWAY дозволяє водіям отримувати інформацію про маршрут та швидкість у режимі реального часу на вітровому склі
- Художня творчість: AR може бути використана для створення інтерактивних та мистецьких інсталяцій. Наприклад, додаток Tilt Brush дозволяє користувачам створювати віртуальні малюнки у тривимірному просторі, взаємодіючи з ними за допомогою AR

Переваги AR для e-commerce бізнесу:

- Клієнти готові купувати більше та частіше у компаній, які дають їм можливість отримувати досвід доповненої реальності, оскільки це зручно
- Клієнти можуть спробувати застосувати товар до того, як купили його
- Доповнена реальність економить час на поїздку в фізичну точку продажу. Це також є елементом безпеки, враховуючи пандемію COVID-19
- AR-технологія формує образ вашої компанії як інноваційної та створює конкурентну перевагу на ринку [2]

Рис. 1. Використання AR для дизайну інтер'єру

Основою технології AR є спеціальні програмні бібліотеки, які дозволяють розпізнавати об'єкти у реальному світі та накладати на них віртуальні об'єкти. AR технології можуть використовувати різні методи для розпізнавання об'єктів, такі як розпізнавання маркерів, розпізнавання образів, розпізнавання рухів та інші.

Типовий процес роботи технології AR може виглядати наступним чином:

- Створення віртуального об'єкта: Спочатку створюється віртуальний об'єкт, який може бути створений за допомогою спеціального програмного забезпечення для розробки AR-додатків
- Розпізнавання оточення: Для розпізнавання оточення та розміщення віртуального об'єкта в просторі використовується камера пристрою, на якому запущений AR-додаток
- Синхронізація рухів: Щоб забезпечити точність розміщення віртуального об'єкта в просторі, AR-додаток зчитує дані про рухи пристрою, що може бути забезпечено за допомогою акселерометра, гіроскопа та інших датчиків
- Відображення віртуального об'єкта: Коли AR-додаток виявляє місцезнаходження віртуального об'єкта, він відображає його на екрані пристрою, із застосуванням відповідної проекції та зміщенням відносно знайденої точки
- Інтерактивність: Зазвичай AR-додатки дозволяють користувачам взаємодіяти з віртуальними об'єктами, наприклад, пересувати їх, змінювати розміри, виконувати дії, що впливають на їх стан
- Оновлення віртуальних об'єктів: AR-додаток може оновлювати віртуальний об'єкт на основі даних про зміни в реальному світі, наприклад, коли об'єкт зміщується, розмір змінюється або коли користувач взаємодіє з ним
- Синхронізація звуку та інших сигналів: Деякі AR-додатки можуть використовувати сигнали зі звуку або інші сигнали, щоб додатково взаємодіяти з користувачем, забезпечуючи звукові ефекти, додаткові візуальні ефекти, або навіть привертаючи увагу до віртуальних об'єктів

Таким чином, технологія AR використовує розпізнавання оточення та датчики руху пристрою, щоб створювати враження, що віртуальні об'єкти існують в реальному світі.

Квест-кімната – це своєрідна розвага, гра, де учасники повинні разом виконати серію завдань, які приведуть до виходу. Зазвичай команда з 2-5 осіб замикається в кімнаті, яка стилізована під якусь тематику, наприклад, відомий фільм. Команді дається певний час, щоб вирішити головоломки, які допоможуть знайти ключ, щоб вийти з кімнати вчасно. Для того щоб зробити пошуки виходу більш цікавими кожна квест-кімната має свою легенду. Команді розповідають її перед початком гри. Антураж кімнати зроблений так щоб гравці максимально занурилися в атмосферу гри і їм здавалося, що все насправді. Головоломки можуть бути різні. Від простих, таких як кодові замки, цифрові панелі до більш складних спеціально розроблених пристроїв з великою кількістю електроніки. Під час проходження квесту тренується увага, командна взаємодія, вміння нестандартно використовувати навколишні предмети, рішучість в екстремальних умовах.

Квест-кімнати вперше з’явилися в Україні в 2014 році і з того часу активно розвиваються. Після відкриття декількох перших квестів всі швидко зрозуміли що це прибутковий бізнес і кількість кімнат почала дуже швидко зростати. Компанії почали пропонувати відкривати квести по франшизі і будували власні.

З ростом конкуренції зростала і якість кімнат. Механізми та антураж ставали все складнішими і красивішими. Загадки і сценарії більш продуманими та незвичайними. Відповідно зростала і вартість будівництва. В перших квест-кімнатах використовувалися звичайні та кодові замки, а ключі та комбінації від них були заховані чи зашифровані доволі примітивно. Сучасні механізми здатні задовольнити найвибагливіших і досвідчених гравців. Вони реагують на звук, світло, тепло. Стеля, підлога чи стіни можуть рухатися і змінювати площу та вигляд кімнати. Виглядають як речі з фантастичних фільмів і здатні працювати так само, як це показано в кіно. За дев’ять років розвитку квест-кімнати змінили свій антураж від шпалер до металу на стінах, від вішалки для одягу до справжнього автомобіля всередині (Рис.2).

Рис. 2. Порівняння складності механізмів перших та сучасних квест кімнат

З іншого боку створювати такі механізми та елементи антуражу стає дедалі складніше, довше і дорожче. На будівництво сучасної квест-кімнати може піти рік часу і сотні тисяч гривень. Величезною проблемою є також пошук спеціалістів які здатні створювати необхідні механізми, елементи антуражу, сценарії загадок. Також недоліком є те що чим складніший механізм тим важче і дорожче його ремонтувати у випадку поломки. У вирішенні цих проблем на допомогу приходить технологія доповненої реальності. Замість створення складної електроніки фізично ефекти можна створити у доповненій реальності і додати в квест.

Переваги та використання AR у квест кімнатах:

- Швидкість створення нових механізмів та елементів антуражу
- Порівняно невисока вартість
- Можливість створити механізми які неможливо реалізувати фізично
- Створені у AR речі не можливо зламати фізично, а отже вони не потребують ремонту
- Можливість швидко змінювати механізми що дає змогу покращувати їх без зупинки роботи квесту

В одній з квест-кімнат є великий елемент антуражу котрий водночас являє собою собою складний механізм. На його розробку і реалізацію було витрачено дуже багато часу і коштів. Його довелося декілька разів переробляти і покращувати. За допомогою технології доповненої реальності такий механізм можна було б зробити швидко, значно дешевше і легко в подальшому модернізовувати. А так як AR дозволяє взаємодіяти з віртуальними об’єктами, то є змога реалізувати подібні елементи квестів з набагато складнішими і красивішими ефектами ніж реальні (Рис. 3).

Рис. 3. Елемент антуражу та механізм квест-кімнати

Наступним великим кроком у розвитку квест-кімнат може стати створення цілого квесту на основі технології доповненої реальності. Великим мінусом з точки зору бізнесу є те що кожен клієнт грає в конкретній кімнаті лише один раз. Це пов’язано з тим що завдання не

можливо змінювати фізично. Антураж і механізми є невід'ємною частиною кімнати і щоб їх змінити потрібно повністю її перебудувати. Якщо ж розробити квест повністю на технології AR буде змога швидко змінювати весь інтер'єр і завдання в приміщенні за лічені хвилини. Таким чином можна використовуючи одну і ту ж площу створити не одну квест-кімнату, а декілька. Один квест в середньому розташований на 30 кв.м. площі. Для того щоб побудувати п'ять квест-кімнат в одному приміщенні, з урахуванням зони очікування, приміщення для співробітників та технічних зон, потрібно приблизно 250 кв.м. Використовуючи технологію AR можна створити п'ять квест- кімнат в приміщенні загальною площею до 100 кв.м., що дає змогу значно заощадити на витратах пов'язаних з утриманням та орендою приміщення під бізнес. Також великим плюсом є швидкість створення таких квестів. На побудову п'яти кімнат потрібні роки, а на створення їх у доповненій реальності – місяці.

Усі крупні провайдери квест-кімнат пропонують розпочати свій бізнес придбавши у них франшизу. AR може стати в нагоді і в цьому випадку. Компанії можуть розробляти презентації бізнесу з використанням доповненої реальності. Це дасть змогу краще донести до потенційних франчайзі суть квест-кімнат і переконати їх в тому що це вигідний і цікавий бізнес та дозволить одразу ознайомитися з прикладами антуражу та механізмів які використовуються в квестах. Вони зможуть зрозуміти що їм потрібно буде розробити та побудувати у власних кімнатах та ознайомитися з приблизною вартістю та строками відкриття бізнесу.

Кожна мережа квест-кімнат рекламує свій бізнес. Навіть через дев'ять років існування квестів в реальному житті величезна кількість людей не знає про цей вид розваг. Завдання маркетологів не просто сказати потенційним клієнтам про квест-кімнати, а швидко пояснити їм що це і переконати в тому що це класний вид відпочинку. Тут в нагоді стає доповнена реальність. Клієнтам можна одразу показати і дати спробувати якийсь елемент з квест-кімнати. Це одразу відповість на всі питання і зацікавить потенційних гравців прийти грати. Таку рекламу можна розміщувати на будь-яких заходах з великої кількістю людей, наприклад виставках, фестивалях або просто в торгових центрах.

Висновки. AR в бізнесі квест-кімнат на даний час майже не використовується, але має велику перспективу. Доповнену реальність можна використовувати для створення складних і дорогих елементів антуражу та механізмів, що значно прискорить їх побудову та знизить вартість. Рекламувати квест-кімнати та франчайзинг за допомогою AR. Створювати квести засновані лише на технології доповненої реальності і таким чином отримувати велику кількість квест-кімнат в одному маленькому приміщенні.

Список використаних джерел

1. Тимошенко Андрій, Як доповнена реальність може допомогти малому і середньому бізнесу?, \\ Режим доступу: https://business.diia.gov.ua/cases/tehnologii/ak-dopovnena-realnist-moze-dopomogti-malomu-i-serednomu-biznesu (останнє звернення 28.03.2023р.)
2. Никулишин Роман, Клієнти готові платити більше, якщо продукт можна оцінити в доповненій реальності. Ось як її впроваджують в e-commerce, \\ Режим доступу: https://forbes.ua/business/klienti-gotovi-platiti-bilshe-yakshcho-produkt-mozhna-otsiniti-v-dopovneniy-realnosti-chas-vprovaditi-ii-v-e-commerce-09042021-1328 (останнє звернення 28.03.2023р.)
3. Чигиринський Артем, Роль технологій доповненої та віртуальної реальності у післявоєнному відновленні українського бізнесу, \\ Режим доступу: https://mc.today/uk/blogs/rol-tehnologij-dopovnenoyi-ta-virtualnoyi-realnosti-u-pislyavoyennomu-vidnovlenni-ukrayinskogo-biznesu/ (останнє звернення 28.03.2023р.)

Робота виконана під науковим керівництвом д.т.н., професора
КРИВОРУЧКО О.В.

МЕТОДИ УПРАВЛІННЯ КАДРОВОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

КОПА В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи управління кадровою безпекою, що використовуються для забезпечення кадрової безпеки на підприємстві, в тому числі з точки зору кібербезпеки. Зазначено переваги їх застосування, пов'язані з побудовою ефективної системи управління кадровою безпекою, включаючи планування, виконання та контроль за застосуванням заходів забезпечення безпеки на підприємстві. Розроблено алгоритм формування системи кадрової безпеки підприємства.

The article explores methods of personnel security management used to ensure personnel security in enterprises, including from the standpoint of cybersecurity. The advantages of their application are noted, which are associated with the construction of an effective personnel security management system, including planning, implementation, and control over the application of security measures at the enterprise. An algorithm for the formation of an enterprise personnel security system has been developed.

Актуальність. Безпека та стабільність підприємства в значній мірі залежить від ефективного управління його кадрами. Розвиток технологій та зміни в економічному середовищі змушують компанії пристосовуватись до нових умов, що вимагає розробки та застосування нових методів управління кадровою безпекою. Крім того, сьогодні важливо не тільки забезпечувати безпеку працівників на робочому місці, а й захищати інформацію та ресурси компанії від зловживань або крадіжок. Тому, методи управління кадровою безпекою повинні включати в себе не тільки питання охорони праці, але й кібербезпеки та захисту конфіденційної інформації.

Актуальність методів управління кадровою безпекою підприємства полягає в тому, що сучасна економіка потребує ефективного управління людськими ресурсами для забезпечення стабільного функціонування підприємства. Кадрова безпека відіграє важливу роль у забезпеченні стабільності та безпеки функціонування підприємства, зокрема, в процесі попередження трудових конфліктів, викривлення конкуренції, крадіжок та інших негативних явищ.

Успішне впровадження методів управління кадровою безпекою може допомогти підприємствам досягти важливих цілей, таких як підвищення ефективності роботи, зниження витрат на оплату працівників, забезпечення стійкості та конкурентоздатності підприємства. Також, реалізація ефективних методів управління кадровою безпекою може знизити ризик відповідальності підприємства за негативні наслідки, пов'язані зі зловживанням або недостатньою компетентністю працівників. Застосування методів управління кадровою безпекою дозволяє зменшити загрози, пов'язані з внутрішніми та зовнішніми чинниками, що можуть впливати на кадрову безпеку підприємства. Ефективне управління кадровою безпекою сприяє підвищенню ефективності роботи працівників, забезпечує високий рівень професійної компетентності та мотивації персоналу, що позитивно відображається на конкурентоздатності підприємства.

Метою статті є дослідження методів управління кадровою безпекою підприємства.

Об'єктом дослідження є управління кадровою безпекою на підприємстві, яке включає в себе комплекс заходів з метою захисту від можливих загроз, що виникають з боку працівників підприємства, а також інших внутрішніх та зовнішніх факторів.

Предмет дослідження – кадрова безпека на підприємстві.

Аналіз попередніх досліджень. Загальнотеоретичні аспекти дослідження методів управління кадровою безпекою підприємства, що активно вивчаються та досліджуються,

представлені в публікаціях вітчизняних та закордонних науковців: О. В. Головатенко, В. І. Коваленка, B. Hofmann, M. Stetzer, A. Zohar, М. Р. Сідельнікової та ін. Автори аналізують сучасні методи управління кадровою безпекою, висвітлюють особливості їх використання та наводять приклади практичного їх застосування.

Виклад основного матеріалу. Кадрова безпека є важливим елементом успішної діяльності будь-якого підприємства. Необхідність управління кадровою безпекою полягає в забезпеченні безпеки працівників і захисті інтересів підприємства від можливих ризиків. Кадрова безпека є однією з ключових складових безпеки підприємства. Це означає, що належне управління кадровою безпекою є необхідним для забезпечення ефективної роботи підприємства та запобігання негативним наслідкам, які можуть виникнути внаслідок внутрішніх загроз [1].

Управління кадровою безпекою підприємства є важливою складовою будь-якої стратегії безпеки організації. Це означає, що керівництво підприємства повинно бути зацікавлене у створенні безпечного та здорового робочого середовища для своїх працівників.

Кадрова безпека на підприємстві включає заходи, спрямовані на захист персональних даних та інформації, які є власністю підприємства, від кібератак, внутрішньої шпигунської діяльності працівників та інших загроз з боку персоналу. Для забезпечення кадрової безпеки в кіберпросторі необхідно вживати комплекс заходів: відбір кваліфікованих спеціалістів з високим рівнем кадрової безпеки та надання їм необхідного навчання з питань кібербезпеки; розробка та впровадження внутрішніх правил та політик з кібербезпеки, які мають бути ознайомлені з усіма співробітниками; використання захисного програмного забезпечення та інших технічних засобів для захисту інформації від кібератак; ведення моніторингу активності працівників на робочих місцях з метою виявлення неправомірних дій та витоків конфіденційної інформації; проведення аудиту та оцінки ризиків з кібербезпеки на регулярній основі; регулярне проведення навчання працівників з питань кібербезпеки; розробка та впровадження плану дій у разі кібератаки та інших кібернападів; взаємодія з органами державного управління та правоохоронними органами в разі виявлення загроз кібербезпеці на підприємстві; розробка політики кадрової безпеки [2, 3].

Після проведення оцінки ризику підприємство повинно розробити політику кадрової безпеки. Це повинен бути документ, який визначає мету та цілі управління кадровою безпекою підприємства, а також встановлює стандарти та процедури, що регулюють дії працівників та керівництва в області кадрової безпеки.

Управління кадровою безпекою в контексті кібербезпеки передбачає застосування спеціальних методів та заходів з метою запобігання кібератакам та збереження конфіденційної інформації на підприємстві. Основні методи управління кадровою безпекою підприємства можна класифікувати на такі групи:

- Система автентифікації та авторизації: метод передбачає використання систем автентифікації та авторизації з метою захисту від несанкціонованого доступу до конфіденційної інформації. До основних методів системи автентифікації та авторизації можна віднести використання паролів, біометричних методів аутентифікації та інших технологій.
- Проведення інструктажів щодо захисту інформації, навчання працівників методам виявлення та запобігання кібератакам, забезпечення належного рівня кібербезпеки у всіх відділах підприємства.
- Шифрування даних: метод передбачає захист конфіденційної інформації від несанкціонованого доступу з використанням криптографічних методів шифрування. Шифрування даних може бути використане для захисту конфіденційної інформації на серверах, в базах даних та на звичайних пристроях.
- Захист інформації: метод передбачає вжиття заходів щодо захисту інформації, яка зберігається на комп'ютерах, серверах та інших електронних пристроях. До основних методів захисту інформації можна віднести шифрування даних,

використання комп'ютерних програм для виявлення та блокування шкідливих програм та вірусів, захист мережі підприємства від несанкціонованого доступу.

- Моніторинг та аналіз результатів управління кадровою безпекою. До таких методів відносять проведення аналізу статистики аварій та небезпек на підприємстві, оцінку ефективності використаних профілактичних та реагуючих заходів, оновлення та коригування політики кадрової безпеки підприємства.
- Аудит кібербезпеки: метод передбачає проведення аудиту кібербезпеки на підприємстві з метою виявлення та усунення проблем з кібербезпекою. Аудит кібербезпеки може бути проведений зовнішніми або внутрішніми експертами з кібербезпеки та має на меті виявлення слабких місць у системі кібербезпеки та розробку рекомендацій щодо їх усунення.

Методи управління кадровою безпекою підприємства можна поділити на три групи: проактивні, реактивні та попереджувальні. Проактивні методи передбачають запобігання можливих проблем. Найбільш ефективним методом є відбір кваліфікованих та досвідчених працівників, які можуть виконувати роботу безпечно. Також до проактивних методів належать проведення навчання та тренінгів, які допоможуть підвищити рівень свідомості працівників щодо безпеки на робочому місці [4].

Реактивні методи управління кадровою безпекою підприємства – це методи, що застосовуються для виявлення і припинення негативних наслідків, пов'язаних з діями співробітників, які порушують правила безпеки на робочому місці. Ці методи в основному реалізуються після виникнення проблеми і можуть включати наступні етапи:

- Реагування на випадок: підприємство звертає увагу на виявлення порушень правил безпеки та реагує на них відповідно до установлених процедур.
- Аналіз проблеми: підприємство з'ясовує причини порушень правил безпеки та знаходить способи їх усунення.
- Пошук рішення: підприємство визначає найкращі методи управління ризиками, щоб запобігти повторенню подій.
- Виконання рішення: підприємство реалізовує заходи, щоб забезпечити безпеку на робочому місці та запобігти порушенням правил безпеки.

Реактивні методи управління кадровою безпекою підприємства можуть бути ефективними для реагування на негативні наслідки, пов'язані з порушеннями правил безпеки. Проте, їх використання не дозволяє підприємству забезпечити повноцінний захист від ризиків, адже такий підхід не передбачає систематичного аналізу та профілактики можливих проблем. Тому, дуже важливо доповнювати реактивні методи проактивними підходами, які дозволять підприємству забезпечувати постійну безпеку на робочому місці та уникати виникнення подібних ситуацій.

Попереджувальні методи управління кадровою безпекою підприємства - це методи, які застосовуються для запобігання виникненню проблем та негативних наслідків, пов'язаних з порушеннями правил безпеки на робочому місці. Ці методи можуть включати наступні етапи:

- Аналіз ризиків: підприємство проводить оцінку ризиків на робочому місці та визначає найбільш критичні зони, де можуть виникнути проблеми з кадровою безпекою.
- Планування профілактичних заходів: підприємство визначає заходи, які можуть запобігти виникненню небезпеки та зменшити ризик.
- Розробка правил та процедур: підприємство встановлює правила та процедури для роботи на робочому місці, щоб забезпечити безпеку та зменшити ризик порушень правил безпеки.
- Тренінг та навчання: підприємство проводить тренінги та навчання для співробітників з питань безпеки на робочому місці, щоб забезпечити їхню згоду з правилами та процедурами та підвищити рівень свідомості щодо безпеки на роботі.

- Контроль та оцінка: підприємство встановлює механізми контролю та оцінки дій з питань безпеки на робочому місці, щоб забезпечити їх ефективність та вчасність.

Попереджувальні методи управління кадровою безпекою підприємства дозволяють забезпечити повноцінний захист від можливих ризиків та небезпек на робочому місці. Ці методи допомагають підприємству забезпечувати постійну безпеку.

Кадрова безпека − це одна з основних складових безпеки, головною метою якої є запобігання та протидія загрозам, що можуть заподіяти шкоду персоналу як основному ресурсу підприємства, а також управління персоналом з метою ефективного використання його потенціалу та запобігання загроз з боку самого персоналу. Алгоритм формування системи кадрової безпеки підприємства − оптимальний метод забезпечення кадрової безпеки (Рис. 1) з урахуванням ресурсних можливостей і цілей підприємства [3].

Рис. 1. Алгоритм формування системи кадрової безпеки підприємства

Алгоритм формування системи кадрової безпеки підприємства може включати наступні кроки:

1. Визначення потенційних загроз кадровій безпеці підприємства: для цього необхідно провести дослідження та аналіз ризиків, оцінити потенційні загрози та їх рівень небезпеки.
2. Встановлення мети та завдань системи кадрової безпеки: метою системи кадрової безпеки повинно бути забезпечення безпеки працівників підприємства та запобігання можливим загрозам для кадрової безпеки. Завданнями системи можуть бути контроль за доступом працівників до конфіденційної інформації, попередження інцидентів зі сторони співробітників та інші.
3. Визначення відповідальних осіб: визначення осіб, які будуть відповідальні за розробку та впровадження системи кадрової безпеки на підприємстві.
4. Розробка та впровадження політики кадрової безпеки: розроблення документів, що регламентують правила та процедури кадрової безпеки на підприємстві, такі як політика конфіденційності, правила безпеки на робочому місці, правила користування інформаційними системами тощо.

5. Встановлення системи контролю та моніторингу: встановлення системи, що дозволяє контролювати та моніторити виконання політики кадрової безпеки, а також виявляти можливі порушення та вчасно реагувати на них.
6. Організація навчання та тренінгів: проведення тренінгів та навчань з кадрової безпеки для всіх працівників підприємства.
7. Аналіз ефективності системи: аналіз ефективності системи кадрової безпеки та внесення необхідних змін для покращення її роботи..
8. Внесення змін та підтримка системи: внесення необхідних змін та підтримка роботи системи кадрової безпеки на підприємстві.

Існує багато потенційних загроз кадровій безпеці підприємства, вони можуть бути різними та залежать від багатьох факторів, таких як розмір підприємства, галузь діяльності, наявність конфіденційної інформації та інших факторів. Основні загрози, які можуть виникнути [2]:

- Втрата даних: хакери можуть зламати системи підприємства та отримати доступ до конфіденційної інформації про працівників, клієнтів або бізнес-операцій. Ця інформація може бути використана для крадіжки ідентичності, шахрайства або розкриття конфіденційних даних.
- Шахрайство: працівники можуть використовувати підставні документи для отримання доступу до конфіденційної інформації або виконання шахрайських дій від імені підприємства.
- Витік інформації: працівники можуть свідомо або несвідомо витікати інформацію за межі підприємства через недбалість або недостатню охорону інформації.
- Втрата працівників: коли працівники підприємства звільняються, вони можуть взяти з собою конфіденційну інформацію, яка може бути використана в шахрайських цілях або передана конкурентам.
- Фізична безпека: працівники підприємства можуть бути підтверджені фізичним загрозам, таким як крадіжка, насильство або терористичні акти.
- Несанкціоновані дії: продаж, обіг або незаконне використання конфіденційної інформації про працівників підприємства можуть призвести до фінансових втрат, порушення довіри клієнтів або репутаційних проблем.
- Соціальний інжиніринг: шахраї можуть використовувати соціальний інжиніринг, щоб отримати доступ до конфіденційної інформації про працівників підприємства. Наприклад, вони можуть надати себе за технічну підтримку або інший офіційний персонал, щоб отримати доступ до паролів та інших даних.

Загрози кадровій безпеці підприємства можна поділити на зовнішні та внутрішні. Зовнішні загрози пов'язані з впливом зовнішнього середовища на діяльність підприємства, тоді як внутрішні загрози пов'язані з діяльністю самого підприємства та його співробітників.

До зовнішніх загроз кадровій безпеці підприємства можна віднести такі фактори: конкуренція на ринку праці: низька привабливість підприємства для потенційних працівників може призвести до зменшення якості кадрів та збільшення ризику втрати кадрів; законодавчі та регуляторні зміни: зміни у законодавстві та регуляторних нормах можуть вплинути на вимоги до кадрової безпеки на підприємстві та вимагати додаткових зусиль для її забезпечення; шпигунство: шпигунство може призвести до витоку комерційної та конфіденційної інформації, що може вкрай негативно позначитись на діяльності підприємства; кібератаки: кібератаки можуть призвести до витоку конфіденційної інформації, порушення прав доступу до ресурсів, втрати даних та фінансових втрат.

Зовнішні загрози кадровій безпеці на підприємстві можуть бути спричинені злочинцями, конкурентами або недружніми державами, які можуть намагатися отримати конфіденційну інформацію, вкрасти матеріальні цінності або завдати шкоди підприємству. Ось кілька способів захисту від зовнішніх загроз кадровій безпеці:

- Забезпечення фізичної безпеки: забезпечення фізичної безпеки на підприємстві може допомогти у запобіганні вторгненню злочинців. Для цього можуть бути встановлені системи відеоспостереження, охорона, контроль доступу та інші заходи.
- Встановлення системи захисту інформації: встановлення системи захисту інформації може допомогти у запобіганні злому систем безпеки та захисту конфіденційної інформації. Для цього можуть бути використані шифрування даних, захист від вірусів, фаєрволи та інші заходи.
- Використання сучасних технологій захисту: для захисту від зовнішніх загроз кадровій безпеці можна використовувати сучасні технології захисту, такі як антивірусні програми, фаєрволи, системи шифрування, аудиторські звіти, системи резервного копіювання тощо.
- Встановлення системи контролю та фільтрації вхідної інформації: встановлення системи контролю та фільтрації вхідної інформації може зменшити ризик надходження шкідливої чи неправдивої інформації, що може призвести до порушення кадрової безпеки.
- Забезпечення безпеки мережі: забезпечення безпеки мережі на підприємстві може допомогти у запобіганні вторгнення злочинців через Інтернет.
- Встановлення контролю над користувачами: встановлення контролю над користувачами може допомогти у запобіганні недоречного використання конфіденційної інформації та матеріальних цінностей.

До внутрішніх загроз кадровій безпеці підприємства можна віднести наступні фактори: крадіжка даних та конфіденційної інформації: співробітники, які мають доступ до конфіденційної інформації, можуть зловживати своїм становищем і використовувати цю інформацію для особистої вигоди або для передачі конкурентам; шахрайство та зловживання повноваженнями: співробітники можуть використовувати свої повноваження для шахрайства, включаючи відмивання грошей, підробку документів та інші дії, що можуть завдати значних збитків підприємству; недостатня кваліфікація та некомпетентність: співробітники, які не мають достатньої кваліфікації або некомпетентні, можуть завдати шкоди підприємству своїми діями або бездіяльністю; порушення правил безпеки: співробітники, які не дотримують правил безпеки на робочому місці, можуть порушувати безпеку своїх колег і завдавати шкоди підприємству; конфлікти та недружні відносини: конфлікти між співробітниками можуть призвести до ворожих відносин і порушення робочого процесу, що може негативно позначитися на діяльності підприємства; недостатня мотивація: співробітники, які не мають достатньої мотивації, можуть бути менш продуктивними та більш схильними до помилок, що може негативно позначитися на діяльності підприємства [2].

Основні заходи для захисту від внутрішніх загроз кадровій безпеці на підприємстві можуть включати:

- Впровадження систем контролю доступу та обмеження прав доступу до конфіденційної інформації та ресурсів.
- Забезпечення безпеки та захисту інформації, шляхом впровадження сучасних технологій та програмних засобів захисту даних.
- Проведення навчань та тренінгів з питань безпеки для всіх співробітників підприємства: забезпечення навчання та підвищення кваліфікації співробітників може допомогти у зменшенні ризику порушення правил безпеки, шахрайства.
- Встановлення механізмів контролю та відслідковування дій співробітників на робочих місцях, а також використання систем моніторингу та аналітики для виявлення відхилень у поведінці співробітників.
- Проведення перевірок та ретельних досліджень нових співробітників та при зміні посади в компанії; проведення аудиту кадрових процесів та процесів управління персоналом з метою виявлення можливих ризиків та шляхів їх усунення.

- Встановлення системи внутрішнього контролю та аудиту: встановлення системи внутрішнього контролю та аудиту може допомогти у виявленні недоречних дій співробітників та шахрайства.
- Проведення періодичного аналізу та оновлення заходів захисту: періодичний аналіз та оновлення заходів захисту від внутрішніх загроз кадровій безпеці.

Основні етапи забезпечення ефективної кадрової безпеки на підприємстві можна умовно поділити на наступні:

1. Аналіз загроз та ризиків. Необхідно визначити потенційні загрози та ризики для кадрової безпеки на підприємстві, оцінити їх вплив та ймовірність виникнення.
2. Розробка стратегії забезпечення кадрової безпеки. На основі результатів аналізу необхідно розробити стратегію забезпечення кадрової безпеки, визначити основні напрямки дій та механізми запобігання виникненню загроз.
3. Реалізація заходів забезпечення кадрової безпеки. На цьому етапі здійснюються конкретні заходи, спрямовані на забезпечення кадрової безпеки, такі як проведення перевірок при прийомі на роботу, застосування заходів контролю доступу до конфіденційної інформації, навчання працівників з питань кадрової безпеки та інше.
4. Контроль та аналіз ефективності заходів. Необхідно систематично контролювати та аналізувати ефективність заходів забезпечення кадрової безпеки, що були впроваджені, та коригувати їх, якщо необхідно.
5. Постійне вдосконалення системи кадрової безпеки. Після проведення аналізу та аудиту необхідно постійно вдосконалювати систему кадрової безпеки на підприємстві.

Висновки. Методи управління кадровою безпекою підприємства дозволяють створити ефективну систему управління кадровою безпекою, що включає планування, виконання та контроль за застосуванням заходів забезпечення безпеки на підприємстві. Використання цих методів дозволяє підвищити рівень безпеки на підприємстві, зменшити ризики втрати конфіденційної інформації, запобігти крадіжкам та злому кібербезпеки. Зокрема, використання методів управління кадровою безпекою з точки зору кібербезпеки, дозволяє підвищити рівень захисту від кібератак, виключити можливість несанкціонованого доступу до важливої інформації та підвищити свідомість співробітників щодо кібербезпеки. Отже, використання методів управління кадровою безпекою є важливою складовою ефективного управління підприємством, яке дозволяє забезпечити безпеку працівників та інформації, що є ключовими ресурсами будь-якої компанії.

Список використаних джерел

1. Красномовець В. А. Методи забезпечення кадрової безпеки підприємства. Вісник Національного університету водного господарства та природокористування. 2012. Вип. 3(59). С. 142–143. Серія «Економіка».
2. Логінова Н. І. Місце кадрової безпеки в економічній безпеці підприємства. Комунальное хазяйство городів: Научно-технический сборник. 2009. № 87. С. 371–376.
3. Основні аспекти забезпечення кадрової безпеки підприємства / О. В. Халіна, Н. О. Козаченко // Наукові записки [Української академії друкарства]. - 2017. - № 2. - С. 133–142. - Режим доступу: http://nbuv.gov.ua/UJRN/Nz_2017_2_16 (останнє звернення 20.03.2023р.)
4. Чередниченко Н. В. Кадрова безпека як складова частина безпеки підприємства. Тези науково-практичної конференції, 28 серпня 2009 року. Суми: СумДУ, 2009. С. 51–53.

Робота виконана під науковим керівництвом к.т.н., доцента
ЗВЄРЄВА В.П.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

КОРЖ І., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи захисту даних інтелектуальної власності. Описано різні типи інтелектуальної власності, такі як авторське право, патентне право та торговельні марки, а також визначена важливість їх захисту. Розглянуто правовий та технічний захист інтелектуальної власності, такі як криптографічні методи, технології DRM та цифрові водяні знаки. Висвітлено необхідність використання комплексного підходу до захисту інтелектуальної власності та наведені приклади успішного використання правового та технічного захисту.

The article discusses methods of protecting intellectual property data. Various types of intellectual property, such as copyright, patent law, and trademarks, are described, and their importance in protection is emphasized. Legal and technical protection of intellectual property is examined, including cryptographic methods, DRM technologies, and digital watermarks. The need for a comprehensive approach to protecting intellectual property is highlighted, and examples of successful use of legal and technical protection are provided.

Актуальність. Дослідження методів захисту даних інтелектуальної власності має велику актуальність у сучасному світі, де інформація стала найціннішим ресурсом. Високо розвинуті технології дозволяють швидко та ефективно використовувати, розповсюджувати та зберігати інформацію, але водночас зростає й ризик її несанкціонованого використання. Крім того, злочинці постійно вдосконалюють свої техніки та методи порушення прав на інтелектуальну власність, що вимагає постійного розвитку технологій та методів захисту. Захист інтелектуальної власності стає все більш важливим завданням для бізнесу, науки та технологій, оскільки порушення авторських прав може призвести до значних втрат. Необхідність захисту інтелектуальної власності стає особливо актуальною в умовах глобалізації та розвитку міжнародної торгівлі, коли можливості для незаконного копіювання та використання інтелектуальної власності зростають. Порушення прав на інтелектуальну власність може призвести до значних економічних втрат для компаній та держав, а також до втрати довіри в споживачів. Тому, захист інтелектуальної власності важливий не тільки для окремих правовласників, а й для всього суспільства. Таким чином, дослідження методів захисту даних інтелектуальної власності є надзвичайно важливим і актуальним у сучасних умовах технологічного прогресу і потребує постійного вдосконалення технологій та методів захисту. Також варто відзначити, що з появою нових технологій та способів обробки інформації з'являються нові виклики та загрози для захисту інтелектуальної власності. Тому, розробка та застосування комплексних методів захисту є необхідною умовою для забезпечення ефективного захисту інтелектуальної власності.

Метою статті є дослідження основних методів захисту інтелектуальної власності, таких як правовий та технічний захист, а також вивчення новітніх технологій захисту.

Об'єктом дослідження є процес використання комплексного підходу до захисту інтелектуальної власності, а також розгляд різних методів технічного та правового захисту, таких як авторське право, патентне право, торговельні марки, криптографічні методи захисту, технології DRM.

Предмет дослідження − методи захисту даних інтелектуальної власності, які можуть бути використані для забезпечення безпеки та захисту прав творців та власників інтелектуальної власності.

Аналіз попередніх досліджень. Попередні дослідження з проблем захисту інтелектуальної власності широко представлені в літературі та наукових публікаціях. Деякі з них присвячені захисту авторських прав, патентного права, технічного захисту, цифрових водяних знаків та інших методів захисту інтелектуальної власності. Одним з досліджень в цій галузі є «Аналіз сучасних методів захисту авторських прав на музичні твори в інтернеті», який був проведений з метою дослідження сучасних методів захисту авторських прав на музичні твори в Інтернеті. У дослідженні було проаналізовано різні технічні та правові методи захисту, такі як DRM, водяні знаки, криптографічні методи тощо. Інше дослідження, «Розвиток технологій захисту інтелектуальної власності», розглядало проблеми захисту інтелектуальної власності в контексті розвитку технологій. У цьому дослідженні було досліджено такі методи захисту, як криптографічні методи, стеганографія, цифрові водяні знаки та інші. Дослідження «Технології DRM в захисті інтелектуальної власності» детально описує технології DRM та їх використання для захисту цифрових творів. Дослідження «Криптографічні методи захисту інтелектуальної власності» описує застосування криптографічних методів для захисту інтелектуальної власності в цифровому середовищі. Загалом, попередні дослідження показали, що нинішні методи захисту є недостатніми для ефективного захисту інтелектуальної власності в цифровому світі. Тому необхідно проводити додаткові дослідження та розробляти нові методи захисту.

Виклад основного матеріалу. Захист даних інтелектуальної власності в сучасному світі є дуже важливою та актуальною темою. Інтелектуальна власність включає різні типи прав, такі як авторське право, патентне право та торговельні марки, які необхідно захищати від неправомірного використання. Для правового захисту існують різні законодавчі акти та юридичні процедури, такі як позови за порушення авторських прав або патентних заявок. Технічний захист може бути здійснений за допомогою криптографічних методів, технологій DRM та цифрових водяних знаків. Однак, щоб забезпечити повний захист даних інтелектуальної власності, необхідно використовувати комплексний підхід, який поєднує як правові, так і технічні методи захисту [1].

Інтелектуальна власність − це права, що виникають у зв'язку зі створенням різних інтелектуальних творів або винаходів. Це можуть бути, наприклад, літературні твори, комп'ютерні програми, музика, фільми, винаходи, технічні розробки, знаки для товарів та послуг тощо. Інтелектуальна власність може бути захищена за допомогою різних методів, зокрема правових та технічних, щоб забезпечити авторам та власникам відповідні права на свої твори і винаходи.

Захист інтелектуальної власності є важливим елементом для стимулювання розвитку економіки та забезпечення інноваційного потенціалу. Ось декілька причин, чому захист інтелектуальної власності є важливим [1, 2]:

1. Захист інтелектуальної власності сприяє збереженню інновацій та стимулює інноваційний розвиток. Якщо винахідник чи автор знає, що його інтелектуальна власність буде захищена, то це збільшує його мотивацію та інтерес до розробки нових ідей і технологій.

2. Захист інтелектуальної власності допомагає зберегти конкурентну перевагу. Компанії, які мають патенти на свої винаходи, можуть захистити свої права та залишатися лідерами на ринку.

3. Захист інтелектуальної власності є важливим для забезпечення відповідної винагороди для творців. Якщо автори не можуть захистити свої права на свої творіння, то вони можуть втратити потенційний дохід від своїх ідей.

4. Захист інтелектуальної власності допомагає забезпечити безпеку та якість товарів та послуг. Якщо товари та послуги не захищені від копіювання, то можуть з'являтися підробки, які можуть бути небезпечними для споживачів.

5. Захист інтелектуальної власності допомагає зберегти культурну спадщину та інтелектуальну різноманітність.

Отже, захист інтелектуальної власності є важливим фактором, що сприяє розвитку інновацій та забезпечує стабільність економіки.

Правовий захист інтелектуальної власності − це система правових норм та процедур, що регулюють права на інтелектуальну власність та їх захист. Основні види інтелектуальної власності, які можуть бути захищені правовими засобами, включають авторське право, патентні права, права на товарні знаки, права на промислові зразки та права на торгові найменування. Для захисту інтелектуальної власності застосовуються різні юридичні інструменти. Основні з них − це реєстрація прав на інтелектуальну власність, визнання прав порушеними, звернення до суду за захистом прав, позовні вимоги на компенсацію шкоди, використання договірних засобів забезпечення захисту інтелектуальної власності тощо. Захист інтелектуальної власності зазвичай здійснюється на рівні країни, але також може бути захищений на міжнародному рівні [2]. У міжнародній сфері найбільш відомі організації, які займаються захистом інтелектуальної власності, це Всесвітня організація інтелектуальної власності (ВОІС) та Європейський патентний офіс (ЕРО). Отже, правовий захист інтелектуальної власності є важливим інструментом, який забезпечує права авторів та власників на їх інтелектуальну власність та сприяє розвитку інновацій та конкуренції в різних галузях економіки.

Авторське право − це один з видів інтелектуальної власності, який надає авторам творів мистецтва та літератури, науковим працівникам та іншим творчим особам право на контроль використання їхніх творів. Згідно з авторським правом, автор має ексклюзивне право на використання свого твору, зокрема на його відтворення, поширення, зміну та інші форми використання. Авторське право є важливим механізмом захисту інтелектуальної власності та сприяє розвитку культури, науки та технологій. Законодавчі норми з авторського права регулюють права творців на їхні твори, а також визначають термін дії прав на твір та процедуру реєстрації авторського права. Для захисту авторського права застосовуються різноманітні юридичні засоби, зокрема позови за порушення авторських прав, звернення до суду за захистом прав, використання ліцензій та договорів на використання творів. У деяких країнах також існують спеціальні органи, які відповідають за захист авторських прав, наприклад, Український державний департамент інтелектуальної власності. Захист авторського права є важливим для забезпечення справедливої компенсації творців та стимулювання подальшого розвитку творчості та інновацій. Водночас, забезпечення ефективного захисту авторських прав вимагає балансу між правами авторів та правами споживачів творів, зокрема правом на доступ до інформації та свободою використання творів у певних обставинах. Для захисту авторського права застосовуються різноманітні юридичні засоби. Найпоширенішим з них є позови за порушення авторських прав, коли автор чи власник права звертається до суду з вимогою зупинити порушення його прав та отримати компенсацію за завдані збитки. Зазвичай у таких випадках доводиться доводити факт порушення авторських прав та збитки, завдані внаслідок цього. У більшості країн існують законодавчі норми, які регулюють права творців на їхні твори та встановлюють порядок захисту авторських прав. В Україні, наприклад, основним законом, що регулює авторське право та суміжні права, є Закон України «Про авторське право та суміжні права». Цей закон визначає права творців на їхні твори, а також встановлює процедури та умови їх захисту [1, 2].

Згідно з цим законом, авторське право є особистим та майновим правом творця, яке надає йому право контролювати використання свого твору і здійснювати контроль за використанням твору іншими особами. Авторське право виникає з моменту створення твору і не потребує реєстрації. Закон також встановлює види творів, які захищені авторським правом, а саме: літературні, наукові, художні та інші твори, які відповідають критеріям оригінальності та інтелектуальної творчості. Захист авторських прав забезпечується як цивільним, так і кримінальним шляхом. Цивільний захист полягає у захисті права власності та права авторства та може бути здійснений шляхом подання позову до суду. Кримінальний захист передбачає відповідальність за порушення авторських прав у вигляді штрафу, умовного засудження, або позбавлення волі. Законодавство України також передбачає санкції за порушення авторських

прав, у тому числі штрафи та заборону використання твору. Також, як і в інших країнах, у разі порушення авторських прав, автор має право звернутися до суду з вимогою відшкодування збитків та зупинення порушення його прав.

Патентне право − це галузь права, яка стосується захисту винаходів, які мають практичне застосування і є новими та оригінальними. Патент надає його власнику ексклюзивне право на використання винаходу протягом певного періоду часу, зазвичай 20 років з дати подання заявки на патент. У патентному праві передбачені вимоги до заявки на патент, яка повинна містити опис винаходу та відомості про його автора, а також заяву про надання патенту. Після подання заявки на патент, вона проходить процедуру експертизи, під час якої перевіряється, чи відповідає винахід критеріям патентної здатності. Якщо патент отримано, то власник патенту може використовувати свій винахід у комерційних цілях та забороняється його використання без його дозволу. Якщо патентне право порушується, власник патенту має право звернутися до суду з вимогою відшкодування збитків та зупинення порушення його прав. У більшості країн існують національні органи, які відповідають за надання патентів та контроль за їхнім використанням. Крім того, існують міжнародні організації, такі як Всесвітня організація інтелектуальної власності (ВОІС), які забезпечують координацію між країнами щодо захисту патентів та інших об'єктів інтелектуальної власності на міжнародному рівні [2].

Торговельна марка − це знак, який ідентифікує товари або послуги певного виробника та відрізняє їх від товарів та послуг інших виробників. Знак обслуговування − це знак, який ідентифікує послуги певного постачальника та відрізняє їх від послуг інших постачальників. Зареєстрована торговельна марка або знак обслуговування надає їх власникові ексклюзивне право на використання цих знаків у комерційних цілях та забороняється їх використання без дозволу власника. Таким чином, зареєстрована торговельна марка або знак обслуговування дозволяють виробнику або постачальнику відрізнятися від конкурентів та створювати імідж бренду. У більшості країн існують законодавчі норми, які регулюють захист торговельних марок та знаків обслуговування. Зазвичай процедура отримання реєстрації торговельної марки або знаку обслуговування передбачає подання заявки, яка містить зображення знака, його опис та відомості про власника. Якщо знак обслуговування або торговельна марка порушується, власник має право звернутися до суду з вимогою зупинення порушення його прав та відшкодування збитків. Міжнародні організації, такі як Всесвітня організація інтелектуальної власності (ВОІС), забезпечують координацію між країнами щодо захисту торговельних марок та знаків обслуговування на міжнародному рівні.

Технічний захист інтелектуальної власності − це застосування технологій та заходів забезпечення безпеки, які допомагають захистити інтелектуальну власність від несанкціонованого використання, крадіжки або підробки. Один з таких методів технічного захисту − це шифрування даних. Шифрування даних дозволяє захистити конфіденційні дані, такі як комерційні та технічні розробки, від несанкціонованого доступу. Дані шифруються таким чином, щоб їх можна було розшифрувати тільки з допомогою ключа, який знає лише власник інтелектуальної власності. Іншим методом технічного захисту є застосування електронних підписів. Електронний підпис − це електронна форма підпису, яка забезпечує ідентифікацію особи, яка підписує документ, та підтвердження автентичності підпису. Застосування електронних підписів дозволяє захистити електронні документи, такі як контракти та патентні заявки, від несанкціонованого доступу та підробки. Технічний захист інтелектуальної власності також може включати застосування технічних засобів захисту від копіювання та розповсюдження програмного забезпечення та інших інтелектуальних власностей. Наприклад, технічний захист програмного забезпечення може включати захист від зворотного інжинірингу, що допомагає уникнути розкриття коду програми та крадіжки програмного коду [1, 3].

Криптографічні методи захисту даних є одним із найбільш ефективних методів захисту інтелектуальної власності, оскільки вони забезпечують захист даних від несанкціонованого доступу та зламу. Криптографія є наукою про захист інформації від несанкціонованого

доступу шляхом застосування криптографічних алгоритмів. Одним із основних методів криптографічного захисту даних є шифрування. Шифрування полягає в перетворенні звичайного тексту (відкритого тексту) у шифротекст за допомогою спеціального алгоритму (шифрувального алгоритму). Шифрувальний алгоритм залежить від ключа, який використовується для шифрування. Зашифрований текст можна розшифрувати за допомогою ключа, який використовується для дешифрування. Інший метод криптографічного захисту даних − це хешування. Хешування є методом, що забезпечує створення унікального відбитка даних, який може бути використаний для перевірки цілісності даних та виявлення будь-яких змін в них. Хешування застосовується для захисту від несанкціонованого доступу до баз даних, програмного забезпечення та інших видів інформації. Криптографічні методи захисту включають також електронний цифровий підпис (ЕЦП). ЕЦП є методом, який забезпечує автентифікацію та цілісність електронних документів та інших даних. ЕЦП гарантує, що документ був створений автором і не був змінений після підписання [2].

До криптографічних методів захисту інтелектуальної власності належать:

1. Симетричне шифрування: використовується один і той же ключ для шифрування та розшифрування інформації. Недоліком цього методу є необхідність довіряти цей ключ всім, хто має доступ до інформації.

2. Асиметричне шифрування: використовується два ключі − приватний та публічний. Приватний ключ зберігається власником інформації, а публічний ключ може бути відкритим для використання будь-якою особою. Цей метод є більш безпечним, оскільки немає необхідності довіряти ключі всім користувачам інформації.

3. Хешування: метод, в якому вихідний текст перетворюється на хеш-код − унікальний набір символів, який не може бути зворотно перетворений в вихідний текст. Хеш-код може використовуватися для перевірки цілісності даних.

4. Цифровий підпис: використовується для підтвердження автентичності документа або повідомлення. Цифровий підпис формується на основі приватного ключа власника інформації та додається до документа. Публічний ключ може бути використаний для перевірки автентичності підпису.

5. Стеганографія − метод захисту інформації, що полягає в таємному вбудовуванні даних в інший файл або повідомлення без зміни зовнішнього вигляду останнього, наприклад, у зображеннях, аудіо або відеофайлах. Таким чином, відправник може захистити свою інтелектуальну власність, вбудовуючи її у зображення чи інший файл і передаючи його безпосередньо або через мережу.

6. Віртуальна приватна мережа дозволяє захистити передачу даних від несанкціонованого доступу, використовуючи шифрування трафіку та підключення через безпечний тунель.

Цифрові водяні знаки є одним з ефективних методів захисту інтелектуальної власності в цифровому середовищі. Це технологія, яка дозволяє ставити на цифрові об'єкти, такі як зображення, відео та аудіофайли, унікальні захистні мітки. Ці мітки можуть бути невидимими для людського ока або мати спеціальний вигляд, наприклад, логотип компанії. Цифрові водяні знаки можуть мати різні функції. Вони можуть використовуватися для визначення авторства, захисту від копіювання, контролю використання та для збору статистичної інформації про користування цифровими об'єктами. Одним з основних переваг цифрових водяних знаків є те, що вони є ефективними для захисту інтелектуальної власності в онлайн середовищі. Вони можуть захистити авторські права на зображення, які можуть бути завантажені з Інтернету і використовуватися без дозволу власника авторських прав. Крім того, вони можуть допомогти виявити плагіат та інші порушення авторських прав [2].

Технології DRM (Digital Rights Management, управління цифровими правами) − це методи та системи, що дозволяють контролювати доступ та використання цифрових матеріалів (відео, музика, електронні книги тощо) та забезпечувати захист авторських прав. DRM-технології можуть використовуватися для захисту від копіювання, заборони відтворення та надання доступу до вмісту тільки тим користувачам, які мають відповідний

дозвіл. Одним з найпоширеніших методів DRM-захисту є шифрування вмісту. Користувачі, які мають доступ до цифрового вмісту, отримують ключ для дешифрування вмісту. Цей ключ може бути збережений на локальному пристрої користувача або використовувати ключ, що генерується з допомогою DRM-серверів, які контролюють доступ до вмісту. DRM-технології також можуть бути вбудовані в обладнання, такі як пристрої для відтворення відео або аудіо. Наприклад, відео-пристрої можуть мати технологію HDCP (High-bandwidth Digital Content Protection), яка забезпечує захист від копіювання високоякісного відео, що передається через цифрові інтерфейси, такі як HDMI. Інші методи DRM-захисту включають управління ліцензіями, цифрові підписи та механізми контролю доступу. Управління ліцензіями визначає умови використання цифрового вмісту та може обмежувати часові рамки використання вмісту або кількість пристроїв, на яких можна використовувати цифровий вміст [3].

Правовий захист інтелектуальної власності є однією з ключових складових захисту інтелектуальної власності. Для захисту авторських прав, патентів, торговельних марок та інших видів інтелектуальної власності в кожній країні існують відповідні законодавчі акти. Правовий захист інтелектуальної власності передбачає можливість звернутися до суду для вирішення питань про порушення права на інтелектуальну власність, отримання компенсації за завдані збитки та забезпечення заборони на подальше порушення права. Крім того, деякі країни мають спеціалізовані суди для вирішення питань інтелектуальної власності, які є більш кваліфікованими та спроможними розглядати складні питання, пов'язані з інтелектуальною власністю. Налагодження ефективного правового захисту інтелектуальної власності є важливим кроком у забезпеченні стійкості та розвитку інноваційної економіки та підтримці прав творців та власників інтелектуальної власності [2].

Технічний захист інтелектуальної власності є одним зі способів захисту прав на інтелектуальну власність. Технічні методи захисту можуть бути використані для захисту авторських прав, патентів, торговельних марок та інших видів інтелектуальної власності. Один зі способів технічного захисту − це захист від копіювання. Наприклад, використання DRM-технологій (Digital Rights Management) дозволяє обмежити доступ до цифрових контентів, таких як музика, книги та інші електронні матеріали, і забезпечити їхню авторську правовласність. Інші методи технічного захисту можуть включати використання водяних знаків, електронних підписів, антивірусного програмного забезпечення та інших технічних засобів, які допомагають встановити автентичність, цілісність та конфіденційність інтелектуальної власності. Технічний захист інтелектуальної власності є важливим елементом захисту прав на інтелектуальну власність. Технічні методи захисту можуть бути більш ефективними в деяких випадках, аніж правові методи, оскільки вони можуть забезпечити більш високий рівень захисту на технічному рівні. Однак важливо пам'ятати, що технічні методи захисту не є абсолютно надійними, і їх можна обійти з використанням відповідного знання та технологічних засобів. Тому технічний захист слід доповнювати правовим захистом для забезпечення найвищого рівня захисту прав на інтелектуальну власність [1, 3].

Один з прикладів успішного використання правового захисту інтелектуальної власності є справа між компаніями Apple та Samsung, яка стала однією з найбільш відомих в історії правових битв між великими технологічними компаніями. У 2011 році компанія Apple подала позов до суду в США, звинувачуючи Samsung в порушенні патентних прав, пов'язаних з їхнім смартфоном Galaxy S. Samsung відповіла позовом, звинувачуючи Apple в порушенні своїх патентних прав на деякі технології, що використовуються в iPhone. Ця справа тривала кілька років та затягувалася через низку апеляційних процесів, але в 2018 році Samsung погодилася заплатити компанії Apple більше 500 мільйонів доларів за порушення її патентних прав. Цей приклад показує, що правовий захист інтелектуальної власності може бути дуже важливим для технологічних компаній, які вкладають значні зусилля та ресурси в розробку нових технологій. Захист інтелектуальної власності може допомогти компаніям захистити свої інновації та зберегти свої інвестиції. Крім того, великою необхідністю є застосування комплексного підходу до захисту інтелектуальної власності, оскільки він може включати як правові, так і технічні заходи захисту [3]. Ще одним прикладом успішного використання

технічного захисту інтелектуальної власності − це захист технології за допомогою DRM (Digital Rights Management) в музичній індустрії. Технологія DRM включала в себе криптографічний захист, що забезпечував шифрування музичних файлів та дозволяв їх відтворювати тільки на пристроях, які були пов'язані з обліковим записом користувача. Це забезпечувало, що лише користувач, який придбав музику, міг її відтворити. Зараз багато інших компаній також використовують технологію DRM для захисту своїх інтелектуальних власностей, включаючи компанії, які займаються видавництвом книг та відеоігор. У 2001 році Apple випустила iPod − портативний програвач музики, який вміщував до 1 000 пісень. Для того, щоб користувачі могли купувати музику для своїх пристроїв, Apple створила онлайн-магазин музики iTunes Store, який використовував технологію DRM, щоб захистити музичні файли від незаконного копіювання та поширення.

Висновки. Захист інтелектуальної власності є важливим аспектом для забезпечення стимулювання інноваційного розвитку та збереження конкурентоспроможності в бізнесі та економіці в цілому. Захист інтелектуальної власності також має важливе значення для захисту споживачів від шахрайства та підробок, що можуть бути небезпечні для здоров'я та безпеки. Захист інтелектуальної власності також сприяє забезпеченню стабільного розвитку ринку та господарства в цілому, забезпечується розробкою нових технологій та відкриттям нових ринків. Також важливо зазначити, що захист інтелектуальної власності сприяє розвитку наукових досліджень та технологій, оскільки вона забезпечує інвестиційну привабливість та довгостроковий розвиток інтелектуальної власності. Отже, захист інтелектуальної власності є важливим елементом економічного розвитку, що забезпечує конкурентоспроможність, інноваційний розвиток та забезпечує безпеку та здоров'я споживачів. Захист інтелектуальної власності є важливим аспектом для бізнесу, наукових досліджень та розвитку технологій. Оскільки це є не лише важливим інструментом забезпечення захисту авторських прав, а й інші форми інтелектуальної власності, такі як патенти, товарні знаки та інші, використовуються для захисту технічних рішень, винаходів та розробок.

У зв'язку з тим, що захист інтелектуальної власності забезпечує конкурентну перевагу на ринку, використання комплексного підходу до захисту стає надзвичайно важливим. Такий підхід передбачає використання різних методів захисту інтелектуальної власності, таких як правовий захист, технічний захист та застосування криптографічних технологій, що дозволяє забезпечити максимальний рівень захисту.

Список використаних джерел

1. Пугач А.В., Петренко В.О. Забезпечення захисту інтелектуальної власності – запорука розвитку та підвищення конкурентоспроможності підприємства. Ефективне використання результатів наукових досліджень та об’єктів інтелектуальної власності: збірник наукових праць за матеріалами ІІІ Міжнар.наук.-практ. конф.(17-18 березня 2021 р.). – НМетАУ, УКРНЕТ, НДІІВ НАПрН України, Дніпро: Юрсервіс, 2021., С. 385-389.

2. Зеров К. О. Особливості захисту авторських прав на твори, розміщені в мережі інтернет: монографія / К. О. Зеров; НДІ інтелектуальної власності. – Київ: Інтерсервіс, 2018. – 220 с.

3. Мартинюк І. В. Використання інформаційних технологій при юрисдикційних та неюрисдикційних способах захисту прав інтелектуальної власності / І. В. Мартинюк // Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття»: у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) – Одеса: Видавничий дім «Гельветика», 2022. – Т. 2. – С. 753-756.

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКА Б.Т.

РОЛЬ МАШИННОГО НАВЧАННЯ В УДОСКОНАЛЕННІ МОДУЛІВ HR

КОРОБКО О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Дане дослідження спрямоване на визначення ролі системи управління людськими ресурсами на основі машинного навчання в HR системах на основі світових наукових джерел. Технологія забезпечує унікальний спосіб введення, опрацювання та виведення даних, що, дає змогу підвищувати показники продуктивності фахівців у напрямку HR. Однак обсяг даних, що генеруються цими системами, ускладнює їхній аналіз та інтерпретацію сприйняття людиною. Машинне навчання стало потужним інструментом для обробки значних об'ємів вхідної інформації.

This study is aimed at determining the role of machine learning-based human resource management systems in HR systems based on global scientific sources. The technology provides a unique way to input, process and output data, which allows to increase the productivity of HR professionals. However, the volume of data generated by these systems makes it difficult to analyze and interpret it in a human way. Machine learning has become a powerful tool for processing large amounts of input.

Актуальність. З появою технологій управління людськими ресурсами зазнало революції, а машинне навчання стало невід'ємним компонентом HR. Алгоритми машинного навчання можуть автоматизувати різні HR-функції, включаючи рекрутинг, утримання співробітників, управління ефективністю та управління талантами. Тому важливо розуміти роль машинного навчання в удосконаленні HR-модулів.

Метою статті є вивчення ролі машинного навчання в удосконаленні модулів управління персоналом, а також визначення переваг і викликів впровадження машинного навчання в HR.

Завдання статті є аналіз алгоритмів машинного навчання, що використовуються в HR, та оцінити їхню ефективність у вдосконаленні HR-модулів.

Об'єктом дослідження є HR-модулі, які можна вдосконалити за допомогою алгоритмів машинного навчання.

Виклад основного матеріалу. Організації а тим паче в технологічних галузях завжди прагнуть наймати співробітників, які більш підковані в цифрових технологіях. В умовах конкурентного ринку вкрай важливо, щоб потенціал кандидата було використано по максимуму для кращого організаційного успіху. Саме тому кожен фахівець у сфері управління людськими ресурсами має на меті оптимізувати обробку потоку даних і скоротити час без шкоди для якості прийняття рішень. У таких умовах людські ресурси залишаються одним з основних відмінних факторів для організації, які можуть бути використані для конкурентного зростання для створення необхідної організаційної цінності. Кінцевою метою інтеграції машинного навчання в управління людськими ресурсами є забезпечення того, щоб людські ресурси організації були активом, а оптимальне використання людського капіталу - безперервним процесом. Тому організації повинні постійно докладати зусиль для вдосконалення своїх систем на основі машинного навчання, щоб йти в ногу з постійно мінливим технологічним ландшафтом і залишатися конкурентоспроможними на ринку.

Управління людськими ресурсами - це галузь знань, орієнтована на впровадження практик і підходів для досягнення організаційних цілей, а інтеграція машинного навчання може дозволити їм приймати рішення на основі даних і відбирати кандидатів з необхідними навичками, щоб досягти успіху в сучасній технологічній індустрії. Кожен фахівець цієї галузі має основними цілями: оптимізувати опрацювання потоку даних і зниження часу без втрати

якості ухвалення рішення. Для досягнення цих цілей, системи на основі машинного навчання повинні охоплювати безліч усталених стратегій і практик, які довели свою ефективність, а також створення нових, характерних для даного контексту, аналітика вхідної та вихідної інформації. Однак, для того щоб управління людськими ресурсами було ефективним, зміни та нововведення приносили позитивні результати або матимуть вигідні наслідки, система має бути орієнтована на більш глибший аналіз введених змінних, які будуть оброблятися за допомогою принципів обробки даних на основі нейронних зв'язків (машинного навчання). Щоб подолати проблеми, пов'язані з оцінкою аналізу, який виконує система, і поліпшити масштабованість систем, заснованих на машинному навчанні, в управлінні людськими ресурсами, організації можуть дослідити передові методи, такі як глибоке навчання, обробка природної мови і комп'ютерний зір. Ці методи дозволяють створювати більш складні моделі, які можуть навчатися на великих обсягах даних і видавати більш точні результати.

Для визначення доцільності використання принципів машинного навчання в HR-системах необхідно провести зіставлення основних принципів машинного навчання з одним із його підвидів, а саме - глибинне навчання (Deep Learning). Таке порівняння має місце через відмінності в способі обробки даних. Варто підкреслити важливість і цінність систем, які надають аналіз або можливість аналізу методів, на яких ґрунтується система під час ухвалення рішення. Оскільки будь-яка система з принципами машинного навчання, незалежно від алгоритмів, на яких вона була побудована, почати аналізувати ввідні дані за структурою, до якої ці дані не призначені або не піддаються аналізу за такими структурами.

Глибинне навчання адаптує багаторівневий підхід до прихованих пластів нейронної мережі. У традиційних підходах до машинного навчання функції визначають і витягують або вручну, або з використанням методів вибору функцій. Однак у цих моделях функції вивчаються і витягуються автоматично, що забезпечує більш високу точність і продуктивність. Як правило, гіперпараметри моделей класифікаторів також вимірюються автоматично. Потрібно враховувати відмінності в класифікації полярності між двома підходами: традиційним машинним навчанням (машина опорних векторів, байєсівські мережі або дерева рішень) і глибоким навчанням (Рис. 1). Так само глибинне навчання має багаторівневий нейронний кластерний зв'язок із прихованими пластами, подібний до нейронів людського мозку. Окрім того це цілісна структура, зібрати аналітику з прихованих пластів, тобто принципи, за якими була дана відповідна відповідь, важко або без відповідного ПЗ неможливо (Рис. 2) [1]. Важко дізнатися, який нейронний вузол був активний і як вузли поводилися для видачі певного результату. Так як для HR систем з машинним навчанням, визначення причин є основним фактором під час вибору таких систем. Важливо вказати і той момент, що глибинне навчання розкриває свій потенціал на великих об'ємах даних, що, своєю чергою, вимагає значних обчислювальних можливостей, але точність обчислення при цьому підвищується [2].

Робота з даними відбувається за принципом "що більше даних, то точніший результат", тобто обчислювальні можливості зростають, на рівні з цим зростають і витрати ресурсів системою на обробку даних. Адміністрування та фінансові витрати вищі, ніж на подібні системи на інших алгоритмах машинного навчання [3].

Виходячи з відмінностей у принципах роботи алгоритмів машинного навчання та окремо глибинного навчання, є відмінності в побудові блоків обробки даних та інша структура аналізу даних (Рис. 1). Після попереднього опрацювання даних, вхідний пласт передає попередньо відсортовану інформацію в приховані пласти, в них же алгоритм ухвалює певне рішення і дає результат. І як зазначалося раніше, важко або немає можливості дати оцінку аналізу, який було проведено системою. Інші алгоритми менш затратні з точки зору технічних вимог, але в той же час на великих обсягах даних кожен наступний обсяг дає менший приріст обчислювальних можливостей програмного забезпечення. Крім того, необхідно знайти компроміс між складністю моделі та можливістю інтерпретації результатів. Хоча складні моделі можуть пропонувати кращу точність, їх часто складніше інтерпретувати, що може бути

проблемою в таких контекстах, як управління людськими ресурсами, де рішення можуть мати значний вплив на життя людей.

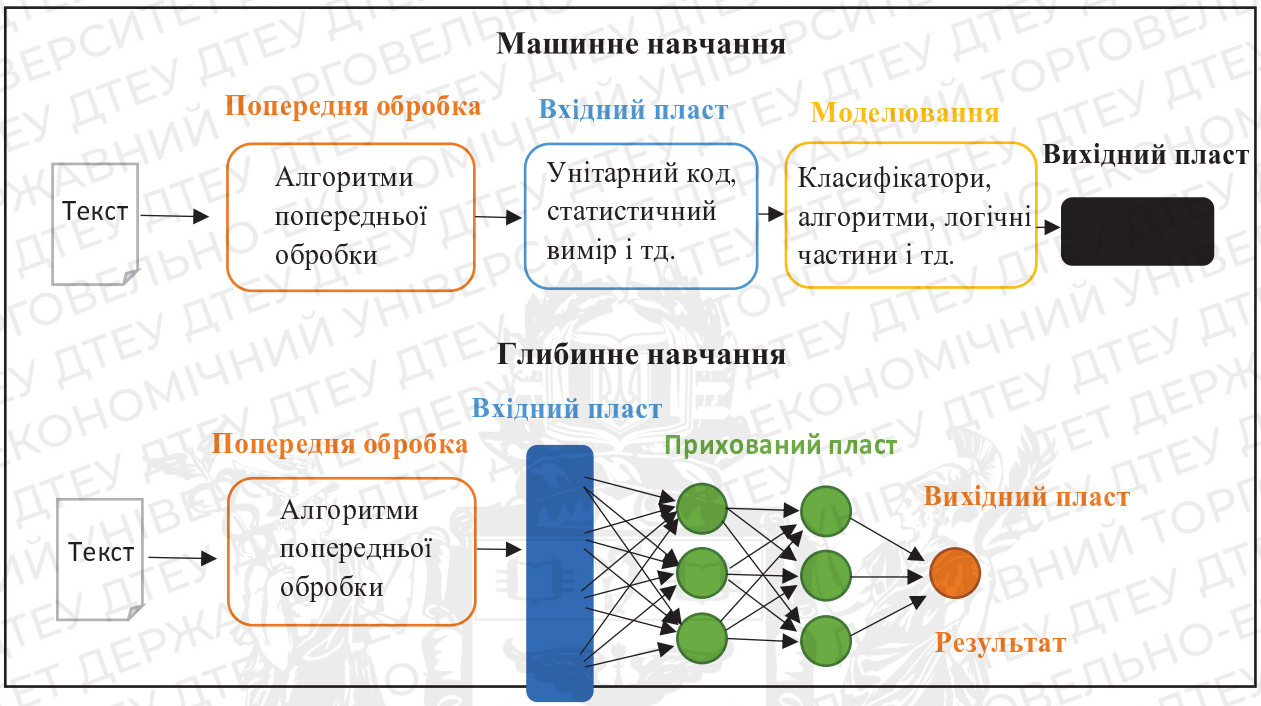


Рис.1. Відмінності між двома підходами до класифікації полярності, машинного навчання (вгорі) і глибокого навчання (внизу).
Джерело: адаптовано автором з [4]

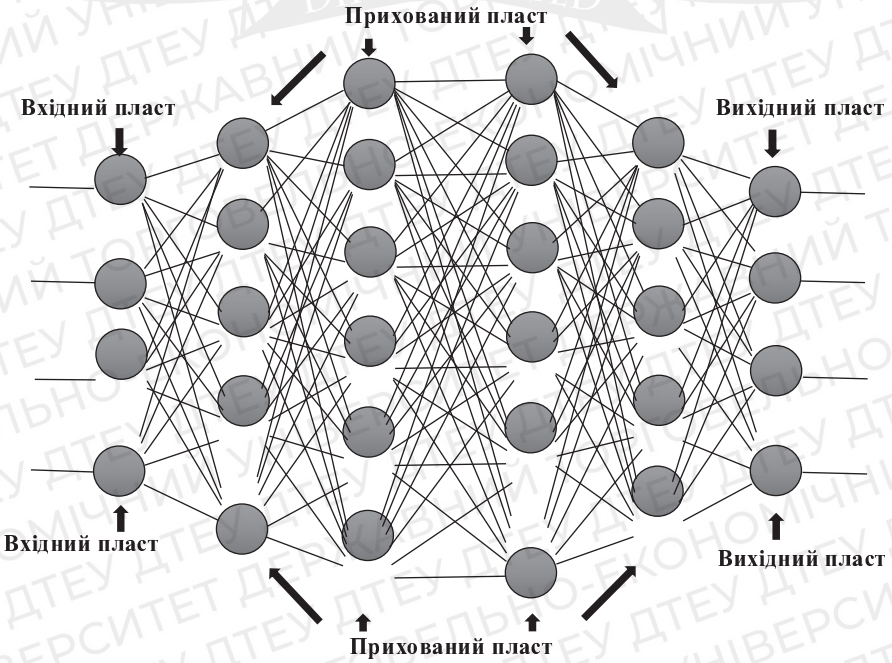


Рис. 2. Типи групування нейронних вузлів у глибинному навчанні
Джерело: Зроблено автором

Викладені вище дані дають розуміння в доцільності розглядати системи, які побудовані на принципах обох алгоритмів. Доповнювати систему, нівелювати недоліки різних алгоритмів машинного навчання для досягнення максимальної продуктивності системи. В свою чергу ці кроки дають можливість програмного аналізу даних, на яких ґрунтувалася система під час видачі результату, що є ключовим фактором під час вибору/створення таких систем.

Аналітика даних систем є важливим аспектом для досягнення результату і вносить у широку сферу HR певні технічні обмеження, як-от адміністрування та підтримка працездатності [5]. Дана аналітика дає можливість фахівцям HR реалізувати завдання поставленими керівництвом, а також залишає простір для зростання в цій галузі та вивчення актуальності аналітики в різних категоріях, що підпадають під категорії управління людськими ресурсами [6]. Що дає приріст у продуктивності даних фахівців. У системах на основі машинного навчання коректність даних і результати опрацювань, які можна витягти з них, мають значний вплив на продуктивність моделей і здатність до навчання. Як наслідок, перед подачею даних на вхід необхідно їх підготувати.

Роль рішень машинного навчання, що обробляють вхідні запити з управління ресурсами необхідні. Адже більшість організацій вже використовують штучний інтелект і різні системи в HR на основі машинного навчання, як-от чат-боти, системи які використовують машинне навчання й автоматизація роботизованих процесів в управлінні людськими ресурсами, що допомагають у рекрутингу, скринінгу, адаптації, інтерв'юванні тощо.

Оскільки використання машинного навчання в управлінні персоналом продовжує зростати, організаціям важливо розуміти потенційні переваги та обмеження цих систем. Однією з головних переваг є можливість спростити й автоматизувати багато HR-процесів, звільнивши час і ресурси для більш стратегічних ініціатив. Наприклад, чат-боти та автоматизовані системи скринінгу можуть швидко та ефективно обробляти первинну комунікацію та оцінку кандидатів, дозволяючи HR-фахівцям зосередитися на більш складних завданнях, таких як співбесіди та адаптація.

Ще однією перевагою HR-систем на основі машинного навчання є їхня здатність аналізувати великі обсяги даних для виявлення закономірностей і тенденцій, які можуть бути не одразу очевидними для аналітиків, що працюють з людьми. Це може бути особливо корисно в таких сферах, як залучення та утримання працівників, де відіграють роль такі складні фактори, як задоволеність роботою, баланс між роботою та особистим життям і компенсація. Аналізуючи дані опитувань працівників, оцінок ефективності роботи та інших джерел, алгоритми машинного навчання можуть допомогти організаціям визначити потенційні сфери для вдосконалення та розробити цільові стратегії для їх вирішення.

HR-системи на основі машинного навчання також можуть допомогти спростити багато адміністративних завдань, пов'язаних з управлінням персоналом, таких як перевірка резюме та складання шорт-листа кандидатів. Чат-боти та інші інструменти на основі машинного навчання можуть обробляти багато рутинних запитів і звернень, які відділ кадрів отримує щодня, звільняючи працівників відділу кадрів для виконання більш складних завдань. Однак важливо зазначити, що системи машинного навчання не є панацеєю від усіх проблем у сфері управління персоналом. Вони ефективні лише настільки, наскільки ефективні дані, на яких вони навчаються, а упередженість навчальних даних може призвести до упередженого прийняття рішень. Важливо також забезпечити прозорість і зрозумілість HR-систем на основі машинного навчання, щоб фахівці з управління персоналом і працівники могли розуміти, як приймаються рішення.

Крім того, машинне навчання можна використовувати для підвищення точності та ефективності програм навчання працівників. Аналізуючи дані про ефективність роботи співробітників і виявляючи слабкі місця, алгоритми машинного навчання можуть рекомендувати індивідуальні навчальні програми, спеціально розроблені для усунення наявних та майбутніх недоліків.

Загалом, використання машинного навчання в управлінні персоналом має потенціал докорінно змінити те, як організації управляють своїми людськими ресурсами. Однак організаціям важливо підходити до цих систем з обережністю і переконатися, що вони впроваджуються таким чином, щоб максимізувати їхні потенційні переваги, мінімізуючи ризики та обмеження. Таким чином, організації можуть гарантувати, що вони використовують новітні технології для підтримки своїх співробітників і досягнення успіху в бізнесі.

Машинне навчання виявляється надзвичайно важливим інструментом в удосконаленні модулів управління ресурсами людських відносин (HR). Аналіз результатів дослідження підтверджує, що машинне навчання може суттєво покращити робочі процеси, оптимізувати прийняття рішень та сприяти більш ефективному управлінню персоналом.

Однією з ключових ролей машинного навчання є здатність до аналізу великих обсягів даних. Модулі HR зазвичай включають велику кількість інформації про співробітників, вакансії, навчання та інші аспекти. Машинне навчання дозволяє автоматизувати процес обробки цих даних, виявляти в них корисні зв'язки та патерни, що забезпечує більш точне та швидке прийняття рішень.

Додатково, машинне навчання може використовуватися для прогнозування тенденцій на ринку праці та внутрішніх змін в компанії. Це дозволяє модулям HR бути готовими до майбутніх викликів та забезпечувати збалансовану робочу силу.

Висновки. Останнім часом спостерігається тенденція до впровадження в різних галузях систем на основі машинного навчання. Одним з головних чинників, що зумовлюють тенденцію впровадження цих систем в різних галузях, є потреба в постійному вдосконаленні. Компанії постійно прагнуть оптимізувати свої процеси, зменшити витрати та підвищити ефективність, і машинне навчання стало потужним інструментом для досягнення цих цілей. Штучний інтелект і машинне навчання використовуються багатьма компаніями у відділах кадрів, де такі системи виконують допоміжну, а інколи й основну роль у наборі персоналу, аналізу продуктивності, збиранню даних, надання інформації в режимі реального часу та наданні точної інформації. В результаті вони можуть надавати цінну інформацію, яка допоможе організаціям приймати обґрунтовані рішення та вдосконалювати HR-процеси в цілому. Впроваджуючи алгоритми машинного та глибокого навчання в HR-системи, організації можуть отримати конкурентну перевагу та краще управляти своїми людськими ресурсами. Ці технології дозволяють організаціям оптимізувати свої процеси, зменшити витрати, підвищити ефективність та приймати рішення на основі даних. Загалом, машинне навчання є потужним інструментом, який має потенціал для трансформації систем управління персоналом та вдосконалення способів управління найціннішим активом організацій - їхніми спеціалістами.

Список використаних джерел

1. Aggarwal C. «Neural Networks and Deep Learning». 2018. 20-43p. ISBN: 978-3-319-94463-0
2. Sukwoong Choi, Namil Kim, Junsik Kim, Hyo Kang. How Does AI Improve Human Decision Making. 2020. 4-6; dx.doi.org/10.2139/ssrn.3893835
3. Neural Networks and Deep Learning. Електронний ресурс. URL: http://neuralnetworksanddeeplearning.com/ (дата звернення 10.04.2023).
4. Gattan M. Deep Learning Technique of Sentiment Analysis for Twitter Database. dx.doi.org/10.3991/ijim.v16i01.27575
5. Abdulquddus Mohammed. HR ANALYTICS: A MODERN TOOL IN HR FOR PREDICTIVE DECISION MAKING. 2019. 52-58; dx.doi.org/10.34218/JOM.6.3.2019.007
6. Gloria Phillips-Wren. Artificial Intelligence for Decision Making. 2006. 2 -10.

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А.М.

ІНЖЕНЕРІЯ СОЦІАЛЬНИХ АТАК ЯК ЗАГРОЗА ФІЗИЧНОМУ ЗАХИСТУ ІНФОРМАЦІЇ

КОРОТИЧ І., 2м курс ФІТ ДТЕУ,
спеціальність "Кібербезпека та захист інформації"

Стаття,висвітлює тему інженерії соціальних атак як загрози фізичному захисту інформації. Інженерія соціальних атак - це процес маніпулювання людьми з метою отримання доступу до конфіденційної інформації або здійснення іншої злочинної діяльності.

Такожс таття розглядає, як такі атаки можуть стати загрозою для фізичного захисту інформації, що означає захист інформації від фізичних загроз, таких як крадіжка комп'ютера або USB-накопичувача, підміна чи крадіжка пристроїв зберігання даних тощо.

The article covers the topic of social attack engineering as a threat to the physical protection of information. Social attack engineering is the process of manipulating people to gain access to confidential information or to carry out other criminal activities.

The article also examines how such attacks can pose a threat to physical information security, which means protecting information from physical threats such as theft of a computer or USB drive, substitution or theft of storage devices, etc.

Актуальність. Тема актуальна оскільки загроза атак соціальної інженерії на фізичну інформаційну безпеку є дуже актуальною і нагальною проблемою в сучасну цифрову епоху. Зі зростанням залежності від технологій та збільшенням обсягів конфіденційної інформації, що зберігається в цифровому вигляді, потенційні наслідки успішної атаки можуть бути руйнівними. Атаки соціальної інженерії стають все більш витонченими і їх все важче виявляти, тому організаціям необхідно вживати проактивних заходів для захисту своєї фізичної інформаційної безпеки.

За останні роки відбулося багато гучних атак соціальної інженерії на фізичну інформаційну безпеку, включаючи інциденти, спрямовані на державні установи, фінансові установи та медичні заклади. Ці атаки призвели до значних фінансових втрат, репутаційних збитків і навіть загрози національній безпеці.

Крім того, пандемія COVID-19 створила нові можливості для атак соціальної інженерії, оскільки віддалена робота та онлайн-спілкування полегшують зловмисникам використання вразливостей. Як наслідок, організаціям необхідно зберігати пильність і вживати проактивних заходів для навчання своїх співробітників та впровадження надійних заходів фізичної безпеки.

Дослідити загрозу атак соціальної інженерії для фізичної інформаційної безпеки та підкреслити важливість вжиття проактивних заходів для захисту від таких атак. Стаття має на меті надати всебічний огляд цього питання, включаючи різні форми атак соціальної інженерії, потенційні наслідки успішної атаки та способи, якими організації можуть захистити себе.

Стаття також має на меті підвищити обізнаність про важливість фізичного захисту інформації та надати рекомендації щодо найкращих практик, яких можуть дотримуватися організації, щоб зменшити ризик атак соціальної інженерії. Висвітлюючи останні тенденції та розробки в цій галузі, стаття має на меті озброїти читачів знаннями та інструментами, необхідними для захисту від атак соціальної інженерії та захисту їхньої конфіденційної інформації.

Інженерія соціальних атак полягає в тому, щоб використовувати соціальні і психологічні методи впливу на людей з метою зламування захисту інформації або отримання несанкціонованого доступу до системи. Такі атаки можуть бути надзвичайно ефективними, оскільки вони використовують людську довіру і схильність до певних видів поведінки.

Фізичний захист інформації включає в себе захист комп'ютерних систем та інших пристроїв, які зберігають, обробляють і передають конфіденційну інформацію. Однак, якщо людина стає слабким ланцюгом у цій системі захисту, то її поведінка може стати вразливою для соціальних атак.

Метою статті є інформування та навчання читачів про загрозу атак соціальної інженерії для фізичної інформаційної безпеки, а також заохочення організацій вживати проактивних заходів для захисту від цієї зростаючої загрози.

Об'єктом дослідження є інженерія соціальних атак.

Предметом дослідження є система захисту персональних даних від соціальних атак.

У сучасну цифрову епоху захист конфіденційної інформації має першорядне значення. Компанії та організації інвестують значні кошти у захист своїх даних від кібератак, але фізична безпека часто залишається поза увагою. Однією з найбільших загроз для фізичної безпеки інформації є атаки соціальної інженерії. Ці атаки використовують психологічні маніпуляції, щоб змусити людей розкрити конфіденційну інформацію або отримати несанкціонований доступ до захищених місць або систем. У цій статті ми розглянемо різні типи атак соціальної інженерії та їхній вплив на фізичну інформаційну безпеку, даний вплив на систему можемо помітити на рис 1.

Рис. 1. Загрози які існують для безпеки

Соціальна інженерія - це форма психологічної маніпуляції, яка полягає у впливі на людей з метою змусити їх розголошувати конфіденційну інформацію, приймати рішення або вчиняти дії, яких вони зазвичай не роблять. Мистецтво соціальної інженерії передбачає використання таких методів, як переконання, обман і видавання себе за іншу особу, щоб завоювати довіру цільової аудиторії. Це метод, який використовують хакери, шахраї та аферисти, щоб обманом змусити людей розкрити конфіденційну інформацію, таку як паролі, номери кредитних карток та персональні дані [1].

Соціальна інженерія - це складна і багатогранна галузь, яка охоплює широкий спектр тактик і методів. Деякі з найпоширеніших методів включають фішинг, привід, приманку та послугу за послугу. Фішинг - це метод, який полягає у надсиланні шахрайських електронних листів або повідомлень, які виглядають як такі, що надходять з надійного джерела, наприклад, банку або соціальної мережі, з метою виманити у жертви конфіденційну інформацію. Створення фальшивого приводу або сценарію, щоб обманом змусити жертву розкрити інформацію або виконати певну дію. Приманка передбачає пропозицію винагороди або заохочення об'єкту, щоб переконати його виконати певну дію або розкрити інформацію. Послуга за послугу передбачає пропозицію вигоди в обмін на інформацію або дію.[2]

Соціальна інженерія - це потужний інструмент, який можна використовувати як для добрих, так і для поганих цілей. В умілих руках вона може бути використана для підвищення безпеки та захисту конфіденційної інформації. Наприклад, соціальну інженерію можна використовувати для перевірки безпеки системи, намагаючись отримати несанкціонований доступ за допомогою тактики соціальної інженерії. Це може допомогти виявити вразливі місця в системі та внести необхідні покращення.

Однак соціальну інженерію часто використовують у недобрих цілях. Хакери та кіберзлочинці часто використовують тактику соціальної інженерії, щоб отримати доступ до конфіденційної інформації, такої як реквізити банківських рахунків, персональні дані та облікові дані для входу в систему. Вони також можуть використовувати тактику соціальної інженерії для поширення шкідливих програм та іншого шкідливого програмного забезпечення. Атаки соціальної інженерії можуть бути дуже ефективними, оскільки вони використовують людський фактор безпеки, який часто є найслабшою ланкою в будь-якій системі безпеки.[5]

Щоб протистояти атакам соціальної інженерії, важливо бути обізнаним з різними тактиками і методами, які використовують соціальні інженери. Організації можуть впроваджувати навчальні програми з підвищення обізнаності про безпеку, щоб розповісти працівникам про небезпеку соціальної інженерії, а також про те, як розпізнавати атаки соціальної інженерії та реагувати на них. Вони також можуть впровадити технічні засоби контролю, такі як брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення, щоб запобігти успішним атакам соціальної інженерії.

На рис 2. зображені типи атак соціальної інженерії.

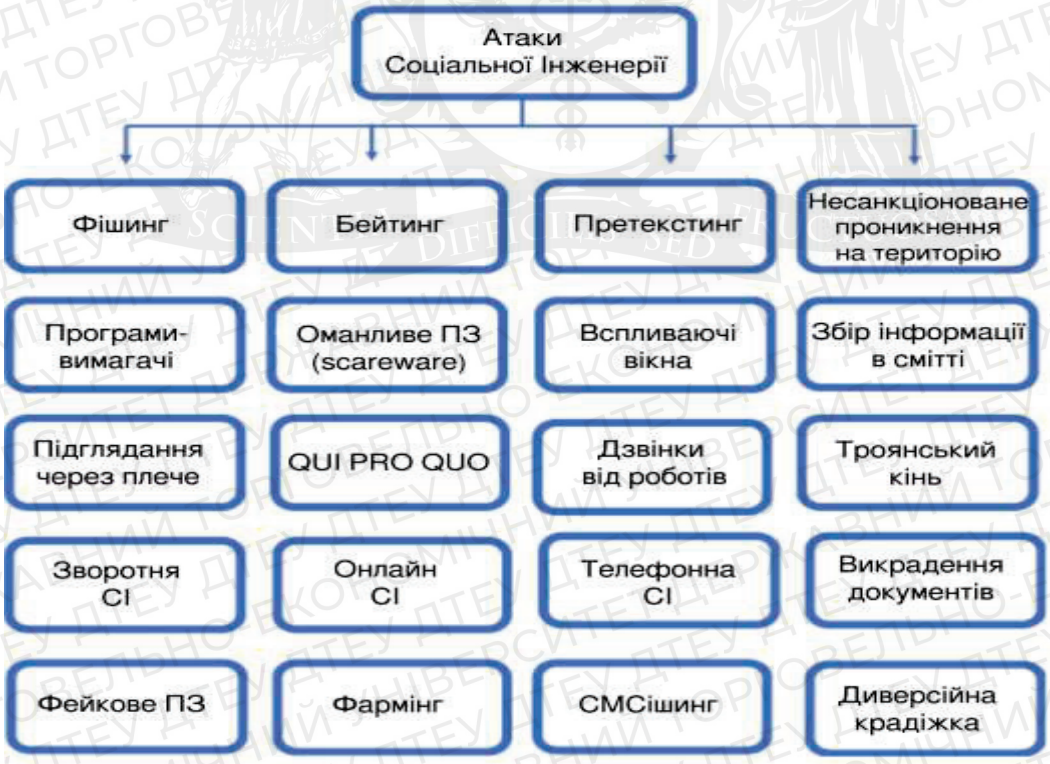


Рис. 2. Типи атак соціальної інженерії

Типи атак соціальної інженерії:

Фішинг: Фішингові атаки передбачають надсилання електронних листів або повідомлень, які виглядають як такі, що походять з легітимного джерела, але насправді походять від зловмисника. Мета цих атак - обманом змусити одержувача надати конфіденційну інформацію, наприклад, облікові дані для входу в систему або фінансову

інформацію. Фішингові атаки можуть бути особливо небезпечними, коли вони націлені на співробітників, які мають доступ до конфіденційної інформації[3].

Приховані атаки: Прихована атака передбачає створення фальшивого приводу або сценарію, щоб завоювати довіру жертви. Зловмисник може видавати себе за представника влади, наприклад, поліцейського або IT-спеціаліста, щоб переконати жертву розкрити конфіденційну інформацію або надати доступ до захищених зон.

Заманювання: Атаки з використанням приманки передбачають пропозицію чогось привабливого, наприклад, безкоштовного USB-накопичувача, в обмін на конфіденційну інформацію або доступ до захищених систем. Ці атаки часто націлені на працівників, які менш уважно ставляться до безпеки.

Quid Pro Quo: Атаки типу "послуга за послугу" передбачають пропозицію вигоди в обмін на конфіденційну інформацію або доступ до захищених систем. Наприклад, зловмисник може запропонувати подарункову картку в обмін на облікові дані для входу в систему[3].

Тейлгейтинг: Переслідування передбачає проходження за уповноваженою особою в безпечну зону без дозволу. Зловмисник може прикинутися загубленим або поспішаючим, щоб отримати доступ до захищеної зони.

Вплив на фізичну інформаційну безпеку:

Атаки соціальної інженерії можуть мати серйозні наслідки для фізичної інформаційної безпеки. Якщо зловмисник отримує доступ до конфіденційної інформації або захищених систем, він може завдати значної шкоди. Наприклад, зловмисник може викрасти конфіденційну інформацію або встановити шкідливе програмне забезпечення на захищену систему. Атаки соціальної інженерії також можуть скомпрометувати заходи фізичної безпеки, такі як системи контролю доступу, обманом змушуючи співробітників надавати несанкціонований доступ до захищених зон.

Атаки соціальної інженерії становлять значну загрозу фізичній інформаційній безпеці. Компанії та організації повинні вжити заходів для навчання співробітників про різні типи атак соціальної інженерії, а також про те, як їх розпізнавати і повідомляти про них. Також важливо впроваджувати надійні заходи фізичної безпеки, такі як системи контролю доступу та камери спостереження, щоб запобігти несанкціонованому доступу до захищених зон. Вживаючи таких заходів, компанії та організації можуть краще захистити свою конфіденційну інформацію від атак соціальної інженерії.[5]

Висновки. Інженерія соціальних атак - це важлива проблема в сфері кібербезпеки, яка потребує уваги та вивчення. Компанії та організації повинні бути обережними і навчати своїх співробітників впізнавати та запобігати соціальним атакам, щоб захистити свою конфіденційну інформацію від зловмисників.

Список використаних джерел

1. Mitnick, K., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.
2. Hadnagy, C. (2018). Social engineering: The science of human hacking. John Wiley & Sons.
3. Goel, S. (2016). Social engineering attacks: A comprehensive guide to phishing, pretexting, and other tactics. Apress.
4. Hadnagy, C. (2015). Unmasking the Social Engineer: The Human Element of Security. John Wiley & Sons.
5. Stajano, F., & Wilson, P. (2011). Security for ubiquitous computing. John Wiley & Sons.

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

МЕТОДИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ WI-FI

КОСТЮК Ю., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні засади побудови захищеної комп'ютерної мережі підприємства з використанням технології Wi-Fi. Зазначено переваги застосування обраної топології, архітектури комп'ютерної мережі підприємства, способів керування мережею, розглядаються питання інформаційної безпеки, надійності системи, вибору програмного та апаратного забезпечення.

The article discusses the basic principles of building a secure enterprise computer network using Wi-Fi technology. The advantages of using the chosen topology, the architecture of the enterprise's computer network, methods of network management are indicated, the issues of information security, system reliability, software and hardware selection are considered.

Актуальність. У сучасному світі активно розвиваються мережні й інформаційні технології. В даний час неможливо знайти підприємство, яке функціонує без впровадженої мережі передач даних. Подібна мережа дозволяє виконувати величезну кількість завдань, максимально спрощуючи різні дії, такі як: обмін інформацією; робота з документами; доступ до різних ресурсів; управління додатками; зберігання інформації. Інформація є дуже цінним ресурсом, тому зловмисники нерідко намагаються отримати доступ до системи підприємства. Вони можуть завдати шкоди, що складається в крадіжці персональних даних і даних компанії, і зараженні системи з повним знищенням ресурсів. Засоби масової інформації дуже часто повідомляють про кібератаки на різні підприємства. Виходить, щоб цього уникнути, потрібно дуже уважно підійти до питання модернізації мережі, особливо з боку безпеки. Не менш важливим є вирішення питання захисту комп'ютерних мереж від можливих атак, направлених на порушення функціонування мереж та окремих вузлів, несанкціонованого доступу до інформації та несанкціонованого використання сервісів мережі. Все це вказує на високу актуальність роботи.

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами: застосовуваними засоби забезпечення інформаційної безпеки, які не відповідають високому рівню; повсюдне використання Інтернет тягне до появи загроз з боку віддалених користувачів; постійне збільшення кількості персональних комп'ютерів, захист яких не відповідає вимогам безпеки; зростання обсягів інформації, що обробляється і зберігається з використанням інформаційних технологій; недосконалість програм і мережевих технологій з точки зору інформаційної безпеки. Тому перед керівництвом будь-якого підприємства рано чи пізно постає питання про об'єднання своєї комп'ютерної мережі з віддаленими майданчиками. Філії в інших містах, замовники, партнери, віддалені співробітники – багатьом групам користувачів може знадобитися надання безпечного доступу до внутрішніх ресурсів мережі.

Метою статті є дослідження особливостей використання методів захисту комп'ютерної мережі підприємства з використанням технології Wi-Fi.

Об'єктом дослідження є розробка захищеної комп'ютерної мережі, яка розробляється для підприємства з використанням технології Wi-Fi.

Предмет дослідження – комп'ютерна мережа підприємства.

Аналіз попередніх досліджень. Загальнотеоретичні аспекти дослідження безпеки комп'ютерної мережі представлені в публікаціях вітчизняних та закордонних науковців: В.О. Хорошко, В.П. Кучернюка, В.С. Заборовського, В.А. Світличного, М.В. Грайворонського, С.Е. Остапова та ін.

Виклад основного матеріалу. В даний час використання комп'ютерних мереж є невід'ємною частиною нашого життя, область їх застосування охоплює всі сфери людської діяльності. Комп'ютерна мережа – це сукупність комп'ютерів і різних пристроїв, що забезпечують інформаційний обмін між комп'ютерами в мережі без використання будь-яких проміжних носіїв інформації. Розвиток комп'ютерних мереж пов'язано як з розвитком власне ЕОМ, що входять до складу мережі, так і з розвитком засобів телекомунікацій [1,2].

З розвитком мережевих технологій виникла потреба в міжмережних екранах, потім в системах запобігання вторгнень. Зараз для захисту персональних даних, крім антивіруса, брандмауера і засобів запобігання вторгнень, необхідно також використовувати засоби контролю цілісності і сканер вразливостей. Коли мережа піддається вторгненню, DoS-атаці або вірусної епідемії, під загрозою опиняється діяльність всієї організації. Це відбувається тому, що збільшується небезпека для операційних ресурсів, призначених для користувача даних, власних коштів і технологій. Інтелектуальна власність може бути вкрадена і неправомірно використано третьою стороною. Захист локальних мереж підприємств з кожним роком стає все більш складним завданням і сьогодні є одним з основних факторів, з якими стикається бізнес. Нові загрози з'являються на регулярній основі, і жодна організація від них не застрахована. Варто зазначити, що кожен раз при появі нового виду небезпечних загроз змінюється саме поняття «безпечна мережа».

Створення захищеної комп'ютерної мережі – це найкращий спосіб організації єдиного інформаційного середовища підприємства. Завдяки їй користувачі отримають доступ до загальних ресурсів, зможуть спільно використовувати принтери та інше мережеве обладнання. Правильно налаштувавши мережу, адміністратор може забезпечити належний рівень секретності і запобігти витоку даних, що становлять комерційну таємницю [3].

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами: застосовувані засоби забезпечення інформаційної безпеки не відповідають високому рівню розвитку інформаційних технологій; повсюдне використання Інтернет тягне до появи загроз з боку віддалених користувачів; постійне збільшення кількості персональних комп'ютерів, захист яких не відповідає вимогам безпеки; зростання обсягів інформації, що обробляється і зберігається з використанням інформаційних технологій; недосконалість програм і мережевих технологій з точки зору інформаційної безпеки.

Мета концепції захищеної корпоративної мережі – закрити трафік корпоративної мережі засобами захисту інформації мережевого рівня і організувати фільтрацію інформації в точках з'єднання з відкритими мережами [2].

В якості фільтрації інформації на інтерфейсах з відкритими мережами застосовуються традиційні рішення: міжмережний екран (firewall) або сервіси захисту типу proxy. Важливим елементом захисту від несанкціонованого проникнення в корпоративну мережу з відкритою є послідовне (каскадне) включення декількох фільтрів-ешелонів захисту. Як правило, між відкритою і корпоративною мережею встановлюється зона контрольованого доступу.

При побудові безпровідних мереж однією з найбільш гострих проблем є забезпечення їх безпеки. Якщо в звичайних мережах інформація передається по дротах, то радіохвилі, які використовуються для бездротових рішень, досить легко перехопити при наявності відповідного обладнання. Принцип дії бездротової мережі призводить до виникнення великої кількості можливих вразливостей для атак і вторгнень. При використанні безпровідного доступу до локальної мережі загрози безпеки істотно зростають. Весь процес організації захищеної комп'ютерної мережі можна розділити на наступні етапи:

1. Розробка мережі. На цьому етапі фахівці обстежують територію банківського підприємства, вислуховують побажання замовника по функціоналу, складають план, технічне завдання і готують обладнання, необхідне для установки.

2. Монтаж. На цьому етапі прокладаються кабелі, проводиться монтаж обладнання та налаштування необхідного програмного забезпечення.

3. Тестування. Фахівці перевіряють роботу, відповідність встановленої мережі загальноприйнятим стандартам якості.

4. Обслуговування. Цей етап включає модернізацію і при необхідності усунення неполадок.

Створена захищена мережа підприємства повинна задовольняти таким основним вимогам: бути легко керованою; захищеною від хакерських атак (захист корпоративної мережі передбачає установку спеціального програмного забезпечення – міжмережного екрана); бути адаптованої до основних типів мережевих пристроїв і кабелів. Завдяки цьому мережу в будь-який момент можна модернізувати.

У зв'язку з швидким розвитком інформаційних технологій і технічних засобів статичні механізми захисту від мережевих погроз часто виявляються неефективними. Забезпечити ефективний захист інформації дозволяють динамічні методи, здатні оперативно виявляти і усувати загрози. Робота динамічних технологій будується на оцінки рівня підозрілості дій в мережі з боку певної служби або процесу [2].

Алгоритм дії щодо усунення атак спрямований на ідентифікацію підозрілих об'єктів. Після цього система реагує необхідним чином на діяльність таких об'єктів, яка може бути націлена на ресурси мережі або комп'ютерного обладнання.

Для захисту мереж від зовнішніх загроз можуть застосовуватися наступні основні методи і технології: застосування портів високої надійності, шифрування даних; використання ефективних антивірусів і сканерів; застосування програмного або апаратного мережевого екрану; установка блокаторів «руткітів» і «сніфферів».

Управління безпекою для мереж може бути різним для різних ситуацій. Домашній або малий офіс може вимагати тільки базової безпеки, у той час як великим підприємствам може знадобитися обслуговування з високим рівнем надійності і розширене програмне і апаратне забезпечення для запобігання злому і розсилання небажаних атак. Інформаційна безпека в комп'ютерних мережах починається з аутентифікації, пов'язаної з введенням імені користувача і пароля – однофакторна. З двофакторної аутентифікацією додатково використовується і додатковий параметр (токен безпеки або «ключ», мобільний телефон), з трехфакторной застосовується і унікальний користувальницький елемент (відбиток пальця або сканування сітківки). Після аутентифікації брандмауер застосовує політику доступу. Ця служба безпеки комп'ютерної мережі ефективна для запобігання несанкціонованого доступу, але цей компонент може не перевірити потенційно небезпечний контент, такий як комп'ютерні черв'яки або трояни, що передаються по мережі. Антивірусне програмне забезпечення або система запобігання вторгнень (IPS) допомагають виявляти і блокувати дію таких шкідливих програм. Система виявлення вторгнень, заснована на скануванні даних, може також відстежувати мережу для подальшого аналізу на високому рівні. Нові системи, які об'єднують необмежену машинне навчання з повним аналізом мережевого трафіку, можуть виявляти активних мережевих зловмисників вигляді шкідливих інсайдерів або цільових зовнішніх шкідників, які зламали комп'ютер користувача або обліковий запис. Крім того, зв'язок між двома хостами може бути зашифрована для забезпечення більшої конфіденційності [1,3].

У забезпеченні безпеки комп'ютерної мережі застосовуються контрзаходи – дії, пристрої, процедура або техніка, які зменшують загрозу, вразливість або атаку, усуваючи або запобігаючи її, мінімізуючи заподіяну шкоду або виявляючи і повідомляючи про його наявність.

Методи і засоби забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави в цілому. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки. Безпека комп'ютерних мереж забезпечується за рахунок політики та практик, прийнятих для запобігання та моніторингу несанкціонованого доступу, незаконного використання, модифікації або відключення мережі і доступних для неї ресурсів. Вона включає в себе авторизацію доступу до даних, яка контролюється мережевим адміністратором. Користувачі обирають або призначають ідентифікатор і пароль або іншу

аутентифікаційну інформацію, яка дозволяє їм отримувати доступ до даних і програм в межах своїх повноважень.

Політика захисту мережі має описувати технологію і процедури, що використовуються для моніторингу стану захисту системи. За допомогою моніторингу виявляються загрози мережі. Контроль активності в мережі може виявити спроби компрометації системи і допомагає виконати аналіз атак. Моніторинг забезпечує відповідність налагоджень засобів мережного захисту вимогам політики безпеки. Загрози для IT-інфраструктури з кожним роком стають все складніше, для захисту від них потрібно застосовувати різні системи і засоби.

Політика захисту мережі має визначати процедури, що використовуються для аудита, тестування і підтримки захисту мережі. Аудит і тестування можуть допомогти при визначенні загального технічного стану та вразливостей мережних компонентів і всієї системи в цілому. Безперервний контроль, супроводження і модифікація системи захисту забезпечує безпеку мережі.

При проєктуванні мережі та вибору безпровідного обладнання також потрібно враховувати не тільки висоту, периметр кімнат, кількість поверхів будівлі, а й інші перешкоди, так як відстань між будівлями-об'єктами підприємсва, коли між ними вона досить велика.

При обранні способу з'єднання декількох філій, вибір зазвичай лежить між прокладкою оптоволоконного кабелю та бездротовим каналом зв'язку. До переваг першого варіанту можна віднести: постійну гарантовану широку смуга пропускання; низьку затримку; підвищення пропускної здатності за рахунок заміни модулів на кінцях каналу.

Безпровідний канал зв'язку – Wi-Fi використовується, коли прокладка кабелю неможлива або занадто дорога, він дозволяє прискорити процес створення мережі. Окрім цього, на відміну від стільникового зв'язку, Wi-Fi мережі використовують діапазон частот, для якого не потрібно придбання ліцензії, відповідно, витрати на мережу зменшуються ще більше. На ринку представлений широкий вибір обладнання Wi-Fi. Однією з основних проблем, характерних для Wi-Fi, є інтерференція, тобто, перетин зон покриття різних станцій. По причині того, що передача сигналу ведеться на вільній частоті, якість зв'язку може значно погіршитися через завади від радіоприладів та домашніх приладів, наприклад, мікрохвильової печі. Окрім цього, умови прийому та передачі погіршують стіни, залізобетонні покриття, сталеві перегородки та ін. Нарешті, до недоліків WLAN можна віднести обмежений радіус дії, який не перевищує 100 метрів в зоні прямої видимості і 50 метрів при передачі інформації всередині приміщення.

Захист WI-FI мережі – досить важливе й актуальне питання при використанні домашньої точки доступу. Захищати її необхідно у зв'язку з тим, що сьогодні існує досить багато способів злому і підключення до мережі сторонніх. Уберегти і захистити свій роутер можна кількома способами, крім цього важливо періодично проводити спеціальні заходи, щоб зберегти його від несанкціонованої атаки або злому. Тільки тоді можна убезпечити особисте з'єднання.

Є три варіанти захисту.

- WEP (Wired Equivalent Privacy) – застарілий і небезпечний метод перевірки автентичності. Це перший і не дуже вдалий метод захисту. Зловмисники без проблем отримують доступ до бездротових мереж, які захищені за допомогою WEP. Не потрібно встановлювати цей режим в налаштуваннях свого роутера, хоч він там і присутній (не завжди).
- WPA (Wi-Fi Protected Access) – надійний і сучасний тип безпеки. Максимальна сумісність з усіма пристроями і операційними системами.
- WPA2 – нова, допрацьована і більш надійна версія WPA. Є підтримка шифрування AES CCMP. На даний момент, це кращий спосіб захисту Wi-Fi мережі. Саме його рекомендують використовувати.
- WPA / WPA2 може бути двох видів:
- WPA/WPA2-Personal (PSK) – це звичайний спосіб аутентифікації. Коли потрібно задати тільки пароль (ключ) і потім використовувати його для підключення до Wi-

Fi мережі. Використовується один пароль для всіх пристроїв. Сам пароль зберігається на пристроях. Де його при необхідності можна подивитися, чи змінити. Рекомендується використовувати саме цей варіант.

- WPA/WPA2-Enterprise − більш складний метод, який використовується в основному для захисту бездротових мереж в офісах і різних закладах. Дозволяє забезпечити більш високий рівень захисту. Використовується тільки в тому випадку, коли для авторизації пристроїв встановлений RADIUS-сервер (який видає паролі).

В топології КМ (комп'ютерної мережі) комутатори використовуються як пристрої для сегментації. Як і мости, вони відносяться до другого рівня моделі OSI. Відрізняються тим, що комутація трафіку значно швидша через те, що вона проходить на апаратному рівні завдяки ASICs (Application Specific Integrated Circuits). Комутатори також мають значно більшу кількість портів. Вони запам'ятовують, який вузол під'єднаний до порту, через IP-адресу вузла. Не можна плутати це мережеве обладнання з комутаторами 3-го рівня. Комутатори 3-го рівня потужніші, переймають усі функції звичайних комутаторів і здатні маршрутизувати трафік. Зазвичай вони використовуються на рівні розподілу та рівні ядра ієрархічної моделі мережі.

Ієрархічна модель КМ представляє собою фундамент для мережевої інфраструктури: підключення користувачів, принтерів, сканерів, WAN маршрутизаторів, мережних екранів, серверів і т.д. Ієрархічна модель ділить мережу на три основні рівні:

1. Рівень доступу (Access Layer) – надає користувачам або пристроям доступ до мережі;
2. Рівень розподілу (Distribution Layer) – поєднує комутатори рівня доступу і надає доступ до різних сервіс організації. Поєднання зазвичай відбуватися по агрегованим каналам;
3. Рівень ядра (Core Layer) – поєднує мережеве обладнання рівня розподілу в великим мережах.

Залежно від ситуації можуть використовуватися один, два або три рівні. Наприклад, для офісу з кількістю користувачів менше десяти можна обмежитися рівнем доступу. Для великої організації, що займає декілька поверхів або цілу будівлю, буде краще побудувати мережу на перших двох рівнях. Для ще більших організацій потрібно використовувати всі три рівня. На Рис. 1 зображена типова 3-рівнева ієрархічна модель мережі, де комутатори рівня доступу підключені до комутаторів рівня розподілу агрегованими каналами, а останні підключені до рівня ядра оптоволоконними з'єднаннями. На другому рівні також використовується технологія стеку.

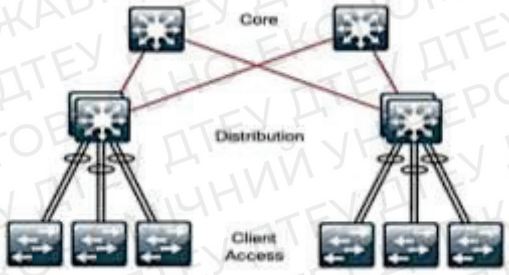


Рис. 1. Ієрархічна модель мережі

Рівень доступу є вхідною точкою для користувачів та мережевих пристроїв. Наприклад: ПК користувача під'єднаний до комутатора рівня доступу крученою парою; мобільний телефон під'єднаний до точки доступу Wi-Fi. Мережеве обладнання не обов'язково повинно мати функції маршрутизації. Воно відповідає за первинну сегментацію мережі. Наприклад, це комутатори рівня доступу. Рівень доступу повинен забезпечити безпеку користувачів та пристроїв мережі від підключених зловмисників або заражених робочих станцій. Засоби захисту:

- DHCP-snooping;
- IP Source guard;

- Port security;
- Dynamic ARP inspection.

Головною задачею рівня розподілу є об'єднання комутаторів рівня доступу в єдину мережу. Це суттєво зменшує кількість лінків. Як правило, саме комутатори рівня розподілу підключають до мережі найнеобхідніші сервіси та модулі. Рівень розподілу є найважливішою частиною всієї мережевої інфраструктури і вимагає високу продуктивність, відмовостійкість. Мережеве обладнання рівня розподілу – це, як правило, комутатори 3-го рівня моделі OSI. Вони здійснюють маршрутизацію трафіку між сегментами мережі (між різними VLAN).

Система безпеки не є однією з головних задач на цьому рівні. Комутатори рівня доступу підключаються до рівня розподілу по агрегованим каналам (Ether Channel), одночасно забезпечуючи відмовостійкість та високу продуктивність. Агрегований канал є поєднанням 2, 3-х або більше фізичних лінків в один логічний. При цьому всі з'єднання передають інформацію, що суттєво збільшує пропускну здатність каналу. У разі відмови одного з лінків, що входить до агрегованого каналу, інформація продовжить передаватися по працездатним лінкам без жодної затримки в роботі мережі. Це головна різниця від традиційної надлишкової моделі, де блокуються додаткові з'єднання (протоколи STP, RSTP) для уникнення петель. При використанні традиційної моделі продуктивність не зростає, лише досягається відмовостійкість. Один логічний лінк замість багатьох фізичних також дозволяє полегшити адміністрування мережею. Комутатори рівня розподілу об'єднуються в стек за допомогою такої технології, як, наприклад, StackWise Plus. Агрегований канал утворюється при об'єднанні портів різних комутаторів стека (Рис. 2).

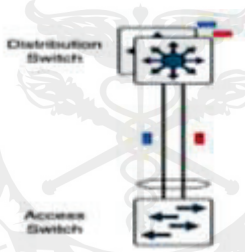


Рис. 2. Схема агрегованого каналу між комутатором доступу та стеком комутаторів розподілу

Іншими словами, логічний інтерфейс утворюється внаслідок об'єднання двох (або більше) портів, при цьому один порт належить першому комутатору стека, а другий – другому комутатору. Обидва порти приймають участь в передачі даних. Таким чином задіяні всі пристрої, забезпечуючи високу продуктивність і відмовостійкість.

Дизайн великих корпоративних мереж підприємства, що охоплюють дві або більше будівлі, зобов'язує використання рівня ядра. Головним завданням рівня ядра є об'єднання всіх комутаторів рівня розподілу в єдину мережу та маршрутизація трафіку. Засобів захисту на цьому рівні не так багато, так як безпека має менший пріоритет, ніж інші функції.

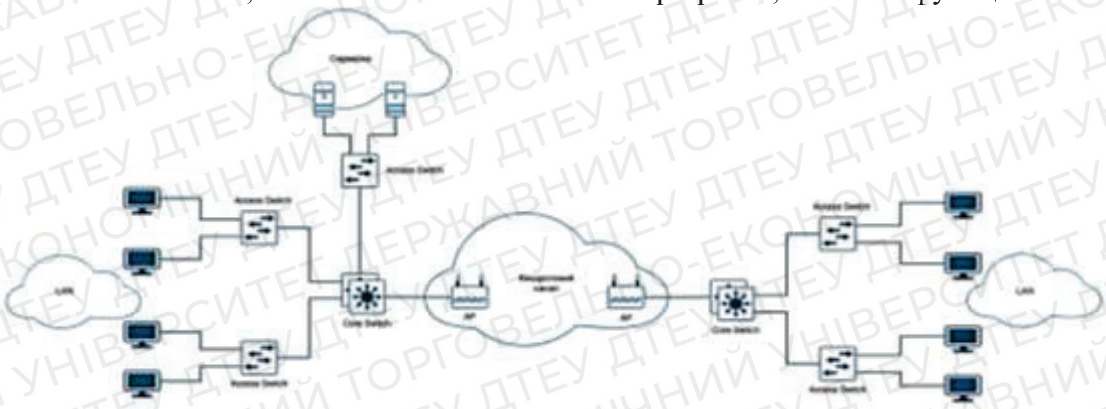


Рис. 3. Структурна схема комп'ютерної мережі в будівлях підприємства

Зрозуміло, що без рівня розподілу в КМ підприємства не обійтися, так як трафік між різними сегментами мережі повинен маршрутизуватися. Комутатори рівня ядра розраховані на велику завантаженість мережі і здатні передавати дані зі швидкістю 40 Гбіт/с. Немає ніякого сенсу придбавати таке обладнання, коли швидкість бездротового каналу між будівлями лише 24 Мбіт/с. По цій причині рекомендується об'єднати рівень розподілу з рівнем ядра (Рис. 3). Це доволі часта практика, і, хоча рівень ядра не буде мати окремого мережевого обладнання, всі його важливі функції будуть будуть виконуватися на рівні розподілу (Рис. 4). Рівень розподілу, до речі, матиме назву Collapsed Core. Проєкт мережі, зображений на Рис. 3 та Рис. 4, підходить підприємству, в якому більша кількість трафіку проходить всередині локальних мереж, а канал зв'язку між ними використовується не так часто. Тепер щодо кількості L2 комутаторів (комутаторів другого рівня моделі OSI, що використовуються на рівні доступу).

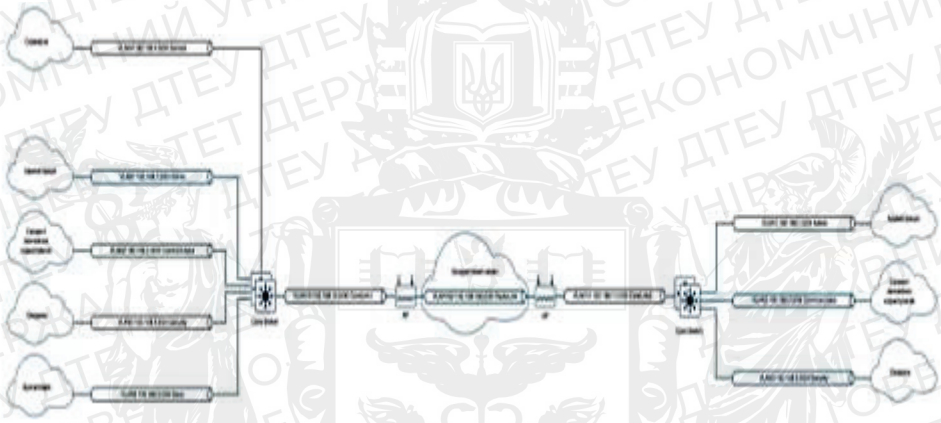


Рис. 4. L3 схема комп'ютерної мережі в будівлях підприємства

Висновки. Задача створення ефективних комплексних систем захисту комп'ютерних мереж може бути вирішена з використанням сукупності методів та технологій, які реалізовані в сучасному телекомунікаційному обладнанні для комп'ютерних мереж, як основи технічної складової таких систем. При виборі та реалізації технологій захисту для конкретної мережі необхідно враховувати особливості структури мережі, спеціалізації роботи підприємства, вірогідність проведення конкретних атак. Налаштування відповідного функціоналу на мережевому обладнанні дозволяє здійснювати контроль відповідності політиці мережевої безпеки та реалізовувати захист максимально близько до можливого джерела порушень, що, у свою чергу, мінімізує можливі негативні наслідки для корпоративної мережі моделі OSI.

Список використаних джерел

24. Yanko A. Система захисту комп'ютерної мережі / A. Yanko, R. Vyhivskyi // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2022. – Т. 2 (68). – С. 91-94. – doi: https://doi.org/10.26906/SUNZ.2022.2.091 (останнє звернення 09.03.2023р.).
25. Кучернюк В. П. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). Мікросистеми, електроніка та акустика. 2017. № 6. Том 22. С. 64-70. URL: http://elc.kpi.ua/article/view/113191 (останнє звернення 09.03.2023р.)
26. Cisco Network Admission Control (NAC) Solution Data Sheet // Cisco. January 23, 2017. \\ Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean (останнє звернення: 09.03.2023р).

Робота виконана під науковим керівництвом к.т.н., доцента
ЗВЄРЄВА В.П.

ВИМОГИ ДО СИСТЕМИ БЕЗПЕКИ ПІДПРИЄМСТВА ТА ОСНОВНІ ПРИНЦИПИ ЇЇ ПОБУДОВИ

КРАВЧУК Ю., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто вимоги функціонального призначення систем контролю та управління доступ (СКУД), функціональний склад і загальні вимоги СКУД, інтеграція та побудова мережі СКУД, охоронна сигналізація, пожежна сигналізація, система управління контроль доступу, функція СКУД, система контролю доступу, система відеоспостереження.

The article discusses the requirements for the functional purpose of access control and control systems (ACC), the functional composition and general requirements of ACC, integration and construction of the ECU network, security alarm, fire alarm, access control management system, ACS function, access control system, video surveillance system.

Актуальність. Системи контролю та управління доступом (СКУД) є необхідним атрибутом будь-якої організації. Існує необхідність обмежити доступ до важливих процесів та захистити ресурси і активи в різних місцях виробництва, включаючи цехи, конвеєри, склади та лабораторії. В сучасному виробництві часто трапляються такі прикрі випадки, як крадіжки, вандалізм власності підприємства, пошкодження майна і навіть напади на співробітників [1]. На теперішній час тенденція розробників зводиться до створення багатофункціональних централізованих систем контролю та управління доступом із використанням радіочастотних технологій (RF) та технологій безконтактних смарт-карт.

Сучасна централізована СКУД може принести користь підприємствам, які не мають контролю доступу або використовують автономні системи на критичних об'єктах. Автономні системи дещо обмежені за своєю природою, і однією з їхніх слабких сторін є нездатність ефективно відстежувати людей, які входять у приміщення, що ускладнює розслідування інцидентів. Різноманітні технології, такі як штрих-коди, QR-коди, Bluetooth, біометрія, RFID, безконтактні смарт-картки та NFC спочатку вивчалися шляхом консультацій з відповідними академічними журналами, статтями та технічними статтями в Інтернеті. Дослідження показують, що найкращі техніки для реалізації є безконтактна смарт-карта.

Основна мета цієї роботи полягає в тому, щоб підкреслити проектування та розробку централізованої системи контролю доступу для загального підприємства, яка також здатна ефективно використовувати зібрані дані для інших корисних завдань, таких як автоматичний хронометраж, планування робочих місць і керування в режимі реального часу.

Об'єкт дослідження – дослідження вимоги щодо функціонального призначення систем контролю та управління доступом (СКУД), функціональний склад СКУД і загальні вимоги до неї, інтеграційна та мережева побудова СКУД, системи охоронної сигналізації, системи пожежної сигналізації, системи контролю і управління доступом, можливості СКУД, систем контролю управління доступом, системи відеоспостереження.

Предмет дослідження – системи контролю та управління доступом.

Виклад основного матеріалу.

Основним завданням СКУД є управління доступом на задану територію, включаючи також обмеження доступу на задану територію, ідентифікація особи, яка має доступ на задану територію, а також облік робочого часу; розрахунок заробітної плати (при інтеграції з системами бухгалтерського обліку); ведення бази персоналу/відвідувачів; інтеграція зі всіма системами безпеки.

Користувацькі права для доступу та ідентифікації можуть бути реалізовані різними методами і засобами, наприклад, використанням паролів, особистих PIN-кодів, радіочастотних технологій, біометрії. Для підтвердження своїх прав особа може пред'явити ті, чи інші ідентифікатори, такі як електронні картки, радіочастотні ідентифікатори, особисті біометричні дані для зчитування системою.

Ключові технології СКУД. З тих пір, як вперше з'явилася концепція електронної системи контролю доступу, вона була протестована та впроваджена з використанням різних технологій. Різні підходи мають свої власні переваги та недоліки.

Далі розглядаються основні технології, які можуть бути використані при проектуванні СКУД.

Штрих-коди та коди швидкого реагування (QR). Обидві технології вимагають прямої видимості, що може спричинити деякі затримки, особливо коли користувачеві важко розташувати коди належним чином для сканування. Хоча вони є недорогим рішенням контролю доступу, вони є технологіями з низьким рівнем безпеки, оскільки коди можна дублювати дуже легко.

Біометрія. Біометрія забезпечує найвищу форму захисту, оскільки усуває певні пристрої облікових даних, забезпечуючи таким чином контроль доступу, який неможливо передавати на відміну від ключів або карток. Однак, завдяки високому рівню безпеки, він також має високі витрати на впровадження. Розгортання біометричних даних для безпеки підприємства на об‘єктах з великою кількістю користувачів та великим трафіком може бути нерозумним, оскільки його характер автентифікації може спричинити збої доступу у точках входу.

Bluetooth. На ринку вже є декілька комерційних продуктів, зокрема Kevo Smart Lock та EC Key, які перетворюють пристрої з підтримкою Bluetooth на ключ. Головною проблемою цього підходу є споживання батареї пристрою (смартфона) користувача. Для того, щоб користувачі могли швидко та зручно подорожувати через точки входу, їх Bluetooth рекомендується вмикати та постійно залишати у видимому режимі. Це розряджає заряд акумулятора мобільних пристроїв, і в разі несправності мобільних пристроїв або розрядження пристроїв слід розглянути плани резервного копіювання.

Радіочастотна ідентифікація (RFID). Все більш поширена технологія з 1970-х років, оскільки ця технологія стає більш доступною. Однією з її головних переваг є той факт, що вона не вимагає прямої видимості і може мати велику дальність читання, що робить її одним з найкращих кандидатів для ідентифікації та відстеження об'єкта. Однак використання пристроїв RFID, які працюють на високій частоті, отже, мають високий діапазон зчитування, не може обмежувати пропускну здатність системи. Тож в ідеалі пристрої, що працюють на низькій частоті (НЧ), були б кращим вибором для систем контролю доступу.

Системи ближнього поля (NFC). Нова технологія, яка дозволила використовувати смартфони як облікові дані користувача. Перевагою такої технології є можливість використання єдиного (комунікаційного) пристрою доступу. Але відсутність стандартизації серед операторів стільникових телефонів, виробників телефонів та виробників безпеки є найбільшою перешкодою на шляху адаптації технології [3].

Безконтактна смарт-карта. Безконтактна смарт-карта використовує радіочастоту між картою та зчитувачем, що не вимагає фізичного вставлення картки, оскільки зчитування здійснюється шляхом її проходження вздовж зовнішньої частини зчитувача. Ці картки відповідають стандарту ISO-14443, із варіаціями типів A, B та C. Оснащені пам'яттю та можливістю шифрування роблять ці карти ідеальним варіантом для програм, які вимагають певного рівня безпеки. Смарт-карта Сантандера є прикладом використання безконтактних смарт-карт для безпечного застосування в навчальних закладах у великих масштабах [2].

Готові комплекти систем контролю доступу – це комплекти складаються з контролера, зчитувача, замку (магнітного або електромеханічного), кнопки виходу, додаткового обладнання (куточок для магнітного замку), кабелю, ключів стандарту Proximity Key (EM-Marine), блоку живлення 12 Вольт та іншого обладнання для самостійного монтажу.

Комплекти СКУД обмежують доступ у приміщення на підприємстві, в офісах і виробництвах, кафе і ресторанах. Системи обмеження доступу зустрічаються практично скрізь і вирішують головні завдання по обмеженню доступу в приміщення. Системи управління контролем доступу дозволяють не тільки обмежувати доступ, але й фіксувати всі події (час приходу і відходу, відпрацьований час тощо), які зберігаються в пам'яті контролера або ж в комп'ютері. Згідно з отриманими звітів на багатьох підприємствах відбувається нарахування заробітної плати.

Перспективна структура централізованої СКУД.

На сьогоднішній день існує дуже багато різновидів СКУД різних виробників, а також її компонентів. Незважаючи на унікальність кожної конкретної системи контролю доступу, вона повинна містити наступні основні елементи (рис. 1).

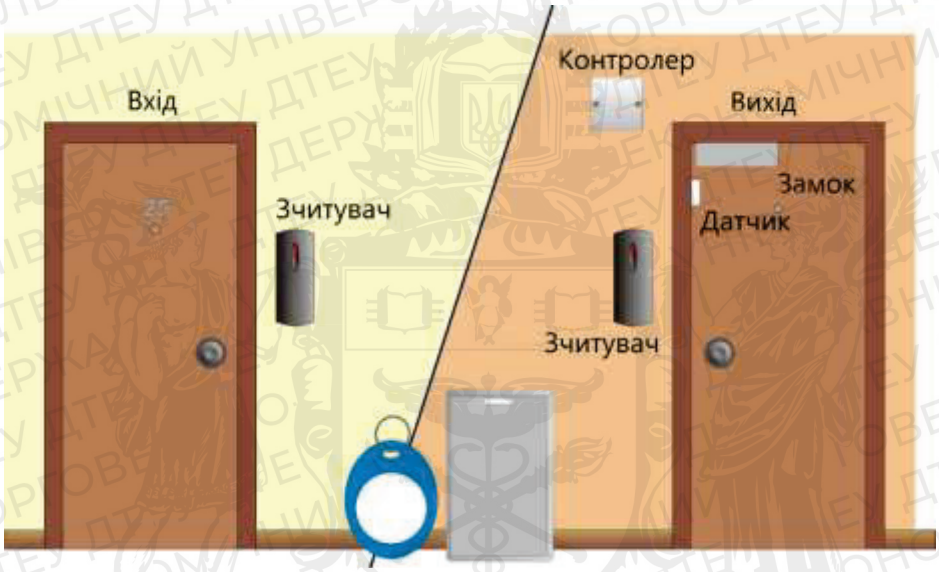


Рис. 1. Схема системи СКУД

Точка контролю. Точка входу, де необхідний бар'єр. Поширені приклади фізичного контролю доступу до точок доступу включають ворота, турнікети та дверні замки. Захищений простір може мати одну точку доступу, наприклад, офіс всередині великого комплексу, або багато точок доступу.

Панель керування. Панель керування СКУД отримує облікові дані від пристрою зчитування та перевіряє, чи є такі дані дійсними. Якщо облікові дані підтверджуються, панель управління передає дані авторизації до точки доступу через сервер контролю доступу, і двері відчиняться. Якщо дані не підтверджені, користувач не зможе отримати доступ.

Зчитувачі розташовуються у точці доступу і надсилають дані з облікових даних на панель керування для автентифікації облікових даних та запит на авторизацію доступу. Якщо використовується клавіатура або біометричний термінал (наприклад, сканування відбитків пальців, ідентифікатор обличчя або сканування сітківки ока), користувачі вводять свій PIN-код або виконують сканування для отримання доступу.

Особисті облікові дані. Більшість СКУД вимагають, щоб користувач мав ідентифікаційні облікові дані, щоб ввести об'єкт або отримати доступ до даних. Прикладами фізичного контролю доступу є облікові дані, зокрема (карти, ключі, токени) та системи введення карток, зашифровані носії, мобільні пристрої, PIN-коди та паролі. Особисті дані відповідають користувачу, який намагається отримати доступ.

Сервер контролю доступу. Сервер контролю доступу зберігає дані користувача, привілеї доступу та журнали аудиту. Залежно від вашої системи, сервер може бути локальним або керованим у хмарі. Необхідно регулярно проводити технічне обслуговування системи та

оновлення програмного забезпечення, щоб захистити систему від злому та можливих порушень безпеки.

Допоміжне обладнання. Це блоки безперебійного живлення, датчики, кнопки, проводка тощо.

Програмне забезпечення – здійснює налаштування та управління обладнанням, моніторинг його параметрів, систематизацію та архівування всієї інформації системи. Воно також здійснює підтримку обміну даними між контролерами і комп'ютером моніторингу, управління доступом і моніторинг пунктів проходу, роботу з базами даних і реєстрацію власників ідентифікаторів, дозволяють здійснювати візуальну ідентифікацію власників «електронних перепусток» на прохідній і для формування різних звітів, а також виконувати додатковий набір функцій.

СКУД повинна забезпечувати виконання таких основних функцій [4]:

- відкривання перерегороджуючих пристроїв контролю (ППК) при зчитуванні ідентифікаційної картки, доступ за яким дозволено в дану зону доступу (приміщення) в заданий часовий інтервал або по команді оператора СКУД;
- заборона відкривання ППК при зчитуванні ідентифікаційної картки, доступ за яким не дозволено у дану зону доступу (приміщення) в заданий часовий інтервал;
- санкціонована зміна (додавання, видалення) ідентифікаційних карток в пристроях керування (ПК) і зв'язок їх з зонами доступу (приміщеннями) і часовими інтервалами доступу;
- захист від несанкціонованого доступу до програмних засобів ПК для зміни (додавання, видалення) ідентифікаційних карток;
- захист технічних і програмних засобів від несанкціонованого доступу до елементів управління, установки режимів і до інформації;
- збереження налаштувань і бази даних ідентифікаційних карток при відключенні електроживлення;
- ручне, напівавтоматичне або автоматичне відкривання ППК для проходу при аварійних ситуаціях, пожежі, технічні несправності відповідно до правил установлених режимом і правилами протипожежної безпеки;
- автоматичне закриття ППК за відсутності факту проходу через певний час після зчитування дозволеної ідентифікаційної картки;
- видачу сигналу тривоги (або блокування ППК на певний час) при спробах підбору ідентифікаційних карток (коду);
- реєстрацію і протоколювання поточних і тривожних подій;
- автономну роботу зчитувача з ППК в кожній точці доступу при відмові зв'язку з ПК.

На об'єктах підприємства, де необхідний контроль збереження предметів, слід встановлювати СКУД, контролюючих несанкціонований винос даних предметів з ОІД по спеціальних ідентифікаційних мітках.

Вимоги до перспективної системи контролю та управління доступом.

Коли справа доходить до вибору системи контролю доступу, слід враховувати багато факторів. Це може варіюватися від того, як система впроваджена, а також від того, як користувачі виглядають для управління та доступу до своєї системи контролю доступу.

Хмарні сервіси.

Впровадження та управління системою доступу до організації починається з вибору між локальною системою контролю доступу та хмарним рішенням. Різниця між двома факторами полягає в тому, як ваша організація буде керувати, масштабувати та керувати своїм повсякденним доступом до будівель.

Інтеграція систем доступу.

Хоча побудова систем контролю доступу відіграє ключову роль у забезпеченні фізичних просторів, більшість систем традиційно вирішують лише половину проблем. На

додаток до знання ситуації за дверима, система може бути більш корисною в інтеграції з іншими системами фізичного захисту, такими як відеоспостереження. Однак різниця між технічними рішеннями щодо відеоспостереження та контролю доступу може призвести до несумісності різних систем.

Формати карток користувачів.

Окрім технічної оцінки систем контролю доступу, організації також повинні враховувати типи облікових даних та методи побудови доступу, які вони будуть використовувати у своїх фізичних просторах. Починаючи з форматів зчитувачів карток, таких як Wiegand та OSDP, розширюючи широкий спектр форматів карток на вибір, захист вашої організації часто починається з тих самих облікових даних, якими володіють користувачі.

Масштабованість.

На початковому етапі досить важко визначити основні параметри системи і тому бажано, щоб система була масштабованою. На додаток до того, як знати, скільки дверей та зареєстрованих користувачів вам знадобиться для побудови доступу, необхідно також врахувати, як системи будуть взаємодіяти між собою під час управління декількома системами контролю доступу або місцями.

Ціна.

Є багато. факторів, які відіграють значну роль у визначенні ціни на систему контролю доступу до організації. Основні витрати, такі як обладнання та програмне забезпечення контролера, можуть складати більшу частину витрат організації, однак існують різні інші витрати, пов’язані з такими речами, як зчитування карток ключів, обслуговування системи та встановлення системи контролю доступу.

Безпека.

На додаток до фізичної безпеки, яку забезпечує контроль доступу, важливо також оцінити додаткові міркування щодо безпеки. Це може варіюватися від того, як ваші контролери доступу до дверей підключаються до системи, а також від вибору правильної форми RFID / безконтактних карток, щоб найкраще захистити вашу організацію.

Зчитувачі пристроїв введення ідентифікаційних об’єктів (ПВІО) повинні забезпечувати [4]:

- зчитування ідентифікаційної картки; порівняння введеної ідентифікаційної інформації зі збереженням в пам'яті або базі даних ПК;
- формування сигналу на відкривання ППК при ідентифікації користувача;
- обмін інформацією з ПК. ПВІО повинні бути захищені від маніпулювання шляхом перебору або підбору ідентифікаційних даних.

Ідентифікатори ПВІО повинні забезпечити зберігання ідентифікаційних даних протягом усього терміну експлуатації для ідентифікаторів без вбудованих елементів електроживлення та не менше 3 років – для ідентифікаторів з вбудованими елементами електроживлення.

Конструкція, зовнішній вигляд і написи на ідентифікаторі і зчитувачі не повинні призводити до розкриття застосовуваних кодів.

Перегороджуючі пристрої контролю з виконавчими пристроями повинні забезпечувати [2]:

- часткове або повне перекриття отвору проходу;
- автоматичне і ручне (в аварійних ситуаціях) відкривання;
- блокування людини всередині ППК (для шлюзів, прохідних кабін);
- необхідну пропускну спроможність.

Пристрої керування мають забезпечувати:

- прийом інформації від ПВІО, її обробку, відображення в заданому вигляді і вироблення сигналів управління ППК;
- ведення баз даних співробітників і відвідувачів ОІД з можливістю завдання характеристик їх доступу (коду, часового інтервалу доступу, рівня доступу та інші);

- ведення електронного журналу реєстрації проходів співробітників і відвідувачів через точки доступу;
- пріоритетний висновок інформації про тривожних ситуаціях в точках доступу.

Установка СКУД на підприємстві вирішує три першочергові проблеми:

- обмеження доступу сторонніх осіб на об'єкт, приміщення, що захищається;
- контроль за пересуванням працівників;
- облік робочого часу.

Обмеження доступу сторонніх осіб – одне з найважливіших завдань. Воно реалізується за рахунок установки блокуючих, керованих пристроїв (електричні замки, турнікети) на входах і виходах приміщень і територій, що захищаються.

Контроль за пересуванням співробітників є не менш важливою функцією, що дозволяє визначити, куди і коли заходив працівник. Ця інформація є корисною як у разі розгляду нештатних ситуацій (наприклад, крадіжка), так і для організації правильної роботи підприємства. Для реалізації цього необхідно, щоб у кожного співробітника був свій унікальний ідентифікатор (карта, електронний ключ, відбиток пальця тощо).

Облік робочого часу, дозволяє керівництву фірми бути в курсі того, скільки годин відпрацював співробітник і наскільки добре дотримувався робочої дисципліни. На деяких підприємствах, за даними автоматизованої системи обліку робочого часу, проводиться розрахунок заробітної плати працівника, згідно з фактично відпрацьованим часом.

Система СКУД, поєднана з охоронною сигналізацією, дає надійний захист будь-якого підприємства. Така система охорони реагуватиме на наступні фактори: несанкціонований доступ на територію підприємства, що охороняється, злам дверей, розбиття вікон та інші подібні дії [5].

В Україні на сьогодні існує близько 35 компаній, які виробляють як технічні засоби, так і програмне забезпечення і надають послуги для формування СКУД під конкретні потреби підприємства. Серед них — CYPHRAX, U-Pro, Orion, SmartSecurity, Tescom, Elko, ВТП Трансекспо Бренд-Енерго Тов., ООО Енерго Інжиніринг, ООО «Ексимтек ПЛЮС», Vel-Trade та ін.

Висновки. Таким чином, з проведеного аналізу можна зробити висновок, що системи контролю та управління доступом є невід'ємною частиною інтегрованої системи підприємства та одним з найважливіших компонентів забезпечення інформаційної та фізичної безпеки на об'єктах інформаційної діяльності.

Список використаних джерел

1. Ворона В.А., Тихонов В.А. Системи контролю та управління доступом. – К.: Телеком, 2010. – 272 с.

2. Системи контролю доступу. – URL: http://studopedia.com.ua/1_30311_sistema-kontrolyu-dostupu.html

3. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / ДержНДІ Спецзв'язку, 2015. – С. 58-60.

4. Дурденко В.А. Розробка класифікації та архітектури побудови інтегрованих систем безпеки / Дурденко В.А. Рогожин А.А. – К.: Інформаційно-обчислювальні керуючі та мережеві системи, 2012. – 336 с.

5. Юдін О.К. Інформаційна безпека держави / О.К. Юдін. — К. : Консум. — 2005. — 576 с.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т.В.

ВИКОРИСТАННЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ЗАХИСТУ ВЕБ-ЗАСТОСУНКІВ

КРАСНОПОЛЬСЬКИЙ О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто використання двофакторної автентифікації як засобу захисту веб-застосунків. Описано процес встановлення та налаштування двофакторної автентифікації для веб-застосунків. Зазначено переваги та недоліки використання двофакторної автентифікації, а також те, які фактори впливають на вибір конкретного методу двофакторної автентифікації. Наведено приклади реалізації двофакторної автентифікації для веб-застосунків та діляться порадами щодо того, як можна покращити безпеку веб-застосунків за допомогою двофакторної автентифікації.

The article discusses the use of two-factor authentication as a means of protecting web applications. The process of installing and configuring two-factor authentication for web applications is described. The advantages and disadvantages of using two-factor authentication are mentioned, as well as the factors that influence the choice of a specific method of two-factor authentication. Examples of implementing two-factor authentication for web applications are provided, and advice is given on how to improve the security of web applications using two-factor authentication.

Актуальність. Актуальність використання двофакторної автентифікації для захисту веб-застосунків полягає в тому, що з кожним роком зловмисники стають все більш винахідливими у способах вторгнення до систем та викрадення даних. Найбільш поширеним методом злому є перехоплення паролів, які користувачі використовують для входу до своїх акаунтів. Також існують атаки, які спираються на соціальну інженерію та інші методи викрадення інформації.

Одним із найефективніших способів захисту є двофакторна автентифікація (2FA), процес безпеки, який вимагає від користувачів надання двох форм ідентифікації для доступу до онлайн-облікового запису або платформи. Як правило, це включає пароль або PIN-код, а також вторинну форму автентифікації, таку як відбиток пальця або код безпеки, надісланий на мобільний пристрій. 2FA необхідна, оскільки вона додає додатковий рівень безпеки обліковим записам користувачів, ускладнюючи їх зламати. За допомогою традиційної автентифікації лише за паролем хакер, який вгадає або викрадає пароль користувача, може отримати доступ до його облікового запису та потенційно викрасти конфіденційну інформацію або здійснити зловмисні дії. Однак за допомогою 2FA, навіть якщо хакер має пароль користувача, йому все одно потрібен другий фактор (наприклад, телефон або токен користувача), щоб отримати доступ. Це значно ускладнює хакерам отримати несанкціонований доступ до облікових записів користувачів.

Використання двофакторної автентифікації дозволяє підвищити безпеку веб-застосунків, оскільки для входу до акаунту користувач повинен підтвердити свою ідентичність за допомогою двох факторів. Це ускладнює завдання зловмисників, які намагаються вторгнутися до системи та зламати акаунт. Крім того, використання двофакторної автентифікації є одним з вимог для деяких законодавчих актів та стандартів щодо захисту конфіденційної інформації, наприклад, PCI DSS, HIPAA, GDPR.

Отже, використання двофакторної автентифікації є актуальним для підвищення безпеки веб-застосунків і захисту конфіденційної інформації.

Метою статті є дослідження важливості використання двофакторної автентифікації для захисту веб-застосунків та допомога користувачам у виборі оптимального методу захисту своїх даних від несанкціонованого доступу.

Об'єктом дослідження є використання двофакторної автентифікації для захисту веб-застосунків від несанкціонованого доступу та розгляд методів її впровадження в різних типах веб-застосунків.

Предмет дослідження —веб-застосунків, які можуть використовувати двофакторну автентифікацію для забезпечення більш високого рівня захисту.

Аналіз попередніх досліджень. Попередні дослідження підтверджують, що методи двофакторної автентифікації є більш надійним та безпечним порівняно з однофакторною автентифікацією. Використання двох незалежних механізмів автентифікації ускладнює процес злому пароля, а також дозволяє користувачеві перевірити свій акаунт у випадку викрадення або втрати своїх доступів. Дослідження науковців доводять те, що успішність методу двофакторної автентифікації залежить від реалізації та налагодження системи. Недостатня захист може призвести до порушення безпеки, тоді як надмірний захист може призвести до складнощів для користувачів та зниження продуктивності. Дослідженню двофакторної автентифікації присвячені праці наступних науковців: T.Petsas(Т. Петсас), G.Tsirantonakis(Г. Цірантонакіс), E.Athanasopoulos (Е. Атанасопулос), Claudia Ziegler Acemyan (Клаудія Зіглер Асемян), Philip Kortum (Філіп Кортум), Jeffrey Xiong (Джеффрі Сюн) та інші.

Виклад основного матеріалу. Захист веб-застосунків є критично важливим, оскільки ці застосунки можуть містити конфіденційну інформацію, таку як особисті дані користувачів, банківські дані та інші конфіденційні дані. Зламані веб-застосунки можуть призвести до викрадення цієї інформації, що може призвести до серйозних наслідків, таких як крадіжка грошей або ідентичності. Для захисту веб-застосунків можна використовувати різні методи, такі як шифрування даних, використання паролів складної структури, контроль доступу та двофакторну автентифікацію. Кожен з цих методів може забезпечити додатковий рівень захисту веб-застосунків та допомогти у запобіганні злому. Захист веб-застосунків також може бути забезпечений за допомогою використання безпечних протоколів, таких як HTTPS. HTTPS забезпечує шифрування даних між веб-сайтом та користувачем, що допомагає у запобіганні злому та доступу до конфіденційної інформації. Незважаючи на застосування різних методів захисту веб-застосунків, важливо знати, що ці методи не є 100% ефективними та можуть мати певні вразливості. Тому важливо постійно підтримувати та оновлювати системи захисту, щоб убезпечити веб-застосунки від потенційних загроз [1].

Захист веб-застосунків є дуже важливим аспектом в сучасній інформаційній безпеці. Зловмисники можуть використовувати різні техніки для отримання несанкціонованого доступу до веб-застосунків, таких як використання вразливостей у програмному забезпеченні, фішингові атаки, підбір паролів та багато іншого. Для захисту веб-застосунків використовують різні методи, включаючи криптографічні методи, контроль доступу, моніторинг та аудит безпеки. Одним з найпоширеніших методів захисту веб-застосунків є автентифікація користувачів. Цей метод дозволяє підвищити рівень безпеки, оскільки зловмиснику не вистачить лише знання пароля, щоб отримати доступ до веб-застосунку. Окрім автентифікації, веб-застосунки можуть бути захищені за допомогою різних інших методів, таких як шифрування даних, моніторинг активності користувачів та застосування правил контролю доступу. Усі ці методи повинні бути використані разом для забезпечення максимальної безпеки веб-застосунків.

Використання двофакторної автентифікації є важливим для забезпечення високого рівня безпеки веб-застосунків. У порівнянні зі звичайною автентифікацією, яка базується лише на знанні логіну та пароля, двофакторна автентифікація вимагає від користувачів підтвердження своєї ідентичності через два різних механізми, що зменшує ризик несанкціонованого доступу до даних [2].

У випадку, якщо зловмисник зламає логін та пароль користувача, він все ще не зможе отримати доступ до системи, якщо двофакторна автентифікація буде використана. Наприклад, у разі використання автентифікації на основі SMS-повідомлень, користувач буде мати доступ до введення додаткового коду, який буде відправлено на його телефон, що зменшить ризик несанкціонованого доступу.

Таким чином, використання двофакторної автентифікації є важливим інструментом для захисту веб-застосунків від кібератак і забезпечення безпеки користувачів. На (Рис. 1) зображено принцип роботи двофакторної автентифікації.

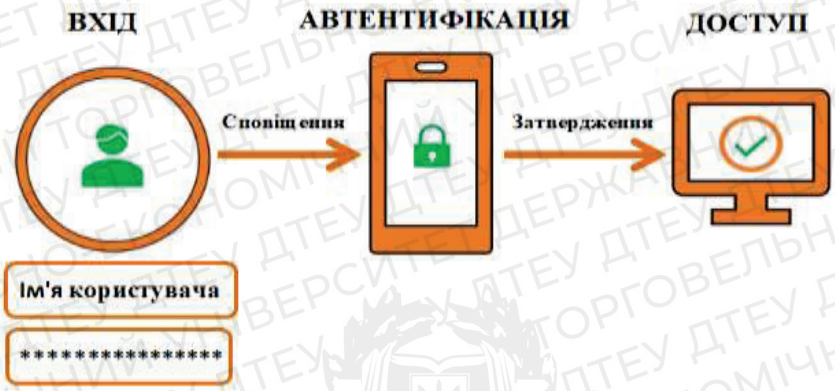


Рис. 1. Принцип роботи двофакторної автентифікації

Двофакторна автентифікація - це процес перевірки ідентичності користувача з використанням двох різних методів аутентифікації. Це забезпечує додатковий рівень безпеки для входу в обліковий запис та захисту від несанкціонованого доступу до веб-застосунків. Зазвичай двофакторна автентифікація використовує комбінацію чогось, що користувач знає (наприклад, пароль або пін-код) та чогось, що користувач має (наприклад, фізичний пристрій, такий як мобільний телефон, на якому встановлено додаток або отримує SMS з кодом). Під час двофакторної автентифікації, коли користувач вводить свої ім'я користувача та пароль на веб-сайті або в додатку, він зобов'язаний підтвердити свою ідентичність через другий крок. Зазвичай це виконується шляхом введення додаткового коду, який надсилається на мобільний телефон, або за допомогою генерування одноразового коду в додатку. Після успішної автентифікації в обліковий запис, користувач може мати доступ до веб-застосунків або додатків, які вимагають автентифікацію, забезпечуючи вищий рівень безпеки та захисту від несанкціонованого доступу [1].

Двофакторна автентифікація (або двоетапна перевірка) – це параметр безпеки, за допомогою якого користувач може захистити свої облікові записи в Інтернеті, додатково підтверджуючи особистість під час авторизації. Замість того, щоб використовувати лише один спосіб підтвердження особистості, такий як пароль, при 2FA необхідно ще вказати одноразовий пароль (OTP), надісланий SMS або електронною поштою.

Таким чином, щоб отримати доступ до облікового запису, зазвичай потрібно вказати лише логін та пароль. Це називається одноетапною перевіркою . Все, що потрібно зробити, це просто ввести облікові дані та увійти в систему. Подібний спосіб авторизації ненадійний. Будь-хто може отримати доступ до адреси електронної пошти. Хакери також легко здатні зламати пароль, якщо він не відповідає нормам безпеки і досить простий (наприклад, «123456»). Двофакторна автентифікація додає додатковий рівень захисту, вимагаючи при авторизації надати набір облікових даних, доступ до яких має лише законний власник облікового запису. В результаті сторонні особи не зможуть отримати доступ до конфіденційних даних [2, 3].

Використання двофакторної автентифікації для захисту веб-застосунків є ефективним способом зменшення ризиків несанкціонованого доступу до конфіденційної інформації та збільшення безпеки користувачів. Для реалізації двофакторної автентифікації можна використовувати різні методи, такі як:

1. Підтвердження через SMS-повідомлення або телефонний дзвінок: у такому випадку користувачеві на його телефон відправляється спеціальний код, який потрібно ввести на сайт для підтвердження ідентичності.

2. Використання автентифікатора: спеціального додатку, який генерує тимчасові одноразові коди або QR-коди, які потрібно ввести на сайт.
3. Використання біометричних даних: таких як відбиток пальця або сканування обличчя.
4. Використання фізичних ключів: таких як USB-ключі або NFC-карти.

Крім того, важливо забезпечити використання надійних паролів та їх регулярну зміну, а також захистити сесії користувачів від зловмисників за допомогою механізмів, таких як HTTPS-захист та токени доступу.

Усі ці заходи разом з використанням двофакторної автентифікації можуть забезпечити високий рівень захисту веб-застосунків від кібератак та зберегти конфіденційну інформацію користувачів.

Сьогодні багато веб-застосунків та сервісів підтримують двофакторну автентифікацію як додатковий рівень безпеки для входу в систему. Наприклад, такі відомі компанії, як Google, Facebook, Twitter, Dropbox, Microsoft та інші, надають можливість використовувати двофакторну автентифікацію для своїх користувачів. Деякі веб-застосунки також надають можливість налаштувати свій власний двофакторний механізм аутентифікації. Зазвичай, використання двофакторної автентифікації в таких сервісах є необов'язковим, але рекомендується для підвищення рівня безпеки користувачів.

Для використання механізму двофакторної автентифікації для захисту веб-застосунків, необхідно виконати декілька кроків [1]:

1. Вибрати механізм двофакторної автентифікації: існують різні типи механізмів, такі як SMS-підтвердження, генератори одноразових паролів (OTP) і біометрична автентифікація. Вибір механізму залежить від ваших потреб та можливостей.
2. Активувати механізм двофакторної автентифікації: більшість веб-сайтів та сервісів мають налаштування для активації двофакторної автентифікації в розділі налаштувань облікового запису. Для активації зазвичай потрібно підтвердити свій номер телефону, електронну пошту або налаштувати генератор OTP.
3. Використовувати механізм двофакторної автентифікації: після активації двофакторної автентифікації, при кожному вході в обліковий запис буде запитуватись додатковий код підтвердження з механізму двофакторної автентифікації. Цей код може бути відправлений на телефон або згенерований з генератора OTP.

Найбільш ефективним вважається використання механізму генератора одноразових паролів (OTP), оскільки він генерує унікальний код підтвердження, який може бути використаний лише один раз. Також слід пам'ятати про необхідність збереження ключа від генератора OTP в безпечному місці, оскільки він є ключовим елементом для отримання коду підтвердження [2].

Основними рекомендаціями щодо використання двофакторної автентифікації для забезпечення максимального рівня безпеки є:

1. Використання двофакторної автентифікацію на всіх облікових записах, які підтримують цю функцію. Це дозволить максимально захистити ваші дані та уникнути можливого взлому облікового запису.
2. Використання сильних паролі для всіх облікових записів та не використовувати один і той же пароль для декількох облікових записів. Використання різних паролів для кожного облікового запису зменшує ризик взлому ваших облікових записів.
3. Використання механізми двофакторної автентифікації, які базуються на різних типах автентифікації. Наприклад, використання пароля та SMS-повідомлення або пароля та автентифікаційного токена зменшує ризик використання одного й того ж механізму автентифікації.
4. Не зберігати свої паролі та інші конфіденційні дані на комп'ютері, який не захищений від злому або віддаленого доступу. Не зберігати свої паролі на публічних комп'ютерах, таких як кіоски, кафе або бібліотеки.

5. Регулярне оновлення своїх паролів та перевірка активних сесій на своїх облікових записах, щоб переконатися, що ніхто не має доступу до особистої інформації без дозволу.
6. Забезпечення безпеки особистих пристроїв та мереж, які використовуються для доступу до особистих облікових записів. Регулярне встановлення оновлення програмного забезпечення на особистих пристроях.

При виборі механізму двофакторної автентифікації для захисту веб-застосунків важливо враховувати кілька факторів, таких як рівень безпеки, зручність використання, сумісність зі смартфоном та іншими пристроями. Основні механізми двофакторної автентифікації, які варто розглянути, включають [1, 3]:

- СМС-повідомлення або телефонний дзвінок - цей метод включає надсилання коду підтвердження на зареєстрований номер мобільного телефону користувача. Для використання цього методу необхідно мати доступ до мобільного телефону.
- Мобільний додаток - цей метод включає використання спеціального додатку для генерації кодів підтвердження. Коди генеруються на основі унікального ідентифікатора акаунту користувача та секретного ключа, який зберігається в додатку. Для використання цього методу необхідно мати смартфон та встановлений на ньому додаток.
- Фізичний токен - цей метод включає використання спеціального фізичного пристрою для генерації кодів підтвердження. Простіші варіанти таких пристроїв виглядають як картки з індикатором або спеціальні USB-ключі. Для використання цього методу необхідно мати доступ до фізичного пристрою.
- Біометричні дані - цей метод включає використання біометричних даних, таких як відбитки пальців або розпізнавання обличчя, для підтвердження особи. Для використання цього методу необхідно мати пристрій зі вбудованим біометричним сканером.

При виборі механізму двофакторної автентифікації важливо враховувати кілька факторів, щоб забезпечити найвищий рівень безпеки [3]:

- Спосіб отримання другого фактору: важливо вибрати спосіб отримання другого фактору, який є зручним і безпечним для користувача. Наприклад, можна використовувати SMS-повідомлення, мобільні додатки або фізичні пристрої, такі як токени або ключі безпеки.
- Рівень безпеки: різні механізми двофакторної автентифікації мають різний рівень безпеки. Наприклад, SMS-повідомлення можуть бути підвержені атакам з використанням перехоплення повідомлень, тоді як фізичні ключі безпеки є найбільш безпечними.
- Вартість та складність реалізації: різні механізми двофакторної автентифікації мають різні вартості і рівні складності реалізації. Наприклад, використання мобільних додатків може бути безкоштовним, але вимагати більшої складності налаштування, тоді як використання фізичних ключів безпеки може бути дорожчим, але більш простим у використанні.
- Підтримка: важливо вибрати механізм двофакторної автентифікації, який підтримується веб-застосунком або сервісом, який ви використовуєте. Наприклад, якщо сервіс не підтримує фізичні ключі безпеки, ви не зможете використовувати їх для автентифікації.

Двофакторна автентифікація має як переваги, так і недоліки. Основні переваги використання двофакторної автентифікації включають [1, 3]

1. Підвищена безпека: використання двох факторів для автентифікації зменшує ризик несанкціонованого доступу до облікового запису.
2. Легкість використання: більшість механізмів двофакторної автентифікації досить прості для використання і не потребують додаткових технічних знань.

3. Гнучкість: користувачі можуть вибирати різні способи другого фактора, що дозволяє їм використовувати той, який їм більше підходить.
4. Зменшення ризику втрати даних: якщо зловмисник зламає пароль, він не зможе отримати доступ до облікового запису без другого фактора.
5. Захист від фішингу: двофакторна автентифікація може захистити від фішингу, коли зловмисник намагається отримати пароль, шляхом підміни веб-сайту або відправлення підробленого листа.

Незважаючи на ці переваги, двофакторна автентифікація має деякі недоліки, зокрема :

1. Складність використання: двофакторна автентифікація може викликати додаткові труднощі для користувача, особливо якщо він не знайомий з процесом. Це може призвести до незадоволення та відмови від використання такого механізму автентифікації.
2. Залежність від доступу до другого фактора: двофакторна автентифікація може бути неефективною, якщо користувач не має доступу до другого фактора, такого як мобільний телефон або ключ-токен.
3. Витрати на впровадження: використання двофакторної автентифікації може бути додатковою витратою для компанії, особливо якщо вона використовує платні механізми автентифікації.

Висновки. Захист веб-застосунків є дуже важливим завданням для підприємств та користувачів. У цьому контексті, двофакторна автентифікація може бути ефективним механізмом для забезпечення безпеки вхідних даних. Основна ідея двофакторної автентифікації полягає у використанні двох різних механізмів для перевірки ідентичності користувача. Це може включати використання пароля та фізичного пристрою, який можна мати при собі, такого як токен або смарт-карту, або використання біометричних даних, таких як відбиток пальця або розпізнавання обличчя. Переваги двофакторної автентифікації включають зниження ризику порушення безпеки від зломів паролів та фішингу, підвищення рівня захисту особистих даних, а також можливість встановлення додаткових прав доступу для різних користувачів. Однак, двофакторна автентифікація також має деякі недоліки, такі як додаткові витрати на обладнання та ресурси, які потрібні для підтримки цього механізму, а також можливість блокування доступу до веб-застосунку в разі втрати пристрою або забутого пароля.

У цілому, двофакторна автентифікація є ефективним механізмом для забезпечення безпеки веб-застосунків, який може допомогти у запобіганні багатьом видам кібератак. При виборі механізму двофакторної автентифікації важливо розглядати функціональні та безпекові вимоги конкретного веб-застосунку, а також забезпечити правильні налаштування та підтримку механізмів для забезпечення безпеки.

Список використаних джерел

1. A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods \\ Режим доступу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=199a71f02c63b4b84a00e9b73fd538d28ed92362 (останнє звернення 13.04.2023р.)

2. Empirical Measurement of Systemic 2FA Usability \\ Режим доступу: https://www.usenix.org/system/files/sec20-reynolds.pdf (останнє звернення 10.04.2023р.)

3. A Usability Study of Five Two-Factor Authentication Methods \\ Режим доступу: https://www.usenix.org/system/files/soups2019-reese.pdf (останнє звернення 10.04.2023р.)

Робота виконана під науковим керівництвом ст. викладача
КОСТЮК Ю.В.

МЕТОДИ ПРОТИДІЇ ЗЛОЯКІСНОМУ КОДУ ТА ШПИГУНСЬКОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕНЮ

КРИВЕНКО О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні технологія створення системи протидії злоякісному коду та шпигунського програмного забезпечення. Зазначено види злоякісного коду та їх засоби протидії. Розглянуто зразки захисту від шкідливих програм за допомогою "Cisco".

The article discusses the basic technology of creating a system for countering malicious code and spyware. The types of malicious code and their countermeasures are specified. Samples of protection against malicious programs with the help of "Cisco"

Актуальність. Шпигунське програмного забезпечення - це ряд шкідливих програм, які дозволяють стежити за діями користувача в мережі Інтернет, а також збирати його конфіденційні дані. Вперше цей термін було вжито в публікації служби новин Usenety в 1995 році [1]. З розвитком технологій кібербезпеки багато шпигунських програм зникли, натомість з'явилися інші, більш складні форми шпигунського програмного забезпечення. Кіберзлочинці можуть використовувати шпигунське програмне забезпечення для отримання особистої інформації, для крадіжки даних або шахрайства.

Злоякісний код або шкідливий програмний засіб — це програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. Може проявлятися у вигляді коду, скрипту, активного контенту, і іншого програмного забезпечення. Треба зазначити що, зловмисні програмні засоби відрізняються від дефективного програмного забезпечення тим, що останнє є легальним програмним забезпеченням, але містить шкідливі помилки, які не були виправлені до випуску. Програмне забезпечення, яке може бути віднесене до «шкідливих програм» може бути заснованим на різних технологіях, володіти абсолютно різним набором функцій і можливостей. Єдине, що об'єднує всі типи шкідливих програм — це мета, з якою вони створюються.

Шпигунське програмне забезпечення (ШПЗ) це як вірус або злоякісний код, який використовується для «шпигунства», він записує всі дії, записує місцезнаходження, IP-адресу, електронні листи, паролі, номери кредитних карт та різні інші дані, з метою передачі цієї інформації третім особам через Інтернет [2].ШПЗ має високу прихованість, - його дуже важко розпізнати без допомоги антивірусного програмного забезпечення, оскільки володіє важким проникненням у систему. ШПЗ гарно шифрується навіть, коли пристрій намагається видалити його з реєстру Windows, і перехоплює всі спроби це зробити. Іноді шпигунське програмне забезпечення ховається всередині нормальної програми.

ШПЗ може розповсюджуватися через офіційні канали, наприклад веб-сайти розробників або веб-магазин Google. У деяких випадках програми містять не саме шпигунське програмне забезпечення, а функції, які можна використовувати як шпигунське програмне забезпечення. Такі функції часто додаються ненавмисно, і розробник зазвичай видаляє ці функції одразу після повідомлення про них. Тим не менш, існує ще багато сумнівних утиліт, які, як повідомляється, містять елементи шпигунського програмного. Оскільки шпигунське програмне забезпечення може збирати інформацію про вас і надсилати її в інше джерело, тому воно становить величезну загрозу конфіденційності та безпеці.

Метою статті є дослідження ефективних технологій та методів захисту від злоякісного коду з метою збереження конфіденціальної інформації.

Об'єктом дослідження є програмне забезпечення для боротьби з шкідливими програмами.

Предмет дослідження - технології системи протидії злоякісному коду.

Аналіз попередніх досліджень. Дослідженню методів протидії злоякісному коду та шпигунському програмному забезпеченю присвячені праці вітчизняних та закордонних науковців: Чобаль О.І., Різак В.М., Пригара М.П., Ковальов О.О., R. Islam, R. Tian, L. Batten, S. Versteeg та інші.

Аналізуючи дослідження проведені рядом вчених можна дійти висновку, що лідируючу позицію займає Symantec на частку якої припадає 13,56% антивірусів. З них 10,75% відносяться до Symantec Endpoint Protection. На другому місці йде антивірус ESET з часткою 12,84%. ESET Endpoint Antivirus та ESET Endpoint Security займають 4,53% та 3,7% відповідно [7] (див.рис.1.).

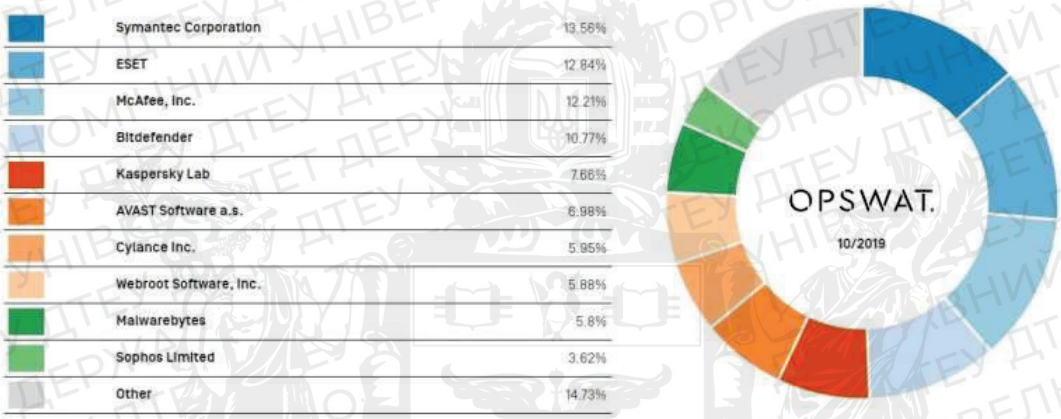


Рис. 1. Популярність антивірусів

Виклад основного матеріалу. В умовах сьогодення можна зазначити велику кількість видів шпигунського програмного забезпечення та злоякісного коду (Рис 2.).

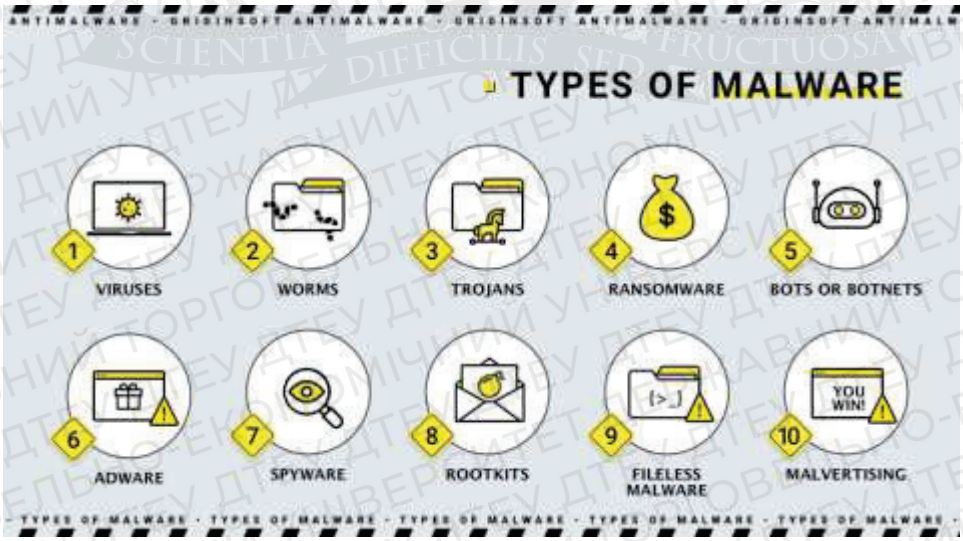


Рис. 2. Види злоякісного коду

Як зазначалося вище основною особливістю таких програм є те, що вони для збору інформації з системи використовують стандартні методи, якими користується ряд інших програм. Завдяки цьому вони можуть не лише збирати, обробляти та передавати зібрані дані третім особам, але і при цьому залишаються непомітними як для користувача так і для захисних программ [8].

Технології постійно розвиваються, як і нові віруси, тому простіше класифікувати їх на типи та види шпигунських програм. Їх можна розділити на чотири основні групи: рекламне програмне забезпечення, файли cookie, трояни та системи моніторингу. Розглянемо найпопулярніші шпигунські програми та шкідливі програми, а саме [3]:

- Кейлоггер – один з найпопулярніших видів шпигунських програм використовується для контролю за натисканням кнопок на клавіатурі.
- Рекламне програмне забезпечення – це вся реклама, яка перекидає користувача в інше місце призначення.
- Троянські програми – надзвичайно небезпечні, тому що вони переймають паролі. Особливо для банківської справи.
- Вебмаяк – зображення, які найчастіше прикріплюються до повідомлень електронної пошти й дозволяють відстежувати поведінку користувачів.
- Руткіт – дозволяє хакеру встановлювати інструменти, які нададуть йому віддалений доступ до обладнання.
- Cookie – файли є різновидом шпигунських програм. Правда, вони менш шкідливі і багато користувачів погоджуються з ними, але вони також дозволяють відстежувати вас в Інтернеті.
- Черви – це шматочки шкідливого коду, які роблять копії. Умови повинні бути правильними, щоб глист розмножувався. Вони створюються переважно за допомогою мов сценаріїв [4].

Технології захисту не стояли на місці, вони теж вдосконалилися. Методи захисту від шкідливих програм стали набагато краще ніж були раніше, тому і шкідливих програм стало набагато менше. Але щоб злоякісний код не зміг видалити або викрасти наші дані, треба проходити процедури захисту персонального комп'ютера, такі як:

Інструменти захисту кінцевих точок забезпечують захист, щоб запобігти зламам кінцевих точок і захистити IT системи від загроз кінцевих точок, включаючи зараження зловмисним програмним забезпеченням і різні кібератаки.

Захист кінцевих точок розширює видимість пристроїв, які традиційно знаходяться за межами периметра безпеки, наприклад особистих ноутбуків і планшетів, які використовуються для роботи, а також корпоративних серверів і робочих станцій.

Антивірусні рішення наступного покоління (NGAV) відстежують і реагують на тактику, прийоми та процедури зловмисників (TTP), щоб допомогти запобігти як відомим, так і невідомим загрозам. Ця технологія була створена, щоб заповнити прогалини, залишені традиційним антивірусним програмним забезпеченням, яке може захищати лише від відомих файлових атак зловмисного програмного забезпечення.

Технологія NGAV пропонує хмарний, системо центричний підхід. Він використовує прогнозну аналітику на основі машинного навчання (ML) і штучного інтелекту (AI) у поєднанні з аналізом загроз для виявлення атак, збору даних криміналістики та реагування на загрози. NGVA може ідентифікувати без файлові атаки без зловмисного програмного забезпечення, зловмисну поведінку та зловмисне програмне забезпечення, реагувати на загрози та збирати дані кінцевої точки для визначення першопричини.

Система запобігання вторгненням (IPS) постійно відстежує мережевий трафік, щоб виявити постійне зараження зловмисним програмним забезпеченням або порушення безпеки. Він також може виконувати відповідні дії в конкретних випадках, які були попередньо визначені адміністратором мережі.

IPS постійно моніторить мережу в режимі реального часу, щоб швидко виявляти й реагувати на потенційні загрози, виконуючи дії для запобігання спостережуваних подій. Він працює, перевіряючи потоки мережевого трафіку на наявність шкідливого програмного забезпечення. Технологія визначає зловмисну діяльність, записує виявлені загрози, повідомляє про виявлені загрози та вживає профілактичних дій для блокування загрози.

Безпека ізольованого програмного середовища забезпечує додатковий рівень захисту від загроз безпеці. Це передбачає використання пісочниці, ізольованого середовища, що імітує

операційне середовище кінцевого користувача, для виконання підозрілого коду. Пісочниця забезпечує безпечне середовище, яке відокремлює загрозу від головного пристрою чи мережі. Це особливо корисно під час роботи зі зловмисним програмним забезпеченням нульового дня та стелс-атаками, гарантуючи, що ви можете ізолювати та перевіряти ці загрози, щоб запобігти їх поширенню.

Брандмауер наступного покоління (NGFW) забезпечує застосування політик безпеки для виявлення та блокування складних атак на рівні протоколу, порту та програми. Ви можете реалізувати цю технологію брандмауера третього покоління в апаратному чи програмному забезпеченні.

Дані, що проходять через Інтернет або мережу, розбиваються на невеликі частини, які називаються пакетами. Брандмауери перевіряють ці пакети, оскільки вони містять вміст, який вимагає доступу до мережі. Брандмауер відповідає за блокування або дозвіл пакетів, запобігаючи потраплянню в мережу зловмисного вмісту, зокрема зловмисного програмного забезпечення.

NGFW використовують традиційні можливості брандмауера разом із новими та покращеними функціями. Традиційні можливості включають: фільтрування пакетів, переклад адреси порту (PAT), трансляція мережевих адрес (NAT), віртуальні приватні мережі (VPN), блокування URL.

NGFW розширює вищезазначене за допомогою функції якості обслуговування (QoS) і додаткових функцій, таких як: запобігання вторгненням, глибока перевірка пакетів, перевірка SSL і SSH, обізнаність із застосуванням, виявлення шкідливих програм на основі репутації [5], нульова довіра.

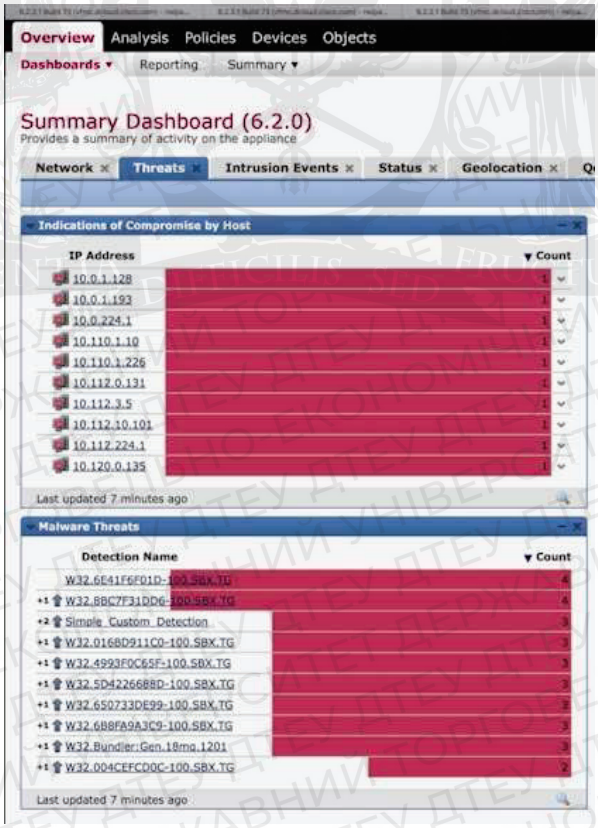


Рис. 3. Приклад роботи Firewall NGFW Demo

Модель нульової довіри – це підхід до безпеки, який усуває неявну довіру та забезпечує сувору автентифікацію користувачів і пристроїв для захисту мережі. Це допомагає забезпечити надійний захист від різних атак, включаючи крадіжку даних і скомпрометовані облікові дані. Ця модель припускає, що довіра особам або пристроям може спричинити багато вразливостей, оскільки навіть авторизовані сторони можуть бути скомпрометовані. Мережа

ніколи не повинна довіряти жодному користувачеві та вимагати автентифікації особи та пристрою в усій мережі, а не лише на периметрі. Реалізація безпеки з нульовою довірою зазвичай передбачає використання мікросегментації для розділення мережевих ресурсів. Ізоляція ресурсів допомагає стримувати загрози в одному мікросегменті мережі, запобігаючи поширенню загрози на інші області. Це мінімізує поверхню атаки та зменшує масштаб шкоди, завданої атакою.

Нульова довіра допомагає створити більш комплексний захист від атак зловмисного програмного забезпечення та програм-вимагачів, надаючи розширені можливості моніторингу та виявлення. Нульова довіра може суттєво обмежити здатність зловмисного програмного забезпечення та програм-вимагачів виконувати боковий рух і заражати додаткові частини корпоративної мережі. Крім того, оскільки людська помилка часто є основною причиною кібератаки, нульова довіра зосереджується на ідентифікації користувача та управлінні доступом.

Висновок: кожна компанія з розробки антивірусного програмного забезпечення рекламує свій продукт переконуючи, що він найкращий. Проте у Топ -5 найкращих програм 2023 року увійшла програма Norton 360, TotalAV, McAfee (лише для США),Bitdefender, Intego. Все більшої популярності набувають антивірусні програми з використанням штучного інтелекту.

Список використаних джерел

1. Матеріал від компанії ESET, "Шпигунські програми". Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/shpionskiye-programmy/ (останнє звернення 04.04.2023р.)
2. Матеріал від gridinsoft, "Що таке шпигунські програми?" державності. Режим доступу: https://gridinsoft.ua/spyware (останнє звернення 04.04.2023р.)
3. Матеріал від dalistrategies, "Що таке шпигунське програмне забезпечення? Як захиститися від нього?" державності. Режим доступу: https://dalistrategies.com/ua/shho-take-shpigunske-programne-zabezpechennya-yak-zahistitisya-vid-nogo/ (останнє звернення 04.04.2023р.)
4. Матеріал від theastrologypage, "Що таке шкідливий код? - визначення з техопедії" державності. Режим доступу: https://uk.theastrologypage.com/malicious-code (останнє звернення 04.04.2023р.)
5. Матеріал від cynet, "Malware Protection Technologies and Techniques" державності. Режим доступу: https://www.cynet.com/malware/malware-protection-6-technologies-to-protect-your-organization/#heading-1 (останнє звернення 04.04.2023р.)
6. ALISA SHEVCHENKO, The evolution of technologies used to detect malicious code. Режим доступу: https://securelist.com/the-evolution-of-technologies-used-to-detect-malicious-code/36177/ (останнє звернення 04.04.2023р.)
7. Найпопулярніші антивіруси. Режим доступу: https://overclockers.ru/blog/Scorpion81/show/31789/samye-populyarnye-antivirusy-na-windows-na-noyabr-2019
8. Програмний продукт для пошуку та виявлення програм типу spyware О.Ковальов, О. Чобаль, В. Різак, М. Пригара . Режим доступу file:///C:/Users

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКО Б.Т.

«ХМАРНИЙ» КВАЛІФІКОВАНИЙ ЕЛЕКТРОННИЙ ПІДПИС

КРИВЕНКО С., 2мз курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто процес використання та зберігання особистого ключа кваліфікованого електронного підпису чи печатки (далі – КЕП), що згенеровано у засобі КЕП – захищеному апаратно-програмному пристрої – криптомодулі, що призначений для реалізації криптографічних перетворень на апаратному рівні та безпечного зберігання особистих ключів зареєстрованих користувачів (далі – Хмарне сховище) кваліфікованого надавача електронних довірчих послуг. Зазначено переваги зберігання та використання особистого ключа КЕП у Хмарному сховищі. Розглянуто як зразок порядок генерації особистого ключа КЕП у Хмарному сховищі кваліфікованого надавача електронних довірчих послуг.

The article discusses the process of using and storing the personal key of a qualified electronic signature or seal (hereinafter - KEP), generated in the KEP tool - a secure hardware and software device - a cryptomodule, which is designed to implement cryptographic transformations at the hardware level and securely store personal keys of registered users (hereinafter - Cloud storage) of a qualified provider of electronic trust services. The advantages of storing and using the KEP personal key in the Cloud storage are indicated. The procedure for generating a personal KEP key in the Cloud storage of a qualified provider of electronic trust services is considered as a sample.

Актуальність. У сучасних умовах розвитку економіки та програмно-технічного прогресу, більшість підприємств намагаються використовувати сучасні технології для оптимізації робочого процесу, зокрема, впровадження електронних сервісів є одним з пріоритетних напрямків, що забезпечує фінансовий розвиток та конкурентоздатність у порівнянні з іншими суб'єктами господарювання.

Обмін електронними даними з контролюючими органами, з іншими підприємствами чи організаціями та у середині підприємства дозволяє покращити процеси управління та контролю діяльності.

Електронний документ – документ, інформацію в якому викладено у вигляді електронних даних, включаючи обов'язкові реквізити документа, одним з яких є електронний підпис автора документи, що відповідає вимогам зазначеним у Законі України «Про електронні довірчі послуги»[1].

В свою чергу електронний підпис це електронні дані, які додаються або логічно пов'язуються з електронного документу [2, с. 6].

Електронна взаємодія користувачів електронних довірчих послуг, що передбачає отримання, відправлення чи зберігання документів, які у паперовому вигляді повинні містити власноручний підпис автора документа, повинна здійснюватися з використанням кваліфікованих електронних довірчих послуг.

Якщо електронний підпис створюється з використанням засобу КЕП та базується на кваліфікованому сертифікаті відкритого ключа то такий підпис вважається кваліфікованим електронним підписом [3].

Метою статті є дослідження особливостей генерації та використання особистих ключів КЕП, що зберігаються у Хмарному сховищі кваліфікованих надавачів електронних довірчих послуг.

Об'єктом дослідження є сервіс Хмарного сховища кваліфікованого надавача електронних довірчих послуг.

Предмет дослідження – Хмарне сховище кваліфікованого надавача електронних довірчих послуг.

Аналіз попередніх досліджень. Дослідження процедури генерації, зберігаються та використання особистих ключів користувачів електронних довірчих послуг, вагоме значення мають дослідження присвячені вивченню електронного підпису (М. Вовк, І. Шепель, Ю. Горбенко, І. Горбенко. та ін.)

Виклад основного матеріалу. Особисті ключі електронного підпису користувачів електронних довірчих послуг можуть бути згенеровано на:

- Незахищений носій користувачів (USB накопичував, CD чи DVD диски та ін.);
- Захищені носії користувачів (Кристал-1, SECURE TOKEN-338, Алмаз-1К та ін.);
- Хмарне сховище кваліфікованого надавача електронних довірчих послуг.

Законодавством встановлені обмеження щодо генерації особистих ключів співробітниками державних органів, генерація здійснюється за особистої присутності працівника державної установи у кваліфікованого надавача електронних довірчих послуг з використанням засобів КЕП.

Також, представники державних органів повинні використовувати виключно кваліфіковані сертифікати відкритих ключів та захищені носії ключової інформації [4].

Деякі надавачі електронних довірчих послуг надають своїм клієнтам послугу дистанційного перевипуску кваліфікованих сертифікатів відкритих ключів, що полягає у формуванні нових кваліфікованих сертифікатів на певний термін (1-2 роки) без особистого відвідування надавача електронних довірчих послуг, у такому випадку ідентифікація користувача здійснюється за даними, що містяться у раніше сформованих сертифікатах відкритих ключів, при цьому здійснюється генерація нового особистого ключа КЕП [3].

У період дії воєнного стану в Україні та протягом місяця з дня його скасування надавачі електронних довірчих послуг можуть здійснювати автоматичний перевипуск кваліфікованих сертифікатів відкритих ключів користувачів без їх особистої присутності. При автоматичному формуванні нових кваліфікованих сертифікатів відкритих ключів генерація нового особистого ключа КЕП не здійснюється, а термін дії скасованого та нового сформованого сертифікатів не повинен перевищувати три роки.

Також, на період воєнного стану та протягом шести місяців з дня його припинення дозволяється використання електронних підписів чи печаток, що базуються на кваліфікованому сертифікаті відкритого ключа без відомостей про те, що особистий ключ зберігається на захищеному носію ключової інформації, окрім випадків передбачених абзацом другим частини другої статті 17 Закону України «Про електронні довірчі послуги» [5].

Перелік надавачів, що здійснюють надання кваліфікованих електронних довірчих послуг зазначається у Довірчому списку, що розміщується на офіційному вебсайті Центрального засвідчувального органу (Міністерство цифрової трансформації України), який здійснює його впровадження та підтримує в актуальному стані (https://czo.gov.ua/trustedlist).

Крім цього, Національний банк України, як засвідчувальний центр, формує та підтримує в актуальному стані відповідний Довірчий список кваліфікованих надавачів електронних довірчих послуг (банків, операторів платіжних систем та організацій, що здійснюють свою діяльність на ринку фінансових послуг та інших) [3].

На вебсайті Центрального завідчувального органу реалізовано сервіс Інструменту моніторингу (https://czo.gov.ua/tool), який дає можливість сформувати тестові сертифікати відкритих ключів для здійснення випробування їх функціонування в різних інформаційно-комунікаційних системах [6].

Хмарний КЕП – це одна з послуг, що може надаватися кваліфікованими надавачами електронних довірчих послуг. На даний час в України тільки деякі кваліфіковані надавачі електронних довірчих послуг реалізували даний сервіс для своїх клієнтів. Їх перелік можливо переглянути скориставшись послугою підпису даних чи автентифікації найпопулярніших надавачів електронних сервісів, наприклад Електронний кабінет Державної податкової служби України (Рис. 1).

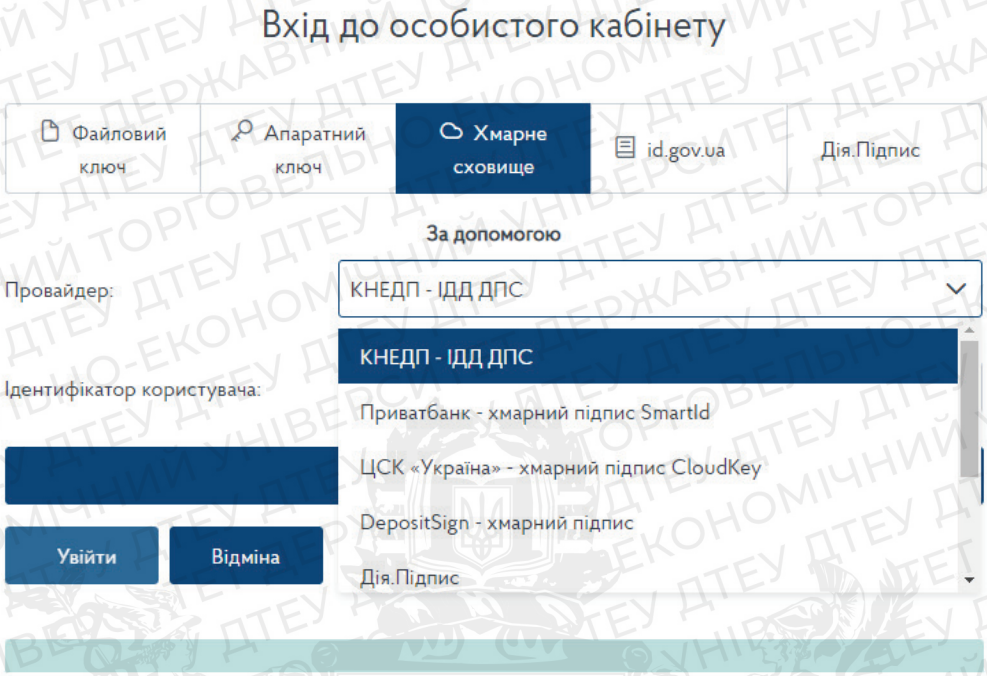


Рис. 1. Перелік кваліфікованих надавачів електронних довірчих послуг

Також, слід розглянути Інтегровану систему електронної ідентифікації id.gov.ua (далі – Сервіс id.gov.ua), що надає можливість здійснити електронну ідентифікацію за допомогою Хмарного КЕП більш ніж на 380 системах автентифікації (Рис. 2).

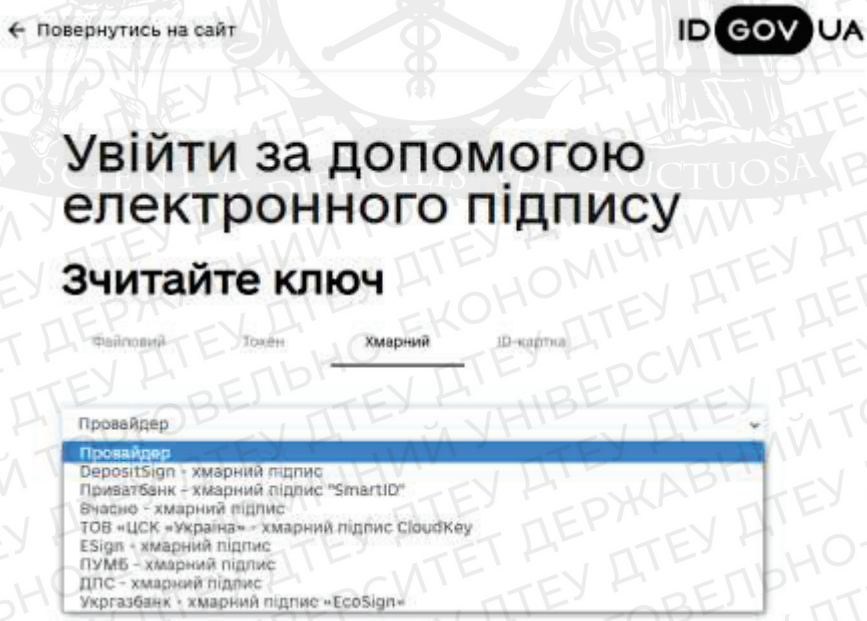


Рис. 2 Інтегрована система електронної ідентифікації

Скориставшись оцінкою стану розвитку сфери електронних довірчих послуг за 2022 рік, що публікується на офіційному вебсайті Центрального засвідчувального органу (Таб. 1), можна визначити, які саме кваліфіковані надавачі електронних довірчих послуг користуються найбільшим попитом серед клієнтів [7].

Таблиця 1.

Кількість сформованих сертифікатів

Кількість сформованих кваліфікованих сертифікатів електронних підписів (без урахування сертифікатів шифрування) за 2022 рік		
Надавач	Усього	Активні
НЕДП АЦСК АТ КБ «ПРИВАТБАНК»	6 849 563	6 592 641
НЕДП «ДІЯ»	5 205 525	2 896 064
НЕДП ТОВ «Центр сертифікації ключів Україна»	748 717	1 068 675
НЕДП ДПС	511 364	887 668
НЕДП АЦСК АТ «Державний ощадний банк України»	132 506	327 257
НЕДП АТ «УКРСИББАНК»	55 354	148 256
НЕДП Державної казначейської служби України	74 509	125 295
НЕДП ДП "УСС"	11 180	130 125
НЕДП "MASTERKEY"	67 540	64 479
НЕДП - АЦСК МВС України	29 811	95 044
Т «СЕНС БАНК»	58 122	53 289
АТ АБ «УКРГАЗБАНК»	30 855	28 525
НЕДП органів прокуратури України	31 336	26 176
НЕДП ЦСК АТ "УКРЗАЛІЗНИЦЯ"	31 718	21 168
Т «ПУМБ»	22 176	21 038
НЕДП ТОВ «ДЕПОЗИТ САЙН»	18 940	19 253
НЕДП «Військова частина 2428»	11 351	16 271
НЕДП «eSign»	12 001	14 346
НЕДП «Центр сертифікації ключів Збройних Сил України»	9 860	8 515
НЕДП ТОВ «Вчасно Сервіс»	4 483	4 110
ЦСК Національного банку України	1 883	4 919
Т «БАНК АЛЬЯНС»	1 710	1 501
НЕДП «АЦСК ринку електричної енергії»	271	420

Т «КРЕДІ АГРІКОЛЬ БАНК»	156	129
асвідчувальний центр	18	38
НЕДП ЦЕЗАІС ТОВ «ІНТЕР-МЕТЛ»	7	0

Проаналізувавши інформацію можна виділити трьох надавачів, що надають послугу Хмарного КЕП та користуються найбільшим попитом серед клієнтів:

1. Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ «ПРИВАТБАНК»;
2. Кваліфікований надавач електронних довірчих послуг «ДІЯ»;
3. Кваліфікований надавач електронних довірчих послуг ТОВ "Центр сертифікації ключів «Україна».

Розглянемо детальніше процедуру генерації особистого ключа у Хмарному сховищі та формування кваліфікованого сертифіката відкритого ключа на прикладі Кваліфікований надавач електронних довірчих послуг «ДЕПОЗИТ САЙН» (далі – Надавач «ДЕПОЗИТ САЙН») (https://ca.depositsign.com).

Для початку необхідно зареєструватися у особистому кабінеті Надавача «ДЕПОЗИТ САЙН» та заповнивши відповідну форму (https://cabinet.depositsign.com/register) (Рис. 3).

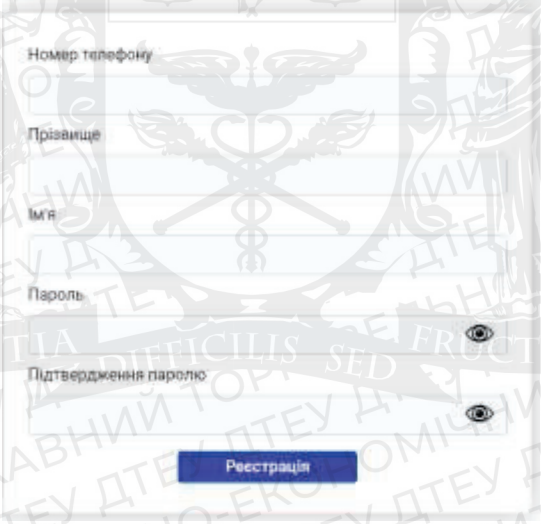


Рис. 3. Форма реєстрації

Підтвердити реєстрацію, зазначивши у відповідному полі код реєстрації, що направляється повідомленням на вказаний номер телефону (Рис. 4).

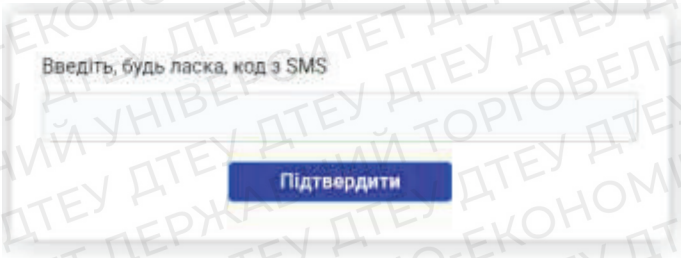


Рис. 4 Форма підтвердження реєстрації

Здійснити авторизацію та натиснути «Сформувати заявку» (Рис. 5).

Рис. 5 Формування заявки

Заповнити відповідні поля у заявці та натиснути «Зберегти» (Рис. 6).

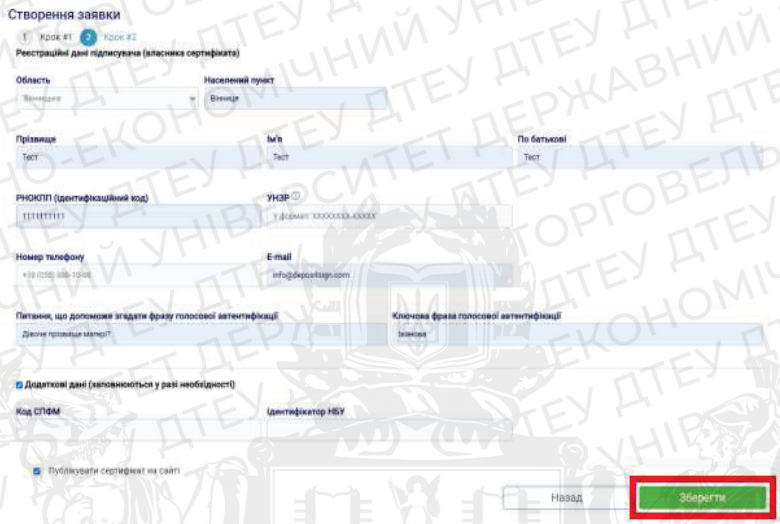


Рис. 6 Формування заявки

Здійснити генерацію особистого ключа КЕП. Після генерації в особистому кабінеті сформується обліковий запис хмарного підпису.

Для формування кваліфікованих сертифікатів відкритих ключів необхідно підготувати відповідний перелік документів та особисто звернутися до представництва Надавача «ДЕПОЗИТ САЙН» для здійснення ідентифікації користувача електронних довірчих послуг.

Розглянемо процедуру підписання електронного документу з використанням особистого ключа що зберігається у Хмарному сховищі Надавача «ДЕПОЗИТ САЙН» у Сервісі id.gov.ua:

1. Обираємо «Підпис файлів» (https://id.gov.ua/sign);
2. Натискаємо «Електронний підпис» та обираємо тип носія, з якого буде зчитано особистий ключ і зазначаємо кваліфікованого надавача електронних довірчих послуг та вводимо Ідентифікатор користувача (Рис. 7).

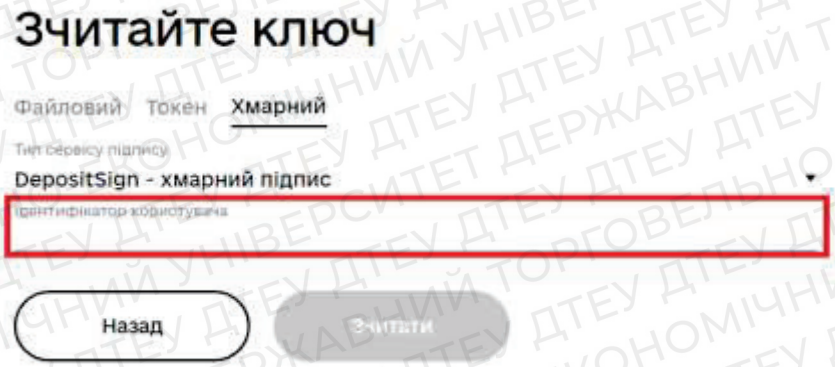


Рис. 7 Формування зчитування ключа

3. Під час зчитування особистого ключа на Ваш смартфон, у додаток «DepositSign» надійде PUSH-повідомлення з посиланням, за яким необхідно перейти для обрання особистого ключа який буде використовуватись для авторизації та підтвердити його використання (Рис. 8);

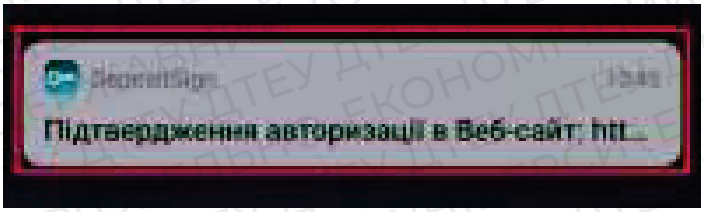


Рис. 8 Формування сповіщення

4. У Сервіс id.gov.ua необхідно перевірити особисті дані та натиснути «Далі» (Рис. 9);

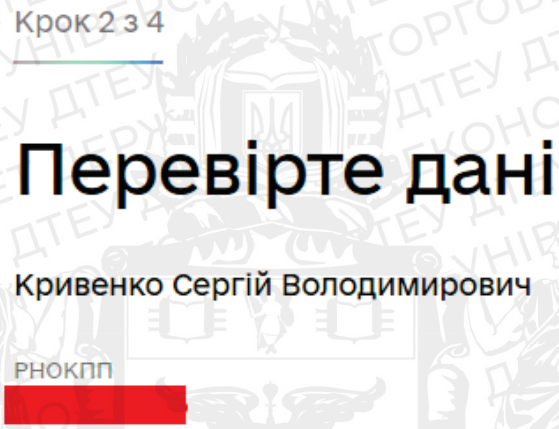


Рис. 9 Формування перевірки даних

5. Обираємо спосіб підписання та файл який необхідно підписати та натискаємо «Підписати» (Рис. 10);

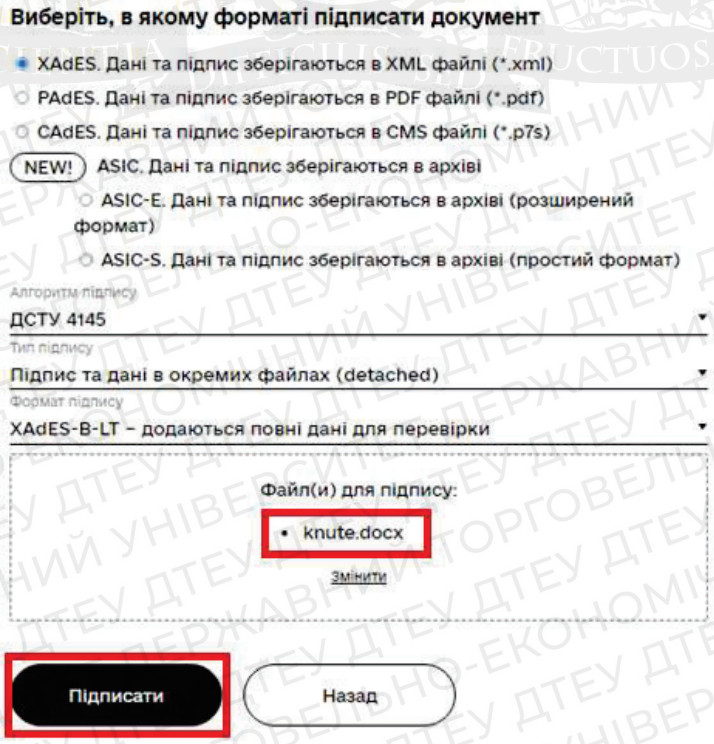


Рис. 10 Формування підпису та зберігання

6. У додаток «DepositSign» надійде PUSH-повідомлення, за яким необхідно перейти для обрання особистого ключа який буде використовуватись для підпису електронного документу;

7. Завантажуємо підписаний електронний документ (Рис. 11);

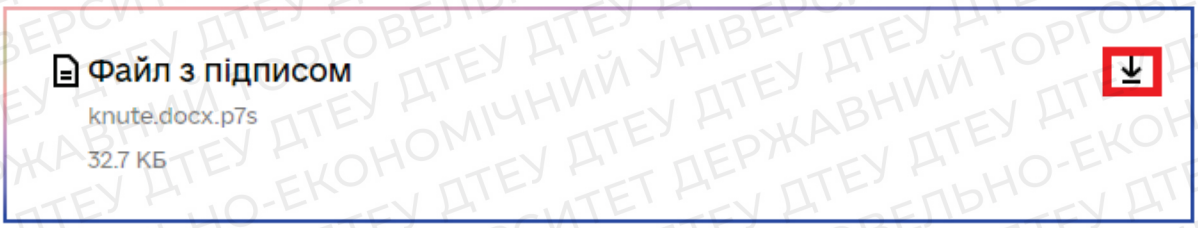


Рис. 11 Формування завантаження підписаного документу

Висновки. За умови використання особистого ключа, що зберігається у Хмарному сховищі кваліфікованого надавача електронних довірчих послуг, сертифікат, що сформується буде містити відмітку про те, що особистий ключ, який відповідає відкритому ключу збережено у засобі КЕП. Такий спосіб зберігання особистого ключа дозволяє уникнути його викрадення, пошкодження чи втрати. КЕП, який сформований з використанням особистого ключа, що зберігається у Хмарному сховищі кваліфікованого надавача електронних довірчих послуг повністю відповідає всім вимогам законодавства України у сфері електронних довірчих послуг.

Список використаних джерел

1. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. – Режим доступу: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15#Text. – Назва з екрана.
2. Горбенко І. Д., Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія. – Видавництво «Форт», 2010. – 608 с.
3. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text. – Назва з екрана.
4. Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності: Постанова Кабінету Міністрів України від 19.09.2018 № 749. – Режим доступу: https://zakon.rada.gov.ua/laws/show/749-2018-%D0%BF#Text. – Назва з екрана.
5. Деякі питання забезпечення безперебійного функціонування системи надання електронних довірчих послуг: Постанова Кабінету Міністрів України 17.03.2022 № 300. – Режим доступу: https://zakon.rada.gov.ua/laws/show/300-2022-%D0%BF#Text. – Назва з екрана.
6. Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг: Наказу Міністерства цифрової трансформації України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.09.2020 № 140/614. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1039-20#Text. – Назва з екрана.
7. Центральний засвідчувальний орган Міністерство цифрової трансформації України. URL: https://czo.gov.ua/development?tab=1 (дата звернення: 28.03.2023).

Робота виконана під науковим керівництвом доцента
ВЛАСЕНКО Л.О.

ПОЛІТИКА БЕЗПЕКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

КРИВОРОТ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто питання політики безпеки конфіденційної інформації на підприємстві, зокрема визначення основних принципів захисту конфіденційної інформації, встановлення відповідальності працівників за її збереження та методи захисту конфіденційної інформації. Досліджено ризики, які пов'язані з неякісним захистом конфіденційної інформації. Описано процедуру створення політики безпеки конфіденційної інформації на підприємстві, що допоможе забезпечити безпеку даних та захистити їх від несанкціонованого доступу та від можливих загроз.

The article deals with the issues of confidential information security policy at an enterprise, in particular, defining the basic principles of confidential information protection, establishing the responsibility of employees for its preservation and methods of confidential information protection. The risks associated with poor protection of confidential information are investigated. The procedure for creating a security policy for confidential information at an enterprise is described, which will help ensure data security and protect it from unauthorized access and possible threats.

Актуальність. Актуальність політики безпеки конфіденційної інформації на підприємстві визначається значущими загрозами, які існують у сфері захисту даних та інформації. Зокрема, зростають кібератаки, вірусні атаки, крадіжки даних та інші загрози, які можуть спричинити серйозні наслідки для діяльності підприємства. Крім того, підприємства повинні дотримуватися законодавства щодо захисту конфіденційної інформації, зокрема згідно зі Законом України «Про захист персональних даних» та іншими нормативними документами. Тому розробка і виконання політики безпеки конфіденційної інформації на підприємстві є важливим заходом для забезпечення захисту конфіденційної інформації та зменшення ризиків втрати даних.

Таким чином, розробка та впровадження політики безпеки конфіденційної інформації на підприємстві є актуальною та необхідною умовою забезпечення стійкої та ефективної діяльності підприємства в умовах зростаючих загроз захисту даних та інформації.

Метою статті є дослідження питання політики безпеки конфіденційної інформації на підприємстві та визначення параметрів, які необхідно враховувати для безпеки конфіденційної інформації на підприємстві.

Об'єктом дослідження є процес захисту конфіденційної інформації від несанкціонованого доступу, збереження цілісності та конфіденційності інформації, а також визначення відповідальності працівників за збереження конфіденційної інформації.

Предметом дослідження є заходи, процедури та політики, що використовуються для захисту конфіденційної інформації в організації.

Аналіз попередніх досліджень. У більшості досліджень щодо захисту конфіденційної інформації на підприємствах зазвичай досліджується ефективність та раціональність політики безпеки конфіденційної інформації на підприємстві, оцінюються наслідки витоків інформації, а також визначаються можливі ризики, що пов'язані з використанням інформації в організації.

Більшість досліджень з цієї області зосереджені на проблемах технічного захисту інформації та використанні різних методів шифрування, проте не менш важливим є врахування людського фактору в безпеці інформації. Деякі дослідження акцентують увагу на питаннях психологічного навчання працівників та розробці процедур управління персоналом в цій області.

Одним зі заслужених дослідників в області захисту конфіденційної інформації є Брюс Шнайер, який є автором декількох книг на тему криптографії та захисту даних. У своїх дослідженнях він зосереджується на аналізі загроз та ризиків, пов'язаних з цифровою безпекою та захистом даних. Також, на цю тему було опубліковано декілька досліджень з боку міжнародних організацій, таких як Міжнародне агентство з атомної енергії (МАГАТЕ) та Європейський союз. У цих дослідженнях було визначено низку стандартів та рекомендацій з приводу захисту конфіденційної інформації на підприємствах [1].

Багато досліджень зосереджуються на визначенні рівня конфіденційності даних та видів інформації, що підпадають під захист, а також на розробці процедур та політик збереження конфіденційної інформації. Окремі дослідження присвячені правилам доступу до конфіденційної інформації, вимогам до користування електронною поштою та соціальними мережами, а також процедурам повідомлення про можливі порушення безпеки даних та визначенню способів ліквідації наслідків інциденту.

Виклад основного матеріалу. У сучасному цифровому світі, де інформація стала найціннішим активом, забезпечення безпеки конфіденційної інформації на підприємстві стає критично важливим завданням. В умовах зростаючих кіберзагроз, крадіжок даних та інших кібератак, розробка та впровадження ефективної політики безпеки стають необхідністю для збереження довіри клієнтів, збереження репутації підприємства та забезпечення стійкого розвитку.

Політика безпеки конфіденційної інформації відіграє роль надійного щита, що захищає не лише цифрові активи, а й репутацію та довіру до організації. Вона передбачає комплексний підхід до захисту даних від несанкціонованого доступу, витоку та порушень конфіденційності. У своєму суттєвому аспекті, політика безпеки охоплює не лише технічні аспекти, але й культурну складову, де всі співробітники беруть активну участь у формуванні безпечного інформаційного середовища.

У світлі постійно зростаючої комплексності кіберзагроз та вимог до захисту даних, розуміння політики безпеки конфіденційної інформації стає важливішим ніж будь-коли. Ця стаття намагатиметься прояснити сутність, важливість та ключові складові цієї політики, щоб сприяти зміцненню безпеки та надійності інформаційних ресурсів підприємства.

Захист конфіденційної інформації є критично важливим завданням для будь-якого підприємства, оскільки від його ефективності залежать не тільки фінансові показники, а й репутація компанії, її взаємовідносини з клієнтами та іншими стейкхолдерами. Проблематика захисту конфіденційної інформації на підприємствах полягає у тому, що незаконний доступ до такої інформації може призвести до витоку даних, крадіжки ідентифікаційних даних, шахрайства, розкриття комерційної таємниці, а також порушення різних законів, які регулюють обіг конфіденційної інформації.

Підприємства повинні бути готові до захисту конфіденційної інформації, що збирається, обробляється та зберігається у їхніх інформаційних системах. Проте, на жаль, багато підприємств не мають достатнього рівня знань та досвіду у цій галузі, що призводить до частих випадків порушення безпеки даних.

Для того, щоб забезпечити ефективний захист конфіденційної інформації на підприємствах, необхідно провести аналіз потенційних загроз та ризиків, розробити відповідні політики та процедури збереження конфіденційної інформації, визначити відповідальних осіб та розподіл обов'язків, встановити правила доступу до інформації та розробити програму навчання для співробітників щодо захисту конфіденційної інформації. Також важливо дотримуватись вимог законодавства та стандартів, що регулюють захист персональних даних та конфіденційної інформації. Ці терміни та поняття пов'язані з захистом конфіденційної інформації на підприємствах. Для забезпечення ефективного захисту конфіденційної інформації необхідно розуміти ці поняття та використовувати відповідні методи та інструменти, такі як шифрування, бекап, авторизація, ідентифікація та автентифікація, аудит тощо.

Навчання співробітників про правила доступу до конфіденційної інформації повинно бути включене до їх вступного навчання та регулярно повторюватися. Співробітники повинні бути свідомі про важливість конфіденційної інформації, про заходи, які повинні бути вжиті для її захисту, та про наслідки її можливої втрати чи неправомірного доступу.

Крім того, підприємство повинно визначити відповідальність за порушення правил збереження та доступу до конфіденційної інформації. Це може включати дисциплінарні заходи для співробітників, які порушують правила, а також відшкодування збитків, спричинених незаконним доступом до конфіденційної інформації. Для забезпечення ефективного захисту конфіденційної інформації, необхідно спочатку визначити рівень конфіденційності даних, тобто ступінь їх важливості та значимості для підприємства. Зазвичай використовуються три рівні конфіденційності даних [1]:

- Високий рівень конфіденційності − це дані, які можуть спричинити серйозні наслідки для підприємства, якщо вони потраплять в руки несанкціонованих осіб. Це можуть бути фінансові дані, персональні дані клієнтів, плани розвитку підприємства та інші важливі дані.
- Середній рівень конфіденційності − це дані, які можуть мати обмежений вплив на підприємство, якщо вони стануть відомі несанкціонованим особам. Це можуть бути, наприклад, інформація про продукти або послуги підприємства, інформація про роботу підприємства тощо.
- Низький рівень конфіденційності − це дані, які не мають значного впливу на підприємство, якщо вони потраплять в руки несанкціонованих осіб. Це можуть бути, наприклад, загальна інформація про підприємство, новини тощо [1, 2].

Після визначення рівня конфіденційності даних, необхідно визначити види інформації, що підпадають під захист. Це можуть бути такі види інформації, як: фінансові дані; персональні дані; комерційна інформація; плани розвитку підприємства; договори та угоди; конкурентна інформація; інтелектуальна власність.

Політика безпеки конфіденційної інформації на підприємстві має на меті забезпечення захисту важливих даних від несанкціонованого доступу, використання, розголошення, пошкодження та втрати. Ця політика передбачає встановлення системи заходів та процедур, які мають на меті запобігти загрозам, що можуть виникнути при обробці та зберіганні конфіденційної інформації.

Вимоги законодавства та стандартів є важливими компонентами в розробці політики безпеки конфіденційної інформації на підприємстві. Організації повинні дотримуватися різноманітних правил та норм, щоб забезпечити належний рівень захисту конфіденційної інформації та виконувати свої обов'язки перед клієнтами та партнерами. Одним з ключових документів є Закон України "Про захист персональних даних", який встановлює вимоги до обробки та захисту персональних даних громадян. Закон вимагає, щоб організації, які обробляють персональні дані, мали відповідні технічні та організаційні заходи для захисту цих даних. Закон також встановлює вимоги щодо зберігання та обмеження доступу до персональних даних.

Іншим документом є міжнародний стандарт ISO/IEC 27001, який встановлює вимоги до систем управління інформаційною безпекою. Стандарт містить вимоги щодо політики безпеки інформації, управління ризиками, захисту від несанкціонованого доступу та ведення журналів, сертифікації та аудиту систем управління інформаційною безпекою. Додатково, існують інші стандарти та регуляторні вимоги, які стосуються захисту конфіденційної інформації, такі як Payment Card Industry Data Security Standard (PCI DSS) для захисту платіжної інформації, або General Data Protection Regulation (GDPR) в Європейському Союзі, що встановлює вимоги до захисту персональних даних. Таким чином, вимоги законодавства та стандартів є важливими складовими політики безпеки конфіденційної інформації на підприємстві. Наприклад, є ряд законодавчих актів, які вимагають від підприємств забезпечувати високий рівень захисту конфіденційної інформації, таких як Закон України

"Про захист персональних даних", Закон України "Про інформацію", Закон України "Про електронний підпис", тощо [2].

Також існують різні стандарти, наприклад, ISO/IEC 27001, які встановлюють вимоги до систем управління інформаційною безпекою та захисту інформації. У практиці, багато компаній використовують стандарти та рекомендації для розробки власних політик безпеки, або ж стежать за відповідністю своїх процедур та практик зазначеним вимогам.

Врахування вимог законодавства та стандартів є важливим елементом впровадження політики безпеки конфіденційної інформації, який допомагає забезпечити високий рівень захисту даних та уникнути можливих юридичних проблем. Окрім того, виконання вимог законодавства та стандартів допомагає встановити спільну базу знань та практик в галузі інформаційної безпеки, що сприяє розвитку цієї галузі та підвищенню її рівня.

Потенційні загрози та ризики − це можливі небажані події або дії, які можуть спричинити втрату конфіденційної інформації або порушення її конфіденційності. До потенційних загроз та ризиків можуть належати: кібератаки − хакери можуть намагатися зламати системи захисту даних на підприємстві і викрасти конфіденційну інформацію; внутрішні загрози − співробітники підприємства можуть ненавмисно або навмисно витікати конфіденційну інформацію, яка може завдати шкоди підприємству або його клієнтам; соціальний інжиніринг − зловмисники можуть використовувати соціальний інжиніринг, щоб отримати доступ до конфіденційної інформації; втрати даних − погане зберігання або резервне копіювання даних може призвести до втрати конфіденційної інформації; недосконаліть процедур − недосконаліть політики безпеки може призвести до неправильного зберігання чи обробки конфіденційної інформації, що призведе до викрадення чи витікання даних.

Розробка процедур та політик збереження конфіденційної інформації − це процес визначення і впровадження набору правил та процедур, які гарантують захист конфіденційної інформації від несанкціонованого доступу, використання або розголошення. Для розробки таких процедур та політик необхідно визначити рівень конфіденційності інформації та види інформації, що підпадають під захист, а також потенційні загрози та ризики, що можуть виникнути [3].

При розробці процедур та політик збереження конфіденційної інформації необхідно враховувати наступні аспекти:

- Доступ до конфіденційної інформації має бути обмеженим та контрольованим.
- Встановити процедури авторизації та ідентифікації користувачів, які мають право отримувати доступ до конфіденційної інформації.
- Визначити, які види інформації підпадають під захист та встановити заходи для забезпечення конфіденційності цих даних.
- Встановити процедури забезпечення захисту інформації від несанкціонованого доступу, використання та розголошення.
- Встановити процедури збереження інформації та регулярну перевірку на наявність вірусів, шкідливих програм, а також зберігати резервні копії даних.
- Встановити процедури утилізації конфіденційної інформації та надійного знищення даних після закінчення їх терміну зберігання.

Визначення відповідальних осіб та розподіл обов'язків є важливим елементом політики безпеки конфіденційної інформації на підприємстві. Це допомагає забезпечити ефективне управління ризиками та підвищити рівень захисту конфіденційної інформації.

Одним з основних відповідальних осіб є керівник підприємства або відповідний менеджер, який відповідає за розробку та впровадження політики безпеки конфіденційної інформації. Ця особа має визначати рівень конфіденційності даних та види інформації, що підпадають під захист, а також забезпечувати відповідний рівень захисту. До інших відповідальних осіб можуть відноситись керівники відділів, відповідальні за обробку та зберігання конфіденційної інформації, технічні спеціалісти, відповідальні за захист мережі та інфраструктури підприємства, та інші працівники, які мають доступ до конфіденційної інформації.

Розподіл обов'язків між відповідальними особами повинен бути чітко визначеним, зокрема стосовно забезпечення фізичного та логічного захисту інформації, здійснення процедур контролю доступу до інформації, забезпечення безпеки мережі та інфраструктури, а також забезпечення процедур повідомлення про можливі порушення безпеки даних та розслідування інцидентів.

Крім того, відповідальні особи повинні бути ознайомлені з політикою безпеки конфіденційної інформації та виконувати свої обов'язки відповідно до неї. Вони повинні знати, які дані вважаються конфіденційними, які процедури повинні бути виконані для захисту цих даних, як повідомляти про можливі порушення безпеки даних, і які наслідки можуть мати такі порушення. Розподіл обов'язків між відповідальними особами повинен бути чітко визначений, і кожна особа повинна мати ясний опис своїх обов'язків. Це допоможе забезпечити, що всі аспекти захисту конфіденційної інформації покриті та що відповідальні особи знають, які дії потрібно вживати у випадку порушення безпеки даних.

Обробка та зберігання конфіденційної інформації повинні відповідати вимогам законодавства та стандартам безпеки інформації. Основні вимоги щодо обробки та зберігання конфіденційної інформації можуть включати наступне: обмеження доступу до конфіденційної інформації; захист від несанкціонованого доступу, використання та розголошення; захист від вірусів та шкідливих програм; резервне копіювання даних; утилізація конфіденційної інформації; аудит доступу. Правила доступу до конфіденційної інформації повинні бути визначені у процедурах та політиках збереження конфіденційної інформації. Основні правила доступу до конфіденційної інформації на підприємстві повинні бути регулювані політикою безпеки і можуть варіюватися залежно від типу і обсягу конфіденційної інформації. Однак деякі загальні правила, які повинні дотримуватися співробітниками, що мають доступ до конфіденційної інформації, включають наступне:

- Аутентифікація: перед тим, як дати доступ до конфіденційної інформації, необхідно переконатися, що користувач, що звертається до інформації, є дійсною особою, яка має право на доступ.
- Авторизація: після того, як була здійснена аутентифікація, користувачеві повинно бути дозволено або заборонено доступ до конфіденційної інформації в залежності від його ролі і функцій на підприємстві.
- Захист даних: конфіденційна інформація повинна зберігатися в безпечному місці з обмеженим доступом, захищеному паролем і шифруванням.
- Оновлення паролів: співробітники, які мають доступ до конфіденційної інформації, повинні оновлювати свої паролі на регулярній основі.
- Моніторинг доступу: необхідно вести журнали доступу до конфіденційної інформації та регулярно перевіряти їх на виявлення підозрілих дій.
- Навчання співробітників: співробітники підприємства повинні бути навчені правилам та процедурам зберігання та обробки конфіденційної інформації, а також підвищувати свою обізнаність щодо потенційних загроз та ризиків безпеки даних.

Під час теоретичного та практичного аналізу політики безпеки конфіденційної інформації на підприємстві були отримані наступні основні висновки [2, 3]:

- Конфіденційна інформація є важливим активом будь-якого підприємства, який потребує захисту від потенційних загроз та ризиків.
- Основні загрози та ризики для конфіденційної інформації на підприємстві пов'язані з несанкціонованим доступом, крадіжкою, втратою, пошкодженням, витоком або неправомірним використанням даних.
- Для забезпечення захисту конфіденційної інформації необхідно розробити та впровадити на підприємстві політику безпеки, яка має включати такі елементи, як розподіл доступу до інформації, шифрування, аутентифікацію та ідентифікацію користувачів, контроль доступу до мережі та інтернет-ресурсів, а також правила використання електронної пошти та соціальних мереж.

- Для забезпечення ефективності політики безпеки конфіденційної інформації необхідно проводити регулярні навчання співробітників підприємства з питань безпеки інформації, а також проводити аудит системи безпеки та вживати необхідні заходи для її покращення.
- Для ефективної реалізації політики безпеки конфіденційної інформації на підприємстві необхідна підтримка керівництва, яка полягає в призначенні відповідальної особи, яка буде відповідати за виконання політики безпеки.

Процедури повідомлення про можливі порушення безпеки даних важливі для того, щоб оперативно виявляти, реагувати та запобігати потенційним загрозам безпеці даних в організації. Опис загальних процедур повідомлення про можливі порушення безпеки даних включає:

- Встановлення каналів повідомлення: в організації повинен бути встановлений канал повідомлення про можливі порушення безпеки даних, такий як електронна пошта, телефонна лінія підтримки або спеціальна онлайн-форма.
- Створення процедур повідомлення: необхідно розробити процедури, які визначають, які дані повинні бути включені в повідомлення про можливі порушення безпеки даних, як швидко повідомлення має бути зроблено та кому повідомлення повинно бути адресовано.
- Своєчасне повідомлення: персонал повинен бути навчений, як повідомляти про можливі порушення безпеки даних та негайно повідомляти відповідні служби.
- Аналіз порушення безпеки даних: служба безпеки повинна аналізувати отримані повідомлення та вживати відповідних заходів для запобігання подібних випадків у майбутньому.
- Інформування сторонніх осіб: у разі порушення безпеки даних, яке може вплинути на сторонніх осіб, необхідно повідомити їх про це та надати необхідну інформацію.
- Збереження записів: організація повинна зберігати записи про повідомлення про можливі порушення безпеки даних та вжиті заходи для їх усунення.

Ці процедури повинні бути регулярно оглядати та оновлювати з метою врахування змін у середовищі та загрозах безпеці даних. Перевірка і оновлення процедур повинні проводитись не рідше одного разу на рік або частіше, якщо з'являються нові загрози або змінюються умови використання даних. Крім того, процедури повідомлення про можливі порушення безпеки даних повинні бути чітко визначені та доступні всім користувачам і співробітникам організації. Всі співробітники повинні бути навчені, як діяти у випадку виявлення можливого порушення безпеки даних та куди повідомляти про це [1, 3].

Розслідування та оцінка ризиків пов'язаних з порушенням безпеки даних є важливим етапом у процесі збереження конфіденційної інформації. Це дозволяє визначити причину порушення та прийняти необхідні заходи для запобігання подібних ситуацій у майбутньому. При розслідуванні порушення безпеки даних слід виконувати такі кроки:

- Визначення масштабів порушення: необхідно визначити, яка кількість даних була скомпрометована, чи були викрадені фінансові дані, персональні дані або інші конфіденційні дані.
- Виявлення причини порушення: необхідно визначити, яким чином відбулося порушення. Чи була порушена процедура збереження даних, чи була допущена помилка працівником, чи була використана нещодавно виявлена вразливість системи безпеки.
- Встановлення наслідків порушення: необхідно визначити, які наслідки можуть бути для компанії та її клієнтів.
- Вжиття необхідних заходів для запобігання подібних ситуацій у майбутньому: на основі отриманих даних необхідно вжити необхідних заходів для запобігання подібних ситуацій у майбутньому.

Визначення способів ліквідації наслідків інциденту є важливою складовою політики безпеки конфіденційної інформації. Це означає, що організація повинна мати план дій у

випадку, якщо станеться інцидент з конфіденційною інформацією. План повинен бути регулярно переглядовий та оновлюваний, щоб відповідати змінам в організації та змінам у загрозах безпеки інформації та повинен включати: визначення виду інциденту та його серйозності; визначення осіб, які повинні бути повідомлені про інцидент, включаючи внутрішніх спеціалістів з безпеки і зовнішніх фахівців, якщо це необхідно; визначення кроків, які повинні бути прийняті для ліквідації інциденту; визначення термінів, у які необхідно повідомити про інцидент і провести його ліквідацію; визначення кроків, які повинні бути прийняті після ліквідації інциденту, щоб запобігти подібним інцидентам у майбутньому [3].

Для забезпечення ефективного захисту конфіденційної інформації на підприємстві можна рекомендувати наступні заходи: встановити політику безпеки конфіденційної інформації на підприємстві, яка має бути доступна для всіх співробітників і регулярно оновлюватися; ввести обов'язкову процедуру ознайомлення з політикою безпеки конфіденційної інформації для всіх нових співробітників і проводити її періодично для старих; встановити систему контролю доступу до конфіденційної інформації, яка повинна бути доступна лише обраним співробітникам, які мають потребу в такій інформації; забезпечити належний рівень захисту інформації на технічному рівні, зокрема шифруванням даних, встановленням брандмауерів та антивірусного програмного забезпечення; забезпечити охорону інформації на фізичному рівні, зокрема обмеженням доступу до приміщень, де зберігається конфіденційна інформація; забезпечити безпеку електронної пошти та соціальних мереж, встановивши обмеження на використання особистих аккаунтів для робочих цілей та шифруванням електронних листів; здійснювати регулярний моніторинг систем безпеки та аудит інформаційної безпеки на підприємстві; проводити навчання та тренінги для співробітників з питань інформаційної безпеки, включаючи засоби виявлення та запобігання соціальному інжинірингу.

Висновки. Для забезпечення безпеки конфіденційної інформації на підприємстві необхідно враховувати багато параметрів, таких як типи даних, їх обсяг, рівень доступу до інформації, рівень конфіденційності інформації , вимоги до зберігання та передачі даних, потенційні загрози та ризики, кваліфікацію персоналу, систему контролю доступу, відповідність нормативно-правовим вимогам тощо. Ці параметри повинні бути враховані у процесі розробки та впровадження системи захисту конфіденційної інформації на підприємстві. Дотримання відповідних параметрів дозволить забезпечити ефективний захист конфіденційної інформації на підприємстві та запобігти її витоку. Помітно, що забезпечення безпеки конфіденційної інформації на підприємстві є важливим елементом забезпечення безпеки в цілому, оскільки викриття такої інформації може призвести до значних матеріальних і моральних збитків для підприємства, його клієнтів та партнерів.

Список використаних джерел

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. Ортинський, В. Л. Економічна безпека підприємств, організацій та установ // Режим доступу: http://westudents.com.ua/glavy/16530-model-pobudovi-sistemi-nformatsyno-bezpeki.html (останнє звернення 12.04.2023р.).
3. Мохнюк А.М., Скорук О.В. Організація та управління інформаційною безпекою на підприємстві: конспект лекцій / Укладачі А.М. Мохнюк, О.В. Скорук. – Луцьк: ПП «Поліграфія», 2017. – 99 с.

Робота виконана під науковим керівництвом ст. викладача
КОСТЮК Ю.В.

МОДЕЛЬ ІНТЕРАКТИВНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ВІДЕОЗВ'ЯЗКУ

КРИКЛЯ В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови та функціонування моделі інтерактивної системи забезпечення відеозв'язку. Зазначено переваги впровадження систем відеозв'язку та розглянуто типові рішення щодо цього питання.

The article deals with the basic principles of construction and functioning of the model of the interactive video communication system. Let's note the advantages of implementing a video system and some typical solutions to this issue.

Актуальність. Система відеозв'язку є потужним інструментом в комунікаційному арсеналі будь-якої компанії. Відеозв'язок дозволяє істотно економити на відрядженнях співробітників і проводити ділові переговори, наради та семінари в режимі реального часу в стінах офісу. Сучасні рішення відеозв'язку, що володіють функціональністю систем високого класу і доступністю простого телефону, істотно розширюють можливості бізнес-комунікацій. Відеозв'язок дозволяє додати до засобів передачі даних і голосу обмін візуальною інформацією.

Метою статті є дослідження особливостей використання моделі інтерактивної системи забезпечення відеозв'язку та створення моделі класів.

Об'єктом дослідження є розробка інтерактивної системи забезпечення відеозв'язку.

Предмет дослідження - модель інтерактивної системи забезпечення відеозв'язку.

Аналіз попередніх досліджень. Дослідженням моделей інтерактивної системи забезпечення відеозв'язку присвячені праці вітчизняних та закордонних науковців: Вікторія Мізюк, Олександр Коваленко, Томас Могі та Аліна Румі.

Виклад основного матеріалу. Розробка програмного забезпечення для відеоконференцій знаходиться на піку розвитку. Причина – підвищений попит на засоби віддаленої співпраці. Людям потрібно продовжувати спілкуватися і працювати, а платформи, що забезпечують відеозв'язок стали, альтернативою спілкуванню в реальному житті.

Ринок програмного забезпечення для відеоконференцій розширюється шаленими темпами. У 2022 році його оцінювали в 25 мільярдів доларів, згідно з іноземними дослідженнями. До 2032 року прогнозується, що він досягне 95 мільярдів доларів.

Існує ряд переваг впровадження системи відеозв'язку, а саме: оптимізація бізнес-процесів, підвищення лояльності клієнтів та співробітників компаній, а також економія їх часу, підвищення ефективності бізнесу.

Відеозв'язок забезпечує:

- проведення презентацій та одночасну роботу з документами учасників;
- оперативність прийняття рішень в надзвичайних ситуаціях;
- ухвалення більш обгрунтованих рішень за рахунок залучення сторонніх експертів;
- швидке і ефективне розподілення ресурсів;
- ефект спілкування співрозмовників в одній кімнаті;
- дистанційне навчання.

Перш ніж почати процес розробки, Необхідно визначити тип майбутнього програмного забезпечення, дані наведені у таблиці 1.

Таблиця 1.

Типи платформ для відеоконференцій

Тип	Опис	Переваги	Недоліки
Платформи для відеоконференцій	Ці платформи забезпечують відеоконференції, функції обміну повідомленнями та записи екрану. Крім того, деякі з них мають зовнішню інтеграцію для керування зустрічами.	Ці платформи не потребують багато ресурсів, оскільки вони адаптуються до пристроїв користувачів і можливостей Інтернету. Зазвичай вони підтримують до 50 учасників конференції одночасно.	Вони можуть не відповідати корпоративним потребам деяких компаній, тому не є найкращим варіантом для віддаленої роботи.
Месенджери	Це такі месенджери, як Facebook, Telegram, WhatsApp і Facetime/iMessage від Apple, які мають функцію відеочату.	Окрім швидкого обміну повідомленнями, вони надають різні можливості для відеочатів. Деякі з месенджерів дозволяють поєднувати дзвінки зазвичай для 2-30 осіб. Деякі застосовують технології AR/VR, щоб дозволити користувачам використовувати спеціальні маски та анімацію.	Месенджери служать додатковим інструментом спілкування для віддалених співробітників, але не можуть замінити програмне забезпечення для відеоконференцій і онлайн-рішення для співпраці.
Програмне забезпечення для онлайн-спільної роботи	Відеоконференції – не єдиний варіант для компаній, яким потрібна віддалена співпраця. Вони вимагають належного підключення, яке покриває всі корпоративні потреби, що пропонує цей тип програмного забезпечення.	Онлайн-інструменти для співпраці пропонують розширені функції, включаючи обмін повідомленнями, відео- та аудіодзвінки, обмін документами, інтеграцію зовнішніх інструментів, таких як Jira та Google Calendar, і групові канали.	Багато рішень на ринку забезпечують ту саму функціональність, що й Microsoft Teams і G-Suite, але все-таки вони побудовані по-різному.

Продовження таблиці 1

Тип	Опис	Переваги	Недоліки
Розважальні платформи	Відеочати використовуються не тільки для роботи, але й для відпочинку. Розваги з друзями чи відеоігри стали стандартом для таких розважальних платформ, як Discord.	Ці платформи дозволяють грати в ігри, влаштовувати відеоконференції, транслювати улюблені ігри та проводити групові та приватні чати.	Ці платформи зазвичай не підходять для роботи, а лише для розваг.

Етапи створення програмного забезпечення для відеозв'язку:

1. Визначення вимог. По-перше, потрібно зрозуміти цільову аудиторію. По-друге, розглянути всі можливі варіанти використання платформи. Скласти їх список, щоб команда краще зрозуміла вимоги.
2. Формування команди. Цей пункт включає в себе пошук команди. Від кількості членів команди буде залежати швидкість розробки.
3. Розробка шаблону інтерфейсу. Дозволить оцінити потенційні випадки використання та зручність використання програмного забезпечення. Від інтерфейсу буде залежати успішність додатку, якщо інтерфейс буде незручний, то додатком не будуть користуватись.
4. Backend розробники. Розробники бекенда відповідають за побудову серверної логіки, впровадження відео та протоколів безпеки та підключення всіх необхідних API. Останній використовується для зовнішньої інтеграції програмного забезпечення, наприклад, платіжних шлюзів або хмарних сервісів.
5. Розробники інтерфейсу. Розробники інтерфейсу відповідальні за створення остаточного вигляду спеціального програмного забезпечення для відеоконференцій. Вони отримують усі проекти та макети та впроваджують їх як окремі робочі елементи на платформі.
6. Дизайнери. Вони розробляють макети та передають їх команді розробників інтерфейсу.
7. QA спеціалісти. Команда із забезпечення якості проводить ручне тестування програмного забезпечення. Якщо спеціалісти з контролю якості виявлять будь-які помилки, вони миттєво повідомлять розробників, щоб вони їх виправили. Контроль якості дозволяє уникнути критичних проблем до випуску.
8. Керівник проекту. Керівники проекту - це ключові люди. Вони також можуть надавати оновлення та пропозиції щодо покращення проекту.
9. DevOps. Інженери DevOps об'єднують всі елементи, які складають проект, налаштовують та розгортають програмного забезпечення. Вони знають специфіку програмістів, тестувальників, системних адміністраторів і допомагають спростити їх роботу.
10. Архітектор рішень. Архітектори рішень надають команді технічну документацію, стандарти та робочі процеси для створення єдиного продукту.
11. Технічний стек. Стек технологій для платформ може відрізнятися залежно від потреб і вимог. Інтерфейс: Adobe Photoshop, figma, HTML, CSS, JavaScript, Redux, React Native, Angular. Backend: c#, Java, Python, NodeJs. Бази даних: MySQL, PostgreSQL, MongoDB, RethinkDB. Розгортання програмного забезпечення: TeamCity, GitLab. Особливу увагу слід виділити захисту даних, шифруванню та відео протоколам.

Основні характеристики програмного забезпечення для відеоконференцій наведено на рис.1.

Рис. 1. Основні характеристики програмної платформи відеоконференції

Опис основних характеристик програмної платформи відеоконференції:

- Реєстрація. Дозволить користувачам реєструватися у внутрішній системі та отримувати ідентифікатор. Процес реєстрації повинен мати простий інтерфейс. Також можем підключити сторонні API, такі як Facebook Login і Google Sign-In, щоб забезпечити швидкий доступ до платформи.
- Обмін повідомленнями. Дозволить людям спілкуватися без відеодзвінків та обмінюватися текстовими повідомленнями під час дзвінка або навіть без нього.
- Профіль користувача. Є обов'язковими для платформ відеоконференцій. Вони містять основну інформацію, як-от ім'я, номер телефону, адресу електронної пошти, посаду та дату народження.
- Сповіщення. Ця функція використовується для сповіщення користувачів про майбутні події або вхідні дзвінки та повідомлення.
- Список контактів. Користувачі повинні мати можливість знаходити інших людей. Платформа має містити пошук за телефоном, іменем або електронною поштою. Можем застосувати додаткові API від Microsoft, Google або будь-якої внутрішньої системи для автоматизованої синхронізації контактів.
- Приватні дзвінки. Є ключовою функцією платформи. Повинен мати простий інтерфейс із аудіо- та відеодзвінками. Користувачі повинні мати доступ до вимкнення мікрофонів або камер і бачити імена один одного.
- Групові дзвінки. Подібний до попереднього з кількома новими функціями. По-перше, повинен бути власник, який може контролювати кімнату. Він може вимкнути звук учасників або дозволити ділитися екранами. У кімнаті також має бути список контактів для запрошення інших учасників.
- Управління даними. Це блок, який можна побачити на стартовому екрані, який вказує на майбутні дзвінки. Існує також можливість інтеграції із зовнішніми календарями для призначення зустрічей.
- Спільний доступ до екрана. Використовується для демонстрації вмісту вашого екрана. Спільний доступ до екрана стане в нагоді під час семінарів, вебінарів і

оглядів. Крім того, користувачі можуть вибрати програми, якими вони хочуть поділитися.

- Спеціальний фон. Дозволить вашим користувачам замінити свій фон на власні зображення. Ця функція може бути корисною для досягнення конфіденційності та маркетингових цілей, якщо ви плануєте спілкуватися з клієнтами

Для реалізації поданих вище характеристик необхідно створити відповідні класи, до яких належать:

1. Клас “користувач” має такі поля: ідентифікатор: “Snowflake"; ім’я: рядок; дискримінатор: рядок; аватар: рядок; бот: логічне значення; прапори: ціле число; тип преміуму: ціле число; багатофакторна автентифікація: логічне значення; локаль: рядок; перевірений: логічне значення; електронна пошта: рядок.
2. Клас “підключення” має такі поля: ідентифікатор: рядок; назва: рядок; тип: рядок; скасовано: логічне значення; інтеграції: масив.
3. Клас “сервер” має такі поля: ідентифікатор: “Snowflake"; ім’я: рядок; значок: рядок; власник: логічне значення; ідентифікатор власника: “Snowflake"; дозволи: ціле число; регіон: рядок; канали: масив; учасники: масив.
4. Клас “канал” має такі поля: ідентифікатор: “Snowflake"; тип: рядок; унікальний ідентифікатор: “Snowflake"; позиція: ціле число; дозвіл перезапису: масив; ім’я: рядок; тема: рядок; “nsfw”: логічне значення; останній ідентифікатор повідомлення: “Snowflake"; обмеження користувача: ціле число; обмеження швидкості на користувача: ціле число; одержувачі: масив; значок: рядок; ідентифікатор власника: : “Snowflake".
5. Клас “запросити” має такі поля: код: рядок; сервер: сервер; канал : канал; приблизна кількість присутніх: ціле число; приблизна кількість учасників: ціле число.
6. Клас “вкладення” має такі поля: ідентифікатор: “Snowflake”; ім’я фалу: рядок; розмір: ціле число; адреса веб-сторінки: рядок; проксі адреси веб-сторінки: рядок; висота: ціле число; ширина: ціле число.
7. Клас “повідомлення” має такі поля: ідентифікатор: “Snowflake”; ідентифікатор каналу: “Snowflake”; автор: “Snowflake”; контент: рядок; позначка часу: позначка часу; відредагована позначка часу: позначка часу; перетворення тексту в мовлення: логічне значення; вкладення: масив; вбудовані: масив; реакції: масив; згадати всіх: логічне значення; згадки: масив; ролі згадок: масив; закріпити: логічне значення; тип: ціле число.
8. Клас “вбудова” має такі поля: ідентифікатор: “Snowflake”; ім’я файлу: рядок; розмір: ціле число; адреса веб-сторінки: рядок; проксі адреси веб-сторінки: рядок; висота: ціле число; ширина: ціле число.
9. Клас “реакція” має такі поля: кількість: ціле число; я: логічне значення.
10. Клас “емодзі” має такі поля: ідентифікатор: “Snowflake”; ім’я: рядок; ролі: масив; вимагає двокрапки: логічне значення; керований: логічне значення; анімований: логічне значення.

Модель класів інтерактивної системи забезпечення відеозв’язку подано на рис. 2

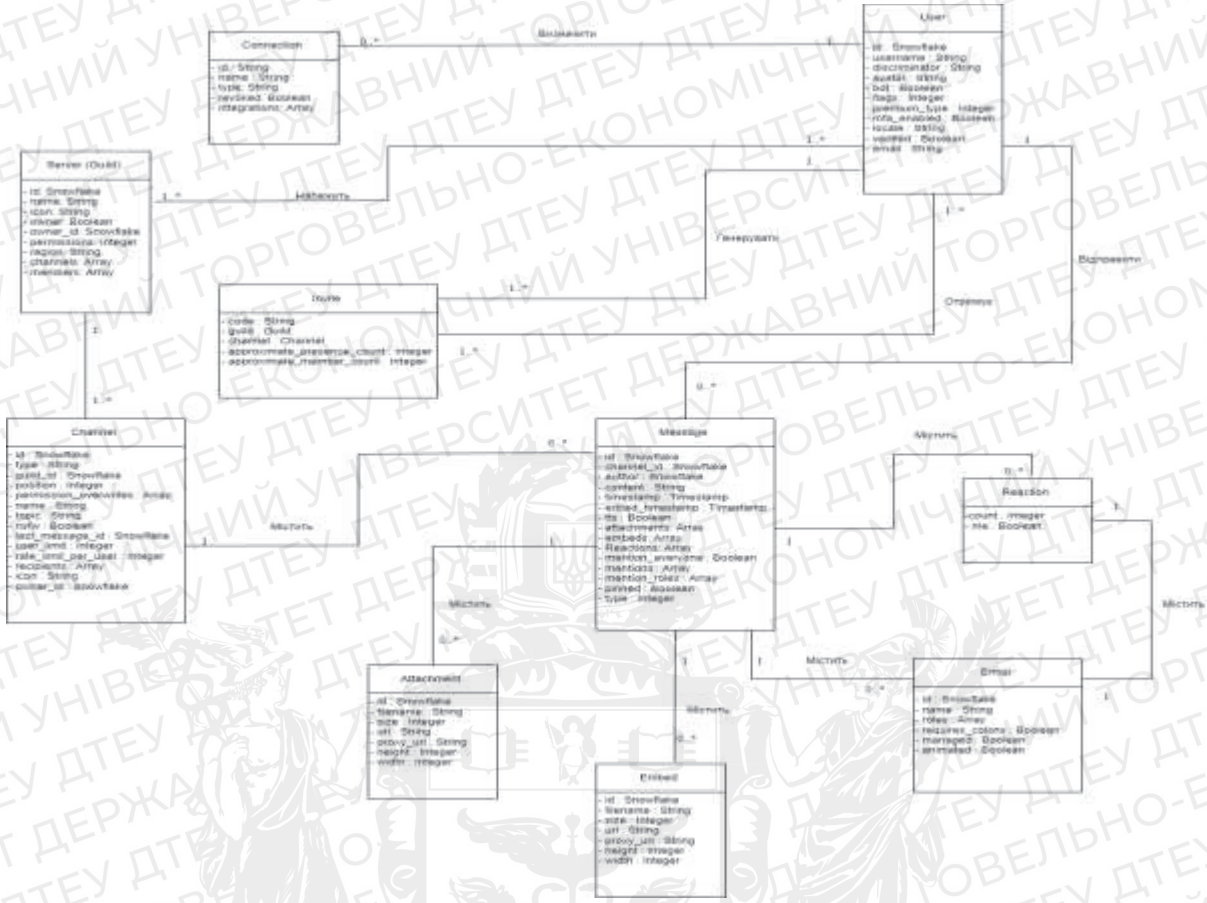


Рис. 2. Модель класів інтерактивної системи забезпечення відеозв'язку

Висновки. Отже, на сьогоднішній день системи забезпечення відеозв'язку – найпопулярніший вид бізнес-зв'язку. Система складається зі спеціального обладнання та програмного забезпечення, створює якісний відео та аудіо контакт між віддаленими учасниками. Те, для чого зовсім недавно потрібно було оформляти тижневе відрядження та летіти через океан, за допомогою системи відеозв'язку можна організувати за лічені хвилини. Саме тому розробка нових моделей забезпечення відеозв'язку є такою необхідною справою у сучасному світі. Було створено модель класів інтерактивної системи забезпечення відеозв'язку, яка є важливою в реалізації основних характеристик платформ відеозв'язку.

Список використаних джерел

1. 31 програмне забезпечення для відеоконференцій на 2023 рік \\ Режим доступу: https://www.ringcentral.com/us/en/blog/video-conferencing-software/ (останнє звернення 04.04.2023р.)
2. Посібник із інтерактивної відеостатистики на 2022 рік \\ Режим доступу: https://tomislavhorvat.com/interactive-video-statistics/ (останнє звернення 04.04.2023р.)
3. Що таке інтерактивне відео? \\ Режим доступу: https://www.wyzowl.com/what-is-interactive-video/ (останнє звернення 04.04.2023р.)

Робота виконана під науковим керівництвом к.т.н., доцента
РЗАЄВОЇ С.Л.

НАВІГАЦІЙНІ СИСТЕМИ ТОГОВЕЛЬНО РОЗВАЖАЛЬНИХ ЦЕНТРІВ ТА МОЖЛИВІСТЬ ЇХ ПОЄДНАННЯ З ТЕХНОЛОГІЯМИ ДОПОВЛЕНОЇ РЕАЛЬНОСТІ

КУБАТІН О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови та функціонування навігаційної системи у Торгівельно розважальних центрах. Зазначено переваги застосування нових технологій, таких як доповнена реальність. Розглянуто як зразок типової навігаційної системи торговельно розважального центру додаток "River Mall".

The article considers the basic principles of construction and operation of the information and management system at retail enterprises. The advantages of using software products in the automation of a commercial enterprise are indicated. The "River Mall" application is considered as an example of a typical navigation system of a shopping and entertainment center.

Актуальність. Сфера людської діяльності торгівля, є однією з ключових для економічного розвитку регіону та країни в цілому. Саме це зумовлює швидкий розвиток інтеграції інформаційних технологій у процес економічної взаємодії між компаніями та остаточним споживачем. Для забезпечення ефективності економіки держави механізми взаємодії виробництва (пропозиції) і споживання (попиту) удосконалюються щороку, а інтеграція інформаційних технологій дедалі стає більш вагомою.

Ми можемо спостерігати як роздрібні торговельні мережі, з власною системою збуту товарів об'єднуються в великі торговельні центри, сумісно використовуючи спільну базу покупців. Така кооперація зумовлює більший попит та змогу привертати ще більше клієнтів до своїх товарів.

Зазвичай жоден магазин не в змозі викласти на прилавки весь асортимент товарів, які є в наявності, або покрити весь спектр потреб покупця. Також потрібно враховувати що кожний магазин має свою цільову аудиторію, і саме таке розташування надає змогу створити центри у яких люди можуть знайти майже всі групи товарів на будь-який смак та гаманець, та мають змогу відпочити.

Всі ці фактори зумовлюють ще більше зростання розмірів торговельно-розважальних центрів та обсяг магазинів які до нього входять. Кожен торговельний центр має свою специфічну архітектурну особливість і дедалі більше стає складніше орієнтуватись у самому центрі, особливо якщо ти маєш на меті знайти магазин конкретного виробника або групи товарів. Звичайно кожен торговельно-розважальний центр має інформаційні столи та електронні вказівники. Але не завжди ці засоби можуть дати людині вичерпне уявлення та інформацію щодо його запиту.

Через це ми дедалі більше можемо спостерігати інтеграцію різних технологій, наприклад таких як використання QR-коду, завдяки якому в комбінації зі смартфоном ми можемо отримати швидкий доступ до відповідного джерела інформації та значно спростити час пошуку. Також один з прикладом такого перетворення є інтеграція навігаційних систем у додатки, які повинні допомогти людині швидше робити пошуки товарів, знаходити потрібні бренди або магазини, та в висновок збільшити швидкість та обсяг продажу до того часу, як людина виснажиться і буде змушена покинути торговельно-розважальний центр.

Метою статті є дослідження особливостей використання навігаційних систем у торговельно-розважальних центрах з метою підвищення ефективності їх функціонування.

Об'єктом дослідження є розробка навігаційної системи торговельно-розважального центру з використанням технології доповненої реальності.

Предмет дослідження – навігаційна система.

Аналіз попередніх досліджень. Дослідженню навігаційних систем, визначенню структури, основних характерних рис присвячені праці вітчизняних та закордонних науковців: Н.О. Голошубова, О.О. Кавун, В.М. Торопков, Бозуленко О. Я..

Виклад основного матеріалу. В економічній системі торгівля посідає особливе місце. Вона забезпечує товарно-грошовий обмін у формі купівлі-продажу у величезних розмірах і відіграє суттєву роль у реалізації соціальної політики, стабілізації реального сектору економіки, розширенні міжгалузевого та міжрегіонального обміну.

Торгівля як галузь господарської діяльності має розгорнуту мережу оптових і роздрібних підприємств, забезпечує зберігання, транспортування і реалізацію товарної продукції предметів споживання. Оскільки більшість предметів особистого споживання проходить через торгівлю, то рівень її розвитку характеризує обсяг і структуру споживання. Торгівля інформує і впроваджує в споживання нові товари, виробництво яких тільки починається, які для споживача є ще невідомими або незвичними. Таким чином, розвиток торгівлі, будучи обумовленим рівнем і темпами розвитку виробництва товарів, в свою чергу, здійснює вплив на промисловість, сільське господарство з одного боку, і на споживання людей – з іншого. Важливе значення торгівлі в тому, що вона сприяє особистій матеріальній зацікавленості людей у підвищенні продуктивності праці, в збільшенні виробництва, в повнішому задоволенні потреб. Торгівля як сфера національної економіки за своєю формою і змістом належить до складних соціально-економічних систем і виконує життєво важливі завдання і функції економічних відносин [1, с. 10].

Саме це і зумовлює її постійний розвиток, видозмінення та перетворення, пошуки та вдосконалення методів покращення ефективності взаємодії виробника товарів та покупців. Одним із таких методів можна зазначити сучасні навігаційні системи, їх появу як явище та розвиток як у сучасних торговельних центрах, так і в інших соціально-економічних сферах життєдіяльності.

Навігаційні системи торговельно-розважальних центрів (надалі ТРЦ) є невід'ємною частиною сучасного міста. Вони дозволяють відвідувачам швидко знайти потрібний магазин або розважальний заклад, а також допомагають орієнтуватись на території ТРЦ. Зараз у використанні є безліч різних навігаційних систем, від простих табличок з написами до складних електронних систем з підключенням до смартфонів.

Однак, з появою технологій доповненої реальності (AR), навігаційні системи стали ще більш ефективними та зручними для відвідувачів ТРЦ. AR дозволяє накладати віртуальну інформацію на реальний світ, що забезпечує користувачам додаткову інформацію про те, де знаходиться певне місце, яку має розміщення та як до нього найлегше дістатись.

Одним з прикладів використання AR в навігаційних системах ТРЦ є додаток (наприклад QR Reader), що дозволяє відвідувачам сканувати QR-коди пересуваючись по самому ТРЦ та отримувати інформацію про певне місце, наприклад, меню ресторану, графік роботи магазину або акційні пропозиції. Такий додаток може бути зручним тим, що дозволяє зекономити час та знайти необхідну інформацію з одного джерела. Наразі на більшості смартфонів достатньо просто навести камеру на QR-код і посилання одразу з’явиться на самому екрані що значно спрощує процес зчитування інформації. Але назвати таке використання AR повноцінним є дуже складним, адже можливості доповненої реальності є значно ширшими ніж можливість швидко зчитувати посилання на різні джерела.

Однією з проблем використання таких методів навігації є певна не упорядкованість та не систематизація інформації яку можна знайти в самому Торговельно-розважальному центрі – певні магазини та ресторани можуть використовувати такі можливості, інші не бачать в цьому ніякої потреби.

Віртуальна реальність досить популярна і в ігровій та освітній сфері, проте використовується і в культурі. Один із найвідоміших музеїв культури і мистецтва у віртуальній реальності — Artheon. У ньому зібрані тисячі оцифрованих творів мистецтва з

колекцій світових музеїв. У додатку можна розглядати експонати з будь-якого боку, створювати свою експозицію та головне — у будь-який час [2].

Цю ідею можна використати для віртуального перегляду товарів з усіх боків без фізичної наявності у самому магазині. Також дуже зручно можна переглянути певний товар у специфічному кольорі, адже не завжди можливо покупцю привезти один товар у десятках, або навіть сотнях варіаціях – наприклад меблева продукція. Через свої габарити це значно спростить і навантаження на торговельну площу, і водночас розширить можливості для передпоказу товару.

Наразі немає прикладів типової імплементації, але розробка даного рішення та його впровадження у торговельний процес вже відбувається. Наприклад, незабаром клієнти інтернет-магазину epicentrk.ua матимуть змогу використати доповнену реальність для придбання меблів. Ця технологія дозволить максимально реалістично візуалізувати товар та показати, як він виглядатиме у конкретній кімнаті та інтер'єрі.

Зокрема, за допомогою функції доповненої реальності покупці зможуть через камеру свого смартфона або планшета подивитися, як виглядатимуть меблі в їхній кімнаті. Щоб скористатися цією функцією, клієнту компанії не потрібно буде встановлювати жодне програмне забезпечення — достатньо лише просканувати QR-код.

Неперервне масштабування корпоративних торгівельних мереж зумовлює постійний пошук для ще більш потужного розвитку, чим по суті й виявляється поява брендованих ТРЦ. Ефект масштабу у корпоративних торговельних мережах виявляє передусім економічний характер наслідків (збільшення кількості магазинів у складі об'єднання відображається на темпах зростання фінансово-економічних показників і передбачає отримання очікуваного рівня прибутковості діяльності) та психологічний характер (збільшення кількості магазинів під однією торговельною маркою забезпечує підвищення рівня запам'ятовування, завоювання та утримання прихильності споживачів) [3, с.84].

Типову сучасну навігаційну систему торговельно-розважального центру можна розглянути на прикладі додатка 'River Mall'.Такі додатки дедалі стають популярніші у сьогодення. Цей додаток розроблений для розв'язання питань по типу паркування, пошуку одягу відповідно до бренду або іншими характеристиками, та є корисним тільки щодо конкретного торговельно-розважального центру. Всі функціональні модулі об'єднує одне завдання – покращити навігацію у торговельному центрі та надати покупцю максимальний комфорт задля покращення товарообігу між виробником та покупцем (Рис.1).

Рис. 1. Інтерфейс додатку "River Mall"

Карта центру частково інтегрована в більш звичну карту міста, якщо розглянути перший поверх, та має навіть певні особливості територіальні для більшого уявлення простору навколо. Ця ж сама система працює і щодо парувальних місць.

Як ми можемо побачити на малюнку покупець може побачити реальну карту торгового центру, перевірити будь-який поверх та зробити сортування за тими товарами в яких він потребує у цей час. Відповідно до запиту додаток надає певний магазин або магазини, після чого стає можливим прокласти маршрут (Рис.2).

Рис. 2. Навігація у додатку "River Mall"

При виборі певного магазину додаток прокладає маршрут та надає підказки щодо пересування, використовуючи звичайну GPS навігацію в поєднанні з іншими технологіями для покращеного орієнтування у просторі. Відправну локацію можна задавати самостійно не використовуючи автознаходження пристрою (Рис.3).

Наразі AR в цьому додатку використовується тільки як можливість просканувати свій паркувальний талон для його подальшої сплати. Можливість більшої інтеграції з AR надала б змогу зробити навігацію більш інтерактивною, інформативною, та логічною. Пересуваючись по території використовуючи AR додаток можна як включити до функціонала персонального помічника який саме на екрані звичайного смартфону надавав вказівки щодо пересування або інформацію щодо магазинів які також можна перевірити щодо наявності групи товарів або розвал які викликали інтерес. Навіть більше, в цю навігацію можна інтегрувати будь-що, від звичайної інформації щодо бренду до популярних товарів тощо [4].

Рис. 3. Маршрут у додатку "River Mall"

Іншим прикладом є використання AR-окулярів для навігації в ТРЦ. Окуляри можуть накладати відображення на реальний світ, що дозволяє відвідувачам ТРЦ дізнатись більше про місце, на якому вони знаходяться, а також про певні пропозиції, акції та події, які відбуваються в магазинах та розважальних закладах. Такий підхід дозволяє зробити навігацію більш інтерактивною та зручною для відвідувачів ТРЦ, а інтеграцію AR ще більш реалістичною. Але наразі практичне використання такого методу є дуже складним, адже AR окуляри є мало популяризовані, а розробка програмного забезпечення може вийти значно дорожче ніж реальна ефективність.

В перспективі, AR може бути використана для створення віртуальної мапи ТРЦ. Наприклад, відвідувач може встановити додаток на свій смартфон та сканувати коди, розташовані на стінах ТРЦ, щоб побачити віртуальну мапу. Такий підхід дозволяє відвідувачам швидко знайти потрібне місце та дістатись до нього. Крім того, такий додаток має багато інших можливостей, наприклад окрім QR-кодів можна додати можливість зчитувати логотипи брендів та видавати інформацію щодо них прямо на смартфоні.

Ще одним важливим аспектом є можливість поєднання навігаційних систем з іншими технологіями, такими як інтернет-маркетинг та інтелектуальний аналіз даних. Наприклад, на основі даних, зібраних навігаційною системою, можна створити персоналізовані рекламні пропозиції для відвідувачів ТРЦ, що дозволить ефективніше залучати клієнтів до магазинів та розважальних закладів.

Навігаційні системи ТРЦ є невід'ємною частиною сучасного міста та можуть бути дуже ефективними з використанням технологій доповненої реальності. AR дозволяє створювати інтерактивні та зручні для відвідувачів ТРЦ навігаційні системи, що покращує їх досвід відвідування ТРЦ та збільшує ефективність маркетингових кампаній магазинів та розважальних закладів.

Однак, при використанні AR для навігації у ТРЦ необхідно враховувати певні технічні та етичні аспекти. Наприклад, необхідно забезпечити належний рівень захисту персональних даних відвідувачів, які використовують AR-додатки. Крім того, додатки повинні бути доступні для користувачів з різними рівнями технічної грамотності, що може вимагати розробки додаткових інтерфейсів та інструкцій користувача.

В заключення, можна сказати, що навігаційні системи ТРЦ з використанням технологій доповненої реальності мають великий потенціал для покращення якісного рівня обслуговування відвідувачів та підвищення ефективності маркетингу магазинів та розважальних закладів. Проте, враховуючи певні технічні та етичні аспекти, необхідно забезпечувати належну реалізацію цих систем та збалансований підхід до використання нових технологій.

Ще однією можливістю для покращення навігації в ТРЦ є використання системи "інтелектуальної" карти. Ця система полягає у використанні датчиків, що відстежують рух відвідувачів та показують їм найближчі магазини, ресторани та інші заклади в ТРЦ. Крім того, система може відображати інформацію про акції, знижки та інші спеціальні пропозиції для відвідувачів.

Але однією із особливостей сучасних навігаційних систем ТРЦ є те, що усі доступні можливості AR використовуються лише частково і не усіма участниками торговельного процесу.

Висновки. Таким чином, можна зробити висновок, що використання навігаційних систем та технологій доповненої реальності у торговельно-розважальних центрах є важливим інструментом для залучення та задоволення клієнтів, покращення їх досвіду покупок та збільшення прибутків компаній-операторів цих центрів. Ці технології також можуть бути використані для збору даних про поведінку та інтереси клієнтів, що дозволить покращити ефективність маркетингових кампаній та рекламних пропозицій.

Проте, необхідно пам'ятати про те, що використання технологій повинне бути збалансованим та не надто інтенсивним, оскільки це може негативно позначитися на досвіді покупок та безпеці клієнтів. Також, необхідно забезпечити високу якість технічної підтримки та забезпечення безпеки даних, щоб запобігти можливим технічним проблемам та злому систем.

Впровадження навігаційних систем та технологій доповненої реальності у торговельно-розважальних центрах є перспективною та важливою тенденцією розвитку цієї галузі, яка дозволяє покращити досвід покупок та залучити нових клієнтів. Проте, необхідно забезпечити правильний баланс між використанням технологій та потребами клієнтів, щоб забезпечити позитивний ефект від їх впровадження.

У підсумку, можна стверджувати, що навігаційні системи тоговельно-розважальних центрів мають великий потенціал для покращення ефективності та якості обслуговування відвідувачів. Технології доповненої реальності та "інтелектуальної" карти можуть допомогти вирішити багато проблем, пов'язаних з навігацією та пошуком потрібних магазинів та закладів. Однак, при розробці та впровадженні таких систем необхідно враховувати певні технічні та етичні аспекти, щоб забезпечити належний рівень захисту персональних даних та забезпечити доступність та зручність для всіх відвідувачів.

Список використаних джерел

27. Бозуленко О. Я., Організація торгівлі : навчальний посібник [для студ. вищ. навч. закл.]. Чернівці : ЧТЕІ КНТЕУ, 2021. 240 с
28. Вигаданий світ: українські проєкти у VR та AR від 04 Липня 2020 \\ Режим доступу: https://creativeeurope.in.ua/posts/ukrainian-projects-vr-ar
29. Підприємницькі мережі в торгівлі: монографія / [Н.О. Голошубова, О.О. Кавун, В.М. Торопков та ін.]; за заг. ред. Н.О. Голошубової. – К.: Київ. нац. торг.-екон. ун-т, 2014. – 344 с
30. Додаток ‘River Mall’ \\ режим доступу: https://apps.apple.com/ua/app/river-mall/id1498766659?l=ua

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д.О.

CRM СИСТЕМИ ЯК ОБОВ'ЯЗКОВА СКЛАДОВА ОПТИМІЗАЦІЇ УСПІШНОГО БІЗНЕСУ В ІНДУСТРІЇ КРАСИ

КУКЛА В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У цій статті розглянуто актуальність використання системи управління взаємовідносинами з клієнтами у салонах краси, зазначено переваги застосування програмних продуктів в процесі автоматизації надання послуг, а також наведено опис основних функцій CRM систем.

In this article examined the relevance of using a customer relationship management system in beauty salons. In addition, we indicated the advantages of using software products in service providing automation, as well as we made a description of the main CRMsystems functions.

Актуальність. Індустрія краси в Україні – це стрімко зростаюча галузь економіки. За даними дослідницької компанії Euromonitor International, обсяг ринку краси в Україні в 2020 році становив більше 2,7 мільярдів доларів США. Ця галузь займає важливе місце в економіці країни, адже забезпечує працевлаштування більше ніж 300 тисяч осіб, включаючи косметологів, майстрів манікюру та педикюру, перукарів та інших спеціалістів. [1] Відсоток ВВП, який генерується галуззю, також є суттєвим. Згідно з даними Міністерства розвитку економіки, торгівлі та сільського господарства України, у 2020 році внесок індустрії краси в ВВП склав близько 1,5%. [2]

Варто зазначити, що CRM (Customer Relationship Management) системи є необхідним інструментом для будь-якого бізнесу, який забезпечує зберігання та управління інформацією про клієнтів. У сегменті індустрії краси актуальність CRM систем також дуже висока. Саме тут залежність від клієнтів є найвищою, оскільки це визначає успіх або невдачу у веденні бізнесу.

За даними статистики, 70% клієнтів салонів краси повертаються за послугами, якщо їх задоволеність першим візитом перевищує 90%. Тому зберігання та аналіз інформації про клієнтів є вкрай важливим, адже допомагає визначити їх потреби і бажання.

Крім того, CRM система дозволяє також автоматизувати процеси запису на послуги, створення розкладу роботи майстрів, розсилку повідомлень про акції та знижки. Як наслідок - мінімізується ймовірність внесення помилкової інформації про клієнтів, а збереження цієї інформації стає більш організованим та ефективним.

Загалом впровадження CRM системи допомагає салонам краси удосконалювати обслуговування клієнтів та збільшувати їх задоволеність. Також це сприяє збільшенню доходів та покращенню репутації бізнесу. [3]

Відповідно, розробка та впровадження CRM систем у салонах краси є важливим етапом в розвитку галузі індустрії краси. Їх використання підвищує конкурентоспроможність бізнесу та робить його більш зручним для клієнтів.

Метою статті є дослідження особливостей використання CRM систем у салонах краси для підвищення продуктивності їх функціонування.

Об'єктом дослідження є розробка компоненти CRM системи салону краси.

Предмет дослідження – CRM система.

Аналіз попередніх досліджень. Дослідження та аналіз CRM систем салонів краси проводять як відомі міжнародні компанії, так і незалежні науковці. Наприклад, компанія "Salesforce", яка є однією з провідних світових розробників CRM систем, має багато публікацій та наукових досліджень на тему використання їхньої системи в салонах краси.

Також є багато науковців, які займаються дослідженням CRM систем в салонах краси. Наприклад, відомий американський науковець Марк Гроув займається дослідженням CRM систем в салонах краси та публікує свої результати у наукових журналах.

У вітчизняному контексті є декілька науковців, які займаються дослідженням CRM систем в салонах краси. Так, М. Самойленко та І. Горбаченко з Харківського національного університету імені В. Н. Каразіна досліджували використання CRM систем в салонах краси України та розробляли рекомендації для їхнього впровадження.

Виклад основного матеріалу. CRM системи в наш час стають незамінними інструментами управління клієнтською базою та автоматизації бізнес-процесів. Ці системи стали особливо популярними в останні роки завдяки збільшенню конкуренції на ринку та необхідності в удосконаленні процесів взаємодії з клієнтами. У сучасному інформаційному світі це невід'ємна частина дієвого управління бізнесом. На фоні пандемії COVID-19, яка значно вплинула на галузь краси, автоматизація бізнес-процесів стала необхідністю для більшості салонів краси.

CRM (управління взаємовідносинами з клієнтами) - це поняття, що включає концепції, які компанії використовують для управління взаємовідносинами зі споживачами, включаючи збір, зберігання та аналіз інформації про споживачів, постачальників, партнерів та їх взаємодію. (Рис. 1).

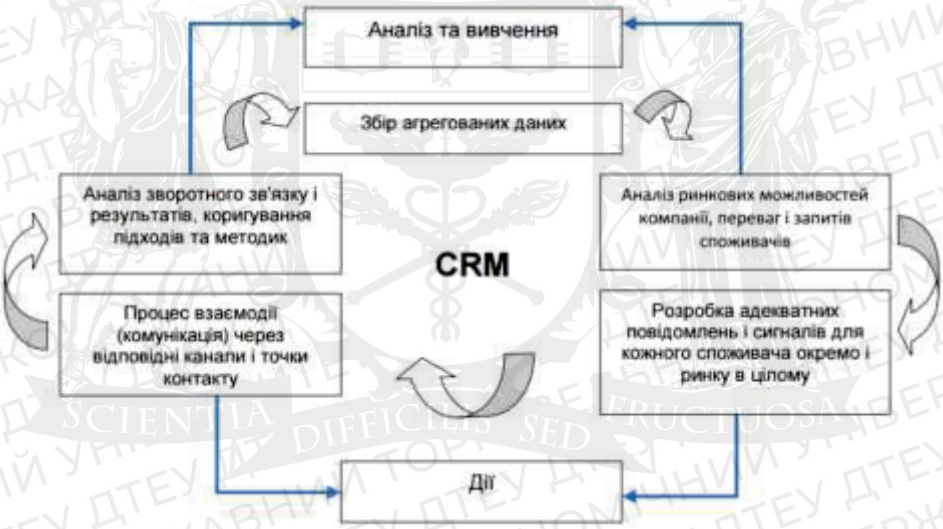


Рис.1. Цикл інформаційних процесів в CRM розроблено автором за джерелом [4]

Сучасна CRM-концепція спрямована на вивчення ринку та конкретних потреб клієнтів. Існують три підходи до автоматизації управління взаємовідносинами з клієнтами, які можуть бути реалізовані окремо. CRM – концепція:

- оперативний підхід – автоматизація споживчих бізнес-процесів для допомоги персоналу з роботи з клієнтами
- аналітичний підхід – аналіз інформації про споживачів з різноманітними цілями
- клієнтський підхід – програма взаємодії зі споживачами без участі персоналу з роботи з клієнтами. З розвитком інноваційних технологій CRM стала функціонувати у віртуальному просторі, поєднавшись з глобальною мережею Інтернет та здобула ряд інструментів, одним з яких є e-CRM-система. Стандартна офлайн CRM-система - це набір додатків, функцій та інструментів, пов'язаних єдиною бізнес-логікою та інтегрованих в єдину корпоративну інформаційну середу компанії. E-CRM-система додає до типових функцій такого класу систем можливості індивідуальної взаємодії з клієнтами у віртуальному просторі. Тобто, вона привносить переваги та динаміку взаємодії з клієнтами за допомогою електронних інструментів

Основна ідея e-CRM-системи полягає у тому, що вона дає можливість підприємствам ефективно керувати взаємодією з клієнтами, зокрема, за допомогою електронної пошти, чат-ботів, месенджерів та інших онлайн інструментів.

До переваг використання E-CRM-системи можна віднести:

- зниження витрат на обслуговування клієнтів. E-CRM-система дозволяє підприємствам знизити витрати на обслуговування клієнтів, так як автоматизує багато процесів, що раніше виконувались вручну;
- підвищення рівня задоволеності клієнтів. За допомогою e-CRM-системи підприємства можуть забезпечити швидкий відгук на запити клієнтів, знизити час очікування відповіді на запит та забезпечити більш індивідуальний підхід до кожного клієнта;
- підвищення ефективності маркетингових кампаній. E-CRM-система допомагає збирати та аналізувати дані про клієнтів, що допомагає підприємствам створювати більш дієві маркетингові кампанії та пропонувати індивідуальні пропозиції для кожного клієнта;
- підвищення конкурентоспроможності. Використання e-CRM-системи на підприємствах робить їх більш конкурентоспроможними на ринку, забезпечуючи якісне обслуговування клієнтів та знижуючи витрати на обслуговування;
- підвищення продажів. E-CRM-система може допомогти підприємствам створити персоналізовану рекламну кампанію для певної групи клієнтів, що збільшить ймовірність їхньої участі в акції та покупки товару.

Збір даних про клієнтів з допомогою e-CRM-системи включає в себе дані про історію замовлень, переглядів товарів, поведінку на сайті та в інших каналах взаємодії з підприємством. Аналізуючи ці дані, менеджери підприємств підвищують результативність спілкування з клієнтами, отримують краще розуміння їхніх потреб для подальшої розробки індивідуальних пропозицій.

Важливим фактором впровадження CRM системи є правильний вибір програмного забезпечення, яке відповідатиме потребам конкретного салону краси. За різними дослідженнями, на сьогоднішній день на ринку представлено багато різних CRM систем для салонів краси, серед яких можна виділити Beauty Pro, CleverBox, YCLIENTS, BloknotApp та інші.

Розглянемо деякі приклади успішного впровадження CRM систем на підприємствах індустрії краси в Україні.

Приміром, мережа салонів ZEBRA є найбільшою в місті Дніпро. Перший салон був відкритий ще сімнадцять років тому, зараз мережа налічує п’ять салонів краси, розміщених у великих торгових центрах. Персонал салонів сумарно складає понад сто майстрів, а у мережі щомісяця обслуговується понад п’ять тисяч клієнтів.

Керувати бізнесом такого масштабу в ручному режимі практично неможливо, тому три роки тому мережа салонів ZEBRA автоматизувала свою роботу за допомогою сервісу для управління салонами краси та клініками Beauty Pro CRM.

Найперше, що треба було виправити – це неефективне управління клієнтською базою даних. Клієнти звикли звертатися в різні салони мережі, але не мали єдиного обліку своїх послуг та знижок. Це призводило до невдоволеності клієнтів та як результат зниження обсягів надання послуг. Для вирішення цієї проблеми за допомогою Beauty Pro було створено єдину базу даних клієнтів, у якій зберігалися дані про послуги, знижки та історію відвідувань. Завдяки цьому зараз клієнти отримують персоналізований підхід до своїх потреб.

Управління запасами інвентарю було іншою проблемою, яку вирішили за допомогою Beauty Pro CRM. Раніше співробітники салону самостійно вводили дані про продаж і замовлення товарів на склад мережі. Це вимагало багато часу і зусиль, а також часто призводило до помилок в обліку запасів. Beauty Pro CRM дозволила автоматизувати цей процес, введення даних про продажі та замовлення тепер здійснюється в режимі онлайн і безпосередньо з касового апарату. Інформація про продажі, запаси та замовлення постійно оновлюється і доступна для аналізу в режимі реального часу. Менеджери взмозі вчасно приймати рішення про замовлення товарів, враховуючи попит клієнтів та стан запасів.

Крім того, Beauty Pro CRM дає можливість плідно вести маркетингові кампанії, що є важливим елементом в успішному функціонуванні будь-якого салону краси. Завдяки системі Beauty Pro менеджери можуть створювати та відстежувати маркетингові кампанії, спрямовані на залучення нових клієнтів та збереження вже існуючих. За допомогою даних клієнтів салонів, менеджери можуть створювати персоналізовані пропозиції та акції, які будуть цікаві для кожного клієнта окремо.

Також система Beauty Pro CRM дозволяє вести ефективний контроль за роботою персоналу. За допомогою системи менеджери можуть відстежувати роботу кожного співробітника, контролювати та аналізувати його особистий результат. (Рис. 2).

Beauty Pro		
розроблено для: салонів краси, spa-салонів, wellnes студій, нігтьових студій, барбершопів, косметологічних клінік, навчальних центрів, приватних майстрів	використовується для: роботи з клієнтами, ведення журналу запису, онлайн запису, роботи з товарами, управління співробітниками, ведення звітів та статистики	показники в цифрах: 7 років на ринку, автоматизовано 3000 салонів краси та клінік, використовується в 16 країнах світу, перекладено на 9 мов

Рис.2. Основні напрями використання CRM Beauty Pro

Отже, Beauty Pro CRM є потужним інструментом для автоматизації бізнес-процесів салонів краси. Ця система дозволяє ефективно вести бізнес, забезпечує кращу взаємодію з клієнтами та забезпечує стабільну роботу підприємств. Крім того, Beauty Pro є надійним інструментом для управління бізнесом в умовах пандемії COVID-19, коли салони краси мусять дотримуватись соціальної дистанції та інших заходів безпеки.

Застосування Beauty Pro CRM у салоні краси може мати значний вплив на розвиток і популяризацію салону серед потенційних клієнтів. Дізнавшись більше про своїх клієнтів, власники салону можуть персоналізувати свої послуги та пропозиції, оптимізувати використання ресурсів та забезпечити зростання прибутку. [5]

Іншим провідним розробником CRM систем є компанія CleverBox. Це українська компанія, яка спеціалізується на розробці та впровадженні CRM систем. Компанія відрізняється високою якістю своїх продуктів та високим рівнем сервісу.

Компанія CleverBox розробила спеціальні інструменти для ведення дієвого діалогу з клієнтами. Так, одним із цих інструментів є автоматична розсилка повідомлень. Ця функція встановлює автоматичну відправку повідомлень клієнтам в певних ситуаціях, наприклад, при підтвердженні запису до майстра або при нагадуванні про поточний стан замовлення. Також зазначена система веде облік дзвінків та електронних листів клієнтів, контролює якість комунікації для вчасного реагування на запити клієнтів.

Окрім автоматизації комунікації з клієнтами, CleverBox CRM має інші важливі функції. Наприклад, з використанням системи можливе планування роботи кол-центру та контроль за якістю обслуговування клієнтів. Примітно, що компанія CleverBox CRM забезпечує підтримку своїх клієнтів протягом всього процесу використання системи. Команда підтримки завжди готова надати кваліфіковану допомогу та відповісти на всі запитання щодо роботи системи.

Важливо, що система компанії CleverBox CRM постійно вдосконалюється, додаються нові функції та можливості. Багаторічний досвід роботи зі своїми клієнтами дає можливість компанії зрозуміти потреби ринку та розробляти інструменти, які повністю задовільнять їхні очікування.

Таким чином, компанія CleverBox CRM пропонує своїм клієнтам функціональну систему, автоматизувати бізнес-процеси та покращувати комунікації з клієнтами. [6]

YCLIENTS також є інноваційною CRM системою для бізнесу, яка була створена в 2014 році у Литві, а пізніше була перенесена в Україну.

Основна ідея системи полягає в тому, щоб допомогти підприємствам з легкістю інтегруватися з потенційними та поточними клієнтами, оптимізувати робочий процес і забезпечити якість обслуговування. Ця CRM система, у першу чергу, призначена для тих, хто працює в сфері краси та здоров'я, таких як салони краси, масажні кабінети, фітнес-центри та інші.

Одна з найбільш важливих функцій YCLIENTS – це онлайн-бронювання послуг в будь-який час та з будь-якого пристрою. Це робить процес бронювання набагато зручнішим для клієнтів, а для бізнесу можливість планувати свій робочий час.

Крім того, система має функціонал для створювання та відстежування рекламних кампаній, аналізу маркетингу, ведення статистики та створення звітів.

Одним з головних переваг YCLIENTS є її зручний та легкий інтерфейс. Користувачі з легкістю орієнтуються в системі та ефективно використовують всі її можливості.

Система також пропонує зручні інструменти для керування співробітниками, зокрема змінами та графіками роботи. Користувач може додавати нових співробітників, встановлювати їхні ролі та обмеження доступу до інформації в залежності від потреб бізнесу. Можливі налаштування автоматичних повідомлень для співробітників, які нагадують про необхідність зробити нові записи або про терміни проведення процедур.

Більше того, система YCLIENTS дозволяє проводити успішний маркетинг, зокрема, створювати рекламні кампанії, розсилки, акції та бонусні програми для клієнтів. Для цього в системі є зручний редактор рекламних оголошень та інструменти для налаштування цільової аудиторії.

У загальному, YCLIENTS – це зручна CRM система, яка допомагає салонам краси оптимізувати свою роботу та підвищити результативність бізнесу. [7]

Також популярною CRM системою для б'юті індустрії в Україні є BloknotApp. Компанія BloknotApp була заснована в Україні в 2017 році. На сьогоднішній день вона є однією з провідних компаній, що працюють в галузі розробки програмного забезпечення для салонів краси.

Важливою функцією BloknotApp є можливість онлайн-бронювання послуг через мобільний додаток. Це зменшує навантаження на адміністраторів та дає змогу клієнтам забронювати зручний для них час без необхідності телефонування до салону.

Також BloknotApp зберігає всю інформацію про клієнтів у централізованій базі даних. Завдяки цьому знаходити необхідну інформацію про клієнтів, таку як історія відвідувань, побажання та пропозиції щодо нових послуг, дуже легко. Як результат клієнти можуть отримувати персоналізований сервіс та почувати себе унікальними і важливими для салону краси.

Водночас, BloknotApp дозволяє керувати фінансами салону краси: створювати рахунки-фактури, виставляти рахунки, відслідковувати оплати та виконувати інші фінансові операції.

Особливістю BloknotApp є можливість підключення до банківської системи, швидко та безпечно проводити фінансові операції з клієнтами та іншими партнерами. BloknotApp надає широкий спектр функціоналу для керування бізнесом в галузі краси та здоров'я.

Крім того, BloknotApp має високий рівень безпеки. Компанія надає велику увагу захисту даних своїх клієнтів. Програма побудована на сучасних технологіях для захисту важливої інформації про клієнтів та про фінансові операції. BloknotApp веде історію змін, що забезпечує контроль за всіма діями співробітників та покращує якість обслуговування.

Додатковою перевагою BloknotApp є можливість інтеграції з іншими популярними сервісами, такими як Google Calendar та MailChimp. BloknotApp має зручний та інтуїтивно зрозумілий інтерфейс, можливість роботи з клієнтами та робочими графіками в одній системі.

Крім того, BloknotApp пропонує низку додаткових функцій, таких як відстеження запасів та замовлень, статистичний аналіз продажів та багато іншого. Загалом, BloknotApp є однією з найкращих CRM систем для б'юті індустрії на сьогоднішній день. Компанія продовжує розвиватися та вдосконалюватися, щоб залишатися лідером на ринку. [8]

Як бачимо, впровадження CRM системи для салону краси є важливим кроком до автоматизації бізнесу, покращення якості обслуговування клієнтів, забезпечення збільшення обсягів продажів та зниження витрат підприємства, а також ведення успішного бізнесу в індустрії краси. Правильний вибір програмного забезпечення та комплексного підходу до автоматизації допоможе салону краси стати конкурентоздатнішим та забезпечити високу якість обслуговування.

Висновок. Відома експертка галузі, засновниця порталу Salonmarketing.pro та авторка книг «Мій салон краси» та «Ми відкрились!» Наталія Гончаренко в одному із своїх інтерв'ю запевнила, що індустрію краси чекає бурхливий розвиток після перемоги України над Російською Федерацією.

По-перше, навіть попри війну, салони краси працюють. Навіть відкриваються нові підприємства. Складнощі, з якими стикаються власники зростають майже щодня, але це не зупиняє відданих своїй справі підприємців.

По-друге, салони краси, які зачинились замінять нові салони.

По-третє, споживацька поведінка послуг краси в Україні сприяє розвитку галузі. На ринок прийдуть більш професійні інвестори, які мають досвід або щонайменше розуміння того, що ринку потрібні різноманітні, а не тільки дорогі послуги.

В-четверте, ще до війни в Україні почав розвиватись б'юті та медичний туризм і ця тенденція відновиться після перемоги дуже швидко, враховуючи репутацію нашої країни в цілому і індустрії краси зокрема. [9]

Отже, актуальність CRM системи для салонів краси не може бути переоцінена. У сучасному світі цифровізація проникає в усі сфери життя людини, зокрема і в індустрію надання послуг. В умовах, коли зовнішнє середовище трансформується, нікому не вдасться опинитися осторонь від процесів, що відбуваються. Адже постає питання: підлаштовуватися під нові умови взаємодії з постачальниками, клієнтами, майстрами або втрачати свої позиції. Саме завдяки цифровізації надання послуг в салонах краси стає більш оперативними та більш зручними як для власників підприємств та їх співробітників, так і для кінцевого споживача.

Список використаних джерел

1. Дослідницька компанія Euromonitor International / Електронний ресурс. – Режим доступу: https://www.euromonitor.com/
2. Міністерство розвитку економіки, торгівлі та сільського господарства України / Електронний ресурс. – Режим доступу: https://www.me.gov.ua/
3. Інформація із блогу компанії по розробці CRM Beauty Pro / Електронний ресурс. – Режим доступу: https://beautyprosoftware.com/ru/blog/
4. Можливості використання CRM-систем / Електронний ресурс. – Режим доступу: https://www.terrasoft.ua
5. Сайт компанії Beauty Pro CRM / Електронний ресурс. – Режим доступу: https://beautyprosoftware.com/
6. Сайт компанії CleverBox / Електронний ресурс. – Режим доступу: https://cleverbox-crm.com/
7. Інформація з Інтернет-видання 032.ua / Електронний ресурс. – Режим доступу: https://www.032.ua/news/3514027/biznes-saloniv-krasi-v-2023-2025-rokah-cogo-cekati.

Робота виконана під науковим керівництвом к.т.н., доцента
РЗАЄВОЇ С.Л.

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ВІД КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

КУКЛІНСЬКИЙ Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні види криптографічних методів, такі як симетричне шифрування, асиметричне шифрування, хешування даних та цифровий підпис. Детально проаналізовано, як криптографічні методи можуть бути використані для захисту інформації на серверах підприємства, робочих станціях та переносних пристроях, а також при передачі інформації через мережу. Описано приклад використання криптографічних методів на підприємстві та розглянуто його результати. Розглянуто переваги та недоліки використання криптографічних методів, а також запропоновано рекомендації щодо їх використання на підприємстві.

The article discusses the main types of cryptographic methods, such as symmetric encryption, asymmetric encryption, data hashing, and digital signatures. It analyzes in detail how cryptographic methods can be used to protect information on enterprise servers, workstations, and mobile devices, as well as when transmitting information over the network. A case study of the use of cryptographic methods in an enterprise is described, and its results are discussed. The advantages and disadvantages of using cryptographic methods are considered, and recommendations for their use in the enterprise are proposed.

Актуальність. Актуальність криптографічних методів захисту інформації на підприємстві від комп'ютерних злочинів полягає в тому, що в даний час комп'ютерні атаки є дуже поширеними і можуть спричинити серйозні наслідки для підприємства. Інформація про клієнтів, фінансові дані, розробки, плани і стратегії підприємства можуть бути скомпрометовані або викрадені зловмисниками. Криптографічні методи дозволяють захистити інформацію від несанкціонованого доступу та зберігати її в зашифрованому вигляді. Крім того, вони можуть забезпечити цілісність даних та підтвердження автентичності відправника. Також вони допомагають забезпечити відповідність законодавству щодо захисту персональних даних та іншої конфіденційної інформації. Крім того, за допомогою криптографічних методів можна перевірити автентичність інформації та забезпечити її недоступність для зловмисників, що забезпечує більш високий рівень захисту.

Актуальність криптографічних методів захисту інформації на підприємстві полягає в тому, що ці методи є одними з найефективніших і надійних способів захисту інформації від комп'ютерних злочинів. Вони дозволяють підприємствам забезпечувати конфіденційність, цілісність та доступність інформації, а також забезпечувати надійний захист від різних видів атак. Отже, використання криптографічних методів є важливим елементом у захисті інформації на підприємстві від комп'ютерних злочинів і може допомогти уникнути серйозних наслідків для підприємства.

Мета статті – є дослідження криптографічних методів захисту інформації на підприємстві від комп'ютерних злочинів та визначення їх ролі у цьому процесі.

Об'єктом дослідження є аналіз криптографічних методів, їх застосування для захисту інформації на різних пристроях та в мережі, а також оцінка ефективності та обґрунтування рекомендацій щодо використання цих методів.

Предмет дослідження – криптографічні методи захисту інформації на підприємстві від комп'ютерних злочинів, зокрема симетричне шифрування, асиметричне шифрування, хешування даних та цифровий підпис.

Аналіз попередніх досліджень. Аналіз попередніх досліджень з криптографічних методів захисту інформації на підприємствах від комп'ютерних злочинів показує, що використання криптографічних методів є важливим елементом в захисті конфіденційної інформації від несанкціонованого доступу. Дослідження в цій області зосереджувалися на різних аспектах криптографії, включаючи симетричне і асиметричне шифрування, хешування даних, цифровий підпис та інші методи. Українські та закордонні вчені: І.С. Самойленко, Брюс Шнайер, Ніл Фергюнсон, Дуглас Стайнберг, Брюс Шнайр займалися дослідженням криптографічних методів захисту інформації на підприємствах від комп'ютерних злочинів. У своїх дослідженнях вони аналізували переваги та недоліки кожного з методів, а також вивчали практичні аспекти їх використання на підприємствах. Зокрема, вони досліджували, як криптографічні методи можуть бути використані для захисту інформації на серверах підприємства, робочих станціях та переносних пристроях, а також при передачі інформації через мережу.

Виклад основного матеріалу. На сьогоднішній день комп'ютерні злочини стали серйозною загрозою для підприємств. Ці злочини можуть призвести до крадіжки конфіденційної інформації, порушення нормативно-правових актів, втрати даних, відключення від Інтернету та збоїв в роботі комп'ютерних систем. Комп'ютерні злочини − це кримінальна діяльність, яка використовує комп'ютерні технології та Інтернет з метою здійснення шахрайства, шпигунства, вандалізму, крадіжки конфіденційної інформації, а також інших кримінальних дій. Крім того, комп'ютерні злочини можуть мати серйозні фінансові наслідки для підприємств, такі як витрати на відновлення інформації та відновлення роботи систем, втрати прибутку, штрафи за порушення нормативно-правових актів та судові витрати.

Отже, захист інформації на підприємстві є дуже важливою задачею, оскільки комп'ютерні злочини можуть стати серйозною загрозою для його діяльності та призвести до значних фінансових втрат. Захист інформації на підприємствах є дуже важливою задачею, оскільки конфіденційність та цілісність даних є критично важливими аспектами успішної діяльності підприємства. Недостатній захист може призвести до наслідків, які мають серйозний вплив на бізнес-процеси підприємства, такі як втрата клієнтів та партнерів, зменшення прибутку, втрата репутації, штрафні санкції та навіть банкрутство. Крім того, захист інформації є важливим для дотримання нормативно-правових вимог та регулювання в галузі захисту даних, що може забезпечити надійність та довіру серед споживачів та інвесторів. Захист інформації також є важливим для забезпечення безпеки працівників та клієнтів підприємства, оскільки в разі порушення безпеки даних можуть стати доступними особисті дані та фінансова інформація, що може призвести до крадіжки особистих коштів та ідентичності, шахрайства та інших злочинів.

Криптографічні методи захисту інформації − це методи та технології, що застосовуються для забезпечення конфіденційності, цілісності та доступності інформації. Криптографічні методи захисту інформації є одним з найбільш ефективних інструментів боротьби з комп'ютерними злочинами. Основні криптографічні методи включають:

1. Симетричне шифрування – метод, який використовує один ключ для шифрування та розшифрування повідомлення. Найпоширенішими алгоритмами симетричного шифрування є AES (Advanced Encryption Standard), DES (Data Encryption Standard) та 3DES (Triple Data Encryption Standard).

Симетричне шифрування – це криптографічний метод, який використовує один ключ як для шифрування, так і для дешифрування повідомлень. Цей метод є одним з найстаріших та найпростіших методів шифрування і використовується для захисту інформації від несанкціонованого доступу. У симетричному шифруванні повідомлення перетворюються в криптограму (шифрований текст) за допомогою алгоритму шифрування і ключа. Коли отримувач отримує криптограму, він використовує той же ключ та алгоритм для

дешифрування повідомлення. Одним з найпоширеніших симетричних алгоритмів шифрування є AES (Advanced Encryption Standard), який зараз використовується у багатьох системах та програмах для захисту даних. Одним з недоліків симетричного шифрування є необхідність безпечного обміну ключами між відправником та отримувачем, а також можливість взлому ключа методом брутфорсу, коли злоумисник перебирає всі можливі комбінації ключів до того моменту, поки не знайде правильний ключ

2. Асиметричне шифрування – метод, що використовує пару ключів − приватний та відкритий − для шифрування та розшифрування повідомлення. Найпоширенішими алгоритмами асиметричного шифрування є RSA та ECC (Elliptic Curve Cryptography).

Асиметричне шифрування – це криптографічний метод, у якому використовується пара ключів: публічний ключ і приватний ключ. Публічний ключ відкритий для використання всіма, тоді як приватний ключ є прихованим і відомим тільки власнику. Коли повідомлення шифрується за допомогою публічного ключа, то тільки власник приватного ключа може його розшифрувати. Це дозволяє захистити повідомлення від прослуховування та збереження конфіденційності даних. Асиметричне шифрування також використовується для підпису повідомлень. Власник приватного ключа може підписати повідомлення, й інші користувачі можуть перевірити цей підпис за допомогою публічного ключа, щоб переконатися в тому, що повідомлення було підписано саме власником приватного ключа, а не кимось іншим. Одним з найпопулярніших алгоритмів асиметричного шифрування є RSA (Rivest–Shamir–Adleman). Він використовується в багатьох криптографічних протоколах, включаючи SSL / TLS для захисту передачі даних в Інтернеті.

3. Хешування даних – метод, який використовує хеш-функції для створення унікального коду з повідомлення або даних. Хеш-функції, такі як SHA (Secure Hash Algorithm), використовуються для створення цифрових підписів та перевірки цілісності даних.

Хешування даних – це процес перетворення вхідних даних будь-якої довжини в фіксований вихідний хеш-код фіксованої довжини. Хеш-функція приймає на вхід блок даних і генерує хеш-код – унікальний ідентифікатор, який можна використовувати для перевірки цілісності даних. Хеш-код зазвичай представляється у вигляді невеликого числа або рядка символів. Хеш-функції повинні відповідати вимогам безпеки та надійності, тобто вони мають бути стійкими до колізій (тобто дві різні вхідні послідовності не повинні генерувати однаковий хеш-код) та малопридатними для зламу. Хеш-функції використовуються в різних областях, таких як криптографія, збереження паролів, контроль цілісності даних, пошук та індексація даних. Наприклад, хеш-функції використовуються для створення підписів цифрових даних, перевірки автентичності повідомлень та ідентифікації відомостей про користувачів в системах аутентифікації. Одним з найбільш відомих алгоритмів хешування є SHA (Secure Hash Algorithm), який розробив Національний інститут стандартів і технологій США. Також існують інші алгоритми, такі як MD5, які використовуються для хешування даних. Проте MD5 вважається менш безпечним, оскільки може бути легко зламано.

4. Цифрові підписи − це електронний еквівалент підпису на папері, який можна використовувати для підтвердження автентичності документа або повідомлення в електронному вигляді. Цифровий підпис створюється за допомогою алгоритму криптографічного хешування та асиметричного шифрування.

Для перевірки цифрового підпису необхідно розшифрувати хеш-код за допомогою відкритого ключа власника підпису і порівняти його з хеш-кодом повідомлення або документа, який також розраховується за допомогою хеш-функції. Якщо значення збігаються, то цифровий підпис вірний і повідомлення або документ вважається автентичним.

Цифрові підписи використовуються в різних областях, таких як електронна комерція, електронна пошта, електронний документообіг та банківські операції. Вони дозволяють забезпечити надійність, цілісність та конфіденційність електронної інформації та перешкоджають можливості підробки даних. Для створення цифрового підпису використовується

асиметричний алгоритм шифрування. Підпис складається з двох частин: відкритого ключа та цифрової підпису. Відкритий ключ повідомляється отримувачу повідомлення, тоді як цифровий підпис створюється за допомогою закритого ключа, який зберігається в таємниці від автора.

5. VPN (Virtual Private Network) − це технологія, яка дозволяє створювати безпечне з'єднання між комп'ютерами за допомогою зашифрованого тунелю. VPN дозволяє захистити інтернет-трафік від шпигунів та хакерів.
6. Електронний підпис − метод, який використовується для забезпечення відповідності електронних документів законодавству про електронний документообіг.
7. Протоколи аутентифікації − методи, що використовуються для перевірки ідентифікації користувачів та встановлення їхнього права доступу до інформації.
8. Кодування повідомлень − метод захисту інформації, при якому повідомлення перетворюються в інший формат. Наприклад, алгоритми кодування можуть перетворювати символи повідомлення в числа або замінювати символи на інші.
9. Розподіл ключів − метод, що використовується для безпечного обміну ключами між віддаленими користувачами. Розподіл ключів може використовувати симетричні та асиметричні шифри.

Захист інформації на серверах підприємства є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Деякі з основних методів захисту інформації на серверах підприємства включають наступне: фізичний захист: серверні приміщення повинні бути захищені від несанкціонованого доступу. Це може бути досягнуто за допомогою контролю доступу, системи відеоспостереження, біометричних систем та ін; захист мережі: мережеві з'єднання повинні бути захищені від атак, таких як DDOS, фішинг та ін. Це може бути досягнуто за допомогою захисту мережі, який може включати в себе мережеві фільтри, системи виявлення вторгнень та інші; парольний захист: доступ до серверів повинен бути захищений за допомогою паролів та інших методів аутентифікації. Користувачі повинні мати сильні паролі та система повинна бути налаштована таким чином, щоб вона вимагала зміну пароля з регулярністю; шифрування даних: дані, які зберігаються на сервері, повинні бути захищені за допомогою шифрування. Це може бути досягнуто за допомогою симетричного або асиметричного шифрування, які були описані вище; резервне копіювання даних: резервне копіювання даних є важливим елементом захисту інформації на серверах. Це може бути досягнуто за допомогою регулярних резервних копій, які зберігаються в окремих фізичних приміщеннях, а також використання систем відновлення даних в разі аварійного відновлення системи.

Захист інформації на робочих станціях та переносних пристроях є важливим аспектом забезпечення безпеки даних в офісному середовищі. Деякі з основних методів захисту інформації на робочих станціях та переносних пристроях включають наступне:

1. Парольний захист: використання паролів для захисту доступу до робочих станцій та переносних пристроїв є основним методом захисту. Користувачі повинні мати сильні паролі та система повинна бути налаштована таким чином, щоб вона вимагала зміну пароля з регулярністю.
2. Шифрування даних: шифрування даних на робочих станціях та переносних пристроях може бути досягнуто за допомогою симетричного або асиметричного шифрування, які були описані вище. Також можна використовувати програми для шифрування даних, які зберігаються на переносних пристроях.
3. Захист від шпигунського програмного забезпечення: використання антивірусного програмного забезпечення та фаєрволів є важливим для захисту робочих станцій та переносних пристроїв від шпигунського програмного забезпечення.
4. Регулярне оновлення програмного забезпечення: регулярне оновлення програмного забезпечення допомагає запобігти вразливостям, які можуть бути використані для атак на робочі станції та переносні пристрої.

5. Захист мережі: мережеві з'єднання повинні бути захищені від атак, таких як DDOS, фішинг та ін. Це може бути досягнуто за допомогою захисту мережі, який може включати в себе мережеві фільтри, системи виявлення вторгнень та ін.

Захист інформації при передачі через мережу є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Деякі з основних методів захисту інформації при передачі через мережу включають наступне:

1. Шифрування даних: шифрування даних може бути досягнуто за допомогою симетричного або асиметричного шифрування, які були описані вище. Це допоможе забезпечити захист від прослуховування та перехоплення даних під час їх передачі через мережу.
2. Використання віртуальних приватних мереж (VPN): використання VPN дозволяє створити безпечний тунель для передачі даних через небезпечні мережі. Дані шифруються та передаються через тунель, що дозволяє забезпечити конфіденційність даних.
3. Використання протоколів безпеки: використання протоколів безпеки, таких як Secure Sockets Layer (SSL) та Transport Layer Security (TLS), є важливим для захисту даних при передачі через мережу. Ці протоколи шифрують дані та забезпечують їх цілісність.
4. Захист від атак: мережеві з'єднання повинні бути захищені від атак, таких як DDOS, фішинг, мережеві вторгнення та інші. Це може бути досягнуто за допомогою захисту мережі, який може включати в себе мережеві фільтри, системи виявлення вторгнень та ін.
5. Використання SSL / TLS: SSL / TLS − це протоколи захисту, які шифрують дані перед їх передачею через мережу. SSL / TLS використовується для захисту веб-сайтів, електронної пошти та інших додатків, що працюють через мережу.
6. Аутентифікація: передача інформації через мережу повинна бути аутентифікована, щоб запобігти підробці та перехопленню даних. Для цього можна використовувати різні методи аутентифікації, такі як логіни та паролі, біометричні методи та інші.

Вибір правильного криптографічного методу залежить від конкретних вимог до захисту даних, ризиків, які необхідно зменшити, та здатності виконувати розрахунки на обраному пристрої. Ось кілька критеріїв, які можна використовувати при виборі криптографічного методу:

1. Вартість застосування: вартість застосування криптографічних методів може бути дуже високою, залежно від використовуваної технології. Тому при виборі методу потрібно враховувати вартість його застосування, а також можливості фінансування проекту.
2. Можливість використання: методи шифрування можуть бути складними для використання та реалізації, тому потрібно забезпечити, що вони можуть бути ефективно застосовані для захисту інформації в конкретній ситуації.
3. Сумісність з іншими системами: при виборі криптографічних методів необхідно забезпечити сумісність з іншими системами та забезпечити можливість обміну даними з ними.
4. Рівень захисту: в залежності від рівня захисту, який потрібно досягти, може бути вибрано різні методи криптографії. Наприклад, якщо потрібно захистити відомості від зламу, може бути використаний асиметричний алгоритм шифрування. Якщо потрібно захистити дані від прослуховування, може бути використано шифрування SSL/TLS.
5. Надійність та стійкість до атак: криптографічний метод повинен бути надійним та стійким до атак, які можуть бути спрямовані на злам цієї системи. Для цього потрібно розуміти можливі загрози та використовувати методи, які забезпечують стійкість до таких атак.

Криптографічні методи є важливою складовою систем захисту інформації, але самі по собі вони не можуть забезпечити повної безпеки даних. Інші методи захисту інформації, такі як фізична безпека, контроль доступу, аудит та моніторинг, повинні використовуватись разом з криптографічними методами для забезпечення повної безпеки інформації. Наприклад, для

захисту інформації на серверах підприємства можуть використовуватись криптографічні методи, такі як SSL/TLS, для захисту даних, які передаються по мережі. Однак, для забезпечення повної безпеки інформації також потрібно використовувати інші методи захисту, такі як регулярні аудити безпеки серверів, захисний периметр, брандмауер та системи моніторингу і виявлення інцидентів. Крім того, для захисту інформації на робочих станціях та переносних пристроях можуть використовуватись криптографічні методи, такі як шифрування диска, яке захищає дані на пристрої в разі його втрати або крадіжки. Однак, щоб забезпечити повну безпеку, також потрібно використовувати інші методи захисту, такі як контроль доступу до пристроїв та фізична безпека. Таким чином, використання криптографічних методів у поєднанні з іншими методами захисту інформації є необхідним для забезпечення повної безпеки даних в організації. Кожен метод захисту повинен бути вибраний в залежності від конкретних потреб організації та способів ризику, які повинні бути усунені.

У криптографії ключі є важливими елементами, які використовуються для шифрування та розшифрування даних, підпису та перевірки цифрових підписів. Ключове управління та зберігання ключів є важливими аспектами криптографії, оскільки вони забезпечують безпеку ключів та інформації, зашифрованої цими ключами.

Ключове управління означає забезпечення безпеки та ефективного використання ключів в організації. Це включає в себе генерацію ключів, дистрибуцію ключів, контроль доступу до ключів та їх використання, а також знищення ключів за потреби. Ключі можуть бути симетричні та асиметричні, і кожний тип ключа має свої вимоги до ключового управління. Зберігання ключів також є важливим аспектом криптографії. Ключі повинні бути збережені в безпечному місці, щоб запобігти їхньому викраденню або використанню несанкціонованими особами. Для зберігання ключів можна використовувати різні методи, такі як використання безпечних пристроїв зберігання ключів (HSM), використання захищених електронних ключниць, розподіл ключів на різних серверах, що забезпечує резервні копії ключів, тощо. Для забезпечення безпеки ключів та інформації, зашифрованої цими ключами, важливо використовувати різні методи захисту, такі як шифрування ключів, використання двофакторної автентифікації при доступі до ключів, встановлення правил контролю доступу до ключів, редагування журналів дій з ключами, тощо.

Розглянемо приклад використання криптографічних методів на підприємстві для захисту даних клієнтів. Припустимо, що підприємство займається продажем товарів онлайн, тому має доступ до особистих даних своїх клієнтів, таких як імена, адреси електронної пошти, номери телефонів і банківські реквізити. Щоб захистити ці дані, підприємство може використовувати криптографічні методи. Один з можливих підходів – використовувати SSL (Secure Sockets Layer) або його наступника TLS (Transport Layer Security) для захищеної передачі даних між веб-сервером підприємства та веб-браузерами клієнтів. Це забезпечує захист від перехоплення даних під час їх передачі через мережу.

Також підприємство може використовувати криптографічні методи для зберігання паролів клієнтів. Замість зберігання паролів у відкритому вигляді, підприємство може зберігати їх у захешованому вигляді, використовуючи алгоритми хешування, такі як SHA-256 або bcrypt. Це знижує ризик вторгнення в систему та компрометації паролів клієнтів. Це дозволяє клієнтам перевірити, що повідомлення дійсно надіслано підприємством та не було підроблено зловмисниками.

Використання криптографічних методів на підприємстві дозволяє значно покращити рівень захисту інформації та запобігти її незаконному доступу. Результати використання криптографічних методів на підприємстві можуть бути наступними:

1. Збільшення рівня безпеки: застосування криптографічних методів дозволяє захистити інформацію від несанкціонованого доступу, зменшити ризики витоку даних, злому систем та інших загроз.
2. Підвищення рівня довіри: використання криптографічних методів дозволяє підтверджувати автентичність даних та ідентифікацію користувачів, що підвищує довіру до системи.

3. Зменшення ризику втрати даних: застосування методів шифрування та резервного копіювання даних дозволяє зменшити ризик втрати даних в результаті випадкового або зловмисного знищення.
4. Підвищення ефективності: застосування криптографічних методів дозволяє збільшити ефективність обробки даних, оскільки шифрування та розшифрування можуть виконуватись автоматично.
5. Забезпечення відповідності вимогам законодавства: використання криптографічних методів дозволяє підприємствам виконувати вимоги законодавства щодо захисту персональних даних та конфіденційності інформації.

Однак, слід зазначити, що використання криптографічних методів не є панацеєю і не забезпечує повну безпеку інформації. Для ефективного захисту необхідно використовувати комплексний підхід та поєднувати криптографічні методи з іншими методами захисту інформації. Також важливо забезпечувати правильне управління ключами та робити регулярну перевірку.

Висновки. Криптографічні методи відіграють важливу роль у захисті інформації на підприємстві. Вони забезпечують конфіденційність, цілісність та доступність даних, що є важливими аспектами у будь-якій організації. Криптографія також дозволяє підприємствам дотримуватись вимог законодавства щодо захисту персональних даних та іншої конфіденційної інформації. Крім того, застосування криптографічних методів допомагає підприємствам забезпечити довіру між сторонами, що сприяє розвитку бізнесу та співпраці з партнерами та клієнтами. Отже, використання криптографічних методів у захисті інформації на підприємстві є дуже важливим для забезпечення конфіденційності, цілісності та доступності даних, зменшення ризику витоку даних та кібератак, дотримання вимог законодавства та забезпечення довіри між сторонами. Основними перевагами використання криптографічних методів у захисті інформації на підприємстві є конфіденційність, цілісність; аутентифікація; незалежність від інших методів захисту. Хоча криптографічні методи забезпечують високий рівень захисту інформації на підприємстві, вони мають деякі недоліки, серед яких: високі витрати на впровадження, складність управління ключами, потреба в постійному оновленні, вплив на продуктивність, ризик втрати ключів. Тому важливо належним чином зберігати та управляти ключами. Ці недоліки не означають, що криптографічні методи не ефективні. Вони лише вказують на те, що підприємство повинно добре розуміти свої потреби та можливості, перш ніж впроваджувати криптографічні методи захисту інформації.

Використання криптографічних методів є важливим кроком для захисту інформації на підприємстві, проте це не єдиний метод захисту. Правильне поєднання криптографічних методів з іншими методами захисту інформації може забезпечити найвищий рівень захисту даних на підприємстві.

Список використаних джерел

1. Лагун А.Е. Криптографічні системи та протоколи: нав. посібник / А.Е. Лагун. – Львів: Видавництво Львівської політехніки, 2013. – 96 с.
2. Горобцов В.О. Криптографічний захист інформації – URL: http://esu.com.ua/search_articles.php?id=1575.
3. Сушко С.А. Практична криптологія – URL: https://bit.nmu.org.ua/ua/student/metod/cryptology/%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1%8F%201.pdf.
4. Класифікація сучасних криптографічних методів – URL: *https://lickeys.ru/uk/zhestkijj-disk/klassifikaciya-sovremennyhkriptograficheskihmetodov//*

Робота виконана під науковим керівництвом к.т.н., доцента
САВЧЕНКО Т.В.

АСПЕКТИ НАЛАШУВАННЯ ПРИСТРОЇВ КОМУТАЦІЇ КОМП'ЮТЕРНИХ МЕРЕЖ

КУПІН О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні аспекти налаштування пристроїв комутації комп'ютерних мереж Кампусів та підприємств. Зазначено переваги застосування програмного забезпечення для організації швидкого налаштування пристроїв комутації комп'ютерних мереж. Розглянуто як зразок виробників сучасних пристроїв комутації Cisco, Aruba, Ruckus.

The article discusses the main aspects of setting up switching devices for computer networks of Campuses and enterprises. The advantages of using software for the organization of quick configuration of computer network switching devices are indicated. Considered as a model of manufacturers of modern switching devices Cisco, Aruba, Ruckus.

Актуальність. У наш час мережі мають вирішальне значення для підтримки компаній, пропонування підключених послуг і можливості співпраці. Оскільки вони з'єднують пристрої, які спільно використовують ресурси. Мережеві комутатори є життєво важливим компонентами усіх мереж.

Метою статі є дослідження аспектів налаштування пристроїв комутації в комп'ютерних мережах з метою підвищення кваліфікації користувачів.

Об'єктом дослідження є пристрої комутації комп'ютерних мереж.

Предмет дослідження – пристрої комутації.

Аналіз попередніх досліджень. Дослідженню особливостей аспектів налаштування пристроїв комутації комп'ютерних мереж, основних характерних рис присвячені праці закордонних науковців: Алессандра Делліні, Леонарда Клейнрока., Аннандро Датта, Фредеріка Й. Хіллса, Волтера Класса.

Виклад основного матеріалу. У наш час мережі відіграють велике значення у підтримці діяльності не лише великих компаній та установ, а й малих підприємств. Ключовими вузлами у всіх цих мережах виступають комутатори. Оскільки вони з'єднують пристрої, які спільно використовують ресурси.

Пристрій комутації, іншими словами комутатор — це апаратний компонент, відповідальний за ретрансляцію даних із мережі до кінцевої точки призначення за допомогою комутації пакетів, ідентифікації MAC-адреси та системи багатопортового мосту.

Якщо розглянути модель OSI – побачимо, що мережевий комутатор працює на рівні 2 каналу передачі даних архітектури взаємодії відкритих систем (Рис.1).

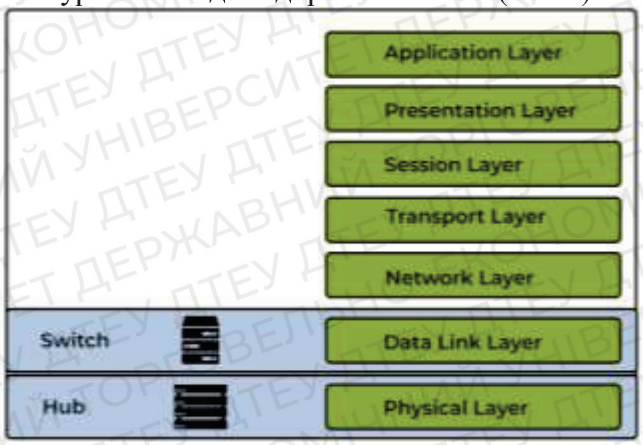


Рис.1. Модель OSI

Вони також можуть функціонувати там, де маршрутизація відбувається на мережевому рівні 3. Комутатори є стандартними компонентами в мережах Ethernet, Fiber Channels, InfiniBand і асинхронному режимі передачі (ATM). Однак більшість сучасних комутаторів використовують Ethernet.

Розглянувши площу інтеграції мережевого комутатора, ми можемо зробити висновок, що він з'єднує майже всі мережеві пристрої (принтери, комп'ютери та бездротові пристрої/точки доступу) і дозволяє користувачам обмінюватися пакетами даних. Комутатори можуть бути, як апаратними, так і програмними віртуальними пристроями, які керують фізичними системами. У сучасних мережевих системах комутатори складають переважну масу мережевого обладнання.

Якщо розглянути принцип роботи комутаторів ми побачимо наступне – коли пристрої під'єднані до комутаторів, вони записують інформацію про керування доступом до медіа (MAC) пристрою. Ця адреса є кодом, який зберігається на картці мережевого інтерфейсу пристрою (NIC), яка є частиною пристрою, яка підключається до комутатора через кабель Ethernet.

Комутатор перевіряє адресу пункту призначення та передає пакет на пристрої через відповідні порти. Більшість комутаторів оснащені можливостями повного дуплексу, щоб мінімізувати ймовірність колізій у мережевому трафіку. Це дає пакетам всю пропускну здатність з'єднання між пристроєм і комутатором.

Незважаючи на те, що комутатори зазвичай виконують функції на рівні 2, вони можуть працювати на рівні 3. Це необхідно для того, щоб можна було створити віртуальні локальні мережі (VLAN) — тобто логічні сегменти мережі, які виходять за межі підмереж. Трафік повинен проходити між комутаторами, щоб переходити з однієї підмережі в іншу, що полегшується завдяки їх вбудованим можливостям маршрутизації.

Мережеві комутатори доступні в різних типах і категоріях для різних випадків використання (Рис.2).

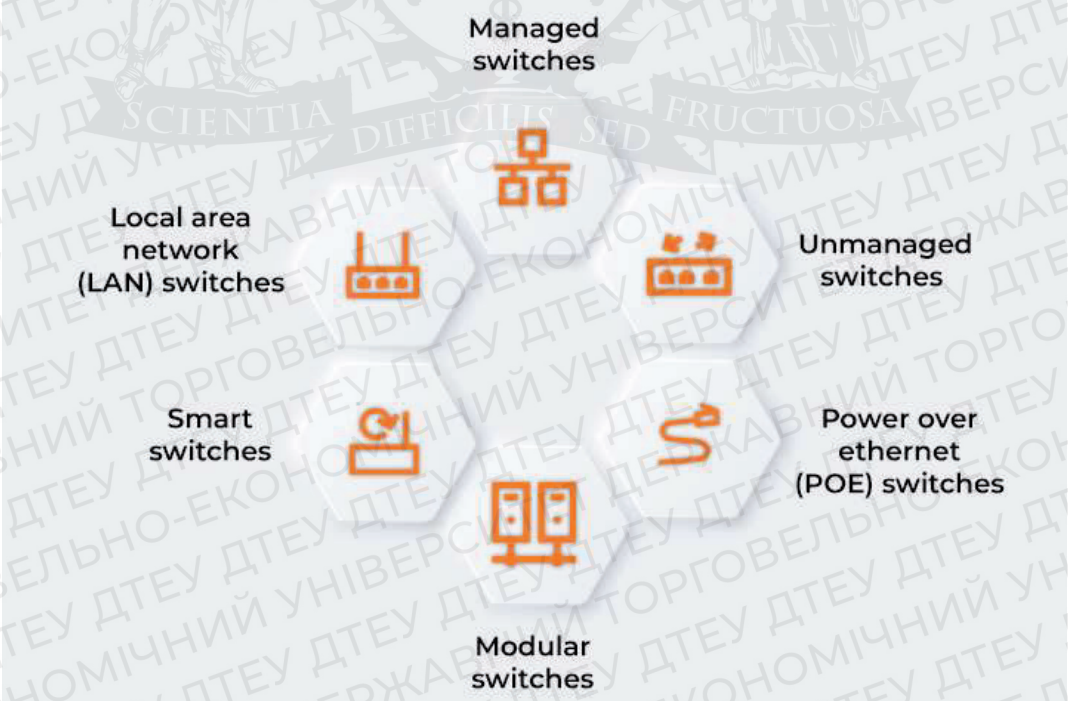


Рис.2. Типи мережевих комутаторів

Комутатори діляться на 6 основних типів [1]:

- Некеровані комутатори
- Керовані комутатори
- Комутатори Power over Ethernet (POE)

- Комутатори локальної мережі (LAN)
- Smart комутатори
- Модульні комутатори

Найпростіші у використанні комутаційні пристрої – це некеровані комутатори. Вони розширюють з'єднання Ethernet локальної мережі, дозволяючи додаткові підключення до Інтернету для локальних пристроїв. Некеровані комутатори відносно дешеві, але низькі можливості роблять їх непридатними для багатьох корпоративних задач.

А ось керовані комутатори використовуються частіше всього у комерційних і корпоративних мережах. Вони забезпечують більшу ємність і можливості для IT-фахівців. Для налаштування керованих комутаторів використовуються інтерфейси командного рядка та Web-інтерфейси.

Для швидкої і зручної інтеграції у свою мережу точок доступу, відеоспостереження, телефонії використовуються комутатори з підтримкою Power over Ethernet (POE). PoE — це спосіб подачі живлення постійного струму на малопотужні пристрої через дріт локальної мережі. Пристрої з цією технологією дозволяють уникнути потреби в додаткових розетках і робить встановлення ефективним. Комутатор із підтримкою PoE також безпечніший, оскільки вихідна потужність низька та інтелектуально керована.

Комутатори локальної мережі зазвичай використовуються для зв'язку між розташуваннями у внутрішній локальній мережі компанії. Ефективний розподіл пропускної здатності запобігає накладанню пакетів даних під час їх переміщення по мережі. Ці комутатори зменшують перевантаженість мережі або вузькі місця, надсилаючи пакет даних лише призначеному отримувачу.

Smart комутатори називають розумними або інтелектуальними. Вони виходять по функціоналу за межі некерованого комутатора, але менші, ніж у звичайного керованого комутатора.

Найгабаритнішими є модульні комутатори. Вони дозволяють за потреби додавати модулі розширення, джерела живлення та вентилятори охолодження забезпечуючи більшу гнучкість у міру зростання мережі. Однак ці комутатори значно дорожчі за стаціонарні та часто використовуються у великих мережах.

Усі ці комутатори окрім некерованих та Smart, ще можуть підтримувати таку функцію, як стекування.

Розібравшись з типами комутаторів, тепер потрібно перейти до аспектів налаштування пристроїв комутації комп'ютерних мереж. До аспектів налаштування відноситься:

- Першим і найголовнішим аспектом у побудові мережі є налаштування мережевої топології (Рис.3). Це означає визначення фізичної структури мережі, включаючи кількість пристроїв, їх розташування та зв'язки між ними.

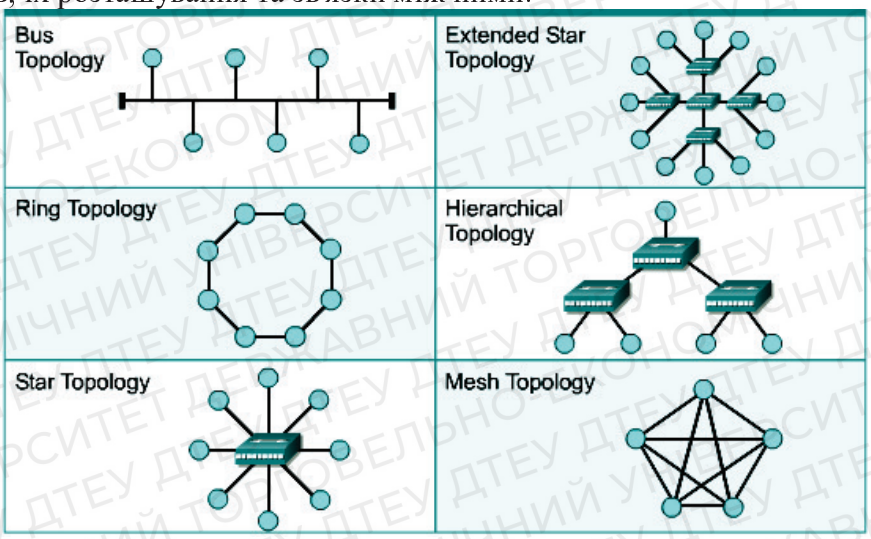


Рис.3. Топологія мереж

- Конфігурація портів. Налаштування портів комутатора є одним із основних аспектів налаштування пристроїв комутації. Це включає в себе налаштування портів для певних типів трафіку, встановлення швидкості передачі даних, дуплексу та увімкнення/вимкнення функцій, таких як Port Security, VLAN.
- Окремо потрібно винести VLAN конфігурацію. Налаштування Virtual Local Area Network (VLAN) дозволяє розділити мережу на логічно окремі сегменти, що може покращити безпеку та керованість мережі (Рис.4).

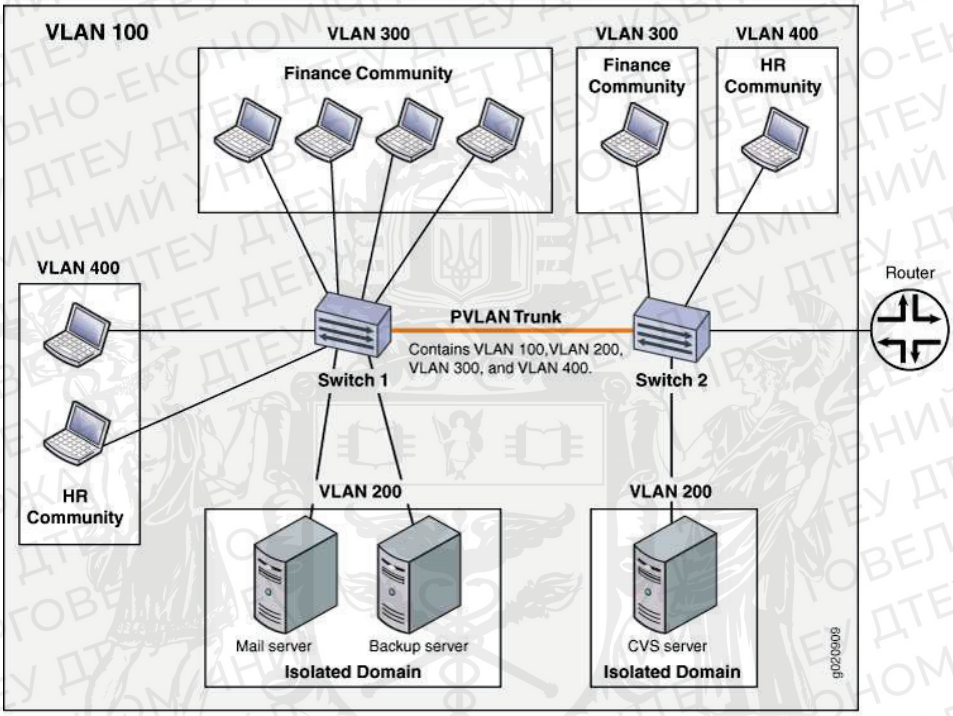


Рис.4. Розбиття мережі на VLAN

На (Рис.4) видно, що користувачі та пристрої поділені на групи: HR, Finance, Servers. Вони всі поєднані комутаторами та певна група знаходиться у відповідному VLAN`і. У такому випадку група користувачів HR ні при яких обставинах не отримає дані від групи Finance, що у свою чергу може гарантувати збереження конфіденційної інформації.

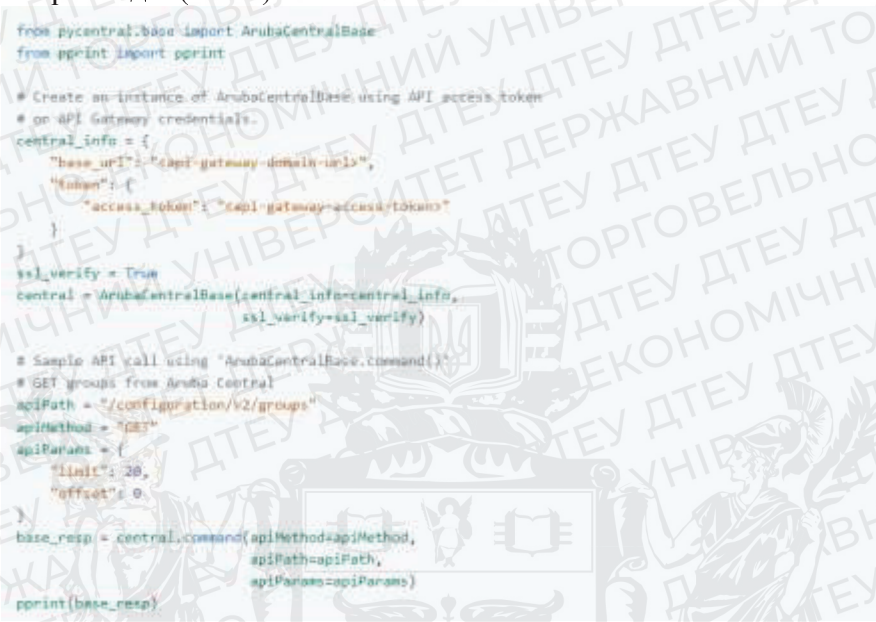
Ще однією функцією налаштування VLAN виступає налаштування тегованих та нетегованих портів.

- Конфігурація безпеки. Безпека є ключовим аспектом налаштування комутаційних пристроїв. До таких функцій безпеки можна віднести: Port Security, ACL, RADIUS і т.п. Ці функції допомагають забезпечити безпеку мережі, запобігти несанкціонованому доступу та захистити від атак.
- Наступним не менш важливим аспектом є налаштування QoS. Quality of Service (QoS) дозволяє оптимізувати продуктивність мережі для різних типів трафіку. Налаштування QoS включає встановлення пріоритету для різних типів трафіку і налаштування засобів контролю трафіку, таких як policing і shaping.
- Моніторинг. Він включає встановлення засобів моніторингу та аналізу трафіку, таких як SPAN і NetFlow. Моніторинг дозволяє адміністраторам відстежувати використання мережних ресурсів та швидко реагувати на проблеми у мережі [2].

Це лише деякі з аспектів налаштування пристроїв комутації. Кінцевий список залежить від конкретних вимог та налаштувань у кожній мережі.

Пристрої комутації як і технології розвиваються з кожним роком. Не так давно у мережах використовувались прості концентратори, а вже зараз за допомогою мов програмування можна керувати керованими комутаторами та всією мережею в цілому.

Як приклад було розглянуто пристрої комутації корпорації Hewlett Packard Enterprise підрозділу Aruba Network. Одже Python є однією з мов програмування, які можна використовувати для програмування комутаторів Aruba [3]. Для програмування комутаторів Aruba з використанням Python доступний набір інструментів ArubaOS-CX, який надає розширений доступ до комутатора за допомогою REST API та бібліотек Python для взаємодії з ним. Ось один з прикладів (Рис.5)



```
from pycentral.base import ArubaCentralBase
from pprint import pprint

# Create an instance of ArubaCentralBase using API access token
# or API Gateway credentials
central_info = {
    "base_url": "<api-gateway-domain-url>",
    "token": {
        "access_token": "<api-gateway-access-token>"
    }
}
ssl_verify = True
central = ArubaCentralBase(central_info=central_info,
                           ssl_verify=ssl_verify)

# Sample API call using "ArubaCentralBase.command()"
# GET groups from Aruba Central
apiPath = "/configuration/v2/groups"
apiMethod = "GET"
apiParams = {
    "limit": 20,
    "offset": 0
}
base_resp = central.command(apiMethod=apiMethod,
                            apiPath=apiPath,
                            apiParams=apiParams)
pprint(base_resp)
```

Рис.5. Здійснення виклику API за допомогою pycentral base

ArubaOS-CX також підтримує використання мови програмування Ansible, що дозволяє автоматизувати задачі на комутаторах Aruba.

Висновок: Сучасний світ, потреби сучасних підприємств та установ не може обійтись без пристроїв комутації та маршрутизації. Будь яка інформація зараз у більшості випадків передається через мережу. Тому актуальність цих пристроїв завжди є на вищому рівні. Згідно із потреб бізнесу, комутаційні пристрої поділені на сегменти: малий бізнес, середній бізнес та Enterprise. В свою чергу кожен сегмент має свої аспекти та правила налаштування пристроїв комутації. А кожен пристрій комутації має різні рівні апаратного та програмного забезпечення, для гарантування безпеки даних.

Список використаних джерел

1. Портал Cisco, Правильний вибір комутаторів для вашого бізнесу \\ Режим доступу: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/understanding-the-different-types-of-network-switches.html (останнє звернення 02.04.2023)
2. Портал Aruba Networks, AOS-CX Monitoring Guide \\ Режим доступу: https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/monitoring_83xx.pdf (останнє звернення 04.04.2023)
3. Публікація Linkedin, Dinusha Madusanka Chandrasinghe System Engineer у Zone24x7, Запуск автоматизації комутатора з Python \\ Режим доступу: https://www.linkedin.com/pulse/start-automation-arubaos-cx-switch-python-chandrasinghe (останнє звернення 21.03.2023)

Робота виконана під науковим керівництвом, доцента
ДЕСЯТКО А.М.

АНАЛІЗ ПІДХОДІВ ДО ВИЯВЛЕННЯ РОСІЙСЬКИХ СЛІВ В УКРАЇНСЬКИЙ ВЕБДОДАТКАХ

ЛАВРІНЕНКО В., 2мз курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

В статті проаналізовано сучасні принципи створення інформаційної системи для виявлення російських слів, у вебдодатках. Розглянуто створення інформаційної-системи та використання готових рішень. Зазначено переваги та недоліки методів виявлення російських слів.

The article discusses modern principles of creating an information system for detecting Russian words in web applications. The creation of an information system and the use of ready-made solutions are considered. The advantages and disadvantages of methods for detecting Russian words are noted.

Актуальність. Згідно з законом «Про забезпечення функціонування української мови як державної» всі українські вебресурси повинні використовувати українську мовну версію. Якщо українська версія вебресурсу відсутня, її необхідно створити. За відсутності української мовної версі, з 16 червня 2022 року передбачається штраф в розмірі від 3400 до 7500 грн, сума штрафу залежить від багатьох чинників, таких як кількість порушень, то що. Якщо вебресурс не відреагує, та не приділить вирішення цьому питанні свій час, повторний штраф буде сягати в розмірі 7500 грн до 11900 грн, інформація актуальна на час написання цієї статті. Даний закон впливає на бізнес, та має на мету забезпечення і захист мовних прав та потреб українців, української мови, зокрема, забезпечення її використання в усіх сферах життя, включаючи офіційне спілкування, освіту, науку та культуру. Забезпечувати доступність та якість мовної освіти, а також розвивати мовну культуру серед населення.

Метою статті є дослідження використання різних методів, для створення антоматизованої інформаційної системи для виявлення російських слів, в українських вебдодатках.

Об'єктом дослідження є процес виявлення російських слів в українських вебдодатках.

Предмет дослідження – підходи, методи та інструменти, які можуть бути використані для ефективного виявлення російських слів в українських вебдодатках.

Аналіз попередніх досліджень. Демонструє що багато вебдодатків, розроблених в Україні, містять російські слова, що порушує мовні права українців і може призвести до отримання штрафів, втрати національної ідентичності. Для виявлення таких слів використовують різні методи та інструменти, які потребують подальшого дослідження та удосконалення.

Для виявлення російських слів в українських вебдодатках існує кілька підходів, кожен з яких має свої переваги та недоліки. Один з таких підходів – це використання морфологічного аналізу. Цей метод ґрунтується на аналізі граматичних ознак слова, таких як час, кількість, рід тощо. Використання морфологічного аналізу дозволяє виявляти російські слова, які були написані українськими літерами.

Цей метод ґрунтується на аналізі морфологічних характеристик слів, таких як закінчення, префікси та суфікси:

- Порівнювати закінчення слів української та російської мов, оскільки вони часто відрізняються одне від одного.
- Під час морфологічного аналізу слово розбивається на основу та закінчення, після чого проводиться перевірка основи на належність до української або російської мови. Слова, які мають російську основу та українське закінчення, можуть бути віднесені до російської мови.

- Аналіз префіксів та суфіксів, які можуть бути специфічні для російської мови. Наприклад, російське слово "перервати" має префікс "пере-", який не використовується в українській мові. Таким чином, якщо слово містить російський префікс або суфікс, то це може вказувати на його походження.
- Використання списку ключових слів з російської мови. Наприклад, такий список може включати такі слова, як "россия", "москва", "рубль", "кремль", "путин" тощо. Після того, як список ключових слів складено, можна провести пошук цих слів у тексті сторінки. При цьому варто враховувати не лише точне співпадіння слів, але й їх форми - наприклад, російське слово "москва" може зустрічатися у формі "Москви", "Москві", "Москвою" тощо.
- Використання програмного забезпечення, яке виконує автоматичний аналіз тексту і визначає мову, до якої він належить.

Інший підхід полягає в застосуванні статистичного аналізу тексту. Цей метод базується на виявленні частоти вживання певних слів і виразів у тексті. Використання статистичного аналізу дозволяє виявляти російські слова, які були написані кирилицею. Один із методів є використання навчальної вибірки текстів, що містять російські та українські слова, для побудови статистичних моделей. Далі ці моделі можна використовувати для визначення ймовірності того, що дане слово є російським. За допомогою цього методу можна виявляти російські слова в українських текстах, навіть якщо вони були додані в текст з помилкою або намірено змінені.

- Розрахунку відсотку вживання російських слів в тексті в порівнянні з українськими словами. Наприклад, якщо відсоток вживання російських слів перевищує певний поріг, можна вважати, що текст містить російський контент.
- Використання біграм для виявлення російських слів. Біграми називаються пари слів, які зустрічаються разом у тексті. За допомогою статистичного аналізу можна визначити, які біграми є типовими для російської мови, і використовувати ці знання для виявлення російських слів у тексті..
- Аналіз контексту для виявлення російських слів. Наприклад, якщо слово часто зустрічається поряд з російськими словами, ймовірно, що воно також є російським.
- Метод TF-IDF. Цей метод дозволяє визначити ступінь важливості певного слова в тексті, порівнюючи його частоту в тексті з частотою використання цього слова в інших текстах. Якщо слово зустрічається рідко в інших текстах, але досить часто в конкретному тексті, то це свідчить про те, що це слово є важливим для розуміння змісту цього тексту.
- Використання алгоритму машинного навчання, який навчається розпізнавати певні ознаки російської мови в тексті, наприклад, наявність специфічних закінчень слів, використання певних словосполучень чи граматичних форм.

Всі ці методи можна поєднувати між собою та з іншими підходами, такими як морфологічний аналіз та інші методи машинного навчання, для досягнення більш точного виявлення російських слів в українських вебдодатках.

В розробці дуже важкі умови, програма має працювати та відповідати критеріям, розробка повинна супроводжуватись документацією, а спеціалісти мають відповідати критеріям. Умови мають бути написані зрозумілі, і завдання які будуть виникати повинні виконуватись в відповідні строки. Розробка автоматизованої системи пошуку російських слів, має починатись зі зрозумілих умов, та призначені самої системи. На даний час та в майбутньому виникає потреба в розробці автоматизованої системи пошуку російських слів в українських вебдодатках. Така система має бути достатньо ефективною та точною, щоб забезпечити максимальний захист мовних прав громадян та виконання законодавства. Автоматизована система пошуку російських слів може використовувати різні методики, наприклад ті що було описані вище.

Автоматизовані системи пошуку слів використовуються в різних сферах, наприклад, в комп'ютерних програмах для обробки текстів, в пошукових системах Інтернету, в системах розпізнавання мови тощо. Ось декілька прикладів автоматизованих систем пошуку слів:

- Пошукові двигуни в Інтернеті, такі як Google, використовують різні алгоритми для пошуку та відображення результатів. Одним з таких алгоритмів є алгоритм TF-IDF (term frequency–inverse document frequency), який визначає важливість кожного слова в тексті, враховуючи частоту вживання слова в тексті та частоту вживання слова в інших документах.
- Програми для обробки текстів, такі як Microsoft Word, можуть автоматично підсвічувати слова, які використовуються надто часто або надто рідко. Такі програми також можуть автоматично відображати синоніми для вибраних слів, що полегшує процес написання тексту.
- Системи розпізнавання мови, такі як Siri від Apple, використовують алгоритми для розуміння мовлення користувача та відповіді на його запити. Для цього системи використовують навчальні моделі, які навчаються розпізнавати та інтерпретувати різні слова та фрази.

Розглянемо приклад використання морфологічного аналізу для виявлення російських слів. Один з прикладів використання морфологічного аналізу для виявлення російських слів на вебсайтах є програмний засіб LanguageTool (Рис.1).

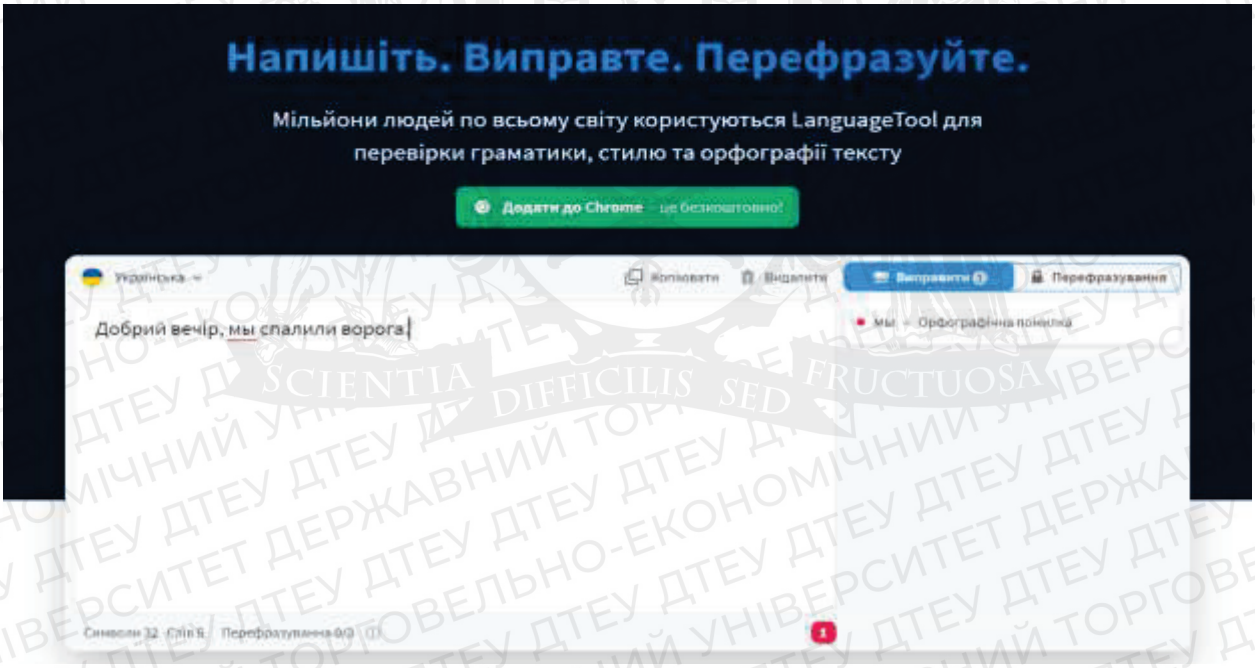


Рис. 1. Інтерфейс вебдодату Language Tool

LanguageTool дозволяє перевіряти текст на наявність помилок, в тому числі й російських слів. LanguageTool використовує морфологічний аналіз для визначення мови слів та їхньої орфографії.

Другий приклад полягає в використання морфологічного аналізу програмного засобу Hunspell, що дозволяє проводити перевірку правопису тексту на основі словника та правил морфології різних мов. У налаштуваннях Hunspell можна вказати список мов в тому числі українську, які повинні бути використані для перевірки тексту, та налаштувати правила перевірки правопису. Hunspell — це засіб перевірки орфографії LibreOffice, OpenOffice.org, Mozilla Firefox і Thunderbird, Google Chrome, а також використовується пакетами пропрієтарного програмного забезпечення, такими як macOS, InDesign, memoQ, Opera і SDL

Trados. Основні можливості. Розширена підтримка мовних особливостей; Кодування символів Unicode, складення та складна морфологія.

Рис. 2. Інтерфейс Hunspell

Покращена пропозиція з використанням схожості n-грам, даних про вимову на основі правил і словника. Hunspell базується на MySpell і також працює зі словниками MySpell. Бібліотека C++ під триліцензією GPL/LGPL/MPL. Інтерфейси та порти: AndroidHunspellService (для Android, на основі форка Chromium Hunspell), Enchant (загальна бібліотека орфографії з проєкту Abiword), XSpell (порт macOS, але Hunspell є частиною macOS з версії 10.6 (Snow Leopard) і тепер достатньо помістити файли словника Hunspell у ~/Library/Spelling або /Library/Spelling для перевірки орфографії), Delphi, Java (JNA, JNI), Perl, .NET, .NET Standard, Python, Ruby (1, 2, 3), UNO, RichEdit. Переклади: Hunspell було перекладено кількома мовами.

Наступна програма з застосуванням морфологічного аналізу для пошуку російських слів на вебсайтах є розробка програми мовою програмування Python з використанням бібліотеки Natural Language Toolkit (NLTK). Ця програма може виявляти російські слова на вебсторінках, використовуючи морфологічний аналіз. Програма спочатку завантажує текст сторінки, а потім проводить морфологічний аналіз кожного слова у тексті. Якщо слово має російську морфологію, то воно додається до списку російських слів. Ще одним прикладом застосування морфологічного аналізу є розробка системи автоматичного виявлення російських слів на вебсайтах з використанням відкритих даних WordNet. Ця система використовує WordNet для знаходження синонімів російських слів. Після отримання списку синонімів, система проводить морфологічний аналіз кожного слова та видаляє слова, які не є російськими. Для розробки автоматизованої системи пошуку російських слів на вебсайтах можна використовувати різні програмні засоби та бібліотеки морфологічного аналізу, такі як Mystem, Pymorphy2, NLTK та інші.

Розглянемо приклади використання статистичного аналізу для виявлення російських слів. Статистичного аналіз пошуку російських слів на сайтах полягає у виявленні російських слів шляхом аналізу тексту сторінки без необхідності виконання запитів до бази даних або зовнішніх ресурсів. Цей метод зазвичай використовується для оцінки мовної ситуації на вебсайтах, а також для виявлення потенційно небезпечного контенту, що може містити пропаганду агресивних чи ворожих до України інтересів. Прикладом є програма YARA, яка є відкритою системою виявлення шаблонів для пошуку специфічних рядків у тексті. Вона може

використовуватися для пошуку російських слів та інших специфічних виразів на вебсайтах. Також можна використовувати спеціальні скрипти або програми, які виконують статистичний аналіз HTML-коду вебсторінок для пошуку російських слів та інших специфічних виразів. Один з прикладів такої програми - grep, який є утилітою командного рядка в UNIX-подібних операційних системах.

- Інструмент Ahrefs: Ahrefs є платним інструментом SEO-аналізу, який може бути використаний для виявлення російських слів на вебсторінках. Це робиться за допомогою функції Content Explorer, яка дозволяє ввести URL-адресу вебсторінки і отримати список всіх слів на сторінці, разом з інформацією про їх частоту вживання та контекст вживання.
- Інструмент Diffbot: Diffbot - це API, яке надає доступ до структурованої інформації з вебсторінок. Цей інструмент може бути використаний для отримання списку всіх слів на вебсторінці, а також для відфільтрування російських слів за допомогою регулярних виразів або мовних аналізаторів.
- Сайт-аналізатор Ahrefs - платформа для вивчення та аналізу SEO-показників вебсайту. Для аналізу слів на сайті, можна використовувати інструмент "Site Explorer", який надає статистику по кількості слів та фраз на сайті, а також їх розташування на сторінках.
- Консоль розробника браузера - це інструмент, який надається у браузері для дебагу вебсайтів. Вона може бути використана для відстеження різних аспектів вебсторінок, включаючи використання слів.
- Власноруч написана програма - програмування статистичного аналізу для виявлення слів можна виконати самостійно з використанням різних мов програмування та бібліотек, таких як Python, Java, JavaScript тощо.

Розглянемо відмінності та різницю в підходах статистичного аналізу, та морфологічного в пошуку російських слів. Статистичний та морфологічний аналіз - це дві різні методи, які можуть використовуватися для пошуку російських слів на вебдадатках. Морфологічний аналіз базується на збігу морфологічної форми слів. Це означає, що програма виявлятиме російські слова, незалежно від того, як вони написані - у відмінкових формах, зі зміненою закінченням чи зі складними похідними словами. Статистичний аналіз використовує інший підхід - він базується на виявленні конкретних слів або фраз, що відповідають певним шаблонам. Наприклад, можна створити список слів або фраз, що зазвичай вживаються у російській мові, і потім знайти їх на сайті. Такий підхід може бути менш точним, оскільки існує можливість пропустити деякі російські слова, які не входять до списку, або знайти слова, які не мають російського походження, але збігаються з шаблоном. Обидва підходи можуть бути корисними для виявлення російських слів на сайтах, але їх ефективність залежить від конкретної ситуації та використовуваної методології.

Проаналізуємо які варіанти продукту вибере кінцевий користувач або бізнес. А саме готове рішення програму для пошуку російський слів у вебдодатках, або написання своєї власної програми. Використання готових програм для виявлення російських слів в українських вебдодатках може бути ефективним та зручним варіантом для користувачів, які не мають досвіду у програмуванні. Готові програми зазвичай мають зроблену значну частину роботи, таку як написання алгоритму виявлення слів, розробку інтерфейсу користувача та відлагодження програми. Однак, написання своєї програми має свої переваги. Зокрема, це дозволяє точніше налаштувати алгоритм виявлення слів під конкретні потреби користувача. Також, при розробці власної програми користувач може бути впевнений у безпеці та конфіденційності своїх даних. Розглянемо основні різниці між використанням готових програм та написанням своєї програми для виявлення російських слів в українських вебдодатках:

- Розробка: для написання власної програми потрібно мати знання з програмування та мати достатньо часу для розробки та відлагодження програми. Готові програми можна встановити та використовувати без необхідності розробки.

- Налаштування: написання власної програми дозволяє точніше налаштувати алгоритм виявлення слів під конкретні потреби користувача. Готові програми можуть мати обмежені налаштування та можуть не задовольняти потребам користувача.
- Вартість: використання готових програм зазвичай коштує гроші, тоді як написання власної програми може бути безкоштовним.
- Безпека та конфіденційність: написання власної програми дозволяє користувачеві бути впевненим у безпеці.

Можемо зробити висновок що остаточний вибір за користувачем або компанією, тому що ситуації різні, та підходи в виборі. Але вибір повинен відповідати вимогам, повністю, або хоч би частково.

Висновки. Виявлення російських слів на українських вебсайтах є актуальною проблемою, особливо в контексті бізнесу, та боротьби з інформаційною агресією. Для виявлення російських слів на українських вебсайтах можна використовувати як морфологічний аналіз, так і статистичний аналіз. Готові програми для виявлення російських слів на українських вебсайтах можуть бути корисним інструментом для розв'язання даної проблеми. Проте, написання своєї програми для виявлення російських слів може бути більш ефективним варіантом, оскільки дозволяє більш гнучко налаштувати алгоритм під конкретні потреби користувача. Оскільки виявлення російських слів на українських вебсайтах є складною задачею, необхідно розвивати та вдосконалювати існуючі методи і інструменти для її вирішення.

Список використаних джерел

1. Шуба М. О. (2018) Підходи до виявлення російських слів в українських вебдодатках, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)
2. LanguageTool – Перевірка граматики, стилю та орфографії онлайн URL: https://languagetool.org/uk
3. Hunspell dictionaries in Studio. URL: https://multifarious.filkin.com/2018/10/31/hunspell-dictionaries-in-studio/
4. Ahrefs – SEO Tools & Resources To Grow Your Search Traffic URL: https://ahrefs.com/
5. Diffbot Knowledge Graph, AI Web Data Extraction and Crawling URL: https://www.diffbot.com/
6. YARA – The pattern matching swiss knife for malware researchers URL: https://virustotal.github.io/yara/
7. Харченко В. (2017) Виявлення російської мови на українських сайтах за допомогою регулярних виразів. Видавництво Springer серія Communications in Computer and Information Science Том 711.
8. Швець А., Василенко В., Кулик О. (2019) Виявлення російської мови в українському вебпросторі за допомогою регулярних виразів. Соловйов В., Харченко В., Кривінська Н. (ред.) Інженерія перспективних інформаційних систем. CAiSE 2019. Конспекти лекцій з обробки бізнес-інформації, том 353.
9. Манжелій Ю. І., Качмар М. М. Автоматичне виявлення російських слів у текстах українською мовою з використанням засобів морфологічного аналізу. Вісник Хмельницького національного університету. https://core.ac.uk/download/pdf/268531695.pdf
10. Гарбера, І.В. Прикладна морфологія: основи автоматичного морфологічного аналізу тексту: Навчально-методичний посібник. https://r.donnu.edu.ua/handle/123456789/2418

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н.О.

ОСНОВНІ ВИМОГИ ДО ПРОГРАМНОЇ КОМПОНЕНТИ ДЛЯ ЗАБЕЗПЕЧЕННЯ РОБОТИ СТРУКТУРНОГО ПІДРОЗДІЛУ ГОТЕЛЬНОГО ГОСПОДАРСТВА

ЛЕЛЕТІНА Є., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Даний дослід присвячений визначенню основних вимог до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства. В статті проаналізовано технічні та функціональні вимоги до програмної компоненти, а також відмічені проблеми, які можуть виникнути при розробці та впровадженні програмного забезпечення в готельний бізнес. Було проведено порівняння різних програмних продуктів та методів їх впровадження з метою вибору оптимального рішення для структурного підрозділу готельного господарства. Дослідження також включало розгляд аспектів безпеки та моніторингу роботи програмної компоненти.

This study is dedicated to determining the main requirements for a software component that provides the operation of the structural unit of hotel management. The article analyzes technical and functional requirements for the software component, as well as identifies issues that may arise during the development and implementation of software in the hotel industry. A comparison of different software products and methods of their implementation was carried out in order to choose the optimal solution for the structural unit of hotel management. The research also included consideration of aspects of security and monitoring of the software component.

Актуальність. Зараз готельний бізнес розпочинає поступово відновлюватися після пандемії та в умовах воєнного стану. Зростання попиту на готельні послуги вимагає від підприємств готельного господарства ефективного використання ресурсів та автоматизації процесів управління. У зв'язку з цим, програмне забезпечення для готелів стає все більш популярним.

Однак, розробка та впровадження програмного забезпечення в готельний бізнес можуть викликати ряд проблем, пов'язаних з вимогами до програмної компоненти. Ці вимоги можуть бути технічними та функціональними. Технічні вимоги стосуються апаратної та програмної частини комп'ютерного обладнання, на якому буде запущена програмна компонента, а також мережевих можливостей. Функціональні вимоги стосуються можливостей програмної компоненти та її інтеграції з іншими системами готельного бізнесу.

Об'єктом нашої статті є програмна компонента забезпечення роботи структурного підрозділу підприємств готельного господарювання.

Метою даного дослідження є визначення основних вимог до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства. Для досягнення цієї мети було поставлено наступні *завдання*:

- проаналізувати технічні та функціональні вимоги до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства;
- визначити основні проблеми, які можуть виникнути при розробці та впровадженні програмного забезпечення в готельний бізнес;
- провести порівняння різних програмних продуктів та методів їх впровадження з метою вибору оптимального рішення для структурного підрозділу готельного господарства;
- розглянути аспекти безпеки та моніторингу роботи програмної компоненти.

У програмній компоненті для структурного підрозділу готельного господарства мають бути враховані технічні вимоги, пов'язані з апаратним забезпеченням та мережевими можливостями.

Один з головних параметрів апаратного забезпечення, що впливає на швидкість роботи програмної компоненти, є процесор. Найбільш оптимальним варіантом для запуску програмної компоненти є процесор з такими характеристиками: кількість ядер - не менше 4; тактова частота - не менше 2,5 ГГц; кеш - не менше 8 Мб. Також важливим параметром є обсяг оперативної пам'яті (ОЗУ), який повинен бути не менше 8 Гб.

Однак, не менш важливими є мережеві можливості, оскільки програмна компонента повинна мати змогу працювати в мережевому середовищі, щоб мати доступ до інших систем готельного бізнесу. Тому, необхідно встановити на комп'ютер програмне забезпечення для мережевого з'єднання.

Функціональні вимоги стосуються можливостей програмної компоненти та її інтеграції з іншими системами готельного бізнесу. Основні функції програмної компоненти повинні включати:

- резервування номерів готелю;
- прийом та обробка заявок на бронювання номерів;
- розрахунок вартості проживання;
- облік фінансових операцій;
- формування звітів та аналітики.

Також, програмна компонента повинна бути інтегрована з іншими системами готельного бізнесу, наприклад, з системою керування запасами, щоб забезпечити своєчасну доставку необхідних ресурсів, або з системою контролю доступу, щоб забезпечити безпеку проживання гостей.

Розробка та впровадження програмної компоненти для структурного підрозділу готельного господарства може стикнутися з рядом проблем. Одна з найбільш значущих проблем - це складність інтеграції програмної компоненти з іншими системами готельного бізнесу. Ця проблема може виникнути через відмінність форматів та структури даних.

Іншою проблемою може стати відсутність відповідного кваліфікованого персоналу для впровадження та підтримки програмної компоненти. Це може призвести до збільшення витрат на навчання персоналу та на залучення зовнішніх консультантів.

Також важливою проблемою є забезпечення безпеки даних, оскільки програмна компонента зберігає конфіденційну інформацію про клієнтів готелю. Для забезпечення безпеки даних необхідно застосовувати захист інформації за допомогою шифрування та автентифікації.

Після розробки програмної компоненти необхідно провести тестування та валідацію, щоб переконатися в правильному функціонуванні компоненти та відповідності її вимогам. Для цього можна використовувати такі методи:

- функціональне тестування;
- тестування на відповідність вимогам;
- тестування на продуктивність;
- тестування на надійність.

Розробка програмної компоненти для структурного підрозділу готельного господарства є важливим завданням, оскільки вона дозволяє автоматизувати процеси бронювання номерів, розрахунку вартості проживання та обліку фінансових операцій. Однак, для успішної реалізації проекту необхідно врахувати вимоги до апаратного та програмного забезпечення, а також вирішити проблеми, пов'язані з інтеграцією компоненти з іншими системами готельного бізнесу, забезпеченням безпеки даних та підготовкою персоналу.

Тестування та валідація програмної компоненти - важливий етап в розробці програмної компоненти, який дозволяє переконатися в правильному функціонуванні компоненти та відповідності її вимогам. Для успішної розробки та впровадження програмної компоненти для структурного підрозділу готельного господарства необхідно дотримуватися певних етапів розробки та тестування, а також враховувати вимоги до апаратного та програмного забезпечення.

Важливими аспектами для успішного впровадження програмної компоненти є відповідність бізнес-процесам готельного господарства, безпека даних, можливість інтеграції з іншими системами та зручний інтерфейс користувача.

На основі проведеного аналізу та порівняння існуючих рішень для автоматизації роботи готелів було визначено, що найбільш ефективною є інтегрована програмна платформа, що включає в себе різні модулі для автоматизації різних бізнес-процесів готельного господарства, таких як бронювання номерів, облік послуг та продуктів, управління персоналом та інше.

Для забезпечення безпеки даних необхідно застосовувати заходи, такі як шифрування, резервне копіювання та забезпечення захисту доступу до системи. Також важливим аспектом є можливість інтеграції програмної компоненти з іншими системами, такими як системи електронного документообігу та системи обліку витрат.

Зручний інтерфейс користувача є важливим фактором успішного використання програмної компоненти. Необхідно забезпечити зручний та інтуїтивно зрозумілий інтерфейс для користувачів різних рівнів кваліфікації та досвіду роботи з комп'ютером.

Схема взаємодії програмної компоненти з іншими системами та базами даних може виглядати наступним чином:

1. Користувачі взаємодіють з програмною компонентою через веб-інтерфейс, що забезпечує взаємодію з додатком на веб-сервері.
2. Програмна компонента взаємодіє з базою даних, що містить інформацію про персонал готелю, зокрема список працівників і їхні робочі графіки.
3. Програмна компонента взаємодіє з системою електронної пошти для надсилання листів повідомлень про робочі графіки із змінами співробітникам.
4. Програмна компонента може взаємодіяти з системою електронної оплати, щоб оплачувати заробітну плату співробітникам.
5. Програмна компонента може взаємодіяти з системою бронювання готелів, щоб забезпечити інформацію про наявність вільних номерів та розміщення гостей в номерах.
6. Програмна компонента може взаємодіяти з системою контролю доступу, щоб забезпечити безпеку та обмежити доступ до певних приміщень для співробітників і гостей готелю.
7. Програмна компонента може взаємодіяти з системою відеоспостереження, щоб забезпечити безпеку на території готелю та контролювати дотримання правил працівниками та гостями.
8. Програмна компонента може взаємодіяти з системою обліку запасів і забезпечення готелю, щоб забезпечити своєчасне поповнення запасів та підтримання оптимального рівня запасів.
9. Крім того, програмна компонента може інтегруватись з системою онлайн-бронювання, щоб автоматично оновлювати інформацію про наявність номерів та їх ціни на веб-сайті готелю. Це значно спростить процес бронювання та зменшить ризик помилкових бронювань.
10. Нарешті, програмна компонента може забезпечувати гостьовий портал, на якому гості зможуть отримувати необхідну інформацію про готель та його послуги, здійснювати онлайн-замовлення послуг та розваг, а також зв'язуватись з адміністрацією готелю. Це підвищить рівень комфорту для гостей та зменшить навантаження на персонал готелю.

Однією з важливих складових програмної компоненти є система звітності, яка дозволяє отримувати різноманітну статистику і звіти щодо роботи структурного підрозділу готельного господарства. Система звітності взаємодіє з базою даних компоненти, а також може взаємодіяти з системами зберігання даних або відправлення звітів електронною поштою.

Програмна компонента для структурного підрозділу готельного господарства має бути розроблена з врахуванням вимог до її архітектури та функціональності, а також забезпечувати високу надійність та безпеку даних. Для успішної реалізації проекту також необхідно врахувати вимоги до апаратного та програмного забезпечення, а також вирішити проблеми,

пов'язані з інтеграцією компоненти з іншими системами готельного бізнесу, забезпеченням безпеки даних та підготовкою персоналу.

Для успішної реалізації проекту необхідно використовувати сучасні методи та інструменти розробки програмного забезпечення, такі як Agile-методології, DevOps-підходи, контроль версій та автоматизоване тестування.

Вибір архітектури програмної компоненти є ключовим етапом в процесі розробки програмного забезпечення. Архітектура повинна відповідати вимогам продукту та принципам проектування програмного забезпечення.

При виборі архітектури програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства було враховано такі фактори:

1. Вимоги до функціональності: програмна компонента повинна забезпечувати можливість бронювання номерів, розрахунку вартості послуг, створенню звітів, підтримки бази даних клієнтів та персоналу готелю.
2. Вимоги до продуктивності: програмна компонента повинна забезпечувати швидку обробку запитів та ефективне використання ресурсів системи.
3. Принципи проектування ПЗ: програмна компонента повинна бути забезпечена високою модульністю, масштабованістю та гнучкістю.

Враховуючи ці фактори, оптимальною є клієнт-серверна архітектуру. Клієнтська частина забезпечує інтерфейс користувача та взаємодію з сервером, а серверна частина забезпечує доступ до бази даних та обробку запитів.

Така архітектура є популярною та має декілька переваг. Клієнтська частина може бути реалізована на різних платформах, що забезпечує більшу гнучкість та доступність для користувачів. Крім того, серверна частина може бути масштабована, що забезпечує підтримку більшого обсягу запитів.

Вибір архітектури програмної компоненти здійснюється з урахуванням вимог до функціональності, продуктивності та простоти системи. Також потрібно враховувати принципи проектування ПЗ, такі як розширюваність, модульність та зручність тестування. В результаті аналізу різних варіантів, можна стверджувати, що найкраще використовувати мікросервісну архітектуру, що дозволяє розділити систему на окремі сервіси, що функціонують незалежно один від одного та забезпечують більшу гнучкість та масштабованість системи. Така архітектура також сприяє зменшенню залежностей між компонентами та полегшує розгортання та підтримку системи.

Архітектура мікросервісів дозволяє розділити систему на невеликі, незалежні модулі - мікросервіси, кожен з яких відповідає за свою функціональність та може бути розгорнутий та масштабований окремо. Це дозволяє досягти більшої гнучкості та швидкості розробки та розгортання, а також покращує можливості масштабування та забезпечує високу доступність системи.

Крім того, мікросервісна архітектура підтримує розподілений розвиток, що дозволяє розробникам працювати паралельно над різними частинами системи та підтримувати їх незалежність. Також, ця архітектура дозволяє легко замінювати та розширювати окремі мікросервіси без впливу на роботу інших частин системи.

У контексті програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства, мікросервісна архітектура дозволить розділити систему на окремі модулі, що відповідають за різні функції, такі як бронювання номерів, ресторанна служба, облік фінансів тощо. Кожен мікросервіс може мати свою власну базу даних, що сприяє відокремленості та безпеці даних.

Застосування мікросервісної архітектури також дозволить підвищувати масштабованість системи, що є критичним для розвитку бізнесу. Крім того, використання мікросервісів дозволить зменшити залежність між різними компонентами системи та спростити процес розгортання та моніторингу окремих сервісів. В результаті, вибір мікросервісної архітектури допоможе забезпечити більш високу гнучкість, масштабованість, надійність та продуктивність програмної компоненти.

Одним з головних викликів при розробці програмної компоненти для структурного підрозділу готельного господарства є забезпечення її інтеграції з іншими системами готельного бізнесу, такими як система бронювання номерів, система обліку фінансів та система управління ресурсами. Для успішної інтеграції необхідно визначити стандарти та протоколи комунікації між компонентами та забезпечити взаємодію з системами, які вже використовуються в готелі.

Крім того, врахування вимог до безпеки даних є критичним аспектом при розробці програмної компоненти для готельного бізнесу. Забезпечення конфіденційності, цілісності та доступності даних є ключовими вимогами до програмного забезпечення готельного господарства. Для досягнення цієї мети необхідно використовувати шифрування, аутентифікацію та авторизацію, а також резервне копіювання даних та моніторинг безпеки.

Розробка програмної компоненти для структурного підрозділу готельного господарства є складним та відповідальним завданням, яке потребує уважного вивчення вимог до функціональності та безпеки даних, використання сучасних методів та інструментів розробки програмного забезпечення та інтеграції з іншими системами готельного бізнесу. Для успішної реалізації проекту необхідно визначити та проаналізувати потреби та вимоги клієнтів та користувачів, а також розробити ефективну стратегію тестування та впровадження програмної компоненти. Дотримання всіх цих критеріїв дозволить досягти високої якості та ефективності роботи структурного підрозділу готельного господарства.

В цілому, розробка програмної компоненти для структурного підрозділу готельного господарства є складним та відповідальним завданням, але за дотриманням всіх вимог та рекомендацій може бути успішно реалізована. Така компонента допоможе підвищити ефективність та якість обслуговування гостей, знизити витрати та покращити управління готельним бізнесом в цілому. Для того, щоб досягти успіху, необхідно забезпечити високу якість програмного забезпечення, а також забезпечити його безпеку та надійність.

Висновки У цій статті ми дослідили основні вимоги до програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства. Зокрема, ми розглянули такі вимоги, як підтримка різноманітних функцій готельної діяльності, надійність та безпека, зручність та ефективність використання, можливість інтеграції з іншими системами, масштабованість та гнучкість.

В цілому, розробка програмної компоненти для забезпечення роботи структурного підрозділу готельного господарства є важливим кроком у покращенні ефективності та якості обслуговування гостей готелю. З використанням сучасних методів та інструментів розробки програмного забезпечення, можна створити надійну та ефективну систему, яка забезпечить успішну діяльність готелю та задоволення потреб клієнтів.

Список використаних джерел

1. Liu, Y., & Chen, C. A service quality evaluation model for hotel online booking systems. Journal of Hospitality and Tourism Technology, №7(2),-2016.- 168-183. doi: 10.1108/JHTT-06-2015-0025
2. Горбачук, В. Використання програмного забезпечення у готельному господарстві. Технології та дизайн,№ 4(32),-2019- С.51-55.
3. Павленко, О. Розробка програмного забезпечення для автоматизації роботи готельного бізнесу. Молодий вчений, №3(35),-2016-С.186-189.
4. Ходаківська, Ю.. Застосування програмного забезпечення у готельному бізнесі. Економічний часопис-XXI, №3-4(2),-2019-С.64-68.

Робота виконана під науковим керівництвом к.е.н., доцента
ТИЩЕНКА Д.О.

ПРОГРАМНО-АПАРАТНІ ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ЛІЩУК О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні програмно-апаратні засоби криптографічного захисту інформації, зокрема принципи роботи симетричного та асиметричного шифрування на прикладі шифрів AES та RSA, а також вітчизняного шифру «Калина». Зазначено переваги використання базових принципів стеганографії для захисту інформації від несанкціонованого доступу.

The article discusses the main software and hardware tools for cryptographic protection of information, in particular, the principles of symmetric and asymmetric encryption on the example of AES and RSA ciphers, as well as the national cipher "Kalyna". The advantages of using the basic principles of steganography to protect information from unauthorized access are noted.

Актуальність. У всі часи інформація була важливим ресурсом, і володіння достовірною та актуальною інформацією завжди давало перевагу одній зі сторін. Проблема захисту інформації виникла на зорі зародження людського суспільства, і актуальність цієї проблеми з кожним днем все зростала. Уже сьогодні людство ступило на новий етап свого розвитку − перехід до нового типу постіндустріального суспільства, де головну роль відіграє інформація. Паралельно з прогресом у сфері інформаційних технологій постійно збільшується і кількість можливих загроз, починаючи від технічних несправностей і закінчуючи діями зловмисників. Постійне збільшення обсягу конфіденційної інформації, широке використання різноманітних технічних засобів для її оброблення, зберігання та передавання, поява нових методів і засобів несанкціонованого доступу до інформації потребують відповідні програмно-апаратні комплекси у сфері криптографічного захисту інформації.

Характерною рисою сучасного суспільства є той факт, що інформація являє собою один із найважливіших ресурсів, а засоби її обробки та зберігання використовуються практично в усіх сферах нашої діяльності − від забезпечення національної безпеки та охорони здоров'я до купівель через інтернет і звичайного спілкування. Постійно збільшується кількість людей, зайнятих виробництвом і споживанням інформації, дедалі більше зростає значущість знань і частка розумової праці. Найостанніші досягнення людства в галузі ІТ активно використовуються в нашому повсякденному житті, і з кожним днем збільшується частка інформаційних технологій у житті суспільства. Цей соціальний і технологічний процес, що є основною движучою силою сучасного суспільства, називається «інформатизація».

Таким чином, людство вже на даному етапі свого розвитку залежить від інформації та інформаційних технологій, що забезпечують її зберігання, обробку та поширення. Тому проблема забезпечення захищеності інформації та інформаційних систем є однією з найважливіших проблем сучасності.

Метою статті є ознайомлення з методами захисту інформації від несанкціонованого доступу, зокрема використання програмно-апаратних засобів криптографічного захисту інформації, а також вивчення стандартів шифрування.

Об'єктом дослідження є дослідження програмно-апаратних засобів захисту інформації та принципів роботи деяких стандартів симетричного та асиметричного шифрування.

Предмет дослідження – програмно-апаратні засоби криптографічного захисту інформації.

Аналіз попередніх досліджень. Дослідженню програмно-апаратних засобів захисту інформації та питанням інформаційної безпеки присвячені праці вітчизняних та закордонних

вчених: Тагер Ель-Ґамаля, Ю.Я. Бобало, Б.А. Бабаяна, М.Д. Кіселичника, А.П. Бондарєва, С.С. Войтусіка, А.Я. Горпенюка, Є.І. Яковенко, В.І. Отенко, І.Я. Тишика та ін.

Виклад основного матеріалу. Сукупністю методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації є захист інформації. Для його забезпечення, сьогодні, використовуються засоби захисту інформації та інформаційних систем, реалізованих на апаратному та програмному рівнях. Важливо зазначити, що організаційні, технологічні й апаратні методи захисту, як правило, не можуть бути здійснені без програмної складової, тому захист інформації досягається реалізацією програмних і апаратних засобів разом.

Найпоширенішими прикладами програмних засобів захисту інформації є такі:

- система контролю і управління доступом;
- антивірусне програмне забезпечення;
- шифрувальне програмне забезпечення;
- мережевий екран або брандмауер;
- система виявлення вторгнень (IDS).

На сьогодні шифрування широко застосовують у комп'ютерній техніці для приховування конфіденційної інформації від несанкціонованого використання і для захищеної передачі інформації між різними елементами інформаційної системи. Існує два основних типи алгоритмів шифрування, заснованих на ключах: симетричні та асиметричні, які називаються алгоритмами із закритим і алгоритмами з відкритим ключем.

Симетричні алгоритми являють собою криптографічні алгоритми, у яких ключ шифрування може бути розрахований за ключем дешифрування і навпаки (Рис. 1). У більшості симетричних алгоритмів ключі шифрування і дешифрування одні й ті самі. Такі алгоритми вимагають, щоб відправник і одержувач узгодили ключ, що використовується, перед початком зашифрованої передачі повідомлень. Безпека симетричного алгоритму визначається ключем, розкриття якого означає, що будь-хто зможе прочитати зашифровані повідомлення.

Схема симетричного шифрування має п'ять компонентів:

- Відкритий текст: це оригінальне повідомлення або дані, які подаються на вхід алгоритму.
- Алгоритм шифрування: виконує різні заміни і перетворення над відкритим текстом.
- Секретний ключ: секретний ключ також вводиться в алгоритм. Точні заміни та перетворення, що виконуються алгоритмом, залежать від перетворення, які виконує алгоритм та залежать від ключа.
- Зашифрований текст: зашифроване повідомлення, яке отримується на виході. Залежить від відкритого тексту і секретного ключа.
- Алгоритм розшифрування − це, по суті, алгоритм шифрування, який виконується у зворотному порядку.

Для сучасних систем криптографічного захисту інформації сформульовано такі загальноприйняті вимоги:

- зашифроване повідомлення має піддаватися читанню тільки за наявності ключа;
- число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, має виходити за межі можливостей сучасних комп'ютерів;
- знання алгоритму шифрування не повинно впливати на надійність захисту;
- незначна зміна ключа має призводити до суттєвої зміни вигляду зашифрованого повідомлення;
- структурні елементи алгоритму шифрування мають бути незмінними;
- довжина шифрованого тексту має дорівнювати довжині вихідного тексту;
- не повинно бути простих залежностей між ключем і відкритим текстом;
- будь-який ключ із множини можливих ключів повинен забезпечувати надійне шифрування;
- алгоритм має допускати як програмну, так і апаратну реалізацію[1, с.125–128].

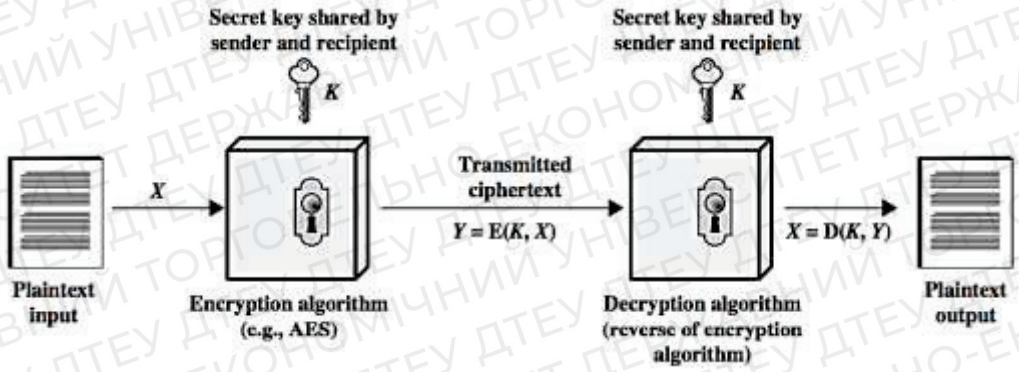


Рис. 1. Модель симетричного шифрування

Ключі, використовувані в криптосистемах мають бути випадковими. Неприпустимо використовувати словникові слова та інші ключі, що легко запам'ятовуються. Часто криптографічні засоби містять у собі засоби генерації випадкових послідовностей, що також забезпечує додатковий захист.

Одна з найпоширеніших операцій при шифруванні це XOR (виключне АБО) − це логічна операція, яка порівнює дві двійкові цифри (біти). Результатом операції XOR є 1, якщо два порівнювані біти різні, і 0, якщо вони однакові. Оператор XOR позначається символом "^".

У криптографії XOR часто використовується для виконання операцій шифрування і дешифрування. Наприклад, простий алгоритм шифрування на основі XOR може використовувати секретний ключ для виконання операції XOR між кожним бітом відкритого тексту повідомлення і відповідним бітом ключа. Розшифрування полягає у виконанні тієї ж операції XOR між зашифрованим текстом і ключем для відновлення вихідного відкритого повідомлення.

До алгоритмів, який відповідає сучасним вимогам відноситься симетричний алгоритм блочного шифрування AES (Advanced Encryption Standard) який ухвалено як стандарт шифрування урядом США. Специфікації алгоритму були опубліковані Національним інститутом стандартів і технологій США 26 листопада 2001 року. AES є найпоширенішим алгоритмом симетричного шифрування в даний час. Підтримка цього алгоритму введена фірмою Intel у сімейство процесорів, починаючи з мікроархітектури Sandy Bridge. Алгоритм прийнято як державний стандарт шифрування. Алгориитм шифрування AES (Рис. 2) передбачає певну кількість раундів, яка визначається довжиною ключа. Наприклад, 128-бітний ключ вимагає 10 раундів, а 256-бітний ключ − 14 раундів. Першим кроком є створення секретного ключа, який буде використовуватися для шифрування та розшифрування даних. Ключ може бути різної довжини, але AES підтримує ключі довжиною 128, 192 і 256 біт. Після того, як секретний ключ згенеровано, він розширюється для створення розкладу ключів. Розклад ключів використовується для створення серії круглих ключів, які будуть використовуватися в процесі шифрування і дешифрування.

AES використовує крок заміни «Substitute Bytes». Цей крок передбачає заміну кожного байта у вхідних даних відповідним байтом з таблиці підстановок (відомої як S-box).

На кроці «Shift Rows» рядки матриці даних зсуваються на певну кількість байт. Перший рядок не зсувається, другий рядок зсувається на один байт вліво, третій рядок зсувається на два байти вліво, а четвертий рядок зсувається на три байти вліво.

Крок «MixColumn» передбачає виконання матричного множення на кожен стовпець матриці даних з фіксованою матрицею.

На наступному кроці круглий ключ, згенерований з розкладу ключів, додається до матриці даних за допомогою операції XOR.

Кроки з 3 по 6 повторюються для певної кількості раундів, залежно від довжини ключа. Для 128-бітного ключа − 10 раундів, для 192-бітного ключа − 12 раундів, а для 256-бітного ключа − 14 раундів.

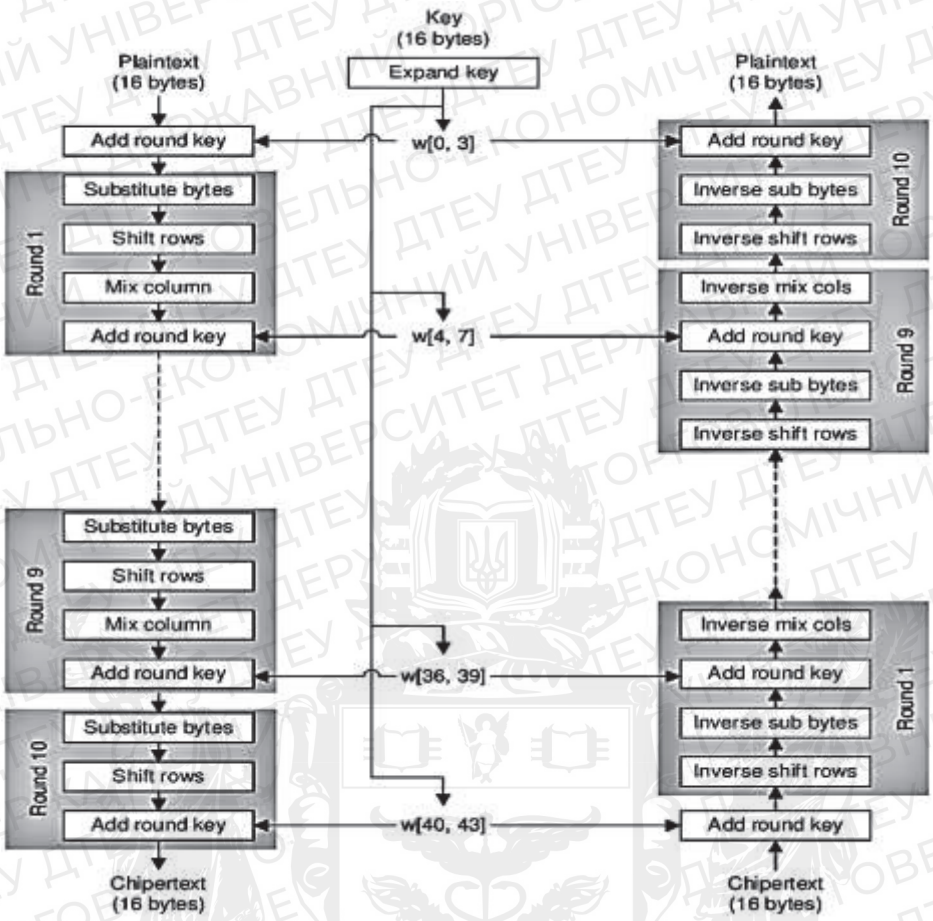


Рис. 2. Блок-схема процесу шифрування та дешифрування AES

Фінальний раунд: останній раунд AES дещо відрізняється від інших раундів. Кроки підстановки та зсуву рядків виконуються як зазвичай, але крок перемішування стовпців пропускається. Ключ останнього раунду потім об'єднується з матрицею даних для отримання зашифрованого результату.

Щоб розшифрувати дані, процес виконується у зворотному порядку. Зашифровані дані піддаються операції XOR з остаточним круглим ключем, після чого кожен з етапів виконується у зворотному порядку.

Український криптографічний стандарт для блокових шифрів, який також відомий як «шифр Калина». Він був розроблений командою українських криптографів і опублікований у 2015 році як Державний стандарт України ДСТУ 7624:2014. Шифр «Калина» − це блоковий шифр із симетричним ключем, який підтримує розміри блоків 128, 256 і 512 біт з розмірами ключів 128, 256 і 512 біт відповідно. Він заснований на шифрі переможця конкурсу AES Rijndael, але має деякі відмінності в конструкції, а саме: інший графік ключів, інша кількість раундів і використання операцій побітового обертання замість операцій зсуву.

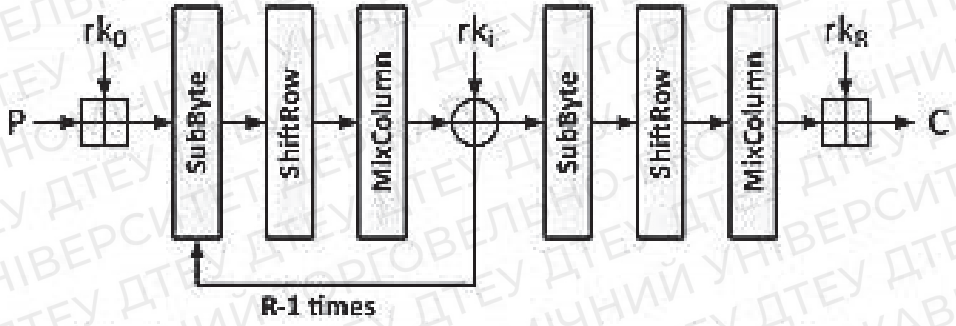


Рис. 3. Функція шифрування Kalyna, де R – кількість раундів

Шифр «Калина» (Рис. 3) розроблений для захисту від широкого спектру атак, включаючи диференціальний та лінійний криптоаналіз, і він був детально проаналізований криптографічною спільнотою. Він також вважається відносно ефективним з точки зору продуктивності, і його було реалізовано в ряді програмних і апаратних платформ. Шифр «Калина» був прийнятий як національний стандарт в Україні і поданий до Міжнародної організації зі стандартизації (ISO) на розгляд як світовий стандарт.

Шифр Kalyna є симетричним блоковим шифром, що означає, що він використовує один і той же секретний ключ для шифрування і розшифрування даних. Працює наступним чином:

- Розширення ключа. 128, 256 або 512-бітний секретний ключ розширюється до більшого набору круглих ключів, які будуть використовуватися в процесі шифрування і розшифрування. Це робиться за допомогою розкладу ключів, який генерує серію раундів ключів.
- Ініціалізація. Відкриті дані розбиваються на блоки фіксованого розміру 128 біт (або 256 чи 512 біт, залежно від обраного розміру блоку). Перший блок піддається операції XOR з "відбілюючим" ключем, який є фіксованим значенням, що слугує для рандомізації вхідних даних.
- Раунди шифрування. Блок відкритого тексту проходить через серію раундів шифрування, де в кожному раунді застосовується комбінація операцій заміни і перестановки. Операція заміни замінює кожен байт відкритого тексту відповідним байтом з таблиці заміни. Операція перестановки змінює порядок байтів у блоці відповідно до фіксованого шаблону.

Після останнього раунду шифрування кінцевий блок зашифрованого тексту створюється шляхом XOR-об'єднання результату останнього раунду з ключем останнього раунду.

Для розшифрування зашифрованого тексту застосовується той самий процес у зворотному порядку. Блок зашифрованого тексту проходить через таку ж кількість раундів розшифрування, в яких застосовуються зворотні операції підстановки і перестановки, що використовуються при шифруванні. Ключ останнього раунду додається до результату останнього раунду дешифрування, щоб отримати вихідний блок відкритого тексту.

Кількість раундів шифрування і розшифрування залежить від обраного ключа і розміру блоку. Наприклад, з 256-бітним ключем і розміром блоку 128 біт, шифр використовує 10 раундів шифрування і розшифрування. З 512-бітним ключем і 256-бітним розміром блоку шифр використовує 14 раундів шифрування і розшифрування.

Асиметричне шифрування – це також процес шифрування даних між двома сторонами, але замість одного ключа для цього використовуються два унікальні, але математично пов'язані ключі. Перший ключ, відомий як відкритий ключ, шифрує дані перед відправкою через Інтернет; другий, закритий ключ, розшифровує дані на стороні одержувача. Ось чому асиметричне шифрування (Рис. 4) також відоме як шифрування з відкритим ключем.

Важливою перевагою асиметричних алгоритмів перед симетричними є відсутність необхідності попередньої передачі секретного ключа. Основним недоліком є обчислювальна складність, а отже, більші витрати ресурсів порівняно із симетричними алгоритмами. Тому на практиці асиметричні криптосистеми використовуються для передавання секретного ключа, а подальший обмін інформацією здійснюється вже за допомогою симетричних криптосистем.

Нині найрозвиненішим методом криптографічного захисту інформації з відомим ключем є RSA, названий так за початковими літерами прізвищ його винахідників (Rivest, Shamir і Adleman). Криптостійкість цього алгоритму ґрунтується на припущенні, що винятково важко визначити секретний ключ за відомим, оскільки для цього необхідно розв'язати задачу про існування дільників цілого числа, тобто на принципі складності факторизації цілих чисел. Ця задача є NP – повною. Відомі точні алгоритми для розв'язання цієї задачі мають експоненціальну оцінку обчислювальної складності, наслідком чого є неможливість отримання точних розв'язків для задач великої та навіть середньої розмірності.

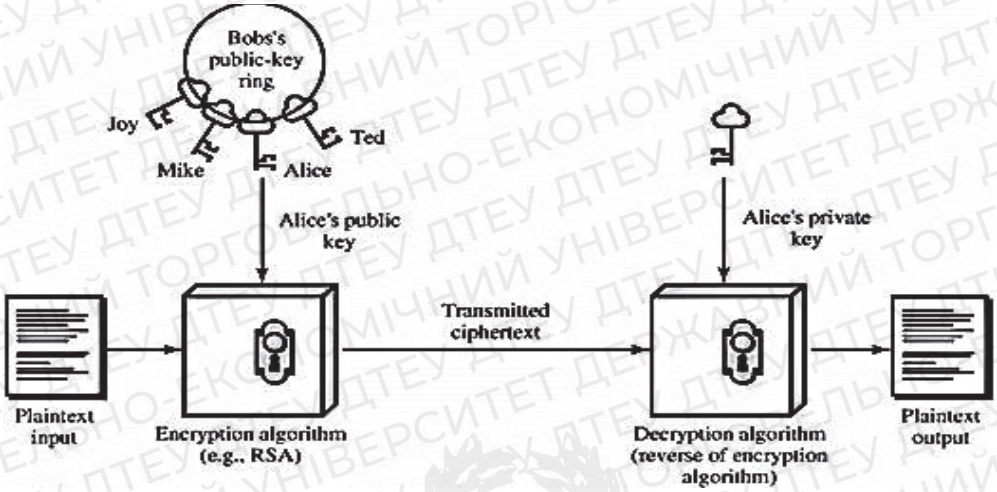


Рис. 4. Модель асиметричного шифрування

RSA використовує блок шифрування змінного розміру та ключ змінного розміру. Ця криптосистема, заснована на теорії чисел, яка є системою блочного шифрування. Вона використовує два простих числа для генерації відкритого і закритого ключів розміром від 1024 до 4096 біт. Ці два різні ключі використовуються для шифрування і дешифрування. Відправник шифрує повідомлення за допомогою відкритого ключа одержувача, і коли повідомлення передається одержувачу, одержувач може розшифрувати його за допомогою власного закритого ключа. Операції RSA можна розбити на три великі етапи: генерація ключа, шифрування та дешифрування [2].

RSA має деякі недоліки у своїй конструкції, тому не є кращим для комерційного використання. Коли для створення ключа вибираються малі значення p та q, то процес шифрування стає занадто слабким, і можна розшифрувати дані, використовуючи теорію випадкових ймовірностей та атаки побічних каналів. З іншого боку, якщо вибираються великі довжини p і q, то це займає більше часу і продуктивність погіршується в порівнянні з AES. Крім того, алгоритм також вимагає однакових довжин для p та q, що на практиці є дуже складною умовою для виконання. У таких випадках необхідна техніка підстановки, яка збільшує накладні витрати системи за рахунок більшого часу обробки. Послідовність подій (Рис.5) виконує алгоритм RSA для шифрування декількох блоків, а розшифрування – для блоків даних, що складаються з 64 біт, за допомогою 64-бітного ключа [2, 3].

Сайфер «Шифр-HSM» − сімейство універсальних високопродуктивних програмно-апаратних мережних криптографічних модулів, які виконують криптографічні перетворення і можуть бути використані у різноманітних прикладних системах.

Мережний криптографічний модуль (Рис. 6) «Шифр-HSM» (далі МКМ «Шифр-HSM» чи HSM) призначений для захищеної генерації, надійного збереження та використання ключів у швидких криптографічних перетвореннях. Для взаємодії користувачів з МКМ «Шифр-HSM» використовуються мережні протоколи транспортного рівня.

Мережний криптомодуль належить до апаратно-програмних засобів криптографічного захисту інформації виду Б підвиду Б2, категорій «Ш», «К» та «П» та класу В2 згідно з Наказом №141 від 20.07.2007 Держспецзв'язку України. Мережний криптомодуль використовується лише у локальній захищеній мережі установи [1, 3].

Даний криптографічний модуль підтримує розглянуті симетричні алгоритми шифрування ДСТУ 7624 та AES, у режимах ECB, OFB, CFB, CBC, CTR. А також асиметричне шифрування алгоритмом RSA за схемами RSAES-PKCS1-v1.5 RSAES-OAEP.

Використання PKCS#11 інтерфейсу для взаємодії з пристроєм дозволяє забезпечити аналогічну функціональність, як і рішення від: Thales (Luna HSM) і nCipher (nShield Connect).

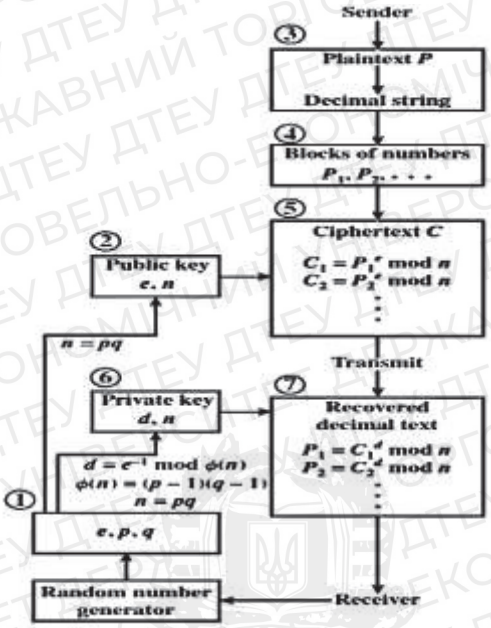


Рис. 5. Обробка RSA декількох блоків

До основних функцій мережного криптографічного модуля «Шифр-HSM» належать:

- Відновлення з резервної копії та відновлення до заводських налаштувань.
- Автентифікація адміністраторів на HSM з використанням захищених носіїв.
- Використання захищених носіїв, як локально, так і віддалено.
- Створення резервних копій внутрішнього стану.
- Зберігання резервних копій модуля на окремому захищеному засобі – МКМ виключно для зберігання резервних копій.
- Реплікація поточного внутрішнього стану одного МКМ на кілька МКМ (до 16 у режимі Master-Slave).
- Віддалене адміністрування з використанням web-інтерфейсу.
- Віддалений моніторинг з використанням web-інтерфейсу та за SNMP.
- Можливість зберігання не лише ключів, а й конфіденційних даних у великій кількості (обмежується обсягом внутрішньої пам'яті, 256, 512 ГБ та 1 ТБ).
- Захист від відкриття та проникнення до МКМ, з фізичним знищенням чи видаленням конфіденційної інформації.
- Виконання криптографічних операцій [3].

Також для захисту інформації використовується стеганографія – наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі повідомлення.

Слово «стеганографія» в перекладі з грецької буквально означає «тайнопис» (steganos − секрет, таємниця; graphy − запис). До неї належить величезна безліч секретних засобів зв'язку, таких як невидиме чорнило, мікрофотознімки, умовне розташування знаків, таємні канали та засоби зв'язку на плаваючих частотах тощо.

На відміну від криптографії, яка приховує вміст повідомлення, стеганографія приховує сам факт його існування. Як правило, повідомлення буде виглядати як що-небудь інше, наприклад, як зображення, стаття, список покупок або лист. Стеганографію зазвичай використовують спільно з криптографією. Перевага стеганографії над чистою криптографією в тому, що повідомлення не привертають до себе уваги. Таким чином, криптографія захищає зміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих посилань. Цифрова стеганографія − напрям стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти. Найчастіше цей метод ґрунтується на надмірності аудіовізуальної інформації. Як правило, внесення спотворень, які перебувають нижче порога чутливості людини, не призводить до помітних змін цієї інформації [1].

Рис. 6. Мережний криптографічний модуль «Шифр-HSM»

Цифрова стеганографія – напрям стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти. Найчастіше цей метод ґрунтується на надмірності аудіовізуальної інформації. Як правило, внесення спотворень, які перебувають нижче порога чутливості людини, не призводить до помітних змін цієї інформації. Захист конфіденційної інформації від несанкціонованого доступу – це сфера, в якій використання комп'ютерної стеганографії є найбільш ефективним. Наприклад, одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і розрядністю 8 біт дає змогу приховати за рахунок заміни найменш значущих розрядів близько 10 кілобайт інформації. Стеганографічні методи, спрямовані на протидію системам моніторингу та управління мережевими ресурсами, дають змогу протистояти спробам промислового шпигунства. Ще однією сферою використання стеганографії є захист авторського права. На графічні зображення може наноситися спеціальна мітка, яка залишається невидимою для очей, але розпізнається спеціальним ПЗ і дає змогу однозначно ідентифікувати файл [1, 3].

Таким чином, сучасна стеганографія поряд із криптографією представляє безліч засобів захисту інформації, і найкращим рішенням буде комбінування як криптографічних, так і стеганографічних методів.

Висновки. Хоча програмне та апаратне забезпечення для захисту інформації має вирішальне значення для захисту даних, воно не є надійним. Кіберзлочинці продовжують розробляти витончені методи обходу заходів безпеки, і витоки даних все ще є поширеним явищем. Тому важливо використовувати кілька рівнів захисту та регулярно оновлювати програмне та апаратне забезпечення, щоб забезпечити найвищий рівень безпеки. Найперспективнішим напрямком у сфері програмно-апаратного захисту інформації є створення комплексних систем, що вирішують широке коло завдань. Розглянуті криптографічні засоби захисту інформації не зможуть надати належний рівень захисту без використання разом з ними мережевих екранів, антивірусних програм та систем виявлення вторгнень та інших засобів в загальній, комплексній системі захисту. Прикладом модулю, що входить до таких систем є розглянутий в статті мережний криптографічний модуль «Шифр-HSM». Загалом, програмне та апаратне забезпечення для захисту даних є необхідними компонентами стратегії кібербезпеки будь-якої організації. Вони повинні використовуватися разом з іншими заходами безпеки, такими як навчання співробітників і оцінка ризиків, для створення комплексної та ефективної системи безпеки.

Список використаних джерел

1. О. Кузнецов, Р. Олійников, Ю. Горбенко, А. Пушкарьов, О. Дирда, І. Горбенко, Обґрунтування вимог, побудування та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів. – 2014. – с. 130 – 141.
2. A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention \\ Режим доступу: https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php (останнє звернення 13.03.2023р.)
3. Матеріали Української ІТ компанії з захисту інформаційних систем «Сайфер» \\ Режим доступу: https://cipher.com.ua/uk (останнє звернення 13.03.2023р.)

Робота виконана під науковим керівництвом старшого викладача
КОСТЮК Ю.В.

МЕТОДИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ: ВІД БІОМЕТРІЇ ДО БЛОКЧЕЙНУ

ЛОБУЦЬКИЙ В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи автентифікації користувачів, які застосовуються в інформаційно-телекомунікаційних системах, що використовуються для ідентифікації користувачів, включаючи традиційні методи, такі як логіни та паролі, біометрична автентифікація та блокчейн-технології. Досліджено можливі загрози для безпеки та приватності, пов'язані з використанням біометричних даних та блокчейн-технологій, і запрпоновано можливі способи зменшення цих ризиків. Розглянуто питання безпеки та приватності використання цих методів.

The article discusses authentication methods used in information and telecommunications systems for identifying users, including traditional methods such as usernames and passwords, biometric authentication, and blockchain technology. Possible security and privacy threats associated with the use of biometric data and blockchain technologies are explored, and potential ways to mitigate these risks are proposed. Security and privacy concerns regarding the use of these methods are also discussed

Актуальність. Методи автентифікації користувачів в інформаційно-телекомунікаційних системах мають велику актуальність у сучасному цифровому світі, де відбувається швидкий розвиток технологій і збільшується кількість онлайн-сервісів та додатків. Автентифікація користувачів є ключовим елементом забезпечення безпеки та захисту приватності в інтернеті, оскільки вона дозволяє переконатися у тому, що користувач має право доступу до системи або додатку, і зменшує ризики кіберзлочинності та зловживання даними. Біометричні технології та блокчейн-підходи до автентифікації стають все більш популярними і мають великий потенціал для покращення безпеки та забезпечення приватності в інтернеті. Однак, їх використання також може мати певні ризики та виклики, пов'язані з захистом персональних даних та можливістю їх зламу.

Тому, розуміння та оцінка різних методів автентифікації є дуже важливою темою для дослідників, працівників галузі інформаційної безпеки та кібербезпеки, а також для користувачів, які хочуть бути впевненими у тому, що їхні дані захищені від несанкціонованого доступу. З цієї причини, забезпечення безпеки та приватності в інформаційно-телекомунікаційних системах є надзвичайно важливим завданням.

Метою статті є дослідження методів автентифікації користувачів в цифровому середовищі, починаючи від біометричних технологій та закінчуючи блокчейн-підходами.

Об'єктом дослідження є аналіз можливостей технологій автентифікації в забезпеченні кібербезпеки та захисту конфіденційної інформації.

Предмет дослідження – методи та технології, що використовуються для ідентифікації та перевірки користувачів у цифровому середовищі.

Аналіз попередніх досліджень. Аналіз попередніх досліджень з питань методів автентифікації користувачів в інформаційно-телекомунікаційних системах показує, що більшість досліджень зосереджена на вдосконаленні методів біометричної автентифікації, таких як розпізнавання обличчя, відбитків пальців, голосу та інших біометричних характеристик. Деякі дослідження також зосереджені на застосуванні методів машинного навчання для вдосконалення процесу автентифікації. Інші дослідження вивчають використання різних методів автентифікації, таких як одноразові паролі та біометричні

токени. Загалом, попередні дослідження показують, що методи автентифікації користувачів є важливою та актуальною темою, і вони постійно вдосконалюються для забезпечення безпеки та приватності користувачів в інформаційно-телекомунікаційних системах. Дослідженню методів автентифікації присвячені праці вітчизняних та закордонних науковців: І. О. Гончаренко, М. С. Карпенко, Ю. А. Довгань, В. М. Колісник, О. І. Нікітіна, М. В. Ісаєва та ін.

Виклад основного матеріалу. У сучасному світі, де інформація є одним із найбільш цінних ресурсів, забезпечення безпеки даних та доступу до них є дуже важливим завданням. Методи автентифікації користувачів є одним із основних засобів забезпечення безпеки в інформаційно-телекомунікаційних системах. В інформаційно-телекомунікаційних системах (ІТС) автентифікація користувачів є важливим і невід'ємним елементом забезпечення безпеки даних та інформаційних ресурсів. Існує багато методів автентифікації користувачів, починаючи від традиційних методів, таких як логіни та паролі, до новітніх, таких як біометрична автентифікація та блокчейн. Основні методи автентифікації користувачів в інформаційно-телекомунікаційних системах включають наступні:

- Логін та пароль: це найбільш поширений метод автентифікації, який вимагає від користувача ввести свій логін та пароль для доступу до акаунту.
- Біометричні методи − методи, які включають використання фізіологічних або поведінкових рис користувача, таких як відбиток пальця, розпізнавання обличчя, голосу або почерку.
- Карти або токені − метод, який використовує фізичний об'єкт, який користувач повинен мати при собі, наприклад, карту з чипом або USB-ключ.
- Двофакторна автентифікація − метод, який включає використання двох або більше методів автентифікації, наприклад, комбінації логіна та пароля з біометричним методом або картою або токеном.
- Одноразові паролі − метод, що використовується для тимчасового доступу до аккаунту та вимагає від користувача ввести одноразовий пароль, який зазвичай надсилається на мобільний телефон або електронну пошту.
- Сертифікати − метод використовує сертифікати, що видаються відповідними органами, для перевірки ідентичності користувача.
- Соціальна автентифікація − метод, що використовується для входу на сайти або додатки за допомогою профілю в соціальній мережі, такі як Facebook або Google.
- Блокчейн-автентифікація − блокчейн може використовуватись як метод автентифікації, особливо в контексті криптовалют та інших децентралізованих додатків. Блокчейн − це розподілена база даних, яка зберігає транзакції у вигляді блоків, кожен з яких містить хеш попереднього блоку. Це створює ланцюжок блоків, який є відкритим і невід'ємним, тому що будь-яка зміна в одному блоку вимагає зміни всіх наступних блоків.

Автентифікація користувачів в інформаційно-телекомунікаційних системах є важливою складовою захисту інформації та даних від несанкціонованого доступу. Проте існують деякі виклики та проблеми, пов'язані з автентифікацією користувачів:

1. Компрометація облікових даних: користувачі часто використовують слабкі паролі або взагалі не змінюють стандартні облікові дані, що легко стає об'єктом атаки хакерів або кіберзлочинців. Також можуть використовуватися атаки підбору паролів.
2. Специфікація стандартів: різні інформаційно-телекомунікаційні системи можуть використовувати різні стандарти для автентифікації користувачів, що може призвести до проблем з сумісністю між системами.
3. Конфіденційність даних: у деяких випадках, при автентифікації користувачів, деякі приватні дані можуть бути збережені на сервері. Це може стати об'єктом атак і злому.
4. Ризик витоку даних: при автентифікації через Інтернет.

5. Вартість та складність розгортання: деякі методи автентифікації можуть бути дорогими у розгортанні та підтримці, а також можуть потребувати значних зусиль користувачів для використання.

В умовах сьогодення автентифікацію можна представити за такими сегментами (Рис.1).

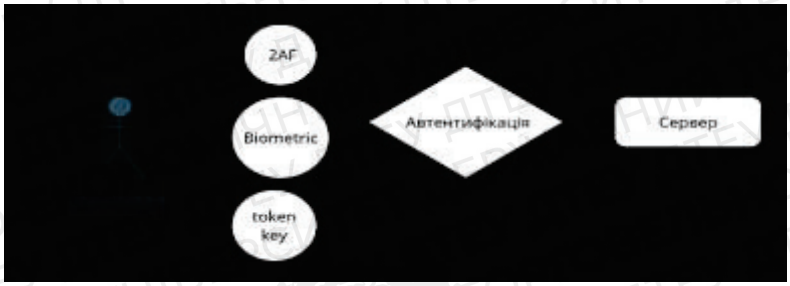


Рис. 1. Сегментація автентифікації

Авторизація за допомогою логіну та пароля − це дуже поширений метод авторизації у багатьох системах, від електронної пошти до соціальних мереж та інтернет-банкінгу. Цей метод авторизації дозволяє користувачам отримувати доступ до своїх особистих акаунтів та зберігати інформацію у захищеній середовищі. Процес авторизації за допомогою логіну та пароля зазвичай складається з наступних етапів: спочатку користувач вводить свій логін та пароль на сторінці авторизації, потім система перевіряє введені дані та перевіряє, чи існує в базі даних користувач з таким логіном та паролем. Якщо введені дані правильні, то користувач отримує доступ до свого акаунта, в іншому випадку він отримує повідомлення про помилку та може спробувати ввести дані знову. Після успішної авторизації система зазвичай встановлює «сесію» - унікальний ідентифікатор, який дозволяє користувачеві працювати з системою без потреби повторного введення логіну та пароля на протязі певної години. У разі авторизації за допомогою логіну та пароля важливо забезпечити безпеку введення та збереження цих даних. Користувач повинен вибирати надійний пароль та не повинен нікому розкривати його. Також система повинна забезпечувати захист від несанкціонованого доступу до бази даних користувачів, де зберігаються логіни та паролі.

Рис.2. Вікно автентифікації

Хоча паролі є важливим інструментом для захисту від несанкціонованого доступу до облікових записів, вони також можуть стати джерелом уразливостей та ризиків для безпеки. Недосконаліть людської пам'яті та легкість забування паролів можуть призвести до використання слабких та недостатньо складних паролів, які можуть бути легко зламані хакерами. Крім того, паролі можуть бути вкрадені шляхом використання шкідливих програм, таких як кейлогери, або через атаки соціального інжинірингу, які маніпулюють людською поведінкою для отримання доступу до паролів.

Одним із найпоширеніших методів автентифікації користувачів є метод введення логіна та пароля. Проте, цей метод є досить уразливим до атак, таких як фішинг та перехоплення даних. Для забезпечення вищого рівня безпеки до застосування приходять методи біометрії. Біометрія – це метод автентифікації користувачів за допомогою їх біологічних рис. До найпоширеніших методів біометрії належать відбитки пальців (Рис.2), розпізнавання обличчя (Рис.3), розпізнавання голосу та розпізнавання раковини вуха. Використання методів біометрії дозволяє забезпечити вищий рівень безпеки, оскільки біометричні дані неможливо підробити чи скопіювати.

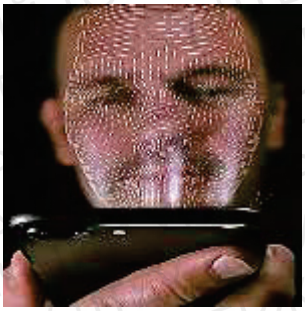


Рис. 3. Принцип дії ехнології Face ID

Технологія Face ID використовується на пристроях компанії Apple, таких як iPhone та iPad. Основним принципом дії є використання технології розпізнавання обличчя за допомогою TrueDepth-камери, розташованої на екрані пристрою. Під час налаштування Face ID, користувач сканує своє обличчя, і пристрій зберігає його математичну модель у спеціальній безпечній зоні, що знаходиться на процесорі пристрою. При подальшому використанні, коли користувач підносить пристрій до свого обличчя, TrueDepth-камера збирає інформацію про форму обличчя, положення очей, ніздрі, рота та інші параметри, і передає її на процесор для порівняння зі збереженою математичною моделлю. Якщо отримана інформація відповідає збереженій моделі, пристрій розблоковується. Основна перевага технології Face ID полягає у її точності та надійності. Крім того, вона працює в широкому діапазоні умов освітлення та дозволяє розпізнавати обличчя у різних позах та уголках. Також вона є безпечнішою порівняно з іншими методами автентифікації, такими як введення пароля, оскільки не може бути підмінена або скопійована [1].

Технологія Touch ID використовує сканер відбитків пальців, що вбудований у кнопку домашнього екрану на пристроях Apple. Кнопка домашнього екрану містить датчик, що реагує на тиск пальця, та сканер відбитків пальців, який визначає унікальні характеристики шкірного відбитка. При реєстрації відбитка пальця датчик сканує пальці користувача та зберігає характеристики відбитка у зашифрованому вигляді на пристрої. При подальшому використанні Touch ID користувач просто натискає на кнопку домашнього екрану для активації датчика сканування відбитка пальця. Сканер відбитків пальців порівнює характеристики нового відбитка зі збереженим, що використовується для перевірки автентичності користувача. Якщо знайдені відбитки збігаються, то пристрій дозволяє доступ користувача до пристрою. Технологія Touch ID забезпечує високий рівень безпеки, оскільки відбитки пальців є унікальними для кожної особи, що зменшує ризик несанкціонованого доступу до пристрою. Крім того, застосування технології Touch ID забезпечує зручність та швидкість використання, оскільки користувачеві не потрібно вводити пароль або пін-код, достатньо лише натиснути на кнопку домашнього екрану [2].

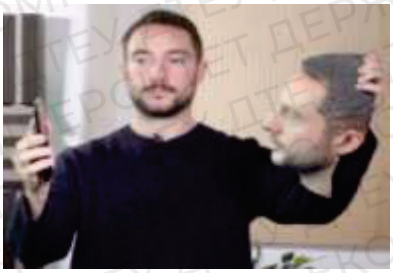


Рис.4. Обхід блокування за допомогою 3D маски

Одна з можливих уразливостей Face ID та Touch ID полягає в тому, що вони можуть бути обмануті фальшивими відбитками пальців або обличчя (Рис.4). Наприклад, дослідники групи CCC (Chaos Computer Club) використали фотографію обличчя користувача та 3D-друкований макет обличчя, щоб успішно обійти захист Face ID на iPhone X. Також були

повідомлення про успішне обходження захисту Face ID з використанням маски, зробленої на 3D-принтері, яка була створена на основі фотографії обличчя.

Також можливе виникнення проблем зі зберіганням біометричних даних, таких як відбитки пальців та обличчя, що може призвести до можливості їх викрадення.

Автентифікація типу картка або токен − це методи авторизації, які дозволяють користувачам отримувати доступ до облікових записів та інших ресурсів шляхом використання карток або токенів замість паролів. Ці методи авторизації дозволяють уникнути багатьох проблем, пов'язаних із паролями, таких як їх вразливість до атак і легкість забування.

Валідація за допомогою картки використовується давно і зазвичай здійснюється за допомогою спеціальних карт-читачів. Користувач вставляє картку в читач, який зчитує інформацію з неї та перевіряє, чи є права доступу до акаунту. Цей метод авторизації є досить безпечним, оскільки картки зазвичай містять вбудовані захисти від копіювання та підробки.

Токені є іншим методом авторизації, який вживається дедалі більше в сучасних системах. Токені − це унікальні коди, які генеруються програмно і використовуються для авторизації користувача. Коди можуть бути відправлені на мобільний телефон або інше зареєстроване пристрій. Користувачі можуть ввести токен у відповідному полі на сайті або у додатку, щоб отримати доступ до ресурсів. Токени є більш безпечними, ніж паролі, оскільки вони є одноразовими та не можуть бути використані знову. Існує також концепція токенів доступу, яка використовується в багатьох API. Токени доступу − це спеціальні коди, які використовуються для авторизації користувача для взаємодії з певним API. Кожен токен є унікальним та має обмежений час дії.

Система автоматично формує заявки на оплату, що дозволяє уникнути помилок в розрахунках, а також спланувати витрати коштів на закупівлю.

Які картки для авторизації можна використовувати різні пристрої та технології, залежно від того, які ресурси та системи необхідно захищати. Найбільш поширеними формами карт для авторизації є:

- Кредитні та дебетові картки − для доступу до банківських ресурсів та операцій з фінансами.
- Смарт-картки − це картки із вбудованим мікропроцесором та пам'яттю. Вони можуть використовуватися для авторизації доступу до комп'ютерних систем, облікових записів, мереж, будівель, автоматизованих систем контролю доступу та інших ресурсів.
- RFID-картки − це картки із вбудованим радіочастотним ідентифікатором (RFID). Вони використовуються для авторизації доступу до приміщень, паркінгів, облікових записів, товарів та інших ресурсів, які потребують ідентифікації за допомогою бездротових технологій.
- USB-токені − це пристрої, що підключаються до USB-портів комп'ютера та містять вбудовані ключі шифрування та інші методи захисту. Вони використовуються для авторизації доступу до комп'ютерів, мереж та інших ресурсів.
- NFC-карти − це картки із вбудованим чіпом та бездротовими технологіями, які можуть використовуватися для авторизації доступу до різних пристроїв, таких як мобільні телефони, планшети та інші ресурси.
- QR-код − це спеціальні зображення, які можуть бути розпізнані за допомогою камери смартфону або сканера. Вони можуть бути використані для авторизації доступу до сайтів, додатків та інших ресурсів [3].

Цей метод автентифікації на основі ключ-токен зазвичай використовується для забезпечення безпеки веб-додатків та API або для фізичних замків. Однак такий метод не є ідеальним і може бути уразливим до деяких атак. Однією з можливих атак на цей метод є крадіжка токена. Якщо зловмисники змогли отримати доступ до токена, то вони можуть використовувати його для отримання несанкціонованого доступу до захищеного ресурсу. Ця проблема може бути розв'язана за допомогою шифрування токенів та використанням протоколів, які забезпечують безпеку токенів, наприклад, OAuth.

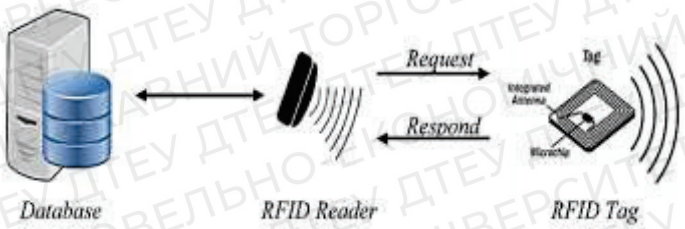


Рис.5. Принцип дії інфраструктури для автентифікації з використанням технології RFID

Ще однією потенційною вразливістю є можливість підробки токена. Якщо зловмисники змогли підробити токен, вони можуть використовувати його для отримання доступу до захищеного ресурсу. Цю проблему можна вирішити за допомогою регулярної перевірки токенів та використання безпечних протоколів обміну інформацією. Крім того, при використанні ключ-токена методом автентифікації можуть бути вразливі, пов'язані зі зберіганням ключів. Якщо ключі зберігаються недостатньо захищеними або вони можуть бути викрадені, це може призвести до загрози для безпеки ресурсу. Загалом, метод автентифікації на основі ключ-токена є досить безпечним і надійним, якщо його використовувати з належною обачністю та застосовувати відповідні заходи безпеки, такі як шифрування токенів та перевірка їх правильності.

Блокчейн-автентифікація (Рис.6). є одним із найбезпечніших методів автентифікації в даний час. Замість того, щоб передавати конфіденційні дані через централізовані сервери, як у традиційних методах, блокчейн-автентифікація використовує технологію розподілених реєстрів для збереження та обробки даних. Основним перевагою блокчейн-автентифікації є те, що вона забезпечує високий рівень безпеки. Блокчейн використовує криптографію для забезпечення безпеки транзакцій та зберігання конфіденційних даних. Це означає, що цей метод автентифікації надає високий рівень захисту від шахрайства та злому. Іншою перевагою блокчейн-автентифікації є її децентралізованість. У традиційних методах автентифікації централізовані сервери зберігають конфіденційні дані користувачів, що робить їх уразливими до атак із боку зловмисників. Блокчейн-автентифікація, з іншого боку, зберігає дані у розподілених регістрах, що робить їх менш уразливими до атак та злому. Однак блокчейн-автентифікація також має деякі недоліки, такі як обмежена масштабованість та повільна швидкість обробки транзакцій. Крім того, використання блокчейн-автентифікації потребує спеціальних технічних знань та ресурсів [4].

2FA на базі блокчейну − це додатковий рівень безпеки, (Рис.7).який використовується для автентифікації користувачів в інформаційно-телекомунікаційних системах. За допомогою 2FA, користувач може підтвердити свою ідентичність, використовуючи два різні методи автентифікації.

Рис.6. Двофакторна аутентифікація на основі технології Blockchain

Методи автентифікації користувачів застосовуються у різних сферах діяльності, включаючи фінанси, медицину, урядові організації та бізнес.

У фінансовій сфері, особливо у онлайн-банкінгу, методи автентифікації використовуються для захисту фінансових транзакцій та даних клієнтів. Наприклад, банки можуть використовувати методи біометрії, такі як сканування відбитків пальців або

розпізнавання обличчя, або використовувати двофакторну автентифікацію, яка включає в себе введення паролю та отримання коду через смс або електронну пошту. Окрім банківської сфери та мереж Wi-Fi, вони знаходять застосування в онлайн-магазинах, соціальних мережах, медичній сфері, громадському транспорті, аеропортах та інших місцях. У соціальних мережах використовуються різні методи автентифікації, такі як логін через обліковий запис Google або Facebook, введення коду, відправленого на електронну пошту, або відбитків пальців на смартфонах зі спеціальними сенсорами. У медичній сфері методи автентифікації можуть використовуватись для захисту медичних даних пацієнтів та контролю доступу до них. Наприклад, лікарі можуть використовувати біометричні методи для входу до систем електронної медичної документації або для доступу до медичних пристроїв, таких як електрокардіографи. Урядові організації також використовують методи автентифікації для захисту даних та забезпечення безпеки державних систем. Наприклад, урядові служби можуть використовувати біометричні методи для контролю доступу до певних приміщень або для автентифікації працівників у системах електронного документообігу.

Висновки. Розвиток методів автентифікації користувачів є однією з актуальних проблем сучасного інформаційного світу, оскільки залежно від використовуваних методів можуть бути різні рівні безпеки і захисту від несанкціонованого доступу до інформації. Однією з перспективних тенденцій є застосування багатофакторної автентифікації, коли для доступу до ресурсів вимагається використання не одного, а кількох методів автентифікації (наприклад, пароля та біометричних даних). Також важливими напрямками розвитку є застосування штучного інтелекту та машинного навчання для покращення точності і швидкості автентифікації, а також застосування блокчейн технологій для забезпечення безпеки та надійності процесу автентифікації. До інших перспективних напрямків розвитку методів автентифікації користувачів можна віднести використання квантових технологій, стандартизацію методів та уніфікацію протоколів, що дозволить забезпечити взаємодію між різними системами та пристроями з різною інфраструктурою і зменшити витрати на розробку та впровадження методів автентифікації. Усі ці напрямки розвитку методів автентифікації користувачів спрямовані на забезпечення максимального рівня безпеки та захисту від несанкціонованого доступу до інформації, що є особливо важливим у сучасному цифровому світі. Використання правильних методів автентифікації є дуже важливим аспектом в забезпеченні безпеки інформаційних систем та даних. Неправильне використання або відсутність методів автентифікації може призвести до різних загроз, таких як несанкціонований доступ до системи, викрадення даних, крадіжка особистої інформації тощо. Застосування сильних методів автентифікації, таких як двофакторна автентифікація з використанням біометричних даних, зменшує ризик порушення безпеки системи та даних, оскільки такі методи є надійними і складними для підробки. Отже, використання правильних методів автентифікації є необхідним елементом забезпечення безпеки інформаційних систем та даних, і має важливе значення у практичній діяльності.

Список використаних джерел

1. Lomas, N. (2017). How Apple's Face ID facial recognition system works.\\Режим доступу: https://techcrunch.com/2017/09/12/how-apples-face-id-facial-recognition-system-works/ (останнє звернення 09.04.2023р.) .

2. "Touch ID vs. Face ID: Which is faster?" by Christian Zibreg, iDownloadBlog.\\Режим доступу: https://www.idownloadblog.com/tag/face-id/ (останнє звернення 09.04.2023р.) .

3. Офіційна документація провайдерів послуг платіжних систем, таких як Visa \\Режим доступу: https://developer.visa.com/docs (останнє звернення 09.04.2023р.) .

4. Документація технології блокчейну на сайті Blockchain \\Режим доступу: https://www.blockchain.com/ru/explorer/api (останнє звернення 09.04.2023р.).

Робота виконана під науковим керівництвом к.п.н, доцента
ЧУБАЄВСЬКОГО В.І.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ ШТРИХКОДУ АБО QR-КОДУ ЛОГІСТИЧНОЇ КОМПАНІЇ

ЛЮТИЙ А., 2м курс ФІТ ДТЕУ
спеціальність 121 «Інженерія програмного забезпечення»

The article deals with the application of barcode technology in logistics management and supply chain. The history and types of barcodes, as well as the advantages and disadvantages of their use in logistics are reviewed. The role of barcodes in improving the efficiency of logistics management and ensuring the accuracy of information on warehouse accounting and cargo tracking is investigated.

У статті розглянуто застосування технології штрихкодів у логістичному менеджменті та ланцюгу постачання. Оглянуто історію та типи штрихкодів, а також переваги та недоліки їх використання в логістиці. Досліджено роль штрихкодів у покращенні ефективності логістичного менеджменту та забезпеченні точності інформації про складський облік та відстеження вантажів.

Предметом дослідження є інформаційна технологія розпізнавання штрихкоду або QR-коду логістичної компанії.

Об'єктом дослідження виступає процес розпізнавання штрихкоду або QR-коду та використання його даних для автоматизації логістичних процесів.

Мета дослідження полягає у визначення ефективності використання інформаційної технології розпізнавання штрихкоду або QR-коду для забезпечення автоматизації та оптимізації логістичних процесів логістичної компанії.

Також можемо виділити такі *підцілі:*

- Дослідження основних технологій розпізнавання штрихкодів та QR-кодів.
- Аналіз використання інформаційної технології розпізнавання штрихкоду або QR-коду в логістичних компаніях.
- Оцінка впливу інформаційної технології розпізнавання штрихкоду або QR-коду на ефективність логістичних процесів.
- Розроблення пропозицій щодо вдосконалення використання інформаційної технології розпізнавання штрихкоду або QR-коду в логістичних компаніях.

Виклад основного матеріалу. Зараз у світі швидко розвивається логістична індустрія, що потребує швидкої та точної інформаційної обробки даних. Інформаційні технології стали необхідним інструментом у цьому процесі, тому розробка та впровадження систем розпізнавання штрихкодів та QR-кодів є актуальною проблемою для логістичних компаній.

У сучасному світі логістичні компанії стикаються зі значними труднощами в управлінні своїм складом та постачальним ланцюгом. Одним зі способів рішення цих проблем є застосування технології штрихкодів. Штрихкоди стали незамінним інструментом у логістичному менеджменті та ланцюгу постачання завдяки своїм перевагам, таким як забезпечення точності та швидкості обліку товарів, зниження рівня помилок та підвищення ефективності роботи складу.

Історія та типи штрихкодів:

Штрихкоди були розроблені у 1948 році та використовувалися в першу чергу у супермаркетах для швидкого сканування товарів при реєстрації їх продажу. З тих пір вони стали широко використовуватися у логістиці та ланцюгу постачання.

Існує кілька типів штрихкодів, зокрема EAN-13, EAN-8, UPC-A, Code 128 та інші. Кожен тип штрихкоду має свої особливості та використовується залежно від конкретних потреб.

Рис.1. Типи штрихкодів

Опис технології.

Штрихкод та QR-код - це графічні символи, які зберігають інформацію про товар або послугу. Штрихкоди зазвичай використовуються для ідентифікації товару, а QR-коди можуть містити більш різноманітну інформацію, наприклад, URL-адреси, контактні дані, текстові повідомлення тощо.

Система розпізнавання штрихкодів та QR-кодів складається з двох основних компонентів: обладнання для зчитування кодів та програмного забезпечення для обробки даних.

Обладнання для зчитування кодів може бути різним. Для штрихкодів це зазвичай сканер, а для QR-кодів може бути використана камера смартфону. Програмне забезпечення, що обробляє дані, зазвичай складається з декількох етапів: зчитування коду, декодування, перевірка на правильність та збереження інформації.

Для зчитування штрихкодів та QR-кодів використовуються спеціальні алгоритми, як і методи, які дозволяють зчитувати та обробляти інформацію з кодів. Ці алгоритми можуть використовувати різні методи зчитування, наприклад, метод читання лінійних штрихкодів або метод читання двовимірних QR-кодів. Використання відповідного методу залежить від типу коду та специфікацій обладнання, яке використовується.

У разі зчитування штрихкодів, програмне забезпечення зчитує штрихкод та декодує інформацію, яка міститься в коді. Далі виконується перевірка на правильність зчитування коду, щоб уникнути помилок при обробці даних. Якщо дані відповідають специфікаціям штрихкоду, то інформація зберігається у відповідній базі даних.

Для зчитування QR-кодів зазвичай використовуються камери смартфону, що дозволяє швидко та легко зчитувати QR-коди у будь-якому місці. Програмне забезпечення спочатку зчитує QR-код, далі декодує інформацію та виконує перевірку на правильність зчитування коду. Якщо дані відповідають специфікаціям QR-коду, то інформація зберігається у відповідній базі даних.

Використання технології штрихкодів в логістиці має декілька переваг порівняно з традиційними методами. Найбільш важливі з них наведені нижче:

Підвищена точність: Сканування штрихкоду забезпечує доставку правильного товару в потрібне місце в потрібний час, зменшуючи ризик помилок в управлінні запасами та обробці замовлень.

Покращена ефективність: Сканування штрихкоду набагато швидше за ручне введення даних, що зменшує час, необхідний для управління запасами та обробки замовлень.

Поліпшена трасованість: Технологія штрихкодів дозволяє легко відслідковувати та відстежувати продукти через ланцюг постачання, від виробника до кінцевого користувача, що полегшує видимість ланцюга постачання.

Рис.2. Складові QR-коду

Недоліки використання штрихкодів в логістиці

Хоча технологія штрихкодів має багато переваг, є деякі недоліки, про які важливо знати:

- Вимоги до обладнання: Щоб використовувати технологію штрихкодів, потрібне спеціальне обладнання, яке може бути досить дорогим.
- Потребує навчання: Щоб користуватися технологією штрихкодів, працівники повинні бути навчені, як правильно сканувати та обробляти дані, що може зайняти час та кошти.
- Чутливість до пошкоджень: Штрихкоди можуть бути пошкоджені або зіпсовані, що може призвести до помилок у скануванні та неправильного розпізнавання даних.
- Обмежена інформація: Технологія штрихкодів обмежується короткими кодами, що може не дозволити передавати достатньо інформації про товар, що є обмеженням для деяких видів продуктів.

Незважаючи на ці недоліки, технологія штрихкодів все ще є популярною в логістичній галузі через свої переваги в ефективності та точності управління запасами та обробки замовлень.

Роль штрихкодів у покращенні ефективності логістичного менеджменту

Штрихкоди забезпечують точність даних та знижують кількість помилок, що дозволяє логістичним компаніям поліпшити свої процеси управління запасами, відстеження та виконання замовлень, а також контролювати рух товарів. Використання штрихкодів дозволяє значно скоротити час на ручне введення даних та уникнути помилок, що може призвести до затримок у доставці товарів та несправностей в системі управління запасами.

- Покращення комунікації: Штрихкоди можуть допомогти покращити комунікацію між різними логістичними частинами компанії, такими як склад, виробництво, транспортування тощо. За допомогою штрихкодів можна легко та швидко передавати інформацію про товари та їх рух, що дозволяє уникнути помилок та покращити співпрацю між різними відділами компанії. Крім того, штрихкоди дозволяють вести документацію про товари та їх рух автоматично, що спрощує процес обліку та звітності.
- Зменшення витрат: Використання штрихкодів дозволяє зменшити витрати на ручне введення даних та уникнути помилок, що може призвести до затримок у доставці товарів та несправностей в системі управління запасами. Крім того, використання штрихкодів дозволяє покращити ефективність роботи працівників та знизити кількість помилок, що може призвести до затримок у доставці товарів та несправностей в системі управління запасами.
- Управління запасами: Штрихкоди дозволяють логістичним компаніям точно відстежувати кількість товарів на складах та здійснювати швидкий облік запасів. Це дозволяє компаніям планувати замовлення, уникати надлишковості та нестачі товарів, що забезпечує більш ефективне використання ресурсів.
- Обробка замовлень: Штрихкоди дозволяють швидко та точно сканувати та обробляти замовлення, що зменшує час обробки та ризик помилок. Також, за допомогою

штрихкодів можна відстежувати рух товарів від моменту отримання замовлення до його доставки, що забезпечує більш точну та швидку обробку замовлень.

- Відстеження вантажів: За допомогою штрихкодів можна відстежувати рух товарів від моменту їх відправки до моменту доставки. Це дозволяє вчасно виявляти та вирішувати проблеми, що виникають під час транспортування товарів, а також підвищує рівень відповідальності за доставку вантажу.

Роль штрихкодів у забезпеченні точності інформації про складський облік

Штрихкоди грають важливу роль у забезпеченні точності інформації про складський облік. Завдяки використанню штрихкодів, можна ефективно відстежувати всі операції з товарами на складі, від приймання до відвантаження, і зберігати цю інформацію в центральній базі даних. Це дозволяє підтримувати точний та актуальний інвентарний облік та запобігати помилкам та втратам товарів.

Крім того, штрихкоди можуть використовуватись для позначення місця розташування товарів на складі, що забезпечує їх точне та швидке знаходження в разі потреби. Також, штрихкоди можуть бути використані для визначення термінів зберігання та керування стоком, що дозволяє уникнути непотрібного складування товарів та зменшити втрати через застарілість.

Отже, використання штрихкодів у складському обліку дозволяє збільшити точність та швидкість операцій, зменшити помилки та втрати товарів та покращити ефективність управління складом в цілому.

Роль штрихкодів у забезпеченні відстеження вантажів

Штрихкоди є важливою технологією в логістиці, особливо у забезпеченні відстеження вантажів. Кожен товар може бути маркований індивідуальним штрихкодом, що дозволяє легко та точно відстежувати його рух по всьому логістичному ланцюжку. Коли товар прибуває на склад, штрихкод сканується, і відомість про його прибуття автоматично оновлюється в системі складського обліку. Так само, коли товар відправляється до клієнта, штрихкод знову сканується, і інформація про відвантаження оновлюється в системі.

Штрихкоди також дозволяють забезпечити точне відстеження термінів придатності товарів на складі. Кожен товар може бути позначений своїм індивідуальним штрихкодом, на якому зберігається інформація про дату виробництва та термін придатності. Коли товар прибуває на склад, його штрихкод сканується, і система автоматично розраховує, скільки часу залишилося до дати закінчення терміну придатності. Це дозволяє операторам складу вчасно забрати товар з полиць, які наближаються до кінця терміну придатності, та запобігти збиткам від зіпсованих продуктів.

Штрихкоди також можуть допомогти у відстеженні використання ресурсів на складі. Кожна одиниця товару може мати свій індивідуальний штрихкод, на якому зберігається інформація про вагу, розмір та інші характеристики. Це дозволяє вести облік кількості відправлених та отриманих вантажів, включаючи інформацію про їхнє місцезнаходження, дату та час пересування та багато іншого. За допомогою штрихкодів можна також визначити, коли та де виникають затримки в доставці, що дозволяє швидко вживати заходів для їх усунення та покращення ефективності логістичного процесу.

Штрихкоди можуть також допомогти забезпечити безпеку вантажу, оскільки вони дозволяють легко відстежувати відправлення з моменту його пакування до моменту доставки. Це дозволяє компаніям вчасно виявляти будь-які втрати або пошкодження вантажу та приймати заходи для їх запобігання в майбутньому.

Загалом, штрихкоди є незамінним інструментом у логістиці та управлінні ланцюгом постачання. Вони допомагають забезпечити точність та швидкість обробки інформації, покращують комунікацію та співпрацю між різними відділами компанії, зменшують час та витрати на складський облік та вантажоперевезення, а також забезпечують безпеку вантажу та вчасне виявлення будь-яких проблем в логістичному процесі.

Однак, при використанні інформаційної технології розпізнавання штрихкодів та QR-кодів необхідно враховувати різні виклики та складнощі. Необхідно забезпечити високу

точність та швидкість зчитування, враховуючи різні типи штрихкодів та QR-кодів, а також забезпечити безпеку даних та зручність використання.

Для досягнення цих цілей необхідно ретельно спроектувати інформаційну технологію, використовуючи відповідні програмні засоби та обладнання. Також необхідно забезпечити високу якість обслуговування та підтримку користувачів, що дозволить компаніям успішно використовувати інформаційну технологію розпізнавання штрихкодів та QR-кодів у своїй діяльності.

Високоякісна інформаційна технологія розпізнавання штрихкодів та QR-кодів має багато переваг для логістичних компаній. Наприклад, вона дозволяє зменшити час, необхідний для обробки даних, а також зменшити кількість помилок, пов'язаних з ручним введенням даних. Крім того, вона дозволяє компаніям легко відстежувати маршрути доставки та відслідковувати рух товарів у режимі реального часу.

Для використання інформаційної технології розпізнавання штрихкодів та QR-кодів у логістиці необхідно використовувати відповідні програмні засоби та обладнання, що дозволяють забезпечити високу точність та швидкість зчитування. Зокрема, для зчитування штрихкодів необхідно використовувати сканери штрихкодів, які можуть бути зв'язані з комп'ютером або мобільним пристроєм за допомогою USB-порту або Bluetooth. Для зчитування QR-кодів можна використовувати камеру мобільного пристрою або спеціальні QR-сканери.

Щоб забезпечити високу якість обслуговування та підтримки користувачів, логістичні компанії повинні мати кваліфіковані технічні служби та надавати регулярні навчання для співробітників, які використовують інформаційну технологію розпізнавання штрихкодів та QR-кодів. Крім того, компанії повинні надавати високоякісну технічну підтримку, яка допоможе користувачам вирішувати проблеми, пов'язані з використанням технології.

Висновок: використання штрихкодів у логістиці та ланцюгу постачання є важливим і корисним інструментом для покращення ефективності та точності обліку вантажів, зниження витрат на перевезення, складання та зберігання товарів, а також для підвищення рівня контролю за рухом товарів в логістичному ланцюзі. Впровадження технології штрихкодів дозволяє компаніям забезпечити точність та своєчасність інформації про товари, покращити комунікацію між різними логістичними частинами компанії та забезпечити більш ефективний контроль за вантажами. Проте, для успішного використання технології штрихкодів у логістиці необхідно вирішувати проблеми, пов'язані з несправністю обладнання, низькою якістю штрихкодів, несправністю системи сканування та можливістю зламу.

Список використаних джерел

1. Р. Р. Панде та Р. К. Шарма, "Barcode technology: A review," Journal of Engineering Science and Technology Review, vol. 5, no. 3, pp. 44-49, 2012.
2. М. С. Сарвар та С. Соомро, "Bar code technology and its application," Journal of Basic and Applied Scientific Research, vol. 2, no. 2, pp. 1198-1204, 2012.
3. А.М.М. Шаріф Уддін та М. А. Хоссейн, "Application of bar code in inventory management: A case study on Olympic Industries Limited, Bangladesh," Journal of Management and Business Administration, vol. 1, no. 1, pp. 11-18, 2015.
4. С.А. Адейемо, "Application of bar code technology in supply chain management in Nigerian firms," International Journal of Research in Management, Science & Technology, vol. 3, no. 1, pp. 79-87, 2015.
5. Ю.К. Двіведі, М. Р. Вейд та С. Л. Лал, "Barriers to the adoption of RFID and barcode technology in hospitals," Knowledge and Process Management, vol. 15, no. 2, pp. 64-72, 2008.

Робота виконана під науковим керівництвом к.е.н., доц.
ТИЩЕНКА Д.О.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ КЛІНІКИ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН

МАРТИНЕЦЬ А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Проблема, порушена у статті, це використання технології блокчейн задля захисту особистої інформації пацієнтів, що звертаються до медичних закладів. У цій статті розглядається важливість захисту персональних даних у медичній сфері, принципи роботи блокчейну, переваги цієї технології та досвід використання на державному рівні. З якими викликами блокчейн стикається відповідно до Загального регламенту захисту даних ЄС (GDPR) та яким чином ця технологія може законно бути впроваджена.

The problem raised in the article is the use of blockchain technology to protect the personal information of patients who seek medical care. This article discusses the importance of protecting personal data in the medical field, the principles of blockchain operation, the advantages of this technology, and the experience of its use at the state level. It covers the challenges that blockchain faces under the European Union's General Data Protection Regulation (GDPR) and how this technology can be legally implemented.

Актуальність. Пандемія COVID-19 та повномасштабна війна підкреслили необхідність цифрової трансформації медицини. Однак, це створило й додаткові ризики для конфіденційності пацієнтів. Медична інформація містить багато деталей про різні аспекти життя індивіда, окрім очевидного стану здоров'я та плану лікування, це можуть бути деталі майнового характеру, особистого життя та біометричні дані. І, як уся інша персональна інформація, вона є під загрозою незаконного збору та використання. Тож, захист персональних даних, які люди надають задля якісного медичного обслуговування, особливо важливий. Необхідно впроваджувати нові, більш якісні технології, що підвищать безпеку персональної інформації та попередять порушення права людини на приватність особистого життя.

Однією із технологій, що має високий рівень безпеки та невразливості, є блокчейн. Платформа на основі блокчейну є ідеальним варіантом для зберігання та обміну даними пацієнтів. Хоча є необхідність в детальному аналізі того, якими способами можливо запровадити цю технологію та які юридичні нюанси слід врахувати.

Ця технологія має ряд переваг, які зможуть спростити медичні дослідження, транспортування медикаментів, створити єдиний медичний реєстр, що полегшить адміністративні процеси та поліпшить взаємодію в галузі охорони здоров'я. Таким чином, впровадження блокчейну в медичну сферу має великі перспективи та майбутнє.

Метою статті є аналіз важливості захисту персональних даних в медичній галузі, аспекти роботи блокчейн-платформ та їх використання в сфері охорони здоров'я задля підвищення рівня безпеки, дослідити яким чином має бути впроваджена ця технологія аби це відповідало законодавчим вимогам.

Об'єкт дослідження – блокчейн як технологія, що забезпечує безпечне зберігання та передачу персональної інформації.

Предмет дослідження – захист персональної інформації у сфері охорони здоров'я за допомогою використання технологій блокчейн, переваги, принципи роботи та її впровадження.

Аналіз попередніх досліджень. Дослідження блокчейн як технології для захисту персональної інформації пацієнтів є не широко досліджуваною у вітчизняній науковій спільноті. Загалом це невеликого об'єму статті в інтернеті від адвокатів, що пояснюють важливість захисту медичної інформації та коментують тонкощі, що пов'язані з правом обробки даних та логікою роботи блокчейн, що може суперечити регламенту про захист

персональних даних. Більше про цю тему пишуть закордонні науковці. Однією із ґрунтовних робіт є робота університетів Об'єднаних Арабських Еміратів факультетів промислової та системної інженерії, електротехніки та комп'ютерних наук та медицини. «Blockchain for Patient Safety: Use Cases, Opportunities and Open Challenges» написана у 2022 році, як і більшість інших статей є нещодавно опублікованою, що свідчить про те, що ця тема є досить новою і багато досліджень цієї теми варто чекати в майбутньому.

Виклад основного матеріалу. Захист медичної інформації пацієнтів є юридичним та етичним обов'язком суб'єктів, що пов'язані з сферою постачання медичних послуг. Згідно зі статтею 3 Закону України "Основи законодавства України про охорону здоров'я" медичною інформацією є "інформація про медичне обслуговування особи або його результати, викладена в уніфікованій формі відповідно до вимог, встановлених законодавством, у тому числі інформація про стан здоров'я, діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/ життєдіяльності людини" [1]. Окрім того, що персональні дані у медичній сфері інформують щодо стану здоров'я пацієнта, його діагнозу та результатів медичного обстеження, вони також можуть містити деталі про генетику (спадкові властивості особи та способи успадкування характеристик у межах групи людей), статеве життя (дані про сексуальну поведінку та орієнтацію), біометричні дані (наприклад, відцифрований підпис, образ обличчя, відбитки пальців, малюнок сітківки ока тощо), інформацію про приватне та сімейне життя (дані немайнового та майнового характеру, інформацію про обставини, події та стосунки, пов'язані з особою та її сім'єю) [2].

Пацієнти (суб'єкти персональних даних), що користуються послугами медичних закладів надають згоду на надання та використання особистої інформації для проведення якісного лікування. Іноді поширення особистої інформації трапляється через недбале ставлення працівників медичної сфери до своїх обов'язків, а з розвитком технологій та цифровізацією даних проблемою можуть стати недосконалі технології захисту. У будь-якому випадку захист медичних даних пацієнтів є юридичним обов'язком лікарень і, як будь-яка інша персональна інформація, вона регулюються Законом України "Про захист персональних даних", що "спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних", і відповідно до статті 7 "забороняється обробка персональних даних (…), що стосуються здоров'я, статевого життя, біометричних або генетичних даних" [3].

Очевидно, що кожна людина прагне до належної реалізації всіх прав, наданих їй законом. Особливої уваги заслуговує сфера охорони здоров'я, в якій людина, звертаючись за медичною допомогою чи консультацією, прагне не лише отримати кваліфіковану послугу, а й бути впевненою що її дані захищенні.

Таким чином, впровадження сучасних та якісних технологій в системи безпеки клінік є необхідним кроком до мінімізування ризиків та попередження ситуацій витоку персональної інформації та неправомірне її використання, а також це сприяє розвитку відчуття довіри пацієнтів до медичних закладів.

Блокчейн є децентралізованою криптографічною системою зберігання та обміну даними. Технологія має шанс бути реалізованим у сферах, де захист персональних даних має надважливе значення тому, що робота блокчейну здійснюється таким чином, що нові блоки завжди зберігаються лінійно за логікою часового порядку. Тобто вони завжди додаються в «кінець» ланцюгу. Після того, як блок додано, важко змінити вміст блоку, оскільки кожен блок містить свій власний хеш (hash), а також хеш блоку перед ним. Хеш-коди створюються математичною функцією, яка перетворює числову інформацію в рядок цифр і літер. Якщо цю інформацію будь-яким чином відредагувати, хеш-код також змінюється.

Припустімо, хакер намагається відредагувати дані транзакцій таким чином, що клієнту доведеться заплатити за покупку двічі, та зі зміною суми транзакції – змінюється хеш блоку. Наступний блок у ланцюжку все ще міститиме старий хеш, і хакерам потрібно буде оновити і цей блок, щоб не залишити слідів. Щоб змінити блок, хакеру потрібно змінити кожен блок у блокчейні. Перерахування всіх цих хешів вимагає вагомої обчислювальної потужності.

Іншими словами, як тільки блок додано до блокчейну, його важко редагувати та неможливо видалити. Щоб вирішити проблему довіри, мережа блокчейн тестує комп'ютери, які хочуть приєднатися та додати блоки. Так, маючи можливість розв'язати складні обчислювальні математичні задачі, комп'ютер має право додати блок до блокчейну. Але процес додавання блоків до блокчейну, відомий у світі криптовалют як «майнінг», непростий. Якщо хакери хочуть скоординувати атаку на блокчейн, їм потрібно буде вирішити складну обчислювальну математичну задачу, вартість якої може перевищити вигоди [4].

Технологія блокчейну використовується у кіберфізичних процесах та явищах, які функціонують через посередників і таким чином наражаються на проблеми, оскільки у більшості випадків дані зберігаються у незашифрованому вигляді і недобросовісні працівники організацій можуть незаконно розповсюджувати приватну інформацію. До того ж зберігання даних на єдиному сервері робить систему вразливою. Тому блокчейн має перспективу активного розвитку у таких галузях як: освіта, наука, фінанси, медицина, туризм, кадри тощо.

Наразі блокчейн використовується, зокрема у боротьбі із корупцією, на державних рівнях багатьох країн. З метою боротьби з корупцією, уряд Грузії ініціював розробку проєкту з реєстрації прав на землю на базі технології блокчейн, що дозволило зменшити операційні витрати на 90%. Сьогодні система дозволяє оформити право власності на земельну ділянку за 10 хвилин, а не за дні. Громадяни мають цифрові сертифікати, які ніхто не може змінити без їхнього дозволу. На рівні Європи варто згадати про систему EBSI, яка була запроваджена у 2018 році, коли 29 країн (усі країни-члени ЄС, Норвегія, Ліхтенштейн) і Європейська комісія об'єднали зусилля для створення блокчейн-партнерства і створення транскордонних сервісів для державних адміністрацій, підприємств, громадян та їхніх екосистем [5].

Отже, технологія блокчейн використовує складні алгоритми для шифрування та захисту даних, що надзвичайно ускладнює доступ хакерам до особистих даних або їх зміну і серед переваг використання блокчейн-технології для захисту даних можна назвати:

– Децентралізоване зберігання: технологія блокчейн — це розподілена база даних, у якій дані зберігаються в мережі комп'ютерів, а не в центральному місці. Децентралізоване сховище дуже ускладнює хакерам вразити систему та викрасти особисті дані, оскільки немає центральної точки збою.

– Захист від несанкціонованого втручання: після запису даних у блокчейні їх майже неможливо змінити чи видалити, що гарантує цілісність і автентичність персональних даних.

– Підвищена транспарентність: технологія блокчейн забезпечує високий ступінь прозорості, оскільки всі транзакції видно та реєструються в загальнодоступній базі. Це дозволяє легко відстежувати, хто і коли отримав доступ до персональних даних.

– Конфіденційність: забезпечення анонімності користувачів, які на відкритих блокових ланцюгах представлені буквено-цифровими загальнодоступними адресами.

Традиційні методи захисту персональних даних є недостатньо ефективними, зокрема в Україні. Інцидент з масовим витоком персональних даних громадян України з додатку "Дія", переважно з водійських прав, є тому підтвердженням. Справжню причину витоку даних ще належить встановити. Проте це грубе порушення прав людей, яке не можна не оминути [6]. А Європейський Союз для удосконалення захисту даних підійшов з юридичної сторони. У 2018 році був прийнятий Загальний регламент захисту даних (GDPR), який встановлює жорсткі вимоги до обробки персональних даних. Вони включають те, що персональні дані мають збиратися законно, прозоро та з дотриманням цільових обмежень, а також важливо те, що юридичні особи несуть значну відповідальність за порушення вимог Регламенту про захист персональних даних. Про ефективність застосування GDPR свідчить статистика, адже за два роки роботи за невідповідність зібрано майже 360 млн євро. Водночас ця статистика свідчить про те, що в Європі все ще є проблеми із захистом персональних даних.

Впровадження блокчейну як технології для захисту персональної інформації має також включати законодавчі нюанси. Відповідно до Загального регламенту захисту даних ЄС (GDPR) є певні протиріччя між технологією блокчейн і захистом даних [7]. GDPR був розроблений за умови того, що персональні дані обробляються централізовано, а застосування

децентралізованих технологій, таких як блокчейн, не відповідають вимогам GDPR. До того ж суть безпеки блокчейну суперечить конфіденційності, необхідної для захисту персональних даних. Щодо України, то, по-перше, за статтею 32 Конституції України встановлено, що конфіденційна інформація про особу не може збиратися, зберігатися, використовуватися та поширюватися без її згоди, а по-друге, виклики, що створює цифрова трансформація українського бізнесу та державних інституцій, та бажання України вступити до ЄС потребує удосконалення законодавства і впровадження правил міжнародного регламенту з GDPR [8] . Тож, в Україні правила регламенту мають діяти.

Про "значне напруження між сутністю технології блокчейну та загальною структурою Загального регламенту захисту персональних даних» було зазначено European Parliamentary Research Service («EPRS») у своєму брифінгу до дослідження 2019 року «Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law» [9]. У результаті розробка проекту блокчейну повинна включати ретельний аналіз того, які дані зберігаються.

Загалом, обробка персональних даних без дозволу суб'єкти є забороненою. Згідно зі статтею 2 Закону України "Про захист персональних даних" "обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем".

Фактично кожен процес блокчейн-системи включений в поняття «обробка даних». Це стосується транзакцій інформації через вузли, зберігання хешів, процесу перевірки, а також це збереження та синхронізація за допомогою децентралізованої системи. Блокчейн повинен регулярно оновлюватись серед усіх учасників мережі, щоб кожен мав найновішу версію повної бази даних – це також вважається обробкою даних. Усі учасники роботи блокчейну – не лише партнери по транзакціях і майнери, а й вузли – беруть участь в обробці даних.

Також виникає проблема з принципом мінімізації даних, коли резервне зберігання обмежене і записи, про персональну інформацію зокрема, зберігаються доти, поки вони потрібні з певної мети. А ось принцип блокчейну і аспект його безпеки якраз полягає в тому, щоб поширювати мережу. Відкритість і прозорість також є проблемами для конфіденційності.

Отже, необхідно знайти умови за яких обробка і мінімізація персональної інформації буде можливою. Першим і найочевиднішим буде запит дозволу клієнта на обробку даних, але є певні перешкоди, що роблять цей метод недієвим. Декларація про згоду вимагає, щоб суб'єкт, що надає дані був проінформований про те, кому будуть передані дані. Неможливо визначити до яких вузлів чи майнерів потрапить ця інформація, неможливо передбачити, хто в майбутньому може бути залучений до мережі чи перегляне дані. Видалення блоків блокчейн взагалі є неможливим, адже основа безпеки технології. Але є варіант в побудові системи таким чином, щоб не можна не було ідентифікаційних даних або обмеження доступу.

Прикладом успішного використання технологій блокчейну, що сумісний із GDPR, є блокчейн заснований на платформі Emercoin, що зберігає дані поза мережею.

Суб'єкти даних вводять персональні дані через веб-інтерфейс, захищений протоколом HTTPS. Внутрішня система шифрує дані, обчислює їхній хеш-ідентифікатор, зберігає зашифровані дані разом із хеш-ідентифікатором і вставляє хеш-ідентифікатор у сховище Emercoi. Таким чином за використання public-private-key cryptography асиметрична криптографія чи криптографічні хеш функції" дані стають анонімними, хоча водночас існування obfuscation techniques (технологія дешифрування кодів), уможливлює доступ до значення хеш-кодів.

За такої логіки роботи та протоколів блокчейн є сумісним із GDPR: легко ідентифікувати того, хто обробляє дані, може бути укладена прозора і законна згода з суб'єктом даних, забезпечується право знати, які дані обробляються, з якою метою та кому вони надаються, дані обробляються безпечним способом, суб'єкти даних мають контроль над

особистими даними: дані можуть бути зміненими і хеш-код буде також оновленим, видалення здійснюється щойно закінчиться термін зберігання чи за запитом суб'єкта даних [10].

Технології блокчейн мають великий потенціал застосування у галузях, що працюють з персональною інформацією, якщо вони будуть врегульовані на законодавчому рівні. Серед таких галузей є медицина та охорона здоров'я. Принципи блокчейну підходять для ведення єдиного бази пацієнтів, лікарів та медичних записів, відстеження поставок лікарських препаратів, дистанційний моніторинг пацієнтів за допомогою мобільних технологій, що зменшує потребу в амбулаторних відвідуваннях і дозволяє дистанційно перевіряти рецепти та інші медичні дані. Це підвищить точність і повноту медичної документації, зменшить адміністративне навантаження.

Електронні медичні записи, що містять персональні дані, використовують задля ефективного обстеження, діагностики та лікування. Цими записами обмінюються лікарі різного профілю аби провести якісну медичну послугу, але під час обміну такою інформацією може виникнути ряд проблем: дані можуть бути втрачені, незареєстровані або змінені. У 2015 році CRICO, підрозділ Фонду управління ризиками Гарвардської медичного університету, проаналізував понад 23 000 заяв і позовів про медичну недбалість, у яких пацієнти зазнали певної шкоди, і виявили, що три з кожних десяти випадків (7149 випадків) включають принаймні один конкретний збій у комунікації [11]. На збій комунікації можуть вплинути не лише навички спілкування, а й випадки того, що медична інформація були неправильно сформована чи незафіксована. Рішенням цієї проблеми є створення бази інформації, що буде сумісною та доступною для всіх. Прозорий обмін даними забезпечить підвищення якості діагностики, інформування про медичні рішення та лікування, а також зменшить ситуації, що шкодять пацієнтам.

Є ряд переваг блокчейну для медичної сфери (Таблиця 1).

Таблиця 1.

Переваги застосування блокчейну для персональних даних пацієнтів клінік

Безпека	Доступ є децентралізованим, що мінімізує ризики хакерських атак.
Хронологія	Інформація в ланцюзі розташована в часовому порядку.
Конфіденційність	Інформація є закодованою і доступна лише за наявності паролю.
Цілісність інформації	Фальсифікація даних є неможливою, інформація в блокчейні не може бути змінена чи видалена без дозволу.
Доступність	До бази можна підключитися з будь-якого пристрою з доступом до Інтернету.

Прикладом впровадження технологій блокчейну в медичній сфері є Естонія. У 2011 році уряд Естонії разом із Guardtime, компанією з кібербезпеки, заснованою в Естонії в 2007 році, застосував технології блокчейну Keyless Signature Infrastructure (KSI) для захисту медичних записів. Основна передумова KSI полягає в тому, що, використовуючи лише криптографію з хеш-функціями В Естонії кожен, хто звертався до лікаря, має власну електронну медичну картку, яку можна переглядати онлайн. Національна інформаційна система охорони здоров'я об'єднує дані від різних постачальників медичних послуг в Естонії для створення спільного запису для кожного пацієнта (станом на 2015 рік понад 95% даних, отриманих лікарнями та лікарями, було оцифровано). Це дозволяє лікарям легко отримувати доступ до електронних медичних записів (тобто результатів аналізів, рентгенівських знімків). Пацієнти можуть переглянути свої попередні візити до лікаря, поточні рецепти, отримати загальні поради щодо здоров'я тощо [12].

Висновки. Блокчейн — це технологія, яка забезпечує захист даних від маніпуляцій завдяки складнощам керування кожною копією блокчейну в мережі. Отже, у цьому сенсі це

підвищує безпеку даних. Безпека досягається завдяки тому, що записи, збережені в блокчейні, стають прозорими та незмінними. А це, у свою чергу, досягається за рахунок резервного та розподіленого зберігання кожного запису на кількох вузлах у великій мережі. Впровадження технології блокчейн у клініках має потенціал для революції в галузі охорони здоров'я та покращення захисту персональних даних. Переваги використання технології блокчейн для захисту даних у галузі охорони здоров'я численні (прозора платформа для обміну персональної інформацією про пацієнтів між постачальниками медичних послуг без шкоди для конфіденційності пацієнтів, точність і послідовність даних, що мінімізує помилки і шахрайство, доступ пацієнтів до контролю над своїми особистими даними про здоров'я, зокрема, хто має до них доступ і як вони використовуються).

Список використаних джерел

1. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 р. № 2801-XII : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text
2. Захист персональних даних у сфері охорони здоров'я: Ірина Сенюта розповіла про дієві інструменти в роботі адвоката | ADVOKAT POST. ADVOKAT POST. URL: https://advokatpost.com/zakhyst-personalnykh-danykh-u-sferi-okhorony-zdorov-ia-iryna-seniuta-rozpovila-pro-diievi-instrumenty-v-roboti-advokata/ (дата звернення: 03.04.2023).
3. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. Костюк П. П. Використання технології блокчейн для забезпечення інформаційної безпеки. *Сучасний захист інформації*. 2020. № 3 (43). С. 22–28.
5. Ярова М. Навіщо впроваджувати блокчейн в державний устрій і як це допоможе у боротьбі з корупцією. *AIN.UA*. URL: https://ain.ua/2022/12/29/bornjakov-pro-blockchain/
6. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн - Юридична Газета. *Юридична газета*. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html
7. Zimprich S. Data protection and blockchain. *dotmagazine*. URL: https://www.dotmagazine.online/issues/security-trust-in-digital-services/data-protection-and-blockchain.
8. Керівник напряму GDPR компанії Nota Group Олена Колченогова виступила на круглому столі «Захист персональних даних в Україні: перспективи євроінтеграції», організованному асоціацією DigitalUkraine - Nota Group. *Nota Group*. URL: http://surl.li/jzvhb/ (дата звернення: 06.04.2023).
9. European Parlament. Blockchain and the General Data Protection Regulation. *BRIEFING*. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf.
10. Dighmelashvili E., Nanadze A., Kotliarov Y., Tsyba S., Blockchain technology is here – is it compliant with GDPR? Електронний ресурс. URL: http://surl.li/ghzxl
11. Malpractice Risks in Communication Failures. CRICO. URL: http://surl.li/ghzxb
12. E-health in Estonia. Republic of Estonia (Ministry of Social Affairs). URL: https://na.eventscloud.com/file_uploads/c5da2a5e465f932e6debe55020e70899_E-health-factsheet.pdf

Робота виконана під науковим керівництвом к.т.н., доцента
ТОКАРА В. В.

SDN МЕРЕЖА ТА ЇЇ ЗАГРОЗИ

МАРЧЕНКО Б., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Програмно-конфігуровані Мережі (Software Defined Networking/SDN) – це поділ площини передачі та управління даними, що дозволяє здійснювати програмне управління площиною передачі, яке може бути фізично або логічно відокремлено від апаратних комутаторів та маршрутизаторів.

Software-defined Networks (Software Defined Networking/SDN) are division of the plane of transmission and data management, which allows to carry out software control of the transmission plane, which can be physical or logically separated from hardware switches and routers.

Актуальність. В останні роки відбулося величезне зростання мережевого трафіку операторів. Значною мірою це було викликано вибуховим зростанням використання онлайн-додатків і хмарних сервісів постійно зростаючим набором дротових і мобільних пристроїв, підключених до мережі. Сьогодні мережеві оператори мають працювати з великою кількістю форматів даних, типів послуг і онлайн-пристроїв, і все це без збільшення операційних витрат і витрат на обладнання.

Однак застарілі мережеві архітектури та їхні інструменти керування не були розроблені, щоб впоратися з таким надзвичайно еластичним попитом. Це суттєво обмежує здатність оператора рентабельно реагувати на вимоги до масштабу, продуктивності та взаємодії з користувачем у сучасних динамічних середовищах або розгортати диференційовані послуги.

SDN забезпечує поділ між функціями площини керування (контролер) і площини даних (комутатор) мереж за допомогою протоколу, який змінює таблиці пересилання в мережевих комутаторах. Це дає змогу оптимізувати мережі на льоту та швидко реагувати на зміни у використанні мережі без необхідності вручну переналаштовувати існуючу інфраструктуру чи купувати нове обладнання. SDN відокремлює керування мережевими пристроями від даних, які вони передають, а комутаційне програмне забезпечення від фактичного мережевого обладнання. Загалом, системи захисту інформації в SDN-мережах на основі протоколу OpenFlow є важливим напрямом досліджень в області мережевої безпеки. Вони дозволяють забезпечити високий рівень захисту мережевої інфраструктури від різних видів атак, що забезпечує надійність та безпеку роботи мережі.

OpenFlow — це протокол зв'язку, який надає доступ до площини пересилання мережевого комутатора або маршрутизатора через мережу.

OpenFlow дозволяє мережевим контролерам визначати шляхи мережевих пакетів у мережі комутаторів. Контролери відрізняються від перемикачів. Це відокремлення контролю від пересилання дозволяє більш складне керування трафіком, ніж це можливо за допомогою списків контролю доступу (ACL) і протоколів маршрутизації.

Метою статті є дослідження основних методів захисту SDN-мереж, включаючи захист від атак на різних рівнях мережі.

Об'єктом дослідження є розробка програмного забезпечення системи захисту інформації в SDN мережі.

Предмет дослідження – SDN мережа.

Аналіз попередніх досліджень. Дослідженню SDN мереж та їх загроз присвячені праці наступних науковців: Jamison Kush (Джемісон Куш), Jim Doherty (Джим Доерті), Kingston Smiler (Кінгстон Сміллер), Doug Marschke (Дуг Марке) та інші.

Виклад основного матеріалу. На сьогоднішній день необхідно знати різницю між традиційною мережею та мережею. Порівняльна характеристика подана в табл. 1.

Таблиця 1

Порівняльна характеристика SDN мережі та традиційної мережі

№	SDN	ТРАДИЦІЙНА МЕРЕЖА
1	Мережа, визначена програмним забезпеченням, — це віртуальний мережевий підхід.	Традиційна мережа — це старий традиційний мережевий підхід.
2	Програмно визначена мережа – це централізоване керування.	Традиційна мережа – це розподілене управління.
3	Ця мережа є програмованою.	Ця мережа не програмується.
4	Програмно визначена мережа є відкритим інтерфейсом.	Традиційна мережа має закритий інтерфейс.
5	У програмно визначеній мережі площина даних і площина керування роз'єднані програмним забезпеченням.	У традиційній мережі площина даних і площина керування монтуються на одній площині.
6	Він підтримує автоматичне налаштування, тому це займає менше часу.	Він підтримує статичну/ручну конфігурацію, тому це займає більше часу.
7	Він може визначати пріоритети та блокувати певні мережеві пакети.	Він веде всі пакети однаково без підтримки пріоритетів.
8	Його легко програмувати відповідно до потреб.	Важко заново запрограмувати та замінити існуючу програму відповідно до використання.
9	Вартість програмно визначеної мережі низька.	Вартість традиційної мережі висока.
10	Структурна складність у програмно визначеній мережі низька.	Структурна складність традиційної мережі висока.
11	Розширюваність висока в програмно визначеній мережі.	Розширюваність у традиційній мережі низька.
12	У SDN легко виявляти несправності та звітувати, оскільки вона централізована.	У традиційній мережі важко усунути несправності та повідомити про них, оскільки вона розподіляється під контролем.
13	Його вартість обслуговування нижча, ніж традиційна мережа.	Вартість обслуговування традиційної мережі вища, ніж SDN.

Традиційна мережа відноситься до старого традиційного способу роботи в мережі, який використовує фіксовані та виділені апаратні пристрої, такі як маршрутизатори та комутатори, для контролю мережевого трафіку.

Неможливість масштабування, безпека та продуктивність мережі є головною проблемою в нинішній зростаючій бізнес-ситуації, тому SDN бере під контроль традиційну мережу. Традиційна мережа є статичною та базується на апаратних мережевих пристроях.

SDN означає мережу, визначену програмним забезпеченням, яка є підходом до мережевої архітектури. Він дозволяє контролювати та керувати мережею за допомогою програмних додатків. Через програмно визначену мережу (SDN) мережева поведінка всієї мережі та її пристроїв програмується централізовано за допомогою програмних додатків із використанням відкритих API.

Програмно визначена мережа покращує продуктивність завдяки віртуалізації мережі. У SDN керовані програмним забезпеченням додатки або API працюють як основа повного

керування мережею, яка може спрямовувати трафік у мережі або спілкуватися з основною апаратною інфраструктурою [1]. Пропоную розглянути архітектуру SDN мережі (рис.1).

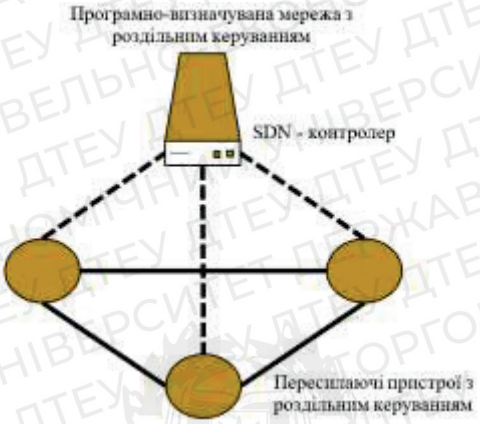


Рис. 1. Архітектура SDN мережі

Архітектура SDN містить п'ять основних компонентів. Кожен з цих компонентів має невід'ємну роль у роботі мережі, у полегшенні роботи обладнання та його обслуговуванні адміністратором мереж.

1. Компонент керування

У SDN використовується набір мережевих додатків для гнучкого керування та простоти реалізації нових додатків та сервісів (маршрутизації, балансування навантаження, застосування політик або рекомендований додаток від постачальника послуг). За допомогою існуючих API організується та автоматизується мережа.

2. Компонент контролю

Є найбільш інтелектуальним та важливим рівнем архітектури SDN. Містить один або кілька контролерів, що пересилають різні типи правил та політик на рівень інфраструктури через південний інтерфейс.

3. Компонент даних

По-третє, рівень даних, також відомий як рівень інфраструктури, представляє пристрої пересилання мережі (маршрутизатори, комутатори, балансувальники навантаження тощо. буд.). Він використовує південні API-інтерфейси для взаємодії з площиною управління, отримуючи правила та політики переадресації для застосування їх до відповідних пристроїв.

4. Північний інтерфейс

Інтеграція між контролером та додатком. В основному інтерфейси є набір інтерфейсів прикладного програмування (API) з відкритим вихідним кодом.

5. Південні інтерфейси

Інтеграція між контролером та мережевими пристроями. Інтерфейси дозволяють передавати політики на площину пересилання.

SDN мережа, в порівнянні з іншими традиційними мережами з розподіленим керуванням має наступні переваги:

- Збільшення видимості мережі;

Огляд мережі в одному місці, що усуває сліпі зони, які є у традиційних мережах.

- Масштабованість;

Гнучкість SDN значно полегшує масштабування бізнес-операцій без ризику перебоїв в обслуговуванні.

- Сумісність із великими даними;

Висока пропускна здатність для паралельної обробки даних та управління ними.

- Поліпшена безпека

З централізацією SDN адміністратори зможуть розробляти та розповсюджувати важливі політики та протоколи безпеки по всій мережі по всіх пристроях та важливих компонентах.

- Відкритий вихідний код;

SDN слід відкритим стандартам та використовується з мережевим обладнанням будь-якого постачальника. Тобто SDN може підключатися до різних хмар, пристроїв та програм.

- Більш ефективний IT-відділ;

Оскільки SDN оптимізує та спрощує керування мережею, ваші IT-фахівці зможуть зосередитися на покращенні надання послуг.

- Економічна ефективність;

SDN дешевше в експлуатації та має нижчу сукупну вартість, вимагаючи менше витрат та підвищуючи ефективність використання сервера [2].

В період сьогодення, більшість SDN мереж використовують стандарт OpenFlow. Давайте розглянемо, що ж таке OpenFlow.

OpenFlow (OF) вважається одним із перших програмно-визначених мережевих стандартів (SDN) .

Він спочатку визначив протокол зв'язку в архітектурах SDN , який дозволив контролеру SDN безпосередньо взаємодіяти з площиною пересилання мережевих пристроїв, таких як комутатори та маршрутизатори, як фізичні, так і віртуальні (на основі гіпервізора), щоб він міг краще адаптуватися до мінливих вимог бізнесу.

Контролер SDN у SDN — це «мозок» мережі SDN, який передає інформацію на комутатори/маршрутизатори «внизу» (через південні API), а програми та бізнес-логіку «вгорі» (через північні API). Останнім часом, коли організації розгортають більше віртуальних накладених мереж SDN , контролерам SDN було доручено об'єднати домени контролерів SDN за допомогою загальних інтерфейсів додатків, таких як OpenFlow і відкрита база даних віртуальних комутаторів (OVSDB).

Щоб працювати в середовищі OF, будь-який пристрій, який хоче спілкуватися з контролером SDN, повинен підтримувати протокол OpenFlow . За допомогою цього інтерфейсу контролер SDN вносить зміни в таблицю потоків комутатора/ маршрутизатора , дозволяючи мережевим адміністраторам розділяти трафік [3].

SDN на основі OpenFlow наразі розгортається в різноманітних мережевих пристроях і програмному забезпеченні, надаючи значні переваги як підприємствам, так і операторам, зокрема:

- Централізоване управління та контроль мережевих пристроїв від кількох постачальників;
- Швидкі інновації завдяки можливості надавати нові мережеві можливості та послуги без необхідності налаштовувати окремі пристрої чи чекати випусків від постачальників;
- Можливість програмування операторами, підприємствами, незалежними постачальниками програмного забезпечення та користувачами (не лише виробниками обладнання) за допомогою загального середовища програмування, що дає всім сторонам нові можливості для підвищення прибутку та диференціації;
- Підвищена надійність і безпека мережі завдяки централізованому й автоматизованому управлінню мережевими пристроями, уніфікованому застосуванню політики та меншій кількості помилок конфігурації;
- Більш детальний контроль мережі з можливістю застосування комплексних і широкомасштабних політик на рівні сеансу, користувача, пристрою та програми;
- Кращий досвід роботи з кінцевим користувачем, оскільки додатки використовують централізовану інформацію про стан мережі [4].

Записи таблиці потоків, якими можна маніпулювати в комутаторі OF (Рис.2).

Рис. 2. Робота в комутаторі OpenFlow

Розвиток мереж породжує нові типи атак, виявлені та невизначені ризики та експлойти нульового дня. Наразі немає історії попередніх реальних атак SDN, тому важко визначити наявні вразливості та створити на їх основі захист.

1. Маніпуляція мережею : критична атака, яка відбувається на площині керування. Зловмисник компрометує контролер SDN, створює неправдиві дані мережі та ініціює інші атаки на всю мережу.

Як захиститися: щоб пом'якшити цю атаку, контролер SDN повинен мати надлишковий об'єкт, а канали зв'язку мають бути захищені за допомогою надійного шифрування.

2. Перенаправлення трафіку : ця атака відбувається на елементи мережі в площині даних. Атака компрометує мережевий елемент, щоб перенаправити потоки трафіку та дозволити прослуховування.

Як захиститися: Захистіть елементи мережі та її канали зв'язку за допомогою надійного шифрування.

3. Атака по бічному каналу : об'єктом цієї атаки можуть бути елементи мережі в площині даних. Інформація про час, наприклад, скільки часу потрібно для встановлення нового мережевого з'єднання, може повідомити зловмиснику, чи існує правило потоку, чи ні.

Як захиститися: Захистіть елементи мережі за допомогою надійного алгоритму шифрування.

4. Маніпуляція програмою : ця атака відбувається в площині програми. Використання вразливості програми може спричинити несправність, перебої в роботі служби або прослуховування даних. Зловмисник може отримати доступ із високими привілеями до програми SDN і виконувати незаконні операції.

Як захиститися: постійно оновлюйте сервери останніми виправленнями.

5. Відмова в обслуговуванні «DoS» : це одна з найпоширеніших атак, яка може впливати на всі частини SDN. Застосувавши DoS, зловмисник може призвести до зниження або повного зриву служб SDN.

Як захиститися: використовуйте методи обмеження швидкості та скидання пакетів.

6. ARP Spoofing Attack : атака Man-in-the-middle, яка також називається отруєнням кешу ARP. Хакер може використовувати ARP-спуфінг, щоб проникнути в мережу, перехопити трафік, змінити його та навіть зупинити. Цей тип атаки пошкоджує інформацію про топологію мережі та додатки SDN, що володіють топологією. Отруєння також може статися через інші протоколи, такі як LLDP або IGMP.

Як захиститися: Рекомендується використовувати надійні методи автентифікації.

7. Експлуатація API : API компонента програмного забезпечення можуть містити вразливості, які можуть дозволити хакеру здійснити несанкціоноване розкриття інформації. Експлуатація API також може статися на північному інтерфейсі та може призвести до руйнування мережевих потоків.

Як захиститися: постійно оновлюйте сервери останніми виправленнями.

8. Перехоплення трафіку : атаки перехоплення – це популярний метод, який використовують хакери для захоплення та аналізу інформації мережевого зв'язку. За допомогою сніфінгу хакер також може підслуховувати дані з мережевих елементів або посилань і викрадати важливу інформацію. Нюхання може статися будь-де, де є постійний рух. У SDN хакер може скористатися перевагами незашифрованого зв'язку, щоб перехопити трафік від центрального контролера та до нього. Зібрані дані можуть включати важливу інформацію про потоки або трафік, дозволений у мережі.

Як захиститися: використовуйте надійний метод шифрування.

9. Вгадування пароля або груба сила : ця атака може відбутися на елементі, що не є SDN. За допомогою вгадування пароля або грубої сили неавторизований користувач може отримати доступ до SDN.

Як захиститися: змініть паролі постачальників за замовчуванням, використовуйте надійні паролі та часто оновлюйте їх [5].

Висновки. Чи може SDN підвищити безпеку? Розгортання SDN все ще незріле, і важко передбачити, як зловмисники будуть націлюватися на інфраструктуру SDN. Знання про атаки та загрози SDN дуже обмежені. Те, що ми бачили та дізналися в історії кібератак і контратак у традиційних мережах, це те, що нові технології приходять разом із новими вразливими місцями .

Щоб повністю присвятити себе SDN, потрібно подбати про деякі проблеми безпеки, наприклад централізоване керування мережею та функції програмування . Але технологія не поверне нас назад у часі, SDN набирає популярності, а її вдосконалення відбуваються надзвичайно швидко. Ймовірно, завдяки SDN ми побачимо набагато більше переваг безпеки порівняно з традиційними мережами.

Список використаних джерел

1. Topology Discovery in Software Defined Networks: Threats, Taxonomy, and State-of-the-Art \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/7534866 (останнє звернення 27.02.2023р.)
2. Security in Software-Defined Networking: Threats and Countermeasures \\ Режим доступу: https://link.springer.com/article/10.1007/s11036-016-0676-x (останнє звернення 27.02.2023р.)
3. Software-Defined Networking: A Comprehensive Survey \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/6994333 (останнє звернення 01.03.2023р.)
4. Jennia Hizver, Taxonomic Modeling of Security Threats in Software Defined Networking \\ Режим доступу: https://www.gti.bh/Library/assets/us-15-hizver-taxonomic-modeling-of-security-threats-in-software-defined-networking-wp.pdf (останнє звернення 01.03.2023р.)
5. SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT\\ Режим доступу: https://www.mdpi.com/2079-9292/10/8/918 (останнє звернення 05.03.2023р.)

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

ТЕХНОЛОГІЇ IDS ТА IPS ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІДПРИЄМСТВА РІТЕЙЛУ

МАРЧУК Б., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Підприємства роздрібної торгівлі збирають величезну кількість персональних даних своїх клієнтів, включаючи імена, адреси, номери телефонів та інформацію про кредитні картки. Таким чином, захист цих даних має вирішальне значення для підтримки довіри клієнтів і уникнення дорогого витоку даних. Останніми роками багато підприємств роздрібної торгівлі запровадили технологію захисту персональних даних, щоб захистити особисту інформацію своїх клієнтів.

Retail businesses collect vast amounts of personal data about their customers, including names, addresses, phone numbers and credit card information. Protecting this data is therefore critical to maintaining customer trust and avoiding costly data breaches. In recent years, many retailers have implemented data protection technology to protect their customers' personal information.

Актуальність. Однією з поширених технологій, що використовується роздрібними підприємствами, є шифрування даних. Це передбачає перетворення конфіденційної інформації в нечитабельний код, який можна розшифрувати лише за допомогою правильного ключа. Підприємства роздрібної торгівлі можуть використовувати шифрування для захисту даних клієнтів як під час передачі через Інтернет, так і під час їх зберігання на своїх серверах.

Ще одна важлива технологія для захисту персональних даних – брандмауери. Брандмауери — це програми, які обмежують несанкціонований доступ до мережі компанії. Впроваджуючи брандмауери, підприємства роздрібної торгівлі можуть запобігти доступу кіберзлочинців до особистої інформації своїх клієнтів.

Окрім шифрування та брандмауерів, підприємства роздрібної торгівлі також можуть впроваджувати системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS). IDS та IPS — це програми, які можуть виявляти та блокувати кібератаки в реальному часі. Ці технології можуть допомогти підприємствам роздрібної торгівлі запобігти витоку даних і захистити особисту інформацію своїх клієнтів.

Нарешті, роздрібні підприємства також можуть використовувати технологію маскування даних. Маскування даних передбачає заміну конфіденційних даних фіктивними, щоб вихідні дані були недоступні неавторизованим користувачам. Роздрібні підприємства можуть використовувати маскування даних для захисту конфіденційних даних, таких як номери кредитних карток або номери соціального страхування.

Метою статті є дослідження та класифікація технологій захисту на підприємствах роздрібної торгівлі.

Об'єктом дослідження є розробка програмного забезпечення захисту підприємств роздрібної торгівлі.

Предмет дослідження – захист персональних даних.

Аналіз попередніх досліджень. Дослідженню менеджерів паролів присвячені праці наступних науковців: Wanda Presthus(Ванда Престус), Linda Andersen(Лінда Андерсен), David Prepletany(Девід Преплетані), Deyan Chen(Деян Чен), Hong Zhao(Хонг Чжао), , Indu Niranjan(Інду Ніранджан), Varun Tandon(Варун Тандон) та інші.

Виклад основного матеріалу. У даній статті ми розглянемо систему виявлення вторгнень (IDS), та систему запобігання вторгнень (IPS) на підприємстві. На рисунку 1 зображена схема роботи системи виявлення вторгнень.

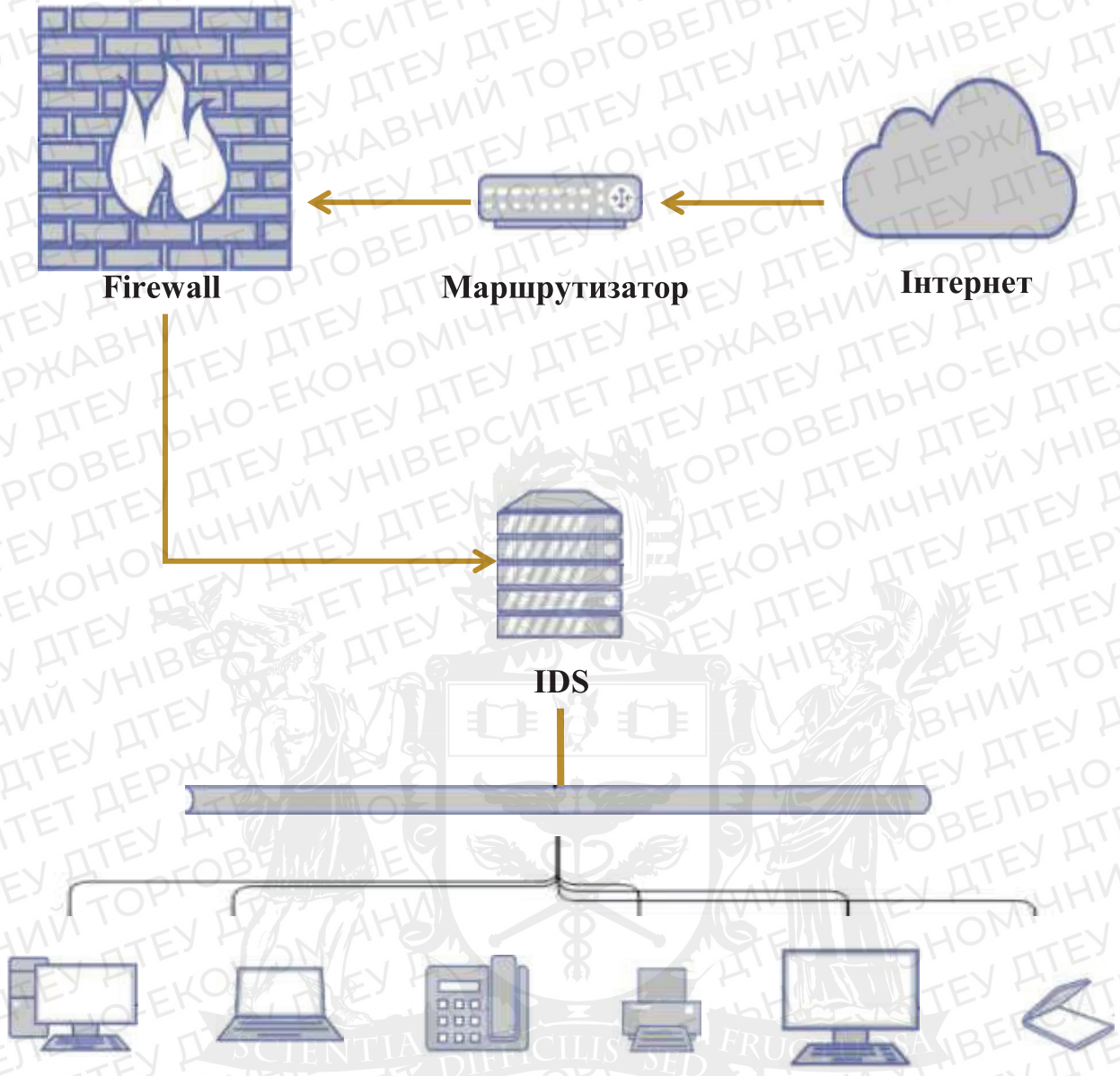


Рис. 1. Принцип роботи системи IDS

Система виявлення вторгнень (IDS) — це технологія мережевої безпеки, спочатку розроблена для виявлення уразливостей цільової програми або комп'ютера.

IDS також є пристроєм лише для прослуховування. IDS відстежує трафік і повідомляє результати адміністратору. Він не може автоматично вжити заходів, щоб запобігти виявленому експлойту захопити систему.

Зловмисники здатні швидко використовувати вразливі місця, коли вони проникають у мережу. Таким чином, IDS не підходить для профілактики. Системи виявлення та запобігання вторгненням важливі для безпеки інформації та керування подіями.

Коли була розроблена IDS, глибина аналізу, необхідна для виявлення вторгнення, не могла бути виконана досить швидко. Швидкість не встигає за компонентами на прямому шляху зв'язку мережевої інфраструктури.

Системи виявлення мережевих вторгнень використовуються для виявлення підозрілої активності, щоб зловити хакерів до того, як буде завдано шкоди мережі. Існують мережеві та хост-системи виявлення вторгнень. IDS на основі хоста встановлюються на клієнтські комп'ютери; мережеві IDS знаходяться в самій мережі.

IDS працює, шукаючи відхилення від нормальної активності та відомі сигнатури атак. Аномальні шаблони надсилаються в стек і перевіряються на протокольному та прикладному

рівнях. Він може виявляти такі події, як отруєння DNS, неправильно сформовані інформаційні пакети.

IDS може бути реалізований, як пристрій безпеки мережі або програмне забезпечення. Для захисту даних і систем у хмарних середовищах також доступні хмарні IDS.

Тепер пропоную розглянути основні типи IDS: на основі мережі, на основі хоста, на основі протоколу, на основі протоколу програми та гібридний.

Два найпоширеніші типи IDS:

1. Мережева система виявлення вторгнень (NIDS).

Мережева IDS контролює всю захищену мережу. Він розгортається по всій інфраструктурі в стратегічних точках, таких як найбільш уразливі підмережі. NIDS відстежує весь трафік, що надходить до та від пристроїв у мережі, роблячи визначення на основі вмісту пакетів і метаданих.

2. Система виявлення вторгнень на основі хоста (HIDS).

IDS на основі хоста відстежує комп'ютерну інфраструктуру, на якій її встановлено. Іншими словами, він розгортається на певній кінцевій точці, щоб захистити її від внутрішніх і зовнішніх загроз. IDS досягає цього, аналізуючи трафік, реєструючи зловмисну активність і повідомляючи призначені органи.

Решта три типи можна описати так:

3. На основі протоколу (PIDS).

Система виявлення вторгнень на основі протоколу зазвичай встановлюється на веб-сервері. Він відстежує та аналізує протокол між користувачем/пристроєм і сервером. PIDS зазвичай знаходиться на передній частині сервера та контролює поведінку та стан протоколу.

4. На основі протоколу додатків (APIDS).

APIDS — це система або агент, який зазвичай знаходиться всередині серверної сторони. Він відстежує та інтерпретує листування за протоколами, що стосуються окремих програм. Наприклад, це відстежуватиме протокол SQL для проміжного програмного забезпечення під час транзакцій із веб-сервером.

5. Гібридна система виявлення вторгнень.

Гібридна система виявлення вторгнень поєднує два або більше підходи до виявлення вторгнень. Використання цієї системи, даних системи або хост-агента в поєднанні з мережевою інформацією для повного уявлення про систему. Гібридна система виявлення вторгнень більш потужна порівняно з іншими системами.

Але зловмисники можуть використовувати численні методи, щоб уникнути виявлення IDS. Ці методи можуть створити проблеми для IDS, оскільки вони призначені для обходу існуючих методів виявлення:

- Фрагментація.

Фрагментація ділить пакет на менші фрагментовані пакети. Це дозволяє зловмиснику залишатися прихованим, оскільки не буде сигнатур атаки для виявлення.

Фрагментовані пакети пізніше реконструюються вузлом одержувача на рівні IP. Потім вони пересилаються на прикладний рівень. Атаки фрагментації генерують шкідливі пакети шляхом заміни даних у складових фрагментованих пакетах новими даними.

- Затоплення

Ця атака спрямована на перевантаження детектора, викликаючи збій механізму керування. Коли детектор виходить з ладу, весь трафік буде дозволено.

Популярним способом спричинити затоплення є підробка законного протоколу дейтаграм користувача (UDP) і протоколу керуючих повідомлень Інтернету (ICMP). Затоплення трафіку потім використовується для маскування аномальної діяльності зловмисника. У результаті IDS матиме великі труднощі з пошуком шкідливих пакетів у величезному обсязі трафіку.

- Обфускація.

Обфускацію можна використовувати, щоб уникнути виявлення, роблячи повідомлення складним для розуміння, тим самим приховуючи атаку. Термінологія обфускації означає зміну програмного коду таким чином, щоб він залишався функціонально нерозрізненим.

- Шифрування

Шифрування пропонує численні можливості безпеки, включаючи конфіденційність даних, цілісність і конфіденційність. На жаль, розробники шкідливих програм використовують атрибути безпеки, щоб приховати атаки та уникнути виявлення[1].

Також необхідно розібратися у роботі системи запобігання вторгненням (IPS). На рисунку 2 показано, як працює дана система.

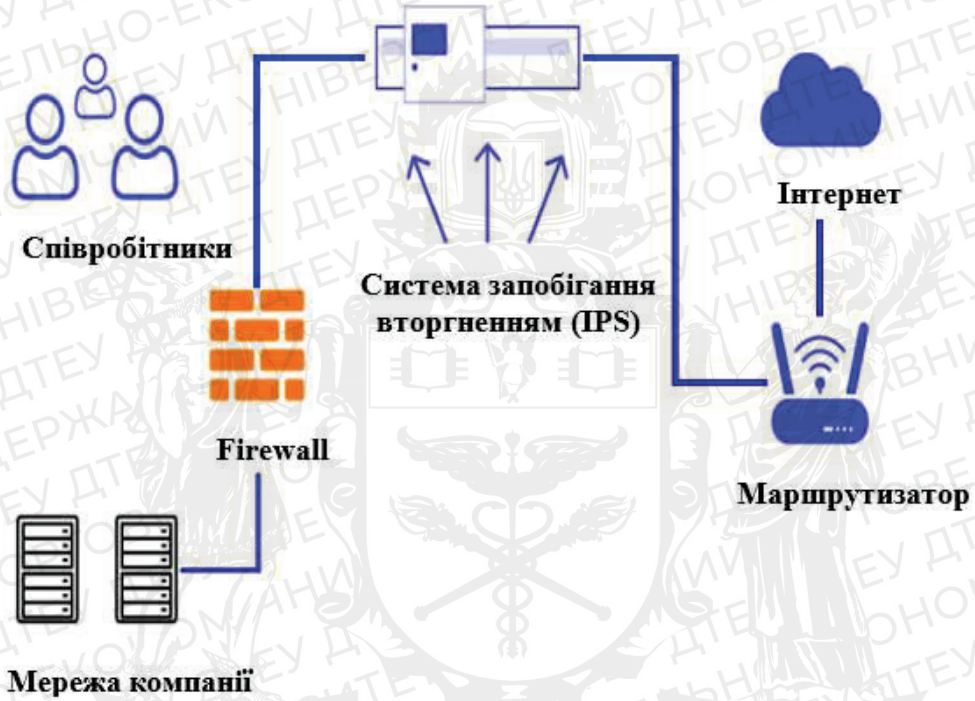


Рис. 2. Принцип роботи системи IPS

Система запобігання вторгненням (IPS) — це інструмент безпеки мережі (який може бути апаратним пристроєм або програмним забезпеченням), який постійно відстежує мережу на наявність зловмисної активності та вживає заходів для її запобігання, зокрема повідомляє, блокує або видаляє її, коли вона відбувається .

Вона є більш досконалою, ніж система виявлення вторгнень (IDS), яка просто виявляє зловмисну активність, але не може вжити заходів проти неї, окрім сповіщення адміністратора. Системи запобігання вторгненням іноді входять до складу брандмауера наступного покоління (NGFW) або рішення для єдиного управління загрозами (UTM). Як і багато інших технологій захисту мережі, вони мають бути достатньо потужними, щоб сканувати великий обсяг трафіку без зниження продуктивності мережі.

Система запобігання вторгненням розміщується в мережі, в потоці мережевого трафіку між джерелом і одержувачем, і зазвичай розташована безпосередньо за брандмауером. Існує кілька методів, які використовують системи запобігання вторгненням для виявлення загроз:

1. На основі сигнатур.

Цей метод зіставляє активність із сигнатурами відомих загроз. Одним із недоліків цього методу є те, що він може зупинити лише раніше ідентифіковані атаки та не зможе розпізнати нові.

2. На основі аномалій.

Цей метод відстежує аномальну поведінку шляхом порівняння випадкових зразків мережевої активності з базовим стандартом. Він більш надійний, ніж моніторинг на основі

сигнатур, але іноді може давати помилкові спрацьовування. Деякі новіші та вдосконалені системи запобігання вторгненням використовують штучний інтелект і технологію машинного навчання для підтримки моніторингу на основі аномалій.

3. На основі політики.

Цей метод дещо менш поширений, ніж моніторинг на основі сигнатур або аномалій. Він використовує політики безпеки, визначені підприємством, і блокує дії, які порушують ці політики. Для цього потрібен адміністратор, щоб установити та налаштувати політики безпеки.

Як тільки IPS виявляє зловмисну активність, вона може виконувати багато автоматичних дій, включаючи сповіщення адміністраторів, скидання пакетів, блокування трафіку з адреси джерела або скидання з'єднання. Деякі системи запобігання вторгненням також використовують «приманку» або приманку цінних даних, щоб залучити зловмисників і не дати їм досягти своїх цілей[2].

Існує кілька типів IPS, кожен з яких має дещо інше призначення:

- Система запобігання вторгненню в мережу (NIPS).

Цей тип IPS встановлюється лише в стратегічних точках для моніторингу всього мережевого трафіку та проактивного сканування на наявність загроз.

- Система запобігання вторгнень на хост (HIPS).

На відміну від NIPS, HIPS встановлюється на кінцевій точці (наприклад, ПК) і переглядає вхідний і вихідний трафік лише з цієї машини. Він найкраще працює в поєднанні з NIPS, оскільки служить останньою лінією захисту від загроз, які подолали NIPS.

- Аналіз поведінки мережі (NBA).

Аналізує мережевий трафік для виявлення незвичайних потоків трафіку, таких як атаки DDoS (розподілена відмова в обслуговуванні).

- Система запобігання бездротовому вторгненню (WIPS).

Цей тип IPS просто сканує мережу Wi-Fi на предмет несанкціонованого доступу та відключає неавторизовані пристрої з мережі.

Система запобігання вторгненням пропонує багато переваг:

- Додаткова безпека.

IPS працює в парі з іншими рішеннями безпеки та може ідентифікувати загрози, які не можуть ці інші рішення. Особливо це стосується систем, які використовують виявлення аномалій. Він також забезпечує чудову безпеку програм завдяки високому рівню обізнаності про програми.

- Підвищена ефективність інших елементів керування безпекою.

Оскільки IPS відфільтровує зловмисний трафік до того, як він досягне інших пристроїв безпеки та елементів керування, це зменшує навантаження на ці засоби керування та дозволяє їм працювати ефективніше.

- Економія часу.

Оскільки IPS значною мірою автоматизована, вона потребує менше часу від IT-команд.

- Відповідність.

IPS відповідає багатьом вимогам відповідності, встановленим PCI DSS, HIPAA та іншими. Він також надає цінні дані аудиту.

- Налаштування.

IPS можна налаштувати з налаштованими політиками безпеки, щоб забезпечити контроль безпеки, специфічний для підприємства, яке його використовує.

Однак організаціям слід бути обережними з IPS, оскільки вони також можуть бути схильні до помилкових спрацьовувань. Помилкове спрацьовування IPS, швидше за все, буде більш серйозним, ніж хибне спрацьовування IDS, оскільки IPS перешкоджає проходженню законного трафіку, тоді як IDS просто позначає його як потенційно шкідливий[3].

Декілька постачальників інтегрують IDS та IPS разом в один продукт — відомий як уніфіковане керування загрозами (UTM), — що дозволяє організаціям впроваджувати обидві технології, одночасно разом із брандмауерами та системами у своїй інфраструктурі безпеки.

Але нам необхідно вирішити, яка з цих систем надійніша. Тому пропоную вам розглянути таблицю 1, щоб зрозуміти основні відмінні риси цих двох технологій захисту персональних даних.

Таблиця 1

Порівняльна характеристика технологій захисту даних

	IDS	**IPS**
Ім'я	Система виявлення вторгнень	Система запобігання вторгненням
Опис	Система, яка відстежує мережевий трафік на наявність підозрілої активності та попереджає користувачів, коли така активність виявлена.	Система, яка відстежує мережевий трафік і попереджає про підозрілу активність, як IDS, але також вживає запобіжних заходів щодо підозрілої активності.
Розташування	На клієнтському комп'ютері встановлено систему виявлення вторгнень на основі хоста. Мережева система виявлення вторгнень знаходиться в мережі.	Розташований між брандмауером компанії та рештою мережі.
Використання	Попереджає про підозрілу активність, але не запобігає їй.	Попереджає про підозрілу активність і запобігає їй.
Помилково спрацьовує	Помилкові спрацьовування IDS зазвичай викликають невеликі незручності. Хоча IDS неправильно позначає законний трафік як зловмисний, це не запобігає входженню трафіку в мережу.	Хибні спрацьовування IPS можуть бути серйознішими. Коли IPS приймає законний трафік за загрозу, він зупиняє легітимний трафік від входу в мережу, що може вплинути на будь-яку частину організації, а не лише на IT-команду.

Висновки. Підсумовуючи, технологія захисту персональних даних є важливою для підприємств роздрібної торгівлі для захисту особистої інформації своїх клієнтів. Застосовуючи шифрування IDS та IPS, підприємства роздрібної торгівлі можуть запобігати кібератакам і захищати особисті дані своїх клієнтів.

Список використаних джерел

1. Information privacy from a retail management perspective \\ Режим доступу: https://www.researchgate.net/profile/WandaPresthus/publication/329040915_Information_Privacy_from_a_Retail_Managment_Perspective/links/5c29f060a6fdccfc70732ba0/Information-Privacy-from-a-Retail-Managment-Perspective.pdf (останнє звернення 27.03.2023р.)

2. Data Security and Privacy Protection Issues \\ Режим доступу: https://ieeexplore.ieee.org/abstract/document/6187862 (останнє звернення 27.03.2023р.)

3. Threat to Retail Business Information Security: Cybersecurity in the Retail Industry \\ Режим доступу: https://www.proquest.com/openview/52d446e8bcd092c8d8464d76976eb89e/1?pqorigsite=gscholar&cbl=18750 (останнє звернення 03.04.2023р.)

Робота виконана під науковим керівництвом ст. викладача
БЕБЕШКА Б.Т.

ВПЛИВ АНАЛІТИЧНИХ СИСТЕМ НА ПРОЦЕС ПРИЙНЯТТЯ РІШЕНЬ В БІЗНЕСІ

МАШЕВСКИЙ О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуті основні аспекти використання аналітичних систем в бізнесі та їх вплив на процес прийняття рішень. Розглянуто як зразок конкретні використання аналітичних систем, які допомогли покращити ефективність бізнесу, а також приведені рекомендації щодо вибору та впровадження аналітичних систем у практичну діяльність компанії.

The article covers the main aspects of using analytical systems in business and their impact on the decision-making process. Concrete examples of the specific uses of analytical systems that have helped to improve business efficiency are examined, and recommendations for selecting and implementing analytical systems in a company's practical activities are provided.

Актуальність. З появою великої кількості даних та розширенням можливостей аналітичних систем, компанії почали все більше використовувати їх для прийняття рішень в бізнесі.

Аналітичні системи дозволяють збирати, обробляти та аналізувати великі обсяги даних, в тому числі дані про попит та пропозицію, ринок та конкурентів, фінансові показники та інші фактори, що впливають на діяльність компанії. Застосування аналітичних систем дозволяє компаніям розуміти свій бізнес, виявляти тенденції та прогнозувати результати, а також приймати обґрунтовані та ефективні рішення.

Окрім того, використання аналітичних систем є необхідністю для компаній в умовах надзвичайної конкуренції та швидкісного розвитку технологій. Компанії, які не використовують аналітичні системи, можуть втратити конкурентну перевагу та не мати можливості адаптуватися до змін на ринку та в своїй галузі. Таким чином, тема є надзвичайно актуальною, оскільки використання аналітичних систем є ключовим фактором успіху для компаній в сучасному світі.

Метою статті є розгляд основних аспектів використання аналітичних систем у бізнесі та їх вплив на процес прийняття рішень. Стаття має допомогти зрозуміти, як аналітичні системи можуть допомогти вдосконалити процес прийняття рішень в компанії, які переваги та проблеми пов'язані з використанням таких систем, а також як вибрати та впровадити аналітичну систему в практичну діяльність бізнесу. Метою статті є також зробити свій внесок у розвиток та популяризацію використання аналітичних систем у сфері бізнесу.

Об'єктом дослідження э розробка аналітичної системи для впливу на процес прийняття рішень в бізнесі.

Предметом дослідження є аналітичні системи.

Аналіз попередніх досліджень показав, що використання аналітичних систем в бізнесі може мати значний вплив на процес прийняття рішень. Наприклад, за дослідженнями McKinsey, компанії, які активно використовують аналітичні системи, мають в 2,6 рази більшу вірогідність досягнути високих показників фінансової ефективності, ніж ті, що не використовують такі системи. Дослідники також відзначають, що аналітичні системи можуть допомогти бізнесу збільшити ефективність процесів, знизити витрати і покращити якість продуктів та послуг. Крім того, вони можуть допомогти виявити нові можливості для зростання та розширення бізнесу, зокрема шляхом аналізу ринку та відстеження поведінки споживачів. Однак, дослідження також показали, що успіх використання аналітичних систем залежить від багатьох факторів, включаючи якість даних, адекватність моделей, які

використовуються для аналізу даних, та належну інтеграцію систем в бізнес-процеси. Також важливо, щоб співробітники компанії були готові до використання аналітичних систем та мали необхідні знання та навички для їх використання.

Виклад основного матеріалу. Впровадження аналітичних систем в бізнесі значно змінило процес прийняття рішень. Раніше рішення приймалися на основі інтуїції, досвіду та зібраних даних. Завдяки аналітичним системам, бізнес може опиратися на більш об'єктивні дані та аналітику, що дозволяє приймати рішення на основі фактів, а не припущень. В сучасних умовах аналітичну систему можна представити таким чином (рис. 1):

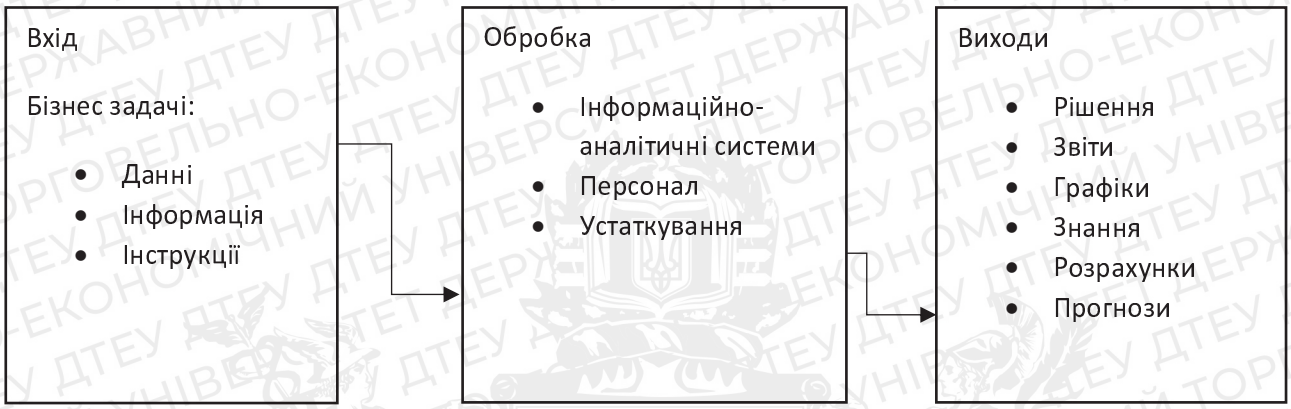


Рис.1. Аналітична система

Процес управління в аналітичних системах можна поділити на три основні етапи: вхідні дані, обробка і аналіз даних, і вихідні дані. Кожен з цих етапів має свої особливості:

- Вхідні дані. На цьому етапі збираються та введені дані, які використовуються в аналітичній системі. Ці дані можуть бути зібрані з різних джерел, таких як бази даних, веб-сайти, соціальні мережі, сенсори тощо. Для забезпечення якості та достовірності даних, можуть використовуватися різноманітні методи валідації та очистки даних.
- Обробка і аналіз даних. Після отримання інформації проводиться обробка та аналіз вхідних даних. Для цього використовуються різні методи та техніки, такі як статистичний аналіз, машинне навчання, нейронні мережі тощо. Основною метою цього етапу є виявлення залежностей та патернів в даних, що може допомогти в розумінні тенденцій та прогнозуванні майбутніх подій.
- Вихідні дані. Коли данні отримані і оброблені виконується візуалізація та передача отриманих результатів користувачам. Для цього можуть використовуватися різні методи та інструменти, такі як дашборди, звіти, графіки тощо. Користувачі можуть використовувати ці дані для прийняття рішень або для подальшого аналізу.

Після того, як дані були оброблені і проаналізовані, результати можуть бути відображені у вигляді звітів, дашбордів або інших візуальних інтерфейсів. Це дозволяє користувачам легко зрозуміти результати і прийняти правильні рішення. Управління зазвичай здійснюється через інтерфейс користувача, який дозволяє налаштувати параметри аналізу та моніторингу [1]. Це може включати в себе налаштування прав доступу для різних користувачів, налаштування різних видів звітів та дашбордів, а також налаштування різних показників та метрик для аналізу.

Розвиток аналітичних систем дозволяє компаніям збільшувати швидкість та точність процесу прийняття рішень. Замість інтуїтивного підходу, керівництво компанії отримує об'єктивні дані, на основі яких можна зробити правильний висновок. Однак, важливо не забувати, що вони не є універсальним рішенням на всі випадки, тому досвід та інтуїція керівництва також залишаються важливими факторами в процесі прийняття рішень.

В бізнес плануванні системи для аналізу даних допомагають як для крупних компаній так і для середніх або малих. Для крупних компаній використовуються складні аналітичні системи, які дозволяють обробляти великі обсяги даних та робити прогнози щодо подальшого розвитку бізнесу. Один з прикладів такої системи що використовуються у крупних компаній – SAP BusinessObjects, яка надає інструменти для збору та аналізу даних з різних джерел, зокрема з баз даних, електронної пошти, соціальних мереж тощо. Вона дозволяє створювати звіти та графіки, які відображають стан бізнесу та його поточні та прогнозовані результати (рис. 2).

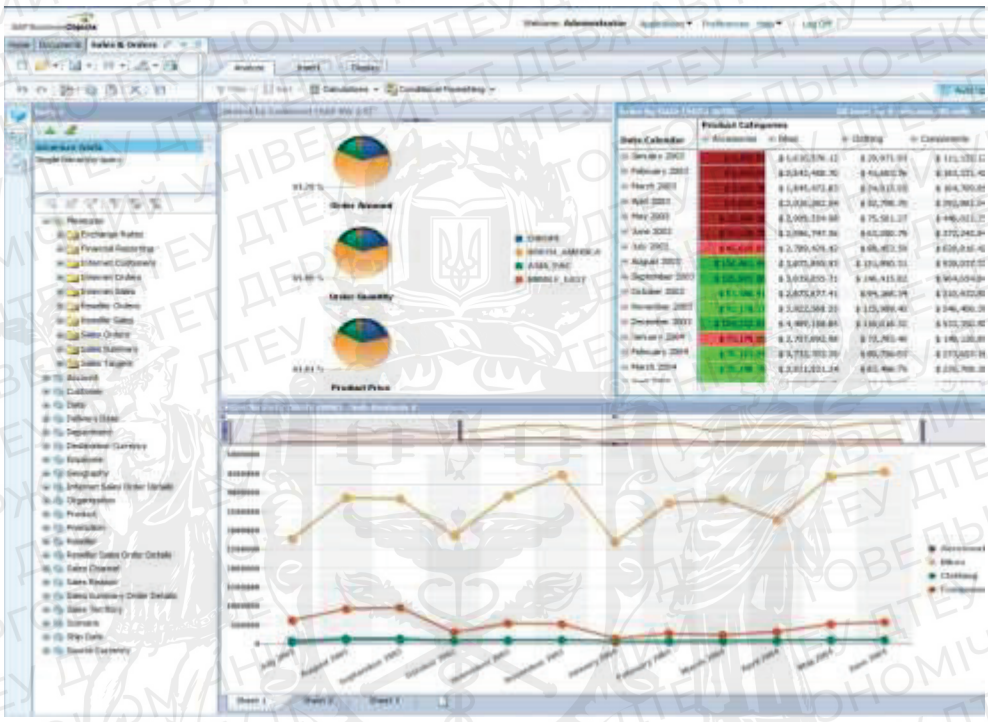


Рис. 2. Sap BusinessObjects інтерфейс програми з вхідними даними, графіками, та діаграмами після обробки даних.

SAP BusinessObjects є однією з найбільш популярних аналітичних систем у бізнесі. Вона надає користувачам широкі можливості для збору, аналізу та візуалізації даних[2]. SAP BusinessObjects використовується в багатьох крупних компаніях, таких як Coca-Cola, Nestle та Procter & Gamble.

У компанії Coca-Cola SAP BusinessObjects використовується для підтримки процесу прийняття рішень та для виконання аналітики даних. Завдяки SAP BusinessObjects аналітики компанії можуть швидко та ефективно аналізувати великі обсяги даних і знаходити тенденції та взаємозв'язки між ними. Компанія також використовує SAP BusinessObjects для підтримки внутрішнього звітності та для автоматизації процесів збору та аналізу даних. У Nestle SAP BusinessObjects використовується для підтримки процесу планування ресурсів підприємства (ERP). Система допомагає спростити та автоматизувати процеси збору та аналізу даних, що дозволяє компанії зосередитися на стратегічних питаннях та підвищенні ефективності бізнесу. SAP BusinessObjects також допомагає Nestle виявляти проблемні зони у процесах виробництва та управління запасами, що дозволяє компанії швидко реагувати на проблеми та покращувати ефективність. У Procter & Gamble SAP BusinessObjects використовується для підтримки процесу прийняття рішень та для виконання аналізу даних. Система дозволяє компанії ефективно збирати та аналізувати дані з різних джерел, що допомагає у прийнятті рішень на основі фактичних даних.

Крім того, SAP BusinessObjects може бути використана для розробки та виконання різних звітів та аналітичних досліджень, таких як аналіз фінансових показників, відстеження витрат на проектах та моніторинг виконання бізнес-планів. Завдяки вбудованій системі

Business Intelligence (BI) можливість візуалізації даних у вигляді графіків, діаграм та інших візуальних засобів, що полегшує сприйняття та аналіз отриманих даних. Система може інтегруватися з різноманітними джерелами даних, такими як бази даних, Excel-файли та інші програмні продукти, що дозволяє отримувати доступ до необхідних даних та інформації безпосередньо з одного місця.

Важливою функцією SAP BusinessObjects є можливість створення панелей керування (dashboards), які дають змогу отримати швидкий огляд найважливіших показників та метрик, що дозволяє швидко реагувати на зміни та приймати вчасні рішення. Також слід зазначити, що SAP BusinessObjects може бути налаштована для різних відділів та функціональних областей, що дозволяє компаніям використовувати систему для вирішення різноманітних завдань та задач. Наприклад, система може бути використана для моніторингу продажів, відстеження витрат на виробництві, аналізу даних про клієнтів та багато іншого.

Однією з кращих програмних забезпечень слід зазначити про Oracle Business Intelligence (рис.3).

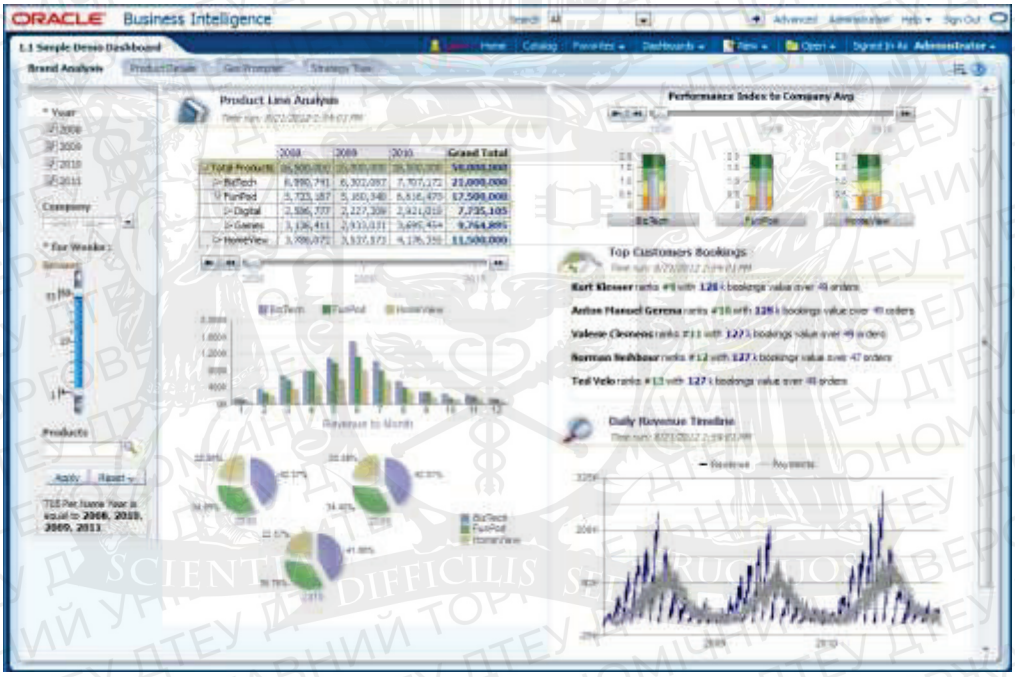


Рис. 3. Інтерфейс звітів Oracle Business Intelligence

Oracle Business Intelligence (OBI) – це повний комплекс рішень для аналітики даних та бізнес-інтелекту, який розробляється компанією Oracle. Ця система надає користувачам різноманітні можливості для створення звітів, аналізу даних та взаємодії з ними в режимі реального часу. Программа складається з таких компонентів, як Oracle BI Server, Oracle BI Answers, Oracle BI Publisher та Oracle BI Interactive Dashboards. Всі ці компоненти взаємодіють між собою, забезпечуючи зручний та ефективний інтерфейс для користувачів.

Один з головних компонентів це Oracle BI Server, який надає доступ до даних з різних джерел, таких як бази даних, файли, веб-сервіси тощо. Сервер забезпечує зручний та швидкий доступ до даних незалежно від їх формату та розміру. Крім того, BI Server надає можливості для створення зв'язків між різними джерелами даних, що дозволяє користувачам аналізувати дані з різних джерел в єдиному інтерфейсі.

Oracle BI Answers представляє собою інтерактивну систему аналізу даних, яка дозволяє користувачам створювати запити до даних, використовуючи візуальний інтерфейс та шаблони запитів. Запити можуть бути збережені та використовуватись для подальшого аналізу даних.

Oracle BI Publisher – це інструмент для створення та розповсюдження звітів. Він дозволяє користувачам створювати звіти в різних форматах, таких як PDF, Excel та HTML, та розповсюджувати їх з максимальною ефективністю.

Oracle BI Interactive Dashboards є однією з ключових компонентів Oracle Business Intelligence. Це інтерактивне веб-додаток, який дозволяє користувачам здійснювати аналіз даних в режимі реального часу та створювати інформаційні панелі з необхідною для них інформацією. Він дозволяє використовувати графіки, таблиці, діаграми та інші візуалізації для представлення даних. Користувачі можуть легко переглядати та порівнювати дані, а також здійснювати фільтрацію та пошук інформації за допомогою вбудованих функцій. Oracle BI Interactive Dashboards також дозволяє використовувати інтерактивні заходи для взаємодії з даними, наприклад, можна здійснювати вибір певних елементів на діаграмі для фільтрації даних в інших частинах інформаційної панелі. Крім того, користувачі можуть експортувати дані з Oracle BI Interactive Dashboards у формати Excel або PDF, що дозволяє зберігати та обмінюватися даними з колегами. Программа також має вбудований функціонал для роботи з безпекою та доступом до даних. Адміністратори можуть налаштовувати рівні доступу до інформації для різних користувачів, груп та ролей. Це дозволяє забезпечити безпеку даних та контролювати доступ до конфіденційної інформації.

Щодо малих та середніх підприємств, часто використовуються простіші аналітичні системи, які дозволяють вести облік продажів, складу та виробництва, а також аналізувати фінансову діяльність. Один з прикладів – QuickBooks (рис. 4), який дозволяє вести бухгалтерський облік, створювати звіти та аналізувати фінансові показники бізнесу[3].

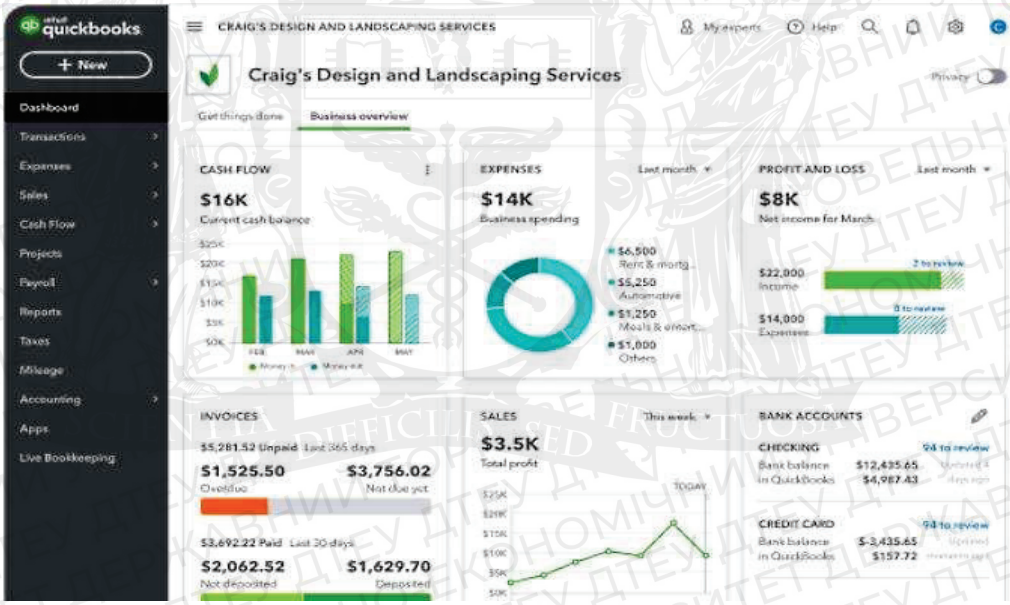


Рис. 4. QuickBooks інтерфейс програми, графіки та звіти.

Основні можливості QuickBooks включають:

- Облік рахунків і платежів: в програмі можна створювати та зберігати інформацію про рахунки клієнтів, постачальників та платежі за них. Можна також додавати оплати та надходження коштів, що спрощує процес взаємодії з контрагентами.
- Операції з банківськими рахунками: програма дозволяє створювати рахунки та відслідковувати операції з банківськими рахунками, включаючи поповнення та виведення коштів.
- Створення звітів: QuickBooks має вбудовані засоби для створення звітів про фінансову діяльність компанії, таких як баланс, звіт про прибутки та збитки, звіт про заборгованості тощо. Звіти можна створювати як за певний період часу, так і за конкретний проект або контрагента.
- Інтеграція з іншими програмними засобами: QuickBooks може інтегруватись з іншими програмними засобами, такими як PayPal, Shopify, Amazon тощо, що дозволяє автоматизувати процеси продажу та звітності.

У загальному, QuickBooks допомагає компаніям ефективно керувати фінансовою діяльністю, складом, проектами та клієнтами, що є особливо важливим для малих та середніх підприємств, які не можуть дозволити собі велику бухгалтерську та фінансову команду.

Крім того, існують спеціалізовані аналітичні системи для різних галузей, наприклад, для логістики, маркетингу, ресторанного бізнесу тощо. Наприклад, у ресторанному бізнесі може використовуватися Toast, який дозволяє вести облік продажів, керувати запасами та персоналом, а також аналізувати відвідуваність та задоволеність клієнтів[4]. Варто відзначити, що у бізнесі можуть використовуватися не тільки готові аналітичні системи, але й спеціально розроблені інструменти, які відповідають потребам конкретної компанії та її галузі.

Висновки. Аналітичні системи є незамінним інструментом для прийняття рішень в бізнесі. Проте, як і будь-який інструмент, вони мають свої переваги та недоліки.

Переваги таких систем включають:

- Підвищення ефективності та продуктивності: аналітичні системи дозволяють бізнес-лідерам отримати доступ до точних даних та статистичної інформації, що забезпечує зростання ефективності та продуктивності в діяльності компанії.
- Збільшення точності прийнятих рішень: аналітичні системи допомагають компаніям приймати рішення на основі даних, що забезпечує більш точне та обґрунтоване прийняття рішень.
- Покращення стратегічного планування: аналітичні системи дозволяють компаніям отримувати значну кількість даних, які можна використовувати для планування та розробки стратегій.
- Отримання конкурентної переваги: за допомогою аналітичних систем компанії можуть аналізувати діяльність своїх конкурентів та знаходити нові можливості для покращення власної продуктивності.

До негативних аспектів відносяться такі пункти:

- Висока вартість: впровадження та підтримка аналітичних систем можуть бути витратними для компаній.
- Складність впровадження: впровадження аналітичних систем може бути складним та вимагати значних зусиль з боку IT-команди.
- Недостатність якісних даних: якість даних може впливати на якість прийнятих рішень. Якщо дані не є достатньо точними, то результати аналітичних систем можуть бути неправильними.

Отже, прийняття рішень на основі аналітичних систем має свої переваги та недоліки. Щоб максимально використовувати переваги аналітики та зменшувати ризики недоліків, важливо ретельно планувати та розробляти відповідну стратегію, залучати експертів та забезпечувати необхідну підготовку персоналу.

Список використаних джерел

1. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, 36(4), 1165-1188.
2. Srivastava, D., & Saxena, S. (2018). Business Intelligence: Concepts, Methodologies, Tools, and Applications. IGI Global.
3. Turban, E., Sharda, R., & Delen, D. (2019). Decision Support and Business Intelligence Systems. Pearson.
4. Kimball, R., Ross, M., Thornthwaite, W., Mundy, J., Becker, B., & Thornthwaite III, W. (2013). The Kimball Group Reader: Relentlessly Practical Tools for Data Warehousing and Business Intelligence. Wiley.

Робота виконана під науковим керівництвом к.т.н., доцента
ХАРЧЕНКА О.А.

МЕНЕДЖЕР ПАРОЛІВ ТА ЙОГО РІЗНОВИДИ

МИРОВЕЦЬ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Менеджери паролів – це інструменти, які допомагають користувачам створювати, зберігати та керувати складними та унікальними паролями для їхніх різноманітних облікових записів в Інтернеті. Таким чином, вони відіграють вирішальну роль у підвищенні онлайн-безпеки та запобіганні кібератакам. Одним з важливих аспектів менеджерів паролів є механізм обміну даними, який дозволяє їм обмінюватися даними користувача між пристроями та програмами.

Password managers are tools that help users generate, store, and manage complex and unique passwords for their various online accounts. As such, they play a critical role in enhancing online security and preventing cyberattacks. One essential aspect of password managers is the data exchange mechanism that allows them to share user data between devices and applications.

Актуальність. Більшість людей ненавидять реєструвати облікові записи, а тим більше створювати паролі. Це може бути причиною, чому вони повторно використовують їх кілька разів під час створення облікових записів.

Однак зараз 2023 рік, і рішення є. Одним із них можуть бути менеджери паролів. З ними ви можете створювати складні паролі та зберігати їх.

Менеджер паролів — це програма, яка дозволяє створювати та зберігати всі ваші паролі в безпечному місці. Більшість із них дозволяють також зберігати дані кредитної картки, а також безпечні нотатки. Для ще більшої безпеки та зручності менеджери паролів також підтримують використання біометричних даних (відбитків пальців або обличчя) замість головного пароля для ще більшої безпеки та зручності.

Паролі необхідні для захисту ваших облікових записів, але вони також можуть дратувати. Автономний менеджер паролів може зробити це безпечнішим і менш виснажливим.

Для більшості інструментів керування паролями користувачу потрібно лише ввести головний пароль, щоб розшифрувати секретні сховища. Це, звичайно, краще, ніж мати справу з десятками і десятками паролів.

Коли ви створюєте новий елемент у менеджері паролів, ви можете створити випадковий пароль. Ці машинно створені рядки складні та довгі з різними типами символів, тому їх практично неможливо вгадати.

Синхронізація є стандартною частиною менеджерів паролів . Ви можете працювати на робочому столі Windows і використовувати телефони iPhone і Android – це не має значення. Усі ваші паролі можуть бути синхронізовані та ідентичні незалежно від того, який пристрій ви використовуєте.

Метою статті є дослідження та класифікація менеджерів паролів, а також їх типи.

Об'єктом дослідження є розробка програмного забезпечення обміну даними між менеджерами паролів.

Предмет дослідження – менеджери паролів.

Аналіз попередніх досліджень. Дослідженню менеджерів паролів присвячені праці наступних науковців: Karen Scarfone(Карен Скарфон), Murugiah Souppaya(Муругія Суппая), Shirley Gaw(), Edward W. Felten(Едвард В. Фелтен), Sruthi Anand(Шруті Ананда), Dr.N.Susila1(доктор Н.Сусіла), Dr.S.Balakrishnan(доктор С.Балакрішнан) та інші.

Виклад основного матеріалу. На перший погляд здається, що користуватися таким менеджером просто, але все одно треба розуміти принцип його роботи. На рис. 1 показано принцип роботи такого менеджеру.

Рис. 1. Принцип роботи менеджера паролів

Менеджер паролів — це невелике сховище (зазвичай база даних), яке зберігає всі ваші облікові дані та паролі (зашифровані) і зазвичай захищене головним паролем або біометричними даними, іноді з додатковим захистом автентифікації, наприклад двоетапною або багатофакторною автентифікацією (MFA). . У більшості конфігурацій, на жаль, додатковий захист автентифікації вимкнено за замовчуванням і має бути увімкнений користувачем.

Зазвичай можна створити кілька сховищ, кожне з яких захищено головним паролем. Найпоширенішим способом створення нових записів у сховищі є розширення браузера. Потім, коли ви вводите інформацію в поле імені користувача та пароля у веб-формі, розширення запропонує зберегти ці облікові дані в сховищі. Після цього поля можуть автоматично заповнюватися під час наступного переходу на той самий веб-сайт.

Сховище можна синхронізувати між кількома пристроями, забезпечуючи вам легкий спосіб заповнити ім'я користувача та пароль у веб-формах без необхідності запам'ятовувати пароль або вводити його безпосередньо. Менеджер паролів допомагає створювати надійні паролі для кожного облікового запису та перевіряти надійність ваших унікальних паролів.

Деякі версії менеджерів паролів дозволяють ділитися обліковими даними з членами родини.

Що робить особисті менеджери паролів привабливими для споживачів, так це те, що багато базових програм менеджерів паролів пропонують безкоштовні версії, хоча й з обмеженими можливостями. Коли ви досягаєте ліміту пароля або вам потрібні додаткові функції, як-от можливість синхронізації між кількома пристроями, потрібно платити, і що більше функцій вам потрібно, то вища ціна.

У менеджерів паролів є свої сильні сторони. За допомогою менеджерів паролів паролі шифруються, і їх можна розшифрувати, лише якщо отримати доступ до них із створеним

користувачем головним паролем. Більшість менеджерів паролів зберігають облікові дані, які використовуються для доступу до кількох облікових записів і програм: ім'я користувача, пароль, назву програми, URL-адресу веб-сайту або IP-адресу системи. Їх можна встановити локально, отримати доступ у хмарі або через мобільні програми. І вони створені для створення довгих складних паролів і автоматичного заповнення пароля в правильному полі, тому людям не потрібно вручну вводити його або вирізати та вставляти[1].

Але давайте задамося питанням, чи є менеджери паролів кращими, ніж створення власних паролів і їх запис?

Для особи, яка хоче захистити особисті паролі, використання менеджера паролів може бути прийнятним. Це, безперечно, краще, ніж паролі, написані на листочках, приклеєних до монітора чи під клавіатурою, збережених у електронних таблицях Excel чи Google-документах або збережених у вигляді звичайного тексту за допомогою плагіна браузера.

Але чи є сенс використовувати один із цих персональних менеджерів паролів для захисту корпоративних паролів?

Якщо ваші цілі — безпека та ефективність підприємства, менеджерів паролів недостатньо. Для компаній перевагу надається рішенням керування привілейованим доступом (Privileged Access Management, або PAM) з причин, які виходять далеко за межі безпеки.

Керування привілейованим доступом — це категорія кібербезпеки, яка стосується того, хто може отримати доступ до привілейованого облікового запису та що вони можуть робити після входу в мережу вашої організації за допомогою цього привілейованого облікового запису. За даними Gartner Research, це один із головних пріоритетів безпеки для зменшення ризику кібератак.

Уніфікований підхід до корпоративного керування паролями за допомогою PAM корпоративного рівня безпечніший і ефективніший, ніж тисячі відключених персональних менеджерів паролів.

Керування привілейованим доступом є більш надійним рішенням безпеки, ніж менеджери паролів. Шукайте рішення PAM, яке пропонує такі функції:

- Висока доступність
- Контроль відповідності та нормативної безпеки
- Автоматичне виявлення привілейованого облікового запису
- Можливість налаштування робочих процесів підтвердження доступу
- Інтеграція з такими корпоративними рішеннями, як ITSM, IGA (керування ідентифікацією та адміністрування) і SIEM (інформація про безпеку та керування подіями)
- Можливість масштабувати бізнес
- Автоматична ротація паролів
- Аудит і звітність щодо використання пароля та безпеки
- Послідовний контроль безпеки

Організації використовують програмне забезпечення PAM, щоб контролювати, хто може використовувати привілейований обліковий запис або отримувати доступ до конфіденційної інформації з можливістю коригувати дозволи та змінювати або видаляти важливі дані. Вони розглядають привілейований обліковий запис як об'єкт, який захищається, обмежуючи розголошення пароля та спільний доступ, надаючи при цьому обмежений за часом доступ до критичних систем. Коли пароль більше не потрібен, він змінюється або термін дії закінчується, тому співробітники та треті сторони не можуть продовжувати отримувати доступ до конфіденційної інформації зі старим паролем.

Менеджери паролів вимагають, щоб окремі користувачі налаштували, підтримували та завжди використовували додаток. Користувач бере на себе всю відповідальність за підтримку технології в актуальному стані та її належне функціонування.

За допомогою LastPass, KeePass, Dashlane та інших персональних менеджерів паролів користувач несе відповідальність за безпеку паролів. Вони повинні виконати важку роботу з

налаштування, ротації паролів і, що найважливіше, переконатися, що сховище паролів використовується постійно.

Завдяки корпоративному PAM-рішенню IT-команда бере на себе відповідальність за технологію захисту корпоративних паролів. Вони роблять роботу, щоб розпочати й підтримувати її.

Менеджери паролів – це охоронці вашого онлайн-світу. Вони захищають ваші облікові записи від зловмисників, генеруючи та запам'ятовуючи надійні унікальні паролі для ваших облікових записів. У той час як деякі зосереджені лише на захисті ваших паролів, деякі виходять за межі, щоб надати вам додаткову гнучкість.

Про деякі з різних типів ми зараз поговоримо:

1. Хмарні менеджери паролів.

Це один із найпопулярніших варіантів для приватних осіб і компаній. Хмарні менеджери паролів шифрують ваші паролі та інші конфіденційні дані та зберігають їх на власних серверах. Основною перевагою хмарного менеджера паролів є легкість доступу з будь-якої точки світу за допомогою будь-якого комп'ютерного пристрою. Основі можливості хмарного менеджера паролів:

- служба централізовано розміщена та підтримується постачальником послуг, тому їх можна розгорнути та отримати доступ до них миттєво;
- модель на основі передплати потребує менших початкових витрат;
- можна збільшити або зменшити відповідно до зростання команди;
- Безпека даних користувача безпосередньо залежить від вибору постачальника послуг.

2. Локальні менеджери паролів.

Локальні менеджери паролів зазвичай віддають перевагу окремим особам і компаніям, які бажають розмістити та керувати менеджером паролів у власному закритому середовищі. Зазвичай вони пропонують функції керування паролями, подібні до хмарного менеджера паролів, але вони дорожчі й зазвичай використовуються підприємствами, які мають доступ до ресурсів і фінансів для підтримки власної інфраструктури. Можливості локальних менеджерів паролів:

- розміщується та обслуговується приватно, щоб уникнути зовнішніх загроз;
- корисно для команд, яким потрібен доступ до паролів навіть за відсутності стабільного підключення до Інтернету;
- вищі початкові витрати;
- додаткові накладні витрати, пов'язані з обслуговуванням, розгортанням і оновленням інфраструктури;
- довший час впровадження, оскільки рішення потрібно розгортати вручну.

3. Мобільні менеджери паролів.

Хоча для мобільних пристроїв доступно багато хмарних програм для керування паролями, iOS і Android пропонують власні менеджери паролів, такі як Apple Keychain і Google Password Manager, що дозволяє користувачам безпечно зберігати паролі на своїх мобільних пристроях. Вони також допомагають, автоматично заповнюючи паролі на веб-сайтах і в мобільних додатках. Можливості мобільних менеджерів паролів:

- легко почати;
- миттєвий доступ до паролів з будь-якої точки світу;
- безкоштовно (входить у вартість мобільного пристрою);
- обмежено для особистого використання через відсутність широких функцій;
- Паролі не можна синхронізувати між пристроями, що працюють на різних платформах.

4. Браузерні менеджери паролів.

Такі популярні браузери, як Chrome, Safari, Firefox і Edge, пропонують вбудовані менеджери паролів, які допомагають користувачам зберігати та керувати своїми паролями.

Паролі, збережені в цих менеджерах паролів, можна синхронізувати між пристроями, які підтримують ці браузери.

- Легко розпочати та керувати;
- Підтримує автоматичне заповнення пароля та автоматично зберігає нові облікові дані облікового запису;
- Безкоштовно;
- Обмежено для особистого використання через відсутність широких функцій;
- Паролі не можна синхронізувати в різних браузерах;
- Небезпечно на спільних пристроях, на яких кілька користувачів мають доступ до браузерів.

Тепер постає питання, який тип менеджера паролів вибрати?

Пристойний менеджер паролів повинен перш за все мати необмежену пам'ять для облікових даних і бути доступним принаймні для основних платформ Windows, macOS, Android та iOS. А оскільки дані передаватимуться між пристроями, вибраний менеджер паролів має переважно шифрувати дані на локальному рівні, оскільки це гарантує, що ваші дані стануть незрозумілими для потенційних хакерів до того, як вони потраплять у хмару або щоразу, коли вони будуть викликані як частина надбудови браузера.

Вибір найкращого менеджера паролів для ваших потреб залежить від кількох факторів. Наприклад, краще використовувати вбудований у пристрій або браузер менеджер паролів, а не використовувати жодного. Однак ви повинні пам'ятати, що вони обмежені та пропонують значно меншу цінність порівняно з безкоштовним хмарним менеджером паролів.

Через постійно зростаючу кількість спроб злому та постійні витоки даних за участю таких великих компаній, як Google, користувачі Інтернету приділяють усе більше уваги збереженню облікових даних облікового запису якомога безпечнішими, використовуючи надійні паролі. Однак запам'ятати десятки, якщо не сотні різних логінів для кожного облікового запису неможливо з людської точки зору, особливо якщо вони настільки складні, як це необхідно для належної безпеки. Менеджери паролів допомагають згадати будь-які дані для входу , серед іншого, але оскільки їхні найважливіші функції в основному однакові, вибрати правильне програмне забезпечення може бути важко навіть для найбільш поінформованих користувачів.

Однак завдяки паралельним порівнянням прийняти таке рішення буде так само легко, як і використовувати саме вибране програмне забезпечення. У таблиці 1 продемонстровані найвідоміші менеджери паролів та їх переваги один над одним.

Таблиця 1

Порівняльна характеристика менеджерів паролів

Основні риси	Lastpass	Dashlane	1Password
Спеціальні поля	НІ	НІ	ТАК
Користувацькі шаблони	ТАК	НІ	НІ
Безкоштовні запрошення клієнтів	НІ	НІ	НІ
Розширення для браузера	ТАК	ТАК	ТАК
Генератор паролів	ТАК	ТАК	ТАК
Сховище	НІ	1ГБ	1ГБ/на користувача
Імпорт даних	ТАК	ТАК	ТАК

Пропоную також поговорити про ризики використання менеджера паролів.

Немає способу залишатися в безпеці на 100% в Інтернеті . Навіть якщо ви використовуєте надійний менеджер паролів, вам слід знати про певні ризики:

1. Усі конфіденційні дані в одному місці .

Ви, мабуть, чули, що більшість людей робить так само. Це саме те, що ви будете робити з менеджером паролів. Ця інформація, ймовірно, також включатиме дані кредитної картки та безпечні нотатки. У разі зламу блокування всіх варіантів оплати та зміна паролів для всіх облікових записів може зайняти достатньо часу, щоб зловмисник завдав шкоди.

2. Резервне копіювання не завжди можливо .

Якщо сервер виходить з ладу, ваша єдина надія – це те, що ваш провайдер зробив резервну копію. Цей ризик зростає в рази, якщо ви вирішите залишити своє сховище в автономному режимі на одному зі своїх пристроїв. Природно, збереження власної резервної копії на незахищеному диску або погано захищеному хмарному сервісі також не допоможе.

3. Не всі пристрої достатньо безпечні.

Хакери використовують ту саму вразливість, щоб отримати всі ваші логіни за одну атаку. Менеджери паролів можуть бути зламані, якщо ваш пристрій інфікований шкідливим програмним забезпеченням . У цьому випадку, якщо ввести головний пароль, він буде записаний, і кіберзлочинці отримають повний доступ до збережених даних. Ось чому користувачам менеджера паролів слід інвестувати в надійний антивірус , який спочатку захистить усі їхні пристрої та зменшить ризики.

4. Не використовує біометричну автентифікацію .

Біометрична автентифікація — це чудовий спосіб підвищити рівень безпеки. Якщо ви налаштуєте свій менеджер паролів на запит відбитків пальців або сканування обличчя, шанси на те, що хтось уразить ваше сховище, стануть незначними.

5. Поганий менеджер паролів .

Якщо він має слабше шифрування, пропонує мало функцій і має погані відгуки, вам не слід його використовувати. Коли мова заходить про безпеку вашого сховища, економія кількох доларів на місяць не повинна бути вашим головним пріоритетом. Це особливо вірно для безкоштовних менеджерів паролів, які часто не мають необхідних функцій безпеки для ефективного захисту ваших облікових даних у будь-який час.

6. Забули головний пароль .

Ви єдина людина, яка це знала, і ваш менеджер паролів не має функції скидання? У цьому випадку ви вже можете розпочати відновлення кожного входу один за одним. Крім того, ви можете зберегти свій головний пароль (або підказку) у фізично безпечному місці[3].

Висновки. Порівняно з альтернативою, яка передбачає запам'ятовування всього або записування облікових даних на наліпках, менеджери паролів є кращим вибором.

Це простий спосіб захистити ваші облікові записи від поширених онлайн-загроз. Усиновлення спочатку може бути дивним і громіздким. Але в цілому менеджер паролів може покращити вашу цифрову безпеку в усіх аспектах.

Список використаних джерел

1. Usability, security and trust in password managers: A quest for user-centric properties and features \\ Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1574013718302533 (останнє звернення 17.03.2023р.)
2. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers \\ Режим доступу: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-li-zhiwei.pdf (останнє звернення 23.03.2023р.)
3. Why people (don't) use password managers effectively \\ Режим доступу: https://www.usenix.org/system/files/soups2019-pearman.pdf (останнє звернення 27.03.2023р.)

Робота виконана під науковим керівництвом ст. викладач,
ШЕСТАКА Я.І.

ПІДХОДИ ДО ПРОЕКТУВАННЯ ТА РОЗРОБКИ ПРОГРАМНИХ ПЛАТФОРМ ЕЛЕКТРОННИХ РИНКІВ

МІРКО І., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади щодо проектування та розробки платформ е-торгівлі як програмного продукту. Розглянуто як зразок архітектуру програмної компоненти e-Market places.

The article discusses the basic principles of designing and developing software platforms of electronic markets. The architecture of the software component is considered as an example e-Market places.

Актуальність. Із зростанням кількості електронних торгових майданчиків зростає потреба в ефективному проєктуванні та розробці програмної платформи, яка може забезпечити безперебійну, надійну та захищену роботу тандему система-користувач, а також відповідати вимогам різних бізнес-моделей.

Розробка платформ електронного ринку є складним процесом, який включає різні проблеми, такі як масштабованість, безпека та зручність використання [2; 3]. Крім того, платформи електронного ринку повинні бути розроблені для підтримки різних бізнес-моделей, таких як B2B, B2C і C2C, що може ще більше ускладнити процес розробки.

В останні роки зростає цікавість до дизайну та розробки платформ електронного ринку. В IT-сегменті було запропоновано численні підходи для вирішення різноманітних викликів, проте все ще бракує комплексних та систематизованих досліджень, які б порівнювали різні підходи проєктування, дизайну, розробки та оцінювали їх ефективність [1; 2; 3].

Метою статті є аналіз та порівняння різних підходів до проєктування та розробки платформи електронного ринку та надання оптимальних висновкіт та практичних рекомендацій для створення ефективної платформи електронного ринку.

Об'єктом дослідження є процес побудова архітектури та проєктування програмних додатків платформ електронних ринків..

Предмет дослідження – платформа е-торгівлі як програмний продукт.

Аналіз попередніх досліджень. Дослідженню архітектури ПЗ, дизайну та проєктуванню додатків, визначенню структури, основних характерних рис платформ електронного ринку присвячені праці вітчизняних та закордонних науковців: В.В. Соколова, Дж. Мартін, Н.М. Тюріна, та ін.

Виклад основного матеріалу.

Платформи електронних ринків стали популярним каналом для компаній, щоб охопити нових клієнтів і розширити свої ринки збуту [4]. Ці платформи є онлайн-платформами, які оптимізують транзакції між покупцями та продавцями та можуть бути класифіковані на різні типи залежно від цільових користувачів, наприклад бізнес-бізнес (B2B), бізнес-споживач (B2C) і споживач-споживач (C2C) [5]. Платформи електронного ринку також можна класифікувати залежно від їхнього масштабу, наприклад, глобальні, регіональні чи локальні [6].

В останні роки відбулося значне збільшення кількості доступних платформ електронного ринку, таких як Amazon, Alibaba та eBay [7]. Платформи електронного ринку забезпечують переваги як для покупців, так і для продавців, такі як розширення доступу до продуктів і послуг, зниження трансакційних витрат і підвищення ефективності ринку [8].

Однак проєктування та розробка платформ електронного ринку може бути складним через такі фактори, як масштабованість, безпека та зручність використання. Вирішення цих

проблем вимагає ретельного планування та врахування різних факторів, таких як вибір архітектури програмного забезпечення, методології розробки та стеку технологій [9].

Загальні проблеми при проєктуванні та розвитку електронних ринків сформувались як у практиків, так і у науковців.

Зорема, науковці визначили різні проблеми при проєктуванні та розвитку електронних ринків, які необхідно вирішити, щоб забезпечити успіх платформи. Деякі з типових проблем, з якими стикаються розробники електронного ринку, включають:

- Масштабованість: електронні ринки повинні мати можливість обробляти велику кількість користувачів і транзакцій, не відчуваючи проблем із продуктивністю [10; 12; 14].
- Безпека: електронні ринки повинні забезпечувати безпеку даних користувачів і транзакцій, щоб створити довіру та запобігти шахрайству [11; 13].
- Зручність використання: електронні ринки повинні бути розроблені з урахуванням досвіду користувачів, щоб полегшити користувачам навігацію та використання платформи [15].
- Інтероперабельність: електронні ринки повинні мати можливість інтегруватися з іншими системами та платформами для полегшення обміну даними та взаємодії [16].
- Адаптивність: електронні ринки повинні мати можливість адаптуватися до мінливих ринкових умов і мінливих потреб бізнесу [10; 11;15].

Проаналізувавши праці вчених та практиків, агрегуємо підходи до проєктування, моделювання та розробки ПЗ:

1. Монолітна архітектура: у цьому підході весь електронний ринок розробляється як єдине інтегроване ціле. Цей підхід є простим і легким у розробці, але він не може бути масштабованим або адаптованим до мінливих потреб бізнесу [1; 2; 5].
2. Архітектура мікросервісів: цей підхід передбачає поділ електронного ринку на менші незалежні сервіси, які можна розробляти та розгортати окремо. Цей підхід пропонує більшу масштабованість, адаптивність і відмовостійкість, але може потребувати більше зусиль у розробці [3; 4; 6].
3. Спеціальне програмне забезпечення: цей підхід передбачає розробку електронного ринку з нуля за допомогою спеціального коду. Цей підхід забезпечує більшу гнучкість і контроль над функціями платформи, але може потребувати більше часу та зусиль для розробки та підтримки [7].
4. Платформа як послуга (PaaS): цей підхід передбачає використання попередньо створеної платформи для розробки електронного ринку. Цей підхід пропонує більшу швидкість і легкість розробки, але він може бути менш гнучким або настроюваним [8; 9].
5. Програмне забезпечення з відкритим кодом: цей підхід передбачає використання програмного забезпечення з відкритим кодом для розробки електронного ринку. Такий підхід забезпечує більшу гнучкість і контроль над функціями платформи, але може потребувати більше зусиль у розробці [10; 11].
6. Власне програмне забезпечення: цей підхід передбачає використання власного програмного забезпечення для розробки електронного ринку. Цей підхід пропонує більшу легкість розробки та підтримки, але він може бути менш гнучким або настроюваним [12; 13].
7. Гнучка розробка програмного забезпечення: цей підхід передбачає ітераційну та поступову розробку, зосереджену на відгуках користувачів і швидкому створенні прототипів. Такий підхід забезпечує більшу адаптивність і задоволення споживачів, але може потребувати більше зусиль у розробці [14; 15].
8. Традиційна розробка програмного забезпечення: цей підхід передбачає послідовну та структуровану розробку, зосереджену на повних і остаточних вимогах. Цей підхід пропонує більший контроль і передбачуваність, але він може бути менш адаптованим до мінливих потреб бізнесу [16; 17].

Зазначимо, що вибір підходу до створення архітектури ПЗ, концептуальної моделі, дизайну ПЗ та розробки ПЗ залежить від різних факторів. Основними факторами є вимоги бізнесу, наявні ресурси та навички і обов'язково досвід команди розробників.

Обираючи шлях та інструменти моделювання, макетування та створення дизайну потрібно визначити критерії оцінки, проаналізувати та порівняти підходи.

Щоб оцінити ефективність різних підходів до комплексної побудови е-платформ потрібно застосувати критеріальний підхід, тобто розглянути кілька критеріїв. Загальноприйнятими критеріями оцінки ПЗ зазвичай є критерії, які відповідають міжнародному Стандарт ISO/IEC 9126, який визначає якість ПЗ , а саме:

1. Масштабованість і продуктивність: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту справлятися зі зростаючим навантаженням користувачів і транзакцій, зберігаючи при цьому прийнятні рівні продуктивності.
2. Безпека та конфіденційність: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту забезпечувати безпеку та конфіденційність даних користувачів, транзакцій та комунікацій.
3. Гнучкість і адаптивність: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту адаптуватися до мінливих бізнес-потреб, можливість запроваджувати нові фічі та функції і інтегруватися з іншими системами.
4. Взаємодія з користувачем та зручність використання: цей критерій оцінює здатність платформи е-торгівлі як програмного продукту забезпечувати зручний та інтуїтивно зрозумілий інтерфейс, що забезпечує ефективне використання клієнтами та іншими зацікавленими сторонами.

Наведені вище критерії можуть допомогти оцінити та порівняти сильні та слабкі сторони різних підходів до архітектури, моделювання, макетування, дизайну та розробки е-платформи як програмного продукту. В якісь мірі можна застосувати один із найпоширеніших аналітичних методів, який дозволяє в комплексі оцінити сильні й слабкі сторони досліджуваного об'єкту, а також можливості й загрози, що впливають на неї - SWOT-аналіз.

Однак відносна важливість кожного критерію може змінюватися в залежності від конкретних потреб і пріоритетів організації. Одним з етапів життєвого циклу програмного продукту, а в нашому випадку, платформи е-торгівлі, є процес створення концептуальної моделі та архітектури додатка.

Опишемо та порівняємо монолітну архітектуру та мікросервіси. Одне з ключових рішень, яке необхідно прийняти під час проєктування та розробки електронних ринків, полягає в тому, чи прийняти монолітну архітектуру чи архітектуру мікросервісів. Монолітна архітектура передбачає розробку електронного ринку як єдиної уніфікованої програми, тоді як архітектура мікросервісів передбачає розбиття програми на менші незалежні служби, які спілкуються одна з одною [17; 18]. Монолітна архітектура має перевагу в тому, що її простіше розробити та розгорнути, оскільки вона вимагає менше компонентів і нею можна керувати як єдиним блоком. Однак це може бути складніше масштабувати та підтримувати, оскільки додаток росте та стає складнішим. З іншого боку, архітектура мікросервісів забезпечує більшу гнучкість, масштабованість і відмовостійкість, оскільки окремі сервіси можна оновлювати, замінювати або масштабувати незалежно один від одного [19; 20]. Вибір між монолітною архітектурою та архітектурою мікросервісів має ґрунтуватися на конкретних потребах і вимогах платформи е-торгівлі. Монолітна архітектура може бути більш доцільною для невеликих, менш складних програм із меншими вимогами до масштабованості та продуктивності. Архітектура мікросервісів може краще підходити для великих, складніших додатків з вищими вимогами до масштабованості та продуктивності.

Ще один важливий фактор при проєктуванні та розробці платформ е-торгівлі – використовувати програмне забезпечення з відкритим кодом чи пропрієтарне програмне забезпечення. Програмне забезпечення з відкритим вихідним кодом є у вільному доступі, і будь-хто може отримати доступ до його вихідного коду, змінити його та розповсюдити. Власницьке програмне забезпечення, з іншого боку, належить певній компанії, і його вихідний

код зазвичай зберігається в таємниці [25; 26]. Програмне забезпечення з відкритим кодом пропонує кілька переваг, таких як економічна ефективність, підтримка спільноти, гнучкість і прозорість. Однак він може мати обмеження щодо безпеки, якості та сумісності з іншими системами. Власницьке програмне забезпечення, з іншого боку, пропонує більшу безпеку, якість і підтримку, але може бути дорожчим і мати обмежені можливості налаштування [27; 28].

Рішення про використання програмного забезпечення з відкритим кодом або пропрієтарного програмного забезпечення має ґрунтуватися на кількох факторах, таких як конкретні потреби та вимоги електронного ринку, наявність досвіду та підтримки, необхідний рівень безпеки та бюджет.

Наприклад сформована концептуальна модель на прикладі програмної компоненти e-Market places (рис.1) відображає всі складові платформи.

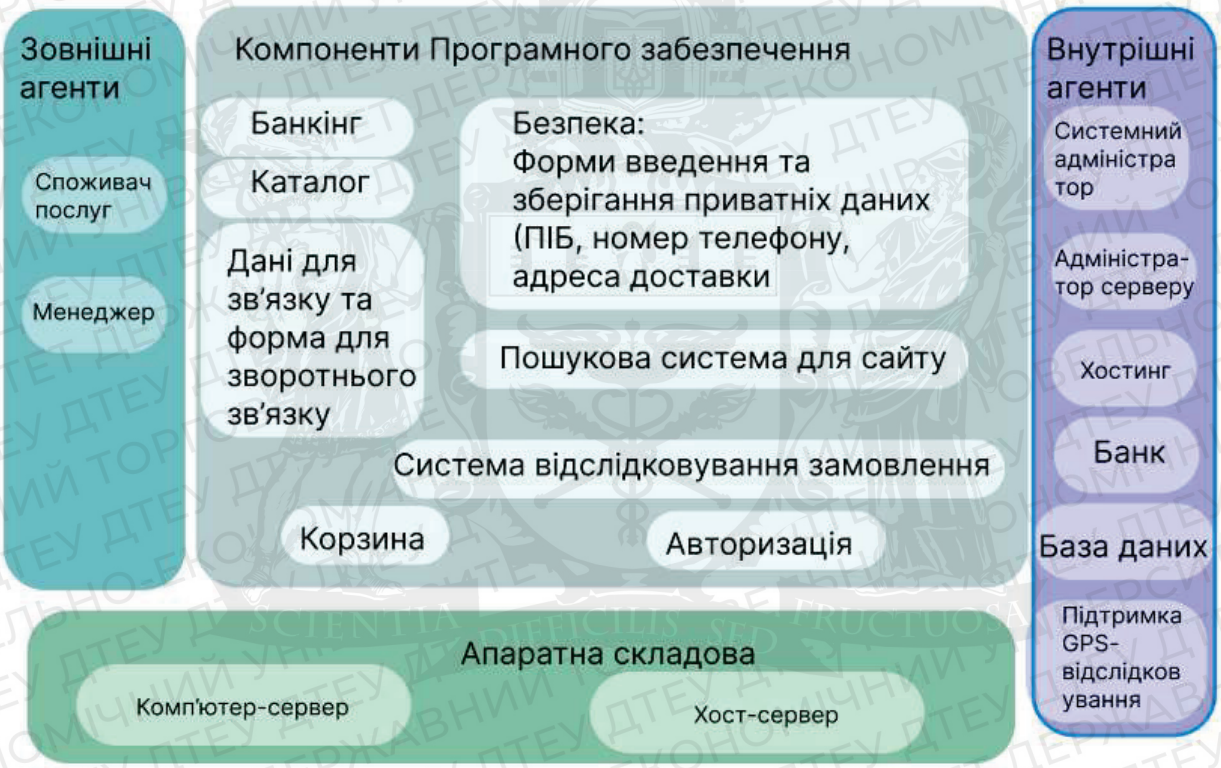


Рис. 1. Концептуальна модель програмної компоненти e-Market places
Джерело: Розроблено автором

Відповідно для розроки архітектури ПЗ застосовується мова UML. Основною причиною використання мови UML є спілкування розробників між собою. Крім того, UML спеціально створювалася для оптимізації процесу розробки програмних систем, що дозволяє збільшити ефективність їх реалізації у кілька разів і помітно поліпшити якість кінцевого продукту.

При модифікації системи об'єктний підхід дозволяє легко включати в систему нові об'єкти і виключати застарілі без істотної зміни її життєздатності. Використання побудованої моделі при модифікаціях системи дає можливість усунути небажані наслідки змін, оскільки вони не ламають структури системи, а тільки змінюють поведінку об'єктів [5].

Приклад архітектури програмної компоненти e-Market places розробленої засобами універсальної мови моделювання UML маємо на рис.2.

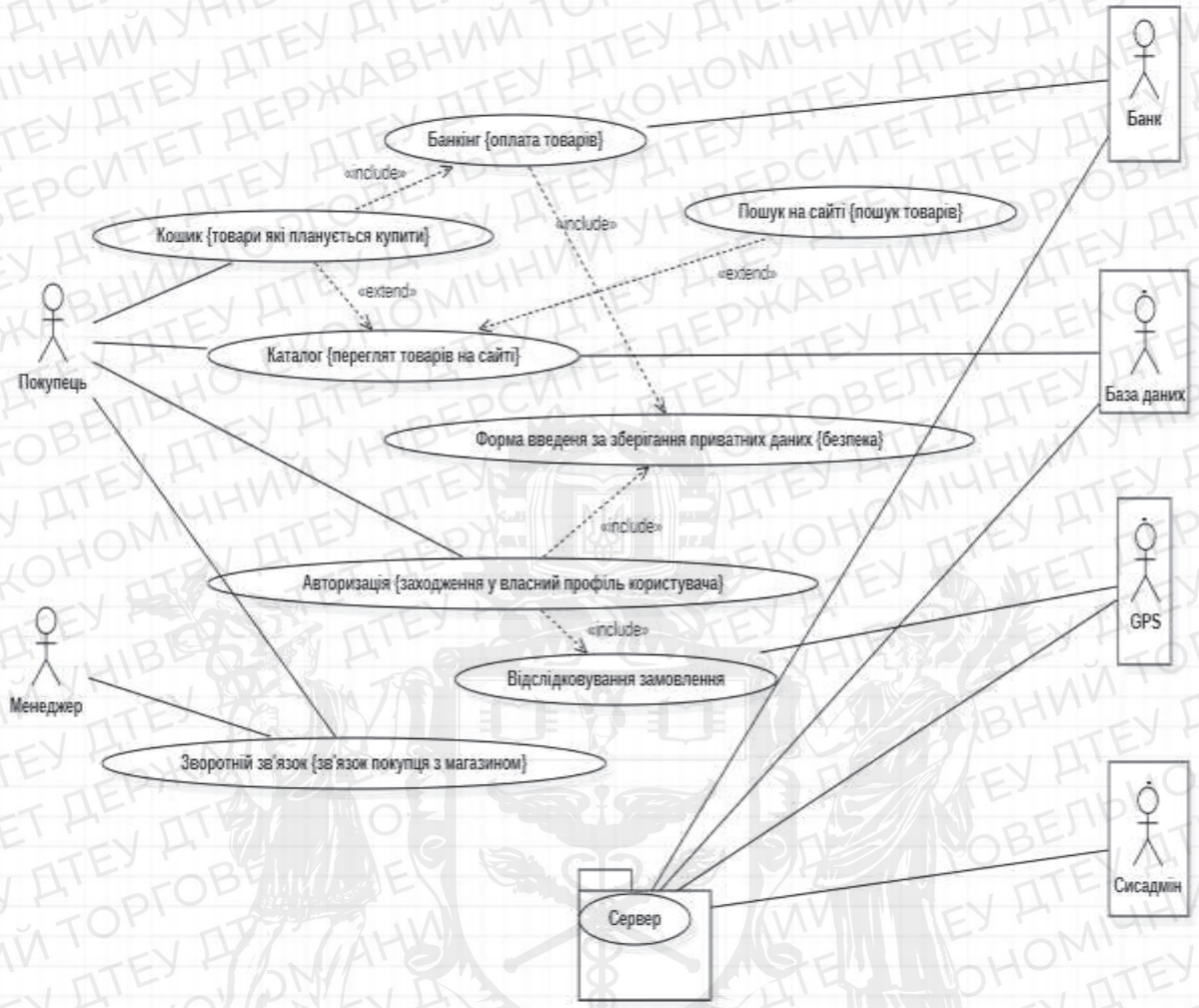


Рис. 2. USE-case програмної компоненти e-Market places
Джерело: Розроблено автором в середовищі StarUML

Висновки. Результати цього дослідження мають кілька наслідків для проєктування та розробки платформ е-торгівлі як програмного продукту. По-перше, використання архітектури мікросервісів може надати переваги з точки зору масштабованості та гнучкості. Однак необхідно ретельно розглянути складність управління та координації мікросервісів, а також запровадити відповідні інструменти та процеси, щоб забезпечити ефективну розробку, розгортання та підтримку платформ на основі мікросервісів.

Використання програмного забезпечення з відкритим вихідним кодом може надати переваги з точки зору економії коштів і внесків інвесторів, але також може вимагати більше зусиль для інтеграції та обслуговування. Слід враховувати рівень підтримки, доступний для програмного забезпечення з відкритим кодом, і досвід, необхідний для його впровадження та підтримки.

Використання гнучкої розробки програмного забезпечення може забезпечити переваги з точки зору ефективності та швидкості реагування. Однак гнучка розробка вимагає більшої координації та спілкування, і може не підійти для всіх організацій чи проєктів.

Нарешті, використання дизайну, орієнтованого на користувача, може покращити взаємодію з користувачем і зручність використання платформ е-торгівлі. Однак це вимагає більшої участі користувачів і відгуків і не завжди може відповідати бізнес-цілям платформи.

Таким чином, проєктування та розробка платформи е-торгівлі як програмного продукту вимагає ретельного розгляду різних факторів, включаючи архітектуру, технологію,

методології розробки та досвід користувача. Потрібно оцінити компроміси між різними підходами та розглянути їхні конкретні вимоги та можливості.

Це дослідження дає розуміння підходів до проектування та розробки платформ електронного ринку та критеріїв їх оцінки. Однак у цій галузі ще належить провести багато досліджень. На підставі результатів цього дослідження зроблено наступні рекомендації для майбутніх досліджень:

1. Подальше дослідження компромісів між монолітною та мікросервісною архітектурами, включно з їхнім впливом на продуктивність, масштабованість і зручність обслуговування.
2. Більш поглиблені дослідження переваг і недоліків різних постачальників PaaS і їх придатності для різних типів платформ електронного ринку.
3. Подальше дослідження проблем і можливостей використання програмного забезпечення з відкритим кодом у розробці платформ електронного ринку.
4. Дослідження ефективності різних гнучких методологій розробки програмного забезпечення в контексті розробки платформи електронного ринку.
5. Більше досліджень про вплив дизайну, орієнтованого на користувача, на взаємодію з користувачем і зручність використання платформ електронного ринку, а також про те, як його можна інтегрувати з гнучкими методологіями розробки.
6. Дослідження використання штучного інтелекту та машинного навчання при проектуванні та розробці платформ електронного ринку, а також їх вплив на масштабованість, продуктивність та досвід користувача.
7. Більше досліджень про проблеми та можливості інтеграції платформ електронного ринку з іншими системами, такими як логістика та платіжні шлюзи.

Загалом ці напрямки досліджень є важливими для вдосконалення дизайну та розвитку платформ електронного ринку, а також для покращення їх масштабованості, продуктивності, безпеки, взаємодії з користувачем та зручності використання.

Список використаних джерел

1. Cao, L., & Zhang, Z. (2011). Supply chain collaboration: Impact on collaborative advantage and firm performance. Journal of Operations Management, 29(3), 163-180.
2. Gao, Q., Liu, J., & He, L. (2018). The effect of online reviews on the performance of new products. Journal of Business Research, 89, 269-280.
3. Kurnia, S., & Chien, S. W. (2017). Electronic marketplaces: A literature review and a call for supply chain management research. International Journal of Operations & Production Management, 37(1), 54-87.
4. Choudhury, M. M., & Harrigan, P. (2014). E-marketplace adoption in the global south: A comparative analysis of institutional drivers and barriers in Egypt and New Zealand. Journal of Global Information Technology Management, 17(2), 73-96.
5. Lee, J. N., & Turban, E. (2001). A trust model for consumer internet shopping. International Journal of Electronic Commerce, 6(1), 75-91.
6. Zhang, L., Xue, Y., & Huang, L. (2018). The impact of trust on sellers' performance in cross-border e-commerce platform. International Journal of Information Management, 38(1), 155-166.
7. Amazon. (nd). Отримано 23 березня 2023 року з https://www.amazon.com/
8. Liang, T. P., Ho, Y. T., Li, Y. W., & Turban, E. (2011). What drives social commerce: The role of social support and relationship quality. International Journal of Electronic Commerce, 16(2), 69-90.
9. Wang, D., & Liang, T. P. (2011). Introduction to the special issue: E-commerce trust and governance. Journal of Electronic Commerce Research, 12(4), 266-270.
10. Chen, J., Xu, Y., Li, L., & Du, R. (2018). Design and implementation of e-commerce platform based on microservice architecture. International Journal of Wireless and Mobile Computing, 14(4), 303-311.

11. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.
12. Ma, X., Ma, J., & Wang, F. (2019). Cloud computing and intelligent logistics: A review and future directions. Computers & Industrial Engineering, 136, 1-13..
13. Pani, A. K., & Mishra, D. (2021). E-commerce logistics: A comprehensive review. Journal of Industrial Integration and Management, 6(3), 1-33.
14. Sun, H., & Zhang, P. (2018). Consumer behavior in social commerce: A literature review. Decision Support Systems, 109, 27-39.
15. Wang, Y., Wang, T., & Zhang, D. (2019). Exploring factors that influence the continuous use of mobile commerce apps: A hierarchical perspective. International Journal of Information Management, 47, 172-184.
16. Wu, L., & Wang, Q. (2020). Knowledge sharing in online health communities: A social commerce perspective. International Journal of Information Management, 50, 366-375.
17. Newman, S. (2015). Building Microservices: Designing Fine-Grained Systems. O'Reilly Media.
18. Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: yesterday, today, and tomorrow. Communications of the ACM, 60(6), 85-93.
19. Lewis, J., & Fowler, M. (2014). Microservices: a definition of this new architectural term. Retrieved from https://martinfowler.com/articles/microservices.html
20. Gorton, I. (2018). Essential software architecture (2nd ed.). Springer.
21. Markham, S., & Azevedo, L. (2015). Custom-built versus software-as-a-service (SaaS) e-commerce platforms: An exploratory study. Journal of Electronic Commerce Research, 16(4), 299-310.
22. Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC Press.
23. Han, S., & Lee, Y. (2017). Platform-as-a-Service (PaaS) adoption: The role of service quality and computer self-efficacy. Journal of Business Research, 75, 177-185.
24. Choudhary, R., & Choudhary, S. (2019). Cloud computing and its evolution: a study of platform as a service. In Proceedings of the 3rd International Conference on Communication and Electronics Systems (pp. 128-132). IEEE.
25. von Krogh, G., Haefliger, S., Spaeth, S., & Wallin, M. W. (2012). Carrots and rainbows: Motivation and social practice in open-source software development. MIS Quarterly, 36(2), 649-676.
26. Red Hat (2020). What is open source software? Retrieved from https://www.redhat.com/en/topics/open-source/what-is-open-source
27. Wohlin, C. (2014). Software quality: the future is already here. Journal of Systems and Software, 89, 3-12.
28. Curtis, B., & Krasner, H. (2015). The business value of open-source software. Journal of Systems and Software, 107, 1-12.
29. Royce, W. (1970). Managing the development of large software systems. In Proceedings of IEEE WESCON (pp. 1-9). IEEE.
30. Beck, K., Beedle, M., Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., ... & Thomas, D. (2001). Manifesto for agile software development. Retrieved from https://agilemanifesto.org/
31. Boehm, B., & Turner, R. (2003). Balancing agility and discipline: Evaluating and integrating agile and plan-driven methods. Addison-Wesley.
32. Schwaber, K. (2004). Agile project management with Scrum. Microsoft Press

Робота виконана під науковим керівництвом д.т.н., професора
КРИВОРУЧКО О. В.

МОДЕЛЬ КОМПОНЕНТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЕЛЕКТРОННОГО СУДУ

МІТУЛ Д., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Стаття присвячена моделі компоненту інформаційної системи електронного суду. Вона розглядає основні складові цієї моделі, їх функції та особливості. Крім того, у статті розглянуто основні вимоги до компонентів інформаційної системи електронного суду, а також важливість використання такої системи для забезпечення швидкого та ефективного судочинства. Для дослідження були використані різні джерела інформації, зокрема законодавчі акти та наукові статті. У результаті проведеного аналізу було зроблено висновок, що інформаційна система електронного суду є важливим елементом сучасної юстиції та є необхідною для забезпечення швидкого та доступного судочинства.

This article is devoted to the model of the component of the electronic court information system. It considers the main components of this model, their functions and features. In addition, the article considers the main requirements for the components of the electronic court information system, as well as the importance of using such a system to ensure fast and efficient judicial proceedings. Various sources of information were used for the research, including legislative acts and scientific articles. As a result of the analysis, it was concluded that the information system of the electronic court is an important element of modern justice and is necessary to ensure fast and accessible justice.

Актуальність: стаття присвячена моделі компоненту інформаційної системи електронного суду, яка є актуальною у зв'язку зі збільшенням кількості судових справ та необхідністю підвищення ефективності роботи судів.

Отже, дана робота має велике значення, оскільки вона допоможе користувачам розібратися з перевагами та недоліками різних типів програмного забезпечення для обміну захищеними даними, а також надасть інформацію про найкращі практики та технології для забезпечення безпеки даних в цифровому світі. Крім того, стаття також може бути корисною для розробників програмного забезпечення, які прагнуть створити оптимальні та безпечні продукти для обміну захищеними даними.

Метою даної роботи є розгляд моделі компоненту інформаційної системи електронного суду та її структури. Крім того, метою є проаналізувати функціональні можливості кожного компоненту та їх взаємодію в системі. За допомогою дослідження моделі компоненту інформаційної системи електронного суду можна зробити висновки про її ефективність та доцільність використання в судовій системі.

Об'єктом дослідження є інформаційна система електронного суду, а предметом – модель компоненту цієї системи. *Предметом дослідження* можна визначити саму модель, її компоненти та особливості їх функціонування в інформаційній системі електронного суду. Також можна зосередитись на аналізі технологічних рішень, що використовуються для забезпечення роботи компонентів моделі, та розглянути їх застосування в інформаційних системах електронного суду.

Аналіз попередніх досліджень. Дослідження теми електронного суду займається багато науковців та дослідників з різних країн світу. Деякі з них: Ф. Гао та І. Ван - у своїй статті "Аналіз реалізації електронного суду в Китаї" досліджують розвиток електронного суду в Китаї, а також аналізують основні проблеми, з якими цей суд стикається [1]. А. К. Іслам - у своїй статті "Електронний суд в Бангладеш: стан та проблеми розвитку" аналізує розвиток електронного суду в Бангладеш, виявляє проблеми, з якими цей суд стикається, та запропоновує шляхи їх вирішення В. Г. Павленко та ін. - у статті "Модель електронного суду

в Україні: теоретичні та прикладні аспекти" досліджують теоретичні та практичні аспекти розробки моделі електронного суду в Україні. М. Г. Сергеєва - у статті "Розвиток електронного судочинства в Україні" досліджує розвиток електронного суду в Україні, описує основні досягнення та проблеми, з якими стикається цей суд [2].

Завданням даної роботи є дослідження структури моделі компоненту інформаційної системи електронного суду та визначення його основних складових. Крім того, метою дослідження є аналіз можливостей використання цієї моделі для покращення ефективності роботи судів та забезпечення доступу до правосуддя для громадян.

Виклад основного матеріалу. В Україні з 15 грудня 2021 року було запроваджено інформаційну систему електронного судочинства. Ця система повинна забезпечити доступність та якість послуг, знизити витрати на адміністративні процеси та підвищити ефективність судової системи в цілому. Для забезпечення функціонування цієї системи необхідно розробити модель компоненту інформаційної системи електронного суду [3].

Одним з головних завдань моделювання є створення систематичного та логічного опису процесів, які відбуваються в системі. Для цього необхідно розробити відповідну модель, що дозволить аналізувати, описувати та управляти процесами електронного судочинства.

Компонент інформаційної системи електронного суду може включати в себе такі елементи:

- Система електронного документообігу, що дозволяє обмінюватися документами між судовими органами, сторонами судового процесу та іншими органами державної влади [4].
- Система підтримки прийняття рішень, що забезпечує можливість ефективного аналізу та обробки інформації, необхідної для прийняття правильного та обґрунтованого рішення.
- Система доступу до бази даних, що містить інформацію про рішення, які були ухвалені в рамках судових процесів, а також про сторони, які беруть участь у цих процесах.
- Система забезпечення безпеки даних, що забезпечує захист персональних даних.

Також, модель компоненту інформаційної системи електронного суду може містити такі складові, як модуль автентифікації користувачів, модуль керування доступом, модуль ідентифікації суб'єктів права, модуль обліку виконання судових рішень, модуль розподілу завдань між користувачами та модуль звітування [3].

Проте, на виконання моделі компоненту інформаційної системи електронного суду впливає ряд факторів, зокрема технічні можливості, доступність та якість програмного забезпечення, рівень кваліфікації персоналу та інші. Тому, для успішного функціонування інформаційної системи електронного суду необхідно враховувати ці фактори та забезпечувати постійне вдосконалення та підтримку системи.

Отже, модель компоненту інформаційної системи електронного суду є важливою складовою ефективного функціонування судової системи та забезпечення доступу до правосуддя. Проте, для її успішного впровадження необхідно враховувати технічні та організаційні аспекти та забезпечувати постійну підтримку та вдосконалення системи.

Однак, існують певні проблеми з використанням компонентної моделі в ІТ-індустрії, зокрема, змістовне описання компонентів може бути складним завданням, а також необхідно ретельно прораховувати залежності між компонентами, щоб уникнути можливих помилок [5].

Загалом, модель компоненту інформаційної системи електронного суду є важливим елементом створення сучасного та ефективного електронного суду. Для її успішної реалізації необхідно здійснювати ретельний аналіз потреб та вимог користувачів, а також враховувати сучасні технології та стандарти в галузі ІТ. Проектування та розробка моделі компоненту повинні здійснюватися згідно зі стандартами, що гарантуватимуть її стабільну роботу та безпеку.

Під час розробки моделі компоненту інформаційної системи електронного суду важливо враховувати низку вимог та рекомендацій, які висуваються до електронних судів.

Однією з таких вимог є забезпечення безпеки та конфіденційності даних, які обробляються в системі. Зокрема, це може стосуватися персональних даних учасників судового процесу, текстів рішень суду та інших документів.

Для забезпечення безпеки та конфіденційності даних у системі електронного суду можуть застосовуватися різні технічні та організаційні заходи. Наприклад, для захисту даних від несанкціонованого доступу можуть використовуватися криптографічні методи, а для забезпечення цілісності даних - методи цифрового підписування.

Окрім того, важливим елементом моделі компоненту інформаційної системи електронного суду є забезпечення доступності системи. Для цього можуть використовуватися різноманітні технічні та організаційні заходи, наприклад, використання резервного копіювання даних, запобігання збоїв у роботі системи та інші.

У цілому, розробка моделі компоненту інформаційної системи електронного суду - це складний процес, який потребує уваги до деталей та врахування різноманітних вимог і рекомендацій. Проте, забезпечення якості та безпеки роботи електронного суду дозволяє покращити якість та ефективність судової системи в цілому, що є важливим аспектом для будь-якої демократичної держави [7].

Для побудови компонентної моделі інформаційної системи електронного суду необхідно визначити функціональні блоки, які будуть складатися з цієї системи. Одним із таких блоків є реєстраційний блок, який містить в собі інформацію про справи та їх стан. До складу реєстраційного блоку входять компоненти, такі як:

- блок реєстрації справ;
- блок реєстрації користувачів;
- блок реєстрації документів;
- блок реєстрації електронних повідомлень [7].

Ще одним важливим блоком є блок авторизації та аутентифікації користувачів. Він забезпечує перевірку ідентифікаційних даних користувачів та надає їм права доступу до відповідних ресурсів системи. Цей блок може включати компоненти, такі як:

- блок авторизації користувачів;
- блок аутентифікації користувачів.

Інші важливі компоненти моделі інформаційної системи електронного суду включають такі блоки:

- блок зберігання та обробки даних;
- блок керування доступом;
- блок звітності та аналітики [7];
- блок інтеграції з іншими інформаційними системами.

Крім того, необхідно звернути увагу на аспекти безпеки інформації. У зв'язку з особливостями роботи інформаційної системи електронного суду, до неї пред'являються підвищені вимоги щодо захисту інформації. Тому в модель системи слід включити блок забезпечення безпеки інформації.

У загальному плані, модель компоненту інформаційної системи електронного суду може мати наступну структуру:

- Компонент авторизації та ідентифікації користувачів. Цей компонент забезпечує перевірку ідентифікаційних даних користувачів та контроль доступу до різних ресурсів системи.
- Компонент електронного документообігу. Цей компонент забезпечує обробку електронних документів, включаючи прийом, зберігання, обробку та передачу електронних документів в рамках судових процесів.
- Компонент судової інформації та аналізу. Цей компонент забезпечує збір та аналіз судової інформації для створення бази знань, яка допомагає вирішувати різні питання в судових процесах.

- Компонент електронної служби підтримки користувачів. Цей компонент забезпечує надання користувачам електронної підтримки з питань, пов'язаних з використанням системи електронного суду.
- Компонент забезпечення безпеки. Цей компонент забезпечує захист інформації в системі електронного суду від несанкціонованого доступу, знищення та модифікації [8].

Ці компоненти можуть мати різну структуру та складатися з різних модулів, але вони взаємодіють між собою для забезпечення повного функціонування інформаційної системи електронного суду.

Однією з ключових складових компонентної моделі інформаційної системи є модель компонентів. Модель компоненту визначає функціональні можливості компоненту, його інтерфейси та протоколи взаємодії з іншими компонентами системи, а також його залежності від інших компонентів.

Модель компоненту інформаційної системи електронного суду має на меті забезпечення ефективної роботи судової системи шляхом створення високопродуктивної та масштабованої інформаційної інфраструктури.

Іншим компонентом моделі є компонент "Інтерфейс користувача", який забезпечує інтерфейс для користувачів системи. Цей компонент забезпечує доступ до функцій системи та можливість управління даними користувачів.

Крім того, модель включає компонент "Система управління даними", який забезпечує зберігання, організацію та обробку даних, що використовуються в системі. Цей компонент забезпечує безпеку та цілісність даних, а також можливість доступу до них відповідно до встановлених правил доступу.

У процесі розробки моделі компоненту інформаційної системи електронного суду, необхідно враховувати вимоги до безпеки та конфіденційності даних, а також забезпечувати швидкий доступ до інформації та її ефективну обробку [8].

Нова модель інформаційної системи електронного суду в Україні відповідає найвищим стандартам якості та безпеки, що дозволяє забезпечити швидкий та ефективний доступ до інформації та забезпечує високий рівень захисту персональних даних.

Проте, важливо зазначити, що успішність реалізації цієї моделі залежить від різних факторів, таких як рівень підготовки фахівців, забезпечення відповідної інфраструктури та налагодження ефективної системи контролю якості. Для досягнення максимальної ефективності та успішної реалізації моделі, важливо забезпечити всі необхідні ресурси та провести необхідний ряд заходів для підготовки фахівців та створення відповідних умов для ефективного впровадження цієї моделі.

Реалізація цієї моделі компоненту інформаційної системи електронного суду є важливим завданням для забезпечення якісної та ефективної роботи електронного судового установи. При використанні такої моделі, можливе створення інтегрованої системи, яка дозволить автоматизувати багато процесів та процедур, що покращить швидкість та якість прийняття рішень. Крім того, ця модель дозволить забезпечити високий рівень захисту інформації та забезпечити її доступність для користувачів. Важливо зазначити, що реалізація такої моделі потребує значних зусиль, в тому числі забезпечення необхідних ресурсів та кваліфікації персоналу.

Отже, модель компоненту інформаційної системи електронного суду є важливою складовою для забезпечення ефективної та безпечної роботи всієї системи. Вона дозволяє забезпечити необхідну функціональність та інтеграцію різних компонентів системи, що дозволяє ефективно вирішувати завдання судової влади та забезпечувати доступ до юстиції для громадян [6].

Висновки: Заключаючи, можна сказати, що модель компоненту інформаційної системи електронного суду є важливою складовою для забезпечення якісного та ефективного функціонування електронної системи юстиції в Україні. Вона передбачає використання різних компонентів, таких як адаптер, мережа, база даних, програмне забезпечення та інші, щоб

забезпечити швидку та точну обробку інформації про судові справи та забезпечити доступ до цієї інформації для відповідних сторін.

Нова модель інформаційної системи електронного суду в Україні відповідає найвищим стандартам якості та безпеки, що дозволяє забезпечити швидкий та ефективний доступ до інформації та забезпечує високий рівень захисту персональних даних.

Проте, важливо зазначити, що успішність реалізації цієї моделі залежить від різних факторів, таких як рівень підготовки фахівців, забезпечення відповідної інфраструктури та налагодження ефективної системи контролю якості. Для досягнення максимальної ефективності та успішної реалізації моделі, важливо забезпечити всі необхідні ресурси та провести необхідний ряд заходів для підготовки фахівців та створення відповідних умов для ефективного впровадження цієї моделі.

Можна зробити висновок, що модель компоненту інформаційної системи електронного суду є важливим елементом в ефективному функціонуванні системи юстиції в Україні.

Реалізація цієї моделі компоненту інформаційної системи електронного суду є важливим завданням для забезпечення якісної та ефективної роботи електронного судового установи. При використанні такої моделі, можливе створення інтегрованої системи, яка дозволить автоматизувати багато процесів та процедур, що покращить швидкість та якість прийняття рішень. Крім того, ця модель дозволить забезпечити високий рівень захисту інформації та забезпечити її доступність для користувачів. Важливо зазначити, що реалізація такої моделі потребує значних зусиль, в тому числі забезпечення необхідних ресурсів та кваліфікації персоналу.

Отже, можна стверджувати, що модель компоненту інформаційної системи електронного суду має важливе значення для покращення роботи судових установ та забезпечення якісного та ефективного надання юридичних послуг. Реалізація цієї моделі може стати важливим кроком вперед у розвитку електронної юстиції в Україні.

Список використаних джерел

1. Шаблій, С. Модель компонентів системи електронного документообігу / С. Шаблій, М. Короткін, Н. Шатова // Науковий вісник Полісся. - 2018. - № 1 (13). - С. 31-39.
2. Бреславська, Г. Моделювання та аналіз процесів в електронних судах / Г. Бреславська, Т. Чуєв // Наукові записки. Серія: Проблеми інформатизації та управління. - 2019. - Т. 33. - С. 62-71.
3. Хамам, М. Розвиток електронного судочинства в Україні: тенденції та перспективи / М. Хамам, С. Буцьо // Правова держава. - 2018. - № 5. - С. 44-51.
4. Урядовий портал: "Електронний суд стане доступним усім українцям до кінця року" (https://www.kmu.gov.ua/news/elektronniy-sud-stane-dostupnim-usim-ukrayincam-do-kincya-roku)
5. Інформаційний портал "Судова влада України": "Електронний суд - це новітній етап розвитку юстиції" (https://www.court.gov.ua/sudova-vlada/elektronniy-sud-tse-novitniy-etap-rozvitku-yustitsiyi)
6. Інтернет-видання "Українська правда": "Електронний суд відкриває можливості, про які раніше не мріяли" (https://www.pravda.com.ua/articles/2020/11/17/7277641/)
7. Інформаційний портал "Yuridicheskaya Gazeta": "Україна відкрила перший в Європі електронний суд" (https://yur-gazeta.com/publications/ukrayina-vidkryla-pershyj-v-yevropi-elektronnyj-sud.html)
8. Інформаційний портал "Legal Practice": "Електронний суд: як працює нова система судочинства" (https://lp.ua/ua/blog/elektronnyj-sud-yak-pracyuye-nova-systema-sudochynstva/)

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н.О.

КОНЦЕПТУАЛЬНІ ПІДХОДИ ПОБУДОВИ АРХІТЕКТУРИ ВЕБ-ДОДАТКУ ЗАСОБАМИ UML

МІЩЕНКО В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто концептуальні підходи до побудови архітектури веб-додатків з використанням засобів UML. Проаналізовано ефективність та універсальність використання засобів UML. Представлено аналоги засобів UML та їх недоліки в порівнянні з засобами UML. Для основних діаграм UML надано приклад використання та описано її внесок у побудову архітектури веб-додатка, розробленого в розрізі магістерського дослідження.

The article discusses conceptual approaches to building the architecture of web applications using UML tools. The efficiency and versatility of using UML tools are analyzed. Analogues of UML tools and their shortcomings in comparison with UML tools are presented. For basic UML diagrams, an example of use is provided and its contribution to the construction of the architecture of a web application developed as part of a master's study is described.

Актуальність. Інтернет займає важливе місце в повсякденному житті людей. Інтернет-технології надають можливість здійснювати багато різних дій, від замовлення товарів та послуг до соціальних інтеракцій. Веб-додатки є однією з ключових складових інтернету. Використовуючи веб-додатки, можна забезпечити швидкий та зручний доступ до інформації, зберігати дані в хмарних сховищах та забезпечувати роботу з великими обсягами даних. Такі додатки дозволяють користувачам забезпечувати взаємодію з різноманітними джерелами даних та оброблювати їх у режимі реального часу. В цілому, веб-додатки є важливими засобами для забезпечення взаємодії з користувачами та ефективного використання ресурсів інтернету. Вони є необхідним елементом інформаційної інфраструктури та економіки.

З огляду на все більше зростаючу популярність веб-додатків, розробники повинні мати достатні знання та навички для створення надійної та ефективної архітектури веб-додатку. У зв'язку з цим, побудова якісної архітектури веб-додатків є критично важливою для їх успішного впровадження та функціонування.

Використання засобів UML при побудові архітектури веб-додатків є найбільш розповсюдженим та ефективним підходом, оскільки UML надає зручний та стандартизований мовник для опису архітектури системи. Детальний аналіз концептуальних підходів до побудови архітектури веб-додатків з використанням засобів UML може бути корисним для розробників програмного забезпечення, які прагнуть забезпечити масштабованість, розширюваність та безпеку своїх веб-додатків.

Також актуальність статті полягає в тому, що побудова архітектури веб-додатків є складним та багатоаспектним процесом, тому знання концептуальних підходів до її побудови може допомогти розробникам зменшити кількість помилок та забезпечити високу якість свого програмного забезпечення.

Метою статті є аналіз концептуальних підходів до побудови архітектури веб-додатків з використанням засобів UML, щоб допомогти розробникам програмного забезпечення зрозуміти основні принципи побудови архітектури веб-додатків та використання засобів UML для її моделювання..

Об'єктом дослідження є розробки архітектури веб-додатку з використанням засобів UML, розгляд підходів до побудови архітектури веб-додатку, з використанням UML, а також оцінку ефективності використання UML для розробки веб-додатків.

Основним завданням статті є дослідити важливість побудови якісної архітектури веб-додатків, проаналізувати концептуальні підходи до її побудови та продемонструвати практичне застосування засобів UML для моделювання архітектури веб-додатків.

Предметом дослідження статті є концептуальні підходи до побудови архітектури веб-додатків з використанням засобів UML. У статті розглядається теоретичний аспект побудови якісної архітектури веб-додатків, що базується на концептуальних принципах, та їх відображення в моделях UML.

Виклад основного матеріалу. Веб-додатки стали необхідним інструментом для бізнесу та користувачів. За допомогою веб-додатків можна здійснювати покупки, забронювати квитки, знаходити інформацію та взагалі отримувати доступ до безлічі різноманітних сервісів. Однак, побудова веб-додатків не є простим завданням, оскільки вони повинні бути ефективними, безпечними та зручними в користуванні.

У цьому контексті концептуальні підходи побудови архітектури веб-додатків грають важливу роль.

Перед появою UML існувало багато мов моделювання, таких як Structured Analysis and Design Technique (SADT), Yourdon Systems Method (YSM), Data Flow Diagrams (DFD) та інші. Однак, жодна з цих мов не була стандартизована і не забезпечувала єдиного підходу до моделювання.

У 1994 році Об'єднана група експертів з об'єктно-орієнтованого моделювання (Object Management Group, OMG) визначила потребу в єдиній мові моделювання для об'єктно-орієнтованого програмування. Це призвело до створення UML в 1997 році. [1].

UML став стандартом моделювання програмного забезпечення і отримав широке використання в індустрії програмного забезпечення і в академічних кругах.

Для побудови архітектури веб-додатку можна використовувати різні підходи.

UML (Unified Modeling Language) - це стандартизована мова моделювання, яка використовується для побудови програмного забезпечення. UML надає засоби для опису різних аспектів програмного забезпечення, включаючи структуру, поведінку та взаємодію між складовими. UML має багато різних діаграм, кожна з яких описує різний аспект програмного забезпечення [2].

BPMN (Business Process Model and Notation) - це мова моделювання бізнес-процесів, яка використовується для опису послідовності роботи бізнес-процесів. Вона дозволяє представити бізнес-процеси у вигляді графів, які відображають послідовність дій [3].

ER-діаграми (Entity-Relationship Diagrams) - це мова моделювання, яка дозволяє описувати концептуальні схеми за допомогою узагальнених конструкцій блоків. Вона дозволяє відобразити взаємозв'язки між таблицями баз даних [4].

FD-діаграми (Data Flow Diagrams) - це мова моделювання, що використовується для опису потоків даних у системі. Вона дозволяє відображати, як дані рухаються в системі та як вони обробляються [5].

ArchiMate - це мова моделювання, що використовується для побудови архітектури додатків та систем. Вона дозволяє описати архітектуру системи з різних точок зору, включаючи бізнес, технічну та інформаційну архітектуру [6].

Аналоги мов моделювання мають свої недоліки в порівнянні з UML. BPMN призначений для моделювання бізнес-процесів, а не архітектури програмного забезпечення, тому він може бути менш корисним для розробників програмного забезпечення. ER-діаграми зосереджені на моделюванні відносин між таблицями баз даних, тому ввони можуть бути менш ефективними для моделювання архітектури програмного забезпечення, яка може містити більше ніж просто бази даних. DFD-діаграми зосереджені на моделюванні потоків даних. ArchiMate більш орієнтований на бізнес-процеси і менш на опис технічних аспектів системи.

UML залишається одним з найпопулярніших та найбільш широко використовуваних засобів для моделювання архітектури програмного забезпечення.

У дослідженнях UML брали участь вчені та дослідники з усього світу, включаючи представників відомих університетів, інститутів та корпорацій такі як Граді Буч [1], Івар Якобсон [1], Джеймс Рамбо [1], Бертран Мейє [7] , Мартін Фаулер [8]. З їхніх напрацювань, можна зробити висновок, що універсальність UML полягає у можливості моделювання різних

аспектів програмного забезпечення, можливості використання для будь-якої мови програмування, ефективному спілкуванні зі стейкхолдерами, плануванні та управлінні проектами, проведенні аналізу та тестуванні програмного забезпечення, наявності великої спільноти користувачів та підтримки, можливості створення готових шаблонів та бібліотек. Всі ці переваги дозволяють розробникам програмного забезпечення більш ефективно розробляти та управляти проектами, зменшуючи час та кошти, та забезпечувати якість програмного забезпечення.

UML є ефективною та адаптивною до будь якого проекту мовою моделювання, оскільки надає засоби для опису різних аспектів програмного забезпечення, включаючи структуру, поведінку та взаємодію між складовими. UML має багато різних діаграм, кожна з яких описує різний аспект програмного забезпечення. Це дозволяє розбити архітектуру веб-додатку на окремі складові та моделювати кожну з них окремо. Наприклад, можна використовувати діаграму взаємодії для опису поведінки додатку, діаграму компонентів для опису структури компонентів та їх взаємодії, діаграму послідовності для опису послідовності виконання дій тощо. Використання UML дозволяє візуалізувати архітектуру веб-додатку, що допомагає зрозуміти його структуру та функціональність. Це може бути корисним для комунікації з іншими учасниками проекту, включаючи розробників, тестувальників та замовників.

Архітектура веб-додатку описує структуру та взаємодію між складовими додатку. Веб-додатки складаються з трьох основних складових: клієнтської сторони, серверної сторони та бази даних. Клієнтська сторона - це інтерфейс, який користувач використовує для взаємодії з додатком. Серверна сторона - це програмне забезпечення, яке забезпечує функціональність додатка та взаємодію з базою даних. База даних - це система, яка зберігає дані, які використовуються додатком [9].

UML дозволяє розробникам побудувати детальну модель системи, яка може включати в себе діаграми класів, діаграми послідовностей та діаграми діяльності, діаграма прецедентів, діаграма станів, діаграма компонентів, діаграма розгортання.

Діаграми дозволяють розробникам зрозуміти функціональність системи, її структуру та взаємодії компонентів, що в свою чергу сприяє якості та ефективності розробки веб-додатку. Після створення всіх необхідних діаграм розробники можуть використовувати їх для створення коду системи та розробки веб-додатку.

У веб-додатках архітектура визначає, як різні компоненти системи взаємодіють між собою та як вони розташовані. Побудова архітектури веб-додатків з використанням UML дозволяє розробникам зосередитися на суттєвих аспектах системи та забезпечити її ефективну та безпечну роботу.

Узагальнюючи, побудова архітектури веб-додатку з використанням UML є важливим етапом розробки будь-якої системи. Вона дозволяє розробникам краще зрозуміти вимоги до системи, визначити її основні компоненти та забезпечити її ефективну та безпечну роботу. Використання UML дозволяє зменшити ризики помилок та підвищити якість розробки, що є важливим для будь-якої компанії, що займається розробкою веб-додатків.

Для візуального представлення структури, поведінки та взаємодії системи або програмного забезпечення розглянемо діаграми UML на прикладах.

Інформація про акторів, та опис випадків використання:

Актори-користувачі: Клієнт – клієнт інтернет-магазину. Менеджер з продажу: користувач, що використовує функції адміністрування сайту.

Актори-зовнішні системи: База даних – база даних, яка зберігає інформацію.

В даній діаграмі наведені відношення між акторами та використаннями, що демонструє зв'язки між акторами та їх поведінкою в системі (Рис.1).

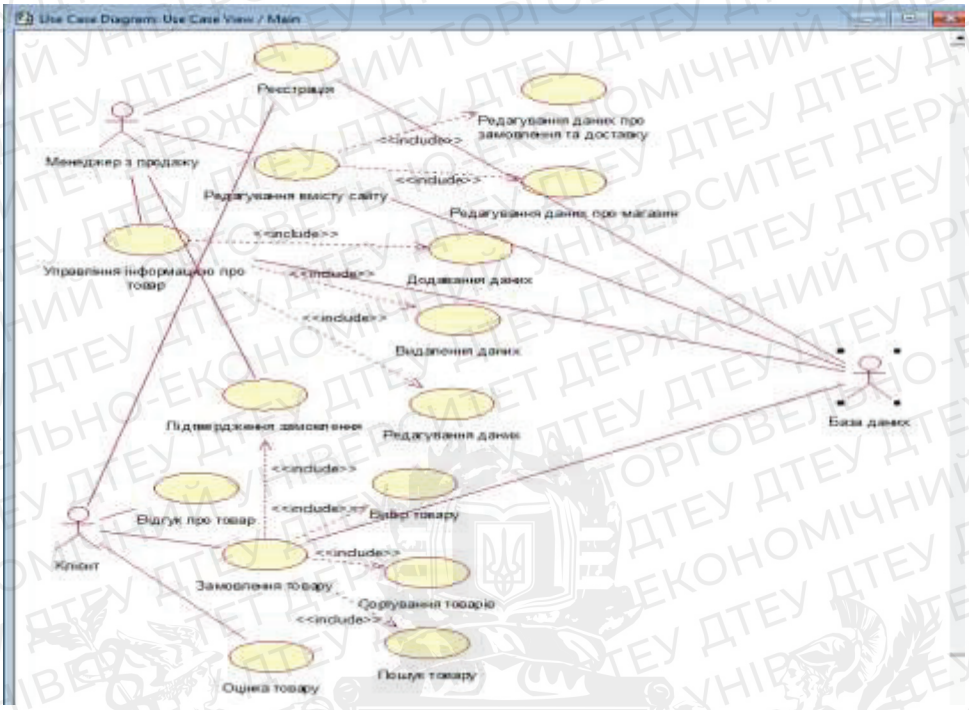


Рис. 1. UML-діаграма використання програмного продукту інтернет-магазину. Джерело:розроблено автором в середовищі IBM Rational Rose Enterprise Edition (скріншот з екрану)

Діаграма демонструє опис процесу авторизації клієнта. Якщо логін та пароль було введено коректно, в браузері відображається особистий кабінет користувача (Рис.2).

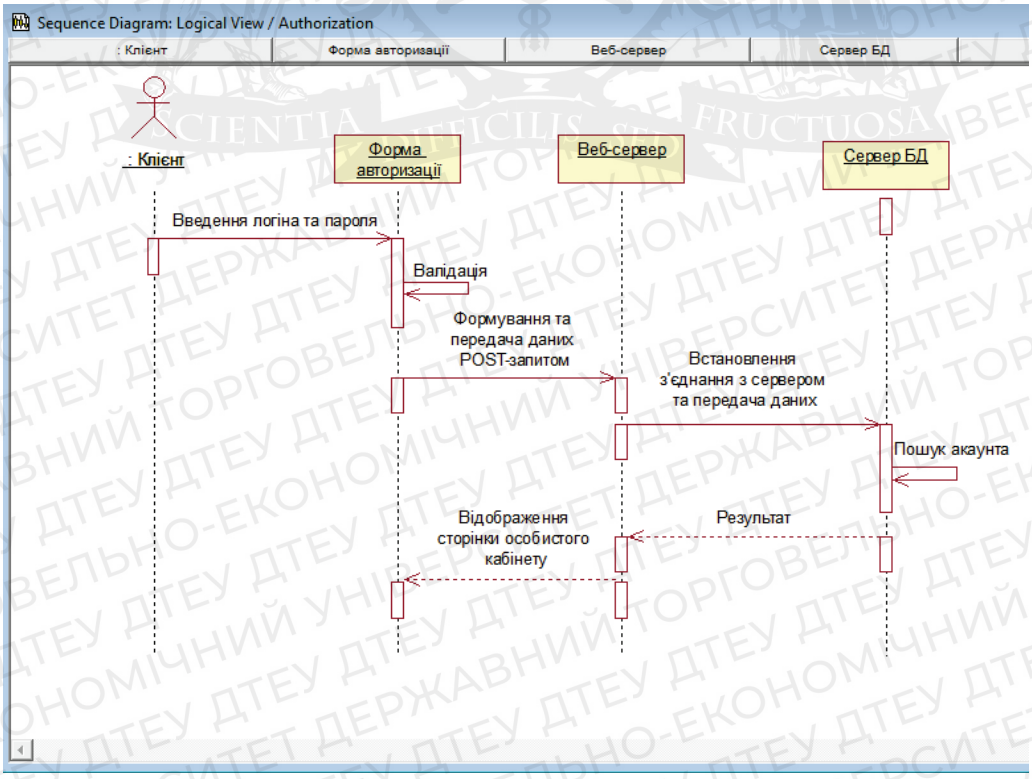


Рис. 2. UML-діаграма послідовності авторизації програмного продукту інтернет-магазину. Джерело:розроблено автором в середовищі IBM Rational Rose Enterprise Edition (скріншот з екрану)

Дана схема демонструє роботу інтернет-магазину, а саме:

При вході на сайт інтернет-магазину користувачу відображається головна сторінка, на якій необхідно зареєструватись або ввести персональні дані, якщо він зареєстрований. Далі потрібно обрати товар, скориставшись функціоналом сайту. Після вибору товару зареєстрованим користувачам запропонують вибрати метод оплати та доставки. Після перевірки всіх даних необхідно підтвердити замовлення. Інформація про зроблене замовлення переглядається менеджером магазину та передається на виконання (Рис.3).

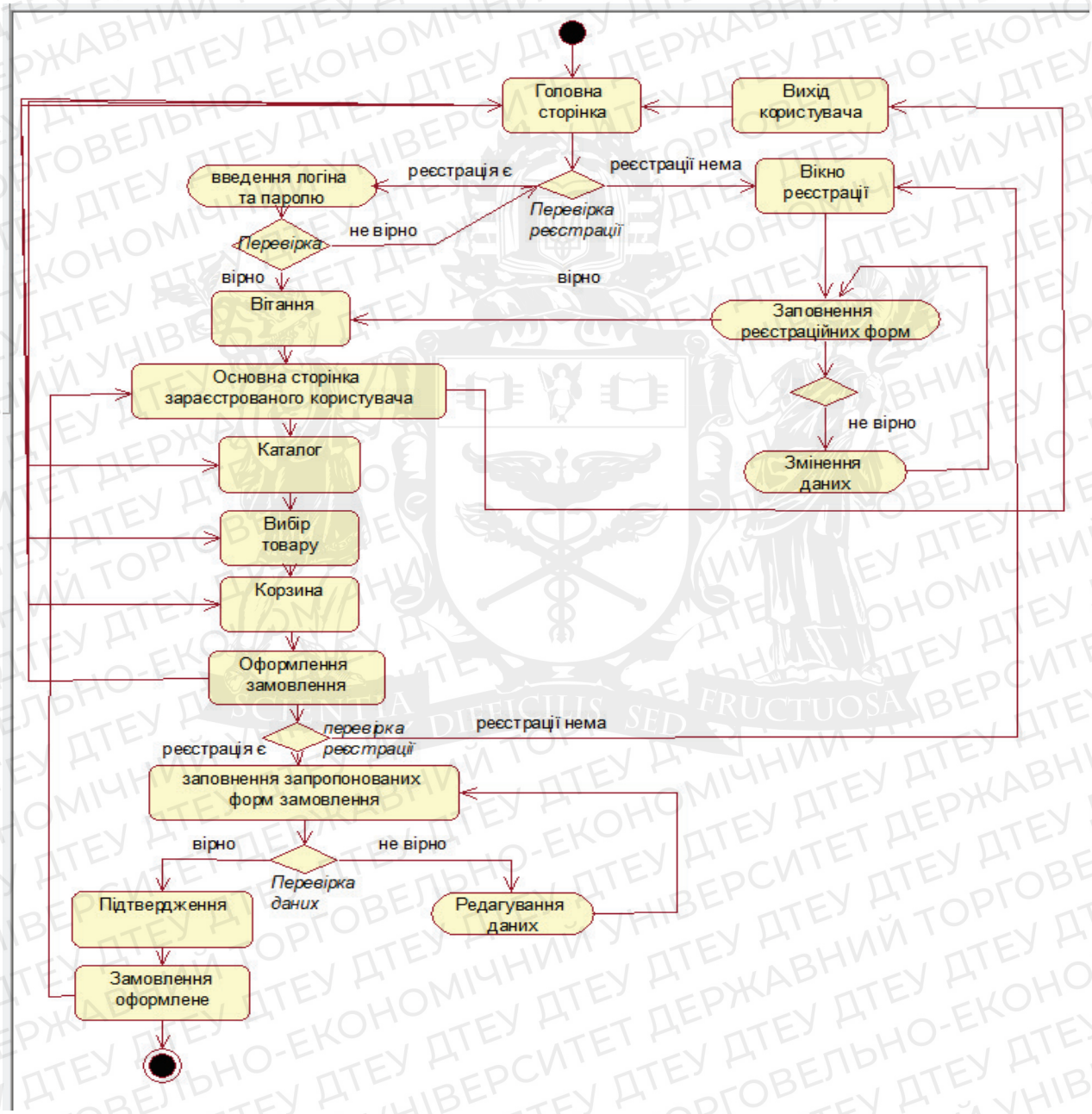


Рис. 3. UML-діаграма діяльності програмного продукту інтернет-магазину. Джерело:розроблено автором в середовищі IBM Rational Rose Enterprise Edition (скріншот з екрану)

Таким чином, основні переваги використання діаграм UML включають:

1. Спрощення спілкування між розробниками та іншими зацікавленими сторонами: діаграми UML надають зручний спосіб спілкування між розробниками та іншими зацікавленими сторонами, які можуть не мати технічних знань.

2. Допомога в розумінні структури системи: діаграми UML допомагають розробникам розуміти структуру системи та взаємодію її компонентів.

3. Виявлення проблем та помилок на ранніх етапах розробки: діаграми UML допомагають виявляти проблеми та помилки на ранніх етапах розробки, коли виправлення їх вартує менше.

4. Підвищення ефективності розробки: діаграми UML допомагають розробникам швидко та ефективно розуміти та змінювати систему.

5. Підтримка документації: діаграми UML можуть бути використані для створення документації про систему.

Висновки. У цій статті було розглянуто деякі концептуальні підходи до побудови архітектури веб-додатків за допомогою засобів UML. Використання UML діаграм допомагає створити чітке та зрозуміле опис програмного забезпечення, його компонентів та взаємодії між ними.

Незалежно від обраної діаграми, основним завданням при побудові архітектури веб-додатку є забезпечення його масштабованості та ефективності. Особливо важливою є підтримка розширюваності, що дозволяє додавати нові функції до додатку без необхідності переписування вже існуючого коду.

Крім того, побудова архітектури веб-додатка повинна враховувати вимоги до безпеки даних та захисту від зловмисників. У цьому контексті важливо розглянути різні варіанти зберігання даних та забезпечення їх конфіденційності та цілісності.

Усі ці аспекти повинні бути враховані при побудові архітектури веб-додатку, тому використання засобів UML може значно полегшити цей процес. Діаграми UML надають можливість створювати чіткі та зрозумілі описи програмного забезпечення, які дозволяють розробникам краще розуміти структуру додатка та взаємодію між його компонентами.

Список використаних джерел

1. Booch G, Rumbaugh J., Jacobson I. Tutorial «The Unified Modeling Language User Guide (2nd Edition)» – USA: Wesley Professional, 1998. – 512 p. ISBN: 0-201-57168-4
2. Larman C. Tutorial «Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd ed.)» – USA: Prentice Hall, 2004. – 630 p. ISBN: 978-0131489066
3. Silver B. Tutorial «Bpmn Method and Style, 2nd Edition, with Bpmn Implementer's Guide» – USA: Cody-Cassidy Press, 2011. – 286 p. ISBN: 978-0982368114
4. Модель «сутність — зв'язок». Електронний ресурс URL: https://uk.wikipedia.org/wiki/Модель_«сутність_—_зв'язок» (останнє звернення 23.03.2023р.)
5. Shelly G., Cashman T., Rosenblatt H. Tutorial «Systems Analysis and Design 7th Edition 4» – USA: Course Technology, 2007. – 702 p. ISBN: 978-1423912224
6. Archimate-overview. Електронний ресурс URL: https://www.opengroup.org/archimate-overview (останнє звернення 25.03.2023р.)
7. B. Meyer. Tutorial «Object-Oriented Software Construction» – USA: Pearson College Div, 2000. – 1296 p.. ISBN: 978-0136291558
8. M. Fowler. Tutorial «UML Distilled: A Brief Guide to the Standard Object Modeling Language» – USA: Addison-Wesley Professional, 2003. – 208 p. ISBN: 978-0321193681
9. L.Shklar, R.Rosen. Tutorial «Web Application Architecture: Principles, Protocols and Practices» – USA: John Wiley & Sons Ltd , 2003, – 357 p. ISBN: 0-471-48656-6

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А. М.

СТРУКТУРИ ДАНИХ В ФУНКЦІОНАЛЬНОМУ ОТОЧЕННІ

МОСКАЛЕНКО В., 2м курс ФІТ ДТЕУ
спеціальність «Інженерія програмного забезпечення»

Ця стаття має на меті проаналізувати властивості, операції та характеристики продуктивності двох модифікацій куп: біноміальних куп та лівоцентрованих куп. Надаючи детальний аналіз цих структур даних та їх застосування в різних контекстах, ця робота сприяє розумінню та проектуванню структур даних у функціональному середовищі. Зокрема, ця робота має на меті дослідити переваги та недоліки біноміальних та лівоцентрованих куп, їхні характеристики продуктивності та придатність для використання у графових алгоритмах та чергах з пріоритетами.

This article aims to analyze the properties, operations, and performance characteristics of two modifications of heaps: binomial heaps and left-centered heaps. By providing a detailed analysis of these data structures and their application in various contexts, this work contributes to the understanding and design of data structures in a functional environment. In particular, this paper aims to investigate the advantages and disadvantages of binomial and left-centered heaps, their performance characteristics, and their suitability for use in graph algorithms and priority queues.

Актуальність. Структури даних відіграють важливу роль в інформатиці, надаючи засоби для організації та маніпулювання даними в ефективний та раціональний спосіб. В останні роки зростає інтерес до функціонального програмування - парадигми, яка наголошує на використанні функцій та незмінних структур даних. Ця стаття досліджує тему структур даних у функціональному середовищі, зосереджуючись на двох специфічних модифікаціях куп: біноміальних купах та лівоцентрованих купах.

Хоча купи є добре відомою структурою даних, їх модифікації у функціональному середовищі є відносно новими і не були широко вивчені. Ця робота має на меті заповнити цю прогалину, надавши детальний аналіз біноміальних та лівоцентрованих куп, їх властивостей, операцій та характеристик продуктивності.

Метою статті є аналіз переваг та недоліків цих структур даних, їхніх характеристик продуктивності та застосування в різних контекстах. Таким чином, ми прагнемо надати уявлення про проектування та використання структур даних у функціональному середовищі.

Для досягнення мети цієї роботи були поставленні наступні **завдання**:

- Надамо детальне визначення біноміальної купи та лівоцентрованої купи.
- Опишемо їх властивості та операції.
- Проаналізуємо їхні характеристики, включаючи часову та просторову складність.
- Обговорити їх застосування в різних контекстах, таких як графові алгоритми та черги з пріоритетами.

Предметом дослідження є структури даних у функціональному середовищі, зокрема біноміальні купи та лівоцентровані купи.

Об'єктом дослідження є аналіз властивостей, операцій та характеристик продуктивності біноміальних та лівоцентрованих куп, а також обговорення їх застосування в різних контекстах.

Виклад основного матеріалу. Біноміальна купа – це структура даних, яка використовується для реалізації пріоритетних черг у функціональному середовищі програмування. Це набір бінарних дерев, де кожне дерево задовольняє властивості купи: батьківський вузол має вищий пріоритет, ніж його дочірні. Дерева в біноміальній купі

будуються за певним шаблоном, де i-те дерево має 2^i вузлів, а корінь кожного дерева має ступінь і. Ступінь вузла - це кількість дочірніх вузлів, які він має.

Біноміальні купи підтримують такі операції: вставка, пошук мінімуму, злиття, зменшення та видалення мінімуму. Щоб вставити елемент у купу, створюється нове дерево, яке об'єднується з існуючою купою. Операція find-minimum повертає елемент з мінімальним пріоритетом, не видаляючи його з купи. Операція злиття об'єднує дві біноміальні купи в одну купу. Операція зменшення використовується для зменшення пріоритету елемента, що вже знаходиться в купі. Операція delete-minimum видаляє елемент з мінімальним пріоритетом з купи.

Біноміальні купи мають кілька переваг над іншими структурами даних у функціональному середовищі. По-перше, вони забезпечують ефективні операції з логарифмічною часовою складністю для вставки, пошуку мінімуму та видалення мінімуму. По-друге, вони підтримують об'єднання двох куп з логарифмічною часовою складністю. По-третє, вони мають гарантовану амортизовану постійну часову складність для операцій зменшення ключа.

Однак біноміальні купи також мають деякі недоліки. Вони вимагають більше місця у порівнянні з іншими структурами даних з пріоритетною чергою. Крім того, операція злиття може вимагати створення та об'єднання нових дерев, що призводить до збільшення використання пам'яті та зниження продуктивності.

Характеристики продуктивності біноміальних куп можна проаналізувати за допомогою математичних формул. Часова складність операції вставки становить $O(\log n)$, де n - розмір купи. Часова складність операції пошуку мінімуму становить $O(1)$, а операції видалення мінімуму - $O(\log n)$. Часова складність операції злиття становить $O(\log n)$, а просторова складність - $O(n)$.

На рисунку 1.1 зображений алгоритм для біноміальних та лівоцентрованих куп.

На додаток до своїх переваг і недоліків, біноміальні купи мають кілька цікавих властивостей, які роблять їх унікальними серед структур даних. Наприклад, біноміальну купу розміру n можна представити у вигляді двійкового числа, де біти 1 відповідають кореням дерев у купі. Ця властивість дозволяє ефективно об'єднувати дві біноміальні купи за допомогою побітових операцій.

Ще однією цікавою властивістю біноміальних куп є їх зв'язок з двійковими числами та зв'язок з двійковим представленням цілих чисел. Зокрема, біноміальну купу можна використовувати для представлення двійкового розкладу цілого числа, при цьому степінь кожного вузла представляє позицію відповідного біта у двійковому представленні.

Ці властивості демонструють багату математичну структуру, що лежить в основі біноміальних куп, і підкреслюють їх потенціал для використання в різних додатках за межами черг пріоритетів. Загалом, біноміальні купи є цікавою структурою даних, яка заслуговує на подальше вивчення та аналіз в контексті функціонального програмування.

Ще однією цікавою властивістю біноміальних куп є їх зв'язок з графовими алгоритмами. Зокрема, біноміальні купи можна використовувати для реалізації алгоритму Дейкстри, відомого графового алгоритму, який використовується для пошуку найкоротшого шляху між двома вершинами у зваженому графі. Використовуючи біноміальну купу для зберігання набору невідвіданих вершин та їх відстаней від початкової вершини, алгоритм Дейкстри може досягти часової складності O(E + V log V), де E - кількість ребер, а V - кількість вершин у графі.

На додаток до алгоритму Дейкстри, біноміальні купи також можна використовувати для реалізації інших графових алгоритмів, таких як алгоритм Прима для пошуку мінімального остовного дерева та алгоритм Крускала для пошуку мінімального остовного лісу. Це підкреслює універсальність біноміальних куп та їхній потенціал для використання у різноманітних додатках, окрім пріоритетних черг.

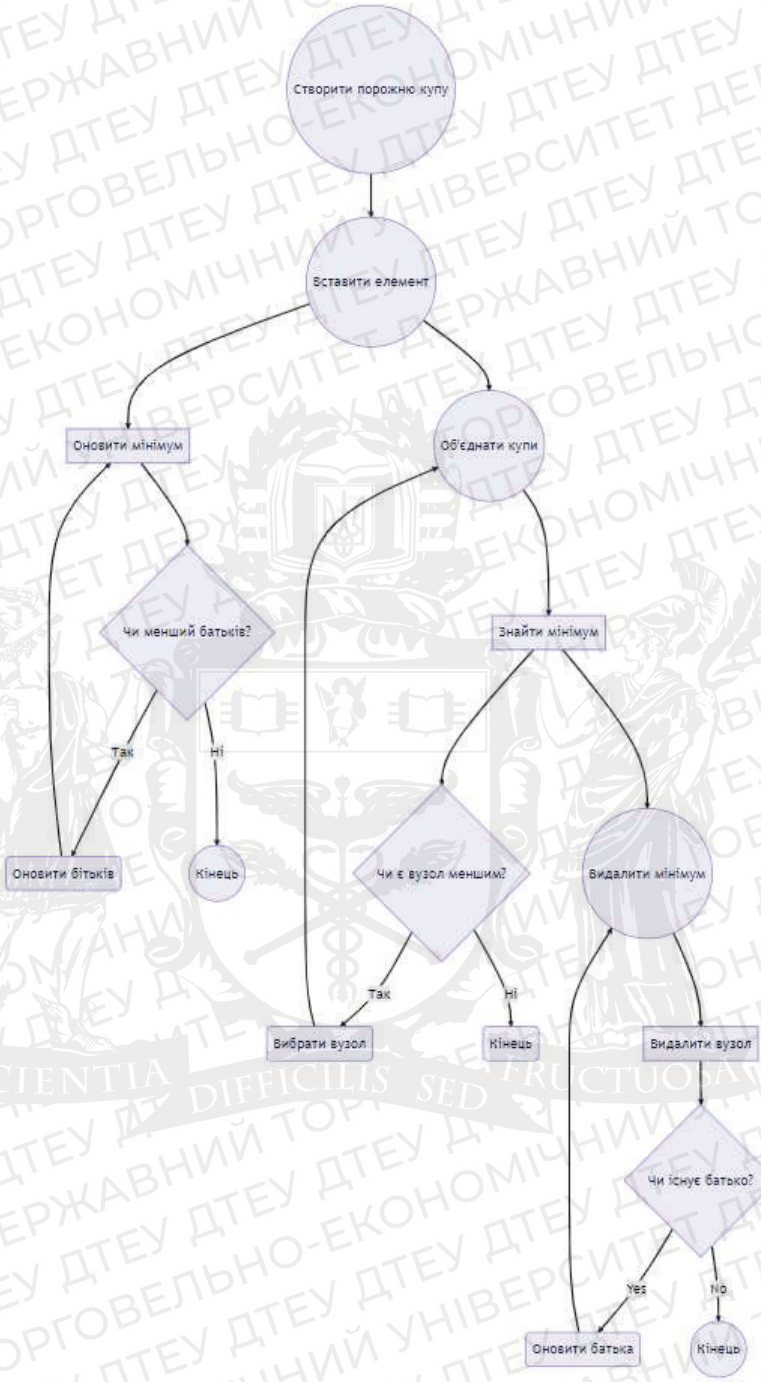


Рис. 1. Алгоритм роботи досліджуваних куп

Загалом, зв'язок між біноміальними кучами і графовими алгоритмами демонструє потужність і гнучкість цієї структури даних в контексті функціонального програмування. Розуміючи і використовуючи цей зв'язок, функціональні програмісти можуть скористатися унікальними властивостями біноміальних куп для ефективного розв'язання широкого спектру задач в теорії графів і не тільки.

Тож, біноміальні купи є корисною структурою даних для реалізації пріоритетних черг у функціональному середовищі програмування. Вони забезпечують ефективні операції і підтримують злиття двох куп, але також мають деякі недоліки, зокрема, збільшене використання пам'яті і повільнішу продуктивність під час операцій злиття. Формули для часової та просторової складності допомагають проаналізувати характеристики продуктивності біноміальних куп і зрозуміти їхню застосовність у різних контекстах.

Лівоцентровані купи – це модифікація стандартної двійкової структури даних купи, що використовується у функціональному програмуванні. У лівоцентрованій купі батьківський вузол завжди більший, ніж обидва його дочірні. Однак, на відміну від двійкової купи, лівий нащадок завжди є повним деревом, а правий нащадок завжди менший за лівий. Це означає, що лівий нащадок завжди є коренем піддерева, а правий нащадок завжди менший за свого батька.

Операції, які підтримуються лівоцентрованими кучами, включають вставку, пошук мінімуму, об'єднання, зменшення та видалення мінімуму. Щоб вставити елемент у купу, його додають як листовий вузол на останній рівень лівого піддерева, а потім відновлюють властивість купи, помінявши вузли місцями за необхідності. Операція пошуку мінімуму повертає елемент з мінімальним пріоритетом, не видаляючи його з купи. Операція злиття об'єднує дві купи, розташовані зліва по центру, в одну купу. Операція decrease-key використовується для зменшення пріоритету елемента, що вже знаходиться у купі. Нарешті, операція delete-minimum видаляє елемент з мінімальним пріоритетом з купи.

У функціональному середовищі лівоцентровані купи мають кілька переваг над бінарними купами. По-перше, вони забезпечують ефективні операції з логарифмічною часовою складністю для вставки, пошуку мінімуму та видалення мінімуму. По-друге, вони підтримують об'єднання двох куп з логарифмічною часовою складністю, але це може бути повільніше порівняно з двійковими кучами. По-третє, вони використовують менше пам'яті, ніж двійкові купи, завдяки своїй структурі.

Однак, лівоцентровані купи також мають деякі недоліки. Операція зменшення клавіші може вимагати перестановки вузлів, що може бути повільнішим порівняно з двійковими кучами. Крім того, властивість лівоцентрованості може ускладнювати виконання деяких операцій.

Характеристики продуктивності лівоцентрованих куп можна проаналізувати за допомогою математичних формул. Часова складність операції вставки становить $O(\log n)$, де n - розмір купи. Часова складність операції пошуку мінімуму становить $O(1)$, а операції видалення мінімуму - $O(\log n)$. Часова складність операції злиття становить $O(\log n)$, а просторова складність - $O(n)$.

Лівоцентровані купи також мають цікаві властивості, які відрізняють їх від інших структур даних пріоритетної черги. Однією з таких властивостей є те, що їх можна використовувати для ефективної підтримки ковзного вікна над послідовністю елементів. Зокрема, ліве піддерево лівоцентрованої купи можна використовувати для представлення поточного вікна, а праве піддерево - для представлення елементів, яких немає у поточному вікні. Ця властивість дозволяє ефективно оновлювати дані та виконувати запити у ковзних вікнах, що є поширеним явищем у багатьох програмах, таких як потокове передавання даних та аналіз часових рядів.

Ще однією цікавою властивістю лівоцентрованих куп є їх зв'язок з числами Фібоначчі. Зокрема, розмір лівого піддерева лівоцентрованої купи з n елементами дорівнює n-му числу Фібоначчі. Ця властивість демонструє зв'язок між лівоцентрованими кучами та послідовністю Фібоначчі, відомою математичною послідовністю з багатьма цікавими властивостями.

Ці властивості підкреслюють потенціал лівоцентрованих куп для використання у різноманітних додатках, окрім черг пріоритетів, зокрема, у ковзних вікнах та послідовностях, пов'язаних з послідовністю Фібоначчі. Загалом, лівоцентровані купи є цікавою структурою даних з унікальними властивостями, які роблять їх цінним доповненням до інструментарію функціональних програмістів.

Ще однією цікавою властивістю лівоцентрованих куп є їх зв'язок зі структурою даних парних куп. Парні купи - це ще один тип пріоритетних структур даних, які підтримують ефективні операції вставки та пошуку мінімуму. Вони засновані на рекурсивній структурі, де кожен вузол має список своїх дочірніх елементів, а мінімальний елемент зберігається в корені.

Лівоцентровані купи можна розглядати як спрощену версію парних куп, де ліве піддерево кожного вузла відповідає списку його дочірніх елементів. Цей зв'язок між лівоцентрованими кучами і парними кучами підкреслює потенціал використання лівоцентрованих куп як будівельного блоку для більш складних структур даних.

Крім того, лівоцентровані купи мають природну рекурсивну структуру, яку можна використовувати для ефективної реалізації рекурсивних алгоритмів. Наприклад, операція злиття двох лівоцентрованих куп може бути реалізована рекурсивно, при цьому менша купа об'єднується з більшою, роблячи її правим дочірнім елементом кореневого вузла. Ця рекурсивна структура також може бути використана для реалізації інших алгоритмів, які вимагають обходу та маніпулювання деревами, таких як обхід та обертання дерев.

Загалом, зв'язок між лівоцентрованими кучами і парними кучами, а також природна рекурсивна структура лівоцентрованих куп демонструють потенціал цих структур даних для використання у різноманітних додатках, окрім черг пріоритетів. Розуміючи і використовуючи ці зв'язки, функціональні програмісти можуть скористатися унікальними властивостями лівоцентрованих куп для ефективного вирішення широкого кола завдань.

Тож, лівоцентровані купи є корисною модифікацією двійкових куп для реалізації пріоритетних черг у функціональному середовищі програмування. Вони забезпечують ефективні операції і використовують менше пам'яті порівняно з бінарними кучами. Однак їхня властивість лівоцентрованості може ускладнювати деякі операції, а операція зменшення може бути повільнішою порівняно з двійковою купою. Формули для часової та просторової складності допомагають проаналізувати характеристики продуктивності лівоцентрованих куп і зрозуміти їхню застосовність у різних контекстах.

Висновки. Отже, у цій статті було досліджено тему структур даних у функціональному середовищі, зосередившись на двох специфічних модифікаціях куп: біноміальних купах та лівоцентрованих купах. Метою цієї роботи було проаналізувати переваги та недоліки цих структур даних, їхні характеристики продуктивності та застосовність у різних контекстах.

Біноміальні купи є добре відомою структурою даних для реалізації пріоритетних черг у функціональному середовищі. Вони забезпечують ефективні операції з логарифмічною часовою складністю для вставки, пошуку-мінімуму та видалення-мінімуму, підтримують об'єднання двох куп та мають гарантовану амортизовану постійну часову складність для операцій зі зменшенням ключа. Лівоцентровані купи - це модифікація двійкових куп, яка забезпечує ефективні операції з логарифмічною часовою складністю для операцій вставки, пошуку-мінімуму та видалення-мінімуму. Вони також використовують менше пам'яті порівняно з бінарними кучами завдяки своїй структурі.

Загалом, ця робота сприяла розумінню та проектуванню структур даних у функціональному середовищі, надаючи уявлення про переваги та недоліки біноміальних та лівоцентрованих куп.

Список використаних джерел

1. Кормен, Т. Х., Лейзерсон, К. Е., Рівест, Р. Л. та Штейн, К. (2009). Вступ до алгоритмів (3-тє вид.). MIT Press.
2. Окасакі, К. (1999). Чисто функціональні структури даних. Cambridge University Press.
3. Brodal, G. S., & Okasaki, C. (1996). Оптимальні чисто функціональні черги пріоритетів. Журнал функціонального програмування, 6(6), 839-857.
4. Sleator, D. D., & Tarjan, R. E. (1986). Самоналагоджувальні бінарні дерева пошуку. Журнал ACM, 32(3), 652-686.

Робота виконана під науковим керівництвом к.е.н., доцента
ТИЩЕНКА Д.О.

МОДЕЛЬ ЗАГРОЗ БЕЗПЕКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

НАГУЛЯК Л., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розроблено модель загроз безпеки конфіденційної інформації підприємства. Описано різні типи загроз, які можуть стати причиною витоку конфіденційної інформації, а також визначено методи, які можуть бути використані для їх виявлення та захисту від них.

The article develops a model of threats to the security of the company's confidential information. The different types of threats that can lead to the leakage of confidential information are described, and the methods that can be used to detect and protect against them are defined.

Актуальність. Питання створення та використання моделей загроз конфіденційної інформації підприємства є дуже актуальним у сучасному світі, де діджиталізація та розвиток інформаційних технологій призвели до збільшення кількості та різноманітності загроз для підприємств. Конфіденційна інформація є важливим активом для більшості підприємств, оскільки вона може включати в себе плани розвитку, стратегії маркетингу, фінансові відомості та інші персональні дані. Якщо ця інформація потрапляє в руки конкурентів або зловмисників, то це може призвести до значних фінансових збитків, втрати довіри та інших негативних наслідків. Тому, моделювання та аналіз загроз конфіденційної інформації є дуже важливим для захисту підприємств від потенційних кібератак та інших загроз, що можуть призвести до витоку конфіденційної інформації. Захист інформації є однією з найбільш важливих задач для керівництва будь-якого підприємства.

Метою статті є розробка моделі загроз безпеки інформації підприємства «IT громада».

Стаття включає опис різних заходів, які можуть бути прийняті підприємствами для захисту своєї конфіденційної інформації від потенційних загроз, таких як кібератаки, фізичний доступ до приміщень, втрати даних тощо. Вона визначає склад і джерела загроз, оцінку можливості їх прояву, шляхи їх здійснення, оцінку очікуваного збитку від реалізації загроз.

Об'єктом дослідження є конфіденційна інформація, якою підприємство володіє та обробляє.

Предмет дослідження – вивчення загроз, які можуть вплинути на конфіденційність інформації, та побудова моделі загроз безпеки конфіденційної інформації підприємства.

Аналіз попередніх досліджень. Дослідження моделі загроз безпеки конфіденційної інформації підприємства були проведені як вітчизняними, так і закордонними дослідниками: Борисенко О.І., Мельник І.А., Шевчук І.В., R. L. Popp, A. T. Sherman, C. M. Eloff, J. E. Labuschagne.

Ці дослідження дозволяють розглянути різні аспекти загроз безпеки конфіденційної інформації підприємства та пропонують різноманітні методи боротьби з цими загрозами. Найбільш ефективним є комплексний підхід до захисту інформації, який враховує різні аспекти безпеки та використовує різноманітні заходи для її захисту – комплексна система захисту інформації. Велику роль при цьому відіграє побудова моделі загроз безпеки інформації.

Виклад основного матеріалу.

Модель загроз безпеки конфіденційної інформації підприємства – це методика оцінки ризиків для конфіденційності, цілісності та доступності інформації та забезпечення інформаційної безпеки на основі ідентифікації та аналізу потенційних загроз. Розглянемо розробку моделі загроз конфіденційної інформації підприємства.

Модель загроз безпеки конфіденційної інформації підприємства «ІТ ГРОМАДА»

1. Загальні положення

1.1 Призначення документу

Модель загроз безпеки конфіденційної інформації (далі – ІзОД) підприємства (далі – Модель загроз) є офіційним керівним документом для керівного складу і співробітників, що обслуговують та експлуатують інформаційно-комунікаційну систему (далі – ІКС) підприємства «ІТ громада» (далі – Підприємства), і призначений для аналізу ризиків, визначення політики безпеки інформації та реалізації заходів захисту ІзОД.

1.2 Види ресурсів ІКС Підприємства

Інформаційно-комунікаційна система (ІКС) Підприємства включає в себе наступні ресурси:

- *Інформаційні ресурси:* дані та інформація, які зберігаються та обробляються в ІКС.
- *Апаратні ресурси:* фізичне обладнання, яке використовується для зберігання, обробки та передачі інформації.
- *Програмне забезпечення:* набір програм, що встановлюється на апаратне забезпечення, яке відповідає за обробку та передачу інформації.

1.3 Склад та вимоги до безпеки ресурсів ІКС Підприємства

Склад та вимоги до безпеки ресурсів ІКС Підприємства наведено в таблиці 1. Опис цих ресурсів формує розуміння того, що необхідно захищати на підприємстві, щоб не було витоку конфіденційної інформації.

Таблиця 1

Склад та вимоги до безпеки ресурсів ІКС Підприємства

№	Вид ресурсу	Назва ресурсу	Вимоги
1	Інформаційні ресурси	Загальнодоступна інформація. Контактна інформація, інформація про надання послуг та тарифи.	Цілісність, доступність
		Організаційно-правові документи Підприємства: установчий договір, статут, штатна чисельність, штатний розпис, посадові інструкції.	Цілісність, доступність, конфіденційність
		Конфіденційна інформація. Фінансові документи Підприємства: головна та касові книги, кошториси, баланси, рахунки, плани закупівель, плани робіт, бухгалтерські звіти. Інформація про клієнтів, постачальників.	Цілісність, доступність, конфіденційність
		Технологічна інформація: плани розміщення обладнання, формуляри на ЕОТ, склад встановленого програмне забезпечення, облікові записи, журнали подій, бази, архіви баз, атрибути доступу, облікові записи.	Цілісність, доступність, конфіденційність
		Персональні дані. Документи щодо особового складу Підприємства: особисті дані, адресні дані працівників, особові рахунки.	Цілісність, доступність, конфіденційність
2	Апаратні ресурси	Сервери баз даних	Цілісність, доступність
		Персональні електронно- обчислювальні машини	Цілісність, доступність
		Комутатори, модеми	Цілісність, доступність
		Дротові та бездротові мережі	Цілісність, доступність
		Службові з'ємні носії	Цілісність, доступність
		Носії ключової інформації	Цілісність, доступність
3	Програмне забезпечення	Операційна система	Цілісність, доступність
		Текстові редактори загального призначення	Цілісність, доступність
		Антивірусне програмне забезпечення	Цілісність, доступність
		ПЗ для бухгалтерії	Цілісність, доступність
		ПЗ для керуванням сайтом	Цілісність, доступність
		ПЗ для обробки баз даних	Цілісність, доступність

2. Загрози безпеці інформації, яка обробляється на підприємстві

Можливі загрози безпеці інформації зведено до таблиці 2. Перелік загроз наведено з передумовами виникнення і з вказівкою на який ресурс направлена загроза.

Таблиця 2

Перелік загроз безпеці інформації, яка обробляється на Підприємстві

№	Загроза	На що спрямовано	Передумови виникнення / джерело
1	Випадкові зміни умов зовнішнього середовища	Апаратні та інформаційні ресурси. Приміщення Підприємства	Стихійні лиха, аварії, землетрус, повінь, пожежа
2	Випадкові зміни внутрішнього середовища	Апаратні та інформаційні ресурси. Приміщення Підприємства	Руйнування будівельних конструкцій, аварії комунікацій, пожежа
3	Збої в роботі компонентів ІКС	Апаратні ресурси	Помилки під час проєктування і розробки компонентів, кібератаки та кіберзлочини, віруси та інші шкідливі програми
4	Помилки та зловживання персоналу	Апаратні та інформаційні ресурси	Порушення правил експлуатації обладнання та технічних засобів
5	Несанкціоноване отримання інформації	Інформаційні ресурси	Помилки та системні неузгодження під час проєктування, порушення правил експлуатації обладнання, розголошення, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми
6	Модифікація інформації	Інформаційні ресурси	Неправильне введення, впровадження програмної закладки, кібератаки та кіберзлочини, віруси та інші шкідливі програми
7	Порушення конфіденційності	Інформаційні ресурси	Недостатня безпека мережі, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми
8	Соціальний інжиніринг	Інформаційні та апаратні ресурси	Злам систем безпеки за допомогою маніпулювання людьми, що працюють на підприємстві
9	Інсайдерська загроза	Інформаційні ресурси	Небезпека від працівників підприємства, які мають доступ до конфіденційної інформації і можуть намагатися використовувати цю інформацію для своєї користі або в користь конкурентів
10	Перехоплення побічних електромагнітних випромінювань і наведень від пристроїв	Інформаційні та апаратні ресурси	Недостатня безпека мережі, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми
11	Несанкціонована зміна конфігурації	Апаратні ресурси	Недостатня безпека мережі, передача або втрата атрибутів розмежування доступу, кібератаки та кіберзлочини, віруси та інші шкідливі програми. Використання систем передачі, що знаходяться під управлінням інших операторів, і надання послуг користувачам, які не є співробітниками підприємства
12	Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення	Інформаційні та апаратні ресурси	Навмисне виведення з ладу елементів ІКС, порушення правил експлуатації обладнання

№	Загроза	На що спрямовано	Передумови виникнення / джерело
13	Порушення зв'язку за рахунок порушення каналу (тракту) передачі	Інформаційні та апаратні ресурси	Атаки на протоколи мережі, комунікаційні служби, нав'язування помилкової службової інформації і режимів роботи в системі управління, як окремих мереж, так і ІКС в цілому, включаючи зміну маршруту передачі інформації та ін.
14	Погіршення стану носіїв даних	Апаратні та інформаційні ресурси	Відсутність передбаченої процедури періодичної заміни
15	Розкрадання обладнання чи носіїв	Апаратні та інформаційні ресурси	Незахищене зберігання, безвідповідальне розміщення
16	Втрата програмних засобів	Програмні засоби	Відсутність резервних копій
17	Порушення функціонування програмного забезпечення	Програмні засоби	Відсутність механізмів контролю власної цілісності
18	Несанкціоноване копіювання програмного забезпечення	Програмні засоби	Неконтрольоване поводження з програмним забезпеченням
19	Використання контрафактного чи скопійованого програмного забезпечення	Програмні засоби та інформаційні ресурси	Неконтрольоване завантаження та використання програмних засобів
20	Обхід механізмів захисту	Інформаційні ресурси	Некомпетентність обслуговуючого персоналу, навмисні дії потенційних порушників

3. Способи нейтралізації загроз безпеки інформації

Способи нейтралізації загроз безпеки інформації, яка обробляється на Підприємстві зведено до таблиці 3.

В таблиці наведено організаційні, фізичні та технологічні засоби захисту, які необхідно виконати для нейтралізації загроз безпеки інформації.

Таблиця 3

Способи нейтралізації загроз безпеки інформації

Загроза	Заходи захисту		
	Організаційні	Фізичні	Технічні
Зміна програмного забезпечення для здійснення модифікації інформації	Визначення повноважень користувачів системи, прав доступу до ресурсів. Проведення навчання користувачів. Встановлення відповідальності. Проведення періодичних оглядів та аудитів.	Розмежування доступу до приміщення. Фізичний захист приміщень.	Завантаження операційної системи та програм з гнучких магнітних дисків. Використання цифрового підпису. Створення кожному користувачеві системи замкнутого середовища, де він може запускати лише певні програми, які дозволені адміністратором системи. Регулярний контроль цілісності виконуваних файлів та налаштувань програмних засобів. Реєстрація подій, здійснення аналізу журналів подій.
Впровадження програмної закладки	Визначення повноважень користувачів. Встановлення відповідальності. Надання інструкцій користувачам.	Розмежування доступу до приміщення. Фізичний захист приміщень.	Захист виконуваних і системних файлів від зміни. Створення кожному користувачеві системи замкнутого середовища, де він може запускати лише певні програми, які дозволені адміністратором системи. Контроль цілісності системи. Використання засобів виявлення нападів.

Загроза	Заходи захисту		
	Організаційні	Фізичні	Технічні
Перехоплення	Надання інструкцій користувачам, проведення навчання. Укладання договорів із зовнішніми організаціями.	Розмежування доступу в приміщенні. Фізичний захист приміщень.	Забезпечення безпеки під час пересування конфіденційної інформації між різними відділами підприємства, а також під час її транспортування до зовнішніх контрагентів. Відправлення даних повинно бути зашифровано і захищено від несанкціонованого доступу. Використання паролів. Використання КЕП. Контроль часу.
Несанкціоно-ване копіювання	Встановлення відповідальності. Інструкції користувачам.	Розмежування доступу в приміщенні. Фізичний захист приміщень.	Реєстрація подій Використання засобів виявлення нападів. Створення облікових записів для кожного користувача з відповідними правами доступу. Використання засобів виявлення вторгнення. Реєстрація подій. Використання КЕП.
Дублювання	Інструкції користувачам. Встановлення відповідальності за порушення правил.	Ізоляція системи, що захищається, від інших систем	Використання КЕП. Контроль часу. Реєстрація подій.
Несанкціоно-ваний доступ до РС	Встановлення відповідальності за порушення правил. Обмеження людей, що мають право конфігурувати ІКС.	Фізичний захист приміщень. Розмежування доступу в приміщення.	Обмеження, розмежування доступу Реєстрація подій. Зміна стандартного імені адміністратора системи захисту. Дозвіл роботи в мережі тільки одного адміністратора. Використання засобів виявлення атак.
Несанкціонова ний доступ до каналу передачі даних	Інструкції користувачам. Встановлення відповідальності за порушення правил.	Захист кабельної системи.	За рамками повноважень.
Напад із зовнішньої мережі	Інструкції користувачам. Встановлення відповідальності за порушення правил	Ізоляція системи, що захищається, від інших систем.	Обмеження числа модемів, що використовуються. Фізична ізоляція робочих станцій для доступу в глобальні мережі від робочих станцій системи. Обмеження доступу до робочих станцій. Реєстрація подій. Використання засобів виявлення нападів. Використання всіх вбудованих в систему засобів захисту.
Несанкціоно-вана зміна конфігурації	Інструкції користувачам. Встановлення відповідальності за порушення правил.	Розмежування доступу в приміщеннях. Фізичний захист приміщень.	Обмеження числа модемів, що використовуються. Фізична ізоляція робочих станцій для доступу в глобальні мережі від робочих станцій системи. Обмеження доступу до робочих станцій. Реєстрація подій. Використання засобів виявлення нападів. Використання всіх вбудованих в систему засобів захисту.

4. Оцінка передбачуваного збитку у разі реалізації загроз

Ціна втрат інформації може бути визначена шляхом експертної оцінки, в якій розглядаються такі фактори, як рівень конфіденційності інформації, сфера використання інформації, можливості її використання для виробництва прибутку, репутаційні витрати та інші фактори. При оцінці збитку розглядаються різні комбінації еквівалентів втрат інформації. Вартість збитків залежить від ефективності її використання порушником, а також від сфери використання інформації – політичної, економічної та ін.

5. Оцінка ризиків

Оцінка ризиків здійснюється на основі вимог ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки» та інших нормативних документів з оцінки ризиків.

Ризики оцінюються за такою формулою:

*РИЗИК = ВРАЗЛИВІСТЬ * НАСЛІДКИ РЕАЛІЗАЦІЇ ЗАГРОЗ*

ВРАЗЛИВІСТЬ = ЗАГРОЗА / (ЗАХОДИ НЕЙТРАЛІЗАЦІЇ ЗАГРОЗИ + АКТИВ),

де: «загроза» має значення 0 за її відсутності, 1 при низькій ймовірності або 2 за її наявності; «заходи нейтралізації загрози» мають значення 0 за відсутності гарантій щодо їх ефективної протидії реалізації загроз щодо певного активу або 2, якщо вони здатні ефективно протидіяти реалізації загроз щодо певного активу; «актив» має значення 1; «/» є математичною операцією ділення; «+» є математичною операцією додавання; «наслідки реалізації загроз» мають значення від 1 до 5 (Значення 1 приймається, коли немає наслідків для діяльності. Значення 5 приймається, коли є критичні наслідки, які можуть призвести до припинення діяльності); «*» є математичною операцією множення. Ризики, які приймають значення більше/рівно 4, вважаються неприйнятними та потребують обов'язкового вжиття заходів щодо їх нейтралізації [1].

Для розрахунку ризиків введемо наступні позначення. Активи Підприємства: А01 – апаратне забезпечення; А02 – програмне забезпечення; А03 – USB та захищені носії інформації, які використовуються в системі; А04 – мережева інфраструктура; А05 – приміщення; А06 – працівники Підприємства; А07 – ділова репутація; А08 – клієнтська база; А09 – журнали аудиту; А10 – архіви (паперові та на носіях).

Джерелом списку загроз візьмемо IT-Grundschutz Catalogues (скорочений варіант каталогу) [2]. Кожній загрозі надано умовне позначення: З01 – пожежа; З02 – несприятливі кліматичні умови; З03 – вода; З04 – забруднення, пил, корозія; З05 – стихійні лиха; З06 – екологічні катастрофи; З07 – важливі події в навколишньому середовищі; З08 – відсутність або збій електропостачання; З09 – відмова або збій мереж зв'язку; З10 – відмова або збій в роботі мережі живлення; З11 – відмова або збій в роботі постачальників послуг; З12 – перешкоджаюче випромінювання; З13 – витік каналами побічних електромагнітних випромінювань і наведень (ПЕМВН); З14 – перехоплення інформації / Шпигунство; З15 – підслуховування.

Оцінка ймовірності впливу загроз на активи наведено в таблиці 4.

Таблиця 4

Вплив загроз на активи

	А01	А02	А03	А04	А05	А06	А07	А08	А09	А10
З01	2	0	1	1	1	1	0	0	2	1
З02	2	0	1	1	0	0	0	0	2	1
З03	1	0	0	0	0	0	0	0	0	1
З04	1	0	1	0	0	0	0	0	0	2
З05	1	0	0	0	1	1	0	0	0	1
З06	1	0	0	0	1	1	0	0	0	1
З07	0	0	0	0	1	1	0	0	0	0
З08	1	0	0	0	0	0	0	0	0	0

309	0	0	0	0	0	0	1	1	0	0
310	1	0	0	0	0	0	1	1	0	0
311	0	0	0	0	1	0	1	1	0	0
312	1	0	1	1	0	0	0	0	0	0
313	1	0	0	1	0	0	1	1	1	0
314	0	0	0	0	0	0	1	1	1	1
315	0	0	0	0	0	0	1	1	0	0

Для кожної загрози проводимо аналіз та визначаємо наслідки впливу загроз за шкалою від 1 балу за відсутності впливу до 5 балів за наявністю максимального впливу загрози. Результати зводимо до таблиці 5.

Таблиця 5

Наслідки впливу загроз на активи

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
301	4	1	4	4	4	3	1	1	4	4
302	4	1	2	3	1	1	1	1	3	3
303	5	1	1	1	1	1	1	1	1	4
304	4	1	2	1	1	1	1	1	1	3
305	4	1	1	1	4	5	1	1	1	4
306	3	1	1	1	4	4	1	1	1	3
307	1	1	1	1	4	4	1	1	1	1
308	4	1	1	1	1	1	1	1	1	3
309	1	1	1	1	1	1	4	4	1	1
310	4	1	1	1	1	1	4	4	1	3
311	1	1	1	1	3	1	4	4	1	1
312	4	1	3	4	1	1	1	1	4	1
313	4	1	1	4	1	1	4	4	4	1
314	1	1	1	1	1	1	4	4	1	1
315	1	1	1	1	1	1	4	4	1	1

Також для кожної загрози визначаємо ефективність протидії реалізації загроз. Величина ефективності протидії реалізації загроз має значення 0 за відсутності гарантій щодо їх ефективної протидії реалізації загроз щодо певного активу або 2, якщо вони здатні ефективно протидіяти реалізації загроз щодо певного активу. Результати ефективності протидії загроз внесені до таблиці 6.

Таблиця 6

Ефективність протидії загроз

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
301	2	0	2	2	2	2	0	0	2	2
302	2	0	0	0	0	2	0	0	2	0
303	0	0	0	0	0	0	0	0	0	0
304	2	0	0	0	2	0	0	0	0	2
305	0	0	0	0	0	0	0	0	0	0
306	0	0	0	0	0	0	0	0	0	0
307	0	0	0	0	0	0	0	0	0	0
308	2	0	0	0	0	0	0	0	0	0
309	0	0	0	0	0	0	2	0	0	0
310	0	0	0	0	0	0	0	0	0	0
311	0	0	0	0	0	0	2	2	0	0
312	2	0	0	2	0	0	0	0	0	0
313	2	0	0	0	0	0	0	0	2	0
314	0	0	0	0	0	0	2	2	2	2
315	0	0	0	0	0	0	2	2	2	0

Використовуючи формули, наведені вище, здійснюємо оцінку ризиків. Результати зводимо в таблиці 7. Процедури оцінки ризиків повинні містити заходи з визначення активів, загроз, вразливостей, ймовірності реалізації загроз та оцінки їх наслідків, заходи з нейтралізації. Значення ризиків є відносною величиною, яка дозволяє оцінювати їх вплив на діяльність Підприємства.

Ризики, які приймають значення більше/рівно 4, вважаються неприйнятними та потребують обов'язкового вжиття заходів щодо їх нейтралізації.

Таблиця 7

Оцінка ризиків

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10
301	3	0	1	1	1	1	0	0	3	1
302	3	0	2	3	0	0	0	0	2	3
303	**5**	0	0	0	0	0	0	0	0	**4**
304	1	0	2	0	0	0	0	0	0	2
305	**4**	0	0	0	**4**	**5**	0	0	0	**4**

306	3	0	0	0	**4**	**4**	0	0	0	3
307	0	0	0	0	**4**	**4**	0	0	0	0
308	1	0	0	0	0	0	0	0	0	0
309	0	0	0	0	0	0	1	**4**	0	0
310	**4**	0	0	0	0	0	**4**	**4**	0	0
311	0	0	0	0	3	0	1	1	0	0
312	1	0	3	1	0	0	0	0	0	0
313	1	0	0	**4**	0	0	**4**	**4**	1	0
314	0	0	0	0	0	0	1	1	0	0
315	0	0	0	0	0	0	1	1	0	0

У Підприємства наявна можливість реалізації загроз конфіденційності, цілісності і доступності інформації шляхом несанкціонованого доступу, тому необхідно дотримуватися вимог політики безпеки інформації. Рекомендується також використовувати апаратно-програмні засоби криптографічного захисту інформації: електронні ключі, IP-шифратори, шлюзи захисту [3].

Модель підлягає перегляду при зміні планів розміщення, умов функціонування і характеристик Підприємства.

Висновки. Модель загроз безпеки конфіденційної інформації підприємства є важливим інструментом для підвищення рівня безпеки інформації та захисту від небажаних вторгнень та атак на корпоративні мережі та інформаційні системи. Оцінка загроз безпеки повинна проводитися періодично для виявлення нових загроз, що можуть виникнути, та оновлення оцінки існуючих загроз. Результати оцінки можуть допомогти організації приймати рішення щодо запобігання потенційним атакам, забезпечення безпеки даних та захисту інформаційної системи в цілому.

Список використаних джерел

1. Наказ від 14.05.2020 №269 Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації».
2. IT-Grundschutz catalogues. – URL: https://www.scribd.com/document/534182501/IT-Grundschutz-catalogues-15th-version-2015-Draft.
3. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. – Харків: Видавництво «Форт», 2012. – 880 с.

Робота виконана під науковим керівництвом к.т.н., доцента
САВЧЕНКО Т.В.

ДОСЛІДЖЕННЯ МЕТОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РИЗИКИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

НЕЧАЄВ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи інформаційної безпеки та ризики несанкціонованого доступу. Сформульована мета дослідження, якою є аналіз основ інформаційної безпеки та ризиків несанкціонованого доступу. Основні засади інформаційної безпеки: викладення ключових принципів та методів, які допомагають забезпечити безпеку цифрових ресурсів, включаючи сильні паролі, шифрування даних, багаторівневу аутентифікацію. Загрози та ризики несанкціонованого доступу: Аналіз типів загроз, з якими стикаються користувачі та організації, такі як фішинг, віруси, хакінг, соціальний інжиніринг. Стратегії та заходи захисту: Вказані рекомендації та практики, які допомагають уникнути ризиків несанкціонованого доступу та забезпечують ефективний захист цифрових активів. Інновації та майбутні виклики: Вказані перспективи розвитку галузі інформаційної безпеки, такі як використання штучного інтелекту, квантової криптографії, захист Інтернету речей та інші інноваційні підходи, а також підкреслено майбутні виклики, пов'язані із забезпеченням кібербезпеки.

The article discusses methods of information security and risks of unauthorized access. The purpose of the research is formulated, which is the analysis of the basics of information security and the risks of unauthorized access. Fundamentals of information security: laying out the key principles and methods that help ensure the security of digital resources, including strong passwords, data encryption, multi-level authentication. Threats and risks of unauthorized access: Analysis of the types of threats that users and organizations face, such as phishing, viruses, hacking, social engineering. Protection strategies and measures: Recommendations and practices are provided to help avoid the risks of unauthorized access and ensure effective protection of digital assets. Innovations and future challenges: Prospects for the development of the field of information security are indicated, such as the use of artificial intelligence, quantum cryptography, protection of the Internet of Things and other innovative approaches, and future challenges related to ensuring cyber security are highlighted.

Актуальність. У сучасному цифровому віці, коли технології залишаються невід'ємною частиною нашого життя, питання інформаційної безпеки виходять на передній план. Швидкий розвиток цифрових засобів спілкування, обміну даними та зберігання інформації до зростання загрози несанкціонованого доступу до конфіденційної та особистої інформації. Актуальність цієї теми обумовлена не лише розширенням можливостей для зловмисників, але й прагненням захистити індивідуальні, корпоративні та державні інтереси в онлайн-середовищі. Однією з найбільших загроз сучасності є несанкціонований доступ до цифрової інформації. Хакерські атаки, фішингові кампанії, крадіжка особистих даних - це лише деякі зі відомих методів атаки, які можуть призвести до серйозних наслідків. Зловмисники можуть отримати доступ до фінансових ресурсів, конфіденційних корпоративних документів, медичних записів чи особистих повідомлень. Порушення конфіденційності та розширення недозволених даних може завдати шкоди як окремим користувачам, так і суспільству в цілому. Зростання кількості пристроїв входу, підключених до Інтернет-речей (IoT), створює нові точки для зловмисників. Від вбудованих систем у побутовій техніці до промислових контролерів, усі вони можуть стати об'єктами атак. Розробка нових методів захисту та забезпечення безпеки IoT-пристроїв стає завданням для дослідників та інженерів. Ризики несанкціонованого доступу також впливають на державну безпеку. Кібершпигунство та кібератаки можуть бути спрямовані

проти критичної інфраструктури, електронних систем голосування, військових систем та інших стратегічно важливих об'єктів. Наслідки таких атак можуть бути драматичними і мають потенціал спровокувати глобальну кризу. Отже, актуальність теми «Інформаційна безпека та ризики несанкціонованого доступу» є безаперечною. Зростання кількості цифрових загроз вимагає постійного вдосконалення стратегій захисту, розробки нових технологій та навчання користувачів основам цифрової безпеки. Тільки шляхом спільних зусиль науковців, інженерів та користувачів можна надійно захистити цифровий світ від загроз несанкціонованого доступу.

Метою статті є висвітлення основ інформаційної безпеки та ризиків несанкціонованого доступу в цифровому середовищі. Основний акцент робиться на аналізі загроз, які виявляються у зв'язку з несанкціонованим доступом до інформації, та розгляді стратегій, спрямованих на їх запобігання та управління. Дана стаття має наступні конкретні мети: Визначте поняття інформаційної безпеки: Стаття пояснює, що така інформаційна безпека та чому вона є важливою для окремих користувачів, організацій та держав; Висвітлити загрози несанкціонованого доступу: Стаття аналізує різноманітні методи та техніку, які створюють зловмисники для отримання несанкціонованого доступу до інформації. Вона розглядає різні типи атак, включаючи хакінг, риболовлю, соціальний інжиніринг; Виявити слідки та ризики: Стаття розглядає можливість слідки несанкціонованого доступу для осіб, організацій та суспільства загалом. Вона досліджує можливості наслідків порушення конфіденційності, цільності та доступності інформації; Пропонувати стратегії запобігання ризикам: Стаття надає конкретні поради та стратегії, які можуть допомогти індивідам і організаціям зменшити ризики несанкціонованого доступу. Це включає в себе використання сильних паролів, багаторівневу аутентифікацію, оновлення програмного забезпечення та інші заходи; Підкреслити важливість освіти та свідомості: Стаття акцентує увагу на необхідності навчання користувачів основам інформаційної безпеки, розпізнавання загроз та вчасного реагування на них; Визначити шлях подолання викликів: Стаття вказує на важливість співпраці між науковцями, інженерами, законодавцями та користувачами для розробки та впровадження ефективних стратегій інформаційної безпеки; В цілому, стаття має на меті поглибити розуміння читачів про важливість інформаційної безпеки, небезпеки, які пов'язані з несанкціонованим доступом, а також способи їх мінімізації та подолання.

Об'єктом дослідження є комплексний спектр цифрових ресурсів, даних, інформаційних систем, мереж та технологій, які є вразливими перед різними загрозами та можуть стати об'єктом атак несанкціонованого доступу.

Предмет дослідження – інформаційна безпека та ризики несанкціонованого доступу в контексті сучасного цифрового середовища.

Аналіз попередніх досліджень. Інформаційної безпеки та ризиків несанкціонованого доступу є місцем для побудови наукової статті. Цей аналіз допомагає використовувати поточний стан знань у цій області, ідентифікувати невирішені аспекти та потреби програми в нових дослідженнях. Огляд літератури; Ключові концепції та теорії; Сфери застосування; Технічні аспекти; Соціальні та психологічні аспекти; Уразливості та вразливі групи; Дієвість заходів безпеки.

Виклад основного матеріалу. Інформаційна безпека – це комплекс заходів та практичних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Конфіденційність виникає у забезпеченні обмеженого доступу до інформації, цілеспрямованість – у запобіганні недозволеним змінам даних, а доступність – у забезпеченні доступу до інформації для авторизованих користувачів. Основи інформаційної безпеки включають принципи, методи та практики, спрямовані на забезпечення захисту конфіденційності, цілісності та доступності інформації в цифровому середовищі. Це важлива галузь, яка має на меті запобігання несанкціонованому доступу, втраті даних та іншим загрозам, які можуть виникнути в результаті використання інформаційних технологій. Основні аспекти інформаційної безпеки включають:

1. Конфіденційність: Цей принцип передбачає забезпечення та збереження конфіденційності інформації. Інформація повинна бути доступна тільки тим особам або суб'єктам, які мають право на її перегляд. Криптографія, контроль доступу та обмеження прав користувачів - це інструменти, які допомагають забезпечити конфіденційність.

2. Цілісність: Цей аспект означає збереження точності та цільності інформації. Дані не повинні бути незаконно змінені, підроблені або втрачені. Для досягнення цільності використовують методи контролю цільності даних та застосування цифрових підписів.

3. Доступність: Принцип доступності, що інформація має бути доступною для авторизованих користувачів у відповідний момент часу. Забезпечення доступності може включати в себе використання резервних копій, механізмів відновлення після збоїв та інші практики.

4. Аутентифікація та авторизація: Аутентифікація при ідентифікації користувача або суб'єкта, щоб забезпечити пізнаваність та перевірку його запису. Авторизація забезпечує рівень доступу, який має користувач після успішної аутентифікації.

5. Захист від загроз: цей аспект включає в себе застосування технічних, організаційних та процедурних заходів для запобігання загрозам, таким як хакінг, віруси, рибальство та інші атаки.

6. Аудит та моніторинг: Системи інформаційної безпеки повинні бути постійно та моніторингу для контролю виявлення аномалій, інцидентів та порушення безпеки. Аудит відстежувати дії користувачів та виявляти незвичну активність.

7. Навчання та свідомість: Освіта користувачів щодо загроз і практичної інформаційної безпеки є ключовою для забезпечення безпеки. Люди повинні розуміти основні ризики та вміти уникати пасток. Ці основи інформаційної безпеки є ключовими для забезпечення надійного захисту інформації в сучасному цифровому світі. Вони допомагають окремим користувачам, бізнесам та організаціям виявляти та запобігати потенційним загрозам та забезпечувати безпеку даних.

Загрози та ризики несанкціонованого доступу: загрози несанкціонованого доступу створює негативні ризики для окремих осіб та організацій. Хакери можуть використовувати техніку хакінгу для проникнення в системи та крадіжки даних. Фішингові атаки включають маніпулювання користувачами з метою отримання їхньої конфіденційної інформації. Соціальний інжиніринг використовує психологічні методи для отримання доступу до системи. Загрози та ризики несанкціонованого доступу є серйозними проблемами для інформаційної безпеки в сучасному цифровому світі. Ці загрози можуть створюватися індивідуальних користувачів, бізнесів, державних структур і суспільства в цілому. Деякі з ключових загроз та ризиків несанкціонованого доступу включають:

1. Хакінг та Кібератаки: Зловмисники можуть використовувати різні методи хакінгу для незаконного доступу до комп'ютерних систем та мереж. Це може включати в себе використання вразливостей програмного забезпечення, включення в систему та вироблення даних.

2. Фішинг: Фішингові атаки передають використання підступних електронних повідомлень або веб-сайтів для отримання конфіденційної інформації, такої як паролі або фінансові дані, від користувачів.

3. Соціальний інжиніринг: Зловмисники можуть використовувати психологічні методи для впливу на людей і отримання доступу до конфіденційної інформації. Це може включати в себе маніпулювання, обман та використання довіри.

4. Викрадання облікових даних: Зловмисники можуть викрасити облікові дані користувачів, такі як ім’я користувачів та паролі, для незаконного доступу до різних облікових записів.

5. Віруси та шкідливий код: Зловмисники можуть розробляти та поширювати віруси, черв'яки та інший шкідливий код, який може пошкодити системи, викрасити дані або навіть знищити інформацію.

6. Внутрішні загрози: Інсайдери, такі як співробітники, можуть завдати шкоди, розкривши конфіденційну інформацію або зловживаючи доступом до системи.

7. Викрадання даних та вимагання викупу: Зловмисники можуть викрадати важливі дані та вимагати викуп для їх повернення або невикладення публічно.

8. Порушення конфіденційності: несанкціонований доступ може привести до витоку конфіденційної інформації, такої як медичні дані, фінансові дані або персональні відомості.

9. Втрати фінансових ресурсів: Зловмісники можуть використовувати незаконний доступ для крадіжки грошей або викрадання фінансової інформації.

10. Загрози для критичної інфраструктури: Атаки на критичну інфраструктуру, так само як енергетичні мережі, можуть викликати серйозні наслідки для суспільства та безпеки.

Ці загрози та ризики підлягають постійному моніторингу, оновлення заходів безпеки та освіти користувачів щодо яких загроз і способів їх запобігання.

Наслідки несанкціонованого доступу: Несанкціонований доступ може призвести до серйозних наслідків. Крадіжка конфіденційних даних може призвести до фінансових втрат для бізнесменів і особистих користувачів. Порушення конфіденційності може вразити репутацію організацій та осіб. Внесення змін у цільність даних може призвести до недостовірних інформаційних потоків. Несанкціонований доступ до інформації може привести до серйозних наслідків для окремих користувачів, бізнесів, установ і суспільства в цілому. Ці слідки можуть мати фінансовий, репутаційний, юридичний та етичний вплив. Деякі з основних наслідків несанкціонованого доступу включають:

1. Фінансові втрати: Зловмисники можуть використовувати незаконний доступ для крадіжки грошей, фінансової інформації або використання фінансових ресурсів.

2. Крадіжка особистої інформації: Несанкціонований доступ може призвести до крадіжки особистої інформації, такої як імена, адреси, номери соціального страхування, медичні записи тощо. Ця інформація може бути використана для шахрайства або ідентифікаційної крадіжки.

3. Порушення конфіденційності: несанкціонований доступ може призвести до витоку конфіденційної інформації, такої як комерційні та технічні дані. Це може вразити репутацію організації та осіб.

4. Втрата даних: Зловмисники можуть спричинити втрату даних або їх видалення, що може мати серйозний вплив на роботу бізнесу, наукових досліджень або особисті дані.

5. Розширення дезінформації: Несанкціонований доступ може призвести до внесення змін в інформацію та її поширення, що може призвести до розширення дезінформації та неправильної інтерпретації фактів.

6. Втрата контролю над системами: Незаконний доступ може призвести до втрати контролю над комп'ютерними системами, мережами та пристроями, які можуть відкрити двері для подальших атак та вікрадення даних.

7. Юридичні наслідки: несанкціонований доступ може призвести до юридичних наслідків, у тому числі судових позовів, штрафів та кримінального переслідування.

8. Завдання шкоди репутації: У випадках втрати конфіденційності інформації або вразливості в безпеці, репутація фізичних осіб, бізнесів або організацій може бути важко пошкоджена.

Стратегії та заходи захисту: Для запобігання ризикам несанкціонованого доступу індивіди та організації можуть використовувати різні стратегії. Важливим кроком є використання сильних паролів та багаторівневої аутентифікації. Регулярне оновлення програмного забезпечення та встановлення патчів є кількістю для зменшення вразливостей. Криптографічний захист даних може забезпечити їх безпеку під час передачі. Для запобігання загрозам та ризикам несанкціонованого доступу індивіди та організації можуть використовувати різні стратегії та заходи захисту. Нижче наведено деякі ключові стратегії та практики, які можуть допомогти забезпечити безпеку інформації:

1. Сильні паролі та багаторівнева аутентифікація: Використовуйте складні паролі, які складаються з комбінації великих та маленьких літер, цифр та спецсимволів. Додатково використовуйте багаторівневий аутентифікатор, який вимагає двох або більше способів перевірки особи.

2. Оновлення програмного забезпечення: Регулярно оновлюйте операційні системи, програми та програмне забезпечення, щоб виправити вразливість та захистити системи від атак.

3. Використання антивірусного програмного забезпечення: Встановіть та оновіть антивірусне програмне забезпечення для виявлення та блокування шкідливого коду.

4. Файрволі: Встановіть файрволі для моніторингу та контролю мережевого трафіку, що входить і виходить із вашої мережі.

5. Шифрування даних: використовуйте шифрування для захисту конфіденційної інформації під час її передачі через мережу або збереження на пристроях.

6. Резервне копіювання: Регулярно створюйте резервні копії важливої інформації, щоб уникнути її втрати в разі атаки або випадкового видалення.

7. Обмеження доступу: Надавайте доступ до інформації лише авторизованим користувачам та обмежуйте їх права відповідно до їх ролі та обов'язків.

8. Освіта та навчання користувачів: Проведіть навчальні програми та інформуйте користувачів про наявні загрози та способи їх запобігання, вчіть їх розпізнавати сприйнятливу ситуацію.

9. Моніторинг та аудит: Встановіть системи моніторингу для виявлення аномалій та незвичайної активності, а також зберігайте перевірені дані про дії користувачів.

10. Фізична безпека: Захищайте фізичний доступ до комп'ютерів, серверів та інших пристроїв, встановлюючи фізичні бар'єри та обмежуючи доступ до приміщень.

Ці стратегії та заходи захисту взаємодіють із єдиною, допомагаючи створити комплексний підхід до інформаційної безпеки та мінімізувати ризики несанкціонованого доступу. Освіта та навчання: Важливою складовою інформаційної безпеки є освіта користувачів. Індивіди повинні бути освіченими щодо методів фішингу, соціального інжинірингу та інших загроз. Організації можуть проводити навчальні програми для співробітників та давати рекомендації щодо безпеки. Освіта та навчання грають критичну роль у забезпеченні інформаційної безпеки та запобіганні ризикам несанкціонованого доступу. Свідомість користувачів щодо наявних загроз та навичок розпізнавання також є великими факторами у забезпеченні безпеки інформації. Ось деякі аспекти освіти та навчання в контексті інформаційної безпеки:

1. Відомість про загрози: Освіта повинна розкрити користувачам різні типи загроз, такі як фішинг, соціальний інжиніринг, віруси, хакінг тощо. Пояснити їхню сутність, можливість наслідки та шляхи запобігання.

2. Безпечне користування мережею: Навчання користувачів правилам безпечного користування Інтернетом та мережевими сервісами. Це може включати в себе використання безпечних паролів, обережне завантаження файлів, обмеження особистої інформації в мережі тощо.

3. Соціальний інжиніринг: Навчання користувачів розпізнавати типові сценарії соціального інжинірингу, які використовують зловмисники для отримання конфіденційної інформації або доступу.

4. Навички розпізнавання фішингу: Користувачі повинні помічати розпізнавати підозрілі електронні повідомлення та веб-сайти, які можуть бути фішинговими атаками.

5. Правила використання паролів: Навчання користувачів про створення сильних паролів, регулярну їх зміну та неповторне використання паролів для різних облікових записів.

6. Впровадження багаторівневої аутентифікації: Пояснення переваг використання багаторівневої аутентифікації та навчання користувачів її на аналізі.

7. Публікація основних принципів інформаційної безпеки: Розробка та розповсюдження матеріалів, які пояснюють основні принципи інформаційної безпеки та надають поради щодо безпеки в мережі.

8. Симуляція атаки: організація симуляційної атаки для користувачів, щоб показати, як швидко можна стати жертвою атаки, якщо не дотримуватися правил безпеки.

9. Тренінг безпеки для персоналу: Для бізнесу та організацій важливо проводити навчання з питань безпеки для свого персоналу, включаючи особливі навички та процедури для конкретної діяльності.

10. Створення культури безпеки: Залучення всього колективу до усвідомлення важливості інформаційної безпеки та сприяння виробленню культури безпеки в організації або спільноті.

Навчання та освіта є постійним процесом, після загрози та технологічний контекст змінюється. Ціль - підготувати користувачів до ефективного реагування на нові виклики та впровадження найкращих практичних заходів безпеки в їх повсюдну діяльність. Інновації та майбутні виклики: З розвитком технологій з'являються нові можливості та виклики в галузі інформаційної безпеки. Використання штучного інтелекту та машинного навчання може сприяти виявленню аномалій та атак. Однак разом з цим викликаються нові загрози, такі як використання штучного інтелекту зловмисниками. Інновації в галузі інформаційної безпеки важливі для адаптації до зростаючих загроз та викликів у цифровому світі. Ось деякі інноваційні тенденції та майбутні виклики, з якими може стикнутися галузь інформаційної безпеки:

1. Штучний інтелект та машинне навчання: використання штучного інтелекту та машинного навчання допоможе автоматично виявити та протидіяти загрозам, а також швидко проаналізувати великий обсяг даних для незвичайної активності.

2. Кібербезпекові аналітичні інструменти: Розробка більш ефективних аналітичних інструментів допоможе передбачати, виявляти та аналізувати нові типи загроз та атак.

3. Квантова криптографія: Розвиток квантової криптографії може забезпечити більшу стійкість до квантових обчислювальних атак та забезпечити безпеку даних у майбутньому.

4. Блокчейн для кібербезпеки: технологія блокчейн може бути використана для забезпечення безпеки транзакцій, ідентифікації та контролю доступу до даних.

5. Захист Інтернету речей (IoT): З ростом кількості підключених до Інтернету пристроїв стає все розробити ефективні методи захисту IoT-пристроїв від атак.

6. Боротьба зі зловмисниками на державному рівні: Зростає важливість співпраці між державами та міжнародними організаціями для виявлення та протидії кібератакам, які можуть порушити роботу країни та глобальної інфраструктури.

7. Гібридні загрози: Зловмисники залишаються більш витонченими та планують гібридні атаки, використовуючи різні канали та методи для досягнення своїх цілей.

8. Підготовка та навчання: Персоналу та користувачам слід надавати постійну підготовку та навчання, після чого загрози змінюються та еволюціонують.

9. Конфіденційність даних: Зростає усвідомлення важливості конфіденційності даних, тому заходи захисту та шифрування залишаються ще актуальнішими.

10. Етичні аспекти інформаційної безпеки: З'являється більше обговорень щодо етики використання інформаційної безпеки, зокрема в галузі збору та обробки персональних даних. Ці інновації та виклики вказують на постійну необхідність розвитку та вдосконалення стратегій інформаційної безпеки, а також на важливість співпраці та обміну досвідом між організаціями та державами для ефективного захисту від сучасних та майбутніх загроз.

Висновки. даної наукової статті підкреслюють критичну важливість інформаційної безпеки та ризиків несанкціонованого доступу в сучасному цифровому світі. Розглянуті аспекти підкреслюють надання постійного зосередження на цю проблему для забезпечення безпеки та конфіденційності інформації. Основні висновки статті включають такі аспекти:

Зростання загроз: Сучасний цифровий світ стикається з постійним зростанням кількості та складності загроз несанкціонованого доступу. Хакерські атаки, фішингові кампанії та соціальний інжиніринг стають все більш винахідливими та небезпечними. Наслідки порушено: Несанкціонований доступ може призвести до серйозних наслідків, які впливають на окремих осіб, організацію та суспільство в цілому. Від фінансових втрат до порушення конфіденційності та поширення дезінформації - слідки можуть бути руйнівними. Можливість освіти: Освіта та навчання грають важливу роль у запобіганні ризикам несанкціонованого доступу. Свідомість користувачів про наявні загрози та навички розпізнавання можуть значно знизити ризики. Технологічний прогрес: Впровадження нових технологій, таких як штучний інтелект та блокчейн, може підвищити рівень інформаційної безпеки. Однак разом з цим, з'являються нові виклики та загрози, пов'язані з використанням цих технологій зловмисниками. Загальна відповідальність: Забезпечення інформаційної безпеки є спільною відповідальністю окремих осіб, організацій та держав. Тільки спільними зусиллями можна досягти надійного захисту від загрози несанкціонованого доступу. Узагальнюючи, ця стаття підкреслює актуальність та важливість інформаційної безпеки та ризиків несанкціонованого доступу в сучасному світі. Розуміння загроз та використання ефективних стратегій захисту є вирішальними для забезпечення безпеки інформації та підтримки стабільності цифрового середовища.

Список використаних джерел

1. Андерсон, Р. (2008). Інженерія безпеки: посібник зі створення надійних розподілених систем. Wiley.
2. Pfleeger, CP, & Pfleeger, SL (2015). Безпека в обчисленнях. Пірсон.
3. Вітмен, М., і Маторд, Х. (2016). Принципи інформаційної безпеки. Cengage Learning.
4. Dhillon, G., & Backhouse, J. (2001). Управління безпекою інформаційних систем у новому тисячолітті. Повідомлення ACM, 44 (4), 125-128.
5. Вакка, JR (2013). Довідник з комп'ютерної та інформаційної безпеки. Морган Кауфман.
6. Шнайєр, Б. (2015). Дані та Голіаф: приховані битви за збір ваших даних і контроль над світом. WW Norton & Company.
7. Мелл П. та Гренс Т. (2011). Визначення хмарних обчислень NIST (Спеціальна публікація 800-145). Національний інститут стандартів і технологій.
8. Cisco. (2020). Річний звіт Cisco про Інтернет (2018–2023). Отримано з https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
9. Symantec. (2019). Звіт про загрози безпеці в Інтернеті: Том 24. Отримано з https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
10. Verizon. (2020). Звіт про розслідування витоку даних. Отримано з https://enterprise.verizon.com/resources/reports/dbir/

Робота виконана під науковим керівництвом с.н.с, доцента
ЗВЄРЄВА В.П.

РОЛЬ BYOD У ЗАХИСТІ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ ВІД КІБЕРАТАК

ОЛЕКСЮК В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розгянуто політику BYOD, її роль у захисті персональних даних працівників у випадку кібератак, а також у діяльності підприємства в цілому. Дана практика може знизити витрати на обладнання для компанії, а також покращити продуктивність працівників, але вона також може створювати загрозу для безпеки даних.

This article examines the BYOD policy and its role in protecting employees' personal data in the event of cyberattacks, as well as in the work of the enterprise as a whole. This practice can reduce a company's hardware costs and increase employee productivity, but it can also pose a threat to data security.

Актуальність. Тема BYOD (Bring Your Own Device, українською – «бери свій власний пристрій») та захисту персональних даних працівників від кібератак є дуже актуальною в сучасному бізнес-середовищі.

BYOD – це підхід, коли працівники використовують власні мобільні пристрої, такі як смартфони, планшети або ноутбуки, для роботи в офісі або поза ним. Цей підхід став дуже популярним, оскільки дозволяє працівникам бути більш продуктивними та ефективними, а також зменшує витрати компанії на придбання дорогих пристроїв.

Однак, з використанням BYOD виникає ризик втрати та зловживання персональних даних працівників. Це може стати наслідком недостатнього захисту пристроїв, що використовуються працівниками, від кібератак.

Кібератаки можуть стати причиною витоку конфіденційної інформації про компанію, її клієнтів та працівників. Зловмисники можуть використовувати віруси, троянські програми, фішинг та інші методи для отримання доступу до пристроїв працівників та викрадення конфіденційної інформації.

Метою статті є аналіз ризиків, пов'язаних з використанням BYOD у бізнес-середовищі, та висвітлення важливості захисту персональних даних працівників від кібератак. Стаття має на меті надати інформацію про те, як вирішити проблему захисту персональних даних від кібератак з використанням BYOD, а також про заходи безпеки, яких необхідно вжити для захисту пристроїв співробітників від кібератак. Крім того, стаття має на меті допомогти керівникам підприємств та IT-спеціалістам у визначенні оптимальних стратегій BYOD для захисту персональних даних співробітників від кібератак.

Об'єктом дослідження є використання BYOD (Bring Your Own Device) в бізнес-середовищі та захист персональних даних працівників від кібератак.

Предметом дослідження є ризики, пов'язані з використанням BYOD в бізнес-середовищі, та заходи безпеки, необхідні для захисту персональних даних працівників від кібератак з використанням BYOD.

Використання власних пристроїв (BYOD) стало популярною тенденцією на сучасних підприємствах, що дозволяє працівникам використовувати свої особисті пристрої, такі як смартфони, ноутбуки та планшети, для виконання робочих завдань. Така практика має численні переваги, зокрема підвищення продуктивності, гнучкості та економію коштів. Однак вона також створює значні ризики для особистих і організаційних даних, особливо в умовах кібератак. У цій статті досліджується роль BYOD у захисті персональних даних співробітників від кібератак, висвітлюються ризики, пов'язані з цією практикою, та стратегії їх зменшення [1].

Тенденція BYOD набула популярності завдяки численним перевагам, які вона пропонує працівникам та організаціям. Працівники все частіше вимагають гнучкості, щоб працювати з будь-якого місця, в будь-який час і на будь-якому пристрої. З іншого боку, організації впроваджують BYOD, щоб зменшити витрати, пов'язані з придбанням та обслуговуванням пристроїв, підвищити задоволеність і продуктивність працівників, а також покращити співпрацю.

Однак BYOD також створює значні ризики для кібербезпеки, які можуть поставити під загрозу безпеку і конфіденційність особистих і організаційних даних. Деякі з найпоширеніших ризиків, пов'язаних з BYOD, включають наступне.

Несанкціонований доступ. Коли працівники використовують особисті пристрої для виконання робочих завдань, вони часто підключаються до публічних мереж Wi-Fi або використовують незахищені мережі, піддаючи конфіденційні дані несанкціонованому доступу.

Втрачені або вкрадені пристрої. Персональні пристрої частіше губляться або викрадаються, відкриваючи доступ до конфіденційних даних стороннім особам. Відсутність шифрування пристрою або надійних паролів також може поставити під загрозу безпеку персональних даних.

Шкідливі програми та віруси. Персональні пристрої можуть бути заражені шкідливими програмами або вірусами, які можуть поширитися на мережу організації, ставлячи під загрозу безпеку особистих і організаційних даних.

Внутрішні загрози. Працівники, які використовують персональні пристрої для виконання робочих завдань, можуть навмисно чи ненавмисно порушити безпеку особистих та організаційних даних, наражаючи їх на кібератаки.

Організації можуть вжити кілька заходів для зменшення ризиків кібербезпеки, пов'язаних з власними пристроями. До них відносяться наступні [2].

Створення політики щодо використання власних пристроїв. Організації повинні розробити чітку політику та інструкції щодо використання персональних пристроїв на робочому місці. Політика повинна визначати прийнятне використання персональних пристроїв, заходи безпеки, необхідні для персональних пристроїв, і наслідки порушення політики.

Проведення регулярних тренінгів з безпеки. Працівники повинні бути навчені найкращим практикам кібербезпеки, зокрема, як виявляти та повідомляти про потенційні кіберзагрози, як захистити персональні пристрої від кібератак та як уникнути ненавмисного розголошення особистих та організаційних даних стороннім особам.

Впровадження контролю доступу. Організації повинні впровадити контроль доступу, який обмежує доступ до конфіденційних даних на основі ролі та обов'язків користувача. Цього можна досягти за допомогою політики паролів, багатофакторної автентифікації та інших засобів контролю доступу.

Шифрування. Шифрування є важливим заходом безпеки, який може захистити персональні дані від несанкціонованого доступу в разі втрати або крадіжки пристрою. Організації повинні вимагати від працівників шифрування їхніх персональних пристроїв, зокрема жорстких дисків, електронних листів і повідомлень.

Віддалене стирання: Віддалене стирання – це функція безпеки, яка дозволяє організаціям видаляти дані з втрачених або викрадених персональних пристроїв. Це гарантує, що конфіденційні дані не будуть скомпрометовані, якщо пристрій потрапить до чужих рук.

Захист персональних даних є важливим аспектом сучасних робочих місць. Зі зростанням залежності від технологій та інтернету персональні дані стають вразливими до кібератак, витоків даних та інших загроз безпеці. BYOD посилює ці ризики, оскільки працівники використовують свої особисті пристрої для виконання робочих завдань, а організація має менше контролю над заходами безпеки, що застосовуються на цих пристроях. Тому організаціям вкрай важливо враховувати захист персональних даних при впровадженні політики BYOD.

Закони про захист персональних даних, такі як Загальний регламент про захист даних (GDPR) і Каліфорнійський закон про конфіденційність споживачів (CCPA), встановлюють керівні принципи і вимоги для організацій, які збирають і обробляють персональні дані. Ці закони вимагають від організацій впроваджувати відповідні заходи безпеки для захисту персональних даних від несанкціонованого доступу, використання, розкриття чи знищення. У контексті BYOD організаціям необхідно забезпечити відповідність своїх політик і заходів безпеки цим законам, щоб уникнути потенційної юридичної відповідальності.

Одним із способів захисту персональних даних у середовищі BYOD є впровадження рішень для управління мобільними пристроями (MDM). Рішення MDM дозволяють організаціям контролювати та керувати персональними пристроями, що використовуються для виконання робочих завдань. Програмне забезпечення MDM може впроваджувати політики безпеки, такі як вимоги до паролів, шифрування та віддалене стирання, щоб забезпечити захист персональних даних у разі втрати або крадіжки пристрою. Крім того, рішення MDM можуть надавати організаціям можливість бачити в реальному часі пристрої, якими користуються співробітники, що дозволяє їм оперативно виявляти потенційні загрози безпеці.

Ще один спосіб захистити персональні дані в середовищі BYOD – впровадити рішення для запобігання втраті даних (DLP). Рішення DLP дозволяють організаціям відстежувати і контролювати передачу даних, запобігати витоку даних і забезпечувати дотримання законів про захист даних. Рішення DLP також можуть виявляти і запобігати несанкціонованому доступу до персональних даних, забезпечуючи додатковий рівень захисту в середовищі BYOD [3].

Організації також можуть використовувати рішення віртуальних приватних мереж (VPN) для захисту персональних даних у середовищі BYOD. Рішення VPN забезпечують безпечне з'єднання між персональними пристроями та мережею організації, дозволяючи працівникам безпечно отримувати доступ до робочих ресурсів. Рішення VPN також шифрують передачу даних, запобігаючи несанкціонованому доступу до персональних даних.

Нарешті, організаціям слід розглянути можливість впровадження плану реагування на інциденти безпеки (SIRP) для швидкого реагування на інциденти безпеки в середовищі BYOD. SIRP визначає кроки та процедури, яких організація повинна дотримуватися у випадку інциденту безпеки, наприклад, витоку даних або кібератаки. Добре розроблений SIRP може допомогти організаціям мінімізувати вплив інциденту безпеки на персональні дані та зменшити ризик юридичної відповідальності.

Впровадження політики BYOD та заходів безпеки для захисту персональних даних не позбавлене викликів. Однією з головних проблем є відсутність контролю над персональними пристроями. Організації не можуть впроваджувати політику безпеки на персональних пристроях, які їм не належать, що ускладнює забезпечення належного захисту персональних даних. Крім того, працівники можуть не дотримуватися політики та заходів безпеки щодо використання власних пристроїв, наражаючи персональні дані на потенційні загрози безпеці.

Ще однією проблемою є складність впровадження та управління політиками та заходами безпеки щодо використання власних пристроїв. Політики та заходи безпеки BYOD можуть відрізнятися залежно від типу персонального пристрою, операційної системи та інших факторів. Тому організаціям необхідно впроваджувати гнучкий і масштабований підхід до політик і заходів безпеки BYOD, щоб гарантувати, що вони можуть відповідати різним персональним пристроям і операційним системам.

Нарешті, впровадження політик і заходів безпеки BYOD може бути дорогим і трудомістким процесом. Організаціям необхідно інвестувати в MDM, DLP, VPN та інші рішення, щоб забезпечити належний захист персональних даних. Крім того, організаціям необхідно регулярно навчати співробітників передовим практикам кібербезпеки, що збільшує витрати і час, необхідні для впровадження політик і заходів безпеки щодо принесених з собою пристроїв.

Тенденція BYOD набула популярності завдяки численним перевагам, які вона пропонує працівникам та організаціям. Однак вона також створює значні ризики для

кібербезпеки, які можуть поставити під загрозу безпеку та конфіденційність особистих та організаційних даних. Організації можуть зменшити ці ризики, встановивши чіткі політики та інструкції щодо використання персональних пристроїв, проводячи регулярні тренінги з безпеки, впроваджуючи контроль доступу, шифруючи персональні пристрої та уможливлюючи віддалене стирання даних. Застосовуючи ці стратегії, організації можуть підвищити безпеку особистих і організаційних даних, користуючись при цьому перевагами BYOD.

Однією з альтернатив BYOD є надання компаніями своїм працівникам власних пристроїв, спеціально призначених для робочих цілей. Такий підхід може запропонувати кілька переваг над BYOD, що зазначено нижче [4].

Підвищена безпека. Пристрої, що належать компанії, можуть підлягати більш суворим політикам і процедурам безпеки, таким як обов'язкове шифрування і можливість віддаленого стирання, що може допомогти забезпечити захист конфіденційних даних у разі порушення безпеки.

Зменшення відповідальності. Коли працівники використовують свої особисті пристрої для роботи, завжди існує ризик того, що конфіденційні дані можуть бути скомпрометовані, якщо пристрій буде втрачено або викрадено. Надаючи пристрої, що належать компанії, роботодавці можуть зменшити свою відповідальність і мінімізувати ризик витоку даних.

Спрощене управління пристроями. В умовах BYOD IT-відділам часто доводиться керувати безліччю різних пристроїв і операційних систем, що може займати багато часу і бути складним завданням. Надаючи пристрої, що належать компанії, IT-відділи можуть зосередитися на управлінні стандартизованим набором пристроїв, які налаштовані для оптимальної безпеки та продуктивності.

Підвищення продуктивності. Пристрої, що належать компанії, можуть бути попередньо налаштовані з необхідним програмним забезпеченням і додатками, які потрібні співробітникам для виконання своєї роботи, що може допомогти усунути необхідність для співробітників витрачати час на налаштування власних пристроїв або усунення технічних неполадок.

Кращий контроль над даними. Коли працівники використовують свої особисті пристрої для роботи, завжди існує ризик того, що дані компанії можуть бути випадково або навмисно передані стороннім особам. Надаючи пристрої, що належать компанії, роботодавці можуть краще контролювати дані та гарантувати, що доступ до них матимуть лише уповноважені особи.

Останніми роками використання власних пристроїв (Bring Your Own Device, BYOD) на робочому місці стає все більш поширеним явищем. Хоча BYOD може запропонувати багато переваг як для роботодавців, так і для працівників, він також створює низку викликів, особливо коли йдеться про безпеку даних.

Однією з головних переваг BYOD є підвищена гнучкість і продуктивність, яку вона може запропонувати працівникам. Завдяки власним пристроям працівники можуть працювати з будь-якого місця і в будь-який час, не прив'язуючись до стаціонарного комп'ютера чи іншої стаціонарної робочої станції. Це може допомогти працівникам краще керувати балансом між роботою та особистим життям і підвищити їхню загальну задоволеність роботою.

Для роботодавців BYOD може запропонувати економію коштів за рахунок зменшення необхідності купувати та обслуговувати власні пристрої для кожного працівника. Крім того, BYOD може допомогти компаніям залучати та утримувати найкращі таланти, пропонуючи більш гнучке та сучасне робоче середовище.

Висновки. Незважаючи на переваги, BYOD може створювати значні ризики безпеки як для працівників, так і для роботодавців. Коли працівники використовують свої особисті пристрої для роботи, вони часто отримують доступ до конфіденційних даних компанії та зберігають їх на своїх пристроях. Ці дані можуть включати конфіденційну ділову інформацію, персональну ідентифікаційну інформацію (PII) та інші конфіденційні дані, які повинні бути захищені відповідно до різних нормативних актів і стандартів відповідності.

Щоб протистояти цим ризикам, компанії, які дозволяють використання власних пристроїв, повинні впроваджувати надійні політики та процедури безпеки. Ці політики повинні стосуватися таких питань, як шифрування, надійні паролі, можливості віддаленого стирання та використання віртуальних приватних мереж (VPN) для захисту даних під час передачі. Компанії також повинні інвестувати в програмне забезпечення для управління мобільними пристроями (MDM), яке може відстежувати і контролювати доступ до конфіденційних даних на персональних пристроях співробітників.

Однак, незважаючи на ці заходи, немає жодних гарантій, що пристрої, які належать працівникам, можуть бути повністю захищені, що призвело до того, що деякі компанії повністю відмовилися від BYOD на користь пристроїв, що належать компанії. Хоча такий підхід може забезпечити більшу безпеку та контроль, він також може бути більш дорогим і менш привабливим для працівників, які віддають перевагу гнучкості у використанні власних пристроїв.

Зрештою, рішення про те, впроваджувати BYOD чи ні, залежатиме від конкретних потреб і культури організації. Компанії повинні ретельно зважити переваги та ризики BYOD і розробити комплексну стратегію захисту та управління пристроями співробітників, незалежно від того, який підхід вони оберуть.

Отже, BYOD пропонує численні переваги з точки зору підвищення гнучкості та продуктивності, але він також створює значні проблеми з безпекою, які необхідно вирішувати шляхом ретельного планування та впровадження політик і процедур безпеки. Компанії, які вирішили дозволити BYOD, повинні бути готові інвестувати в необхідні технології та ресурси для захисту та управління пристроями, що належать працівникам, а ті, хто обирає пристрої, що належать компанії, повинні бути готові взяти на себе додаткові витрати, пов'язані з таким підходом. Зрештою, ключ до успіху полягає в розробці комплексної стратегії, яка збалансовує переваги та ризики BYOD і відповідає конкретним потребам організації.

Список використаних джерел

1. M.T. Banday, M.M. Algahtany, "Bring Your Own Device (BYOD) security in the organizations: Challenges and solutions", International Journal of Computer Science and Information Security, vol. 17, no. 2, 2019.
2. K.S. Ali, "Personal data protection in BYOD environments: An overview of mobile device management", International Journal of Advanced Computer Science and Applications, vol. 10, no. 9, 2019.
3. N. Hasan and M. H. Azman, "BYOD security in the workplace: A review of the challenges and solutions", 2018 International Conference on Information and Communication Technology for the Muslim World (ICT4M), Kuala Lumpur, Malaysia, 2018.
4. S. M. Aslam, S. M. Shiraz, A. Zafar, "BYOD security: Challenges, issues and solutions", 2019 International Conference on Computer and Information Sciences (ICCIS), Karachi, Pakistan, 2019.
5. Наказ від 14.05.2020 №269 Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації».
6. IT-Grundschutz catalogues. – URL: https://www.scribd.com/document/534182501/IT-Grundschutz-catalogues-15th-version-2015-Draft.

Робота виконана під науковим керівництвом к.т.н., доцента
САВЧЕНКО Т.В.

ЕКСПЕРТНА СИСТЕМА ДЛЯ ВИБОРУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ВИМОГ ТА УПОДОБАНЬ ІТ-ФАХІВЦІВ

ОСАДЧУК М., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті описано розробку експертної системи для вибору програмного забезпечення на основі вимог та уподобань ІТ-фахівців. Система забезпечує можливість введення користувачем необхідної функціональності та характеристик, що повинні бути враховані при виборі ПЗ. На основі цих даних система надає рекомендації щодо оптимальних варіантів програмного забезпечення. Розроблена система була протестована на декількох прикладах вибору ПЗ, і була успішно використана для вирішення задачі вибору програмного забезпечення. Результати дослідження підтверджують, що розроблена експертна система може бути корисною для ІТ-фахівців, які займаються вибором ПЗ.

The article describes the development of an expert system for selecting software based on the requirements and preferences of IT professionals. The system provides the user with the ability to enter the necessary functionality and characteristics that should be considered when selecting software. Based on this information, the system provides recommendations for optimal software options. The developed system was tested on several examples of software selection and was successfully used to solve the software selection problem. The research results confirm that the developed expert system can be useful for IT professionals involved in software selection.

Актуальність. В сучасному світі ІТ-технології швидко розвиваються, а ринок програмного забезпечення пропонує величезну кількість продуктів, які мають різні характеристики та можливості. Вибір оптимального програмного забезпечення для виконання конкретних завдань може стати справжнім викликом для ІТ-фахівців. У цьому контексті розробка експертної системи, яка допоможе вибрати найбільш відповідне програмне забезпечення на основі вимог та уподобань користувачів, стає актуальною та необхідною.

Метою дослідження є розробка ефективного та точного інструменту для вибору програмного забезпечення, який забезпечує задоволення вимог та уподобань ІТ-фахівців.

Об'єктом дослідження є процес вибору програмного забезпечення, а предметом дослідження є експертна система для автоматизації цього процесу.

Завданнями дослідження є аналіз попередніх досліджень в цій області, вивчення особливостей процесу вибору програмного забезпечення, розробка алгоритмів та методів роботи експертної системи, тестування та оцінка її ефективності.

Предметом цієї наукової статті є розробка експертної системи для вибору програмного забезпечення на основі вимог та уподобань ІТ-фахівців.

Для досягнення поставленої мети, було проведено аналіз попередніх досліджень та визначено основні проблеми, що виникають під час вибору програмного забезпечення. На основі отриманих результатів була розроблена експертна система, яка використовує методи штучного інтелекту для аналізу вимог та уподобань користувачів та вибору оптимального програмного забезпечення для їх потреб.

Аналіз попередніх досліджень в області вибору програмного забезпечення показав, що це завдання може бути досить складним, особливо коли необхідно враховувати вимоги та уподобання різних ІТ-фахівців. Одним з підходів до вирішення цієї проблеми є використання експертних систем.

Експертні системи – це комп'ютерні програми, які імітують поведінку людини-експерта, щоб допомогти вирішити складні проблеми. Ці програми особливо корисні в додатках зі штучним інтелектом, оскільки їх можна використовувати, коли немає експерта або

якщо найняти його занадто дорого. Експертні системи можуть полегшити навчання та оптимізувати час, що призведе до підвищення продуктивності праці. Вони також часто використовуються для ознайомлення з галуззю та висвітлення поточних і потенційних застосувань.

Побудова експертної системи може бути тривалим, багаторічним процесом, який потребує багато правок зі сторони кінцевих користувачів які будуть використовувати її вже під свої певні унікальні задачі. Однак, незважаючи на те, що вони не вимагають великих і релевантних наборів даних для навчання, експертні системи страждають від обмежень ефективності, масштабованості та застосовності. Крім того, інтерфейси користувача для експертних систем часто розробляються з використанням Visual Basic[1], що робить їх популярним вибором для багатьох програм.

Основні компоненти експертної системи включають базу знань, механізм виведення (логічний двигун) та інтерфейс користувача. База знань містить інформацію, яка відображає знання та досвід експертів у певній галузі. Механізм виведення відповідає за аналіз інформації, яка надходить від користувача, та генерацію рекомендацій на основі знань, зібраних у базі знань.

З точки зору переваг, діагностика несправностей виявилася однією з найбільш корисних областей застосування для впровадження систем, заснованих на знаннях, а діагностичні системи, засновані на неглибоких знаннях, були високоефективними у вузькому домені, пов'язаному з конкретними завданнями. З іншого боку, недоліки експертних систем включають відсутність сприйняття системи користувачами, неможливість утримати розробників, і відносно мало опубліковано саме стосовно модельних підходів для розробки експертних систем [5]. Щоб подолати ці недоліки, архітектура нейронної експертної системи дозволяє автоматично створювати базу знань шляхом навчання на прикладах висновків, що дає змогу вивчати шаблони з нерелевантними входами та виходами. Крім того, до системи можна додати евристику для роботи з неповною інформацією та для пояснення висновків.

Експертна система може бути корисною для вибору програмного забезпечення, оскільки вона може виконувати багато виснажливих завдань, які люди можуть бути не в змозі виконати. Це також може допомогти зменшити кількість часу та грошей, необхідних для вибору програмного забезпечення, оскільки воно може швидко проаналізувати дані та надати список рекомендованого програмного забезпечення. Крім того, це може бути корисним в інших сферах управління людськими ресурсами, наприклад, під час найму, навчання та оцінки ефективності. В результаті експертна система може забезпечити ефективне рішення для вибору програмного забезпечення. Крім того, експертна система може допомогти підвищити точність і якість процесу відбору. Він може забезпечити більш надійні та послідовні результати, ніж людська система, оскільки він може ідентифікувати та усувати будь-яке потенційне упередження. Крім того, оскільки експертна система може швидко і точно аналізувати дані, вона може надати більш точні та надійні рекомендації щодо вибору програмного забезпечення. Це може допомогти скоротити кількість часу та грошей, необхідних для вибору програмного забезпечення. Підсумовуючи, експертні системи можуть бути корисними при виборі програмного забезпечення та інших сферах управління людськими ресурсами. Вони можуть надати швидші, точніші та надійніші результати, ніж людські системи, а також можуть зменшити кількість часу та грошей, необхідних для вибору програмного забезпечення.

Експертна система – це комп'ютерна програма, призначена для імітації поведінки людини-експерта . Це одна з найкорисніших програм штучного інтелекту , яка складається з інтерфейсу користувача, підсистеми пояснення, механізму логічного висновку та бази знань. Ядром експертної системи є база знань, яка зберігає правила, об'єкти, загальні випадки, винятки та відношення. Компоненти експертної системи дозволяють людині-експерту впоратися з певною проблемою, а систематичний дизайн експертної системи може бути розроблений за допомогою Уніфікованої мови моделювання (UML).

Експертні системи є програмними системами, які використовують бази знань та правил, щоб допомогти користувачеві вирішувати складні задачі в певній галузі. У випадку вибору програмного забезпечення, експертна система може аналізувати вимоги та уподобання користувачів, оцінювати різні параметри програмного забезпечення, такі як функціональність, продуктивність та безпека, та надавати рекомендації щодо вибору найбільш підходящого варіанту. Результати тестування експертної системи показали її ефективність та точність в роботі.

Різні автори пропонують різні підходи до розробки експертних систем для вибору програмного забезпечення. Деякі автори пропонують використання методів штучного інтелекту, таких як нейронні мережі та генетичні алгоритми, для покращення ефективності експертної системи. Інші автори пропонують використання методів множинного критерію прийняття рішень, які дозволяють враховувати різні критерії та обмеження при виборі програмного забезпечення.

Одним з основних етапів процесу вибору програмного забезпечення є збір вимог та уподобань користувачів. Для ефективного використання експертної системи для вибору програмного забезпечення, необхідно детально проаналізувати ці вимоги та уподобання та перетворити їх на формальні критерії та обмеження.

Після збору вимог та уподобань, експертна система може провести аналіз різних варіантів програмного забезпечення та згенерувати список підходящих варіантів. Цей список може бути відфільтрований та відсортований за різними критеріями, такими як ціна, функціональність та безпека. Після цього користувач може ретельно ознайомитися з кожним з варіантів та визначитися з вибором, що найкраще відповідає його потребам.

Процес вибору програмного забезпечення є складним і може включати в себе різні критерії, такі як вартість, функціональність, масштабованість та інші. Крім того, можуть бути наявні обмеження, такі як сумісність з існуючим програмним забезпеченням та обмеженнями на час впровадження. Експертна система повинна враховувати ці критерії та обмеження для того, щоб дати користувачеві якісну рекомендацію.

Для розробки експертної системи для вибору програмного забезпечення можна використовувати різні методології. Нижче наведені деякі з них.

1 Методологія знань. Методологія знань є однією з основних методологій розробки експертних систем. Вона передбачає розробку бази знань, що містить правила та факти з певної галузі. Ця база знань потім використовується для прийняття рішень. В експертній системі для вибору програмного забезпечення правила та факти можуть бути пов'язані з різними критеріями та обмеженнями, які необхідно враховувати при виборі програмного забезпечення.

2 Методологія множинного критерію прийняття рішень. Методологія множинного критерію прийняття рішень передбачає врахування різних критеріїв та обмежень при виборі програмного забезпечення. В експертнній системі для вибору програмного забезпечення ця методологія може використовуватися для призначення вагових коефіцієнтів для кожного критерію та обмеження, що дозволить зробити більш об'єктивний вибір.

3 Методологія аналізу ієрархій. Методологія аналізу ієрархій (AI) - це методологія, що дозволяє порівнювати різні критерії та обмеження на основі їх важливості. В експертній системі для вибору програмного забезпечення AI може використовуватися для визначення важливості різних критеріїв та обмежень для користувача та призначення вагових коефіцієнтів кожному критерію та обмеженню.

Розробляючи експертну систему для IT-фахівців, слід враховувати кілька основних факторів. Важливо, що система розроблена з використанням модульного підходу, щоб її було легко оновлювати та покращувати в майбутньому. Крім того, система повинна бути розроблена так, щоб вона була зручною для користувача, з ясним і лаконічним інтерфейсом користувача, який легко зрозуміти. Крім того, система повинна бути розроблена з можливістю масштабування вгору або вниз залежно від потреб користувача, дозволяючи системі рости разом з вимогами користувача. Безпека також є важливим фактором, оскільки система

повинна бути розроблена таким чином, щоб захищати дані та інформацію користувача. Нарешті, система повинна бути розроблена таким чином, щоб мати можливість інтегруватись з іншими існуючими IT-системами, забезпечуючи безперебійну взаємодію між користувачем і системою.

Першим кроком у розробці експертної системи для вибору програмного забезпечення є збір вимог та уподобань користувача. Цей крок включає в себе визначення критеріїв, які важливі для користувача, таких як функціональність, масштабованість, вартість та інші. Крім того, можуть бути визначені обмеження, такі як сумісність з існуючим програмним забезпеченням та обмеження на час впровадження.

Після збору вимог та уподобань користувача наступним кроком є розробка бази знань, яка містить правила та факти з певної галузі. У випадку експертної системи для вибору програмного забезпечення ця база знань міститиме правила та факти, пов'язані з критеріями та обмеженнями, які були визначені на першому кроці. Наприклад, якщо одним з критеріїв є масштабованість, то база знань може містити правила, які вказують на те, які програмні продукти є більш масштабованими за інші.

Для того, щоб користувач міг взаємодіяти з експертною системою, необхідно розробити інтерфейс користувача. Цей інтерфейс може бути у вигляді веб-сторінки або додатка, що встановлюється на комп'ютер користувача. В інтерфейсі користувач може ввести свої вимоги та уподобання, а також переглянути рекомендації, які згенерувала експертна система.

Після розробки бази знань та інтерфейсу користувача необхідно розробити правила інтерпретації, які допоможуть експертній системі зрозуміти вимоги та уподобання користувача. Ці правила можуть бути в основному у вигляді логічних правил, які забезпечують виконання порівняння та забезпечення рекомендацій.

Останнім кроком у розробці експертної системи для вибору програмного забезпечення є розробка алгоритму вибору. Цей алгоритм використовується для порівняння вимог та уподобань користувача з базою знань та визначення найбільш підходящого програмного забезпечення для користувача.

Розробка користувацького інтерфейсу експертної системи може допомогти IT-фахівцям зробити його зручним для користувача. Наприклад, TaxCut — зручна експертна система, призначена для полегшення взаємодії користувачів із програмним забезпеченням. Розробка гнучкого та зручного для користувача інтерфейсу є важливою для забезпечення високої якості обслуговування клієнтів. Щоб забезпечити зручність, інтерфейс користувача повинен бути розроблений з використанням знайомих користувачеві термінів. Крім того, інтерфейс користувача має бути розроблений таким чином, щоб він дозволяв користувачеві розробляти власну систему та був простим у використанні та надавав дані для ситуацій «що, якщо».

Інтерфейс користувача також повинен містити назву системи та призначення експертної системи. Усі ці компоненти необхідно об’єднати для створення комплексної та зручної експертної системи . Інтерфейс користувача також повинен мати можливості та дедуктивну силу, щоб зробити СУБД зручною для користувача. Нарешті, інтерфейс користувача повинен бути розроблений таким чином, щоб включати як спеціалістів, так і неспеціалістів. Отже, це зробить систему зручною та гнучкою для користувачів.

При розгляді функцій, які повинні бути включені в експертну систему, є важливі функції, які повинні бути присутніми для того, щоб гарантувати, що програма не потребує технологій, що виходять за межі сучасного рівня. Ці функції включають набір правил, базу даних відповідної інформації, спосіб пошуку інформації, інтерфейс, який дозволяє користувачам вводити запитання та отримувати відповіді, а також спосіб оновлення системи за потреби. Крім того, бажані функції допоможуть вказати програми, які мають найбільші шанси на успішне впровадження. Такі функції включають зручний інтерфейс, можливість навчатися на основі введених користувачем даних, здатність інтегруватися з іншими програмами чи базами даних і здатність надавати користувачеві зворотний зв’язок. Добре

спроектована експертна система також повинна включати механізм відстеження та моніторингу продуктивності системи з метою виявлення будь-яких потенційних проблем або покращень, які можна зробити. Нарешті, система повинна мати можливість тестування та перевірки для забезпечення точності та надійності. Усі ці функції необхідні для того, щоб експертна система була корисною для ІТ-фахівців і надавала їм інформацію та знання, необхідні для прийняття обґрунтованих рішень.

Висновки. У цій статті було розглянуто експертну систему для вибору програмного забезпечення на основі вимог та уподобань ІТ-фахівців. Визначено ціль, мету, завдання, об'єкт дослідження та предмет дослідження даної експертної системи. Було описано процес розробки експертної системи та її складові елементи, які включають базу знань, інтерфейс користувача, правила інтерпретації та алгоритм вибору.

Експертні системи здатні забезпечити велику кількість переваг, зокрема, вони здатні розглядати велику кількість варіантів вирішення проблеми, забезпечують однаковість вирішення проблеми при однакових вихідних даних та здатні підтримувати та оновлювати свою базу знань.

Експертні системи для вибору програмного забезпечення можуть бути корисним інструментом для ІТ-фахівців, які шукають оптимальне програмне забезпечення для вирішення конкретної задачі. Вони допомагають скоротити час на пошук та вибір програмного забезпечення та зменшити ризики неправильного вибору.

У майбутньому, експертні системи для вибору програмного забезпечення можуть бути ще більш розробленими та удосконаленими. Наприклад, вони можуть використовувати машинне навчання для покращення рекомендацій та врахування нових продуктів програмного забезпечення. Також можливим є використання експертних систем для вибору інших типів технічних засобів, таких як апаратне забезпечення.

У цілому, експертні системи для вибору програмного забезпечення мають великий потенціал для вирішення проблем в галузі ІТ, забезпечуючи швидке та ефективне рішення при виборі програмного забезпечення на основі вимог та уподобань ІТ-фахівців. Це може значно зменшити час та зусилля, необхідні для вибору програмного забезпечення, та допомогти забезпечити якість та продуктивність у роботі з програмним забезпеченням.

Список використаних джерел

1. Григор'єва І. А., Євтух М. Д. Методика формування експертної системи підтримки процесу вибору програмного забезпечення // Вісник Національного університету "Львівська політехніка". Серія: Комп'ютерні системи та мережі. – 2014. – № 807. – С. 118–126.
2. Довгань В. І., Сотнікова О. М. Експертна система вибору програмного забезпечення для автоматизованої системи управління // Наукові праці ДонНТУ. Серія "Інформатика, кібернетика та обчислювальна техніка". – 2015. – Вип. 2 (28). – С. 75–81.
3. Дударєв О. В. Експертна система вибору програмних продуктів на основі вимог користувачів // Вісник Чернігівського національного технологічного університету. Серія: Технічні науки. – 2018. – № 1 (85). – С. 114–120.
4. Костенко А. І., Лавренюк Є. М., Осьмак О. В. Експертна система підтримки прийняття рішень з вибору програмного забезпечення // Наукові праці ДонНТУ. Серія "Інформатика, кібернетика та обчислювальна техніка". – 2019. – Вип. 1 (35). – С. 68–75.
5. Кузнецов О. О., Ярмак Н. М. Експертна система вибору платформи для розробки програмного забезпечення // Вісник Київського національного університету технологій та дизайну. Серія: Технічні науки та архітектура. – 2017. – № 1 (89). – С. 119–125.

Робота виконана під науковим керівництвом к.е.н, старшого викладача
ФРАНЧУК Т. М.

ПРОГРАМНА РЕАЛІЗАЦІЯ ОНЛАЙН-СЕРВІСУ ПІДБОРУ КОМПЛЕКТУЮЧИХ ДЛЯ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

ПАВЛІВСЬКИЙ Я., 2м ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади розробки прогрмної платформи сервісу онлайн-підбору комплектуючих для персонального комп'ютера. Зазначено переваги користуванням даного сервісу та варіанти розробки. Також було враховано фактор конкурентоспроможності на ринку серед подібних сервісів.

The article discusses the basic principles of building an online component selection service for a personal computer. The advantages of using this service and development options are indicated. The factor of competitiveness in the market among similar services was also taken into account.

Актуальність. Онлайн-сервіси підбору комплектуючих для персонального комп'ютера стали дуже популярними останніми роками. Це пов'язано з тим, що люди стали частіше замовляти комплектуючі в Інтернеті, а не в магазинах. Онлайн-сервіси дозволяють користувачам легко знайти потрібні комплектуючі та порівняти їх характеристики та ціни.

Один з головних факторів, що зумовили популярність сервісів підбору комплектуючих, - це зростання інтересу до геймінгу та розвиток інтернет-технологій. Люди стали більше часу проводити за комп'ютерами, а отже, інтересуватись якістю та продуктивністю своїх комп'ютерів.

Існує також зростаючий інтерес до збільшення продуктивності комп'ютера за допомогою підбору правильних комплектуючих. Онлайн-сервіси дозволяють користувачам знайти оптимальний баланс між ціною та характеристиками.

Сервіси онлайн-підбору комплектуючих для персонального комп'ютера є дуже актуальними в наш час. Розвиток інтернет-технологій та електронної комерції дозволяє людям з усього світу купувати товари в мережі з будь-якого місця та в будь-який час. Особливо це стосується комплектуючих для персональних комп'ютерів.

Основні переваги використання сервісів онлайн-підбору комплектуючих для персонального комп'ютера такі:

1. Зручність та швидкість: Користувачі можуть знайти необхідні комплектуючі за допомогою спеціальних сервісів всього за кілька хвилин. Вони можуть шукати комплектуючі за різними параметрами, такими як ціна, виробник, характеристики, розмір і т.д.
2. Великий вибір: Онлайн-магазини пропонують великий вибір комплектуючих для персональних комп'ютерів, що значно збільшує ймовірність того, що користувач знайде необхідний товар.
3. Знижки та пропозиції: Онлайн-магазини часто пропонують різні знижки, акції та пропозиції, що дозволяє зекономити кошти під час покупки комплектуючих.
4. Доставка до дому: Більшість онлайн-магазинів пропонують доставку товарів до дому, що дозволяє користувачам зекономити час та зусилля, не відходячи від комп'ютера.
5. Комфортний відбір товару: Онлайн-магазини надають можливість детального ознайомлення з товарами, їхніми характеристиками та відгуками користувачів. Це дозволяє зробити збір даних та прийняти рішення про покупки.

Метою статті є дослідження особливостей використання сервісів з онлайн-підбором комлектуючих для персонального комп'ютера та їх ефективність.

Об'єктом дослідження є розробка сервісу онлайн-підбору комплектуючих для персонального комп'ютера.

Предмет дослідження – програмні інструменти онлайн сервіс підбору.

Аналіз попередніх досліджень. Дослідженню оптимізації процесу підбору комплектуючих для пк за допомогою програмної реалізації онлайн-сервісу присвячені праці: Самара О. С., Гаврилюк Дмитро, Пилипенко Оксана, Коваленко Олександр.

Виклад основного матеріалу. За останні кілька років, ринок комп'ютерних комплектуючих значно змінився, і з'явилися нові можливості для тих, хто шукає спосіб оновити свій персональний комп'ютер. Однією з таких можливостей є використання сервісів онлайн-підбору комплектуючих. Ці сервіси дозволяють користувачам знайти все необхідні для свого ПК, враховуючи їх потреби та бюджет.

Онлайн конфігуратор ПК - це спеціальна програма, за допомогою якої користувач зможе підібрати потрібну йому конфігурацію ПК, не виходячи з дому. Іншими словами конфігуратор ПК - автоматизований ресурс по підбору комплектуючих для персонального комп'ютера. Можна сказати, що конфігуратор ПК - це аналог продавця-консультанта в магазині. У даній системі також, як і запитавши у консультанта, можна також отримати інформацію про сумісність тих або інших комплектуючих між собою, отримати пораду про вибір ПК для роботи з конкретними програмами, дізнатися вартість комп'ютера і, виходячи з цієї інформації, одержати найбільш підходящий варіант готової конфігурації ПК.

У цій статті ми розглянемо переваги та недоліки використання таких сервісів.

Переваги сервісу онлайн-підбору:

1. Ефективність. Онлайн-підбір комплектуючих дозволяє швидко знайти їх для вашого ПК. Вам не потрібно витрачати час на пошук та порівняння різних товарів, а сервіс зробить це за вас.
2. Придатність до використання. Більшість сервісів онлайн-підбору дуже прості та зрозумілі в користуванні. Вони надають зручний інтерфейс, який дозволяє з легкістю знайти необхідні комплектуючі.
3. Гнучкість. Сервіси онлайн-підбору дозволяють вибрати комплектуючі з різних виробників, моделей та цінових категорій. Вам не потрібно обмежувати себе тільки одним виробником або моделлю.
4. Економічність. Використання даних сервісів може допомогти зекономити кошти. Вони дозволяють знайти комплектуючі за кращими цінами та зіставити різні варіанти.

Сервіси онлайн-підбору комплектуючих для ПК є корисними для людей, які не розуміються в складних технічних аспектах комп'ютерів, але хочуть зібрати або оновити свій ПК. Ці сервіси надають можливість легко і швидко знайти потрібні компоненти, враховуючи всі необхідні технічні характеристики, такі як сумісність, розмір, потужність, вартість та інші.

Це особливо корисно для тих, хто не має часу або можливості досліджувати різні компоненти та їх характеристики, або не має достатньої кваліфікації, щоб правильно підібрати компоненти для свого ПК. Сервіси онлайн-підбору комплектуючих для ПК надають їм зручний та легкий спосіб знайти всі необхідні деталі для свого ПК та зберегти час та гроші, які можна було б витратити на невдалі спроби вибрати потрібні компоненти самостійно.

Рис. 1. Схема онлайн торгівлі

Оптимізація процесу підбору комплектуючих для ПК з використанням програмної реалізації онлайн-сервісу може принести численні переваги для користувачів, що шукають оптимальний варіант конфігурації свого комп'ютера.

Однією з головних переваг є часова ефективність. Замість того, щоб витрачати час на пошук і аналіз різноманітних комплектуючих, користувач може скористатися сервісом та отримати швидкий та точний варіант підбору, що значно зберігає час.

Крім того, програмна реалізація дозволяє підбирати комплектуючі на основі різних параметрів, таких як вартість, продуктивність, розмір, сумісність тощо. Це допомагає користувачеві знайти найбільш підходящу конфігурацію за його вимогами та можливостями.

Окрім цього, онлайн-сервіс може враховувати такі фактори, як технічні характеристики вже наявних комплектуючих та їх сумісність з іншими елементами комп'ютера. Таким чином, користувач може уникнути проблем зі сумісністю та зберегти кошти на зайвих покупках.

Крім цього, використання програмної реалізації дозволяє зменшити ймовірність помилок та неуважних дій, що можуть виникнути при ручному підборі комплектуючих. У загальному, використання онлайн-сервісу для підбору комплектуючих дозволяє значно спростити та оптимізувати процес вибору та покупки комп'ютерної техніки, що є важливим фактором у сучасному світі інформаційних технологій.

Сервіси онлайн-підбору комплектуючих для ПК є дуже важливими на ринку інформаційних технологій. За останні кілька років зростання інтересу до комп'ютерних ігор, відеомонтажу та інших завдань, які вимагають потужного комп'ютера, призвело до збільшення попиту на користувачів, які бажають зібрати свій власний ПК з оптимальними комплектуючими.

Сервіси онлайн-підбору комплектуючих для ПК дозволяють користувачам з легкістю зібрати свій власний ПК, відповідний їхнім потребам та бюджету. Це допомагає зменшити час, який потрібен для відбору компонентів, а також дозволяє користувачам уникнути помилок при виборі несумісних комплектуючих. Крім того, сервіси підбору комплектуючих для ПК можуть допомогти користувачам зменшити витрати на придбання компонентів, оскільки вони можуть порівняти ціни на різних платформах та виробниках.

На ринку сервісів онлайн-підбору комплектуючих для ПК є багато конкурентів, і тому компанії, які розробляють такі сервіси, повинні постійно покращувати свої продукти та додавати нові функції, щоб зберігати свою конкурентну перевагу. Від цього залежить їхній успіх на ринку та популярність сервісу серед користувачів.

Конкуренція сервісів з онлайн підбору комплектуючих для ПК є досить великою і динамічною. На ринку присутні багато компаній, що пропонують схожі послуги, тому важливо мати конкурентні переваги та додаткові функції, що привертають клієнтів.

Однією з основних конкурентних переваг є точність та повнота баз даних з комплектуючими. Клієнти часто вибирають сервіс, який надає найбільш повну та актуальну інформацію про наявні на ринку комплектуючі. Також важливо мати простий та зручний інтерфейс, щоб клієнти могли швидко та легко знайти потрібний компонент.

Іншим важливим аспектом є цінова конкуренція. Клієнти зазвичай шукають найкращу пропозицію за доступною ціною. Тому сервіси з онлайн підбору комплектуючих, що надають можливість порівнювати ціни на різних платформах, мають більші шанси на успіх. Також важливо мати додаткові функції, які можуть привернути клієнтів. Наприклад, деякі сервіси можуть пропонувати можливість складання власної конфігурації ПК з врахуванням потреб користувача, або надавати гарантію на придбані комплектуючі.

Окрім цього, важливо мати рекламну стратегію, яка допоможе залучити нових клієнтів. Такі сервіси можуть використовувати різні маркетингові інструменти, такі як контекстна реклама, соціальні мережі, пошукова оптимізація та інші.

Сервіс, який розробляється буде враховувати ці критерії, щоб конкурувати на ринку з подібними сервісами. В умовах проектування підтримки прийняття рішень при підбору комп’ютерної техніки, це пошук способу, якій задовольняє вимогам функціональності

системи засобами наявних технологій з урахуванням заданих обмежень. Складність проектування проявляється в тому, що воно не є конструктивною задачею, як аналіз вимог чи реалізація проекту розв'язків. Проектування описується як окремий етап розробки проекту проміжний між аналізом та розробкою.

Для розробки сервісу з онлайн підбору комплектуючих для ПК потрібно використовувати різні технології, які допоможуть створити функціональний та ефективний продукт. Основними технологіями, які можна використовувати для розробки такого сервісу, є:

1. Бази даних: важливо мати точну та повну базу даних з комплектуючими, щоб користувачі могли швидко та легко знайти потрібні компоненти. Для зберігання даних можна використовувати реляційні або нереляційні бази даних, такі як MySQL, MongoDB, PostgreSQL тощо.
2. Front-end технології: для створення інтерфейсу користувача можна використовувати різні front-end технології, такі як HTML, CSS, JavaScript та фреймворки для них, наприклад, React, Angular, Vue.js тощо.
3. Back-end технології: для створення логіки та обробки запитів від користувачів можна використовувати різні back-end технології, такі як Python, PHP, Ruby, Node.js тощо. Також для розробки back-end можна використовувати фреймворки, такі як Django, Flask, Laravel, Express тощо.
4. API технології: для забезпечення взаємодії між front-end та back-end можна використовувати API технології, такі як REST або GraphQL.
5. Хмарні технології: для зберігання та обробки даних можна використовувати хмарні технології, такі як Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) тощо.

Для розробки сервісу з онлайн підбору комплектуючих для ПК можна використовувати різні моделі, наприклад Waterfall. Основна суть моделі Waterfall у тому, що етапи залежать один від одного і наступний починається, коли завершений попередній, утворюючи таким чином поступальний (каскадний) рух уперед.

Паралелізм етапів у каскадній моделі, хоч і обмежений, але можливий для абсолютно незалежних між собою робіт. При цьому інтеграція паралельних частин все одно відбувається на якомусь наступному етапі, а не в рамках одного. Команди різних етапів між собою не комунікують, кожна команда відповідає чітко за свій етап.

Недоліками цієї моделі є отримання результату по проходженню всіх етапів і складність виявлення помилок. Повертатися назад важко. Не зрозуміло що повертати: якщо стався збій на якомусь етапі, його наслідки видно тільки в кінці.

Дана модель зрозуміло і чисто вкладається в документи, наприклад в договори і роадмапи при наявності чітко визначених контрольних точок. У будь-який момент можна легко зрозуміти чи була пройдена та чи інша точка контролю чи ні, і чи дотримані терміни. З цих причин довготривалі і особливо великі проекти, розраховані на десятиліття і залучення великої кількості організацій-учасників, керуються переважно waterfall.

Користувачі конфігуратора ПК можуть використовувати його для створення власних унікальних конфігурацій ПК, які відповідають їх потребам і бюджету. Основні кроки використання конфігуратора ПК включають наступне:

1. Вибір типу ПК: Користувач вибирає тип ПК, який йому потрібен, наприклад, робочий ПК, ігровий ПК або ноутбук.
2. Вибір компонентів: Користувач вибирає компоненти ПК, які йому потрібні, наприклад, процесор, материнську плату, оперативну пам'ять, жорсткий диск, відеокарту, блок живлення та інші. Кожен компонент має різні варіанти, які можуть бути вибрані в залежності від бюджету та потреб користувача.
3. Редагування конфігурації: Користувач може редагувати конфігурацію, змінюючи компоненти або додавати нові.

4. Збереження та завантаження конфігурації: Користувач може зберегти побудовану конфігурацію та завантажити її в майбутньому для використання.

5. Рекомендації щодо вибору оптимальної конфігурації: Конфігуратор ПК може надавати користувачам рекомендації щодо вибору оптимальної конфігурації на основі їх потреб та бюджету.

Ось схема схема структурного розгортання системи:

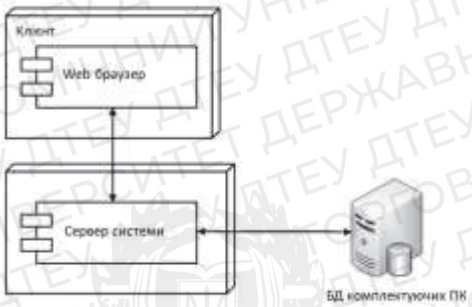


Рис. 3. Схема структурного розгортання системи програмної платформи

Схема структурного розгортання системи є важливою частиною проектування будь-якої складної інформаційної системи. Вона допомагає визначити потрібне обладнання та програмне забезпечення, необхідне для реалізації системи, а також дозволяє зрозуміти, як різні компоненти взаємодіють між собою та з іншими системами. Загалом, схема структурного розгортання системи дозволяє розробникам та інженерам зрозуміти фізичну реалізацію системи та забезпечити її ефективність та надійність.

Висновки. У результаті аналізу конкурентних сервісів та технологій, які можна використовувати для розробки сервісу з онлайн підбору комплектуючих для ПК, можна зробити висновок, що такий сервіс може бути дуже корисним для користувачів. Завдяки йому, користувач може зібрати оптимальний комп'ютер для своїх потреб, не витрачаючи багато часу та коштів на дослідження та вибір.

Важливим етапом розробки сервісу є використання відповідних моделей для підбору оптимальної конфігурації комп'ютера. Застосування таких моделей може зменшити кількість помилок при підборі комплектуючих та забезпечити вищу точність в роботі сервісу.

Однак, важливо також забезпечити зручний та інтуїтивно зрозумілий інтерфейс користувача, щоб зробити процес підбору комплектуючих максимально доступним та зрозумілим для широкого кола користувачів.

Отже, створення сервісу з онлайн підбору комплектуючих для ПК може бути вигідним та корисним для користувачів, що може допомогти вирішити проблему вибору оптимальної конфігурації комп'ютера.

Список використаних джерел

1. Блог Evergreen – методології розробки ПЗ. [Електронний ресурс] – Режим доступу: https://evergreens.com.ua/ua/articles/software-development-metodologies.html
2. Роман Марченко, DAN IT Education. Електронний ресурс] – Режим доступу: https://dan-it.com.ua/uk/blog/rozrobka-z-boku-front-end-shho-ce-take-i-chim-vidriznjaietsja-vid-back-end/
3. West Stream - Як створити свій сайт самостійно? Електронний ресурс] – Режим доступу: https://wsart.com.ua/yak-stvoriti-sviy-sayt-samostiyno/

Робота виконана під науковим керівництвом канд. техн. наук, доц.
РЗАЄВОЇ С. Л.

UNITY ЯК ПЛАТФОРМА ДЛЯ РОЗРОБКИ ОСВІТЯНСЬКОГО ІГРОВОГО КОНТЕНТУ

ПАСЕШНИК О., 2м курс ФІТ ДТЕУ
спеціальність 121 "Інженерія програмного забезпечення"

У статті розглянуто можливість використання платформи Unity в навчальних цілях, його функціонал, історію а також розглянуто його структуру і переваги які він може надати задля покращення освітнього процесу і збільшення зацікавленості учнів до навчання.

The article considers the possibility of using the Unity platform for educational purposes, its functionality, history, as well as its structure and advantages that it can provide to improve the educational process and increase students' interest in learning.

Актуальність. На Unity сьогодні розробляють багато різних проєктів які приносять великі прибутки своїм власникам, при цьому вона як платформа для розробки освітянського ігрового контенту є також досить актуальною в сучасному світі. За останні кілька років ігрові технології стали все більш популярними в освіті, і все більше навчальних закладів та компаній починають використовувати ігрові інтерактивні програми для покращення ефективності навчання та залучення учнів до процесу навчання. Завдяки широкому спектру інструментів та можливостей, які надає Unity, розробники можуть створювати навчальні ігри з використанням різних видів взаємодії та інтерактивності, що може забезпечити краще засвоєння матеріалу учнями.

Метою статті є вивчення можливостей платформи Unity, в тому числі для розробки освітянського ігрового контенту. Дослідження інструментів та технології які присутні в Unity, які можливості для інтерактивного навчання можна реалізувати на цій платформі, та які є приклади успішної реалізації ігрового контенту за допомогою рушія Unity. Результати дослідження допоможуть зрозуміти, наскільки ефективно можна використовувати Unity для розробки навчальних ігор та як можна покращити якість освітнього контенту, щоб забезпечити кращі результати в процесі навчання.

Об'єктом дослідження є використання платформи Unity для створення освітянського контенту.

Предмет дослідження - Unity, як платформа для розробки освітянського ігрового контенту.

Аналіз попередніх досліджень. Unity була заснована в Копенгагені Ніколасом Френсісом, Йоахімом Анте та Девідом Хельгасоном. Її історія почалася на форумі OpenGL у травні 2002 року, де Френсіс розмістив оголошення про пошук співробітників для розробки шейдер-компілятора з відкритим вихідним кодом (графічного інструменту) для нішевої групи розробників ігор на базі Mac, таких як він сам. На нього відгукнувся Анте, на той час старшокласник з Берліна. Анте доповнив зосередженість Френсіса на графіці та геймплеї інтуїтивним розумінням внутрішньої архітектури. Оскільки гра, над якою він працював з іншою командою, нікуди не йшла, вони співпрацювали над шейдером неповний робочий день, поки кожен з них займався своїми власними проектами ігрового рушія, але вирішили об'єднати зусилля при особистій зустрічі. Щоб об'єднати кодові бази своїх рушіїв, вони розбили наметове містечко в квартирі Хельгасона на кілька днів, поки його не було в місті. План полягав у тому, щоб заснувати ігрову студію на базі потужної технічної інфраструктури, яку також можна було б ліцензувати.

Хельгасон і Френсіс працювали разом ще зі школи, працюючи над різними проектами з веб-розробки і навіть над короткочасними спробами кіновиробництва. Хельґасон навчався в Копенгагенському університеті, працюючи веб-розробником-фрілансером. Він допомагав, де

міг, а через кілька місяців перейшов на повний робочий день, продавши свою невелику частку у фірмі з веб-розробки своїм партнерам [1].

Ігровий рушій Unity був випущений у 2005 році з початковою підтримкою ПК з Windows та веб-браузерів. З часом він став більш досконалим, що дозволило Unity розширити роботу до десятка чи близько того співробітників. Переломним моментом стала середина 2008 року, коли Apple представила iPhone App Store, що привело до появи ігрових додатків для iOS. Іншим великим прогресом став випуск MMORPG FusionFall від Cartoon Network, створеної на Unity3D із 8 мільйонами гравців. Unity також знайшла клієнтів серед великих компаній, таких як Electronic Arts, Microsoft і Ubisoft. У 2011 році Unity придбала анімаційну компанію під назвою Mecanim, покращивши основну технологію ігрового рушія. Сьогодні Unity та її 285 співробітників у всьому світі працюють над розробкою ігор для різних платформ, таких як iOS, Android, Windows, Mac, Linux, веб-браузери, PS3, Xbox 360 і Wii U. Unity3D використовують для створення складних ігор для iOS і Android. Незважаючи на гучні імена, які використовують Unity3D, засновник Unity - Helgason - пишається тим, що їх технологію можуть використовувати не тільки великі компанії, але і менші розробники. “Великі компанії завжди могли створювати ігри, вони б зрозуміли це і купили технологію або створили її самі" "Де ми дійсно досягли успіху, так це в тому, щоб ці маси людей могли не просто створювати ігри, а створювати ігри, використовуючи ті ж інструменти, що й великі хлопці" [2].

Також вивченням цього питання займались такі науковці як: Д.В. Мацокін, І.М. Пахомова та С.М. Цирульник.

Цирульник С.М., у своїй статті розглянув поняття доповненої реальності та акцентувався на застосуванні технології доповненої реальності в освітньому процесі підготовки студентів технічних спеціальностей. Вивчав актуальність та переваги використання даної технології в освітньому процесі [9].

Д.В. Мацокін та І.М. Пахомова в своїх дослідженнях пояснили актуальність такого підходу для учнів та студентів і на практиці показали як можна використовувати доповнену реальність. Вони створили додаток для учнів який допомагає вивчати фізику [10].

Виклад основного матеріалу. Ігровий рушій — це середовище розробки програмного забезпечення, яке також називають «архітектурою гри» або «ігровою структурою» з налаштуваннями та конфігураціями, які оптимізують і спрощують розробку відеоігор на різних мовах програмування. Ігровий движок може включати 2D- або 3D-графічний движок, який сумісний з різними форматами імпорту, фізичний рушій, який імітує дії в реальному світі, штучний інтелект (ШІ), який автоматично реагує на дії гравця, звуковий механізм, який керує звуковими ефектами, механізм анімації та безліч інших функцій [4].

Unity має дві основні переваги перед іншими передовими інструментами розроблення ігор: надзвичайно продуктивний візуальний робочий процес і потужна міжплатформна підтримка. Візуальний робочий процес є досить унікальною річчю, що виділяє цей інструмент із більшості інших середовищ розробки ігор. У той час як інші інструменти розроблення ігор найчастіше являють собою мішанину розрізнених частин, які потрібно контролювати, або, можливо, бібліотеку, для роботи з якою потрібно налаштовувати власне інтегроване середовище розробки (Integrated Development Environment, IDE), ланцюжок складання та інше в цьому роді, робочий процес в Unity прив'язаний до ретельно продуманого візуального редактора. У цьому редакторі ви будете компонувати сцени майбутньої гри, пов'язуючи ігрові ресурси і код в інтерактивні об'єкти. Саме він дає змогу швидко і раціонально створювати професійні ігри, забезпечуючи небачену продуктивність праці розробників і надаючи в їхнє розпорядження вичерпний перелік найсучасніших технологій у галузі відеоігор [5].

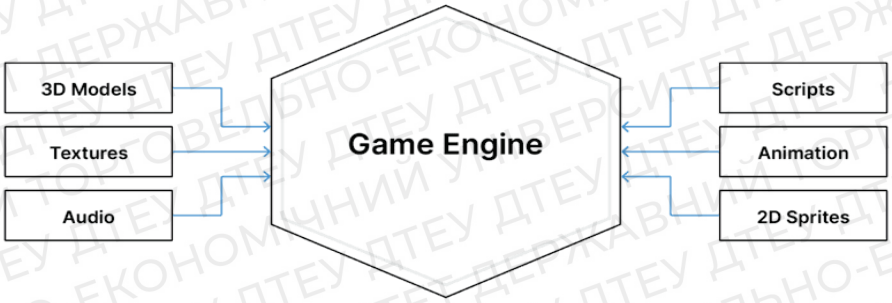


Рис. 1. Ігровий рушій [3]

Unity - це потужна технологія, яка має необмежені можливості для творчості і розвитку. Завдяки своїм інструментам та функціям, Unity може бути використана для створення різноманітних ігрових жанрів, анімаційних фільмів та навчальних проєктів. Unity дозволяє максимально реалізувати творчий потенціал та працювати над проектами в будь-якій галузі, тому можна сказати, що обмеження є лише уявою і продуктивністю [8].

Якщо ми говоримо про особливості Unity, то до таких можна віднести наступні пункти:

- Кросплатформеність: Unity дозволяє створювати ігри та додатки для різних платформах:

Рис. 2. Підтримка платформ [6]

- Візуальний редактор: Unity має вбудований візуальний редактор, який дозволяє легко створювати і налаштовувати 3D та 2D об'єкти, освітлення, камери та інші складові ігрового світу без потреби в програмуванні.
- Система скриптів: Unity має вбудовану систему скриптів, яка дозволяє програмувати поведінку ігрових об'єктів на різних мовах програмування, таких як C#, JavaScript, Boo.
- Фізика: Unity має потужну систему фізики, яка дозволяє використовувати реалістичну фізику для руху об'єктів, колізій та ін.

- Інтеграція з іншими програмами: Unity дозволяє інтегрувати зовнішні програми та ресурси, такі як 3D-моделі, звукові доріжки, відео.
- Підтримка VR і AR.

Unity - це важлива платформа для розробки VR та AR проектів, яка підтримує майже всі доступні гарнітури VR і надає численні пакети для розробки додатків на ARCore та ARKit. AR Foundation дозволяє розробникам Unity створювати додатки AR для Android та iOS одночасно, знижуючи складність розробки. Unity також пропонує XR Interaction Toolkit, щоб зробити процес розробки VR та AR ігор ще більш простим та доступним. Отже, Unity можна назвати одним з провідних підрядників у сфері розробки технологій XR [8].

Також Слід навести приклади одних з найбільш популярних ігор які були створенні за допомогою Unity:

- Valheim
- Genshin Impact
- Ori and the Blind Forest
- Cuphead
- Pokemon Go
- Hollow Knight
- The Forest

Так наприклад, якщо взяти Genshin Impact, відповідно до Sensor Tower за два роки з вересня 2020 року до вересня 2022 року вона стала третьої за доходами в Google Play та App Store, заробивши 3.7 млрд доларів. Слід сказати що цей результат йде без врахування прибутку з ПК [7].

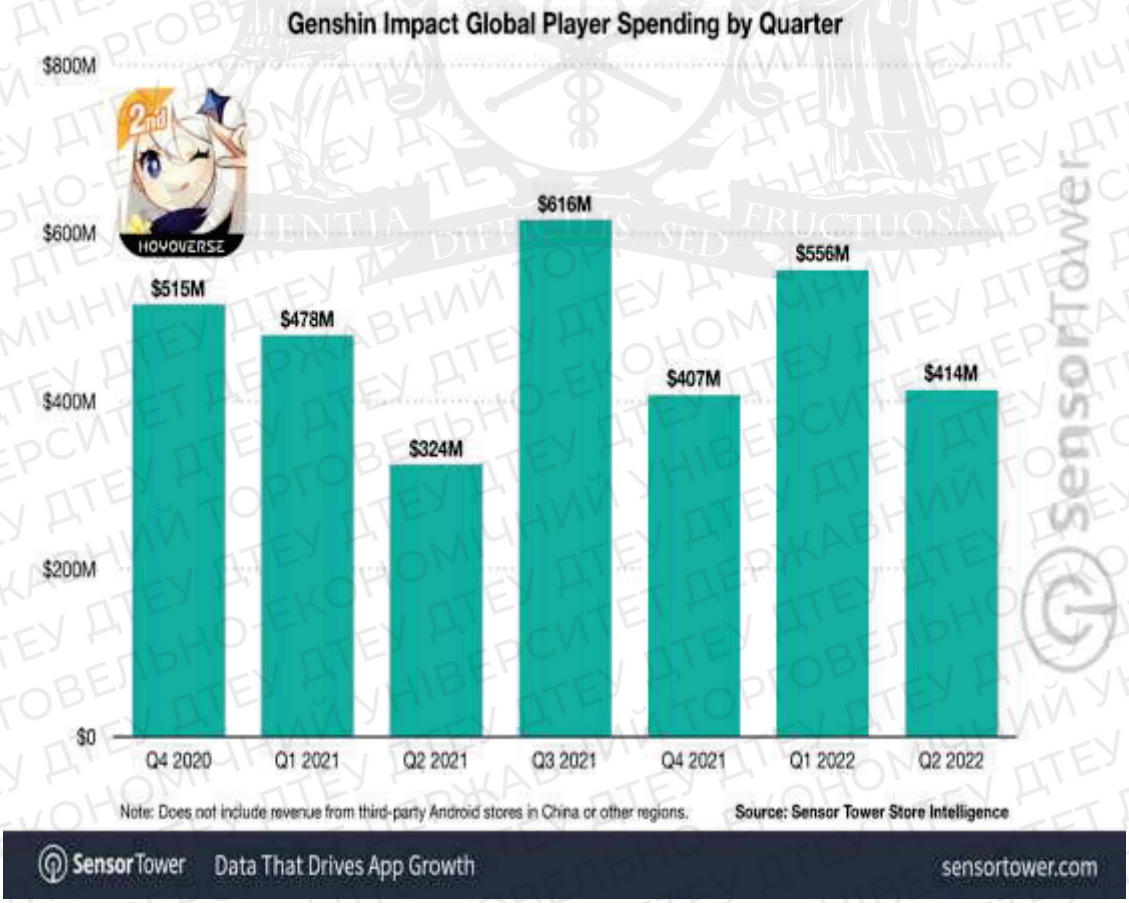


Рис.3. Genshin Impact Global Spending by Quarter [7]

Цей приклад демонструє що рушій Unity є досить конкурентоспроможним і прибутковим для створення ігор.

На сьогодні вивчення нових технологій та їх використання в навчанні стає все більш актуальним завданням в сучасному освітньому процесі, тому що використання таких технологій може допомогти підвищити якість освіти та забезпечити студентам зручний та цікавий спосіб здобуття знань. Враховуючи це, з'являється все більше програмних інструментів, спрямованих на полегшення процесу навчання та покращення ефективності навчання. Одним з таких інструментів може бути Unity, так як він має досить широкий функціонал.

Unity надає можливість створювати інтерактивні візуалізації, симуляції та ігри, що можуть бути використані в різних навчальних аспектах. Наприклад, Unity можна використовувати для створення інтерактивних уроків з геометрії або фізики, де студенти можуть досліджувати різні сценарії і спостерігати за результатами. Також Unity має широкий вибір інструментів для створення анімацій та спеціальних ефектів, що можуть бути використані для створення технічних процесів, візуалізації даних тощо.

Однак, є певні недоліки використання Unity в навчальних цілях. Наприклад, навчання розробки в Unity може бути складним і потребувати від студентів вміння програмування та розуміння математичних концепцій. Крім того, використання Unity може вимагати потужних комп'ютерів для запуску складних ігор та симуляцій. Але можна сказати що позитивні аспекти у його використанні набагато більші.

У вищих навчальних закладах ми також можемо використовувати Unity, тому як приклад ми можемо взяти і розробити гру-тест за допомогою якої студенти могли б поліпшити свої знання в зручному для них форматі і практично будь де, адже таку гру можна буде використовувати як на комп'ютері так і на телефоні. На рисунку 4 дизайн-макет такої гри.

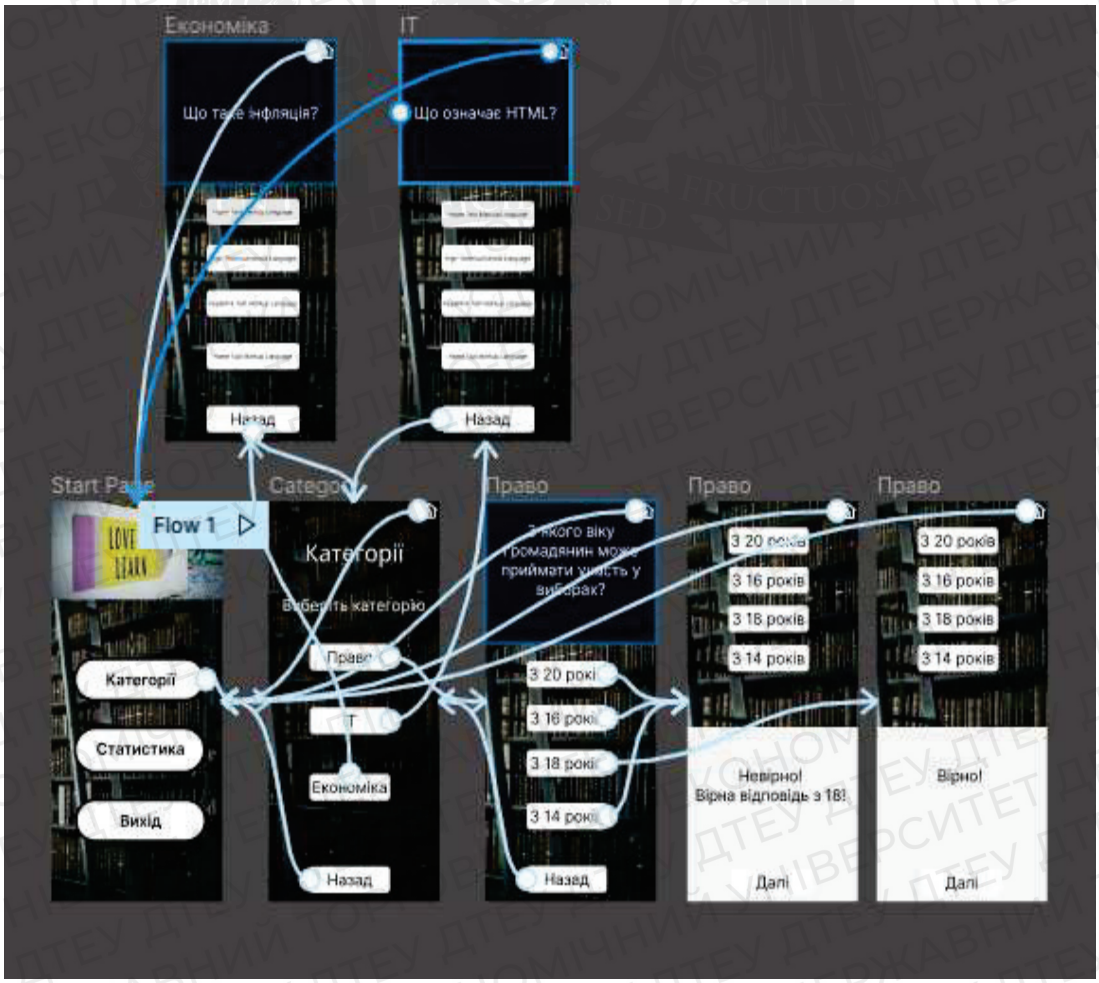


Рис. 4. Приклад гри-тесту.

Джерело: Розроблено автором в середовищі Figma (Скріншот екрану)

Висновки. У статті досліджено потребу в освітянському ігровому контенті в закладах вищої освіти та його значення для покращення навчального процесу. Розглянуто можливість використання платформи Unity в навчальних цілях, а також її функціонал, історію та структуру. Досліджено переваги, які Unity може надати у збільшенні зацікавленості учнів до навчання, зокрема забезпечення візуалізації складних понять, сприяння інтерактивному навчанню та стимулювання творчого мислення. Також висвітлено можливість застосування платформи для вивчення різноманітних галузей знань, таких як право, інформаційні технології та інші. Застосування платформи Unity дозволяє створювати інтерактивні симуляції та візуалізації складних процесів, що може допомогти в засвоєнні теорії та практики в цих галузях знань. Загалом, використання цієї платформи в навчальних закладах може сприяти покращенню якості освіти та підвищенню мотивації учнів до навчання.

Список використаних джерел

1. Eric Peckham. How Unity built the world's most popular game engine. URL: https://techcrunch.com/2019/10/17/how-unity-built-the-worlds-most-popular-game-engine/ (дата звернення 28.03.2023)
2. Jon Brodkin How Unity3D Became a Game-Development Beast. URL: https://www.dice.com/career-advice/how-unity3d-become-a-game-development-beast (дата звернення 28.03.2023)
3. Ілля Сафронов. Що таке Unity? Курс для митців. URL: https://gamedev.dou.ua/forums/topic/38048/ (дата звернення 28.03.2023)
4. Glossary Gaming Engines. URL: https://www.arm.com/glossary/gaming-engines (дата звернення 28.03.2023)
5. Joe Hocking. Unity in Action: Multiplatform Game Development in C# with Unity 5. Publisher: Manning. 2018. 400p.
6. Офіційний сайт Unity. URL: https://unity.com/solutions/multiplatform (дата звернення 29.03.2023)
7. Офіційний сайт Sensor Tower. URL https://sensortower.com/blog/genshin-impact-mobile-two-years-analysis (дата звернення 30.03.2023)
8. Lindsay Schardon_ What is Unity? – A Guide for One of the Top Game Engines. URL: https://gamedevacademy.org/what-is-unity/#What_is_Unity (дата звернення 30.03.2023)
9. Tsyrulnyk, S. (2019). Застосування технології доповненої реальності у процесі підготовки фахівців з радіоелектроніки. Електронне наукове фахове видання "відкрите освітнє е-середовище сучасного університету", 355-362. URL: https://doi.org/10.28925/2414-0325.2019s32 (дата звернення 04.04.2023)
10. Мацокін, Д. В., & Пахомова, І. М. (2020). Платформи й мобільні додатки для створення та використання контенту із технологією доповненої реальності в освітньому процесі. *Проблеми сучасної освіти*, (11), 153-160. URL: https://periodicals.karazin.ua/issuesedu/article/view/17672 (дата звернення 06.04.2023)

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А.М.

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ПЕРСОНАЛЬНИХ ДАНИХ У ВЕБ-СИСТЕМАХ

ПІХМАНЕЦЬ А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Стаття присвячена технологіям виявлення вразливостей персональних даних у веб-системах. У ній досліджуються загальні питання захисту персональних даних, такі як їх визначення, властивості, рівні захисту та забезпечення безпеки. Розглянуті різні види вразливостей персональних даних, що можуть виникати у веб-системах, а також рекомендації щодо їх виявлення та виправлення. Автори наголошують на необхідності регулярного аудиту та тестування веб-систем з метою виявлення та виправлення вразливостей персональних даних та забезпечення їх безпеки.

The article is devoted to the technologies of detecting vulnerabilities of personal data in web systems. It explores the general issues of personal data protection, such as their definition, properties, levels of protection, and security. Various types of vulnerabilities of personal data that may arise in web systems are considered, as well as recommendations for their detection and correction. The authors emphasize the need for regular auditing and testing of web systems to detect and correct vulnerabilities of personal data and ensure their security.

Актуальність статті полягає в тому, що персональні дані стали надзвичайно цінними для кіберзлочинців, що призвело до зростання кількості кібератак на веб-системи з метою викрадення персональних даних користувачів. Тому виявлення та виправлення вразливостей персональних даних у веб-системах є надзвичайно важливим завданням для забезпечення їх безпеки та захисту користувачів від можливих кібератак. Дана стаття містить детальний огляд загальних питань захисту персональних даних та різні види вразливостей персональних даних, що можуть виникати у веб-системах, а також рекомендації щодо їх виявлення та виправлення. Отже, ця стаття має велике значення для розуміння проблеми захисту персональних даних та допоможе фахівцям забезпечити безпеку веб-систем та користувачів.

Метою статті є дослідження технологій виявлення вразливостей персональних даних у веб-системах. У статті будуть проаналізовані загальні питання захисту персональних даних, види вразливостей персональних даних, що можуть виникати у веб-системах, та методи їх виявлення та виправлення. Метою статті є також надання рекомендацій фахівцям з області кібербезпеки щодо захисту веб-систем та персональних даних користувачів від можливих кібератак.

Завданнями статті є:

- Дослідження загальних питань захисту персональних даних та їх важливості для користувачів веб-систем.
- Аналіз видів вразливостей персональних даних, що можуть виникати у веб-системах, та їх характеристик.
- Вивчення технологій виявлення вразливостей персональних даних у веб-системах та методів їх виправлення.
- Надання рекомендацій фахівцям з області кібербезпеки щодо захисту веб-систем та персональних даних користувачів від можливих кібератак.

Результатом статті буде поглиблене розуміння проблем захисту персональних даних у веб-системах, а також навичок виявлення та виправлення вразливостей персональних даних.

Об'єктом статті є технології виявлення вразливостей персональних даних у веб-системах.

Результатом дослідження є опис видів вразливостей персональних даних, що можуть виникати у веб-системах, та методів їх виявлення та виправлення.

Було визначено, що вразливості персональних даних можуть виникати через недостатні заходи безпеки, недостатню аутентифікацію користувачів, недостатню захист мережевого трафіку та інші фактори. В статті було описано типи вразливостей, такі як SQL-ін'єкції, Cross-Site Scripting (XSS), CSRF (Cross-Site Request Forgery) та інші.

Для виявлення вразливостей персональних даних веб-систем було проаналізовано методи, такі як сканування портів, сканування веб-додатків, аналіз коду, тестування з використанням зломника (penetration testing) та інші. Було наголошено на важливості постійного моніторингу веб-систем та забезпечення безпеки в режимі реального часу.

У статті було описано також методи виправлення вразливостей персональних даних, такі як патчі, оновлення програмного забезпечення, внесення змін у налаштування серверів та інші.

Результатом дослідження є набір рекомендацій для фахівців з кібербезпеки щодо захисту веб-систем та персональних даних користувачів. В статті було наголошено на важливості захисту персональних даних та розглянуто кроки, які можуть бути прийняті для запобігання можливих кібератак.

Зв'язок людей через Інтернет стає все більш популярним і важливим у сучасному світі. Інтернет-сервіси і веб-сайти пропонують користувачам широкий спектр послуг і можливостей, від соціальних мереж до онлайн-банкінгу і електронної комерції. Однак, збільшення обсягу зберігання та обробки персональних даних у веб-системах призводить до збільшення ризику витоку даних і порушення приватності. У зв'язку з цим, забезпечення безпеки та конфіденційності персональних даних стає все важливішим завданням для розробників веб-систем та користувачів.

Один з способів захисту персональних даних - це виявлення вразливостей веб-систем, які можуть бути використані зловмисниками для зламування безпеки даних. Виявлення вразливостей дозволяє розробникам веб-систем вчасно виявляти та виправляти потенційні проблеми безпеки, тим самим зменшуючи ризик порушення безпеки даних. Водночас, це також дозволяє користувачам забезпечити свої дані веб-системи вищим рівнем захисту.

Отже, розробка технологій виявлення вразливостей персональних даних у веб-системах - це важлива проблема для забезпечення безпеки та конфіденційності персональних даних. Ця стаття присвячена дослідженню різних технологій виявлення вразливостей та їхнього застосування у практиці.

Поняття технології виявлення вразливостей персональних даних у веб-системах.

Технологія виявлення вразливостей персональних даних у веб-системах - це процес виявлення слабких місць у системі збору та обробки персональних даних, що можуть бути використані зловмисниками для незаконного доступу до цих даних або їх крадіжки. Ця технологія дозволяє підвищити рівень безпеки персональних даних, які збираються та обробляються веб-системами, і зменшити ризик втрати цих даних [1, 11].

Веб-системи є джерелом значної кількості персональних даних, таких як імена користувачів, адреси електронної пошти, паролі, кредитні картки, медичні записи та інші. Ці дані є дуже цінними для зловмисників, які можуть використовувати їх для зловживань, крадіжки особистості та шахрайства [2].

Один з ключових факторів, що забезпечують безпеку персональних даних у веб-системах, є виявлення та усунення вразливостей. Вразливості - це слабкі місця в системі, які можуть бути використані для отримання несанкціонованого доступу до даних. Виявлення та усунення вразливостей є важливими процесами, що допомагають зменшити ризик порушення безпеки даних у веб-системах [3, 12].

Один з типів вразливостей, що можуть бути знайдені у веб-системах, - це SQL-ін'єкція. Ця вразливість відбувається тоді, коли зловмисник може ввести SQL-запит у форму на веб-сайті, що призводить до виконання несанкціонованого запиту до бази даних. Це може

дозволити зловмиснику отримати доступ до конфіденційних даних, які зберігаються у базі даних [10].

Ще одна вразливість, що можна знайти в веб-системах - це кросс-сайт скриптінг (XSS). Ця вразливість дозволяє зловмисникам вставляти скрипти на веб-сторінки, які відвідують інші користувачі. Це може призвести до крадіжки даних, таких як паролі та кредитні картки [9].

Одним із способів виявлення уразливостей є підходи, що базуються на побудові або аналізі моделей загроз. Моделі загроз відображають сценарії або послідовності дій, які можуть призвести до порушення конфіденційності, цілісності або доступності даних. Для побудови моделей загроз часто використовуються уразливості, що вже були виявлені та вивчені, а також типові сценарії атак [4].

Іншим підходом є використання технологій аналізу коду програмного забезпечення, які можуть допомогти виявити уразливості на рівні джерела. Наприклад, статичний аналізатор коду може знайти ділянки коду, які можуть призвести до SQL-ін'єкції або переповнення буфера. Динамічні інструменти аналізу виконання програм можуть виявляти уразливості на основі взаємодії програми з оточенням [10].

З врахуванням того, що веб-системи містять багато персональної інформації, включаючи ім'я, електронну пошту, паролі, фінансову інформацію та інше, важливо забезпечити безпеку даних у веб-системах. Для цього можуть бути використані різні технології та підходи. Зараз на ринку існує багато технологій та підходів до виявлення вразливостей персональних даних у веб-системах. Ось деякі з них:

- Сканування портів: ця технологія дозволяє виявляти вразливості, пов'язані з портами веб-серверів, на яких розміщені веб-системи.
- Тестування на проникнення: ця технологія дозволяє виявляти вразливості, пов'язані зі зломом системи, з використанням спеціальних програм для тестування на проникнення.
- Відслідковування атак: цей підхід полягає в використанні спеціальних програм, які відслідковують вразливості в режимі реального часу та надсилають повідомлення про спроби злому.
- Використання SSL-шифрування: ця технологія дозволяє захистити персональні дані, передані між користувачем та веб-системою, від прослуховування.
- Використання різноманітних методів аутентифікації: цей підхід дозволяє забезпечити захист від несанкціонованого доступу до персональних даних за допомогою використання різноманітних методів аутентифікації, таких як паролі, коди підтвердження та інші.

Ще одним підходом є використання технологій тестування на проникнення, що дозволяють виявити уразливості шляхом спроб використання вразливостей програми з метою отримання доступу до конфіденційної інформації або злому системи.

Крім того, важливо пам'ятати про регулярне виконання аудиту безпеки системи, що дозволяє виявляти уразливості та проводити профілактичні заходи для їх запобігання. Аудит безпеки включає перевірку параметрів системи, конфігурацію мережі, аналіз журналів подій та інших системних параметрів [6].

Однак, незважаючи на наявність різних методів виявлення уразливостей, цей процес завжди залишається складним та вимагає великої уваги.

Методи виявлення вразливостей персональних даних у веб-системах. Існує кілька методів виявлення вразливостей персональних даних у веб-системах, такі як:

1. Аналіз коду програми. Цей метод використовується для виявлення слабких місць у коді програми, що можуть бути використані для незаконного доступу до персональних даних. Цей метод зазвичай використовується на етапі розробки програмного забезпечення [3-4, 5].

2. Тестування на проникнення. Цей метод використовується для симуляції атак на веб-систему з метою виявлення слабких місць, які можуть бути використані зловмисниками. Під час тестування на проникнення використовуються різні інструменти, які дозволяють виявляти вразливості веб-системи та проводити тестування безпеки [4, 5].

3. Аналіз безпеки мережі. Цей метод використовується для виявлення вразливостей в мережі, яка забезпечує доступ до веб-системи. Під час аналізу безпеки мережі досліджуються різні аспекти, такі як налаштування мережевих пристроїв, наявність захисних механізмів та інші параметри, які впливають на безпеку веб-системи [6, 5].

4. Моніторинг системи. Цей метод використовується для постійного відслідковування подій у веб-системі з метою виявлення незвичайної поведінки та потенційних загроз безпеці персональних даних. Моніторинг системи зазвичай проводиться за допомогою спеціальних програмних засобів, які дозволяють аналізувати журнали подій та виявляти потенційні загрози [9, 5].

Інструменти виявлення вразливостей персональних даних у веб-системах.

Існує багато інструментів, які дозволяють виявляти вразливості персональних даних у веб-системах. Деякі з них наведені нижче:

1. Nessus. Цей інструмент дозволяє проводити тестування на проникнення та виявляти вразливості веб-системи. Він містить базу даних з вразливостями та дозволяє виконувати різноманітні сканування, щоб виявляти потенційні загрози безпеці [9, 7].
2. Metasploit. Цей інструмент є потужним інструментом тестування на проникнення, який дозволяє використовувати різні експлойти для злому веб-системи. Він має велику базу даних з вразливостями та дозволяє проводити автоматизовані тестування на проникнення [1, 6, 7].
3. Burp Suite. Цей інструмент є одним з найпопулярніших інструментів для тестування на проникнення. Він має багато різноманітних функцій, таких як перехоплення трафіку, модифікація запитів та відповідей, аналіз вразливостей та інші [7].
4. OpenVAS. Цей інструмент є відкритим інструментом тестування на проникнення та виявлення вразливостей. Він має базу даних з вразливостями та дозволяє проводити сканування веб-систем для виявлення потенційних загроз безпеці [7].
5. Wireshark. Цей інструмент є програмою для аналізу мережевого трафіку. Він дозволяє перехоплювати трафік, аналізувати його та виявляти потенційні загрози безпеці [2, 7].

Заходи для запобігання вразливостей персональних даних у веб-системах

Щоб запобігти вразливостям персональних даних у веб-системах, необхідно вживати певні заходи безпеки. Нижче наведено деякі з них:

1. Шифрування даних. Важливо застосовувати шифрування для захисту персональних даних під час їх передачі через мережу. Це можна зробити за допомогою протоколів шифрування, таких як SSL або TLS.
2. Регулярні оновлення програмного забезпечення. Регулярні оновлення програмного забезпечення дозволяють виправляти виявлені вразливості та підвищувати загальний рівень безпеки веб-системи [8].
3. Використання складних паролів. Важливо використовувати складні паролі для доступу до веб-систем. Це дозволяє зменшити ризик злому пароля та неправомірного доступу до персональних даних.
4. Автентифікація та авторизація. Важливо реалізувати механізми автентифікації та авторизації для забезпечення захисту персональних даних веб-системи від неправомірного доступу.
5. Захист від SQL-ін’єкцій та інших атак. Важливо використовувати заходи для запобігання SQL-ін’єкціям та іншим типам атак, таким як валідація даних та коректна обробка введених даних [10].
6. Захист від Cross-Site Scripting (XSS). Важливо використовувати заходи для запобігання атакам XSS, таким як екранування спецсимволів та фільтрація введених даних [9].

Висновки.

Виявлення вразливостей персональних даних у веб-системах є надзвичайно важливим для забезпечення безпеки та захисту персональних даних. Існує багато інструментів для виявлення вразливостей, які дозволяють проводити тестування на проникнення та аналіз веб-

систем. Однак, на практиці, найбільш ефективним є комплексний підхід, що включає в себе використання різних інструментів та заходів безпеки.

Захист персональних даних є важливою складовою сучасного світу, оскільки захист даних є основою для захисту особистої свободи та приватності людини. Тому, забезпечення захисту персональних даних у веб-системах має важливе значення для бізнесу та суспільства в цілому.

Висновки, які можна зробити, полягають у тому, що необхідності регулярного аудиту та тестування веб-систем з метою виявлення та виправлення вразливостей персональних даних. Також важливо враховувати рекомендації та заходи безпеки при розробці та експлуатації веб-систем.

Отже, виявлення вразливостей персональних даних у веб-системах є актуальною темою, оскільки персональні дані є важливим ресурсом для бізнесу та суспільства в цілому. Для захисту персональних даних веб-систем необхідно використовувати комплексний підхід, який включає в себе використання різних інструментів та заходів безпеки. Регулярне тестування та аудит веб-систем дозволить виявляти та виправляти вразливості персональних даних та забезпечити захист цих даних від неправомірного доступу.

Список використаних джерел

1. OWASP. (2021). Top Ten Project. Retrieved from https://owasp.org/Top10/
2. NIST. (2020). Guide to Privacy Risk Assessment. Retrieved from https://www.nist.gov/publications/guide-privacy-risk-assessment
3. European Commission. (2018). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
4. Zhang, Y., Han, J., & Cheng, J. (2020). Security vulnerabilities and protection of personal information in web applications: A review. Journal of Ambient Intelligence and Humanized Computing, 11(8), 3475-3490. https://doi.org/10.1007/s12652-019-01314-6
5. Acunetix. (2021). The ultimate guide to web application security. Retrieved from https://www.acunetix.com/blog/docs/the-ultimate-guide-to-web-application-security/
6. SANS Institute. (2021). SANS Top 20 Critical Security Controls. Retrieved from https://www.sans.org/sans-top-20-critical-security-controls/
7. Zawoad, S., Hasan, R., & Hasan, M. (2019). Detecting and preventing web application security vulnerabilities: A survey. Journal of Network and Computer Applications, 138, 1-23. https://doi.org/10.1016/j.jnca.2019.04.019
8. Microsoft. (2021). Best practices for preventing information leaks. Retrieved from https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/best-practices-for-preventing-information-leaks
9. IBM Security. (2021). Data privacy and protection. Retrieved from https://www.ibm.com/security/data-privacy
10. Veracode. (2021). Web Application Security: What You Need to Know. Retrieved from https://www.veracode.com/security/web-application-security.
11. Bebeshko, B., Khorolska, K., Kotenko, N., Kharchenko, O., & Zhyrova, T. (2021). Use of neural networks for predicting cyberattacks. Paper presented at the CEUR Workshop Proceedings, , 2923 213-223. http://ceur-ws.org/Vol-2923/paper23.pdf
12. Lakhno V., Akhmetov B., Ydyryshbayeva M., Bebeshko B., Desiatko A., Khorolska K. (2021) Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In: Vasant P., Zelinka I., Weber GW. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_42

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКО Б.Т.

ЗАХИСТ ДАНИХ ПРИ ПЕРЕДАЧІ ІНФОРМАЦІЇ В КАНАЛАХ БЕЗДРОТОВОГО ЗВ'ЯЗКУ В УКРАЇНІ

ПЛОХИЙ М. 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто канали бездротового зв'язку в Україні, а також описано основні проблеми захисту передачі інформації. Розглянуто різні типи зловмисних атак, що можуть бути спрямовані на бездротові мережі, а також запропоновані різні методи захисту даних при передачі інформації в бездротових мережах в Україні.

This article examines wireless communication channels in Ukraine, and also describes the main problems of information transmission protection. Different types of malicious attacks that can be aimed at wireless networks are considered, as well as different methods of data protection during information transmission in wireless networks in Ukraine are proposed.

Актуальність. Тема захисту даних при передачі інформації в каналах бездротового зв'язку є дуже актуальною в Україні, так само як і в інших країнах світу. Зростаюча популярність бездротових технологій та зростаюча кількість пристроїв, які використовують бездротовий зв'язок, робить цю тему надзвичайно важливою. Україна, як і багато інших країн світу, залежить від бездротових мереж для забезпечення зв'язку в багатьох сферах, включаючи бізнес, медицину, громадський транспорт та інші. Проте, бездротові мережі можуть бути дуже вразливими до різних видів кібератак, таких як перехоплення даних, віруси та зловмисний код. Це може призвести до крадіжки конфіденційної інформації, в тому числі фінансових даних, медичної інформації, персональних даних та інших.

Таким чином, захист даних при передачі інформації в каналах бездротового зв'язку є надзвичайно важливою проблемою в Україні, яка потребує серйозної уваги та заходів щодо її вирішення.

Метою статті є дослідження проблем захисту даних при передачі інформації в каналах бездротового зв'язку є дуже актуальною в Україні. Також метою є спонукання до свідомого використання бездротових мереж та до виконання правил безпеки в процесі передачі даних через ці мережі.

Об'єктом дослідження є процес передачі даних через бездротові мережі і проблеми, які виникають у зв'язку з недостатнім захистом цих даних.

Предметом дослідження є способи забезпечення безпеки і захисту даних, які передаються через бездротові мережі в Україні.

Аналіз попередніх досліджень. Дослідження на тему захисту даних при передачі інформації в каналах бездротового зв'язку в Україні ведуться вже протягом кількох років. Серед українських вчених, які займалися цією темою, можна відзначити таких: Калашникова Ірина Валентинівна - доктор технічних наук, професор, провідний науковий співробітник Інституту телекомунікацій та глобальної інформації при НАН України; Губаренко Сергій Олександрович - доктор технічних наук, професор, головний науковий співробітник Інституту телекомунікацій та глобальної інформації при НАН України; Лисенко Андрій Вікторович - доктор технічних наук, професор, завідувач кафедри інформаційної безпеки та комп'ютерних технологій в Національному технічному університеті України "Київський політехнічний інститут". Деякі з них були присвячені загальним питанням захисту даних в бездротових мережах, тоді як інші були спрямовані на вивчення конкретних аспектів цієї теми. Наприклад, в дослідженні "Аналіз методів захисту бездротових мереж в Україні" автори проаналізували різні методи захисту бездротових мереж, які використовуються в Україні. У дослідженні було встановлено, що більшість бездротових мереж в Україні використовують метод WPA2 для захисту даних, але також було виявлено проблеми з безпекою деяких мереж. Інше

дослідження, "Аналіз методів криптографічного захисту даних в бездротових мережах" було спрямоване на вивчення методів криптографічного захисту даних в бездротових мережах. У дослідженні було досліджено такі методи захисту даних, як AES, DES і RSA, і було встановлено, що захист даних, які передаються через бездротові мережі, може бути підвищений, якщо використовувати сучасні методи криптографічного захисту.

Загалом, попередні дослідження підтверджують необхідність ретельного аналізу протоколів зв'язку і методів захисту для забезпечення безпеки при передачі даних в каналах бездротового зв'язку. Також дослідження підкреслюють важливість постійного вдосконалення заходів захисту даних для забезпечення безпеки від нових загроз.

Виклад основного матеріалу. Захист даних при передачі інформації в каналах бездротового зв'язку є важливою проблемою в сучасному світі, де бездротові мережі використовуються в різних сферах діяльності, включаючи бізнес, освіту, медицину та інше.

За даними Державної служби статистики України, станом на 2021 рік, понад 50% населення України користується бездротовим інтернетом. Крім того, кількість підключень до мобільного інтернету в Україні зростає щороку. За даними Асоціації операторів зв'язку України (АОЗТ), станом на кінець 2020 року, в Україні налічувалося понад 51 мільйонів підключень до мобільного інтернету, що є на 9% більше порівняно з 2019 роком.

Також, за даними Всесвітнього інтернет-ресурсу Speedtest.net, середня швидкість інтернет-з'єднання в Україні зросла в 2020 році на 23,9%, до 54,21 Мбіт/сек. З цим показником Україна займає 63 місце у світовому рейтингу.

Україна має законодавчу базу, що регулює захист персональних даних, включаючи дані, що передаються в каналах бездротового зв'язку. Основним законом в цій сфері є Закон України "Про захист персональних даних", прийнятий у 2010 році [4].

Згідно з цим законом, оператори мереж зв'язку повинні забезпечувати захист персональних даних під час їх збору, обробки та передачі. Оператори мереж повинні також забезпечувати конфіденційність та цілісність даних, що передаються в каналах бездротового зв'язку.

Національний регуляторний орган - Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ) - має право встановлювати вимоги щодо захисту персональних даних в мережах зв'язку.

Захист даних в каналах бездротового зв'язку є критичним завданням, оскільки такі мережі набувають все більшої популярності і застосовуються в багатьох галузях [5, с. 75].

Захист даних має здійснюватися, насамперед, шляхом проведення виваженої та збалансованої політики держави в електронній сфері, яка має три основні вектори:

- захист інформаційних прав і свобод людини, захист державної безпеки в електронній сфері та захист національного
- інформаційного ринку, економічних інтересів держави в електронній сфері, національних виробників інформаційної продукції [1].

Інформаційна політика інформаційного забезпечення важлива в Україні з кількох причин. По-перше, в умовах росту кількості інформації, яку ми передаємо та обробляємо, важливо мати політику, яка допоможе забезпечити належний захист цієї інформації. Захист персональних даних, конфіденційності комерційної інформації, та іншої важливої інформації є ключовим елементом інформаційної політики. По-друге, інформаційна політика допомагає управляти ризиками, пов'язаними зі зберіганням та обробкою інформації. Вона включає в себе планування заходів безпеки, оцінку ризиків, розробку політики доступу, використання технологій захисту даних, та інші заходи для забезпечення безпеки інформації. По-третє, інформаційна політика допомагає забезпечити дотримання вимог законодавства в галузі захисту інформації. Зокрема, в Україні існують закони та правила, які встановлюють вимоги щодо захисту персональних даних, конфіденційності інформації, та інших аспектів безпеки інформації. Інформаційна політика допомагає забезпечити дотримання цих вимог.

Така політика допомагає забезпечити належний захист персональних даних, управляти ризиками, та дотримуватись вимог законодавства.

Україна має основні цілі інформаційної політики інформаційного забезпечення. Основними з них є:

- захист інформаційного суверенітету держави (особливо захист національного інформаційного простору з інформаційним ресурсом і систем формування масової суспільної свідомості) в сучасних умовах глобалізації та інтернаціоналізації процесів в електронній сфері;
- рівня інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами;
- реалізацію конституційних прав і свобод громадян, суспільства і держави на інформацію [3 с. 384].

Україна має декілька типів каналів бездротового зв'язку, які використовуються для передачі інформації.

Таблиця 1.

Канали бездротового зв'язку та методи передачі інформації

Тип каналу	**Метод передачі інформації**
GSM (2G)	Частотна модуляція з фазовим зсувом (GMSK)
UMTS (3G)	Квадратурна фазова модуляція (QPSK) та 16-кувантова амплітудна модуляція (16QAM)
LTE (4G)	Квадратурна фазова модуляція (QPSK, 16QAM, 64QAM)
5G	Квадратурна фазова модуляція (QPSK, 16QAM, 64QAM) та 256QAM
Wi-Fi	Квадратурна амплітудна модуляція (QAM) та фазова модуляція (PM)
Bluetooth	Частотна гопперова модуляція (FHSS) та широкосмугова частотна модуляція (WBFM)
NFC (ближньодіапазонна комунікація)	Амплітудна модуляція (AM)
Zigbee	Частотна модуляція з фазовим зсувом (FSK) та квадратурна амплітудна модуляція (QAM)
LoRa	Розширення спектру частоти (FSK) та розширення спектру частоти з фазовим зсувом (FSK + PSK)

Wi-Fi використовує радіохвилі для передачі даних між різними пристроями. Wi-Fi є широко поширеною технологією в Україні і використовується для бездротового доступу до Інтернету, а також для бездротової мережі у побутових та офісних приміщеннях.

Bluetooth використовує радіохвилі для передачі даних між різними пристроями на невеликій відстані. Bluetooth використовується для передачі даних між мобільними пристроями, такими як смартфони, планшети, навушники, та інші пристрої.

NFC використовується для безконтактної передачі даних між двома пристроями. NFC використовується для безконтактної оплати, обміну даними між пристроями, інтерактивних рекламних кампаній та інших сценаріїв.

Zigbee використовується для передачі даних на коротких відстанях між різними пристроями. Zigbee використовується в інтернеті речей, смарт-домах, системах безпеки та інших промислових застосуваннях.

LTE використовується для передачі даних у мережах мобільного зв'язку. LTE є стандартом 4G та використовується для передачі даних на великій відстані у діапазонах частот, що належать операторам мобільного зв'язку.

5G передбачає значні покращення швидкості передачі даних, зниження затримок мережі та підвищення пропускної здатності. 5G також використовує діапазони частот, які належать операторам мобільного зв'язку, але знаходиться у процесі розгортання.

LoRaWAN використовується для підключення різних пристроїв до Інтернету речей на великі відстані. Ця технологія використовується для збір даних з датчиків віддалених пристроїв у міських та сільських областях, де інші технології можуть бути неефективними.

Важливо зазначити, що кожна з цих технологій має свої власні вимоги до захисту даних та протоколи безпеки, які повинні бути дотримані при передачі інформації в каналах бездротового зв'язку.

Згідно статистики (Рис.1) можна зробити висновок, що з кожним роком користувачів бездротової мережі стає все більше. Отже, збільшується необхідність посилювати захист передачі даних.

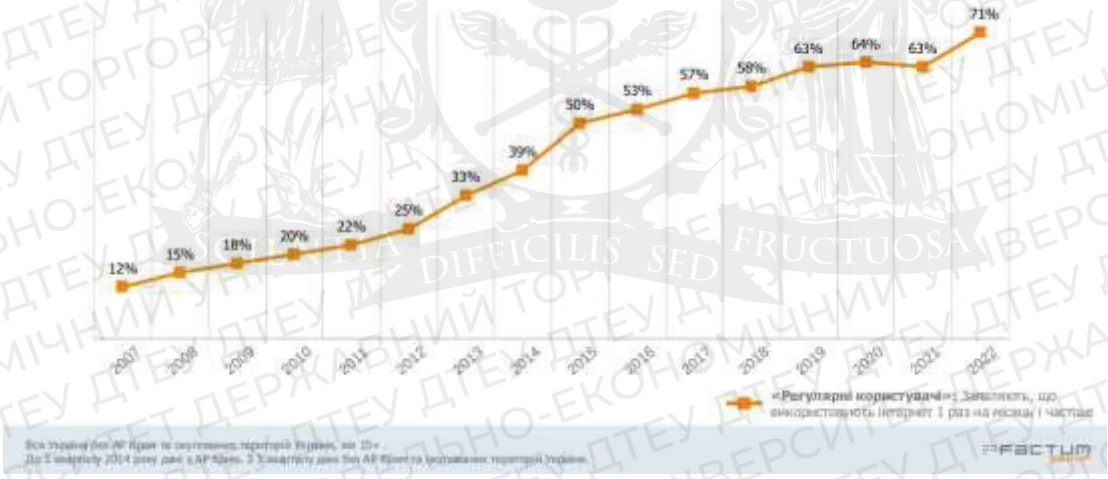


Рис. 1. Динаміка користування Інтернетом в Україні

Найбільш поширеною проблемою безпеки в бездротових мережах є недостатня захист від несанкціонованого доступу до мережі та передаваної інформації [8, с. 217].

Існує кілька ризиків та викликів, пов'язаних із захистом даних при передачі інформації в каналах бездротового зв'язку в Україні. Основні з них:

1. Небезпека перехоплення даних. При передачі інформації в каналах бездротового зв'язку, дані можуть бути перехоплені зловмисниками, які можуть використовувати ці дані для своїх злочинних цілей.
2. Недостатня захищеність мережі. Часто мережі бездротового зв'язку можуть бути недостатньо захищеними від зловмисників, які можуть використовувати ці мережі для атак на комп'ютери та інші пристрої користувачів.
3. Відсутність шифрування. Якщо передача даних не зашифрована, зловмисники можуть легко зрозуміти та використовувати ці дані.
4. Відсутність обмежень доступу. У разі відсутності обмежень доступу до бездротових мереж можуть використовуватися незаконними користувачами для зловживання.

5. Недостатній захист пристроїв. Якщо пристрої не мають достатньої захищеності, зловмисники можуть здійснювати атаки на ці пристрої та отримувати доступ до важливої інформації.

Для забезпечення захисту даних в каналах бездротового зв'язку необхідно застосовувати комплексний підхід, який включає в себе технічні та організаційні заходи [7, с. 41].

Загалом, захист даних при передачі інформації в каналах бездротового зв'язку є важливою задачею, яку необхідно вирішувати з урахуванням законодавчих вимог та використанням сучасних технічних засобів захисту даних.

Законодавчі вимоги регулюються Міністерством інформаційної політики України. Основними завданнями Міністерства інформаційної політики України є:

- забезпечення формування державної політики щодо діяльності засобів масової комунікації;
- формування стратегії інформаційної політики держави та забезпечення її дотримання;
- реалізація державної політики у сферах поширення інформації, просвітницької діяльності і використання національних інформаційних ресурсів;
- створення умов для розвитку інформаційного суспільства, а також у сфері здійснення державного нагляду (контролю) за діяльністю засобів масової комунікації незалежно від їх підпорядкування і форми власності [3].

Один із способів захисту даних в каналах бездротового зв'язку - це шифрування, яке дозволяє забезпечити конфіденційність інформації та запобігти її неправомірному доступу [6].

Існує кілька методів захисту даних при передачі інформації в каналах бездротового зв'язку в Україні:

- Використання методів ідентифікації користувачів, таких як аутентифікація по сертифікату, паролю або відбитку пальця.
- Використання фаєрволів та інших засобів захисту мережі від несанкціонованого доступу.
- Використання методів фізичного захисту, таких як зберігання пристроїв з підключенням до бездротової мережі в захищених приміщеннях або використання замків та інших засобів захисту.

Для забезпечення безпеки передачі даних в каналах бездротового зв'язку можна використовувати різні методи шифрування, такі як WPA2, WPA3, або інші стандарти шифрування даних, які відповідають вимогам безпеки. Для аутентифікації користувачів можуть використовуватись такі методи, як паролі, сертифікати, біометричні дані.

Протокол WPA2 залишається одним з найбільш популярних та ефективних методів захисту бездротових мереж. Він забезпечує високий рівень безпеки, використовуючи сильне шифрування трафіку та слабкі ключі шифрування на основі протоколу WPA2 були покращені за останні роки, але все ще існують деякі вразливості, які можуть бути використані зловмисниками для отримання доступу до бездротової мережі [11].

Протокол WPA2 (Wi-Fi Protected Access II) є одним з найбільш поширених протоколів для захисту бездротового зв'язку. Цей протокол був розроблений з метою покращення безпеки бездротових мереж Wi-Fi, що використовують стандарт 802.11. Протокол WPA2 використовує алгоритми шифрування AES (Advanced Encryption Standard) і TKIP (Temporal Key Integrity Protocol), що дозволяє забезпечити високий рівень захисту даних в бездротових мережах. Крім того, WPA2 включає в себе механізм аутентифікації IEEE 802.1X, який дозволяє перевіряти ідентифікацію користувача та дозволяти доступ до мережі тільки авторизованим користувачам. WPA2 також має певні недоліки, що можуть бути використані для атак на бездротову мережу. Наприклад, атака на перехоплення WPA2-PSK ключа, яка полягає у вилученні пароля для доступу до мережі, може бути успішною в разі використання слабкого пароля.

Однак, навіть з використанням таких протоколів, існують можливості для атак на бездротові мережі, такі як атака "чоловік-у-середині" (Man-in-the-Middle) або атака "зміни довіри" (Trust Hijacking). Тому, для забезпечення ефективного захисту даних у каналах бездротового зв'язку, необхідно використовувати додаткові заходи захисту, такі як захист від DDoS атак, захист від зловмисних програм, захист від перехоплення сигналу та інші. Крім того, важливо дотримуватись правильної конфігурації мережі та використовувати сильні паролі для доступу до мережі.

Оператори мереж зв'язку повинні також забезпечувати захист від несанкціонованого доступу до мережі, зокрема, використовуючи мережеві протоколи, такі як MAC-адреса, які обмежують доступ до мережі лише для авторизованих користувачів.

MAC-адреса є унікальним ідентифікатором мережевої карти, який використовується для передачі даних в мережах з локальним доступом. Кожна мережева карта має свій власний MAC-адрес, що дозволяє ідентифікувати її в мережі та передавати дані [10].

MAC-адреса (Media Access Control address) - це унікальний ідентифікатор, який призначений для кожного мережевого пристрою, такого як комп'ютер, смартфон, роутер або інший пристрій, який може бути підключений до мережі. MAC-адреса може бути відображена у вигляді шістнадцяткового числа, яке складається з шести пар цифр і літер, розділених двокрапкою. Кожний виробник мережевих пристроїв призначає унікальний MAC-адрес своїм пристроям. Це дозволяє мережевому обладнанню ідентифікувати та взаємодіяти з іншими пристроями у мережі. Крім того, MAC-адреса використовується для контролю доступу до мережі, наприклад, при налаштуванні списку дозволених пристроїв для підключення до Wi-Fi.

MAC-адреса працює на другому рівні моделі OSI (Data Link Layer). Вона використовується для передачі даних між двома пристроями в мережі, що знаходяться на одному рівні мережевої моделі. Наприклад, коли комп'ютер надсилає запит до сервера, він включає MAC-адресу свого мережевого адаптера, щоб інші пристрої в мережі могли відправити відповідь.

Окрім того, користувачі бездротових мереж повинні дотримуватись певних правил безпеки, таких як використання складних паролів, не використовувати мережі без авторизації, встановлення програмного забезпечення для захисту від шкідливих програм.

Дуже важливо ретельно перевіряти налаштування бездротової мережі та використовувати надійні паролі для забезпечення безпеки під час передачі даних в бездротовому режимі [9, с. 117].

Україна має національний регуляторний орган, який відповідає за розвиток та нагляд за забезпеченням ефективної та безпечної роботи телекомунікаційних послуг. Цим органом є Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ).

Національний регуляторний орган має право проводити перевірки операторів мереж зв'язку на дотримання вимог щодо захисту персональних даних, включаючи дані, що передаються в каналах бездротового зв'язку. В разі порушення вимог щодо захисту даних можуть бути застосовані адміністративні, грошові та кримінальні санкції. Проведення перевірок з боку НКРЗІ є важливим елементом забезпечення захисту персональних даних в Україні, оскільки це забезпечує виконання законодавчих вимог та відповідність міжнародним стандартам у цій сфері.

Висновки. Захист даних при передачі інформації в каналах бездротового зв'язку в Україні є важливою задачею, яка вимагає використання різноманітних технічних та організаційних заходів, включаючи дотримання законодавчих вимог та правил безпеки операторами мереж та користувачами.

Забезпечення безпеки при передачі даних в каналах бездротового зв'язку в Україні є необхідним завданням для захисту особистих даних користувачів та запобігання можливим кібератакам. Для досягнення цієї мети потрібні спільні зусилля операторів мереж та користувачів. Незахищені мережі можуть бути легко підмінені та скомпрометовані

зловмисниками, що може призвести до витоку конфіденційної інформації, викрадення особистих даних та ідентифікаційної інформації. Це може призвести до серйозних проблем з безпекою та фінансовими збитками.

Тому, щоб забезпечити безпеку та захист конфіденційної інформації, необхідно використовувати ефективні заходи безпеки в мережах Wi-Fi та інших каналах бездротового зв'язку. Це включає в себе використання протоколів шифрування, встановлення файрволів та систем ідентифікації користувачів, регулярне оновлення програмного забезпечення та інші заходи безпеки.

Важливою є розробка та впровадження нових технологій та стандартів бездротового зв'язку, які забезпечують високий рівень безпеки при передачі даних. Наприклад, розробка нових протоколів шифрування та аутентифікації, які відповідають вимогам безпеки та можуть бути використані для захисту даних під час їх передачі в каналах бездротового зв'язку. Необхідно проводити регулярні навчання та тренінги для операторів мереж зв'язку та користувачів, щоб підвищити рівень обізнаності щодо правил безпеки при використанні бездротового зв'язку та запобігти можливим кібератакам.

Захист даних при передачі інформації в каналах бездротового зв'язку в Україні є важливою та актуальною темою, яка потребує уваги та дій з боку всіх зацікавлених сторін. Тільки за спільних зусиль можна забезпечити високий рівень безпеки при використанні бездротового зв'язку та запобігти можливим кібератакам.

Список використаних джерел:

1. Корупційні ризики в діяльності державних службовців: роз'яснення міністерства юстиції України від 12.04.2011 р. [Електронний ресурс]. — Режим доступу: http://zakon5.rada.gov.ua/laws/show/n0026323-11].
2. Дзьобань О.П., Ставицька О.В. Депривaційний стан суспільства і питання національної безпеки // О.П. Дзьобань, О.В. Ставицька / Психологічні аспекти національної безпеки: Тези Другої Міжнародної науково-практичної конференції. — Львів : Львівський державний університет внутрішніх справ, 2008. — С. 70–75.
3. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю.С. Шемшученка, І.С. Чижа. — К.: ТОВ «Юридична думка», 2006. — 384 с.
4. Закону України від 1 червня 2010 року № 2297-VI «Про захист персональних даних» - Стаття 10.
5. Карпенко В.І., Захист інформації в комп'ютерних системах та мережах, Київ, 2014. 75-75с.
6. Баклан О.Ю., «Безпека інформації в комп'ютерних системах», Київ, 2013.
7. Яковенко Ю.О., «Інформаційна безпека: навчальний посібник», Київ, 2012. 41 с.
8. Козачок О.М., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. / «Безпека комп'ютерних систем: підручник» / Київ, 2015. 217 с.
9. Матяш О.В. Комп'ютерна безпека. Захист інформації. - К.: Навчальна книга, 2018. 117-120 с.
10. Джеймс Ф. Куроуз і Кіт В. Росс. Комп'ютерні мережі: підхід «зверху вниз. 7-е видання. 2019 р. 70-75 с.
11. Абдала А.С. «Безпека бездротової локальної мережі: Огляд протоколів WEP, WPA та WPA2». 2021 рік. 311-316 с.

Робота виконана під науковим керівництвом д.е.н., професора
ТОКАРЯ В.В.

РІЗНОВИДИ ГЕНЕРАТИВНИХ МОДЕЛЕЙ У ГРАФІЧНИХ ПРОГРАМАХ ДЛЯ РОБОТИ З ТРИВИМІРНОЮ ГРАФІКОЮ

ПОБЕРЕЖНИЙ В., 2м курс ФІТ ДТЕУ,
спеціальність 121“Інженерія програмного забезпечення”

У статті розглянуто певні різновиди генеративних моделей у програмі для роботи з тривимірною графікою, Blender. Зазначено переваги та недоліки використаних підходів в ході створення та стилізації 3D-об’єктів.

The article considers certain types of generative models in the software program for working with 3D-graphics, Blender. The advantages and disadvantages of the approaches used in the creation and stylization of 3D-objects are noted.

Актуальність генеративних моделей в різних сферах людської діяльності, попри очевидний попит використання в ігровій індустрії, підтверджується масштабністю у використанні даного методу для вирішення різноманітних задач. Цей підхід шириться від генеративно створених, художніх одиниць із розмаїттям візерунків у візуальному мистецтві, до додатку IKEA Place із алгоритмом створення 3D-меблів, а також вкрай актуальних на сьогодні генеративних моделей для автоматизованого розпізнавання й ідентифікації ворожої техніки. Ми маємо потребу в швидкому та ефективному створенні складних тривимірних моделей, що могли б відображати реальні об'єкти та процеси для вдалого відтворення нами віртуальних світів, відповідних до наших бажань, цілей та запитів. Як наслідок - отримуємо технологічні пропозиції в якості різновидів генеративних моделей-шаблонів для роботи з тривимірною графікою.

Традиційні методи створення 3D-моделей вимагають значних зусиль та часу. У цьому контексті можливість генеративності контенту через певні патерни стала необхідним інструментом для ефективного та швидкого створення моделей, що задовольняють високі стандарти якості. Це надає можливість автоматично генерувати складні моделі з витратою ресурсу спеціаліста лише на налаштування шаблону, що в свою чергу дозволяє зосередитися на творчому процесі та оптимізувати часові затрати.

Метою даної статті є дослідження різновидів генеративних моделей у графічній програмі для роботи з тривимірною графікою. В статті будуть розглянуті можливості програми Blender, її модифікатора Array, інтеграції бібліотеки PyTorch3D, що дають змогу зрозуміти, яким чином генеративні моделі можуть бути використані для створення 3D-моделей.

Об'єктом дослідження є різновиди генеративних моделей у графічній програмі для роботи з тривимірною графікою.

Предмет дослідження - графічна програма Blender.

Аналіз попередніх досліджень. Дослідженням генеративних моделей займались у своїх працях такі іноземні науковці: Jiajun Wu, Chengkai Zhang, Tianfan Xue, William T. Freeman, Joshua B. Tenenbaum, Lyle Regenwetter, Amin Heyrani Nobari, Faez Ahmed, Haisheng Li1, Yanping Zheng, Xiaoqun Wu, Qiang Cai1, Tianyu Zhou, Weidan Xiong, Yuki Obata, Carlos Lange, Yongsheng Ma.

Виклад основного матеріалу. Генеративні моделі можна описати як клас алгоритмів, які використовуються для створення нових даних, які вони ніколи не бачили раніше, але які можуть здатися реальними або достатньо правдоподібними для їх відтворення. Принцип роботи генеративних моделей полягає в тому, що вони використовують створені алгоритми здатні продукувати на основі існуючих даних нові. Ці алгоритми можуть включати в себе випадкові числа, математичні формули, генеративні сітки та інші техніки для створення даних.

Що робить генеративну модель об'єктів у тривимірному просторі привабливою? Вважається, що хороша генеративна модель повинна здатна створювати тривимірні об'єкти, які є одночасно різноманітними та реалістичними. Зокрема, для того, щоб тривимірні об'єкти мали варіації, генеративна модель повинна здатна виходити за рамки запам'ятовування та перекомбінування частин або елементів з попередньо визначеного репозиторію для створення нових форм; а для того, щоб об'єкти були реалістичними, у згенерованих прикладах повинні бути дрібні деталі [1].

Один з підходів, який певним чином задовольняє характеристику унікальності створених об’єктів та містить в собі частку випадковості це процедурна генерація. Концепт вдало існує та часто застосовується в іграх для вирішення проблем великих світів, майже нескінченних масштабів та відтворення унікального ігрового досвіду для гравців у таких продуктах як “No Man’s Sky”, “Minecraft”, “Don’t Starve” і багатьох інших, менш популярних ігрових одиницях.

Принцип процедурної генерації полягає в створенні певного алгоритму, який автоматично створює об’єкти що виходять із заданих раніше або випадкових параметрів [2]. У Blender відтворення алгоритму здійснюється за допомогою використання Blender’s Python API. Із використанням розділу “Scripting”, в Blender розширюються функціональні можливості створення об’єктів та їх генерації.

Створимо генеративну модель що буде абстракцією невеликого поля кубів із сіткою(7x7), алгоритм якої буде працювати перебираючи вказану розмірність(комірки), моделювати на певній відстані можливу кількість об’єктів, спираючись на вказані нами дані: розмір, перепади висоти, візуальні матеріали(колір). Створивши новий скрипт “cube.py” дамо дозвіл на викликання функцій програми за допомогою мови “Python”.

```
import bpy
import random
```

Додамо відстань що буде дозволяти генерування кубів без появи їх всередині один одного та переберемо кожне місце сітки, де міг бути створений куб.

```
spacing = 2.2
for x in range(7):
        for y in range(7):
```

Також надамо обчислення розташування поточного місця створення з генеруванням випадкової висоти.

```
location = (x * spacing, y * spacing, random.random() * 2)
```

Оголосимо куб та визначимо правило використання ним кольорів в залежності від згенерованого значення висоти(попередньо створених матеріалів жовтого та фіолетового кольорів).

```
bpy.ops.mesh.primitive_cube_add(
        size = 2,
        enter_editmode = False,
        align = 'WORLD',
        location = location,
        scale = (0.5, 0.5, 0.5))

item = bpy.context.object
if random.random() < 0.2:        item.data.materials.append(bpy.data.materials['Material.Purple'])
else: item.data.materials.append(bpy.data.materials['Material.Yellow'])
```

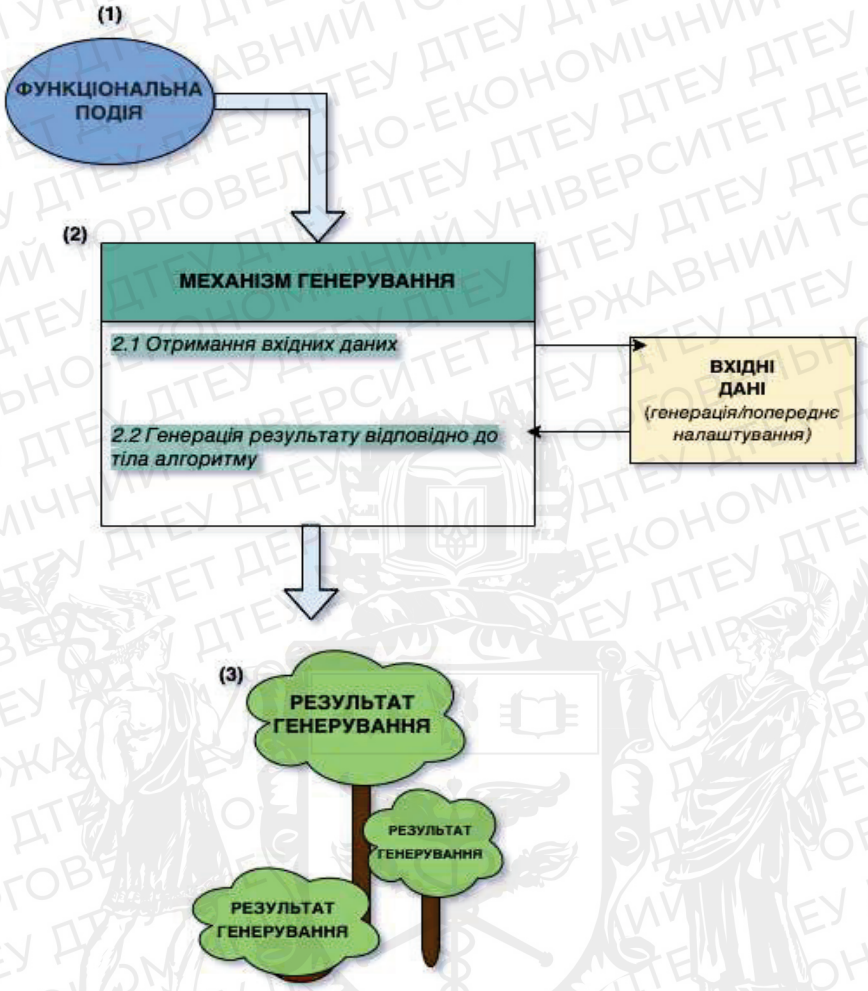


Рис. 1. Схема відпрацювання процедурної генерації

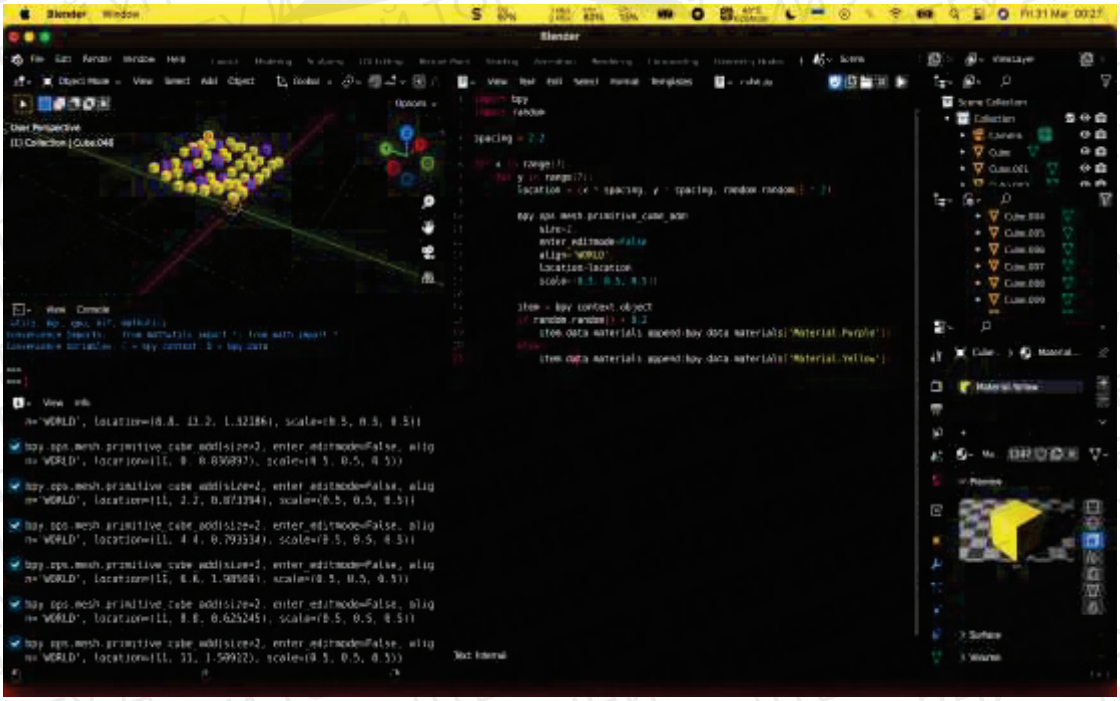


Рис. 2. Результат відпрацювання процедурної генерації

Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Дана операція дозволила згенерувати абстракцію поля кубів з певними унікальними характеристиками та параметрами, які були, в деякій мірі, попередньо визначеними. В більш змістовній, не абстрактній генеративній моделі що організована алгоритмом, повністю випадкова вибірка вхідних даних може спричинити руйнацію початкової задумки та відхилення від цілей спеціаліста який її використовує.

Отже, повна унікальність такого графічного шаблону остаточно досягається за допомогою сторонніх маніпуляцій над новоствореними об'єктами. Використання даного методу підходить для масивних даних, одноманітних скупчень об'єктів, які можуть формувати на загальному тлі навколишнього середовища. Процедурна генерація вдало застосовується для створення оточення ігрових світів, що все ж таки мають обмеження та визначені правила автоматичного генерування як по обсягу (в ролі оптимізаційних рішень відносно зменшення загального навантаження на систему, яка запускає програму в якій об'єкти моделюються), так і в законах формування самого ігрового рівня(для збереження змісту генеративної моделі).

Отримання відмінностей можливе в процесі генерування об'єктів методом параметричного моделювання. Параметричне моделювання являє собою процес з можливістю зміни форми геометрії моделі, щойно змінено значення розміру. Параметричне моделювання реалізується за допомогою коду комп'ютерного програмування, такого як сценарій для визначення розмірів і форми моделі. Такі моделі також візуалізуються в програмах для 3D-креслень, щоб нагадувати атрибути реальної поведінки оригінального проекту. Досить часто параметрична генеративна модель використовує інструменти моделювання на основі функцій для маніпулювання її атрибутами. Параметричне моделювання є альтернативою для створення точної моделі за допомогою редагування параметрів, що могло б полегшити процеси 3D-дизайнерів, наприклад, створення циліндру, застосувавши мінімальне редагування декількох параметрів (верхній діаметр, нижній діаметр і висоту), замість того, щоб вручну додавати примітиви з нуля або перетягувати їх із основної форми.

В розмаїтті інших корисних модифікатор, Blender впроваджує "Array", що дозволяє створювати масив копій базового об'єкта, де кожна копія зсувається відносно попередньої будь-яким із кількох можливих способів. Вершини в суміжних копіях можуть бути об'єднані, якщо вони знаходяться поруч, що дозволяє генерувати гладкий subdivision surface. Базові опції модифікатора дозволяють створити достатню кількість копій для розміщення в межах довжини об'єкта кривої, зазначеного в параметрі Curve, створити достатню кількість копій для розміщення в межах фіксованої довжини, заданої параметром Length та згенерувати визначену кількість копій, вказану в параметрі Count [3].

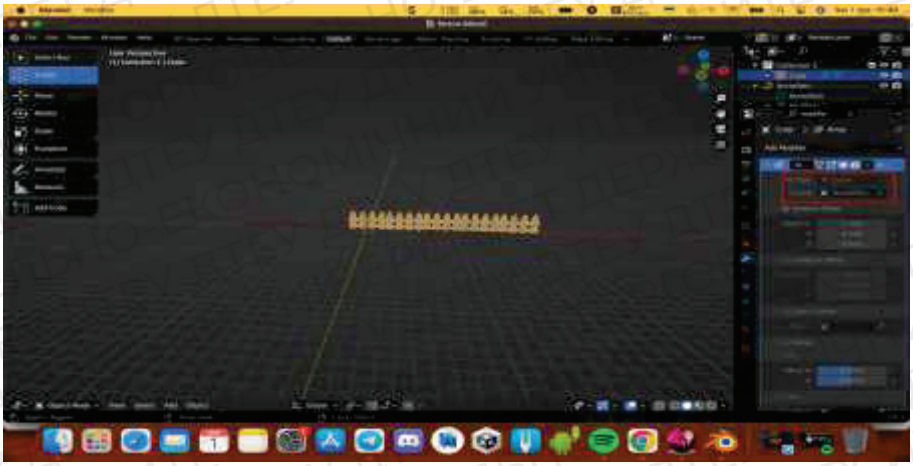


Рис. 3. Результат застосування опції "Fit Curve" в параметрі Fit Type.
Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Рис. 4. Результат застосування опції "Fit Length" в параметрі Fit Type.
Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Рис. 5. Результат застосування опції "Fixed Count" в параметрі "Fit Type".
Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Цей модифікатор може бути корисним у поєднанні з плитковими сітками для швидкого створення великих сцен, зручний для створення складних повторюваних форм. За допомогою поєднання базових опцій та реалізованих у модифікаторі параметрів зміщення(відносного, постійного та орієнтованого на інший об'єкт), така генеративна модель може слугувати альтернативою процедурному моделюванню і є більш дружньою для використання, оскільки не залучає спеціаліста до роботи з алгоритмом та відтворенням окремих правил генерації у коді. Перевагою цього методу також є ефективне використання пам'яті, оскільки цей модифікатор зберігає кількість об'єктів у пам'яті як один елемент, що зменшує обсяг виділення самої пам'яті, який використовується для збереження об'єктів.

Інший глобальний підхід, що задовольняє низку потреб відмінності та, в більшій мірі, реалістичності згенерованих моделей є генерація об'єктів за допомогою навчання глибоких нейронних мереж(GANs). GAN — це структура для генерації об'єктів за допомогою змагальної оцінки процесу, яка має глибокий вплив на розробку методів генерації в глобальному розумінні.

GAN реалізується шляхом поєднання генератора G і дискримінатор D. D класифікує, чи його вхідні дані створені чи взяті з «реальних» даних. G. фіксує розподіл даних і намагається фальсифікувати «реальні» дані, щоб змусити дискримінатора зробити неправильне судження. G і D можна розглядати як двох гравців у міні-максимальній грі, які тренуються одночасно, мета формулюється наступним чином:

$$(minG)(maxD)V(D,G) = E_{p_r}[log\ log\ D(x)] + E_{p_z}\left[log\ log\left(1 - D(G(z))\right)\right] \quad (1)$$

де p_r є розподілом даних навчального набору, і z є випадковим вектором із попереднього розподілу шуму p_z , $D(x)$ є вихідним скаляром D що вказує на можливість що x взятий з навчального набору. І G навчений будувати карту z між простором даних $G(z)$, знижує ймовірність того, що D відрізняє $G(z)$ прийшовшого з p_g а не p_r . Навчання стандартних GAN вимагає лише анотаційної інформації (правдивої чи хибної) джерела даних і оптимізовано відповідно до вихідних даних дискримінатора. Умовний GAN відноситься до додавання умов c в реальних даних, G і D . Функція c , яка може бути інформацією про клас або іншою додатковою інформацією, використовується для контролю навчання мережі. А функцію втрат можна визначити як:

$$L_D^{CGAN} = E_{p_r}[log\ log\ D(x\,|c) + E_{p_z}\left[log\ log\ \left(1 - D\big(G(c)\big)\right)\right] \quad (2)$$

Щоб вирішити проблему зникнення градієнта, яка може виникнути під час навчання, і уникнути нестабільності процесу навчання, WGAN-GP використовується для навчання всієї моделі. Наша цільова функція полягає в наступному:

$$: L_D = -E_{p_r}[D(c)] + E_{p_z}\,[D(G(z|c)] + \alpha E_{p_{\hat{x}}}[(\|\|\nabla_{\hat{x}} D(\hat{x})\|\|_2 - 1)^2] \quad (3)$$

де $p_{\hat{x}}$ позначає розподіл, який рівномірно відбирається на прямій лінії між p_r і p_g . Тут p_z визначається рівномірним розподілом по [0, 1], а втрата дискримінатора додається градієнтним штрафом з α = 10 як запропоновано в WGAN-GP.

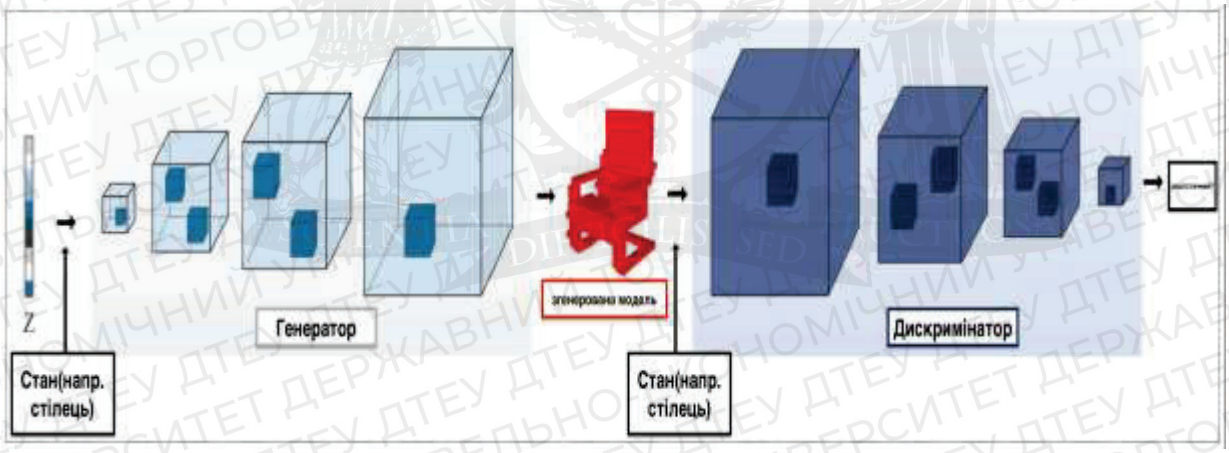


Рис. 6. Архітектура мережі генерації тривимірної моделі.
Джерело: [4]

Генератор навчений відображати низьковимірний ймовірнисний простір у 3D-моделях, щоб досліджувати тривимірне розмаїття. Моделі генеруються на основі заданих умов без довідкових зображень і моделей CAD. Дискримінатор відрізняє згенеровані 3D-моделі від «реальних» даних і повертає результат генератору для керування його навчанням [5].

У Blender можна використовувати GANs для генерації 3D-об'єктів за допомогою бібліотеки PyTorch3D. Один з прикладів застосування реалізований в навчальних матеріалах сервісу(за застосування Google Colab), що дозволяє деформувати вихідну сітку, щоб сформувати цільову сітку за допомогою функцій втрат.

Починаючи з мешу сфери, ми вивчаємо зсув до кожної вершини сітки таким чином, щоб прогнозована сітка була ближчою до цільової сітки на кожному кроці оптимізації. Щоб досягти цього, ми мінімізуємо: відстань між прогнозованою (деформованою) і цільовою сіткою(chamfer_distance). Однак лише ця мінімізація між прогнозованою та цільовою сіткою призведе до негладкої форми, в залежності від параметрів що будуть вказані(від 1.0 до 0.0).

Ми забезпечуємо плавність, додаючи регуляризатори форми до цілі. А саме додаємо: mesh_edge_length, який мінімізує довжину країв у прогнозованій сітці; mesh_normal_consistency, який забезпечує узгодженість між нормалями сусідніх граней; mesh_laplacian_smoothing, який є регуляризатором. Після встановлення та імпортування в середовище Blender необхідних модулів torch, torchvision та pytorch3d. Завантажуємо файл розширення obj(примітив дельфіна) і створюємо сітку об'єкту та читаємо її(за допомогою load_obj). Далі ми нормалізуємо масштаб і центруємо цільову сітку, щоб вона помістилася в сфері радіуса 1 з центром (0,0,0). Також масштабування по центру буде використано, щоб привести прогнозовану сітку до початкового центру та масштабу. Потрібно зауважити, що нормалізація цільової сітки прискорює оптимізацію, але не є обов'язковою саме в цьому процесі, тож ми лише створюємо структуру сітки для цільової сітки та ініціалізуємо вихідну форму як сферу радіуса 1. При візуалізації вихідної та цільової сітки необхідно відбирати зразки рівномірно з поверхні сітки, яку ми використовуємо. Наступним етапом є цикл оптимізації в якому ми деформуємо вихідну сітку, зміщуючи його вершини. В ньому форма параметрів деформації дорівнює загальній кількості вершин у src_mesh. В оптимізаторі, ми будемо мати параметри кількості кроків оптимізації, вагу для chamfer loss, mesh edge loss, mesh normal consistency та mesh laplacian smoothing, сума якої пізніше надасть нам графічне розуміння загальних втрат. Вкажемо період побудови для загальних втрат та ініціалізуємо оптимізатор, після чого приступаємо до деформування сітки, де нам необхідно вибрати 5 тисяч точок із поверхні кожної сітки та порівняти два набори точок, обчислюючи chamfer loss. Друкуємо та зберігаємо витрати, проводимо побудову сітки та запускаємо раніше організований оптимізаційний процес. Відобразимо наші втрати.

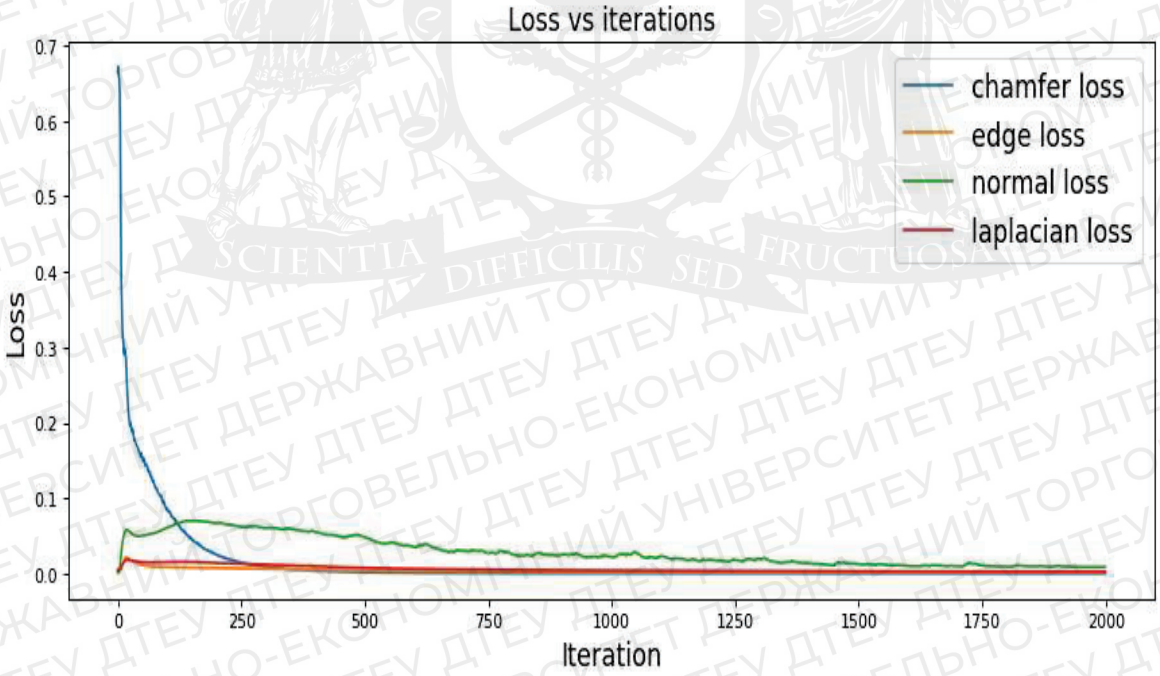


Рис. 7. Загальні ітераційні втрати
Джерело: скрін з екрану

Збережемо нашу створену сітку, де виберемо вершини і грані остаточної прогнозованої сітки, нормалізуємо масштаб до вихідного цільового розміру та кінцево фіксуємо спрогнозований меш(знову за допомогою save_obj) [6]. Отримаємо наступний результат в якому видно мінімальну розбіжність відносно заданого оригіналу.

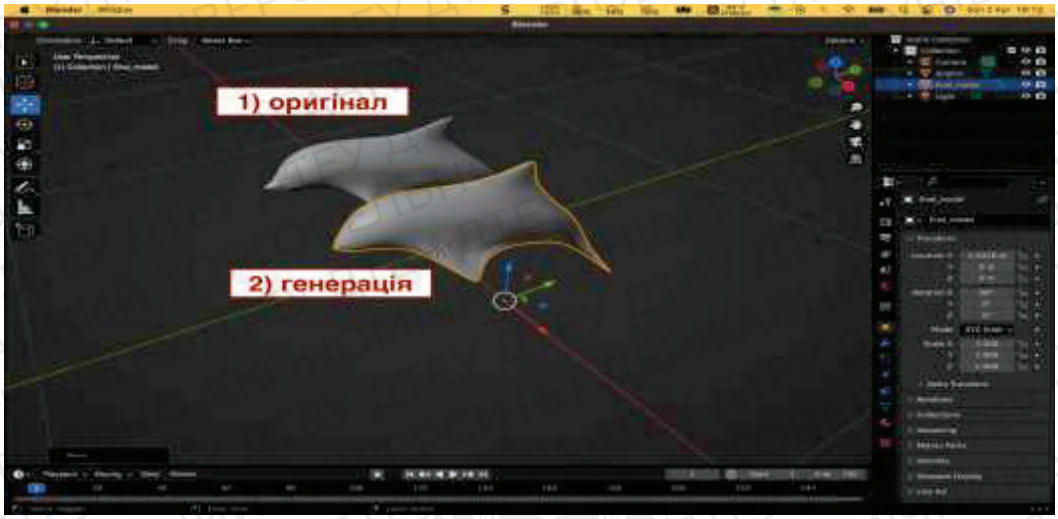


Рис. 8. Вхідний та вихідний результати
Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Якщо поекспериментувати із вказанням значень втрат, та мінімізувати їх(w_edge = 0.0, w_normal = 0.00, w_laplacian = 0.0) згенерований об’єкт буде менш відповідним до більш реалістичного оригіналу, та матиме явні пошкодження генерації, що не зовсім задовольняє початкову ціль.

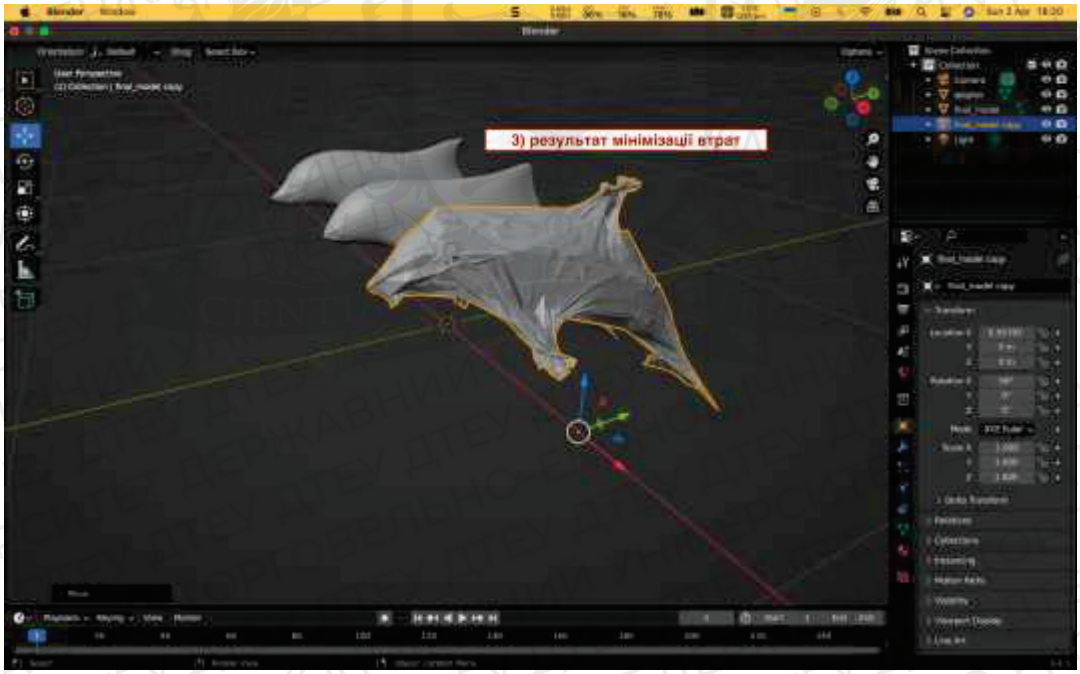


Рис. 9. Результат генерації з мінімізацією втрат.
Джерело: розроблено автором в середовищі Blender(скрін з екрану)

Отже, за допомогою навчальних матеріалів PyTorch можемо завантажувати сітку з файлу розширення obj, ініціалізувати структуру даних під назвою «Сітки», налаштувати цикл оптимізації та використовувати чотири різні функції втрати сітки для корекції генерування об’єкту з наявною можливістю інтегрування бібліотеки в робочий процес програми Blender.

Деформування вихідної сітки для створення цільової сітки за допомогою функцій втрат в є важливим кроком у генерації нових 3D-об'єктів. Цей процес дозволяє створити моделі з більш складною формою та більш точною геометрією. PyTorch3D надає функції втрат, які дозволяють точно порівняти дві сітки та визначити, наскільки вони відрізняються. Це важливо при генерації нових сіток, оскільки нейронна мережа повинна навчатися генерувати нові

об'єкти, які якомога більше схожі на зразок. Використання функцій втрат дозволяє зменшити відстань між зразком та сгенерованою моделлю, що покращує якість генерації. Отже, використання даної бібліотеки в Blender для деформування вихідної сітки за допомогою функцій втрат допомагає в створенні та використанні генеративних моделей, оскільки дозволяє точніше генерувати нові 3D-об'єкти з більш складною формою та більш точною геометрією, що може вирішити низку специфічних задач в яких загальні рішення процедурної та параметричної генерації не підходять.

Висновки. Процедурна генерація дозволяє швидко створювати багато різних варіантів об'єктів, проте, деталізація та відтворення складних форм може бути обмеженою. Параметричне генерування дає більшу свободу у створенні складних форм та деталізації об'єктів. Однак, процес налаштування параметрів може бути трудомістким. 3D GANs є найбільш складною генеративною моделлю для використання, але вона може створювати найбільш подібні до натренованих об'єкти, допомагаючи у вирішенні проблем, де є вкрай важливо отримати максимальну реалістичність та деталізацію. Такі моделі здебільшого доцільно використовувати у візуалізації архітектурних проектів, інтерактивних додатків, на виробництві та промисловості, технологіях доповненої чи віртуальної реальності. Дана генеративна модель може бути дорогим процесом, що потребує великої кількості ресурсів, обчислювальної потужності та є менш гнучкою у порівнянні з іншими методами генерації. У загальному, використання різних видів генеративних моделей в Blender вимагає певної кількості досвіду, технічної компетентності та має свої переваги, а їх недоліки реально мінімізувати правильно визначивши цілі та задачі проєкту, де вони беруться у використання.

Список використаних джерел

1. Jiajun Wu, Chengkai Zhang, Tianfan Xue, William T. Freeman, Joshua B. Tenenbaum. (2017). Learning a Probabilistic Latent Space of Object Shapes via 3D Generative-Adversarial Modeling \\ Режим доступу: https://arxiv.org/pdf/1610.07584.pdf (останнє звернення 05.04.2023)
2. Tianyu Zhou, Weidan Xiong, Yuki Obata, Carlos Lange, Yongsheng Ma. (2022). Digital Manufacturing: Chapter 2. Digital product design and engineering analysis techniques \\ Режим доступу: http://surl.li/gqykf (останнє звернення 05.04.2023)
3. Матеріали некомерційної організації Blender Foundation. (2023). Offical Blender Documentation. Generative Modeling: Array Modifier \\ Режим доступу: http://surl.li/gqyko (останнє звернення 05.04.2023)
4. Haisheng Li1, Yanping Zheng, Xiaoqun Wu, Qiang Cai1. (2019). 3D Model Generation and Reconstruction Using Conditional Generative Adversarial Network: “Figure 1” \\ Режим доступу: http://surl.li/gqykx (останнє звернення 05.04.2023)
5. Haisheng Li1, Yanping Zheng, Xiaoqun Wu, Qiang Cai1. (2019). 3D Model Generation and Reconstruction Using Conditional Generative Adversarial Network \\ Режим доступу: https://www.atlantis-press.com/journals/ijcis/125911591/view#bibr-R9 (останнє звернення 05.04.2023)
6. Матеріали компанії Meta Platform Inc. (2023). Deform a source mesh to form a target mesh using 3D loss functions \\ Режим доступу: https://pytorch3d.org/tutorials/deform_source_mesh_to_target_mesh (останнє звернення 05.04.2023)
7. Lyle Regenwetter, Amin Heyrani Nobari, Faez Ahmed. (2022). Deep Generative Models in Engineering Design: A Review \\ Режим доступу: https://decode.mit.edu/assets/papers/2022_regenwetter_review.pdf (останнє звернення 05.04.2023)

Робота виконана під науковим керівництвом доцента кафедри інженерії програмного забезпечення та кібербезпеки,
ДЕСЯТКО А. М.

СУЧАСНІ ТЕНДЕНЦІЇ АВТОМАТИЗАЦІЇ УПРАВЛІНСЬКОГО І НАВЧАЛЬНОГО ПРОЦЕСІВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

ПОЛІГУШКО А., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Стаття присвячена дослідженню тенденцій застосування інформаційних технологій у сфері управління та навчання в закладах вищої освіти. Основна увага приділяється автоматизації процесів управління та навчання, опису сучасних тенденцій та переваг, недоліків та перспектив розвитку в даній сфері.

Article is dedicated to the study of trends in the use of information technology in the management and education in higher education institutions. The main focus is on the automation of management and learning processes, describing current trends and advantages, disadvantages, and prospects for development in this field.

Актуальність. У світі інформаційних технологій дедалі більше уваги приділяється автоматизації процесів в усіх сферах, включаючи навчальну. Розвиток нових інформаційних технологій та платформ для онлайн-навчання надає можливості для ефективнішого та більш доступного навчання. Автоматизація також має свої недоліки та виклики, такі як проблеми з кібербезпекою та приватністю, недостатня взаємодія між викладачами та студентами тощо, тому, вивчення сучасних тенденцій та перспектив розвитку автоматизації управлінських та навчальних процесів у закладах вищої освіти є важливим та актуальним.

Автоматизація управлінських та навчальних процесів є актуальною темою у сучасному світі. Вона дозволяє підвищити ефективність управління та навчання, зменшити витрати на робочу силу та матеріальні ресурси. У цій статті розглянуто сучасні тенденції автоматизації управлінського та навчального процесів у закладах вищої освіти.

Метою статті є дослідити сучасні тенденції автоматизації управлінських та навчальних процесів у закладах вищої освіти, проаналізувати переваги та недоліки використання інформаційних технологій в цій сфері, а також визначити перспективи розвитку автоматизації управління та навчання в закладах вищої освіти.

Завдання статті полягає у:

- Огляді літературних джерел та аналізі публікацій, що стосуються автоматизації управлінських та навчальних процесів у закладах вищої освіти.
- Аналізі переваг та недоліків використання інформаційних технологій в сфері управління та навчання в закладах вищої освіти.
- Визначенні перспектив розвитку автоматизації управління та навчання в закладах вищої освіти.
- Формулюванні рекомендацій щодо вдосконалення процесів автоматизації управління та навчання в закладах вищої освіти на основі результатів дослідження.

Об'єктом дослідження є тенденції застосування інформаційних технологій у сфері управління та навчання в закладах вищої освіти.

Предметом дослідження є автоматизація процесів управління та навчання, опис сучасних тенденцій та перспектив розвитку в даній сфері, а також переваги та недоліки використання інформаційних технологій у навчальному процесі.

Застосування інформаційних технологій є необхідним елементом автоматизації управлінських процесів в закладах вищої освіти. Завдяки використанню різноманітних програмних засобів та інформаційних систем, можливо автоматизувати процеси збору, обробки та збереження інформації, що дозволяє значно полегшити роботу управлінських структур та підвищити їх ефективність.

Управління в закладах вищої освіти є складним та багатогранним процесом, що вимагає відповідального підходу та використання сучасних технологій. Однією з таких технологій є автоматизація управлінських процесів. Вона дозволяє забезпечити швидку та точну обробку даних, встановити систему контролю за виконанням завдань, зменшити кількість помилок та підвищити рівень ефективності управління.

Одним із прикладів автоматизації управління є використання спеціальних програмних засобів для управління процесом навчання. Такі засоби дозволяють створювати та зберігати розклад занять, контролювати відвідуваність та успішність студентів, встановлювати дедлайни для здачі робіт та інші завдання.

Впровадження інформаційних технологій в освітній сектор може стати каталізатором для інноваційних методів викладання та навчання, підвищення залученості студентів і підвищення академічної успішності [1, с. 48].

Один із прикладів застосування інформаційних технологій у процесі управління в закладах вищої освіти - це використання систем електронного документообігу. Це дозволяє значно спростити процес обміну документами між управлінськими структурами, забезпечити швидкий доступ до необхідної інформації та підвищити рівень безпеки збереження даних.

Також інформаційні технології дозволяють автоматизувати процеси планування та контролю навчального процесу, що дозволяє ефективно використовувати ресурси закладу та забезпечити якісну підготовку студентів. Наприклад, системи електронного навчання дають можливість вчителям та студентам здійснювати навчання та контроль знань в режимі онлайн, що значно полегшує процес навчання та контролює успішність студентів.

Отже, використання інформаційних технологій є важливим елементом автоматизації управління в закладах вищої освіти, що сприяє поліпшенню якості управління та підвищенню ефективності процесів.

В сучасних умовах університети активно використовують електронні системи управління навчальним процесом. Ці системи забезпечують можливість зберігання, обробки та аналізу великих обсягів інформації, що сприяє покращенню якості навчання та оптимізації роботи викладачів.

Однією з найбільш поширених електронних систем управління навчальним процесом є Learning Management System (LMS), такою, наприклад, є «МІА: Освіта». Ця система дозволяє студентам отримувати доступ до електронних матеріалів, викладачам - контролювати навчальний процес та взаємодіяти зі студентами в онлайн-режимі, а адміністрації - контролювати виконання навчальних планів та аналізувати результати навчання.

Крім того, електронні системи управління навчальним процесом дозволяють автоматизувати процеси планування навчальних курсів, відстежування виконання навчальних завдань та оцінювання студентів. Це дозволяє покращити якість навчання, сприяє більш ефективному використанню часу викладачів та студентів, а також зменшує кількість адміністративної роботи, пов'язаної з управлінням навчальним процесом.

Використання електронних систем управління навчальним процесом дозволяє створити зручні інструменти для спілкування між викладачами та студентами, а також дозволяє відстежувати прогрес студентів та реагувати на їх потреби у реальному часі. Крім того, використання цих систем дозволяє забезпечити доступ до навчальних матеріалів з будь-якого пристрою.

Інтеграція ІКТ у сектор освіти призвела до появи нових методів викладання та навчання, таких як змішане навчання та перевернуті класи, які довели свою ефективність у підвищенні успішності учнів [2, с.31].

Автоматизація процесу планування та контролю за навчальним процесом є ще однією важливою тенденцією в управлінні вищою освітою. Застосування інформаційних технологій в цих процесах дозволяє збільшити ефективність та точність планування, зменшити кількість помилок та зайвих витрат часу. Це дозволяє викладачам та адміністраторам швидко та зручно створювати розклади занять, враховуючи наявність аудиторій, наявність викладачів, потреби студентів тощо.

Автоматизація процесу контролю за виконанням навчальних планів дозволяє вчителям швидко та ефективно відстежувати успішність студентів, виявляти проблеми та надавати необхідну допомогу. Крім того, це дозволяє студентам отримувати негайний зворотний зв'язок щодо їхньої успішності та відразу коригувати свої дії.

Контроль за навчальним процесом також може бути автоматизованим. Системи автоматичної оцінки та відстеження успішності студентів можуть використовувати алгоритми для оцінки та аналізу навчальних результатів, що дозволяє підвищити якість контролю та сприяти розвитку індивідуальних методів навчання.

Наприклад, такі програмні засоби як "Moodle" або "Microsoft Teams" дозволяють викладачам створювати та організовувати віртуальні класи, додавати в них матеріали, викладати завдання та оцінювати роботи студентів. Також ці системи можуть бути інтегровані з електронними бібліотеками та іншими базами даних для забезпечення швидкого та зручного доступу до інформації.

Такі інструменти як автоматизовані інформаційні системи, програмне забезпечення та електронні платформи дозволяють забезпечити високий рівень якості навчання та ефективність управління в закладах вищої освіти. Вони дозволяють прискорити процес навчання, забезпечити доступ до великої кількості інформації та зменшити затрати на управління навчальним процесом.

Електронні підручники та навчальні посібники є однією з основних тенденцій використання інформаційних технологій у навчальному процесі в закладах вищої освіти. Ці матеріали можуть містити різноманітні форми навчання, такі як відеоуроки, аудіозаписи, інтерактивні тести та завдання, що дозволяє студентам засвоювати матеріал на свій власний темп та з будь-якого місця з доступом до Інтернету. Крім того, електронні підручники та навчальні посібники можуть бути оновлені та доповнені в режимі онлайн, що дозволяє студентам мати доступ до актуальної та свіжої інформації. Такі матеріали можуть бути дуже корисні для дистанційного навчання, яке стало набагато популярнішим в останні роки. Також електронні підручники та навчальні посібники можуть бути інтегровані з іншими електронними системами управління навчальним процесом, такими як система електронного навчання чи система автоматизованого тестування, що забезпечує більш зручну та ефективну організацію навчального процесу для студентів та викладачів.

Ще однією з тенденцій використання інформаційних технологій у навчальному процесі є використання відеоуроків та вебінарів. Це особливо актуально у зв'язку з пандемією COVID і російсько-українською війною, через що заклади освіти були вимушені перейти на дистанційну форму навчання. Відеоуроки є корисним інструментом для вивчення нового матеріалу або поглиблення знань в певній темі. Вони можуть бути розміщені на різних платформах, таких як YouTube, або спеціалізовані платформи навчання, які надають доступ до відеоуроків від провідних фахівців у різних галузях, таких як Coursera або Prometheus. Вебінари - це живі онлайн-презентації, під час яких провідний експерт пояснює певну тему та відповідає на запитання учасників. Вони можуть бути проведені за допомогою різних платформ, таких як Zoom, Google Meeting, Microsoft Teams, або спеціалізовані платформи для вебінарів. Відеоуроки та вебінари забезпечують доступ до навчання з будь-якого місця, де є доступ до Інтернету. Крім того, вони можуть бути записані та використані в якості додаткового матеріалу для підготовки до екзаменів або інших важливих подій [3, с. 4].

Автоматизація навчальних процесів у закладах вищої освіти також є важливою тенденцією сучасності. Вона дозволяє підвищити ефективність навчання та забезпечити кращу якість знань студентів. Однією з основних переваг автоматизації навчальних процесів є можливість забезпечення індивідуального підходу до кожного студента, використовуючи різноманітні методи навчання.

Одним із прикладів автоматизації навчальних процесів є використання електронних курсів та онлайн-навчання. Це дозволяє студентам вивчати матеріал у своєму темпі та в зручний для них час, а також забезпечує доступ до багатої бази знань та матеріалів. Крім того, автоматизація дозволяє студентам брати участь у віртуальних лекціях та семінарах,

спілкуватися з викладачами та іншими студентами, що забезпечує взаємодію та обмін досвідом.

Електронні підручники також стали невід'ємною частиною у навчальному процесі. Основне його завдання на етапі отримання нових знань полягає у залученні в процес навчання інших, ніж традиційний підручник, можливостей людського мозку, зокрема, слухової та емоційної пам'яті, з метою максимального полегшення розуміння та запам'ятовування навчального матеріалу. Текстова частина супроводжується численними перехресними посиланнями, що дають змогу скоротити час пошуку необхідної інформації. Такий підручник може мати аудіо- або відеозапис лекторського викладу матеріалу. Але використання електронних підручників дозволяє формувати тільки певний рівень знань у студентів, тоді як формування практичних навичок і компетенцій в такому випадку є неможливим [3, с. 45].

Електронні системи контролю знань є ще однією тенденцією використання інформаційних технологій у навчальному процесі. Ці системи можуть бути використані для проведення онлайн тестування, оцінювання завдань, роботи з електронними тестами та іншими методами оцінювання знань студентів.

Електронні системи контролю знань дозволяють автоматизувати процес оцінювання та зберігання результатів, що полегшує роботу викладачів та адміністраторів навчального закладу. Крім того, такі системи можуть надавати додаткові можливості для аналізу даних про навчальні досягнення студентів та виявлення проблемних місць у навчанні.

Також електронні системи контролю знань можуть бути інтегровані з іншими електронними системами управління навчальним процесом, що дозволяє створювати єдину інформаційну систему для ефективного управління навчальним процесом в цілому.

Застосування інформаційних технологій управління та навчання має ряд переваг, серед яких:

- Збільшення ефективності та швидкості обробки інформації. Інформаційні технології дозволяють обробляти інформацію значно швидше, ніж людина, що забезпечує швидке та точне прийняття рішень.
- Зменшення витрат на паперову документацію та збереження даних. Інформаційні системи дозволяють зберігати та обробляти інформацію в електронному вигляді, що зменшує витрати на паперову документацію та зберігання даних.
- Забезпечення доступності інформації для користувачів. Інформаційні технології дозволяють швидко та легко забезпечити доступ до інформації користувачам, що робить процес управління та навчання більш доступним та ефективним.
- Підвищення якості навчання та забезпечення індивідуального підходу. Застосування інформаційних технологій дозволяє забезпечити індивідуальний підхід до навчання, забезпечити різноманітність форм та методів навчання, що підвищує якість навчання.
- Можливість доступу до навчального матеріалу у будь-який час та в будь-якому місці[4, с. 27]

Хоча автоматизація управлінських та навчальних процесів має багато переваг, вона також має певні недоліки, які слід враховувати:

- Високі витрати на розробку та впровадження інформаційних систем. Розробка, підтримка та оновлення програмного забезпечення можуть бути дуже витратними, особливо для закладів з обмеженим бюджетом.
- Залежність від технології. Якщо система автоматизації навчання відмовляє, це може призвести до затримок у проведенні занять та оцінюванні.
- Віддаленість від людського контакту. Деякі студенти можуть відчувати віддаленість від викладачів та інших студентів, особливо якщо навчання відбувається виключно в онлайн-форматі.

- Використання застарілих технологій. Багато закладів вищої освіти мають застарілу техніку та програмне забезпечення, що може призвести до проблем зі сумісністю та ефективністю автоматизованих систем.

Сучасні технології дозволяють значно полегшити та покращити управління та навчання в закладах вищої освіти. Автоматизація управлінських та навчальних процесів дозволяє забезпечити ефективну та точну обробку даних, зменшити кількість помилок та витрат на робочу силу, а також підвищити якість навчання та знань студентів.

Однак, разом з тим, автоматизація вимагає розробки та впровадження спеціальних програмних засобів, а також може призвести до зниження кількості робочих місць, що пов'язані з управлінням та навчанням.

Крім того, важливо враховувати етичні аспекти впровадження автоматизації в управління та навчання. Наприклад, необхідно забезпечувати конфіденційність даних студентів та викладачів, а також забезпечувати право на вільний вибір методів навчання та доступ до необхідної інформації для всіх студентів.

Загалом, можна зробити висновок, що автоматизація управлінських та навчальних процесів є важливою тенденцією сучасності в закладах вищої освіти. Вона дозволяє підвищити ефективність та точність управління, зменшити кількість помилок та витрат на робочу силу, а також підвищити якість навчання та знань студентів. Однак, важливо розробляти нові напрями роботи та навчання для спеціалістів, які займаються автоматизацією, та враховувати етичні аспекти впровадження автоматизації в управління та навчання.

Висновки. У результаті дослідження було встановлено, що автоматизація управлінських та навчальних процесів є актуальною та перспективною тенденцією в сучасній вищій освіті. Застосування інформаційних технологій дозволяє знизити витрати часу та зусиль на адміністративні та рутинні процеси, підвищити якість та ефективність управління, забезпечити доступність та якість навчання.

Проте, також було виявлено недоліки та обмеження в застосуванні інформаційних технологій, такі як можливість технічних збоїв та проблем з безпекою даних, необхідність кваліфікованого персоналу та відповідних знань та навичок користування цими технологіями.

Отже, можна стверджувати, що використання інформаційних технологій у вищій освіті є невід'ємною складовою сучасного навчально-виховного процесу, який підвищує якість та ефективність навчання, а також сприяє покращенню управління закладами вищої освіти.

Список використаних джерел

1. Осадчий В.В., Осадча К.П. Сучасні реалії і тенденції розвитку інформаційно-комунікаційних технологій в освіті. Інформаційні технології і засоби навчання, Т. 48, № 4, с. 47–57, 2015.
2. Іванова С. Застосування сучасних технологій та інноваційних методів навчання у вищих навчальних закладах. Інформаційні технології та Інтернет у навчальному процесі та наукових дослідженнях: навч. посіб. – 2018. – 295с.
3. Полянська А.С. Круглий стіл: Інноваційні методи викладання у вищій школі: обмін досвідом та кращі практики. – Івано-Франківськ: ІФНТУНГ, 2020. – 192 с.
4. Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми: збірник. наук. пр. – Вип. 42. – Київ-Вінниця: ТОВ фірма «Планер», 2015. – 471 с.

Робота виконана під науковим керівництвом к.е.н, старшого викладача
ФРАНЧУК Т.М.

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ ДЛЯ ПРОГНОЗУВАННЯ ЗАПІЗНЕНЬ ГРОМАДСЬКОГО ТРАНСПОРТУ

ПОНОМАРЕНКО С., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У сучасному світі, де технології розвиваються зі швидкістю світла, застосування машинного навчання в різних галузях стає все більш поширеним. Однією з таких галузей є транспортна індустрія, де машинне навчання може бути застосоване для вдосконалення різних процесів, включаючи прогнозування запізнень громадського транспорту. У статті досліджено, як компанія Google використовує технології машинного навчання для прогнозування запізнень громадського транспорту. Розглянуто методи збору та аналізу даних про рух транспорту та алгоритми машинного навчання, які використовуються для прогнозування запізнень.

In the modern world, where technologies are developing at the speed of light, the use of machine learning in various industries is becoming increasingly widespread. One of such industries is the transportation industry, where machine learning can be applied to improve various processes, including predicting delays in public transportation. In this article, we will investigate how Google uses machine learning technologies to predict delays in public transportation. We will examine the methods of collecting and analyzing data on transportation movement and the machine learning algorithms used to predict delays.

Актуальність. У сучасному світі, технології змінюють наш спосіб життя та роботи. Застосування машинного навчання в різних галузях стає все більш поширеним і дозволяє вдосконалювати процеси та забезпечувати високу точність в прийнятті рішень. Однією з таких галузей є транспортна індустрія, де застосування машинного навчання може значно покращити якість послуг та зменшити час очікування для пасажирів громадського транспорту.

Прогнозування запізнень громадського транспорту є важливою задачею для забезпечення точності та своєчасності. Технології машинного навчання, такі як нейронні мережі, можуть допомогти вирішувати цю задачу, збираючи та аналізуючи великі обсяги даних про рух транспорту та прогнозуючи його рух у майбутньому.

Однією з компаній, яка застосовує машинне навчання для прогнозування запізнень громадського транспорту, є Google. Компанія використовує свою платформу Google Maps для збору даних про рух транспорту та аналізує їх, використовуючи алгоритми машинного навчання для прогнозування запізнень. Це дозволяє пасажирам більш точно планувати свій маршрут, а компаніям громадського транспорту покращити ефективність свого руху та забезпечити більш якісне обслуговування.

Прогнозування запізнень громадського транспорту - це лише один із прикладів того, як машинне навчання може забезпечити більш точну та швидку обробку даних у різних галузях.

Метою статті є дослідження того, як компанія Google використовує машинне навчання для прогнозування запізнень громадського транспорту, зокрема методів збору та аналізу даних про рух транспорту та алгоритмів машинного навчання, що застосовуються для прогнозування запізнень.

Об'єктом дослідження є застосування технологій машинного навчання компанією Google для прогнозування запізнень громадського транспорту.

Предмет дослідження - використання технологій машинного навчання для прогнозування запізнень громадського транспорту.

Аналіз попередніх досліджень у сфері прогнозування запізнень громадського транспорту засвідчив, що вже було проведено досить багато досліджень з використанням

різноманітних методів машинного навчання, таких як регресійна аналітика, дерева рішень, нейронні мережі тощо.

Серед таких робіт були:

- Дослідження "Real-Time Prediction of Bus Arrival Time using Automatic Vehicle Location (AVL) Data" (2011) виконане Dr. Yanfeng Ouyang, Department of Civil and Environmental Engineering, University of Illinois at Urbana-Champaign.
- "Predicting Transit Bus Arrival/Departure Times using General Transit Feed Specification Data" (2014) виконане Rongjie Yu, Alireza Khani, та Wei (David) Fan, Department of Computer Science, Florida State University.
- "Real-time estimation of public transport vehicle arrival times at a stop using GPS data" (2017) виконане Sunil Kumar Jha, Rajesh Kumar Tiwari, та Shweta Singh, Department of Electronics and Communication Engineering, Birla Institute of Technology.
- "Improving Public Transit System Performance through Real-Time Data Analysis" (2019) виконане Ashish Kumar та Upendra Kumar, Department of Electrical [2].

Ці дослідження охоплюють різні аспекти прогнозування запізнень громадського транспорту, від використання GPS-даних та дані з загальних транспортних розкладів до застосування методів машинного навчання та глибинного навчання. Результати цих досліджень можуть допомогти покращити ефективність транспортних систем та зробити їх більш доступними для користувачів.

Виклад основного матеріалу. Машинне навчання - це підхід до розв'язання задач штучного інтелекту, що дозволяє комп'ютерам вчитися з досвіду та покращувати свої результати з часом. В контексті прогнозування запізнень громадського транспорту, машинне навчання може бути використане для створення моделей, що будуть прогнозувати час прибуття транспортного засобу на зупинку на основі даних про його рух та інші фактори, такі як трафік та погодні умови.

- Навчання з учителем (supervised learning) - один зі способів машинного навчання, в ході якого випробувана система примусово навчається за допомогою наявної множини прикладів «стимул-реакція» з метою визначення «реакції» для «стимулів», які не належать до наявної множини прикладів.
- Навчання без учителя (unsupervised learning) - моделі навчаються на основі непозначених даних, у яких відомі лише вхідні дані. Цей тип навчання використовується для задач кластеризації, зменшення розмірності та виявлення аномалій, де не відомі бажані вихідні дані.
- Підсилення (reinforcement learning) - це галузь машинного навчання, натхнена біхевіористською психологією, що вивчає питання про те, які дії (англ. actions) повинні виконувати програмні агенти в певному середовищі (англ. environment) задля максимізації деякого уявлення про сукупну винагороду (англ. reward).
- Передбачення (predictive learning) - моделі навчаються на основі зіставлення вхідних даних зі збереженими прикладами, щоб передбачати результати для нових вхідних даних. Цей тип навчання використовується для задач прогнозування, де необхідно передбачити майбутні значення на основі історичних даних. [3].

У випадку прогнозування запізнень громадського руху, застосовуються моделі машинного навчання з учителем, в яких вхідними даними є інформація про попередні маршрути та дані GPS, а вихідними даними - прогнозований час прибуття транспортного засобу на зупинку. На основі цих даних моделі навчаються передбачати, наскільки може затриматися рух транспорту на наступних зупинках, що допомагає уникнути запізнень та зробити транспортну систему більш ефективною. [4, с. 3-4].

За останні кілька років прогрес у галузі штучного інтелекту та машинного навчання дозволяє застосовувати їх для покращення ефективності транспортних систем. Один з головних проблем громадського транспорту - це запізнення рейсів, що може призвести до нестачі часу та стресу для пасажирів. Google зайнялася проблемою запізнення громадського

транспорту та розробила модель прогнозування запізнення автобусів з високою точністю, що базується на машинному навчанні та статистичних методах.

Сотні мільйонів людей у всьому світі щоденно користуються громадським транспортом для своєї робочої дороги, і понад половина всіх поїздок здійснюється автобусами. При зростанні міст у всьому світі, пасажири хочуть знати, коли очікувати затримки, особливо на автобусних маршрутах, які часто зупиняються у заторах. Хоча напрямки громадського транспорту, що надає Google Maps, інформуються багатьма транспортними агентствами, які надають дані в режимі реального часу, є багато агентств, які не можуть надати ці дані через технічні та ресурсні обмеження. Сьогодні Google Maps представив систему передбачення затримок на автобусні маршрути, що включає прогнозування затримок автобусів в сотнях міст у всьому світі, починаючи від Атланти до Загреба, до Стамбула, до Маніли та інших міст. Це поліпшує точність визначення часу громадського транспорту для понад шістдесяти мільйонів людей.

Приклад поїздки автобусом в середу після обіду у Сіднеї. Фактичний рух автобуса (синій) відстає від опублікованого розкладу (чорний) на декілька хвилин. Швидкості руху автомобільного трафіку (червоний) впливають на автобус, наприклад, сповільнення на відстані 2000 метрів, але довга зупинка на відстані 800 метрів суттєво уповільнює рух автобуса порівняно з автомобілем. [1].

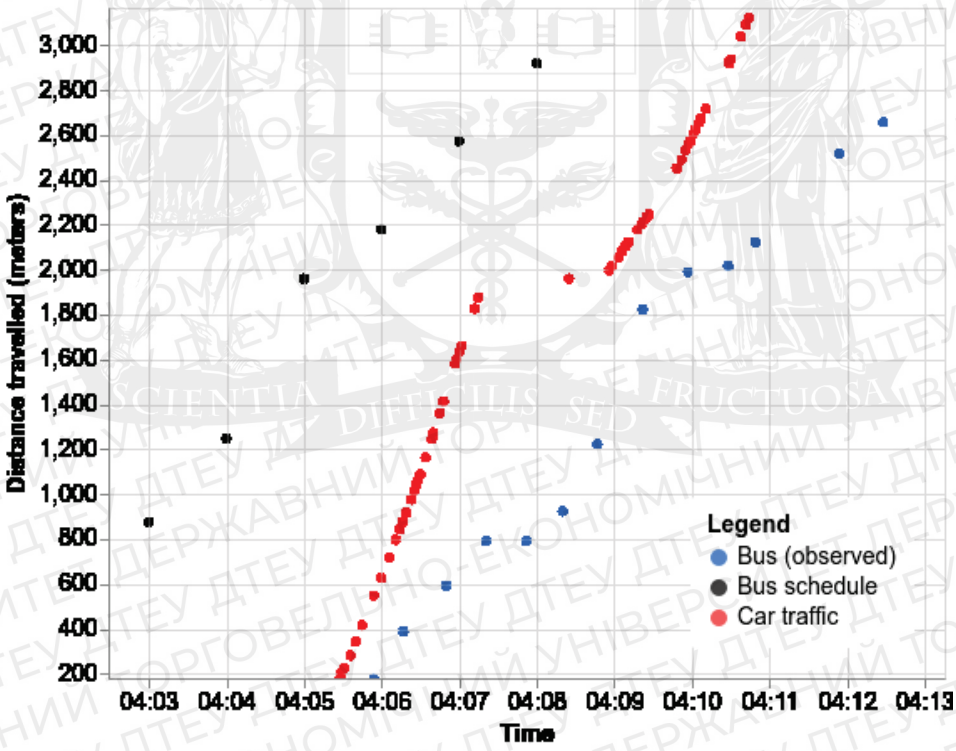


Рис. 1. Графік пройденої відстані в залежності від часу [1]

Для розробки моделі використовували тренувальні дані з послідовностей позицій автобусів в часі, які надходили з потоків реального часу транспортних агенцій, і відповідно до цього зв'язували їх зі швидкістю руху автомобільного трафіку на маршруті автобуса під час подорожі. Модель поділяється на послідовні одиниці часу, які відповідають кожному шматочку часової лінії автобуса, і кожна одиниця передбачає тривалість. Пара прилеглих спостережень зазвичай охоплює багато одиниць, через нерегулярність звітності, швидкість руху автобусів і короткі відрізки доріг і зупинок. Ця структура добре підходить для нейронних послідовних моделей, подібних до тих, що останнім часом успішно застосовуються у мовному процесінгу, машинному перекладі тощо. Ця модель є простішою. Кожна одиниця передбачає свою тривалість незалежно, а кінцевий результат - сума передбачень для кожної одиниці. У

відміну від багатьох послідовних моделей, ця модель не потребує вивчення комбінування виходів одиниць та передачі стану через послідовність одиниць. Замість цього, структура послідовності дозволяє навчити моделі тривалості окремих одиниць та оптимізувати "лінійну систему", де кожна спостережена траєкторія присвоює загальну тривалість сумі багатьох одиниць, які вона охоплює.

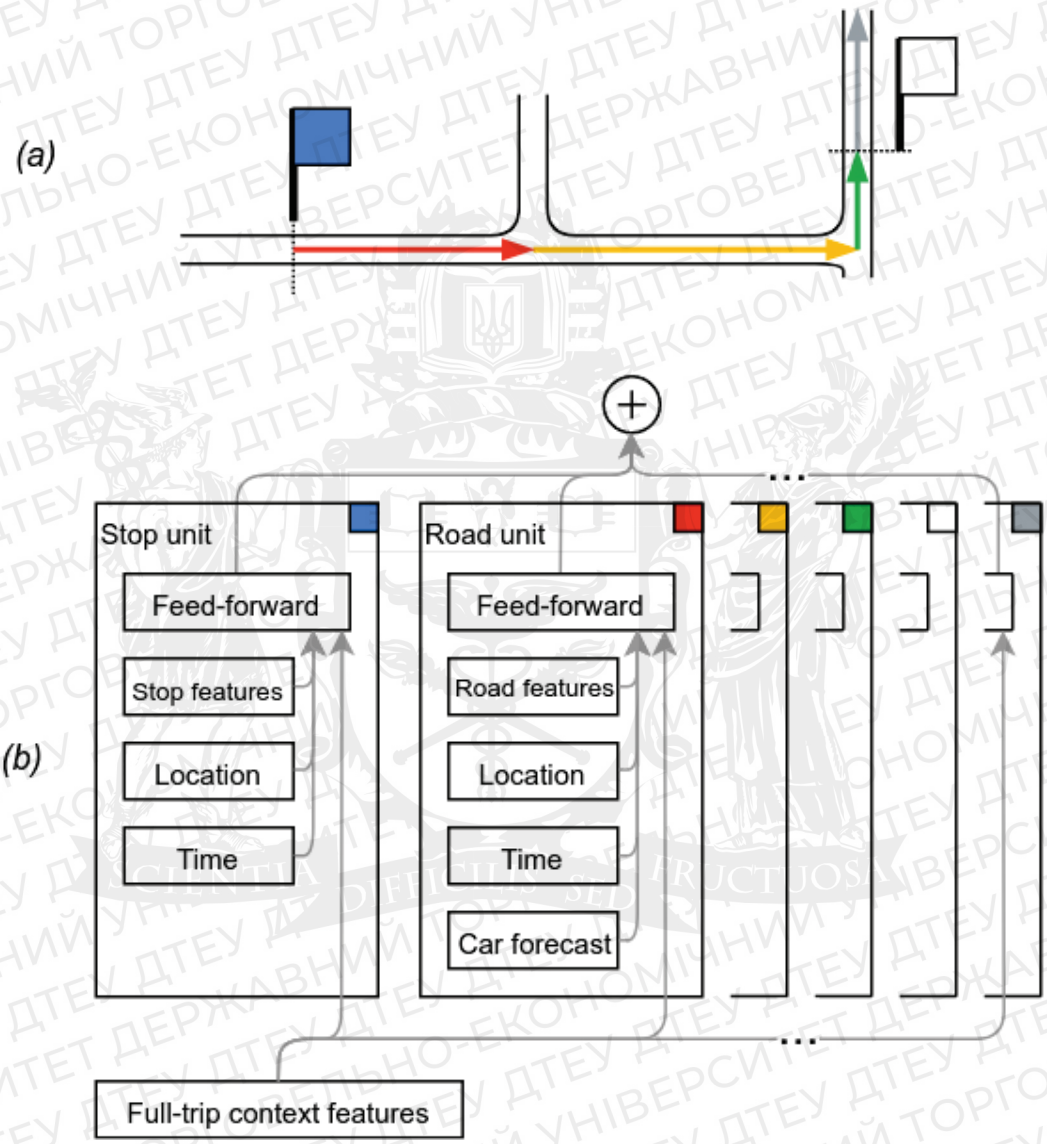


Рис. 2. Щоб змоделювати поїздку на автобусі (а), яка починається з синьої зупинки, модель (б) додає прогнози затримок з одиниці часової шкали для синьої зупинки, трьох ділянок дороги, білої зупинки тощо. [1]

З використанням комбінації даних про час, відстань та окремі події, штучний інтелект дозволяє Google надавати передбачення, не потребуючи розкладів автобусів, які надаються громадськими транспортними організаціями.

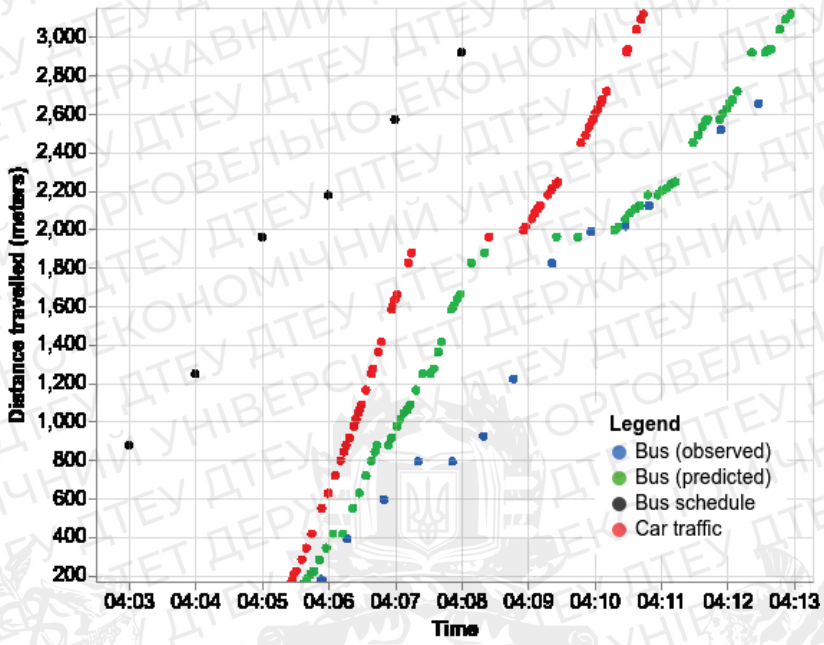


Рис. 3. Розклад автобусів(зелений колір). [1]

Для створення моделі збирається інформація про місцезнаходження автобусів від транспортних компаній для тренувальних даних, після чого вона узгоджується зі швидкістю руху автомобілів на маршруті. Потім послідовна модель враховує кожну очікувану зупинку або зниження швидкості, таку як час та відстань, необхідні для того, щоб автобус зменшив швидкість та зупинився біля зупинки.

Висновки. У цій статті машинне навчання використовується для покращення прогнозування тривалості подорожі автобусом. Розроблена модель використовує дані про позиції автобуса з часом, щоб передбачити тривалість подорожі на кожній вулиці та зупинці. Використання машинного навчання дозволило розробникам покращити точність прогнозування із залученням додаткових даних, які не були доступні раніше. Крім того, використання машинного навчання забезпечило більш гнучкий і ефективний підхід до прогнозування тривалості подорожі, що може бути корисним для підвищення якості громадського транспорту та зручності пасажирів.

Список використаних джерел

1. Google AI Blog: "Improving Public Transit Accessibility with Machine Learning"\\ Режим доступу:https://ai.googleblog.com/2019/08/improving-public-transit-accessibility.html

2. IEEE Xplore: "Enhancing the Accessibility of Public Transit with Machine Learning"\\ Режим доступу:https://ieeexplore.ieee.org/document/8683749

3. Cornell University Library: "Enhancing the Accessibility of Public Transit with Machine Learning"\\ Режим доступу: https://arxiv.org/abs/1908.02325

4. Матвійчук А., Шестопалов О. Машинне навчання. Загальний підхід. Київ: Видавництво "Ліра", 2019. ISBN 978-966-376-673-7.

Робота виконана під науковим керівництвом канд. пед. наук, доцента КОТЕНКО Н.О.

РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗВ'ЯЗУВАННЯ ЗАДАЧ ВИЩОЇ МАТЕМАТИКИ НА ОСНОВІ АНАЛІЗУ СУЧАСНИХ ПЛАТФОРМ

ПРИХОДЬКО М., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У даній статті розглянуто сучасні платформи для розв'язання задач вищої математики. Проведено аналіз та порівняння платформ за різними критеріями, такими як доступність для мобільних пристроїв та людей з обмеженими можливостями. Було виявлено, що жодна з платформ не є ідеальною, але кожна має свої переваги та недоліки. На основі отриманих результатів, було сформульовано рекомендації щодо кращих практик розробки програмного забезпечення для розв'язування задач вищої математики. Також було проаналізовано основні функції, які повинна містити така платформа.

This article discusses modern platforms for solving higher mathematics problems. An analysis and comparison of the platforms was carried out according to various criteria, such as accessibility for mobile devices and people with disabilities. It was found that neither platform is perfect, but each has its advantages and disadvantages. Based on the obtained results, recommendations were formulated regarding the best practices of software development for solving higher mathematics problems. It also analyzed the main functions that such a platform should contain.

Актуальність. Використання програмного забезпечення для розв'язування математичних задач набуває все більшої популярності в сучасному світі. Університети та наукові установи активно використовують цей вид ПЗ для вирішення складних завдань вищої математики. Крім того, таке програмне забезпечення знайшло застосування в різних індустріях, таких як фінансові послуги, технічний дизайн та інженерія.

Отже, дана стаття є актуальною для широкого кола читачів, які зацікавлені в використанні програмного забезпечення для розв'язування математичних завдань різної складності, а також для тих, хто цікавиться розвитком технологій у цьому напрямку.

Метою статті є аналіз існуючих платформ для розв’язування задач вищої математики та визначення їхніх переваг та недоліків з урахуванням вимог щодо доступності для різних категорій користувачів, зокрема для людей з особливими потребами.

Об’єктом дослідження є платформи для розв’язування задач вищої математики.

Завдання статті полягає в наступному:

– проаналізувати різні платформи для розв’язування задач вищої математики, їх функціональні можливості, цільову аудиторію та особливості роботи з ними;
– визначити переваги та недоліки кожної платформи з урахуванням вимог щодо доступності для різних категорій користувачів;
– визначити найкращі практики для розробки програмного забезпечення для розв’язування задач вищої математики з урахуванням виявлених недоліків платформ, які використовуються на сьогоднішній день.

Математика - це наука, яка вимагає від людей великої уваги та точності. Розв'язування складних математичних задач може бути дуже важким завданням, тому багато людей звертаються до різних платформ, щоб отримати допомогу в цьому процесі. На сьогоднішній день існує багато різних інструментів, які допомагають вирішувати майже будь-яку математичну задачу.

Для початку, проаналізуємо декілька існуючих платформ для розв'язування задач з вищої математики, дослідимо їхні можливості та обмеження.

Платформа Wolfram Mathematica є однією з найбільш відомих платформ для розв'язування складних математичних задач. Вона розроблена для студентів, науковців, інженерів та інших фахівців, які працюють з математикою та комп'ютерними науками.

Wolfram Mathematica забезпечує розв'язування різних задач, включаючи чисельне та символьне розв'язування, обробку даних, графічний аналіз та візуалізацію. Це робить його одним з найпопулярніших інструментів для розв’язування математичних задач. Крім того, Wolfram Mathematica має інтегровані засоби для символьних обчислень, диференціальних рівнянь та функціонального аналізу [1].

Незважаючи на те, що Wolfram Mathematica є потужним інструментом для розв'язування складних математичних задач, він має деякі обмеження, які можуть зменшувати його ефективність і корисність для користувачів.

Одним з найбільших недоліків є висока вартість платформи, що робить її недоступною для багатьох користувачів, особливо студентів та молодих дослідників. Крім того, інтерфейс платформи може бути складним для користувачів, які не мають достатнього досвіду в роботі з програмним забезпеченням.

MATLAB - це платформа для зручної роботи з математичними обчисленнями та програмуванням, яка дозволяє розв'язувати системи рівнянь та інші математичні завдання. Ця платформа є однією з найбільш використовуваних у наукових дослідженнях, інженерному проектуванні та в інших областях, пов'язаних з математикою та комп'ютерними науками.

Однією з основних переваг MATLAB є його зручний інтерфейс, що дозволяє легко розробляти та запускати програми з математичними обчисленнями, використовуючи вбудовані функції та інструменти. Крім того, MATLAB має велику кількість додаткових пакетів та інструментів, що дозволяють розширювати його можливості та використовувати його для різних цілей, включаючи обробку сигналів, обробку зображень, моделювання та багато іншого.

MATLAB також має можливості для роботи з великими обсягами даних та високопродуктивними обчислювальними задачами, що робить його ідеальним вибором для багатьох наукових та інженерних досліджень [2].

Однак, MATLAB має деякі недоліки, включаючи високу вартість ліцензій, що може стати перешкодою для користувачів з обмеженим бюджетом. Крім того, MATLAB може бути менш ефективним для деяких видів математичних обчислень порівняно з іншими інструментами.

Mathway – це платформа для розв'язування математичних задач, яка спеціалізується на розв'язуванні алгебраїчних, геометричних та інших математичних задач. Вона має багато корисних функцій, таких як відображення кроків розв'язання задачі, що допомагає користувачам зрозуміти процес розв'язання та покращити свої знання в математиці.

Mathway доступна на комп'ютерах та мобільних пристроях, що дозволяє користувачам користуватися платформою в будь-який час та в будь-якому місці. Також, Mathway може бути корисною для людей з обмеженими можливостями, оскільки має можливість користування платформою для людей з вадами зору та іншими особливостями.

Одним з недоліків Mathway є те, що для доступу до деяких функцій потрібна платна підписка. Крім того, Mathway не має такої великої кількості функцій, які є у більш широких платформ, таких як Wolfram Mathematica або MATLAB.

GeoGebra - це додаток, який дозволяє користувачам виконувати різноманітні математичні операції та розв'язувати задачі. Додаток має широкий спектр функцій, включаючи побудову графіків, обчислення похідних та інтегралів, розв'язування рівнянь та систем рівнянь. Окрім цього, GeoGebra дозволяє створювати власні математичні об'єкти та використовувати їх для розв'язання задач. Додаток має інтуїтивний інтерфейс та може бути використаний як на комп'ютерах, так і на мобільних пристроях [3].

GeoGebra має певну адаптацію для людей з особливими потребами. На сайті платформи є можливість вибрати темний фон та збільшити розмір тексту, що полегшує користування додатком людям з вадами зору. Крім того, GeoGebra має функцію для збільшення об'єктів на

екрані, що полегшує роботу людям зі зниженою здатністю до моторики. Також, є можливість додавання аудіо та відео-коментарів до створених математичних об'єктів, що забезпечує доступність для людей зі зниженим слухом. Хоча додаток не має спеціальної адаптації для людей з особливими потребами, деякі функції додатку можуть бути корисними для покращення доступності для людей з вадами зору, слуху та моторики.

Однак, GeoGebra має деякі недоліки. Наприклад, додаток може бути менш ефективним для розв'язання деяких складних математичних задач, порівняно з іншими спеціалізованими додатками. Крім того, для користувачів без попереднього досвіду з математикою, додаток може бути складним у використанні.

Загалом, GeoGebra є корисним додатком для студентів, викладачів та інших користувачів, які займаються математикою. Додаток має великий потенціал для використання в навчанні та розв'язуванні різних математичних задач.

Symbolab є потужною та зручною платформою для розв'язування математичних задач, яка надає користувачам широкий спектр інструментів. Зокрема, на платформі можна відображати графіки, обчислювати похідні та інтеграли, розв'язувати системи рівнянь та багато іншого. Крім того, Symbolab має спеціалізовані функції для розв'язування складних математичних задач, таких як вирішення лінійних диференціальних рівнянь [4]. Платформа доступна на комп'ютерах та мобільних пристроях.

Однак, Symbolab має свої недоліки. Розв'язання деяких складних математичних задач може бути менш точним порівняно з альтернативними платформами. Також важко використовувати платформу для користувачів, які не мають попереднього досвіду з математикою та розв'язанням математичних задач. Важливо зазначити, що Symbolab не адаптована для користувачів з особливими потребами, такими як вади зору та інші обмеження.

Після дослідження різних платформ для розв'язування задач вищої математики, можна зробити висновок, що жодна з них не є ідеальною. Деякі з них забезпечують велику кількість функцій, але не є дуже зручними у використанні, інші мають простий інтерфейс, але не мають достатньої функціональності.

Також не всі проаналізовані платформи можуть бути зручними для користувачів з вадами зору або нездатністю користуватися мишкою. Для забезпечення максимальної доступності для користувачів з різними потребами, важливо враховувати їхні потреби при розробці інтерфейсів платформ.

В результаті дослідження були визначені кращі практики, які можуть бути використані для розробки ПЗ для розв'язування задач вищої математики. Основними критеріями, на які варто звернути увагу при створенні програмного забезпечення для розв'язування задач вищої математики, є:

- Зручність використання. Програмне забезпечення має бути легким у використанні та зрозумілим для користувача, незалежно від його рівня кваліфікації.
- Функціональність та можливості. Програмне забезпечення повинно мати всі необхідні можливості для розв'язування задач вищої математики.
- Доступність для мобільних гаджетів. Зважаючи на те, що все більше користувачів використовують мобільні пристрої, важливо забезпечити доступність програмного забезпечення на таких пристроях.
- Доступність для людей з особливими потребами. Програмне забезпечення повинно бути зручним у використанні для людей з різними вадами зору та здатності до користування мишкою.

Основною метою розробки програмного забезпечення є спрощення роботи з вищою математикою для користувачів різного рівня знань та кваліфікації. Пріоритетом є простота та зрозумілість інтерфейсу, які дозволять користувачам швидко та ефективно вирішувати математичні задачі. Важливими аспектами є надійність та точність отримуваних результатів, а також підтримка користувачів та допомога у вирішенні проблем, що виникають під час використання програми [5].

Розробка майбутнього програмного забезпечення буде здійснюватися з використанням мови програмування Python. Вона є однією з найбільш популярних мов програмування для розробки програмного забезпечення, особливо в галузі математичного моделювання. Її легкість вивчення та простота використання дозволяють розробникам швидко створювати ефективне програмне забезпечення для розв'язування складних математичних задач.

Крім того, Python має велику кількість бібліотек та фреймворків, що дозволяє розробникам ефективно використовувати готові рішення для розв'язування задач з різних галузей математики та науки.

Наприклад, бібліотека NumPy дозволяє працювати з масивами даних та виконувати різні математичні операції, а бібліотека Matplotlib дозволяє візуалізувати дані та результати розрахунків у вигляді графіків та діаграм.

Також, бібліотека SciPy надає інструменти для розв'язування різноманітних наукових та інженерних задач, включаючи оптимізацію, інтерполяцію, інтегрування та обробку сигналів. Бібліотека SymPy, з іншого боку, надає можливості символьного обчислення, що дозволяє виконувати складні математичні операції з використанням символів та формул. Ці бібліотеки дозволяють розробникам ефективно використовувати готові рішення та зосередитися на розв'язуванні самої математичної задачі [6].

Забезпечення доступності для мобільних гаджетів є необхідним етапом у розробці програмного забезпечення для вирішення математичних задач. Користувачі зможуть використовувати додаток на своєму смартфоні чи планшеті в будь-який момент часу та в будь-якому місці, що дозволить їм бути більш продуктивними та ефективними.

Крім того, доступність додатку для мобільних гаджетів може збільшити його популярність та залучити нових користувачів. На сьогоднішній день, мобільні пристрої стали необхідними елементами нашого життя, і більшість людей використовують їх для доступу до різноманітних сервісів та додатків. Головною метою є забезпечення максимальної доступності та зручності для користувачів. Додаток повинен легко знаходитися та завантажуватися з мобільних магазинів додатків, а також мати інтуїтивно зрозумілий та зручний інтерфейс для користувачів.

Важливим елементом розробки програмного забезпечення є його документація та підтримка користувачів. Детальна та зрозуміла документація дозволяє користувачам ознайомитися з можливостями програмного забезпечення та швидко розв'язати свої задачі. Підтримка користувачів від розробників дозволяє швидко відповідати на запитання та проблеми користувачів, а також вдосконалювати програмне забезпечення з урахуванням їхніх вимог та пропозицій.

Розглядається можливість впровадження режиму для людей з обмеженими можливостями, що забезпечить доступність програми для користувачів з різними потребами. Наприклад, можна розробити спеціальний інтерфейс для людей з вадами зору або низькою моторикою, який дозволить користувачам взаємодіяти з програмою без перешкод. Також можна впровадити інтерфейс з голосовим керуванням для людей з вадами зору або використовувати штучний інтелект для розпізнавання голосових команд.

Крім того, конкурентні ціни на платформу сприятимуть привабливості продукту для широкого кола користувачів. Низькі витрати на використання програмного забезпечення зроблять його доступним для великої кількості людей, включаючи невеликі компанії та стартапи з обмеженим бюджетом.

Безпека та надійність програмного забезпечення буде забезпечуватися конфіденційністю користувачів. Запобігання витоку даних та забезпечення приватності користувачів - це одні з головних пріоритетів розробників програмного забезпечення, що забезпечить надійність та довіру до продукту.

Для досягнення високої продуктивності програми та зручного інтерфейсу користувача необхідно поєднати різні технології та методи, що сприятимуть оптимальним результатам та комфортній роботі користувачів з програмним забезпеченням.

Загалом, створення програмного забезпечення для розв'язування задач вищої математики - це складний та багатоаспектний процес, який вимагає від розробників глибоких знань та уваги до деталей. Проте, якщо правильно підійти до цього процесу, можна створити високоякісне програмне забезпечення, яке допоможе користувачам розв'язувати складні математичні задачі з максимальною продуктивністю та ефективністю.

Висновки. Було проведено аналіз декількох платформ для розв'язання математичних задач, і встановлено, що кожна з них має певні переваги та обмеження.

Серед найбільш популярних платформ можна виділити Wolfram Mathematica, Symbolab, Mathway та GeoGebra. Wolfram Mathematica є дуже потужним інструментом, здатним розв'язувати складні математичні задачі, проте інтерфейс платформи може бути складним для користувачів без відповідного досвіду роботи з програмним забезпеченням.

Symbolab є більш детальним та зрозумілим інструментом, проте розв'язання деяких складних математичних задач може бути менш точним порівняно з альтернативними платформами. Платформа Mathway має багато корисних функцій, таких як візуалізація кроків розв'язання задачі, проте вона має обмежену функціональність у безкоштовній версії.

GeoGebra популярна платформа, яка поєднує в собі широкий спектр функцій та інструментів для виконання різних операцій з математикою, включаючи графіки, геометрію та алгебру. Недоліком GeoGebra є обмежена потужність та функціональність порівняно з такими платформами як Wolfram Mathematica. Вона менш адаптована для розв'язання складних задач та не має такої широкої бібліотеки інструментів. Крім того, GeoGebra не підтримує такий широкий спектр типів розв'язання задач, як Symbolab або Mathway.

Для розробки програмного забезпечення щодо розв'язання математичних задач було б доцільно використати кращі практики з кожної платформи. Наприклад, користувачам потрібно бачити детальні розв'язання задач для розуміння шляху досягнення відповіді. Крім того, розробникам програмного забезпечення варто звернути увагу на важливість його доступності для людей з обмеженими можливостями. Також варто розглянути можливість створення мобільного додатку для зручності користувачів.

Отже, програмне забезпечення для розв'язання математичних задач повинно бути потужним та детальним, зрозумілим та доступним, а також забезпечувати можливість візуалізації та розв'язання різних типів задач. Крім того, його інтерфейс має бути інтуїтивно зрозумілим та простим у використанні для різних категорій користувачів.

Список використаних джерел

1. Wolfram Mathematica. – 2023. [Електронний ресурс]. – Режим доступу : https://www.wolfram.com/mathematica/index.php.en?source=footer
2. MathWorks. – 2023. [Електронний ресурс]. – Режим доступу : https://www.mathworks.com/products/matlab.html
3. GeoGebra – 2023. [Електронний ресурс]. – Режим доступу : https://www.geogebra.org/calculator
4. Symbolab – 2023. [Електронний ресурс]. – Режим доступу : https://www.symbolab.com
5. Величко В. Є. Вільне програмне забезпечення в електронному навчанні майбутніх учителів математики, фізики та інформатики. – 2021. [Електронний ресурс]. – Режим доступу : https://www.researchgate.net/publication/331469364_VILNE_PROGRAMNE_ZABEZPECENNA_V_ELEKTRONNOMU_NAVCANNI_MAJBUTNIH_UCITELIV_MATEMATIKI_FIZIKI_TA_INFORMATIKI
6. Jake VanderPlas. Python Data Science Handbook. – 2016. [Електронний ресурс]. – Режим доступу : https://jakevdp.github.io/PythonDataScienceHandbook/

Робота виконана під науковим керівництвом к.пед.н., доцента
ЖИРОВОЇ Т.О.

АНАЛІЗ ТЕХНОЛОГІЙ ТА МЕТОДІВ РЕКОМЕНДАЦІЙ ВІДЕО КОНТЕНТУ

ПШЕНИШНИЙ П., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Відео контент - важлива частина нашого життя, і рекомендаційні системи допомагають нам знайти контент, який нас цікавить. Netflix - провідна компанія, що використовує машинне навчання та аналіз даних для рекомендацій відео контенту. У статті ми розглянемо, як Netflix та інші компанії використовують рекомендаційні системи відео контенту та як ці системи впливають на наші споживацькі звички.

Video content is an essential part of our lives, and recommendation systems help us find content that interests us. Netflix is a leading company that uses machine learning and data analysis for video content recommendations. In this article, we will discuss how Netflix and other companies use video content recommendation systems and how these systems affect our viewing habits.

Актуальність. З розвитком інтернету та цифрових технологій відео контент став невід'ємною частиною нашого життя. Згідно з даними, відео контент став одним з найбільш популярних форматів онлайн контенту, зокрема на YouTube щодня переглядається більше мільярда годин відео. Проте, зростає конкуренція серед компаній, які надають відео контент, і важливим є не лише створення цікавого та якісного контенту, але й залучення та утримання аудиторії.

У цьому контексті рекомендаційні системи відео контенту стають ключовим інструментом для залучення та утримання аудиторії. Вони допомагають користувачам знайти контент, який їх цікавить, та сприяють збільшенню кількості переглядів відео контенту. Компанії, які надають відео контент, активно використовують рекомендаційні системи, щоб залучити нових користувачів та зберегти існуючих.[1,с.2-3]

Однією з провідних компаній, яка використовує рекомендаційні системи відео контенту, є Netflix. Ця компанія зарекомендувала себе як лідер у своїй галузі завдяки високому рівню персоналізації та індивідуалізації рекомендаційного алгоритму. Netflix використовує машинне навчання та аналіз даних, щоб збирати та обробляти інформацію про користувачів та їх поведінку. На основі цих даних компанія створює індивідуальні рекомендації для кожного користувача, що робить досвід перегляду відео на Netflix більш приємним та зручним.

Метою статті дослідження технологій та методів, що використовуються в рекомендаційних системах відео контенту, з основним фокусом на підходах, які застосовує компанія Netflix.

Об'єктом дослідження є технології та методи рекомендації відео контенту в рекомендаційних системах, з основним фокусом на Netflix.

Предмет дослідження - аналіз технологій та методів рекомендації відео контенту, які використовуються в різних рекомендаційних системах, з урахуванням особливостей підходів, які використовує компанія Netflix.

Аналіз попередніх досліджень. Попередні дослідження показали важливість технологій та методів рекомендації відео контенту для користувачів і платформ відеострімінгу, таких як Netflix, YouTube і Amazon Prime Video. Наприклад, дослідження компанії Netflix, яке було опубліковано в 2016 році, вказує на те, що понад 75% переглянутих фільмів та серіалів на платформі були віднайдені завдяки рекомендаціям. Інше дослідження, проведене університетом Carnegie Mellon, показало, що удосконалення алгоритмів рекомендацій може покращити задоволення користувачів від контенту на 7-8%.

Виклад основного матеріалу.

Відео контент зараз є однією з провідних форм розваг і навчання. Залежно від платформи, яку вони використовують, провайдери відео контенту застосовують різні технології та методи рекомендацій для залучення користувачів. Одним із таких прикладів є Netflix, який використовує різні технології та методи рекомендацій для збільшення кількості переглядів відео контенту та покращення користувацького досвіду.

Рис. 1. Рекомендаційна система Netflix та Big data.[2]

Netflix використовує комбінацію різних методів для рекомендації відео контенту; основні методи, які використовує Netflix, включають колаборативну фільтрацію, рекомендації на основі контенту, глибинне навчання та інтерактивні рекомендації.

Колаборативна фільтрація - це рекомендаційна технологія, що базується на аналізі даних про взаємодію користувачів з контентом і використовується в різних секторах, таких як електронна комерція, соціальні мережі, музика та кіноіндустрія. У випадку Netflix колаборативна фільтрація використовується для аналізу даних про взаємодію користувачів з відео контентом, таких як рейтинги, відгуки та перегляди. На основі цих даних Netflix може зрозуміти, який контент користується найбільшою популярністю серед користувачів і які фактори впливають на їхній вибір. Існує два типи спільної фільтрації: на основі користувачів і на основі об'єктів.

У випадку фільтрації на основі користувача Netflix аналізує поведінку користувача і порівнює її з поведінкою інших користувачів, які мають схожі інтереси. Наприклад, якщо поведінка користувача А і користувача В дуже схожа, ймовірно, що рекомендації, які відповідають користувачеві В, також будуть відповідати користувачеві А.

У випадку об'єктно-орієнтованого підходу Netflix аналізує схожість між різним відео контентом і рекомендує користувачам контент, схожий на той, що їм вже подобається. Наприклад, якщо користувачеві дуже подобається певний фільм, йому можуть бути рекомендовані фільми зі схожими темами, жанрами або акторами.

Колаборативна фільтрація може бути ефективним способом рекомендувати відео контент, оскільки вона враховує вподобання та інтереси кожного користувача. Однак колаборативна фільтрація також має певні обмеження. Одним з обмежень є проблема “холодного старту”, яка виникає, коли користувачі є новачками на платформі і не мають достатньо даних про свою поведінку для надання точних рекомендацій. Щоб подолати цю проблему, Netflix використовує такі методи, як рекомендації на основі популярності контенту,

рекомендації на основі контенту та глибинне навчання. Крім того, колаборативна фільтрація вразлива до певних типів атак, таких як атаки з несправжніми користувачами (sybil attacks) та маніпуляційні атаки, які можуть спотворювати рекомендації та впливати на поведінку користувачів. Загалом, колаборативна фільтрація є ефективним і широко використовуваним методом рекомендації відео контенту, який дозволяє Netflix надавати користувачам персоналізований і цікавий контент. Однак він має обмеження і потребує постійного вдосконалення технологій і методів аналізу даних, щоб максимізувати точність рекомендацій.

Рекомендації на основі контенту - це метод рекомендацій, який використовує Netflix. Платформа аналізує відео контент, який подобається користувачам, і рекомендує контент зі схожим змістом. Рекомендації на основі вмісту можуть враховувати такі фактори, як жанр, акторський склад, характеристики режисера та тематика відео контенту. Netflix використовує підхід рекомендацій на основі контенту, щоб рекомендувати фільми та телешоу, які можуть сподобатися користувачам. Компанія аналізує якості контенту, який користувачі переглянули або високо оцінили, і рекомендує схожий контент. Наприклад, якщо користувач дивиться багато комедійних фільмів, Netflix порекомендує йому інші комедійні фільми та телешоу. Крім того, Netflix також аналізує поведінку користувачів, наприклад, коли вони дивляться контент, і використовує цю інформацію для надання рекомендацій. Наприклад, якщо користувач дивиться фільм вночі, платформа може порекомендувати фільми або драми з нічною атмосферою. Зокрема, Netflix використовує алгоритмічну систему рекомендацій під назвою “Cinematch”, яка аналізує попередні вибори та оцінки користувачів для надання рекомендацій. Система також включає машинне навчання, наприклад, технологію глибокого навчання. Загалом, рекомендації на основі контенту - це ефективний підхід до надання контенту, який користувачам може бути цікаво переглянути. Такі рекомендації дозволяють користувачам мати більш персоналізований досвід перегляду.

Глибинне навчання - це метод, який використовує Netflix для покращення рекомендацій, використовуючи інформацію про перегляд та поведінку на платформі. Netflix використовує нейронні мережі для аналізу поведінки користувачів та рекомендації відео контенту. Глибинне навчання допомагає Netflix зрозуміти, що привертає увагу користувачів і які фактори впливають на їхній вибір відео. Ця техніка може автоматично виявляти складні взаємозв'язки між вхідними та вихідними даними. У випадку з Netflix глибинне навчання використовується для аналізу великих обсягів даних відео контенту та інформації про користувачів, щоб зрозуміти, які фактори впливають на вибір користувачів. Наприклад, глибинне навчання можна використовувати для автоматичного виявлення закономірностей у поведінці користувачів, таких як перегляди відео, рейтинги та відгуки. За допомогою глибинного навчання Netflix може адаптувати рекомендації до конкретних інтересів і поведінки кожного користувача. Однією з переваг глибинне навчання є те, що воно може автоматизувати багато процесів, які раніше вимагали багато ручної роботи. Наприклад, використовуючи глибинне навчання для автоматичного відбору та категоризації великих обсягів відео контенту, Netflix може значно збільшити кількість контенту, доступного для користувачів. У світі, де обсяг доступного відео контенту стрімко зростає, глибинне навчання може дозволити Netflix залишатися конкурентоспроможним, дозволяючи швидко і ефективно аналізувати великі обсяги даних і надавати користувачам персоналізовані рекомендації щодо контенту.

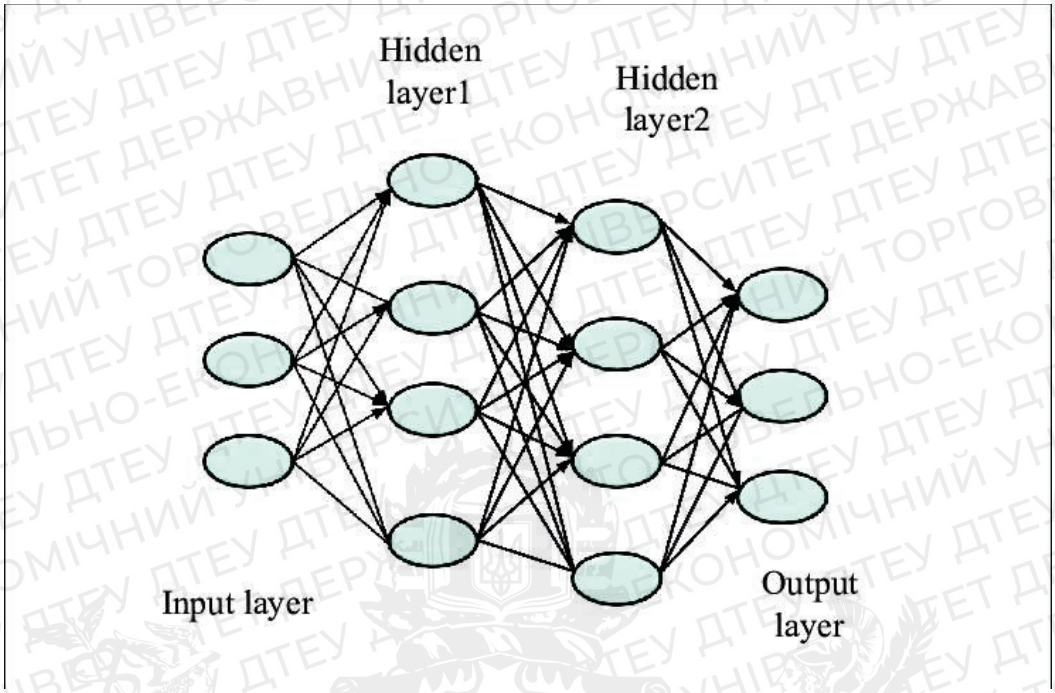


Рис. 2. Базова структура глибокої нейронної мережі.[3]

Інтерактивні рекомендації - це новий підхід до алгоритмів рекомендацій, який дозволяє користувачам взаємодіяти з рекомендованим контентом і вказувати свої вподобання, підвищуючи точність рекомендацій і покращуючи користувацький досвід. Наприклад, Netflix може запитувати користувачів про їхній настрій та емоції і рекомендувати відео контент, який може відповісти на ці запитання. Інтерактивні рекомендації - це новий підхід до алгоритмів рекомендацій, який дозволяє користувачам взаємодіяти з рекомендованим контентом і вказувати свої вподобання, підвищуючи точність рекомендацій і покращуючи користувацький досвід. Netflix вперше представив інтерактивні рекомендації у фільмі "BlackMirror:Bandersnatch", який вийшов на екрани у 2017 році. Це був інтерактивний проект, який дозволяв глядачам впливати на історію, обираючи поведінку головного героя. На основі реакції глядачів Netflix міг запропонувати подальші варіанти сюжету та надати персоналізовані рекомендації.

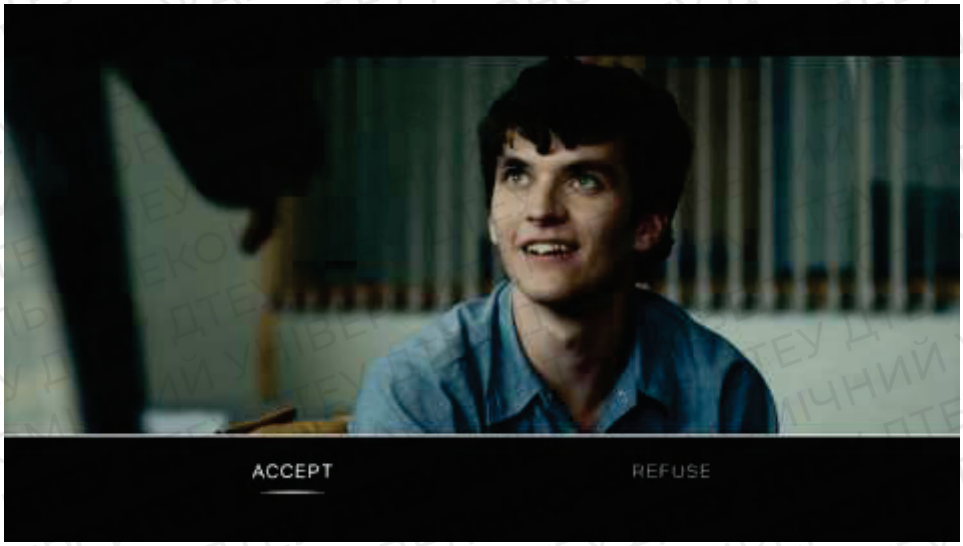


Рис. 3. Приклад інтерактивної рекомендації у фільмі.

Після успіху "Bandersnatch" Netflix продовжив поширювати інтерактивність на інші фільми та серіали, дозволяючи глядачам взаємодіяти з пропонованим контентом і обирати

власну сюжетну лінію. Це дозволяє Netflix збирати більше даних про вподобання та інтереси користувачів, що дає змогу надавати більш точні та персоналізовані рекомендації. Інтерактивні рекомендації також включають елемент експериментів спільноти для моніторингу реакції користувачів на новий контент і збору відгуків, що допоможе вдосконалити алгоритми рекомендацій і надавати кращі рекомендації в майбутньому. Окрім методів і прийомів надання рекомендацій, Netflix також використовує надану користувачем інформацію про нього для надання персоналізованих рекомендацій. Наприклад, Netflix збирає дані про вподобання користувачів, а також інформацію про вік, стать і географічне розташування для надання персоналізованих рекомендацій. Таким чином, Netflix використовує різні технології та методи рекомендацій, щоб залучити користувачів і покращити їхній досвід. Поєднуючи такі методи рекомендацій, як спільна фільтрація, рекомендації на основі контенту, глибинне навчання та інтерактивні рекомендації, Netflix може надавати персоналізовані рекомендації щодо відео контенту для кожного користувача.

Компанія постійно вдосконалює свої технології та методи рекомендацій, щоб забезпечити найкращий користувацький досвід. Наприклад, у 2020 році Netflix запустив нову функцію Top 10, яка показує 10 найпопулярніших відео контенту на локальному ринку користувача. Це полегшує користувачам пошук нових шоу та фільмів, які користуються популярністю серед інших користувачів у їхньому регіоні. Крім того, Netflix також використовує відео аналітику та машинне навчання для аналізу відео контенту та підбору його відповідно до інтересів користувачів, аналізує зв'язок між жанрами та темами, щоб надавати користувачам персоналізовані рекомендації, аналізує користувацький досвід під час перегляду відео контенту, щоб зрозуміти, які елементи контенту приваблюють глядачів і як їх можна покращити в майбутньому [3].

Висновки. Технології та методи рекомендації відео контенту є ключовими для відеоплатформ, таких як Netflix, які стикаються з великою кількістю контенту та зростаючими очікуваннями користувачів. Рекомендаційні системи, які використовуються на таких платформах, базуються на складних алгоритмах та машинному навчанні, що дозволяє їм надавати користувачам персоналізовані рекомендації та поліпшувати загальне задоволення від контенту. Дослідження показують, що удосконалення цих технологій може покращити якість рекомендацій та задоволення користувачів від перегляду відео контенту.

Список використаних джерел

1. Bansal, R., & Saini, R. (2021). A Hybrid Recommendation Algorithm Using Association Rule Mining and Collaborative Filtering. Complexity, 2021, 1-13. c: 10.1155/2021/8875700
2. Smith, J. Building a Netflix Recommendation System. Analytics Vidhya. https://medium.com/analytics-vidhya/building-a-netflix-recommendation-system-7b1fec90f83e.
3. ResearchGate. (n.d.). The basic structure of the deep neural network (DNN). Retrieved, from https://www.researchgate.net/figure/The-basic-structure-of-the-deep-neural-network-DNN_fig1_355756076
4. Іваницький, А., Маруняк, І., & Хом'як, І. (2019). Розвиток рекомендаційних систем в онлайн-сервісах: приклад Netflix. Маркетинг і менеджмент інновацій, (4), 68-75. https://doi.org/10.21272/mmi.2019.4-06

Робота виконана під науковим керівництвом канд. пед. наук, доцента
КОТЕНКО Н.О.

АСПЕКТНО-ОРІЄНТОВАНЕ ПРОГРАМУВАННЯ ДЛЯ ПОЛІПШЕННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

РИБКІН Я., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті досліджується застосування аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури. Відзначається, що мікросервісна архітектура є потужним інструментом для розробки та підтримки програмного забезпечення. Однак, вона також може бути складною для розуміння та підтримки через велику кількість компонентів, що можуть змінюватись динамічно. Аспектно-орієнтоване програмування надає зручний спосіб для розділення перехресних аспектів в програмному забезпеченні та забезпечення їх незалежної розробки та підтримки. У статті розглядаються основні принципи аспектно-орієнтованого програмування, його застосування в мікросервісній архітектурі та приклади реалізації.

The article explores the use of aspect-oriented programming to enhance microservices architecture. Microservices architecture is a powerful tool for developing and maintaining software, but it can also be complex to understand and maintain due to the large number of components that can change dynamically. Aspect-oriented programming provides a convenient way to separate cross-cutting concerns in software and ensure their independent development and maintenance. The article discusses the basic principles of aspect-oriented programming, its application in microservices architecture, and examples of implementation.

Актуальність. У сучасному світі інформаційних технологій, мікросервісна архітектура стала ключовою стратегією для будівництва гнучких та масштабованих програмних додатків. Ця архітектурна парадигма передбачає розбиття складних додатків на невеликі, незалежні компоненти, що спрощує розробку, розгортання та обслуговування. Однак, при рості розміру та складності мікросервісних систем виникає низка викликів, пов'язаних зі збереженням їхньої ефективності, розширюваністю та управлінням.

Розробка програмного забезпечення на основі мікросервісної архітектури є однією з найбільш популярних практик в індустрії програмного забезпечення. Проте, розробка та підтримка мікросервісної архітектури може бути важкою через складність зв'язків між компонентами та змінність архітектури. Одним з підходів для зменшення складності мікросервісної архітектури є застосування аспектно-орієнтованого програмування. Цей підхід дозволяє зменшити залежності між різними частинами програмного забезпечення та забезпечити більшу гнучкість та модульність.

Метою даної статті є дослідження можливості використання аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури. Ми дослідимо, як застосування аспектно-орієнтованого програмування дозволяє зменшити складність мікросервісної архітектури та забезпечити більшу гнучкість та модульність програмного забезпечення. Ми також розглянемо основні принципи аспектно-орієнтованого програмування та приклади його застосування в мікросервісній архітектурі.

Для досягнення мети було поставлено наступні завдання:

- проаналізувати поняття аспектно-орієнтованого програмування та мікросервісної архітектури;
- розглянути можливості використання аспектно-орієнтованого програмування для зменшення залежностей між різними компонентами мікросервісної архітектури;
- дослідити застосування аспектно-орієнтованого програмування для забезпечення безпеки та моніторингу мікросервісної архітектури;

- порівняти підходи, що використовують аспектно-орієнтоване програмування, з іншими підходами, які застосовуються для поліпшення мікросервісної архітектури;
- зробити висновки щодо ефективності використання аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури.

Об'єктом дослідження є мікросервісна архітектура, яка є популярним підходом для розробки програмного забезпечення.

Предметом дослідження є застосування аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури.

Аналіз попередніх досліджень. Раніше дослідження показали, що мікросервісна архітектура може бути складною в розробці та підтримці через залежності між різними компонентами. Застосування аспектно-орієнтованого програмування може допомогти зменшити ці залежності та забезпечити більшу гнучкість та модульність програмного забезпечення.

У дослідженні, проведеному Дж. Гу та його колегами (2018), автори запропонували використання аспектно-орієнтованого програмування для забезпечення моніторингу та аналізу мікросервісної архітектури. Аспекти використовувалися для збору метрик та статистики від різних компонентів системи, що дозволило покращити моніторинг та аналіз архітектури.

У дослідженні, проведеному Б. Штулецом та його колегами (2017), автори досліджували застосування аспектно-орієнтованого програмування для забезпечення безпеки в мікросервісній архітектурі. Аспекти використовувалися для виконання додаткових перевірок безпеки при виконанні різних операцій, що дозволило забезпечити більшу безпеку програмного забезпечення.

Обидва дослідження показують можливості застосування аспектно-орієнтованого програмування для поліпшення різних аспектів мікросервісної архітектури, що підтверджує актуальність нашої статті та мотивує дослідження даного підходу детальніше.

Виклад основного матеріалу. Мікросервісна архітектура є однією з найпопулярніших архітектурних підходів в програмному забезпеченні. Вона спрощує процес розробки, деплою та масштабування складних систем. Однак, при збільшенні кількості мікросервісів, архітектура може стати складною для управління та розуміння.

Аспектно-орієнтоване програмування (АОП) - це методологія програмування, що дозволяє виділяти спільні аспекти програми та використовувати їх для поліпшення якості та керованості програмного коду. Використання АОП для поліпшення мікросервісної архітектури може допомогти зменшити складність та зробити архітектуру більш модульною та керованою.

У даній статті ми розглянемо основні поняття АОП та його використання для поліпшення мікросервісної архітектури.

Першим кроком до використання АОП для поліпшення мікросервісної архітектури є розбиття мікросервісів на аспекти. Для цього можна проаналізувати функціональність кожного мікросервісу та виділити спільні аспекти, які можна використати для поліпшення керованості та якості коду.

Наприклад, мікросервіс, що відповідає за обробку замовлень, може мати спільну функціональність з мікросервісом, що відповідає за обробку платежів. Ці спільні аспекти можуть бути використані для реалізації більш керованої та якісної функціональності.

Після розбиття мікросервісів на аспекти можна використовувати поради для поліпшення їх функціональності та якості коду. Наприклад, можна використовувати передпоради для перевірки вхідних даних та забезпечення їх правильної ініціалізації. Також можна використовувати післяпоради для обробки результатів виконання та очищення даних. Навколопоради можуть використовуватись для обробки виключень та забезпечення правильної обробки даних.

Для використання АОП можна також використовувати анотації, які дозволяють позначати код для застосування певних порад. Анотації можуть бути використані для позначення методів або класів, які мають бути покриті певними порадами.

Наприклад, можна використовувати анотації для позначення методів, які мають бути покриті передпорадами для перевірки вхідних даних. Це дозволяє забезпечити правильну ініціалізацію даних та зменшити ризик помилок при виконанні методів.

Для використання АОП для поліпшення мікросервісної архітектури можна також використовувати зв'язки між аспектами. Зв'язки можуть бути використані для забезпечення правильної взаємодії між різними аспектами та їх правильного виконання.

Наприклад, можна використовувати зв'язки для забезпечення правильної взаємодії між мікросервісами, що відповідають за обробку замовлень та платежів. Це дозволяє забезпечити правильну обробку замовлень та платежів та зменшити ризик помилок.

Для кращого розуміння використання АОП для поліпшення мікросервісної архітектури, розглянемо приклад застосування АОП у мікросервісній архітектурі.

Припустимо, що ми маємо мікросервісну архітектуру, що складається з двох сервісів - сервісу обробки замовлень та сервісу оплати. Сервіс обробки замовлень отримує запити на обробку замовлень, перевіряє їх валідність та передає до сервісу оплати для здійснення оплати. Сервіс оплати отримує запит на здійснення оплати та передає результат оплати до сервісу обробки замовлень.

Ми хочемо використовувати АОП для покращення функціональності та якості коду у нашій мікросервісній архітектурі. Для цього ми використовуємо підхід, де ми використовуємо певні поради для кожного сервісу та зв'язки між ними для забезпечення правильної взаємодії між сервісами.

Необхідно забезпечити правильну обробку вхідних даних в обох сервісах. Для цього ми використовуємо передпоради, які перевіряють валідність вхідних даних перед тим, як вони будуть передані до сервісів.

У сервісі обробки замовлень ми використовуємо передпораду для перевірки валідності замовлення перед тим, як він буде переданий до сервісу оплати. Якщо замовлення не є валідним, то передпорада генерує виключення, яке повертається до клієнта.

У сервісі оплати ми також використовуємо передпораду для перевірки валідності вхідних даних. Перевіряється, чи містить запит на оплату достатньо інформації для здійснення оплати. Якщо інформація не є валідною, то передпорада генерує виключення, яке повертається до клієнта.

Помилки можуть виникати в будь-якому сервісі, і ми хочемо забезпечити правильну обробку помилок в нашій мікросервісній архітектурі. Для цього потрібно використовувати поради, які визначають правильну поведінку у випадку помилки.

У сервісі обробки замовлень ми використовуємо пораду, яка визначає правильну поведінку у випадку, якщо сервіс оплати недоступний. Якщо сервіс оплати недоступний, то сервіс обробки замовлень повертає помилку, що сервіс оплати недоступний. Це дозволяє клієнту правильно обробляти помилки та надає відповідну поведінку.

У сервісі оплати ми також використовуємо пораду, яка визначає правильну поведінку у випадку, якщо замовлення недоступне. Якщо замовлення недоступне, то сервіс оплати повертає помилку, що замовлення недоступне. Це дозволяє клієнту правильно обробляти помилки та надає відповідну поведінку.

Журналювання та моніторинг є важливим елементом мікросервісної архітектури. Потрібно забезпечити правильну реєстрацію та моніторинг наших сервісів, щоб бути впевненими у правильному функціонуванні системи.

Для журналювання ми використовуємо ELK-стек, який складається з Elasticsearch, Logstash та Kibana. Ми збираємо дані з різних сервісів та записуємо їх у Elasticsearch. Для збору даних використовується Logstash, який зчитує дані з журналів наших сервісів та пересилає їх до Elasticsearch. Кібана використовується для відображення та аналізу даних.

Для моніторингу можна використовувати Prometheus та Grafana. Prometheus збирає метрики з наших сервісів та зберігає їх у власному сховищі. Grafana використовується для відображення метрик та аналізу їх стану.

Застосування аспектно-орієнтованого програмування в нашій мікросервісній архітектурі дозволяє нам ефективно управляти різноманітними аспектами функціональності наших сервісів, забезпечувати їх взаємодію та підтримувати цілісність системи в цілому. Крім того, використання порад дозволяє нам забезпечити правильну поведінку сервісів у випадку помилок, а моніторинг та журналювання допомагають відслідковувати та аналізувати роботу нашої системи.

У майбутньому можна очікувати дальшого розвитку мікросервісної архітектури та зростання числа систем, які використовують цей підхід. Для ефективного впровадження мікросервісної архітектури необхідно використовувати інструменти, які дозволяють ефективно управляти функціональними аспектами сервісів та забезпечувати їх взаємодію. Аспектно-орієнтоване програмування може бути одним з таких інструментів, який дозволяє зосередитися на функціональних аспектах сервісів та забезпечує легкість управління їхнім поведінкою. Крім того, використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність.

Наступним кроком у розвитку мікросервісної архітектури може бути використання контейнерів та оркестраторів. Контейнери дозволяють забезпечити ізольованість сервісів та їхню мобільність, тобто можливість запуску на будь-якому сервері, що підтримує контейнеризацію. Оркестратори дозволяють автоматично керувати розгортанням та масштабуванням контейнерів, що забезпечує швидке відновлення після помилок та високу доступність системи в цілому.

Контейнеризація та оркестрація можуть бути досить складними процесами, тому необхідно використовувати ефективні інструменти для їх управління. Наприклад, Docker може бути використаний для створення контейнерів, а Kubernetes - для оркестрації їх розгортання та керування ними. Використання цих інструментів дозволяє зменшити складність розгортання та управління мікросервісами, забезпечуючи ефективну та швидку роботу системи.

У підсумку можна зробити висновок, що аспектно-орієнтоване програмування може бути ефективним інструментом для поліпшення мікросервісної архітектури. Використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність. Контейнеризація та оркестрація дозволяють забезпечити мобільність та ефективне керування мікросервісами. Використання цих технологій може допомогти зменшити складність розгортання та управління мікросервісами та забезпечити швидку відновлюваність після помилок та високу доступність системи в цілому.

Проте, важливо зазначити, що використання аспектно-орієнтованого програмування, контейнеризації та оркестрації є лише інструментами для поліпшення мікросервісної архітектури. Для успішного розгортання та ефективної роботи системи необхідно також враховувати багато інших аспектів, таких як безпека, моніторинг, тестування та інші. Крім того, важливо визначити, коли використання мікросервісної архітектури є доцільним та чи варто розгортати її в конкретному проекті.

Аспектно-орієнтоване програмування є ефективним інструментом для поліпшення мікросервісної архітектури. Використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність. Контейнеризація та оркестрація дозволяють забезпечити мобільність та ефективне керування мікросервісами.

Однак, важливо зазначити, що використання аспектно-орієнтованого програмування, контейнеризації та оркестрації є лише частинами процесу побудови ефективної мікросервісної архітектури. Для успішного розгортання та ефективної роботи системи необхідно також враховувати багато інших аспектів, таких як безпека, моніторинг, тестування та інші. Крім того, важливо визначити, коли використання мікросервісної архітектури є доцільним та чи варто розгортати її в конкретному проекті.

В цілому, аспектно-орієнтоване програмування може бути корисним інструментом для побудови ефективної мікросервісної архітектури. Використання цього підходу може допомогти зменшити складність розгортання та управління мікросервісами та забезпечити швидку відновлюваність після помилок та високу доступність системи в цілому. Однак, важливо враховувати багато інших аспектів та використовувати підходи та інструменти, які найбільше відповідають потребам конкретного проекту.

Для того, щоб успішно використовувати аспектно-орієнтоване програмування, необхідно мати достатній рівень знань та досвіду в програмуванні та мікросервісній архітектурі. Крім того, важливо розуміти, що використання цього підходу не є універсальним рішенням для всіх задач і не підходить для кожного проекту.

Особливо важливо враховувати аспекти безпеки та захисту даних під час використання мікросервісної архітектури. Кожен мікросервіс повинен мати достатній рівень захисту, а також виконувати певні стандарти щодо захисту даних. Крім того, важливо забезпечувати моніторинг та логування для швидкої виявлення та виправлення помилок.

Також важливо враховувати витрати на побудову та підтримку мікросервісної архітектури. Зазвичай це вимагає великих витрат на інфраструктуру та залучення додаткового персоналу. Тому перед розгортанням мікросервісної архітектури варто ретельно обміркувати, чи варто такі витрати та чи є можливість їх компенсувати в результаті більш ефективної роботи системи.

Усі ці фактори підтверджують, що використання мікросервісної архітектури та аспектно-орієнтованого програмування є складним завданням, яке вимагає великої кількості знань, досвіду та ретельного аналізу. Однак, якщо використання цих підходів проводиться правильно та враховується весь комплекс аспектів, то можна досягти високої ефективності та доступності системи.

Також важливе належне тестування та валідація системи перед використанням в реальних умовах. Це допоможе виявити та виправити помилки та ускладнення перед тим, як користувачі почнуть використовувати систему.

У зв'язку з розгортанням мікросервісної архітектури та використанням аспектно-орієнтованого програмування, важливо також звернути увагу на стилі програмування, які використовуються. Оскільки мікросервісна архітектура передбачає розподілення функцій між різними сервісами, кожен з яких має свою відповідальність, стилі програмування повинні бути зорієнтовані на створення зрозумілої та легко модифікуємої кодової бази.

Крім того, важливо враховувати питання масштабованості системи при використанні мікросервісної архітектури та аспектно-орієнтованого програмування. Якщо зростання обсягу даних або навантаження стає непередбачуваним, можуть виникнути проблеми з пропускною здатністю та продуктивністю. Тому важливо забезпечувати масштабованість системи та можливість розширення її функціональності при необхідності.

Аспектно-орієнтоване програмування є потужним підходом, який дозволяє розширювати функціональність програмного забезпечення, знижувати повторення коду та поліпшувати читабельність та обслуговуваність коду. Крім того, використання мікросервісної архітектури дозволяє розподілити функції системи між різними сервісами, забезпечити гнучкість та швидкість внесення змін.

Комбінування аспектно-орієнтованого програмування з мікросервісною архітектурою може принести значні переваги в розробці та підтримці програмного забезпечення. Ці підходи забезпечують можливість підтримувати чистоту коду та дозволяють зосередитись на бізнес-логіці системи, що забезпечує більш швидку та ефективну розробку та підтримку.

Однак, варто пам'ятати, що використання таких підходів також може мати свої недоліки, зокрема ускладнення підтримки системи та необхідність відповідних знань та досвіду у використанні цих технологій.

У підсумку, аспектно-орієнтоване програмування та мікросервісна архітектура є потужними інструментами у розробці програмного забезпечення. Використання цих підходів дозволяє підвищити якість та ефективність розробки та підтримки системи, забезпечуючи

гнучкість та швидкість внесення змін у відповідь на потреби користувачів та зміни бізнес-вимог. Однак, перед використанням цих технологій необхідно провести відповідну оцінку вартості та потенційних недоліків, щоб забезпечити оптимальне використання ресурсів та досягнення поставлених цілей.

Висновки. У даній статті ми розглянули важливість мікросервісної архітектури для сучасних розподілених систем. Ми дослідили проблеми, які можуть виникнути при розробці та підтримці мікросервісної архітектури та вказали на те, як аспектно-орієнтоване програмування може допомогти у вирішенні цих проблем.

Можна сказати, що мікросервісна архітектура є важливим елементом розподілених систем та дозволяє підвищити масштабованість та ефективність системи в цілому. Однак, для ефективної підтримки мікросервісної архітектури необхідно використовувати підходи, які дозволяють ефективно управляти функціональними аспектами сервісів та забезпечувати їх взаємодію.

Аспектно-орієнтоване програмування є одним з таких підходів, який може допомогти розробникам у вирішенні цих проблем. Використання порад та патернів, таких як retry, circuit breaker, bulkhead та інших, може забезпечити правильну поведінку сервісів у випадку помилок, що дозволяє зменшити час відновлення роботи системи.

Моніторинг та журналювання є також важливим елементом підтримки мікросервісної архітектури. Використання інструментів, таких як ELK-стек та Prometheus з Grafana, дозволяє ефективно збирати та аналізувати дані, що є необхідним для підтримки роботи системи в цілому.

Отже, можна зробити висновок, що аспектно-орієнтоване програмування може бути ефективним інструментом для поліпшення мікросервісної архітектури. Використання аспектів дозволяє зосередитися на функціональних аспектах сервісів, забезпечуючи легкість та гнучкість у впровадженні функціональних вимог. Поради та патерни, такі як retry, circuit breaker, bulkhead та інші, дозволяють забезпечити правильну поведінку сервісів у випадку помилок, що є важливим елементом підтримки мікросервісної архітектури.

Аспектно-орієнтоване програмування може бути ефективним інструментом для поліпшення мікросервісної архітектури. Використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність. Контейнеризація та оркестрація дозволяють забезпечити мобільність та ефективне керування мікросервісами. Проте, важливо враховувати багато інших аспектів при розгортанні та управлінні мікросервісами. Використання мікросервісної архітектури повинно бути обґрунтованим та доцільним для конкретного проекту.

Список використаних джерел

1. M. Fowler, "Microservices: Decomposing Applications for Deployability and Scalability," 2014.
2. D. Duka, A. Shtroo, "Design Patterns for Microservices Architecture," IEEE, 2018.
3. S. Newman, "Building Microservices: Designing Fine-Grained Systems," 2015.
4. В. Єфименко. Мікросервісна архітектура: концепції, технології, інструменти// Системні технології, -2019-№ 4 (34). – С. 38–49.
5. М. Матвєєва. Аспекти технології мікросервісів в розробці програмного забезпечення// Наукові праці Донецького національного технічного університету-2019-№ 3. – С. 105–116.
6. Ю. Данилюк. Архітектура мікросервісів як підхід до розробки високопродуктивних систем// Програмна інженерія та інформаційні технології, -2018.- № 2. – С. 83–96.

Робота виконана під науковим керівництвом к.е.н, старшого викладача
ФРАНЧУК Т.М.

АВТОМАТИЗАЦІЯ ОБЛІКУ СУБ'ЄКТІВ НАДАННЯ ГУМАНІТАРНОЇ ДОПОМОГИ В УМОВАХ ВОЄННОГО ЧАСУ

РУДЕНКО В., курсу 2м ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто проблематику в обліку та реалізації гуманітарних питань в умовах воєнного часу. При написанні статті були використані зауваження та пропозиції волонтерської організації "East coast aid". Розглянуто ключові моменти для створення аналітичної сисетмти обліку для обліку гуманітарної допомоги.

The article describes problems in documenting and implementing humanitarian issues in the wartime. During the writing and research process, the comments and advice of the "East Coast Aid" volunteer organization were used. Advantages of "East Coast Aid" website will be described and analyzed in the article.

Актуальність. В реаліях нинішнього світу важливу роль у допомозі армії відіграють волонтерські організації , що виконують місії в Україні та інших країнах. Будь яка допомога має бути систематизована обліком та зареєстрована для контролю її використання та мінімізації виникнення ризиків. Саме тому доречним буде впровадження новітніх IT-технологій при створенні та впровадженні обліку. При збільшення фондів , і використання більшої кількості ресурсів критичним стає питання доцільності використання коштів та ресурсів для максимально ефективного контролю та мінімізації ризиків. У реаліях сьогодення , люди по всьому світі почали об'єднуватись для допомоги Україні. Тому дуже важливо аби вся інформація про надання допомоги була у вільних інтернет джерелах. Таким чином , люди зі всього світу можуть приєднуватись до гуманітарної допомоги , при довірі фонду та розумінні його функціоналу. Тому критично важливе мати відкриту та інноваційну методологію системи обліку та вдалу інтернет концепцію.

Метою статті є дослідження особливостей ведення облікових систем при наданні гуманітарної допомоги з метою підвищення ефективності їх функціонування та використання.

Об'єктом дослідження є розробка системи обліку для надання гуманітарної допомоги постраждалим внаслідок російської агресії.

Предмет дослідження - аналітична система обліку суб'єктів з використанням IT-технологій.

Аналіз попередніх досліджень. При дослідженні проблематики систем обліку були використаний власний досвід, досвід інших гуманітарних організацій та їх досвід аналітичних систем обліку та нормативно-аналітична база аналітичних інформаційних систем.

Виклад основного матеріалу. Для початку ведення обліку , потрібно отримувати дані від користувачів для їх ідентифікації в системі та контролю повторної допомоги. Дуже багато людей зараз потребують допомоги і важливо ставити пріоритети на тих кому справді потрібна допомога і хто просто використовує волонтерів для власних потреб. Для унеможливлення зловживанням допомоги. Саме тому важливо вести облік для більш точного розуміння проблематики даного питання. У межах цієї моделі визначено пріоритетні данні для внесення у бази даних с подальшим використанням їх для обліку та аудиту системи. Адже дуже важливо своєчасний та запланований аудит , що дає більш чітке бачення проблеми. Вмілий аудит закриває питання перевірки достовірності діяльності підприємства у сфері фінансів, а й надання керівнику рекомендацій, виконуючи які можна збільшити ефективність роботи компанії.

Для ведення обліку потрібно отримувати дані з запиту для ведення списку користувачів (Рис.1). У цій формі користувач вказує свої дані , такі як ім'я та прізвище що буде ключем для реєстрації, сам запит - яка саме допомога потрібна для більш точного розуміння необхідного.

Е-мейл та телефон для контакту с користувачем та додатково вказує чи потрібна допомога спеціаліста, бо зараз виросла кількість людей які потребують роботу психолога чи юриста для узгодження своїх проблем. Таким чином ми отримуємо для реєстрації необхідні дані від користувача. Та маємо дані для обліку , що допоможе в подальшому ефективно використовувати ресурси , та унеможливить зловживання гуманітарною допомогою або крадіжок

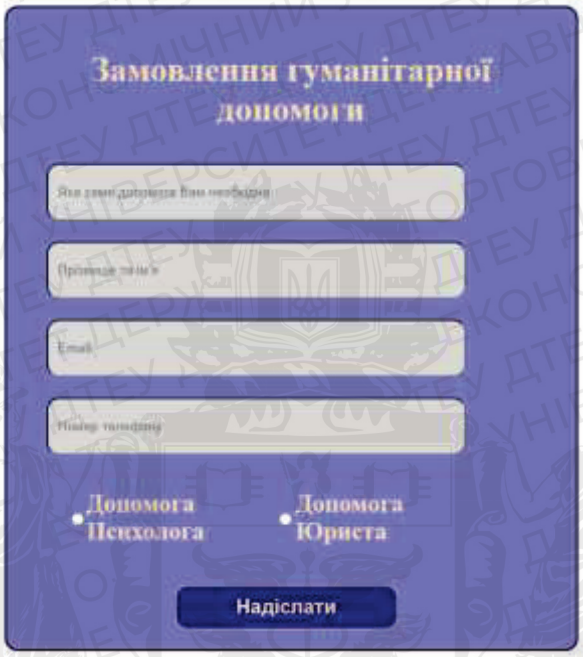


Рис. 1. Форма запиту на допомогу

Метою ведення обліку і складання фінансової звітності є надання користувачам для прийняття рішень повної, правдивої та неупередженої інформації про фінансове становище, результати діяльності та рух грошових коштів підприємства.

Основною метою обліку і складання фінансової звітності є забезпечення достовірної, повної та доступної інформації про фінансові результати, позицію та діяльність організації. Ця інформація використовується для прийняття рішень, залученні інвестицій і кредитування, а також при проведенні аудиту чи аналізу фінансової звітності. Основна мета обліку та складання фінансової звітності спрямована на забезпечення відповідності інформації корпоративним законам, вимогам і правилам організації, акціонерів та інвесторів, а також для забезпечення здатності управління приймати правильні рішення. Не слід забувати, що облік і складання фінансової звітності є невід'ємною складовою надання достовірної, повної та доступної інформації про фінансові результати, позицію та діяльність організації інвесторам та стороннім учасникам.

У рамках міжнародної гуманітарної допомоги під час війни застосовуються різні методи надання допомоги та загострення уваги на супроводжуваних осіб. Серед них можна виділити наступні ключові методи:

1. Захист прав людини: надання правової охорони та захисту людям, які переживають наслідки війни.
2. Захист життя та здоров'я: надання допомоги у лікуванні, підтримка програм щодо дотримання гігієни та профілактики болячих хвороб.
3. Освіта: надання далі доступу до освіти для дітей та дорослих на територіях, перебуваючих під впливом війни.
4. Надання безпечних притулків: створення спеціалізованих притулків для людей, які намагаються приховатися від військових дій та втратилих своє помешкання.

5. Надання матеріальної допомоги: надання харчування, одягу, житла та інших необхідних ресурсів до потреб людей, які знаходяться у ситуації примусового переселення.

6. Підтримка проектів побудови: підтримки будівництва шкіл, будівель, інфраструктури та інших об'єктів, які допомагають постраждалим та захищеним людям прийняти постійне місце проживання.

Гуманітарна допомога є різновидом благодійництва, а не видом благодійної допомоги і має спрямовуватися відповідно до обставин, об'єктивних потреб, **згоди її отримувачів** та за умови дотримання вимог Закону України "Про благодійну діяльність та благодійні організації" від 05.07.2012 р. № 5073-VI (далі — Закон № 5073 від 05.07.2012 р. № 5073-VI (далі — Закон № 5073). Про це зазначено у статті 1 Закону № 1192 (про гуманітарну допомогу). А в статті 3 Закону № 5073 мова йде лише про цілі та сфери благодійної діяльності, які повинні співпадати при отриманні гуманітарної допомоги і здійснення благодійництва. Етапи ведення обліку продемонстровано на Рис.2.

Рис. 2. Етапи ведення обліку

На першому етапі обліку слід зрозуміти що саме потрібно , яка саме допомога необхідна. Для реєстрації допомоги ми використовуємо дані отримані з форми (*Рисунок 1).* Отримані дані ми контролюємо в *Excel.* На наступному етапі ми дивимось в системі можливість допомоги в кожному випадку. На останньому етапі , якщо є можливість допомоги , надається гуманітарна допомога.

Гуманітарна допомога – добровільна, безкорислива та усвідомлена діяльність фізичних або юридичних осіб (спонсорів), що виражається через особисту та/або майнову допомогу юридичним особам, які в офіційному порядку визнані отримувачами гуманітарної допомоги, ґрунтується на принципах законності, гуманності, рівності та здійснюється із гуманних мотивів для досягнення суспільно-значимих цілей. Гуманітарна допомога має свої особливості:

- вона завжди має чітко визначений цільовий характер та передбачає кінцевого адресата;
- переслідує особливо значимі напрями здійснення благодійності;
- має у якості суб'єктів донора та юридичну особу зі спеціальним статусом отримувача гуманітарної допомоги;

- розрізняє отримувача гуманітарної допомоги та набувача (фізичну особу – кінцевого споживача);
- потребує письмової пропозиції донора про її надання;
- потребує згоди на її отримання з боку отримувача гуманітарної допомоги;

Отримувачі або набувачі гуманітарної допомоги відповідають критеріям соціальної незахищеності або матеріальної незабезпеченості. Зазначені обставини можуть бути спричинені такими подіями: важкими життєвими обставинами; стихійним лихом; значним погіршенням стану здоров'я; надзвичайним станом.

Після замовлення допомоги та реєстрації допомоги. Оператор у програмі MS Excel отримує заповнені користувачем дані.

Дані отримуються за допомогою введення користувачем даних у поля для введення та опрацьовуються закладеними функціями, методами сортування та фільтрування, розміщених у програмі Excel. Користувач може ввести дані вручну або використати інші функції для імпортування даних з інших файлів або з бази даних. Також можна використовувати функції автозаповнення, які дозволяють автоматично вводити дані в поля з наявними списками значень. Крім того, в даяких випадках можна використати макроси, які дозволяють автоматизувати процес завантаження даних з інших файлів або баз даних у форму Excel (за потреби). Введені дані генеруються в таблицю зручну для користування (Рис.3).

Ім'я та прізвище	Email	Номер телефону	Необхідна допомога	Допомога Юриста	Допомога психолога
Володимир Руденко	vldvrudenko@gmail.com	+380667161144	Необхідна допомога юриста	+	-
Гурженко Лариса	lngurszenko@gmail.com	+380667206666	Речі першої необхідності, їжа, інформація	-	-
Мостовий Андрій	mostovoi@gmail.com	+380667197865	Інформація , їжа , допомога психолога	-	+
Ткаченко Ігор	tkachenkoihor@gmail.com	+380677154521	Допомога юриста , психолога та їжа	+	+
Оксана Білик	biliuk@gmail.com	+380688171234	Інформація , речі першої необхідності	-	-
Валентина Кучерук	kucheruk@gmail.com	+380667182123	Допомога юриста , їжа	+	-

Рис. 3. Облік отриманих даних

Функціональність рішень даного типу ведення обліку гуманітарної допомоги :

- Легкість використання користувачів
- Зручність ведення обліку
- Отримання великої кількості даних користувачів
- Можливість самостійного внесення допомоги
- Реєстрація користувача
- Неможливість обману системи

Тому даний варіант отримання та використання даних є зручним, інноваційним та досить надійним для ведення обліку надання та отримання допомоги. Також важливим етапом надання допомоги є фото-фіксація для подальшої звітності перед спонсорами (Рис.4). Фото-фіксація може бути зроблена за допомогою різних методів, включаючи ручне зняття фотографії, використання планшетних пристроїв або смартфонів для зняття фотографії, а також використання відеофіксації для збору далі глибоких даних. Використовуючи ці методи, підприємства/фундації можуть зафіксувати процеси, відстежувати результати і зробити звіти для більш ефективної звітності. Якщо прийнято рішення використовувати фото-фіксацію, підприємства/фундації можуть використовувати спеціальну програму для збору, відстеження і аналізу даних. Ця програма може дозволити підприємству/фундації збирати фото-фіксацію, відстежувати її зміни і аналізувати дані, щоб отримати більш детальну інформацію про процеси і звіти про продуктивність. Система також може містити функції для відстеження процесів, визначення тривалості кожного процесу і далі генерування звітів для подальшого аналізу логістики.

Рис. 4. Приклад фото-звіту партнерами з фундації "Із покликом в серці"

Висновки. Аналітична система обліку суб'єктів надання гуманітарної допомоги в умовах воєнного часу призначена для організації та підтримки роботи з надання гуманітарної допомоги на території України та інших країн в умовах воєнного часу. Ця система має цілий спектр засобів для аналізу ситуації та подальших дій планування руху для надання гуманітарної допомоги. Система містить інструменти для збору, аналізу та обробки інформації щодо суб'єктів надання гуманітарної допомоги. Система також дозволяє збирати інформацію про тих, хто надалі хоче планувати дії для надання гуманітарної допомоги. Система ще надає можливість використання засобів аналітики, аналізу та візуалізації для отримання додаткових даних, які можуть допомогти в прийнятті оптимальних рішень. Ці дані далі використовуються для планування дій по наданню гуманітарної допомоги. Також система містить механізми для контролю доступу до інформації та можливості змінювати її. Це дозволяє збирати оновлену інформацію про суб'єкти надання гуманітарної допомоги, далі планування дій для надання гуманітарної допомоги. За допомогою цієї аналітичної системи можна підтримувати і контролювати процес надання гуманітарної допомоги в умовах воєнного часу, а також забезпечувати належне використання та планування дій для надання гуманітарної допомоги як по напрямках так і по логістиці.

Список використаних джерел

1. Косинський В.І. Сучасні інформаційні технології : навч. посіб. / В.І. Косинський, О.Ф. Швець. – Київ : Знання, 2011. – 594 с.
2. Чернишенко А. Аналітично-інтелектуальні системи обліку суб'єктів. Берлін: Springer, 2012. - 645 с.
3. Карп'юк О. Розробка аналітично-інтелектуальних систем облік ДАЛІ. Київ: Видавництво «Знання», 2009. - 326 с.
4. Карацуба Н. Програмування інтелектуальних аналітичних систем: посібник. Київ: Видавництво «Знання», 2014. - 421 с.
5. S. K. Pal and P. Mitra, Pattern Recognition Algorithms for Data Mining, Chapman & Hall CRC Press, Boca Raton, FL, May 2004, ISBN: 1-58488-457-6

Робота виконана під науковим керівництвом д.т.н., проф.
КРИВОРУЧКО О.В.

ВИКОРИСТАННЯ ОНЛАЙН-ПЛАТФОРМ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ ТА ЕФЕКТИВНОСТІ НАВЧАННЯ В ОСВІТНІХ ЗАКЛАДАХ

РУДИЧ М., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто використання онлайн-платформ для підвищення якості та ефективності навчання в освітніх закладах. Детально розглянуті переваги використання онлайн-платформ в освіті, різні типи онлайн-платформ для навчання, технологічні можливості онлайн-платформ, практичні приклади використання онлайн-платформ у різних освітніх закладах та їх ефективність та проблеми з безпекою даних та недостатня соціальна інтерактивність.

The article discusses the use of online platforms to improve the quality and efficiency of learning in educational institutions. The advantages of using online platforms in education, different types of online learning platforms, technological capabilities of online platforms, practical examples of using online platforms in different educational institutions and their effectiveness, as well as problems with data security and lack of social interactivity are discussed in detail.

Актуальність. Онлайн-платформи для навчання є одним з найбільш актуальних і швидко розвиваючихся напрямків у сучасній освіті. У сучасному світі навчання стає все більш цифровим і інтерактивним, а використання онлайн-платформ дозволяє учням отримувати знання та навички в більш зручному та ефективному форматі. Онлайн-платформи дозволяють учням вивчати матеріали у будь-який час та в будь-якому місці, не прив'язуючись до певного місця та часу. Це особливо важливо для тих, хто зайнятий роботою або іншими обов'язками, оскільки онлайн-платформи дозволяють організовувати навчання згідно з їх індивідуальним графіком та потребами. Крім того, використання онлайн-платформ дозволяє вчителям та учням використовувати різноманітні технологічні інструменти, такі як інтерактивні відео, аудіозаписи, тести та ігри, що сприяє більш ефективному засвоєнню матеріалу. У світлі умов, що швидко змінюються у світі, навчання на онлайн-платформах дозволяє учням отримувати актуальну інформацію та знання, оновлювати та розширювати свої навички та компетенції відповідно до потреб ринку праці, котрі постійно змінюються. В цілому, використання онлайн-платформ у навчанні є дуже актуальним та ефективним способом підвищення якості та ефективності освітнього процесу в наш час.

Використання онлайн-платформ у освіті дозволяє розширити географію навчання та участь у навчальному процесі. Особливо важливим це є для студентів, які живуть у віддалених регіонах, де доступ до якісної освіти може бути обмеженим. Онлайн-платформи дають таким студентам можливість навчатися у кращих вчителів та викладачів, брати участь у дискусіях та отримувати зворотний зв'язок на рівних умовах з іншими студентами з різних частин світу. У світлі цих переваг використання онлайн-платформ у навчанні є необхідним кроком у розвитку сучасної освіти і має бути широко прийнято в освітніх установах по всьому світу.

У даний час багато університетів і коледжів використовують онлайн-платформи для надання онлайн-курсів, які дозволяють студентам здобувати знання та навички з будь-якого місця та у зручний для них час. Такі курси можуть бути корисними для студентів з різних куточків світу, які хочуть отримати освіту в іншій країні, але не мають можливості переїхати. Крім того, використання онлайн-платформ дозволяє університетам та коледжам залучати кращих викладачів та вчених з різних країн для надання курсів та лекцій, що покращує якість освіти.

Метою статті є дослідження особливостей використання онлайн-платформ для підвищення якості та ефективності навчання в освітніх закладах.

Об'єктом дослідження є розробка онлайн-платформи дистанційного навчання.

Виклад основного матеріалу. Однією з основних переваг використання онлайн-платформ в освіті є їх зручність та доступність. Учні та викладачі можуть використовувати онлайн-платформи у будь-який час та з будь-якого місця, маючи доступ до матеріалів та інструментів, необхідних для ефективного навчання та викладання. Крім того, використання онлайн-платформ дозволяє значно зменшити часові та фінансові витрати на навчання, оскільки не потрібно відвідувати навчальні заклади та оплачувати витрати на проїзд, проживання та харчування.

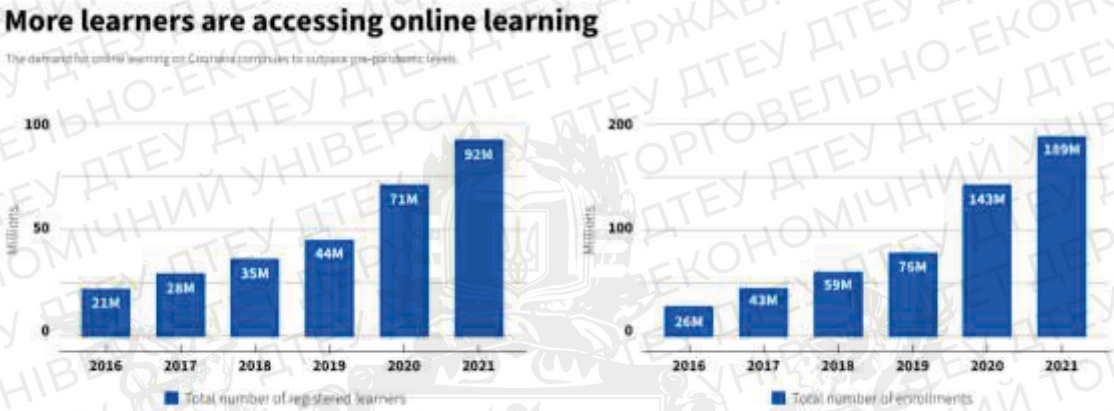


Рис. 1. Приріст нових користувачів онлайн-платформи Coursera. У 2021 році на курси зареєструвалося понад 20 мільйонів нових учнів. (https://www.weforum.org/agenda/2022/01/online-learning-courses-reskill-skills-gap/)

Гнучкість - ще одна важлива перевага онлайн-платформ в освіті. Вони дозволяють учням та викладачам працювати в більш гнучкому форматі, вибираючи зручний час та місце для навчальних занять. Це особливо важливо для студентів, які мають щільні графіки або обмежений доступ до навчальних закладів. Завдяки гнучкості онлайн-платформ, учні можуть працювати за своїми індивідуальними темпами, а викладачі можуть адаптувати свій курс до потреб конкретних студентів.

Використання онлайн-платформ також сприяє підвищенню якості освіти, оскільки це дозволяє використовувати найсучасніші технології та методи навчання. Це забезпечує більш глибоке розуміння матеріалу, більш ефективний обмін знаннями та навичками між учасниками освітнього процесу, а також підвищення мотивації учнів. Крім того, використання онлайн-платформ дає можливість викладачам та студентам використовувати різні формати та методи навчання, такі як відеоуроки, онлайн-тести, форуми для дискусій та багато іншого.

Окрім того, використання онлайн-платформи в освітньому процесі також забезпечують більшу прозорість та доступність інформації. Учасники навчального процесу можуть з легкістю отримати доступ до інформації про розклад занять, вимоги до оцінювання та навчальні матеріали, що зменшує ймовірність помилок та непорозумінь.

Сучасні онлайн-платформи для навчання мають значні технологічні можливості, які можуть суттєво підвищити якість та ефективність процесу навчання. Однією з найбільш важливих є можливість створення унікальних та інтерактивних навчальних матеріалів та інструментів для саморозвитку. Вона дозволяє використовувати різноманітні мультимедійні формати, такі як відео, аудіо, графіка та інтерактивні елементи, щоб зробити навчальний матеріал більш доступним, зрозумілим та запам'ятовуваним. Це особливо важливо для студентів, які мають різні стилі навчання та потребують більш гнучкого підходу до вивчення матеріалу. Крім того, багато платформ надають інструменти для створення власних навчальних матеріалів, що дозволяє викладачам та студентам створювати контент, який відповідає їх потребам та унікальним навчальним цілям. Це також може суттєво покращити ефективність навчання та підвищити мотивацію студентів. Наприклад, платформа Adobe Captivate надає можливість створювати інтерактивні навчальні курси, які можуть бути

індивідуально налаштовані під кожного студента. Ще одним прикладом є платформа Edpuzzle, яка дозволяє викладачам створювати відеоуроки з інтерактивними питаннями та завданнями. Ці приклади демонструють, як онлайн-платформи можуть бути використані для створення унікальних та інтерактивних навчальних матеріалів та інструментів для саморозвитку.

Platform	Major Traffic Country	Traffic in Million
BYJU's	India	60-70 M
Khan Academy	United States	45-55 M
Study	United States	25-30 M
Vedantu	India	25-30 M
Duolingo	United States	12-18 M
Masterclass	United States	12-18 M
Udemy	India	10-18 M
Coursera	United States	8-12 M
Instructables	United States	8-12 M
Edx	United States	3-5 M

Рис. 2. Статистика найпопулярніших онлайн-платформ у світі. Дані станом на липень 2021 року. (https://www.vdocipher.com/blog/elearning-statistics)

Існує безліч практичних прикладів успішного використання онлайн-платформ у освіті, що демонструють їх ефективність. Наприклад, Гарвардський університет використовує онлайн-платформу edX для проведення курсів, які можуть бути доступні безкоштовно для всіх бажаючих. Курс "CS50: Introduction to Computer Science" зібрав більше 2,5 мільйонів зареєстрованих студентів з усього світу, що підтверджує великий потенціал онлайн-платформ для поширення знань та доступності освіти.

Іншим прикладом є використання онлайн-платформи Coursera, яку використовують більше 200 університетів, включаючи Мічиганський університет та Каліфорнійський університет у Сан-Франциско, для проведення онлайн-курсів. Більше 77 мільйонів людей зареєструвалися на курси Coursera, що підкреслює популярність та успішність онлайн-освіти. Також варто зазначити приклад використання онлайн-платформи Khan Academy в школах США. Ця платформа надає безкоштовні відеоуроки з різних предметів, які дозволяють учням навчатися в своєму власному темпі та приділяти більше часу складним темам. Ця платформа отримала високу оцінку учнів та вчителів за її простоту використання та ефективність. Був зроблений порівняльний аналіз кількох популярних онлайн-платформ для навчання, здійснений на основі наукових досліджень та відомих відгуків:

- Google Classroom - це безкоштовна платформа, розроблена Google, яка використовується в багатьох школах та університетах для організації навчальних процесів в режимі онлайн. Вона відома своїм простим та зручним інтерфейсом, який сприяє ефективній взаємодії між вчителями та студентами. Google Classroom надає можливість створювати віртуальні класи, додавати завдання, взаємодіяти зі студентами через спеціальні функції коментування та оцінювання завдань. Вона також інтегрується з іншими продуктами Google, такими як Google Docs, Google Drive, що дозволяє зручно організовувати та зберігати навчальні матеріали.
- Moodle - це відкрита платформа для навчання, яка використовується в багатьох навчальних установах по всьому світу. Вона відома своєю гнучкістю та можливістю налаштовувати різноманітні активності, такі як форуми, тестування, завдання та інші, що дозволяє вчителям створювати різноманітні навчальні сценарії відповідно до своїх потреб.

Moodle також має велику спільноту користувачів, що надає можливість обміну досвідом та розробки нових функцій.

- Blackboard - це одна з найстаріших та відомих платформ для навчання, що використовується в багатьох університетах та вищих навчальних закладах. Вона відома своєю високою функціональністю, такою як можливість створення курсів, завдань, форумів, тестувань та інших активностей. Вона також має розширені можливості для взаємодії зі студентами, включаючи можливість надавати зворотний зв'язок та оцінювати роботи. Blackboard також надає інструменти для ведення електронного журналу та моніторингу активності студентів, що дозволяє вчителям відстежувати прогрес студентів.
- Coursera - це онлайн-платформа для навчання, яка спеціалізується на вищій освіті та пропонує віртуальні курси від провідних університетів та організацій по всьому світу. Вона відома своєю високою якістю навчання, професійними викладачами та різноманітністю курсів з різних галузей знань. Coursera надає можливість студентам проходити курси у власному темпі, має вбудовану систему оцінювання та забезпечує доступ до різноманітних навчальних ресурсів.
- EdX - це ще одна відома онлайн-платформа для навчання, яка пропонує курси від провідних університетів та організацій. Вона відома своєю відкритістю та безкоштовним доступом до багатьох курсів, а також своєю акцентом на науковій та технічній освіті. EdX також надає можливість проходити курси за власним графіком та взаємодіяти з викладачами та іншими студентами.
- Schoology - це платформа для навчання, спрямована на розподілені школи та навчальні заклади. Вона надає вчителям можливість створювати віртуальні класи, додавати матеріали, давати завдання, забезпечувати зворотній зв'язок та оцінювати роботи студентів. Особлива риса Schoology - це можливість налаштовувати процес навчання з урахуванням індивідуальних потреб студентів, розробляти персоналізовані навчальні плани та використовувати аналітику для відстеження успішності студентів.
- Edmodo - це соціальна мережа для навчання, яка забезпечує можливість створювати віртуальні класи, спілкуватися зі студентами, додавати матеріали та завдання, оцінювати роботи студентів та проводити тести. Вона також дозволяє вчителям створювати спільноти та співпрацювати з іншими вчителями, обмінюватися ресурсами та ідеями. Edmodo має також функції для забезпечення безпеки та конфіденційності даних студентів.

Імерсивні технології та їх роль у навчанні. Інклюзивне навчання, що передбачає можливості для різних типів учнів, включаючи тих, хто має особливі освітні потреби, є важливим напрямом розвитку освіти в сучасному світі. Одним з потужних інструментів, який може сприяти реалізації інклюзивного навчання, є використання імерсивних технологій. Імерсивні технології, такі як віртуальна реальність (VR), розширена реальність (AR) та змішана реальність (MR), забезпечують користувачам унікальні можливості взаємодії з віртуальним оточенням та досвідом, що може бути багатоцільовим і відповідати різним освітнім потребам.

Одним з важливих аспектів імерсивних технологій в контексті інклюзивного навчання є можливість створення доступного навчального середовища. Завдяки використанню VR, AR або MR, можна створити віртуальні класні кімнати, в яких можуть брати участь учні з різними освітніми потребами, включаючи тих, хто має фізичні обмеження, аутизм, дислексію та інші відхилення. Наприклад, віртуальна реальність може надати можливість учням з фізичними обмеженнями взаємодіяти з віртуальним оточенням, відтворюючи реальний світ, який може бути недоступним для них в реальному житті. AR може бути використана для візуалізації складних концепцій або взаємодії з навколишнім середовищем, забезпечуючи можливість взаємодії з віртуальними об'єктами в реальному часі. Змішана реальність може забезпечити комбінацію віртуальних та реальних елементів, що може сприяти більшій взаємодії та зрозумінню матеріалу для учнів з різними типами сприйняття.

Іншим важливим аспектом використання імерсивних технологій в інклюзивному навчанні є можливість індивідуалізації навчального процесу. Завдяки інтерактивності та гнучкості імерсивних технологій, учні можуть вчитися власним темпом, відповідно до своїх

потреб та рівня навчання. Віртуальні симуляції, наприклад, можуть надати можливість учням випробувати різні сценарії та вирішувати завдання, що відповідають їхнім особистим потребам та здібностям.

Крім того, імерсивні технології можуть забезпечити більш активну та залучену участь учнів у навчальному процесі. Завдяки можливості взаємодії з віртуальними об'єктами та оточенням, учні можуть відчувати більшу мотивацію до вивчення матеріалу, використовувати свої навички та розвивати критичне мислення.

Проте, варто відзначити, що використання імерсивних технологій в інклюзивному навчанні також вимагає ретельного підходу до планування та розробки навчальних матеріалів, а також врахування різноманітних освітніх потреб учнів. Додатково, важливо враховувати етичні аспекти використання імерсивних технологій в інклюзивному навчанні. Наприклад, необхідно враховувати можливість виникнення дискримінації або стереотипів у віртуальних середовищах, які можуть вплинути на деякі групи учнів. Також варто враховувати захист персональних даних учнів та забезпечення кібербезпеки в процесі використання імерсивних технологій.

Важливо забезпечити доступність імерсивних технологій для всіх учнів, включаючи тих, хто має фізичні, сенсорні або когнітивні обмеження. Наприклад, використання контролерів рухів або інших альтернативних інтерфейсів може забезпечити доступність для учнів з обмеженою рухливістю. Забезпечення адаптивності інтерфейсів, взаємодії та контенту може допомогти учням з різними особливостями в сприйнятті та сприяти їхньому повноцінному навчанню.

Безпека даних. З використанням онлайн-платформ у навчанні існують деякі проблеми, які можуть негативно впливати на якість освіти. Однією з таких проблем є безпека даних. У онлайн-середовищі, де персональні дані зберігаються та обробляються, існує ризик їх утікання та використання зловмисниками. Недавно був виявлений випадок взлому бази даних онлайн-школи Edmodo, де зловмисники отримали доступ до особистих даних учнів та вчителів, включаючи їх імена, адреси електронної пошти та хешовані паролі. Також, при використанні хмарних сервісів, дані можуть бути доступні третім особам, якщо не вживати необхідні заходи безпеки. У 2020 році, через пандемію COVID-19, були зареєстровані декілька випадків порушення безпеки на популярних платформах для дистанційного навчання, таких як Zoom та Microsoft Teams. Такі витоки можуть призвести до серйозних наслідків, таких як крадіжка особистості та шахрайство, що може негативно позначитися на довірі до онлайн-платформ в цілому.

Іншою проблемою, пов'язаною з використанням онлайн-платформ, є недостатня соціальна інтерактивність. На відміну від традиційних освітніх методів, які включають у себе спілкування в класі та співпрацю з іншими учнями, онлайн-платформи можуть створювати відчуття ізоляції та відсутності спілкування. Деякі учні можуть відчувати себе некомфортно у віртуальному середовищі та втрачати інтерес до навчання. Наприклад, у дослідженні, проведеному в Швеції, виявлено, що учні, які використовували онлайн-платформи як основний інструмент навчання, мали великі труднощі з комунікацією з іншими учнями та отримували низькі оцінки за соціальну підтримку.

Ще однією проблемою, пов'язаною з використанням онлайн-платформ, є віддаленість від викладача та відсутність можливості отримати негайну відповідь на запитання. У традиційній освіті студенти можуть задавати запитання та отримувати відповіді від викладача під час занять. Однак, на онлайн-платформах, зокрема в масових відкритих онлайн-курсах, цей процес може бути ускладненим через велику кількість студентів та відсутність особистого контакту з викладачем. Для вирішення цих проблем необхідно приймати заходи щодо підвищення безпеки даних, такі як використання сучасних технологій шифрування та двохфакторної аутентифікації. Крім того, потрібно приділяти більше уваги соціальній інтерактивності в онлайн-навчанні, наприклад, пропонуючи можливості для спілкування з іншими учнями та організовуючи спільні проекти та дискусії. Такі заходи допоможуть створити більш комфортне та інтерактивне навчальне середовище, яке буде більш

привабливим для учнів та підвищить якість освіти. Також слід враховувати, що онлайн-навчання не повинно повністю заміняти традиційні методи навчання, а повинно використовуватись як доповнення до них. Традиційні методи навчання, такі як спілкування в класі, взаємодія з вчителями та співпраця з іншими учнями, мають важливе значення для розвитку соціальних навичок та особистісного зростання учнів. Також не всі типи матеріалів можна ефективно навчати онлайн. Деякі навчальні дисципліни, такі як музика, образотворче мистецтво та фізична культура, вимагають присутності вчителя та реальної взаємодії з іншими студентами.

Висновки. У даній науковій роботі були розглянуті основні аспекти використання онлайн-платформ в освіті. Були розглянуті різні типи платформ, такі як мобільні додатки, онлайн-курси, вебінари та інші, а також технологічні можливості, які дозволяють створювати унікальні та інтерактивні навчальні матеріали та інструменти для саморозвитку.

Далі були представлені практичні приклади використання онлайн-платформ у різних освітніх установах та була показана їхня ефективність. Однак були виявлені проблеми, пов'язані з безпекою даних, недостатньою соціальною інтерактивністю та можливою заміною традиційних методів навчання. В результаті аналізу було зроблено висновок, що онлайн-навчання повинно розглядатися як доповнення до традиційних методів навчання, а не як їхня повна заміна. Використання онлайн-платформ в освіті може значно розширити можливості навчання та забезпечити доступність освіти для всіх категорій населення. Для того, щоб ефективно використовувати онлайн-платформи в освіті, необхідно вирішувати проблеми, пов'язані з безпекою даних та соціальною інтерактивністю, та стимулювати розвиток таких платформ з урахуванням індивідуальних потреб учнів. Також слід забезпечувати підтримку для традиційних методів навчання та використовувати онлайн-платформи в поєднанні з ними.

Список використаних джерел

1. The Chronicle of Higher Education. "Coursera Announces Details for Selling Certificates and Verifying Identities" \\ Режим доступу: http://chronicle.com/blogs/wiredcampus/coursera-announces-details-for-selling-certificates-and-verifying-identities/ (останнє звернення 30.03.2023р.)
2. "Benefits of e-learning", eLearning Industry \\ Режим доступу: https://elearningindustry.com/benefits-of-elearning (останнє звернення 30.03.2023р.)
3. Understanding Different Types Of Online Education \\ Режим доступу: https://www.edtechreview.in/elearning/understanding-different-types-of-online-education/ (останнє звернення 30.03.2023р.)
4. 8 Reasons Your Company Should Prioritize Remote Learning \\ Режим доступу: https://www.learndash.com/8-reasons-your-company-should-prioritize-remote-learning/ (останнє звернення 30.03.2023р.)
5. The New Story of Online Education Has Yet To Be Written \\ Режим доступу: https://elearningindustry.com/the-new-story-of-online-education-has-yet-to-be-written (останнє звернення 30.03.2023р.)
6. "Top eLearning Authoring Tools", eLearning Industry \\ Режим доступу: https://elearningindustry.com/directory/software-categories/elearning-authoring-tools (останнє звернення 30.03.2023р.)
7. Udemy. "Udemy: Online Courses Anytime, Anywhere" \\ Режим доступу: https://www.udemy.com/about/ (останнє звернення 30.03.2023р.)

Робота виконана під науковим керівництвом к.е.н., доцента
ПАЛАГУТИ К.О.

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ НА ПІДПРИЄМСТВІ

САЛОГУБ В., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні принципи, методи та засоби захисту персональних даних. Розглядаються найбільш поширені загрози для безпеки персональних даних в інтернеті, такі як хакерські атаки, шахрайство та фішинг. Зазначено особливості зберігання персональних даних у безпечному місці і захист їх від несанкціонованого доступу, оскільки використання цих даних може стати причиною крадіжки особистої інформації, фінансового шахрайства та інших злочинів. Досліджено процес захисту конфіденційності, цілісності та доступності персональної інформації, що збирається та обробляється підприємствами, державними установами та іншими суб'єктами обробки персональних даних

The article discusses the basic principles and methods of protecting personal data. The most common threats to the security of personal data in the internet, such as hacking attacks, fraud, and phishing, are examined. The article highlights the peculiarities of storing personal data in a secure location and protecting it from unauthorized access, as the use of such data can lead to theft of personal information, financial fraud, and other crimes. The process of protecting the confidentiality, integrity, and availability of personal information collected and processed by businesses, government agencies, and other data processors is also explored.

Актуальність. На сьогоднішній день питання захисту персональних даних постає особливо гостро для державних установ та підприємств, які в силу своєї діяльності агрегують та використовують відомості про фізичну особу. Відповідно Закону України «Про захист персональних даних», Закону «Про захист інформації в інформаційно-телекомунікаційних системах» та багатьох підзаконних нормативних актів такі відомості повинні захищатись від несанкціонованого ознайомлення, модифікації та розповсюдження. На тлі стрімкого розвитку технологій інформація про людину стала цінним товаром, а оборот ринку, де торгують персональними даними, оцінюється мільярдами доларів. Підписавши Угоду про асоціацію з ЄС, Україна погодилась на забезпечення захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів. Тому ухвалення нового закону «Про захист персональних даних» є обов'язковим для інтеграції України в ЄС. Виходячи з євроінтеграційних прагнень України, ухвалення цього закону має особливу важливість, адже для того щоб наша держава стала повноцінним членом ЄС, ми повинні відповідати стандартам Євросоюзу в різних галузях. І одна з таких галузей – це забезпечення права на приватність, іншими словами – захист персональних даних.

Захист персональних даних є важливою темою в сучасному світі, оскільки зростає кількість зловмисників, які намагаються використовувати ці дані зі злочинними цілями. Тому необхідно дотримуватися певних правил та процедур, щоб забезпечити захист персональних даних.

Мета статті – проаналізувати механізми захисту персональних даних користувачів.

Об'єктом дослідження є аналіз методів та засобів захисту персональних даних користувачів на підприємстві.

Предмет дослідження – персональні дані користувачів на підприємстві.

Аналіз попередніх досліджень. На сьогодні саме персональні дані та інформація є знаряддям гібридної війни Російської Федерації проти нашої держави. Інформація використовується як інструмент скоєння правопорушень, також активно використовується в політиці і веденні інформаційних війн. Вивченням проблематики захисту персональних даних

займались провідні науковці О.О. Золотар, А.Ю. Нашинець-Наумова, Т.С. Перун, А.Ю. Щербіна. Проте, сьогоденний стан теоретико-практичного забезпечення адміністративно-правового режиму інформаційної безпеки в Україні, не в повній мірі відповідає вимогам ситуації, що склалася у зв'язку з веденням Російською Федерацією війни проти України.

Виклад основного матеріалу. У сучасних умовах суспільного розвитку, питання захисту персональних даних активно обговорюється не лише на національному рівні, а й на міжнародному. Це спричинено основною мірою вчинення правопорушень щодо незаконних дій щодо персональних даних осіб, що є суб'єктами певних міжнародних операцій [1].

Одним з найбільш проблемних питань в еру інформаційних технологій є захист персональних даних. До того ж у світі, поглиненому глобалізацією, дані користувача однієї країни можуть використовувати треті особи з будь-якого куточка світу (в тому числі незаконно). Проблеми захисту персональних даних можуть виникати в різних сферах життя, включаючи інтернет, медичну та фінансову галузі, державні органи, мережі соціальних мереж та інші. Персональні дані − це будь-яка інформація, що може ідентифікувати конкретну особу. Це може бути ім'я, адреса, номер телефону, адреса електронної пошти, фотографії, номери документів тощо. Відповідно до Закону України «Про захист персональних даних», персональні дані класифікуються на три категорії [2]:

1. Загальні персональні дані − це інформація про фізичну особу, яка ідентифікується або може бути ідентифікована, включаючи, наприклад, ім'я, прізвище, адресу, номер телефону, електронну адресу тощо.
2. Спеціальні категорії персональних даних − це інформація про расу, національність, політичні переконання, релігійні чи філософські переконання, стан здоров'я, статеву орієнтацію, сексуальну поведінку та інші особливо чутливі дані.
3. Біометричні персональні дані − це інформація, яка отримується в результаті біометричної ідентифікації фізичної особи, така як відбитки пальців, голос, обличчя, форма долоні та інші біометричні ознаки.

Закон України «Про захист персональних даних» встановлює спеціальні правила щодо обробки кожної з цих категорій персональних даних. Так, для обробки спеціальних категорій персональних даних потрібно отримати додаткову згоду фізичної особи або мати іншу підставу для такої обробки. А обробка біометричних персональних даних можлива лише за згодою фізичної особи або за наявності іншої підстави, встановленої законодавством.

Персональні дані можуть бути класифіковані за різними критеріями. Найбільш поширеною класифікацією є та, яка відповідає регуляторному середовищу Європейського Союзу, зокрема захищених Загальним регламентом про захист персональних даних (GDPR), який захищає конфіденційність таких даних: основна інформація про особу; веб-дані; IP-адреса; дані-cookie та теги RFID; біометричні дані тощо. Ця класифікація дозволяє розуміти, які типи персональних даних збираються та обробляються компаніями та організаціями (Рис. 1) [1, 3, 5].

Щоразу після оцінювання відповідного рівня захисту варто враховувати ризики, які спричиняє обробка, зокрема випадкове або незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних. GDPR вказує на шифрування, як на основну вимогу безпеки даних. Окрім цього, підприємствам потрібно оцінити ризики, а потім вжити заходів, що пом'якшують ризики, які вони виявляють. Оскільки жодне підприємство не може повністю визначити або передбачити всі ризики для своїх даних, і жоден підхід до периметра безпеки не є надійним, підприємства повинні шифрувати свої дані, щоб забезпечити відповідність до GDPR [4]. За допомогою шифрування, не залежно від того чи є порушення, дані будуть належно захищені. Ядром системи захисту є програмно-апаратний комплекс Keysecure, залежно від типу даних. Навколо Keysecure, залежно від типу даних, що мають захищатися, архітектури системи зберігання даних та сервісів, що беруть участь в обробці даних, можна застосовувати такі програмні продукти Gemalto:

- ProtectV – для шифрування диків віртуальних машин VMWare, AWS, Asure;
- ProtectDB – для шифрування баз даних Oracle, MS SQL, IBM DB2, Teradata;

- ProtectFile – для вибіркового шифрування папок та файлів на робочих станціях користувачів та файлових серверах Windows Linux.

Рис. 1. Вимоги до обробки персональних даних згідно GDPR

Gemalto пропонує широкий вибір продуктів для забезпечення надійної аутентифікації користувачів, що складається з аутентифікаторів на основі особистого сертифікату користувача (eToken, Smartcard MD Prime), генераторів одноразових паролів (Mobile PASS), систем (SAC, SAM, SAS, Network Logon)

Важливо зберігати персональні дані у безпечному місці і захищати їх від несанкціонованого доступу, оскільки використання цих даних може стати причиною крадіжки особистості, фінансового шахрайства та інших злочинів. Згідно з GDPR, персональні дані можуть бути класифіковані наступним чином:

1. Основні персональні дані − це дані, які можуть ідентифікувати конкретну особу, такі як ім'я, прізвище, адреса, номер телефону та ін.
2. Спеціальні категорії персональних даних − це дані, які стосуються особливих категорій осіб, таких як інформація про расову або етнічну належність, політичні переконання, релігійні переконання, громадянство, генетичні та біометричні дані, стан здоров'я та інші.
3. Дані про користувача − це дані, які збираються на основі взаємодії користувача з продуктом або послугою, такі як IP-адреса, історія перегляду, дані про використання тощо.
4. Дані про транзакції − це дані, які стосуються фінансових транзакцій, такі як дані про кредитні картки та банківські рахунки.
5. Дані про місцезнаходження − це дані, які пов'язані з місцезнаходженням користувача, такі як GPS-координати та інші дані про місцезнаходження.

За рівнем конфіденційності персональні дані можна поділити на дві категорії: загальнодоступні та конфіденційні. Загальнодоступні дані − це дані, які доступні для загального використання та не містять конфіденційної інформації, такі як ім'я, адреса електронної пошти та номер телефону. Конфіденційні дані − це дані, що містять особисту інформацію, таку як медична інформація, фінансові дані, номера соціального страхування тощо. За призначенням персональні дані можна класифікувати на декілька видів: для ідентифікації, для контактів, для відслідковування та інших цілей. Дані для ідентифікації містять інформацію, яка дозволяє ідентифікувати конкретну особу, наприклад, ім'я, прізвище та дата народження.

Витік персональних даних може бути наслідком багатьох факторів, включаючи кібератаки, недостатньо захищені мережі та пристрої, недбале ставлення до обробки даних та

несанкціонований доступ до інформації. Ось деякі загрози, які пов'язані з витоком персональних даних [2, 4]:

1. Крадіжка особистої інформації: злочинці можуть використовувати викрадені персональні дані, щоб скоїти шахрайства, відкрити кредитні картки, взяти кредити чи отримати інші види фінансових послуг на ім'я потерпілого.
2. Соціальна інженерія: злочинці можуть використовувати викрадені персональні дані, щоб переконати людей поділитися іншою конфіденційною інформацією.
3. Рекламні кампанії: деякі компанії можуть збирати та продавати персональні дані, щоб показувати рекламу, яка пристосована під конкретного користувача. Однак, якщо ці дані потраплять у руки зловмисників, вони можуть бути використані для здійснення шахрайств.
4. Викрадення конфіденційної інформації: викрадені персональні дані можуть містити конфіденційну інформацію про бізнеси та їх клієнтів. Ця інформація може бути використана для здійснення крадіжок і торгівлі на чорному ринку.

Кібератаки – це одна з найбільш серйозних загроз для безпеки персональних даних. Кібератаки можуть бути спрямовані на викрадення, втручання або вивчення персональних даних. Ось деякі типи кібератак, які можуть бути спрямовані на персональні дані:

- Фішинг – атака, в якій злочинці намагаються зловити користувачів шляхом підробки веб-сайтів або електронних листів, щоб отримати доступ до їх персональних даних, таких як ім'я, адреса електронної пошти, пароль тощо.
- Віруси і шпигунське програмне забезпечення – програми можуть бути розроблені для збору персональних даних користувачів без їх знання або згоди. Віруси можуть також використовуватися для знищення або зміни персональних даних. Розповсюдження шкідливих програм – атака, при якій зловмисники використовують вразливості в програмному забезпеченні, щоб отримати доступ до персональних даних. Шкідлива програма може бути розповсюджена через електронну пошту, файлообмінні мережі, підроблені веб-сайти.
- DDoS-атаки – атаки, в яких злочинці використовують ботнет, щоб перенавантажити сервер веб-сайту, що призводить до його недоступності. Ця атака може бути використана для викрадення персональних даних з серверів веб-сайту.
- SQL-ін’єкції – атаки, в яких злочинці використовують вразливості в програмному забезпеченні веб-сайту, щоб отримати доступ до бази даних, де зберігаються персональні дані користувачів.
- Zero-day атаки – атаки, в яких злочинці використовують вразливості в програмному забезпеченні, які ще не були виявлені розробниками або ще не були виправлені.

Персональні дані потрібно захищати з багатьох причин. По-перше, такі дані містять конфіденційну інформацію про особу, що може бути використана для крадіжки особистості, злочинних дій або недобросовісної діяльності. По-друге, захист персональних даних є важливою складовою прав людини на приватність, інші конституційні та законодавчі права, що забезпечують гідність та свободу особи. Крім того, велика кількість компаній та установ збирають та зберігають персональні дані своїх клієнтів, співробітників та інших осіб. Ці дані можуть бути використані для різних цілей, наприклад, для реклами, маркетингу, аналітики, наукових досліджень тощо. Однак, це також означає, що зберігання та обробка персональних даних потребують дотримання певних стандартів та законодавчих вимог, щоб уникнути порушення приватності та інших прав особи.

Захист персональних даних – це процес захисту конфіденційності, цілісності та доступності персональної інформації, що збирається та обробляється підприємствами, державними установами та іншими суб'єктами обробки персональних даних. Це може включати будь-які дії з персональною інформацією, такі як збір, зберігання, використання, передача та видалення. Захист персональних даних є важливою проблемою в інформаційному суспільстві, оскільки все більше людей використовують Інтернет і здають свої персональні дані на зберігання. Основні принципи захисту персональних даних включають (Рис. 2) [5]:

1. Збір та обробка персональних даних повинні здійснюватися лише за наявності згоди власника даних або на законній підставі. Обробка персональних даних має здійснюватися на законній підставі, відповідно до засад справедливості та прозорості.
2. Легальність, справедливість та прозорість – персональні дані повинні збиратися та оброблятися законно, справедливо та прозоро.
3. Обмеження фінальності – персональні дані повинні збиратися тільки для визначених, конкретних та законних цілей.
4. Точність – персональні дані повинні бути точними та актуальними.
5. Обмеження зберігання – персональні дані повинні зберігатися лише протягом необхідного часу. Збереження персональних даних повинно здійснюватися в безпечному та захищеному від несанкціонованого доступу місці.
6. Дані мають бути оброблені тільки у визначені цілях, за якими вони були зібрані. Дані мають бути достовірні, повні та актуальні.
7. Мінімізація обробки – обробка персональних даних має обмежуватись лише тими даними, які є необхідними.
8. Конфіденційність та безпека – означає, щоб персональні дані були захищені від несанкціонованого доступу, втрати, зміни або пошкодження, а також щоб вони оброблялися відповідно до вимог конфіденційності та безпеки.

Рис.2. Основні принципи захисту персональних даних

Основні проблеми захисту персональних даних включають:

1. Втрата даних: компанії можуть втратити дані через неналежне зберігання, катастрофи або технічні проблеми. Це може призвести до втрати особистих даних та порушення приватності.
2. Крадіжка даних: хакери можуть зламати систему безпеки компанії і отримати доступ до бази даних з персональними даними користувачів. Це може стати причиною крадіжки особистих даних та ідентифікації особи.
3. Крадіжка даних: хакери можуть зламати систему безпеки компанії і отримати доступ до бази даних з персональними даними користувачів. Це може стати причиною крадіжки особистих даних та ідентифікації особи.
4. Використання даних без дозволу: деякі компанії можуть використовувати персональні дані користувачів без їхньої згоди для реклами, маркетингу або інших цілей. Це може порушувати права на приватність користувачів.

5. Недостатній захист даних: компанії можуть мати недостатній рівень захисту даних, що може стати причиною крадіжки та витоку персональних даних.
6. Спільний доступ до даних: деякі компанії можуть передавати персональний доступ користувачам.

Типові підходи аналізу, організації та забезпечення захисту персональних даних під час їх автоматизованої обробки включають в себе [3, 5]:

- класифікацію інформації в інформаційно-телекомунікаційній системі (ІТС) з визначенням окремих характеристик та технологій обробки персональних даних;
- реалізацію відповідних юридично-правових та організаційно-розпорядчих заходів щодо використання персональних даних на підприємстві;
- підготовка договорів та протоколів із фізичними особами щодо використання їх персональної інформації;
- підготовка відповідних внутрішніх розпоряджень щодо експлуатації автоматизованих систем, призначених для обробки персональних даних;
- підготовка відповідних регламентних документів щодо доступу та використання персональних даних, які збираються та накопичуються в рамках баз даних;
- виконання робіт для реєстрації бази персональних даних в рамках єдиного Державного реєстру баз персональних даних;
- створення комплексної системи захисту інформації в автоматизованих системах, призначених для обробки персональних даних відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закону «Про захист персональних даних»;
- організація та проведення державної експертизи комплексної системи захисту інформації в автоматизованих системах, призначених для обробки персональних даних.

Існує багато технологій захисту персональних даних, які можуть бути використані для захисту конфіденційної інформації: шифрування даних, хешування, маскування даних, техніки розподілу ключів, безпечний протокол передачі, безпечне зберігання даних, багаторівневий доступ до даних, контроль доступу, антивірусне програмне забезпечення, захист мереж, аутентифікація користувача, захист пристроїв [2, 6].

Шифрування даних − це процес перетворення звичайного тексту в зашифрований варіант, який може бути прочитаний лише за допомогою ключа шифрування. Шифрування може бути застосоване до різних типів даних, включаючи електронні повідомлення, файли, бази даних та інші. Криптографія використовується для забезпечення конфіденційності та цілісності даних шляхом шифрування даних, щоб зробити їх нерозбірливими для сторонніх користувачів. Два основні методи криптографії − симетричний та асиметричний [6]. Хешування: хеш-функції перетворюють вхідні дані будь-якої довжини в фіксований вихідний розмір. Це дозволяє використовувати дані, не розкриваючи їх в оригінальному форматі.

Маскування даних − метод захисту персональних даних використовується для забезпечення конфіденційності даних, замінюючи значення чутливих даних на значення, які є безпечними для публічного використання. Наприклад, можна замаскувати персональні дані, такі як ім'я та адреса, залишивши тільки першу літеру.

Техніки розподілу ключів − методи, які дозволяють безпечно розподілити ключі шифрування між декількома користувачами, що забезпечує безпеку при обміні даними. Підписи − математичний метод, що дозволяє довести автентичність даних. Підписи створюються з використанням приватного ключа і перевіряються з використанням відкритого ключа. Безпечний протокол передачі даних − такий протокол забезпечує захист від перехоплення та зміни даних під час їх передачі по мережі. Найбільш поширеними протоколами є HTTPS, SSH, SFTP та інші. Безпечне зберігання даних − це використання спеціальних алгоритмів та методів для забезпечення безпеки даних під час їх зберігання на сервері або в базі даних. Найбільш поширеними методами є резервне копіювання даних, контроль цілісності даних та їх реплікація на різних серверах.

Багаторівневий доступ до даних − це використання різних рівнів доступу до даних залежно від рівня доступу користувача. Наприклад, для адміністраторів доступ до конфіденційної інформації може бути обмеженим, а для звичайних користувачів − обмеженим лише до відкритої інформації. Контроль доступу − це технологія, що забезпечує обмеження доступу до конфіденційної інформації лише для користувачів, які мають необхідні дозволи для цього. Контроль доступу може використовувати методи, такі як базова та двофакторна аутентифікація або ідентифікація по IP-адресі. Аутентифікація користувача − процес перевірки, що користувач, який намагається отримати доступ до системи, є тим, за кого він себе видає. Може включати в себе використання пароля, біометричних даних, токенів або інших методів ідентифікації користувача.

Антивірусне програмне забезпечення − це програмне забезпечення, що допомагає захистити комп'ютер від вірусів та шкідливих програм, які можуть призвести до витоку персональних даних. Захист мереж − це технології, які використовуються для захисту мережі від атак зовнішніх користувачів, таких як хакери. Це може включати в себе використання мережевих файрволів, систем виявлення вторгнень та інших технологій. Захист пристроїв − це технології, які використовуються для захисту пристроїв від зловмисних програм та інших загроз безпеці, що можуть використовувати вразливості операції.

Висновки. Захист персональних даних користувачів в інтернеті є надзвичайно важливим, оскільки використання цих даних без дозволу може призвести до серйозних наслідків, таких як крадіжка особистої інформації, фінансові та інші злочини. Основні методи і засоби захисту персональних даних включають криптографію, хешування, перетворення, маскування даних, сильні паролі, двофакторну автентифікацію та засоби шифрування даних для забезпечення максимального захисту особистої інформації. Для того, щоб захистити свої персональні дані, користувачам слід також звертати увагу на дотримання вимог законодавства з питань захисту персональних даних та бути обережними при наданні своєї особистої інформації в інтернеті. Для забезпечення максимального захисту персональних даних необхідно використовувати всі доступні засоби та методи захисту, щоб зменшити ризики їхньої крадіжки та зловживання.

Список використаних джерел

1. Мачуський В. Захист персональних даних на підприємстві. – URL: *https://www.businesslaw.org.ua/zahyst-personalnyx-danyx-na-pidpryemstvi/*
2. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.
3. Щербіна А.В., Макушев П.В. Поняття персональних даних та загальні правові засади їх використання: іноземний досвід. Право і суспільство. – 2013, № 2. – С. 70-76.
4. Німченко, Т.В. Алгоритм виявлення несанкціонованого витоку персональних даних мережевими каналами. / Т.В. Німченко, І.М. Мужик, А.І. Мужик // Вісник інженерної академії України, 2014. − № 3-4. − С. 199-203.
5. Шабатура М.М., Салашник Р.О. Аналіз методів захисту персональних даних за українським законодавством і GDPR. 2021, т. 3, 2. С. 51-57.
6. Козак В. Захист персональних даних та правила приватності при дослідженнях в Інтернет. – URL: *http://uam.in.ua/upload/medialibrary/de7/de7199d7eeaf41d8582cbff76d2f4368.pdf*

Робота виконана під науковим керівництвом к.т.н., доцента
САВЧЕНКО Т.В.

ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

САМОЙЛЕНКО Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто криптографічні методи та інструменти для захисту інформації, які є важливою частиною повної системи захисту інформації. Зазначено різні методи шифрування та пояснено, що таке електронні підписи. Також проаналізовано законодавчу базу для застосування криптографічних методів захисту інформації.

The article discusses cryptographic methods and tools for information protection, which are an important part of a complete information security system. Various encryption methods are mentioned and electronic signatures are explained. The legislative framework for the use of cryptographic methods for information protection is also analyzed.

Актуальність. Для повного задоволення потреб сучасного суспільства необхідне інформаційне забезпечення всіх сфер людської діяльності і, зокрема, надійний захист інформації. Особливо гостро ця проблема постає у зв'язку з масовою комп'ютеризацією, об'єднанням комп'ютерів у комп'ютерні мережі та використання Інтернету.

Теорія захисту інформації доводить, що якщо система захисту побудована з урахуванням усіх сучасних методів і засобів захисту, а також якщо на підприємстві є ретельно відібраний і навчений персонал, який не робить помилки, то дії зловмисників у такій системі неможливі. Однак це не зовсім так. З часом система захисту застаріває, змінюється персонал і втрачається пильність, зловмисники знаходять нові способи атак і способи подолання захисту, які були невідомі на момент створення системи захисту.

Отже, якщо у вас є розуміння щодо надійності вашої інформаційної безпеки, безпеки системи, все ж слід пам'ятати основне правило: жодна система захисту не може довго протистояти цілеспрямованим діям вмілого зловмисника, озброєного сучасною технікою. Це правило розроблено багаторічним досвідом фахівців з інформаційної безпеки і є універсальним. Це не залежить від рівня захисту, доброчесності користувачів і адміністраторів, апаратного та програмного забезпечення. Правило стверджує, що проблема не в тому, чи зловмисники зламають систему захисту, а в тому, коли вони це зроблять. І мета захисту інформації полягає в тому, щоб збій системи стався якомога пізніше.

Аналіз останніх досліджень і публікацій. Проблемам створення та функціонування засобів криптографічного захисту інформації присвячено достатньо публікацій у відкритих джерелах, зокрема таких науковців, як Пономаренко В.С. [1], Вербицький О.В. [2], Хорошко В. А. [3], Фаль О.М. [4].

Пономаренко В.С. у своїх працях у системній формі розглядає питання створення симетричних та асиметричних криптографічних систем захисту інформації.

Вчений Вербицький О.В. вивчає проблеми протидії та розслідування злочинів, скоєних у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж.

Вчені Хорошко В. А. та Фаль О. М. описують засоби теорії дискового шифрування, процедури управління ключами, основи розробки та впровадження криптографічних засобів. протоколи та механізм електронного цифрового підпису.

Мета статті. Визначити та опрацювати основні криптографічні методи та засоби захисту, види шифрування. Проаналізувати програмне забезпечення іноземних та українських розробників, призначене для криптографічного захисту інформації.

Об'єктом дослідження є використання різних методів криптографічного захисту інформаційних ресурсів.

Предметом дослідження є криптографічний захист.

Виклад основного матеріалу. Одним із елементів комплексної системи захисту інформації є криптографічний захист інформації. Цей вид захисту інформації реалізується шляхом перетворення інформації за допомогою ключів на основі математичних методів. Використання криптографічних методів має дві мети - приховати інформацію шляхом її шифрування та підтвердити значущість документів за допомогою електронного цифрового підпису. Іншими словами, на думку В. В. Поповського, криптографічні методи вирішують дві задачі – забезпечення конфіденційності інформації шляхом запобігання витягу зловмисником інформації з каналу зв'язку та забезпечення цілісності інформації шляхом запобігання зміні інформації та внесенню в неї неправдивого змісту [1].

Існує два розділи науки, пов'язані з криптографічними методами: криптографія і криптоаналіз, які разом утворюють криптологію.

Криптографія вивчає математичні перетворення, які дозволяють шифрувати інформацію.

Криптоаналіз вивчає методи дешифрування без знання секретного ключа [1].

Засоби криптографічного захисту інформації поділяються на:

- засоби, що реалізують криптографічні алгоритми перетворення інформації;
- засоби, системи та комплекси захисту від нав'язування неправдивої інформації з використанням криптографічних алгоритмів перетворення інформації
- засоби, системи та комплекси, призначені для виготовлення та розповсюдження ключів криптографічний захист інформації;
- системи та комплекси, що входять до комплексів захисту інформації від несанкціонованого доступу та використовують криптографічні алгоритми перетворення інформації [2].

Засоби криптографічного захисту разом із ключем та іншими видами документації, які забезпечують необхідний рівень захисту, утворюють криптографічну систему [2]. Шифрування дозволяє захистити інформацію шляхом перетворення її в незрозумілий текст (шифртекст) з можливістю подальшого розшифрування (дешифрування). Шифрувати можна як прості тексти, так і комп'ютерні файли.

Рис. 1. Алгоритм шифрування данних

Шифрування поділяється на симетричне та асиметричне.

Симетричне шифрування використовує один секретний ключ як для шифрування, так і для дешифрування. Асиметричне шифрування використовує відкритий ключ і інший секретний ключ для дешифрування, згенерований за допомогою генераторів псевдовипадкових чисел.

Асиметричне шифрування також називається шифруванням з відкритим ключем. Недоліком симетричного шифрування є необхідність передачі ключа особі адресованого тексту, що тягне за собою його розкриття та дешифрування інформації зловмисниками. Перевагою симетричного шифрування є його вища швидкість, ніж асиметричне шифрування, оскільки асиметричне шифрування використовує довші ключі, що збільшує час шифрування.

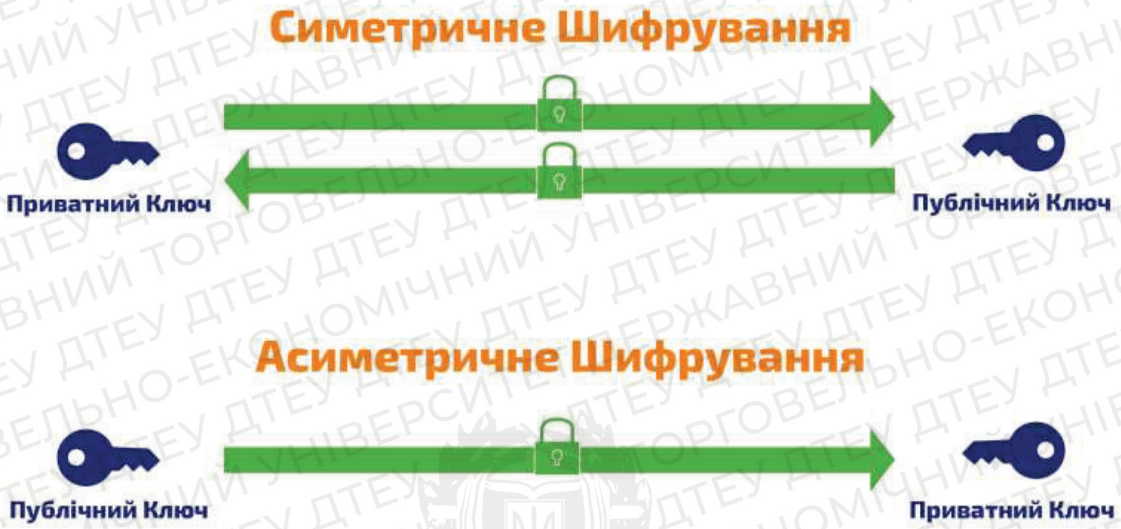


Рис. 2. Схема симетричного і асиметричного шифрування

Спосіб шифрування тексту базується на алгоритмі, і зашифрований текст можна розшифрувати лише за допомогою ключа. Для надсилання повідомлень різним одержувачам можна використовувати один алгоритм з різними ключами. Секретність визначається ключем, а не алгоритмом, оскільки більшість алгоритмів відомі широкому загалу. У зв'язку зі збільшенням продуктивності комп'ютера ймовірність знаходження ключів шляхом перебору комбінацій зростає, тому нам доводиться використовувати все довші й довші ключі, що збільшує час на шифрування [3]. Важливою характеристикою методів шифрування є їх криптостійкість, тобто для криптографічного захисту інформації в комп'ютерній мережі необхідно створити спеціальний сервіс, який генерує ключі та розповсюджує їх між користувачами мережі.

Для створення електронного підпису необхідно контрольна сума та додаткова інформація, яка шифрується за допомогою закритого ключа відправника. Щоб уникнути перехоплення та повторного використання, до підпису додається порядковий номер. Електронний підпис дозволяє підтвердити авторство документа та гарантує цілісність інформації та відсутність спроб її спотворення. Документ складається з тексту, електронного підпису та сертифіката користувача, що містить дані користувача, його ідентифікаційне ім'я та відкритий ключ дешифрування для перевірки підпису адресата документа [3].

Електронний підпис дозволяє захистити інформацію від таких злочинних дій:

– «відмова від авторства», коли автор документа відмовляється від авторства;

– «фальсифікація», коли одержувач документа його підробляє;

– «переробка», коли одержувач документа вносить зміни до нього;

– «маскування», коли користувач маскується під іншого користувача.

Для підтвердження повідомлення мають бути виконані наступні умови:

– відправник повинен поставити підпис у повідомленні, який містить додаткову інформацію, яка залежить від повідомлення та одержувача повідомлення, але відома лише відправнику;

– правильний підпис не можна зробити без додаткової інформації;

– підпис має залежати від часу, щоб старі повідомлення не могли бути використані; це відрізняє електронний підпис від рукописного;

– одержувач повинен мати можливість перевірити, що підпис належить відправнику та є правильним щодо повідомлення. Таким чином, електронний підпис – це вид пароля, який залежить від відправника, одержувача та змісту повідомлення [4].

Рис.3. Перевірка справжності ЕЦП

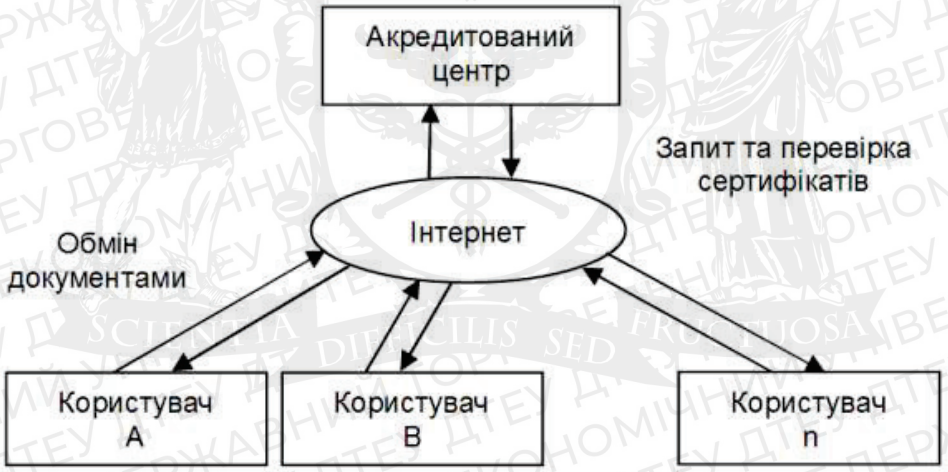


Рис.4. Схема взаємодії користувачів електронного цифрового підпису

Відповідно до Закону України «Про електронні документи та електронний документообіг» електронний підпис є обов'язковим реквізитом електронного документу, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу та накладенням електронного підпису завершує створення електронного документа. Закон України «Про електронний цифровий підпис» визначає правовий статус електронного цифрового підпису, згідно з яким електронний цифровий підпис - це вид електронного підпису, отриманий у результаті криптографічного перетворення набору електронних даних, що додається до цього набору або логічно поєднується з ним і дозволяє підтвердити його цілісність та ідентифікацію підписувача.

Електронний цифровий підпис накладається за допомогою закритого ключа та перевіряється за допомогою відкритого ключа. Порядок криптографічного захисту інформації з обмеженим доступом, розголошення якої спричиняє (може завдати) шкоди державі, суспільству, особі в Україні визначається Положенням про порядок криптографічного захисту

інформації в Україні. Згідно з цим Положенням для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або є власністю держави, використовуються допущені до експлуатації криптосистеми та засоби криптографічного захисту [6].

Використовуються лише засоби криптографічного захисту, які мають сертифікат відповідності [7].

Існує велика кількість програмних продуктів, призначених для криптографічного захисту інформації, як іноземних розробників, так і українських.

Однією з найкращих програм для шифрування інформації є BestCrypt від фінської компанія Jetico. Він дозволяє створити зашифрований контейнер для зберігання інформації на будь-якому типі носія і призначений для роботи як під Windows, так і під Linux. Програма може додатково використовувати один із найнадійніших алгоритмів, реалізованих із 256-бітним ключем: Rijndael (AES), Blowfish і Twofish. Новіші версії алгоритму Blowfish можуть використовувати 448-бітний ключ [8].

Також відома програма «Private Disk» від молдавської компанії «Dekart». Він дозволяє створити зашифрований віртуальний диск для зберігання інформації. Шифрування здійснюється за допомогою алгоритму AES 256. При роботі з інформацією файли на віртуальному диску мають ті ж властивості, що й незашифровані, доки користувач не заблокує доступ. Віртуальний диск захищений від вірусів, троянів і шпигунського програмного забезпечення за допомогою вбудованого Disk Firewall [9].

Є система криптографічного захисту інформації «Карма» від української компанії «NetCom Technology». Він призначений для забезпечення використання електронного цифрового підпису та шифрування, зокрема, в юридично значимому електронному документообігу. Особливістю цієї системи є можливість додавати до електронного цифрового підпису зображення власноручного підпису. В результаті електронний документ матиме вигляд паперового [10].

ТОВ «СКЗ «КриптоСофт» пропонує програмний комплекс криптографічного захисту інформації «Криптосервер» для роботи під MS Windows 8, MS Windows 10. Цей комплекс забезпечує захист даних, що передаються через незахищені публічні (Інтернет) або відкриті (наприклад, виділені лінії, MPLS) канали. Дані захищені шифруванням на основі вітчизняних алгоритмів шифрування. Максимальний рівень обмеження доступу до інформації, що захищається цим пакетом, — «конфіденційно» [11].

Висновки. Забезпечення криптографічного захисту інформаційних ресурсів є надзвичайно важливою задачею у сучасному цифровому світі. Криптографічний захист дозволяє захищати конфіденційні дані від несанкціонованого доступу та забезпечувати цілісність та автентичність інформації.

Для забезпечення криптографічного захисту використовуються різні методи, такі як симетричне та асиметричне шифрування, хеш-функції, електронні підписи та інші. Кожен з цих методів має свої переваги та недоліки, тому їх використання залежить від конкретної ситуації.

При забезпеченні криптографічного захисту необхідно враховувати різні атаки, такі як перехоплення, підроблення, внесення змін та інші. Тому важливо використовувати потужні алгоритми та ключі відповідної довжини для захисту інформації.

Забезпечення криптографічного захисту є складним процесом, який потребує високої кваліфікації фахівців та великої уваги до деталей. Однак, правильно реалізований криптографічний захист може забезпечити високий рівень безпеки інформаційних ресурсів.

Криптографія – це сукупність методів перетворення даних, спрямованих на приховування їх інформаційного змісту. Система криптографічного захисту інформації – це сукупність криптографічних алгоритмів, протоколів і процедур для формування, поширення, передачі та використання криптографічних ключів. Саме повідомлення називається відкритим текстом. Зміна зовнішнього вигляду повідомлення для приховування його суті називається шифруванням. Криптографічний захист може забезпечити умови конфіденційності та

цілісності передавання даних у відкритих мережах, а також анонімність об'єкта та умови його залучення до DIR.

Криптографічний захист є необхідним елементом сучасної інформаційної безпеки. Він дозволяє зберегти конфіденційність, цілісність та доступність інформації в різних сферах діяльності, таких як банківський сектор, медицина, військова та державна сфери, торгівля та інші.

Криптографічний захист реалізується за допомогою різних методів шифрування та електронних підписів. Ці методи забезпечують захист інформації від несанкціонованого доступу, змін та втрати. Крім того, законодавча база в різних країнах визначає правила використання криптографічних методів в різних сферах діяльності.

Забезпечення криптографічного захисту вимагає комплексного підходу та регулярного оновлення заходів захисту. Крім того, важливо використовувати надійні криптографічні методи та інструменти, які відповідають сучасним вимогам безпеки. Використання криптографічних методів захисту інформації є необхідністю для забезпечення безпеки від зловмисних атак та збереження конфіденційної інформації.

Список використаних джерел

1. Пономаренко, В. С., Журавльова, І. В., і Туманов, В. В. (2003). *Основи захисту інформації: навчальний посібник*. Харків: Вид. ХДЕУ.
2. Вербицький, О. В. (2018). *Вступ до криптології*. Львів: Вид-во НТЛ.
3. Хорошко, В. А., і Чекатков А. А. (2017). *Методи і засоби захисту інформації.* Київ: Юніор.
4. Фаль, О. М. (2003). *Криптографія: основні ідеї та застосування.* Київ: ІВЦ Видавництво «Політехніка».
5. *Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV.* URL: http://zakon4.rada.gov.ua/laws/show/851-15 (станом на 26.03.2023).
6. *Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV.* URL: http://zakon4.rada.gov.ua/laws/852-15 (станом на 26.03.2023).
7. *Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 № 505/98*. URL: http://zakon4.rada.gov.ua/laws/show/505/98 (станом на 26.03.2023).
8. Private Disk - найкраща програма для шифрування файлів. URL: http://www.private-disk.net (станом на 26.03.2023).
9. *Система «KARMA». Універсальна система криптографічного захисту інформації (н.д.).* URL: http://www.eos.com.ua/eos/ua/products/carma (станом на 26.03.2023).
10. Сіра, О., і Каткова, Т. (2017). Formation of securities portfolio under conditions of uncertainty. *Eastern-European Journal of Enterprise Technologies*, 1(4 (85)), 49–55. https://doi.org/10.15587/1729-4061.2017.9228 [in English].
11. Раскін, Л., Сіра, О., і Каткова, Т. (2019). Dynamic problem of formation of securities portfolio under uncertainty conditions. *EUREKA Physics and Engineering*,6, 73–82. https://doi.org/10.21303/2461-4262.2019.00985 [in English].

Робота виконана під науковим керівництвом к.т.н., доцента
ЗВЕРЄВА В.П.

ДОСЛІДЖЕННЯ ШЛЯХІВ ІДЕНТИФІКАЦІЇ ПОРУШНИКА В ІНФОРМАЦІЙНО КОМУНИКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

САСІН Є., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпеката захист інформації»

У статті розглянуто різні методи та технології ідентифікації порушника в IT-системах та мережах, зокрема, системи виявлення вторгнень (IDS,IPS), машинне навчання та штучний інтелект , аналізу журналів подій, відслідковування поведінки користувача тощо. Також будуть розглянуті технології захисту від DDoS-атак та інших шкідливих впливів на мережу.

The article discusses various methods and technologies for identifying intruders in IT systems and networks, including intrusion detection systems (IDS, IPS), machine learning and artificial intelligence, event log analysis, user behavior tracking, and more. The technologies for protecting against DDoS attacks and other harmful influences on the network will also be considered.

Актуальність : В сучасному світі, інформаційні технології стали невід'ємною частиною життя людей та бізнес-процесів. За останні роки кількість кібератак та інших інформаційних загроз значно збільшилась, що свідчить про необхідність підвищення рівня захисту інформації та ідентифікації порушників.

З метою захисту інформації та забезпечення безпеки користувачів, компанії та установи вкладають значні зусилля в розробку та вдосконалення методів ідентифікації порушників в інформаційно-комунікаційних системах та мережах. Це включає в себе розробку нових технологій, таких як машинне навчання, біометричні технології та аналіз мережевого трафіку, а також поєднання цих технологій для розробки комплексних систем ідентифікації порушників. Оскільки розвиток інформаційних технологій не зупиняється, а навпаки, прискорюється, проблема ідентифікації порушників в інформаційно-комунікаційних системах та мережах є надзвичайно актуальною і потребує постійного вдосконалення та дослідження.

Злочинці використовують різні методи, щоб отримати нелегальний доступ до конфіденційної інформації, налагоджують ботнети, проводять фішингові атаки, вимагають викуп зашифрованої інформації, та інше. Такі напади можуть призвести до серйозних наслідків, таких як втрата конфіденційної інформації, викрадення грошей, порушення роботи систем та мереж, та інше. Тому, ідентифікація порушника є надзвичайно важливою задачею, яка дозволяє вчасно виявляти та реагувати на потенційні загрози. При цьому, потрібно зазначити, що швидкість та ефективність ідентифікації порушника залежить від рівня захисту системи та мережі, та застосованих методів і технологій.

Крім того, стаття зосередить увагу на питаннях приватності та захисту персональних даних під час процесу ідентифікації порушника. Будуть розглянуті способи забезпечення конфіденційності та захисту даних користувачів.

Мета статті :Проаналізувати способи ідентифікації порушення безпеки в інформаційно комунікаційних системах та мережах.

Об'єктом дослідження є безпека інформаційно-комунікаційних систем та мереж.

Предмет дослідження – засоби ідентифікації порушника та забеспечення безпеки в IT-системах.

Аналіз попередніх досліджень - попередні дослідження на тему ідентифікації порушника в інформаційно-комунікаційних системах та мережах відображають актуальність даної проблеми та її складність. Нижче представлено огляд деяких з них.

Стаття " Технології захисту в інформаційно-комунікаційних системах " авторства А. В. Жилін, О. М. Шаповал, О. А. Успенський була опублікована в 2020 році [1]. У статті автори досліджують проблему оцінки ризиків виникнення кібератак на мережеві пристрої. Вони наводять приклади різних типів кібератак та їх можливі наслідки, а також описують загрози,

які створюються різними типами мережевих пристроїв. Автори також пропонують методику оцінки ризиків, яка базується на підходах до аналізу вразливостей та вимог до захисту інформації. Автори проводять експерименти з оцінки ризиків виникнення кібератак на мережеві пристрої за допомогою розробленої методики. Вони порівнюють отримані результати з іншими методами оцінки ризиків та наводять приклади можливих заходів для зменшення ризиків виникнення кібератак, а також вказують на необхідність подальшого дослідження даної проблеми з урахуванням змін у технологічному середовищі.

Стаття «Аналіз ризиків безпеки інформаційної системи іт-підприємства» за авторства Карпович І.М, Гладка О.М, Наконечна Ю.А. була опублікована в 2020 році [2]. В статті досліджується проблема оцінки інформаційної безпеки корпоративних інформаційних систем (КІС). Автори розглядають підходи до визначення інформаційної безпеки та її складових елементів, а також наводять різні класифікації загроз інформаційній безпеці, а також описуються основні методи та моделі оцінки інформаційної безпеки, зокрема методології оцінки ризику, метод аналізу вразливостей, метод визначення потреби у захисті інформації тощо. В статті наводяться переваги та недоліки кожного з методів, а також порівнюються їх застосування в різних сферах.

Загалом, попередні дослідження підтверджують необхідність розробки та впровадження ефективних методів та технологій ідентифікації порушників в інформаційно-комунікаційних мережах.

Виклад основного матеріалу. Основною метою розвитку способів ідентифікації порушників в інформаційно-комунікаційних системах та мережах є забезпечення високого рівня безпеки інформації, що зберігається та передається по цих системах. Ідентифікація порушників дозволяє реалізувати наступні цілі.

1. Запобігання кібератакам: Ідентифікація порушників дозволяє швидко виявляти зловмисників, які намагаються завдати шкоди інформації, і приймати ефективні заходи для запобігання кібератакам.
2. Підвищення рівня захисту інформації: Ідентифікація порушників дозволяє забезпечити підвищений рівень захисту інформації від несанкціонованого доступу, втрати та знищення.
3. Покращення ефективності виявлення інцидентів: Ідентифікація порушників дозволяє швидко виявляти та локалізувати інциденти, що відбуваються в мережі, і вчасно приймати заходи для їх вирішення.
4. Забезпечення відповідності нормативним вимогам: В деяких секторах, наприклад, у фінансовій та медичній галузях, ідентифікація порушників є вимогою нормативно-правових актів та стандартів.
5. Зниження ризику фінансових втрат: Ідентифікація порушників дозволяє зменшити ризик фінансових втрат, які можуть виникнути в результаті кібератак.

Порушники в ІТ системах можуть мати різні цілі, в залежності від їх мотивації та потреб. Основні цілі порушників в ІТ системах можуть включати:

Отримання конфіденційної інформації: Порушники можуть бути зацікавлені в отриманні конфіденційної інформації, такої як банківські реквізити, паролі, персональні дані та інші конфіденційні дані. Вони можуть використовувати отриману інформацію для злочинних цілей, таких як крадіжка грошей, шахрайство, викрадення ідентичності та інші.

Викрадення грошей: Порушники можуть намагатися викрасти гроші з банківських рахунків, використовуючи крадіжку банківських реквізитів, фішинг та інші методи.

Навмисне завдання шкоди: Порушники можуть намагатися завдати шкоди системам та мережам, використовуючи віруси, шкідливі програми, вразливості та інші методи. Це може призвести до втрати даних, перерв у роботі систем та інших негативних наслідків.

Викрадення ідентичності: Порушники можуть намагатися викрасти ідентичність користувача, отримавши доступ до їх облікового запису та використовуючи його для злочинних цілей, таких як шахрайство, крадіжка грошей та інші.

Експлуатація комп'ютерних ресурсів: Порушники можуть намагатися використовувати комп'ютерні ресурси, такі як обчислювальна потужність та мережева пропускна здатність, для виконання своїх завдань, таких як криптовалютний майнінг.

Новітні способи та тактики протидії порушникам ІТ безпеки постійно еволюціонують, тому їх може бути багато. Ось декілька прикладів:

Машинне навчання та штучний інтелект: Використання машинного навчання та штучного інтелекту для виявлення аномальної поведінки та ідентифікації загроз може допомогти в ранньому виявленні порушників. Метод машинного навчання відіграє важливу роль у виявленні порушників в інформаційно-комунікаційних системах та мережах. Застосування методів машинного навчання може допомогти в ідентифікації зловмисних дій та зниженні ризику кібератак.

Основна ідея полягає в тому, що система машинного навчання отримує доступ до великої кількості даних про поведінку користувачів та інформаційних процесів, і на їх основі будує модель нормальної поведінки. Після цього система може виявляти незвичайні або ненормальні дії, які можуть бути індикатором зловмисних атак.

Основні методи машинного навчання, що використовуються для виявлення порушників в інформаційно-комунікаційних системах та мережах, включають:

- Навчання з учителем (supervised learning) - при цьому використовується набір даних, які містять інформацію про нормальну та аномальну поведінку. Система використовує ці дані для створення моделі, яка може виявляти ненормальну поведінку, що може бути пов'язано зі зловмисними атаками.
- Навчання без учителя (unsupervised learning) - при цьому система працює з даними, які не мають позначок про нормальну та аномальну поведінку. Система сама намагається знайти патерни та залежності в даних, що можуть бути пов'язані зі зловмисною діяльністю.
- Півнавчання (semi-supervised learning) - при цьому використовуються як дані з позначками, так і без них. Така модель дозволяє покращити якість виявлення аномальної поведінки в порівнянні з навчанням без учителя.

Багатофакторна аутентифікація: Використання більш надійної багатофакторної аутентифікації (наприклад, використання паролю та додаткового підтвердження, такого як відбиток пальця або обличчя) може зменшити ризик несанкціонованого доступу до системи.

Системи виявлення вторгнень: Використання систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS) може допомогти виявити та блокувати загрози в реальному часі. Два загальних метода виявлення, що використовуються однаково інструментами IDS та IPS, – це виявлення на основі підписів та виявлення на основі аномалії. IDS та IPS, які використовуються для визначення підписів які відповідають профілю відомих атак. Атаки виявляються за допомогою вивчення шаблонів даних, заголовків пакетів, адрес джерела та пунктів призначення. Виявлення на основі підписів є чудовим для виявлення встановлених атак. Однак виявлення на основі підписів неефективне при виявленні атак з нульовим днем, які не відповідають іншим встановленим підписам атаки.

Тестування вразливостей: Регулярне тестування вразливостей може допомогти виявити потенційні проблеми з безпекою та забезпечити швидке виправлення недоліків.

Моніторинг системи: Системний моніторинг може допомогти виявити незвичайну активність або аномальну поведінку в ІТ системі. Це може бути здійснено за допомогою спеціальних програмних засобів, які записують дії користувачів, системні події та інші параметри.

Журналізація даних: Ведення детальних журналів дій користувачів та системних подій може допомогти виявити аномальність в поведінці та діях.

Аналіз трафіку: Аналіз трафіку мережі може допомогти виявити незвичайну активність, яка може вказувати на присутність порушника в мережі.

Аудит безпеки: Аудит безпеки може допомогти виявити потенційні проблеми з безпекою в системі та допомогти зрозуміти, які заходи є необхідними для забезпечення захисту.

Кібербезпекові вправи: Проведення кібербезпекових вправ та тренувань для перевірки та підвищення рівня готовності до кібератак може допомогти компаніям та установам виявляти та захищатися від потенційних загроз.

Існує багато прикладів кібербезпекових вправ, які можуть бути проведені для перевірки та підвищення рівня готовності до кібератак. Деякі з них:

1. Соціальний інжиніринг - проведення вправ з тестування соціального інжинірингу для виявлення слабких місць у свідомості співробітників щодо кібербезпеки. Це може включати тестування співробітників на їхню готовність відповідати на підозрілі електронні повідомлення або надавати чутливу інформацію.
2. Вправи "чорного ящика" - тестування систем безпеки на можливість проникнення зловмисників. Це може включати спроби використання вразливостей в програмному забезпеченні або мережевих пристроях, щоб отримати несанкціонований доступ до системи.
3. Вправи на виявлення інцидентів - тестування реагування на кіберінциденти з метою виявлення, як швидко можна виявити та відреагувати на такі інциденти. Це може включати тестування процедур попередження, реагування та відновлення після кібератаки.
4. Вправи з кібербезпеки мереж - проведення вправ з тестування захисту мереж від кібератак. Це може включати тестування на відновлення після DoS атаки, відновлення від розриву мережі або на відстеження трафіку, що виходить з мережі.
5. Вправи на тренування співробітників - проведення вправ на тренування співробітників з кібербезпеки.

Створення культури кібербезпеки є важливим елементом забезпечення безпеки в організації. Основною метою створення культури кібербезпеки є забезпечення того, щоб кожен працівник розумів, що кібербезпека є його особистою відповідальністю та розумів, як він може допомогти у забезпеченні безпеки всієї організації. Ці заходи можуть бути використані окремо або в комбінації.

Способи виявлення та протидії кіберзагрозам на прикладі DDoS атаки. DDoS атаки (атаки з використанням великої кількості запитів) є одними з найпоширеніших видів кібератак на сьогоднішній день. Існує безліч методів захисту від DDoS атак, ось декілька з них:

- Використання CDN (Content Delivery Network): CDN дозволяє розподіляти навантаження між різними серверами, що дозволяє зменшити вплив DDoS атак на окремий сервер.
- Використання фільтрації трафіку: Фільтрація трафіку дозволяє виділяти запити, які можуть бути пов'язані з DDoS атакою та блокувати їх.
- Використання облачних технологій: Використання хмарних технологій може допомогти забезпечити захист від DDoS атак, оскільки вони можуть забезпечити широкі канали зв'язку та високу міру масштабованості.
- Використання захисних мереж: Використання захисних мереж може допомогти забезпечити захист від DDoS атак, оскільки вони можуть блокувати небезпечний трафік та забезпечити захист від небезпечних запитів.
- Використання програмного забезпечення для захисту від DDoS атак: Існує безліч програмного забезпечення, яке може забезпечити захист від DDoS атак. Це може бути програмне забезпечення, яке забезпечує фільтрацію трафіку, блокування атак, розподіл навантаження та інше.
- Підвищення міцності інфраструктури: Підвищення міцності інфраструктури, наприклад, збільшення пропускної здатності мережі та серверів, може допомогти зменшити вплив DDoS атак.

Прикади систем ідентифікації кіберзагроз. На сьогоднішній день на ринку існує багато різних систем детекції інтранет-атак. Ось декілька прикладів:

1. Snort - це безкоштовна система детекції вторгнень (IDS) та інтранет-атак, яка працює в режимі реального часу і використовує базу даних правил для виявлення потенційно небезпечної активності в мережі.
2. Suricata - це інша відкрита система IDS та інтранет-атак, яка працює в режимі реального часу та використовує машинне навчання та інші технології для виявлення потенційно небезпечної активності в мережі.
3. Darktrace - це комерційна система детекції інтранет-атак, яка використовує технології штучного інтелекту та машинного навчання для автоматичного виявлення та реагування на кібератаки всередині корпоративної мережі.
4. Cisco Stealthwatch - це інша комерційна система детекції інтранет-атак, яка використовує машинне навчання та інші технології для виявлення потенційно небезпечної активності в мережі та забезпечення захисту мережі в реальному часі.
5. McAfee Network Security Platform - це ще одна комерційна система IDS та інтранет-атак, яка використовує різноманітні методи аналізу трафіку та машинного навчання для виявлення та блокування потенційно небезпечної активності в мережі.
6. Zeek (раніше відома як Bro) - це безкоштовна система мережевого моніторингу та виявлення вторгнень, яка використовує відкритий код та різноманітні методи аналізу трафіку для виявлення потенційно небезпечної активності в мережі.

Ці системи детекції інтранет-атак можуть бути встановлені та налаштовані на різних рівнях складності, залежно від потреб та бюджету компанії. Вони допомагають виявляти та реагувати на кібератаки всередині мережі.

Висновки. У статті було проведено дослідження шляхів ідентифікації порушника в інформаційно-комунікаційних системах та мережах. Було проаналізовано різноманітні методи та алгоритми ідентифікації. В результаті дослідження було встановлено, що ефективність методів ідентифікації порушника значно залежить від характеру нападу та використаної вразливості. Було визначено, що найбільш ефективним є комплексний підхід, який включає в себе використання різних методів ідентифікації.

Отже, на основі проведеного дослідження можна зробити висновок про необхідність постійного підвищення рівня безпеки інформаційно-комунікаційних систем та мереж. Для цього потрібно використовувати комплексний підхід до ідентифікації порушника та постійно вдосконалювати методи та алгоритми ідентифікації, щоб бути готовими до різноманітних типів нападу.

Список використаних джерел

1. Жилін А. В., Шаповал О.М. , Успенський О.А. Технології захисту в інформаційно-комунікаційних системах. Режим доступу: https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf
2. Гладка І.М, Наконечна О.М. Аналіз ризиків безпеки інформаційної системи іт-підприємства Режим доступу: https://doi.org/10.32838/2663-5941/2020.5/12
3. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids.
4. Критерії захищеності інформації в комп'ютерних системах від несанаційного доступу. НД ТЗИ 2.5004-99. Режим доступу: https://tzi.com.ua/downloads/2.5-004-99.pdf

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

СОЦІАЛЬНИЙ ІНЖИНІРИНГ: СУТНІСТЬ І МЕТОДИ ПРОТИДІЇ

СЛИВЕНКО О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розкрито сутність і методи протидії соціальному інжинірингу. Визначено генезис походження соціального інжинірингу. Сформовано взаємозв'язок між розповсюдженням вірусу COVID-19, війни Росії проти України і постійної необхідності адаптації людей до зовнішніх факторів з соціальним інжинірингом. Відокремлено низку заходів з детальним описом концепції. Зазначається, що комплексне використання методів протидії допоможе знизити рівень успішних атак за всіма методами.

The article reveals the essence and methods of combating social engineering. The genesis of the origin of social engineering is determined. The relationship between the spread of the COVID-19 virus, Russia's war against Ukraine and the constant need to adapt people to external factors with social engineering has been established. A number of measures are separated with a detailed description of the concept. It is noted that the integrated use of countermeasures will help reduce the level of successful attacks by all methods.

Актуальність. Глобальне поширення вірусу COVID-19, війна Росії проти України і постійна необхідність адаптації людей до зовнішніх факторів призвели до прискореного впровадження технологій та цифровізації, тому більшість інформації зараз зберігається у цифровому форматі. Даний факт підкреслив важливість навчання людей розпізнавати потенційні кіберзагрози та важливість навчання правильному використанню технологій з урахуванням основних критеріїв інформації: цілісність, конфіденційність та доступність. Відсутність такого навчання викликає недовіру до ролі людського фактору в інформаційній безпеці. Більше того, часто забувають про зв'язок людського фактору із інформаційною безпекою, що пов'язано з наголосом на технічних і процедурних заходах, необхідних для вирішення загальних проблем безпеки. У результаті більшість кіберзагроз виявляються за допомогою систем виявлення вторгнень, брандмауерів або антивірусного програмного забезпечення, тому соціальна інженерія є основною загрозою, оскільки з нею неможливо боротися цими звичайними засобами.

Звернення до безпеки з соціальної, технічної та когнітивної точок зору потрібне для ефективної обробки людських факторів, залучених до інформаційної безпеки. Поєднуючи людські характеристики з технологічними характеристиками, можна створити організаційну культуру, щоб мінімізувати ризики, пов'язані з атаками соціальної інженерії. Незалежно від рівня впливу, культура інформаційної безпеки є ключовим фактором уникнення потенційних небезпек, яким може бути піддана інформація. Завдяки реалізації навчання користувачі отримують необхідні знання, які сприяють гарному розумінню стратегій атак соціальної інженерії та розвитку здатності протидіяти й обмежувати потенційні наміри завдати шкоди [1]. Як наслідок, щоб досягти етапу, коли підтримка інформаційної безпеки стає діяльністю, яка виконується несвідомо та на постійній основі, необхідно впровадити організаційну культуру, встановлену через згоду та підтримку користувачів.

Мета статті. Розкрити сутність і методи протидії соціальному інжинірингу.

Об'єктом дослідження є процес протидії соціальному інжинірингу.

Предмет дослідження – соціальний інжиніринг.

Аналіз попередніх досліджень. Формулювання наукової думки в окресі соціального інжирингу є різнорідною та масштабною. У сучасній науковій площині з'являються роботи присвячені механізмам та принципам протидії соціальному інжинірингу на об'єктах господарювання.

О. Юдін, О. Матвійчук-Юдіна та О. Супрун [2] провели аналіз існуючих сучасних методів соціальної інженерії та визначено технології використання різних класів методів в інформаційно-психологічній війні, а також застосування деструктивних засобів інформаційної безпеки, як складової психологічного впливу на особистість і суспільство.

У [3] схарактеризовано основні підходи до тлумачення понять «прикладні комунікаційні технології», «соціальний інжиніринг». Авторка вдається до порівняльного вивчення методологічних систем аналізу соціальних комунікацій і комунікаційних технологій у світовій та вітчизняній науці.

Н. Баландіна, М. Василенко, В. Слатвінська та С. Сисоєнко [4] довели потребу в новому методологічному підході до побудови моделі поведінки людини в цифровій сфері, спрямованої на захист інформації в соціальному інжинірингу. Запропоновали синергійно-криптографічний підхід до побудови моделі поведінкових проявів в умовах соціального інжинірингу та в інтересах захисту інформації.

Подібні дослідження також проведено іноземними авторами, зокрема Х. Мумтаз, С. Самріна, І. Номан [5], Ф. Гассан [6], А. Очоа, А. Акеро [7], С. Врговец, І. Бернік, Б. Маркель [8], Г. Асанте [9], Ф. Рубія, Ю. Аффан, Л. Лін, В. Цзяньмін [10], Ф. Лову, Х. Нандере [11], К. Янгкен [12], К. Четіуі, Б. Бах, А. Аламі, А. Банассе [13], К. Штайнметц, Т. Холт [14]. та інші.

Однак, незважаючи на масштабність наукових досліджень за окресленою тематикою, питання розкриття сутності і методів протидії соціальному інжинірингу залишається відкритим та потребує детального опрацювання.

Виклад основного матеріалу. Примус, психологічна маніпуляція та методи індоктринації – це лише невелика частина способів, за допомогою яких уявлення, думки та переконання однієї людини порушуються або навіть замінюються уявленнями, думками та переконаннями іншої людини. Соціальний інжиніринг також відноситься до цієї категорії. Визначення терміну «соціальний інжиніринг» представляє певну складність, оскільки визначення, пов’язані з соціальним інжинірингом, відрізняються залежно від середовища, яке використовується для їх отримання. Найперша згадка про соціальний інжиніринг датується 1894 роком, у період індустріалізму, коли у своїх працях голландський радикал Дж. С. Ван Маркен наголосив на необхідності розвитку технічної експертизи в «управлінні людськими проблемами». Як визначено в онлайн-словнику Dictionary.com, соціальний інжиніринг пояснюється як «використання централізованого планування в спробі керувати соціальними змінами та регулювати майбутній розвиток і поведінку суспільства» [15]. Це визначення обмежує мету соціального інжинірингу використанням людського фактору шляхом використання комунікації та засобів, за допомогою яких він досягається. У контексті застосовності до інформаційної безпеки соціальний інжиніринг відноситься до дії обману особи з метою розкриття конфіденційної інформації, отримання несанкціонованого доступу або вчинення шахрайства шляхом спілкування з цією особою з метою завоювання її довіри [5]. Сукупність таких заходів з метою збору інформації, підробки або несанкціонованого доступу, від традиційного «шахрайства» відрізняється тим, що часто є одним із багатьох кроків у складнішій схемі доступу до інформації.

Існування кількох визначень, пов'язаних із соціальним інжинірингом, підкреслює його широку застосовність у багатьох сферах. Використовується в політичному, освітньому, релігійному чи корпоративному середовищі, соціальний інжиніринг використовується для перепланування поведінки мас. Юристи та психологи вдаються до тактики, яку використовує соціальний інжиніринг, щоб зібрати інформацію, яка інакше не була б розголошена. Уряд використовує соціальний інжиніринг через свою владу над людьми, які перебувають під його владою, при цьому людський мозок налаштований дотримуватись вказівок влади.

Продавці – це соціальні інженери, які використовують свою здатність переконувати людей звертатися до їхніх потреб і задовольняти їх за допомогою товарів або послуг, які вони комерціалізують. Приклади, звичайно, можна продовжувати, але наведених достатньо, щоб підкреслити той факт, що соціальний інжиніринг використовується щодня людьми та установами в різних соціальних рівнях.

Незалежно від типології, до якої підпадають ініціатори соціального інжинірингу, ефективність соціального інжинірингу пояснюється використанням людських помилок, таких як: прийняття рішень під впливом емоцій, бажання допомогти, необережність у знайомих ситуаціях та ігнорування інформації, яка сприймається не вірно.

Для того, щоб застосувати соціальний інжиніринг на практиці, обов'язковим є вивчення окремих осіб та їхньої поведінки, щоб сприяти досягненню очікуваного результату, незалежно від причини, з якої використовується соціальний інжиніринг.

Теоретично атаки соціального інжинірингу можуть бути зосереджені на технологіях або на окремих особах [6]. Технологічний підхід до соціального інжинірингу полягає в підробці прикладної системи, щоб змусити користувача надати конфіденційну інформацію за допомогою спливаючих вікон, спаму, шкідливих програм, шпигунського програмного забезпечення або фішингових атак. Користувач може отримати спливаюче вікно, яке вказує на те, що комп'ютерна програма, яка зараз використовується, зіткнулася з певними проблемами, які обмежують її функціональність, доки комп'ютерна програма не зможе повторно увійти, ввівши ідентифікатор і пароль. Ввівши ці дані, хакер, який створив спливаюче вікно, зможе отримати доступ до мережі та комп'ютерної системи за допомогою облікових даних користувача. Спам-повідомлення містять вкладення, у яких троянський вірус або інша шкідлива програма впливає на системи та мережі [7]. У загальному комплексі наслідки дії таких атак варіюються від уповільнення роботи системи до знищення даних і втручання в усю комунікаційну мережу.

Поширюючи законну програму, яка містить зловмисне або шпигунське програмне забезпечення, жертву можна змусити її завантажити, вважаючи, що програма є утилітою, яка покращує продуктивність комп'ютера.

Фішингові атаки – це найпоширеніші атаки, які здійснює соціальний інжиніринг [8], під час яких до жертв звертаються за допомогою електронних листів або телефонних дзвінків. Ці атаки можна класифікувати за п'ятьма категоріями: цільовий фішинг, китобійний фішинг, вішинговий фішинг, інтерактивний фішинг із голосовою відповіддю, фішинг через невідомі корпоративні електронні листи [9]. Для отримання даних зловмисники створюють відчуття терміновості або застосовують тактику залякування. Варто зазначити, що фішингові кампанії можуть бути орієнтовані на велику кількість випадкових користувачів або конкретну особу чи групу.

Усі ці форми фішингу включають фальшиві веб-сайти, веб-сайти PayPal, програмне забезпечення для страхування, рекламу, антивірус, безкоштовні пропозиції чи призи, за допомогою яких зловмисник може дізнатися ім'я жертви, фізичну адресу, дані кредитної картки тощо.

Атаки, спрямовані на слабкі сторони поведінки людини або такі, що передбачають отримання конфіденційної інформації без використання технологічних вразливостей, ілюструють другу категорію атак соціального інжинірингу.

Видача себе за іншу особу або викрадення персональних даних особи передбачає встановлення легітимності з жертвою шляхом зв'язування та об'єднання даних, відомих про жертву. Для цього необхідно, щоб соціальний інженер, який ініціює цей тип атаки, заздалегідь мав достовірну історію, яка не викликає підозр у жертви.

Занурення спрямоване на отримання інформаційних товарів або документів. Наприклад, якщо зловмисник отримує список з іменами співробітників або список телефонних номерів, він стає бенефіціаром багатьох можливостей соціального інжинірингу: імена та номери телефонів співробітників можуть бути використані для крадіжки особистих даних або для ініціювання фішингової атаки.

Обман, на відміну від шахрайства з метою отримання фінансової чи матеріальної вигоди, часто використовується, щоб збентежити жертву або прийняти швидкі рішення.

Шпигунство та підслуховування зображують типи атак соціального інжинірингу, які здійснюються зловмисником, коли він знаходиться поблизу жертви. Ці атаки можуть

призвести до отримання пароля користувача, коли він записаний на документах, доступних іншим.

Отже, незважаючи на численні форми, атака соціального інжинірингу передбачає використання соціальних навичок для отримання достатньої кількості даних для компрометації або зміни інформаційних систем організації [10].

У будь-якій успішній атаці, здійсненій у рамках соціального інжинірингу, дотримується низка етапів: збір інформації, вилучення, претекст, переконання, націлювання та розпізнавання.

Збір інформації – найретельніший етап соціального інжинірингу, який здійснюється шляхом спостереження за жертвою. Тривалість цієї стадії може варіюватися від кількох годин до кількох років, оскільки інформація не збирається відразу, а потім співвідноситься одна з одною для створення профілю жертви.

Виявлення можна визначити як здатність отримувати інформацію за допомогою логіки, тому її може бути важко виявити. По суті, проведення цієї стадії досягається проведенням дізнання. Перетекст ілюструє стадію атаки, коли соціальний інженер може прийняти фальшиву особу, яка може вплинути на прийняття жертвою певних рішень. Роль соціального інженера полягає в тому, щоб визначити спосіб мислення жертви, щоб ефективно використовувати її навички. Це здійснюється за допомогою розумових хитрощів, і, залежно від умонастрою співрозмовника, соціальний інженер вдасться до емоційної маніпуляції, зверне особливу увагу на слова, які можуть бути використані в розмові.

Коли звернення до інтересів жертви є успішним, соціальний інженер використовує переконання, щоб заставити жертву діяти від його імені, встановлюючи визначені цілі, завойовуючи довіру жертви, через взаємність або гнучкість.

Етап націлювання показує, що, на відміну від інших атак на людей, атаки соціальної інженерії сформульовані для конкретної людини.

Останній етап, розпізнавання, є формою збору інформації, за допомогою якої соціальний інженер отримує достатньо даних для планування та здійснення атаки на намічену ціль.

Стосовно України, як приклад реалізації соціального інжинірингу варто наголосити на пандемії 2019 року та війні 2022 року.

Пандемія, яка послідувала за глобальним поширенням вірусу COVID-19, а згодом і форм SARS-CoV-2, підвищила обізнаність про те, що фейкові новини можуть загрожувати загальному здоров'ю членів суспільства. Пандемія, яка розвивалася двома хвилями, перша з середини березня 2020 року, а друга – з січня 2021 року, породила нове поширене політичне, соціальне та економічне явище: інфодемію. Це явище було запроваджено Всесвітньою організацією охорони здоров'я, яка використала термін «інфодемія», щоб описати поширення дезінформації та неправдивої чи доброзичливої інформації серед великих спільнот людей одним словом. Соціальні інженери скористалися контекстом пандемії, щоб отримати допомогу від Центрів контролю та профілактики захворювань, продавати підроблені продукти (наприклад, набори тестів), звинувачувати расові групи, уряди та іммігрантів у поширенні вірусу та поширювати хаос і соціальні розбіжності, які призвели до рухів проти масок, проти вакцинації та навіть проти 5G.

Останнім і далекосяжним політично вмотивованим нападом соціальної інженерії є російсько-українська війна, яка почалася ще в лютому 2022 року. Вторгнення президента Росії Володимира Путіна в Україну також призвело до найнижчого рівня відносин між Москвою та Заходом з часів холодної війни. Російські військові та розвідувальні органи націлили на Україну через дезінформацію, намагаючись зобразити Україну та українських урядовців агресором у цьому конфлікті. Твердження російського президента мають на меті підживити ілюзію, що Україна розпалює насильство, тому російські військові дії на українській території є необхідними, для уникнення глобального конфлікту. За словами Джо Ондрака, керівника відділу розслідувань лондонської фірми Logically, яка займається відстеженням

дезінформації, російська риторика підтримується безліччю цифрових активістів, які потроюють фейкові новини про Україну.

Протидія методам соціального інжинірингу – це комплекс організаційно-режимних заходів, що включає:

– проведення перевірочних заходів при прийомі працівників на роботу, що включають всебічне вивчення особистісних якостей кандидата, його оточення, сфери інтересів та інформації про минулу трудову діяльність;

– контроль вхідної кореспонденції, що надходить в електронному вигляді до поштових скриньок співробітників, незалежно від рівня повноважень та привілейованості;

– перевірки наявності службової інформації конфіденційного характеру у відкритих інформаційних мережах;

– регулярне проведення занять із співробітниками організації щодо правил роботи з інформацією конфіденційного характеру та навчання навичкам протидії методам соціальної інженерії;

– контроль за дотриманням технології обробки інформації на технічних засобах організації;

– запис та подальший аналіз телефонних переговорів співробітників з використанням службових засобів зв'язку;

– проведення виховної роботи з метою підвищення мотивації працівників, прищеплення відданості дорученій справі;

– проведення періодичних перевірок професійної придатності співробітників організації щодо забезпечення інформаційної безпеки.

До основних методів протидії соціальному інжинірингу варто віднести:

1. Формування правильних переконань (передумов)
2. Використання дедукції (не індукції)
3. Перевірка достовірності
4. Знання логічних помилок

Формування правильних базових переконань (передумов) необхідне для формування адекватної картини світу тобто стійке переконання що Земля кругла, організація про мене подбає, моя безпека – моя відповідальність, тощо.

Дедукція (не індукція), тобто електронна пошта безпечна, зі мною такого не станеться, тощо.

Перевірка достовірності, тобто незалежне/достовірне джерело, експеримент.

Логічні помилки: «після» не означає «внаслідок», думка авторитету чи думка більшості, хибна аналогія, аргументація до традиції («у нас так заведено»).

Висновки. У роботі розкрито сутність і методи протидії соціальному інжинірингу. Враховуючи сучасний рівень геополітичної напруженості та посилення кібер-злочинів у всіх галузях господарювання, застосування соціального інжинірингу оперативно підлаштовується під поточну ситуацію і набуває ефективності особливо щодо тих користувачів, які непоінформовані про ризики та загрози цифрового середовища. Сучасний соціальний інжиніринг дає можливість коригувати соціальну реальність, використовуючи методи прогнозування, планування та програмування. Досліджено різні методи соціальної інженерії, розглянуто приклади, проведено розбір методів захисту та виведено пропозиції, комплексне використання яких допоможе знизити рівень успішних атак за всіма методами.

Перспективами подальшого дослідження є формулювання технологій протидії соціальному інжинірингу на об'єктах господарювання.

Список використаних джерел

1. Мочурад Л. І., Бойко Н. І., Яцків М. В. Моделювання стресової ситуації людини в автоматизованих системах управління технологічними процесами, Науковий вісник НЛТУ України, 2020. т. 30. № 1. С. 152-157. http://doi:10.36930/40300126
2. Інформаційно-психологічна війна та технологіх соціального інжинірингу [Електронний ресурс] / О. К. Юдін, О. В. Матвійчук-Юдіна, О. М. Супрун // Наукоємні технології. 2021. № 2. С. 130-139. – Режим доступу: http://nbuv.gov.ua/UJRN/Nt_2021_2_5
3. Бондаренко І. Прикладні комунікаційні технології у фокусі методології соціального інжинірингу. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Соціальні комунікації. 2020. Том 31 (70). № 3. Частина 3. С. 199-205.
4. Баландіна Н. М., Василенко М. Д., Слатвінська В. М., Сисоєнко С. В. Підхід до моделювання поведінкових проявів у соціальному інжинірингу в інтересах захисту інформації. Вісник Черкаського державного технологічного університету. Серія технічні науки. Вип. 4. 2020. С. 57-66. http://doi:10.24025/2306 4412.4.2020.222064 URL: http://vtn.chdtu.edu.ua/article/view/222064/225697
5. Mumtaz H., Samrina S., Noman I. (2023). Social Engineering and Data Privacy. http://doi:10.4018/978-1-6684-6581-3.ch010.
6. Hassan F. (2023). SOCIAL ENGINEERING ATTACKS TECHNIQUES. International Journal of Management Science and Engineering Management. № 03. P. 18-20.
7. Ochoa A., Acero A. (2022). The Journey of Engineering into Social Justice and Peacebuilding: A Review of the XV Conference of the International Network of Engineering, Social Justice and Peace. International Journal of Engineering Social Justice and Peace. № 9. P. 5-14. http://doi:10.24908/ijesjp.v9i1.15573.
8. Vrhovec S., Bernik I., Markelj B. (2022). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. Computers & Security. P. 125. http://doi:10.1016/j.cose.2022.103038.
9. Asante G. (2022). Social Engineering Attacks: A Clearer Perspective. International Journal of Computer Applications. № 184. P. 53-62. http://doi:10.5120/ijca2022922057.
10. Rubia F., Affan Y., Lin L., Jianmin W. (2022). Strategies for counteracting social engineering attacks. Computer Fraud & Security. 2022. http://doi:10.12968/S1361-3723(22)70583-0.
11. Lowu F., Nandere H. (2022). Simulation Model of Social Engineering Attacks in Business Enterprises. № 11. P. 2021. http://doi:10.7176/JIEA/11-2-10.
12. Youngkeun C. (2022). Workplace Violence and Social Engineering Among Korean Employees. http://doi:10.4018/978-1-6684-7464-8.ch018.
13. Chetioui K., Bah B., Alami A., Bahnasse A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science. P. 656-661. http://doi:10.1016/j.procs.2021.12.302.
14. Steinmetz K., Holt T. (2022). Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations. Social Science Computer Review. https://journals.sagepub.com/doi/full/10.1177/08944393221117501.
15. Онлайн-словник. – Режим доступу. – https://www.wiki-data.uk-ua.nina.az/Dictionary.com.html (останнє звернення 24.03.2023р.).

Робота виконана під науковим керівництвом док. екон. наук, проф. ТОКАРА В.В.

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ WEB-САЙТІВ ТА МЕТОДІВ ЇХ УСУНЕННЯ

СТЕПЕНКО І., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто різноманітні методи та інструменти для виявлення та усунення вразливостей web-сайтів. Досліджено різні види атак, такі як SQL-ін'єкції, XSS-атаки та CSRF-атаки, а також методи їх запобігання. Описано роботу різних сканерів вразливостей, таких як OWASP ZAP, Burp Suite, Acunetix та Nessus, а також сканера вразливостей на сайти Nikto.

The article examines various methods and tools for detecting and eliminating vulnerabilities in websites. Different types of attacks such as SQL injections, XSS attacks, and CSRF attacks, as well as methods for preventing them, are investigated. The article describes the operation of various vulnerability scanners such as OWASP ZAP, Burp Suite, Acunetix, and Nessus, as well as the Nikto vulnerability scanner for websites.

Актуальність. Дослідження вразливостей web-сайтів та методів їх усунення є дуже актуальними у наш час, оскільки з кожним роком кількість web-сайтів та їх важливість для бізнесу та суспільства зростає. Із збільшенням кількості web-сайтів зростає і загроза їх вразливостей. Згідно статистики, більше 60% усіх атак в Інтернеті відбуваються через вразливості web-сайтів. Нападники використовують ці вразливості для викрадення даних користувачів, встановлення шкідливих програм або впровадження зловмисного коду на серверах web-сайтів. В разі вразливості web-сайту зловмисник може здійснювати різноманітні атаки, такі як викрадення конфіденційної інформації, редагування даних, введення шкідливого коду, відправку спаму та багато іншого. Це може призвести до серйозних наслідків для бізнесу, які можуть зазнавати фінансових втрат або втрати довіри клієнтів. Дослідження вразливостей web-сайтів та розробка методів їх усунення є важливою для забезпечення безпеки в Інтернеті. На жаль, більшість web-сайтів не забезпечують достатньої безпеки та мають вразливості, які можуть бути використані для атак.

Тому, дослідження вразливостей web-сайтів та розробка методів їх усунення має велике значення для забезпечення безпеки в Інтернеті, а також для захисту конфіденційності та безпеки користувачів web-сайтів. Тема є надзвичайно актуальною, і вона постійно вдосконалюється та розширюється відповідно до нових викликів та загроз у сфері кібербезпеки.

Метою статті є дослідження проблеми вразливостей web-сайтів та підвищення рівня свідомості про важливість захисту web-додатків від зловмисних атак та надання практичних порад щодо захисту web-сайтів від вразливостей.

Об'єктом дослідження є процес виявлення та усунення вразливостей в web-сайтах, які можуть призвести до некоректної роботи сайту, втрати конфіденційної інформації, порушення безпеки відвідувачів сайту та можливого внесення шкідливого коду.

Предмет дослідження – web-сайти та їхні вразливості, які можуть бути використані зловмисниками для здійснення різних видів кібератак, таких як SQL-ін'єкції, XSS-атаки, CSRF-атаки.

Аналіз попередніх досліджень. Дослідження вразливостей web-сайтів та методів їх усунення є актуальною темою для багатьох дослідників з усього світу. Серед українських вчених, які займалися цією темою, можна відзначити таких: В. Ю. Степанович, професор кафедри програмної інженерії та інформаційних технологій Національного авіаційного університету, який досліджує питання безпеки програмного забезпечення, включаючи вразливості web-сайтів та методи їх виявлення та усунення; К. М. Гуцало, кандидат технічних

наук, доцент кафедри інформаційних технологій та захисту інформації Львівської політехніки, який займається питанням захисту інформації, включаючи вразливості web-сайтів та методи їх усунення. Серед зарубіжних вчених, які займалися цією темою, можна відзначити таких: Джейсон Халперн (Jason Halpern), доцент кафедри інформаційної безпеки та зв'язку Нью-Йоркського технологічного інституту, який досліджує питання кібербезпеки, включаючи вразливості web-сайтів та методи їх виявлення та усунення; Хуан Хосе Перес (Juan Jose Perez), професор кафедри програмування та технологій інформаційної безпеки університету Ла-Ріоха (Іспанія), займається питанням інформаційної безпеки, включаючи вразливості web-сайтів та методи їх виявлення та усунення.

Виклад основного матеріалу. Дослідження вразливостей web-сайтів та методів їх усунення є дуже важливим процесом для забезпечення безпеки та захисту web-додатків. Це дозволяє виявляти потенційні загрози безпеці та вчасно приймати заходи для їх усунення. Існує безліч різних методів тестування web-додатків на наявність вразливостей, таких як сканування вразливостей, ручний аналіз, тестування від зловмисників та інші. Після виявлення вразливостей web-сайту необхідно прийняти заходи для їх усунення. Цей процес може включати в себе розробку патчів для web-додатків, встановлення спеціальних правил безпеки, зміну налаштувань сервера та баз даних, встановлення додаткових механізмів захисту тощо. Статистичне дослідження найбільш поширених уразливостей web-ресурсів проводять для того, щоб з’ясувати, які вразливості найчастіше зустрічаються та які заходи повинні бути прийняті для їх усунення [1].

За даними звіту OWASP, найбільш поширеними уразливостями web-додатків є: Injection − включає SQL Injection та вразливості, пов’язані з введенням даних, такі як LDAP та XML; Broken Authentication and Session Management − включає вразливості, пов’язані з недостатньою аутентифікацією та керуванням сесіями користувачів; Cross-Site Scripting (XSS) − включає вразливості, пов’язані з введенням скриптів на web-сторінки, що можуть бути виконані у web-браузері користувача; Broken Access Control − включає вразливості, пов’язані з недостатньою перевіркою доступу до ресурсів web-додатка; Security Misconfiguration − включає вразливості, пов’язані з неправильним налаштуванням безпеки web-додатка; Insecure Cryptographic Storage − включає вразливості, пов’язані з недостатньою захистом криптографічних ключів та інших конфіденційних даних; Insufficient Logging and Monitoring − включає вразливості, пов’язані з недостатнім збором та аналізом логів, які можуть бути використані для виявлення та вирішення проблем з безпекою; Insecure Communications − включає вразливості, пов’язані з використанням небезпечних протоколів зв’язку, таких як HTTP замість HTTPS; Improper Error Handling − включає вразливості, пов’язані з недостатньою обробкою помилок, які можуть призвести до розкриття конфіденційної інформації [2, 3].Додатково, для забезпечення безпеки web-додатків можна використовувати різноманітні техніки, такі як шифрування даних, контроль доступу до ресурсів, перевірку введення даних, моніторинг діяльності користувачів тощо. Дослідження вразливостей web-сайтів та методів їх усунення є важливою складовою процесу захисту web -додатків від атак та зловмисного використання. Цей процес складається з кількох етапів, таких як ідентифікація вразливостей, аналіз ризиків, виправлення вразливостей та перевірка ефективності виправлень.

Ідентифікація вразливостей зазвичай здійснюється за допомогою сканерів вразливостей для автоматичного виявлення потенційних проблем web-додатків. Сканери вразливостей можуть виявляти багато різних типів вразливостей, таких як SQL-ін'єкції, крос-сайт скриптінг (XSS), вразливості налагодження та багато інших. Однак, не завжди сканери вразливостей здатні виявити всі можливі вразливості web-сайту. Для виявлення більш складних вразливостей може знадобитися ручний аналіз коду web-сайту. Ручний аналіз дозволяє більш детально проаналізувати код web-сайту та виявити потенційні проблеми, які не можуть бути виявлені сканерами вразливостей. Після сканування web-сайту, сканер визначає потенційні вразливості та надає звіт про результати сканування. На цьому етапі можуть виявлятися різні типи вразливостей, такі як SQL ін'єкції, крос-сайт скриптінг (XSS),

аутентифікаційні та авторизаційні проблеми, ініціювання зловмисного коду та багато іншого. Після ідентифікації вразливостей важливо провести аналіз ризиків, щоб з'ясувати потенційний вплив вразливостей на безпеку web-додатку та його користувачів. Це може включати визначення потенційних наслідків використання вразливостей, оцінку ризику втрати даних або можливості витоку конфіденційної інформації. Після аналізу ризиків, наступним етапом є виправлення вразливостей. Цей процес може бути складним та включати в себе виправлення коду, встановлення нових захисних заходів та перевірку налаштувань сервера. Важливо, щоб виправлення були внесені швидко та ефективно, щоб зменшити час, протягом якого вразливість може бути використана [2].

Дослідження вразливостей web-сайтів тестуванням на проникнення (Penetration Testing або Pentesting) полягає у спробі використання потенційних вразливостей зловмисником для злому web-сайту або отримання несанкціонованого доступу до конфіденційної інформації. При проведенні тестування на проникнення використовуються різні інструменти, включаючи сканери вразливостей, експлоіти та інші програмні засоби [1, 2].

Іншим методом дослідження вразливостей є аудит безпеки web-сайту. Цей метод полягає у вивченні web-сайту та його коду з метою виявлення потенційних проблем безпеки. Аудит безпеки може бути проведений як вручну, так і за допомогою автоматичних інструментів. У разі виявлення вразливостей web-сайту, необхідно прийняти кроки для їх усунення. Це може включати в себе патчінг вразливостей, встановлення обмежень на ввід даних користувачів, налаштування прав доступу до файлів та багато іншого. Для кращої ефективності необхідно регулярно тестувати web-додатки на вразливості та виконувати вимоги безпеки, щоб захистити web-додатки від потенційних загроз.

Web-сервер − це програмне забезпечення, яке надає доступ до web-сторінок через Інтернет. Він обробляє запити від браузерів і надсилає відповіді у вигляді web-сторінок, зображень, відео та іншого контенту.

Однією з найбільш поширених вразливостей web-серверів є кросс-сайтовий скриптінг (XSS). Ця атака полягає в тому, що зловмисник вставляє в шкідливому вигляді скрипти на web-сторінку, яку відвідує жертва [2]. Коли браузер жертви завантажує web-сторінку, він виконує шкідливий скрипт із вмісту сторінки, що може призвести до злочинних дій. Ще однією вразливістю є атака SQL Injection, коли зловмисник вводить SQL-запит в поле для вводу на web-сторінці. Якщо web-сервер не перевіряє вхідні дані на валідність, це може призвести до витоку конфіденційної інформації або навіть до повного контролю над web-сайтом. Окрім того, web-сервер може стати жертвою DDoS-атаки, коли зловмисники намагаються перевантажити сервер великою кількістю запитів одночасно. Це може призвести до відмови в обслуговуванні і виключення сервера з мережі. Вразливості web-серверів та атаки на них можна класифікувати за декількома критеріями. Основні з них: за типом вразливості (кросс-сайтовий скриптінг (XSS): внедріння SQL-запитів (SQL injection); незапобіжність у разі введення великої кількості даних або завантажень (Denial of Service атаки); вразливості, пов'язані з конфігурацією web-сервера або його додатків; вразливості web-сервера, які дозволяють отримати додаткові права доступу до системи; за зонами вразливості: web-додатки, які взаємодіють з сервером; операційна система; мережевий протокол, який використовується для зв'язку між клієнтом і сервером; за характером атаки: атаки на аутентифікацію і авторизацію; атаки на мережу; атаки на програмне забезпечення; атаки на апаратне забезпечення; атаки на процеси й операційну систему [3].

Щоб зменшити ризик вразливостей web-серверів, слід використовувати оновлене програмне забезпечення і виконувати регулярні перевірки на наявність вразливостей. Також слід забезпечити доступ до web-сервера за допомогою безпечних протоколів, таких як HTTPS, і використовувати сильні паролі для адміністративних облікових записів.

Незважаючи на те, що це не повний перелік критеріїв класифікації вразливостей та атак на web-сервери, такий підхід допомагає розробникам та адміністраторам зрозуміти характер вразливостей та захистити системи від атак. Для запобігання атакам, рекомендується використовувати сучасні методи захисту, такі як WAF (Web Application Firewall), IDS

(Intrusion Detection System), IPS (Intrusion Prevention System), а також виконувати регулярні перевірки на наявність вразливостей та оновлення програмного забезпечення [2, 4].

Статистика вразливостей web-додатків є складною та змінюється з часом. Проте, деякі статистичні дослідження та звіти можуть надати загальну картину.

За даними OWASP Top 10 − це список найбільш поширених вразливостей web-додатків, який публікується організацією OWASP (Open Web Application Security Project) кожні 3 роки [2]. Останнє оновлення було зроблено в 2022 році. Згідно статистичних даних з останнього звіту маємо: 63% web-додатків мають проблеми з аутентифікацією та авторизацією; 50% web-додатків мають проблеми з введенням даних, включаючи SQL-ін'єкції та XSS; 27% web-додатків мають проблеми зі захистом конфіденційності даних, включаючи витік інформації та недостатній захист від атак типу CSRF (Cross-Site Request Forgery); 23% web-додатків мають проблеми з захистом від вразливостей, пов'язаних з бізнес-логікою додатку; 20% web-додатків мають проблеми з захистом від вразливостей, пов'язаних з мережевою інфраструктурою.

Таким чином, статистика вказує на те, що вразливості web-додатків є серйозною проблемою та потребують уваги при розробці та захисті web-додатків.

Ієрархія захисту web-серверів полягає в застосуванні різних рівнів захисту на різних рівнях інфраструктури web-сервера. Це дозволяє забезпечити більш ефективний захист від атак і зменшити ризик компрометації системи в цілому. Основні рівні ієрархії захисту web-серверів такі [1, 3, 6]:

1. Фізичний рівень захисту − розглядаються фізичні аспекти захисту web-серверів. Це можуть бути заходи забезпечення фізичної безпеки, наприклад, захист приміщення, в якому знаходиться сервер, від несанкціонованого доступу або надмірної вологості та температурних умов.
2. Мережевий рівень захисту – включає заходи забезпечення безпеки мережі, на якій працює web-сервер. Цей рівень передбачає захист сервера від мережевих атак, таких як DDoS, сканування портів, атаки на протоколи мережі та інші. На цьому рівні можуть використовуватись різні технології, такі як фільтрація трафіку, віртуальні приватні мережі (VPN), мережеві маршрутизатори, мережеві екрани (firewalls) та інші.
3. Захист програмного забезпечення − розглядаються заходи забезпечення безпеки операційної системи, на якій працює web-сервер, а також програмного забезпечення, яке використовується на web-сервері. До таких заходів можна віднести налаштування прав доступу, оновлення програмного забезпечення та встановлення антивірусного програмного забезпечення.
4. Рівень захисту від вразливостей web-додатків − це захист web-додатків, які працюють на web-сервері. Включає в себе регулярне оновлення програмного забезпечення, захист від вразливостей, пов'язаних з додатками, тестування вразливостей та контроль доступу до додатків. Це також захист web-додатків від різних видів атак, таких як SQL-ін'єкції, XSS-атаки, атаки на сесії та багато інших
5. Захист даних − забезпечує захист даних, які зберігаються на web-сервері. Включає в себе використання захисту баз даних, резервного копіювання даних, контроль доступу до даних та захист даних від втрати або крадіжки.
6. Рівень захисту операційної системи – забезпечує захист від атак, які спрямовані на операційну систему, такі як переповнення буферу, отримання некоректних даних, недопустимі параметри та інші.
7. Рівень додаткових заходів – це рівень додаткових заходів захисту, таких як захист від злому паролів, забезпечення безпеки резервного копіювання, забезпечення конфіденційності даних, захист від злому прав доступу тощо.
8. Захист мережі – налаштування мережевої інфраструктури та встановлення системи мережевої безпеки, яка забезпечує безпеку мережевого зв'язку, включаючи мережеві пристрої, такі як маршрутизатори, комутатори та файрволи.

Захист сайтів та web-проектів – це важлива задача, яка потребує системного підходу та використання різних заходів безпеки. Ось кілька порад, які можуть допомогти захистити web-проект [3, 6]:

- Використання надійного програмного забезпечення та оновлення його, встановлювати всі оновлення для операційної системи та програмного забезпечення, включаючи web-сервер, базу даних, CMS (Content Management System) тощо.
- Захист від Cross-Site Request Forgery (CSRF) – це атака, при якій зловмисник використовує web-сторінку, щоб виконати небажані дії в ім'я користувача. Для захисту від CSRF потрібно використовувати механізми токенів та перевіряти джерело запиту.
- Захист від атак на сесії – наприклад, зловмисник може вкрасти ідентифікатор сесії та використовувати його для отримання несанкціонованого доступу до web-додатку. Для захисту від таких атак необхідно використовувати безпечні механізми автентифікації та авторизації.
- Захист від DDOS атак – це атаки, при яких web-сервер отримує велику кількість запитів, що призводить до перевантаження сервера та його відмови у обслуговуванні. Для захисту від DDOS атак можна використовувати спеціальні системи захисту, наприклад, CDN (Content Delivery Network).
- Захист даних користувачів шляхом шифрування та використанням безпечних протоколів зв'язку, таких як SSL / TLS.
- Моніторинг web-проекту на предмет виявлення аномальної активності та кібератак.
- Захист від SQL-ін'єкцій та XSS атак – це дві найбільш поширені вразливості web-додатків. Щоб запобігти цим атакам, потрібно забезпечити належну обробку та валідацію введених даних на стороні сервера.
- Перевірка коду web-додатків на вразливості та недостатки з використанням спеціальних інструментів.

Деякі з поширених вразливостей web-сайтів та методи їх усунення [4, 5]:

1. SQL-ін'єкції – вразливість, при якій зловмисник може виконати SQL-запит на сервері, використовуючи введені користувачем дані. Це може призвести до витоку конфіденційної інформації або зміни даних на сервері. Дуже часто для запобігання SQL-ін'єкціям необхідно використовувати параметризовані запити та перевірку введених даних на стороні сервера.

Щоб виявити та запобігти SQL-ін'єкціям, можна використовувати наступні практики: використання параметризованих запитів є найбільш ефективним способом запобігання SQL-ін'єкціям, оскільки вони дозволяють включити користувацькі дані в запит безпечним чином; фільтрування та перевірка даних, які вводяться користувачами на web-сайті, обмеження прав доступу до бази даних, регулярне оновлення програмного забезпечення, використання відповідних інструментів для перевірки вразливостей web-додатків та баз даних.

2. XSS атаки – вразливість, при якій зловмисник може внести код на сторінку сайту, який виконується в браузері користувача. Це може призвести до виконання небажаних дій на сторінці або витоку конфіденційної інформації. Для запобігання XSS атакам необхідно валідувати та екранувати введені дані на стороні сервера та використовувати Content Security Policy (CSP).

Щоб виявити та запобігти XSS атакам, можна використовувати наступні практики: виконання валідації та екранування даних, які вводяться користувачами на web-сайті, потрібно переконатися, що введені дані відповідали очікуваному формату та не містили небезпечних символів; використання Content Security Policy (CSP), що дозволяє вказати, з яких джерел може завантажуватись вміст на web-сторінках; використання безпечних функцій для відображення даних на web-сторінці; використання HTTP заголовків, таких як Content-Security-Policy; регулярне оновлення програмного забезпечення.

3. CSRF-атаки – це атаки, при яких зловмисник використовує web-сторінку, щоб виконати небажані дії в ім'я користувача. Для усунення цієї вразливості необхідно використовувати механізми токенів та перевіряти джерело запиту.

Щоб виявити та запобігти CSRF-атаки, можна використовувати наступні практики: використання токенів CSRF – це випадкові рядки, які генеруються на сервері та передаються на сторону клієнта. Клієнт повинен включити цей токен в кожен запит до сервера, щоб сервер міг перевірити, чи є запит дійсним; використання методів POST та PUT, оскільки ці методи не можуть бути виконані з інших доменів; встановлення куків з атрибутом "HttpOnly", оскільки атрибут забороняє JavaScript доступ до кукі, що робить неможливим отримання токенів CSRF через JavaScript; встановлення заголовків безпеки дозволяють вказати браузерам, які дії можуть бути виконані на сторінці та які ресурси можуть бути завантажені; використання перевірки джерела запиту, оскільки перевірка джерела запиту дозволяє перевірити, чи є запит відповідним до домену, з якого користувач відправив запит; обмеження терміну дії сесій, якщо сесія зберігається на стороні клієнта, вона може бути вкрадена та використана зловмисником для виконання CSRF атак; використання SSL / TLS, оскільки вони забезпечують захищене з'єднання між користувачем та web-сайтом, що допомагає запобігти витоку інформації.

4. Вразливості в роботі з файлами – це вразливості, які дозволяють зловмиснику завантажувати та виконувати небажаний код на сервері. Для усунення цієї вразливості необхідно обмежувати права доступу до файлів та використовувати правильну валідацію файлових даних.
5. Недостатній захист сесій – вразливість, при якій зловмисник може перехопити ідентифікатор сесії та отримати несанкціонований доступ до облікового запису користувача. Для запобігання цьому необхідно використовувати захист сесій, такий як HTTPS та механізми автентифікації та авторизації.
6. Недостатній захист від DDOS атак – вразливість, при якій web-сервер отримує велику кількість запитів, що призводить до перевантаження сервера та його відмови у обслуговуванні. Для запобігання цьому можна використовувати зах

Сканери вразливостей для web-сайтів – це програмні інструменти, які дозволяють автоматично виявляти вразливості web-додатків. Вони працюють шляхом сканування web-сайту та його компонентів, таких як форми введення, посилання, заголовки, параметри URL тощо з метою виявлення потенційних вразливостей, які можуть бути використані зловмисниками для атак на сайт.

Існує безліч різних сканерів вразливостей для web-сайтів, деякі з яких є безкоштовними, а інші платними. До найвідоміших сканерів вразливостей для web-сайтів належать [6]:

1. OWASP ZAP (Zed Attack Proxy) – це сканер вразливостей web-додатків, який розробляється та підтримується групою волонтерів з усього світу в рамках проекту OWASP (Open Web Application Security Project). Абсолютно безкоштовний сканер вразливостей web-додатків, який може використовуватися як для ручного тестування, так і для автоматизованого сканування web-додатків.

Основні функції OWASP ZAP: активний сканер: сканує web-додатки на наявність вразливостей та допомагає знайти уразливі місця в додатках; пасивний сканер: аналізує трафік між користувачем та сервером, знаходячи можливі вразливості; Spider: сканує web-сайти, знаходячи всі доступні сторінки та ресурси; Fuzzer: автоматично тестує web-додатки на наявність вразливостей, використовуючи різні варіанти введення даних; Interception Proxy: дозволяє перехоплювати та змінювати запити та відповіді між браузером та сервером. OWASP ZAP може бути корисним інструментом для розробників web-додатків та тестувальників, що дозволяє покращити безпеку web-додатків та забезпечити захист від потенційних атак зловмисників. Проте, слід зазначити, що сканер вразливостей не є універсальним інструментом, який може знайти всі можливі вразливості в web-додатку. Він може бути використаний як допоміжний інструмент.

2. Burp Suite – це інструмент для сканування вразливостей та тестування безпеки web-додатків, який дозволяє здійснювати ручні та автоматичні тести з урахуванням специфіки web-протоколу HTTP та HTTPS.

Основні функції Burp Suite включають: сканування вразливостей: Burp Suite здійснює автоматичний аналіз web-додатків та виявляє можливі вразливості, такі як SQL-ін'єкції, XSS атаки, CSRF атаки та інші; ручне тестування: Burp Suite надає можливість проводити ручні тестування web-додатків, що дозволяє більш детально досліджувати потенційні вразливості та знайти їх експлойти; перехоплення трафіку: Burp Suite може перехоплювати трафік між клієнтом та сервером, що дозволяє досліджувати та аналізувати запити та відповіді, що відправляються на сервер; зміна трафіку: Burp Suite дозволяє змінювати запити, що відправляються на сервер, що дозволяє тестувати поведінку web-додатка в різних умовах та знайти потенційні вразливості; визначення тестових скриптів: Burp Suite дозволяє визначати тестові скрипти, що можуть бути виконані автоматично, що дозволяє збільшити ефективність процесу тестування безпеки web-додатків. Burp Suite є платним інструментом, але має безкоштовну версію з обмеженим функціоналом.

3. Acunetix – це інструмент для сканування вразливостей та тестування безпеки web-додатків. Він використовує технології сканування з високою швидкістю, що дозволяє виявляти багато різних вразливостей web-додатків.

Основні функції Acunetix включають: сканування вразливостей: Acunetix здійснює автоматичний аналіз web-додатків та виявляє можливі вразливості, такі як SQL-ін'єкції, XSS атаки, CSRF атаки та інші; перевірка безпеки web-сайту: Acunetix дозволяє перевірити безпеку web-сайту в цілому, зокрема, оцінити рівень безпеки та виявити можливі проблеми з безпекою; забезпечення відповідності з нормами безпеки: Acunetix може перевірити web-додаток на відповідність з різними нормами безпеки, такими як OWASP Top 10, PCI DSS та інші; перехоплення трафіку: Acunetix може перехоплювати трафік між клієнтом та сервером, що дозволяє досліджувати та аналізувати запити та відповіді, що відправляються на сервер; звіти та аналіз результатів: Acunetix надає звіти про виявлені вразливості та можливість аналізу результатів сканування, що дозволяє зосередитися на найбільш критичних проблемах з безпекою. Acunetix є комерційним інструментом з різними пакетами та цінами в залежності від обсягу сканування.

4. Nessus – це інструмент для сканування вразливостей та тестування безпеки web-додатків та мережевих систем. Він дозволяє здійснювати автоматичний аналіз web-додатків та мережевих систем на предмет вразливостей, таких як вразливості у програмному забезпеченні, слабкі паролі, некоректні налаштування сервера та інші.

Основні функції Nessus включають: сканування вразливостей: Nessus здійснює автоматичний аналіз мережевих систем та web-додатків та виявляє можливі вразливості; аналіз конфігурації: Nessus дозволяє аналізувати конфігурацію мережевих систем та web-додатків та виявляти некоректні налаштування, які можуть створити вразливості; розподілена архітектура: Nessus може працювати в розподіленому середовищі та сканувати мережеві системи та web-додатки з різних серверів; результати сканування: Nessus надає детальні результати сканування та допомагає розуміти важливість кожної вразливості та надає рекомендації по їх виправленню; інтеграція: Nessus може інтегруватись з іншими інструментами безпеки, такими як SIEM (Security Information and Event Management), що дозволяє краще контролювати та моніторити стан безпеки мережі. Однак Nessus є платним інструментом, але має безкоштовну версію для домашнього використання з обмеженим функціоналом.

5. Nikto – це відкрите програмне забезпечення для сканування web-сайтів на наявність вразливостей та уразливих точок. Nikto дозволяє здійснювати автоматичний аналіз web-сайтів та виявляти можливі вразливості, такі як незахищені каталоги, файлові вразливості, некоректні налаштування сервера та інші.

Основні функції Nikto включають: сканування вразливостей: Nikto дозволяє здійснювати автоматичний аналіз web-сайтів та виявляти можливі вразливості; аналіз

конфігурації: Nikto дозволяє аналізувати конфігурацію web-сайтів та виявляти некоректні налаштування, які можуть створити вразливості; результати сканування: Nikto надає детальні результати сканування та допомагає розуміти важливість кожної вразливості та надає рекомендації по їх виправленню; модульність: Nikto має модульну структуру та дозволяє користувачам додавати свої власні модулі сканування; крос-платформовість: Nikto може працювати на різних операційних системах, включаючи Windows, Linux та MacOS; налаштування: Nikto має багато налаштувань, які дозволяють користувачам налаштувати сканування відповідно до їх потреб. Nikto є безкоштовним інструментом та доступний для завантаження з офіційного сайту. Він може бути використаний для виявлення широкого спектру вразливостей на web-сайтах, але він не забезпечує повного тестування безпеки web-додатків [5, 6].

Кожен з цих сканерів має свої переваги та недоліки, і вибір конкретного інструмента залежить від конкретних потреб та вимог тестування.

Висновки. Дослідження вразливостей web-сайтів та методів їх усунення є дуже актуальною темою в сучасному світі, де web-додатки стають все більш поширеними та важливими для бізнесу та користувачів. Відсутність належного захисту може призвести до крадіжки даних, втрати конфіденційності, порушення цілісності системи та багатьох інших проблем. Виявлені вразливості web-сайтів можуть призвести до втрати конфіденційної інформації, внутрішніх атак, фішингових атак, крадіжки даних користувачів, відмови в обслуговуванні і багатьох інших негативних наслідків. Тому, для забезпечення безпеки web-додатків, необхідно використовувати різні методи захисту та регулярно перевіряти сайти на наявність вразливостей. Серед методів захисту можна виділити: захист від SQL-ін'єкцій, XSS-атак та CSRF-атак; використання сканерів вразливостей, таких як OWASP ZAP, Burp Suite, Acunetix, Nessus, Nikto; регулярне оновлення web-додатків і фіксування виявлених вразливостей. Отже, дослідження вразливостей web-додатків є надзвичайно важливим процесом, який повинен бути проводжений регулярно для забезпечення належного рівня безпеки web-сайтів та їх користувачів. Використання правильних методів та інструментів може допомогти зменшити ризики вразливостей та забезпечити належний захист web-додатків.

Список використаних джерел

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
2. Bhavani A.B. Cross-site Scripting Attacks on Android WebView / A.B. Bhavani // International Journal of Computer Science and Network. – 2013. – Vol. 2, Issue 2. – 5 p. \\ Режим доступу: http://ijcsn.org/IJCSN-2013/2- 2/IJCSN-2013-2-2-03.pdf (останнє звернення 24.03.2023р.).
3. Аналіз причин виникнення вразливостей у веб-додатках \\ Режим доступу до ресурсу: https://www.ptsecurity.com/wwen/analytics/web-vulnerabilities-2020 (останнє звернення: 24.03.2023р).
4. Захист сайтів і веб-додатків \\ Режим доступу до ресурсу: https://cybermolfar.io/services/web-application-security/ (останнє звернення: 24.03.2023р).
5. Web Application Security Statistics \\ Режим доступу до ресурсу: http://projects.webappsec.org/f/wasc-wafec-v1.0.pdf (останнє звернення: 24.03.2023р).
6. Website Security Statistics Report: 2015. \\ Режим доступу: https://info.whitehatsec.com/Website-StatsReport-2015.htm (останнє звернення: 24.03.2023р).

Робота виконана під науковим керівництвом к.т.н., доцента
ЗВЄРЄВА В.П.

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНИХ СИСТЕМ В ОСВІТНІЙ ПРОЦЕС

СУГАК О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто поняття інформаційної системи та визначено з яких компонентів вона складається. Наведено переваги та недоліки використання інформаційних систем у навчанні. Досліджено та розглянуто сучасні інформаційні системи, що широко використовуються в освітніх процесах.

The article defines the concept of an information system and identifies its components. The advantages and disadvantages of using information systems in education are demonstrated. The modern information systems that are widely used in educational processes are studied and considered.

Актуальність. Технології все більше впливають на нинішній світ і відмова від їх використання є неправильним вибором, що лише стоятиме на шляху до покращення. Люди переходять від застарілих методів навчання, які не забезпечують актуальністю своїх знань, можуть містити в собі застарілі дані, для зміни яких потребують багато часу та матеріалів.

Вже давно студентське суспільство активно користується інтернетом для успішного навчання, підготовки та досліджень.

Але з розвитком технологій та успіхом у дослідницьких проєктах, з урахуванням сучасних проблем, що вплинули на весь світ як пандемія та війна, переселення в інші країни - людство знайшло спосіб покращити освітній процес та зробити його максимально доступним для будь-кого. Ним стало використання інформаційних систем задля навчання.

Раніше для того, щоб керівник міг передати знання своїм підлеглим, потрібно було знаходити місце, час для зустрічі, узгоджувати купу послідовних питань. Такі ситуації витрачали багато ресурсів і були можливі та доступні не для всіх.

Для того, щоб дізнатися про сучасні методи та бібліотеки специфічних тем, необхідно було шукати книги та надзвичайно детально шукати інформацію в просторах інтернету. Щоб вивчити нові технології, потрібно було проходити дорогі курси та купувати багато літератури, оскільки вона була не розповсюдженою.

Але інтегрування інформаційних систем (ІС) стало можливістю до полегшеного процесу навчання, передачі інформації, зустрічей в онлайн-режимі. Цей процес неймовірно полегшив та скоротив етапи доступу до інформації. На момент пандемії він дав можливість не зупиняти навчальні процеси, а розширити можливості для навчання, причому зробити його набагато доступнішим, ніж будь-коли: зі сторони людини - тобто не залежно від віку, статі та інших чинників; та зі сторони технологій, тобто будь-хто, хто має вихід до мережі. Під час війни постраждало багато освітніх закладів, студенти вимушено виїхали в інші країни, проте онлайн-навчання за допомогою різних систем допомагає продовжувати освітній процес та не зупиняти прогрес поточного навчання.

Метою статті є дослідження поняття інформаційних систем, які інформаційні системи було інтегровано для освітніх процесів та визначення переваг та недоліків їх використання в освіті.

Об'єктом дослідження є інформаційна система.

Аналіз попередніх досліджень - праці по дослідженню інтеграції технологій в навчальний процес писали такі сучасні науковці як: Тюркмен Хакан, Кіммонс Ройс, Акрам Хюма, Хартман Ріта, Марло Джексон, Генота Лаурейн, Ледвіг Крістін та інші.

Предмет дослідження - взаємодія інформаційних систем з суб'єктами освітнього процесу з метою поліпшення якості навчання та результативності навчально-виховного процесу.

Завданням є дослідити наявні інформаційні системи, які використовуються в освіті та знайти приклади успішних практик використання інформаційних систем в освітніх закладах, які існують системи управління навчальним процесом, електронні бібліотеки, системи дистанційного навчання; переваги та недоліки такого формату навчання.

Виклад основного матеріалу. Ті, хто стикаються з терміном інформаційної системи, полягають, що загальне поняття інформаційної системи означає якесь програмне забезпечення та його складові. Проте вона містить в собі набагато більше. Найбільш влучно описано ІС так: інформаційна система - це набір людей, інформаційних технологій та бізнес-процесів для досягнення бізнес-мети [1]. Вона складаються з взаємопов'язаних елементів, які працюють для обробки, зберігання, збору та інших маніпуляцій з інформацією, що використовується для прийняття рішень.

Як і в будь-якій системі, можна розписати такі її компоненти (Рис.1).

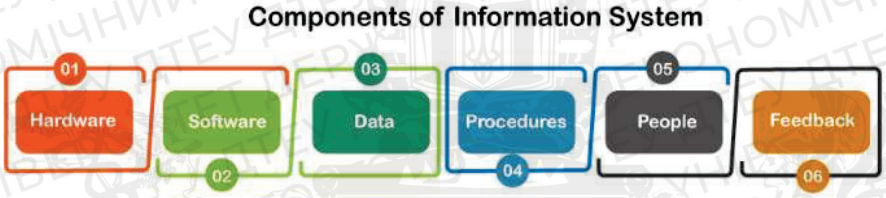


Рис. 1. Компоненти інформаційної системи [1]

Устаткування та програмне забезпечення забезпечують технічне функціонування, інформація та процедури телекомунікації визначають які дані будуть оброблятися та яким способом відбуватимуться маніпуляції даними. Люди та відгуки відповідають за частину, де необхідна людська експертиза та відгук, що покращує кінцевий продукт відповідно до певних вимог [2].

Ізабель Бозада-Джонс (координатор поглибленого навчання для міських шкіл в штаті Огайо) в своїх роздумах наголошує про те, що задля того, щоб змінити в кращу сторону життя дітей і навчити їх чомусь новому, трансформувати і поліпшити освіту, необхідно повністю дозволити старим практикам померти і створити та використовувати щось краще та прогресивніше [3].

Використання інформаційних систем у навчанні не є примхою слідування технологічним досягненням. Вони є пріоритетними, оскільки освітні заклади отримають користь від їх інтеграції:

- Студенти матимуть більшу мотивацію до навчання, поліпшуватимуть свої результати, зменшуватимуться часові затрати за рахунок використання онлайн платформ.
- Інформаційні системи допоможуть студентам управляючи бібліотекою: з можливістю перегляду доступних книг в інтернеті з будь-якого місця в будь-який час, бібліотекар відстежуватиме запити книг для кожного студента та поповнюватиме доступну літературу.
- Не лише студенти отримуватимуть користь, а й викладачі, адже впровадження нових технологій підвищує цифрову грамотність та розвиває нові їх компетенції, збільшуючи їх зону росту.
- Також до переваг необхідно додати прозору комунікацію між студентством та вчителями. ІС допоможуть співпрацювати та спілкуватися для кращого керування та організації освітнього процесу, легшого відстежування та управління академічної діяльності. Створить чесний та правильний процес іспиту шляхом автоматизації всіх етапів екзаменування, що дасть швидкий результат.

Проте, незважаючи на значний перелік переваг інтеграції інформаційних систем в освітній процес, можна виділити і такі недоліки:

- Неповна заміна традиційного навчання. Звісно для спеціальностей та програм, що тісно зв'язані з ІТ-сферою, немає необхідності фізичної присутності на лекціях, семінарах. Але студенти, що потребують практичних навичок, експериментів, дослідів - для них вона необхідна, тому ІС не зможе повністю замінити традиційне навчання.
- Технічні проблеми. У разі збоїв, недоступності сервісів, поломки серверів, освітній процес зупиниться до моменту, поки не будуть вирішені усі питання та не полагоджено обладнання.
- Залежність від технологій. Для навчання мінімально потрібен доступ до мережі інтернет та наявність технічного обладнання. В сучасних реаліях при тривалих відключеннях світла порушувався процес навчання, що негативно впливало на результати студентів.
- Неправильне використання. Якщо неправильно використовувати можливості інформаційних систем, то можна не підвищити ефективність навчання, а створити перепону до доступності матеріалів та бажання її освоєння.
- Міжнародні стандарти. Розробка інформаційних систем створюється за певних стандартів, проте не всі вони є універсальними для всіх країн. Це може завадити співпрацювати з матеріалами інших країн та визнавати дипломи і кількість кредитів матеріалу.

Наразі у світі існує величезна кількість таких систем: від платних до безкоштовних, для звичайних студентів та бізнес-користувачів. Основною їх ціллю є навчання та поліпшення навичок. Розглянемо системи, що широко відомі в суспільстві та часто використовуються в освітніх процесах.

Coursera - це платформа для онлайн-курсів, яка надає доступ до навчальних програм від провідних університетів та компаній світу [4]. Її можна охарактеризувати як ІС, оскільки забезпечує інтеграцію і обмін даними між різними компонентами платформи, такими як користувачі, курси, лекції, завдання, відео матеріали та інші ресурси.

Ця платформа має зручний інтерфейс для користувачів, щоб вони могли швидко та легко знайти необхідний курс, зареєструватись на нього та освоїти матеріал. Крім того, платформа забезпечує можливість контролю навчання шляхом здачі тестів та отримання сертифікатів про успішне завершення курсу. Вона збирає курси та матеріали з усього світу та забезпечує інтеграцію зовнішніми ІС як соцмережами, поштовими сервісами для підвищення ефективності користування платформою.

Google Workspace є однією з найпопулярніших інформаційних систем для освіти та бізнесу. Ця ІС надає безліч інструментів для ефективної співпраці, комунікації та навчання. Для освіти Google Workspace пропонує спеціальний пакет інструментів, що називається Google Workspace for Education. Він включає в себе різноманітні застосунки, такі як Google Classroom, Google Drive, Google Docs, Google Sheets та інші (Рис.2).

З їх допомогою викладачі мають можливість створювати і редагувати документи в режимі реального часу та офлайн, надавати завдання та відстежувати їх виконання, проводити онлайн-уроки. Студенти в свою чергу можуть відслідковувати свої завдання, їх виконання та оцінювання, створювати плани та організовувати свої навчальні процеси. Користувачі можуть взаємодіяти між собою за допомогою пошти, чату або ж відеоконференцій. Будь-хто може користуватися застосунками, що є великим плюсом, оскільки є доступним для всіх верств населення, більш того, Google Workspace є доступним на різних пристроях та операційних системах, що робить цю інформаційну систему універсальною [5].

Prometheus - це найбільше навчальна платформа в Україні, яка надає інструменти для створення, організації та проведення навчальних курсів та іспитів онлайн [6]. Ця інформаційна система призначена для використання в освітніх установах, компаніях та організаціях з метою забезпечення зручного та ефективного онлайн-навчання. ІС дозволяє викладачам створювати інтерактивні курси та завдання, які можуть бути доступні для учнів у будь-який зручний для них час для проходження. Платформа також надає можливість створювати тестові завдання та

іспити з автоматичною перевіркою, що дозволяє викладачам ефективно та швидко оцінювати знання студентів.

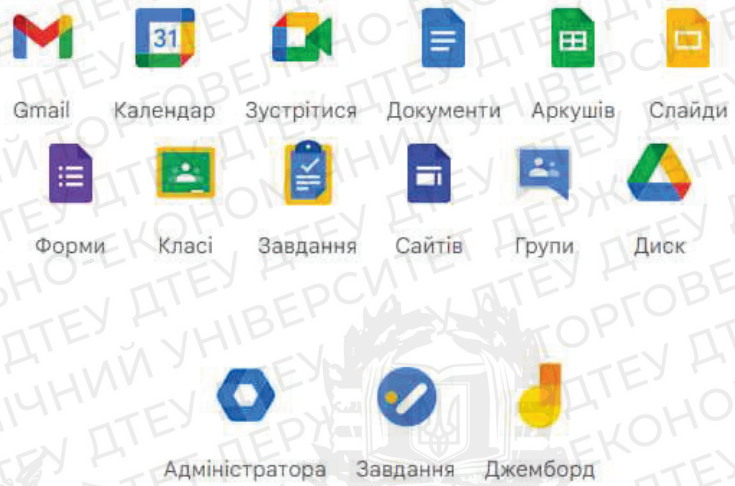


Рис. 2. Сервіси від Google Workspace [5]

Однією з головних переваг Prometheus є те, що платформа є безкоштовною та відкритою для використання, що дозволяє учасникам освітнього процесу отримувати доступ до якісної онлайн освіти незалежно від їхнього фінансового стану. Крім того, Prometheus має велику кількість інструментів для відстеження прогресу студентів, що дозволяє викладачам ефективно спілкуватися зі студентами, консультувати їх та покращувати якість навчання. Вона має два доступи до навчання: безкоштовний та Prometheus+ (Рис. 3). Такий поділ дає можливість навчатись будь-кому на безкоштовній основі та створювати й проходити ексклюзивні курси для певних категорій студентів з розширеними можливостями для навчання.

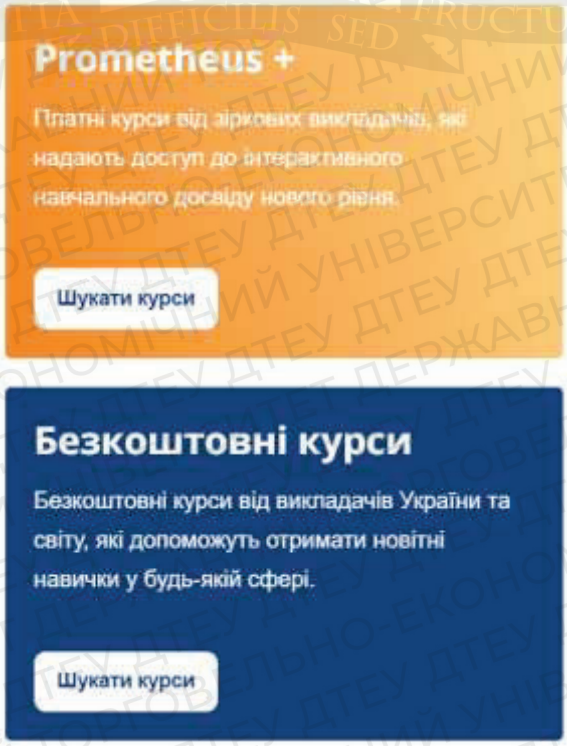


Рис. 3. Вибір каталогу до курсів Prometheus [6]

Окрім навчання студентства, потрібно враховувати і звичайних людей у повсякденному часі. Вони живуть у постійному русі технологій та навчання є стимулом до подальшого розвитку. Саме тому створили такі компанії як AcademyOcean, Docebo.

Docebo - це хмарна платформа управління навчаннями, яка дозволяє підприємствам і навчальним організаціям створювати та керувати ефективними програмами навчання для співробітників, клієнтів та партнерів [7]. Платформа має такі функції як: створення, організація та виконання онлайн-курсів, тестування та інших завдань навчання в будь-який час та з будь-якого місця, що робить її ефективною системою для дистанційного навчання (Рис.4).

Рис. 4. Навчальний цикл в Docebo [7]

Платформа має різноманітні інструменти для моніторингу та оцінювання результатів навчання, такі як звіти та аналітика і також інтегрується з багатьма іншими системами, що дозволяє легко і ефективно інтегрувати Docebo з існуючими системами управління навчаннями та іншими інформаційними системами. Крім того, потрібно додатково зазначити про забезпечення безпеки даних та конфіденційності, що є дуже важливим для бізнес та навчальних організацій.

Схожою системою за функціоналом є AcademyOcean (Рис.5). Це інформаційна система, яка також дозволяє компаніям та навчальним закладам створювати власні онлайн-курси, тренінги та іспити для своїх співробітників та студентів і відслідковувати показники виконання завдань. Для більш ефективного навчання, система пропонує різні методики та інструменти, такі як відео уроки, інтерактивні завдання та тести, відгуки та коментарі, які дозволяють користувачам взаємодіяти та ділитися своїми думками та враженнями, що покращує освітній процес [8]. AcademyOcean має досить доступну ціну та можливість безкоштовного використання для невеликих груп користувачів.

Рис. 5. Українська розумна система для бізнесу [8]

Проте недоліками останніх систем є менший поріг доступності. З широким функціоналом, вони мають лише платний доступ, тому дані ІС підходять для бізнес компаній, що хочуть розвивати своїх клієнтів та працівників.

Висновки. Аналізуючи розглянутий в статті матеріал, можна зробити висновок, що інтеграція інформаційних систем в освітній процес є надзвичайно корисним процесом. Вона матиме позитивний вплив на навчання та покращить якість освіти. Інформаційні системи можуть забезпечувати більшу доступність матеріалів для студентів, зменшувати часові затрати на пошук необхідної інформації та покращувати результати навчання. Вони оцінюватимуть чесно та швидко результати перевірок. Також, ІС зможе допомогти в управлінні бібліотекою та сприяти більш ефективній комунікації між студентами та викладачами, за рахунок збільшення можливих методів спілкування.

Проте, важливо взяти до уваги, що неправильне використання інформаційних систем може не тільки погіршити ефективність навчання, але й створити додаткові перепони до доступності матеріалів та бажання її освоєння. Крім того, повна заміна традиційного навчання, особливо для студентів, що потребують практичних навичок, може зробити інформаційні системи менш ефективними в певних випадках. Можливим виходом з цієї ситуації є використання VR та AR технологій, які зможуть наочно показати студентам необхідні практичні роботи, створювати досліди, без необхідності бути присутнім фізично на занятті.

Інтеграція інформаційних систем у освітній процес є невід'ємною частиною сучасної освіти. Вона дозволяє створити навчальне середовище, яке сприяє залученню та мотивації учнів, поліпшенню якості навчання та спрощенню взаємодії між учасниками навчального процесу. Для досягнення успіху в інтеграції інформаційних систем слід уважно розглядати переваги, виклики та кращі практики, спираючись на спільний зусилля педагогів, технологічних експертів та адміністраторів. В результатах цієї спільної праці полягає справжній потенціал технологій у трансформації навчального процесу.

Отже, висновки полягають в тому, що інформаційні системи мають великий потенціал для використання в освітньому процесі, але поки їх необхідно розглядати як допоміжні засоби та правильно використовувати, щоб досягти найбільш ефективних результатів.

Список використаних джерел

1. Information System Definition [Електронний ресурс]. – Режим доступу : https://www.javatpoint.com/information-system-definition
2. What is information systems? Definition, uses, and examples [Електронний ресурс]. – Режим доступу : https://zapier.com/blog/what-is-information-systems/
3. To Improve a Child's Education, We Must Be Willing to Let Old Practices Die [Електронний ресурс]. – Режим доступу : https://www.edsurge.com/news/2023-04-05-to-improve-a-child-s-education-we-must-be-willing-to-let-old-practices-die
4. Coursera`s mission, vision [Електронний ресурс]. – Режим доступу : https://about.coursera.org/
5. Creating new possibilities in higher education [Електронний ресурс]. – Режим доступу : https://edu.google.com/intl/en_ALL/why-google/for-your-institution/higher-ed-solutions/
6. Про нас. Prometeus [Електронний ресурс]. – Режим доступу : https://prometheus.org.ua/about-us/
7. All your learning challenges, solved [Електронний ресурс]. – Режим доступу : https://www.docebo.com/
8. Розумна система для навчання [Електронний ресурс]. – Режим доступу : https://academyocean.com/ua

Робота виконана під науковим керівництвом к.т.н., доцента
РЗАЄВОЇ С.Л.

АНАЛІЗ ВІДПОВІДНОСТІ ПЛАТІЖНИХ СИСТЕМ ДО НОРМ GDPR

ТРЕТЬЯКОВ М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

Ця стаття присвячена аналізу відповідності платіжних систем до норм. Вона включає перевірку законодавчої відповідності, безпеки, зручності та вартості використання платіжних систем для користувачів та бізнесу. Детальніше буде розглянуто різноманітні питання, пов'язані з відповідністю платіжних систем до норм та їхніх можливостей у сучасному світі.

This article is dedicated to the analysis of compliance of payment systems with regulations. It includes checking the legislative compliance, security, convenience, and cost-effectiveness of using payment systems for users and businesses. Further, a variety of issues related to the compliance of payment systems with regulations and their capabilities in the modern world will be discussed.

Актуальність дослідження. Зі збільшенням використання платіжних систем у цифровій економіці захист персональних даних став гострою проблемою. Загальний регламент захисту даних (General Data Protection Regulation, GDPR) — це нормативна база, спрямована на захист персональних даних осіб у межах Європейського Союзу (ЄС) і має значний вплив на платіжні системи. Ця стаття є актуальною, оскільки містить поглиблений аналіз відповідності платіжних систем нормам GDPR.

Метою цієї статті є аналіз відповідності платіжних систем нормам GDPR. Цей аналіз має на меті визначити основні виклики та ризики, з якими стикаються платіжні системи з точки зору захисту даних, і оцінити рівень їх відповідності нормам GDPR. Крім того, ця стаття має на меті надати рекомендації платіжним системам щодо покращення відповідності GDPR та зменшення ризиків, пов’язаних із захистом даних.

Об’єктом дослідження є платіжні системи та їх відповідність нормам GDPR. Це дослідження має на меті визначити типи даних, які обробляють і зберігають платіжні системи, основні виклики та ризики, з якими стикаються платіжні системи щодо захисту даних, а також рівні відповідності платіжних систем нормам GDPR.

Предметом цього дослідження є структура відповідності GDPR та її ключові компоненти. Це дослідження має на меті надати огляд системи відповідності GDPR і того, як платіжні системи можуть застосовувати її до своїх операцій. Крім того, це дослідження роз’яснює ролі та обов’язки різних учасників у забезпеченні відповідності GDPR у платіжних системах.

Оскільки світ стає все більш цифровим, платіжні системи стали важливою частиною економіки [1]. Однак через величезну кількість особистих даних, які обробляють платіжні системи, виникає занепокоєння щодо захисту конфіденційності та даних людей. Тут вступає в дію Загальний регламент захисту даних (GDPR).

GDPR — це всеосяжний регламент захисту даних, який набув чинності в травні 2018 року і призначений для посилення захисту персональних даних і конфіденційності осіб у Європейському Союзі (ЄС). Він поширюється на всі компанії, які обробляють персональні дані громадян ЄС, незалежно від того, де розташована компанія [2]. Це означає, що платіжні системи, які збирають і обробляють величезні обсяги персональних даних, також повинні відповідати нормам GDPR.

Актуальність GDPR для платіжних систем неможливо переоцінити. Платіжні системи використовуються для обробки фінансових транзакцій, і тому вони обробляють конфіденційні особисті дані, такі як номери кредитних карток, реквізити банківського рахунку та особиста ідентифікаційна інформація [1]. Якщо ці дані не захищені належним чином, це може призвести

до серйозних фінансових і репутаційних дзбитків як для платіжних систем, так і для їх користувачів.

Основні принципи та вимоги GDPR включають отримання інформованої та чіткої згоди від осіб перед обробкою їхніх персональних даних, впровадження відповідних технічних та організаційних заходів для захисту персональних даних, надання особам права доступу та виправлення своїх персональних даних, а також повідомлення про порушення даних. до контролюючих органів протягом 72 годин [4, 5].

Рис. 1. Відповідність GDPR [8]

У цій статті ми розберемо відповідність платіжних систем нормам GDPR. Ми оглянемо платіжні системи, їх діяльності з обробки даних і рамок відповідності GDPR. Оцінимо відповідність платіжних систем нормам GDPR та визначимо найкращі практики. Ми також обговоримо наслідки невідповідності нормам GDPR для платіжних систем і надамо рекомендації щодо підвищення відповідності GDPR.

Платіжні системи є важливою частиною цифрової економіки, що дозволяє окремим особам і компаніям здійснювати електронні транзакції. Ці системи, які включають процесори кредитних і дебетових карток, мобільні платіжні програми та онлайн-платіжні шлюзи, відповідають за обробку величезних обсягів персональних даних. Однак це також означає, що вони вразливі до витоку даних, кібератак та інших ризиків захисту даних.

Щоб зрозуміти відповідність платіжних систем нормам GDPR, важливо спочатку мати розуміння про ці системи та їх діяльності з обробки даних. Платіжні системи можна визначити як платформи, які полегшують переказ грошей від однієї організації до іншої, як правило, за допомогою електронних засобів. Ці системи відіграють вирішальну роль у цифровій економіці, дозволяючи компаніям здійснювати операції з клієнтами та постачальниками по всьому світу.

Одним із основних типів даних, які платіжні системи обробляють і зберігають, є персональні дані. Це може включати таку інформацію, як імена, адреси, адреси електронної пошти та номери телефонів. Крім того, платіжні системи також обробляють конфіденційні фінансові дані, такі як номери кредитних карток, реквізити банківських рахунків та історії транзакцій [3]. Усі ці дані є дуже конфіденційними та мають бути захищені, щоб запобігти несанкціонованому доступу, крадіжці чи неправомірному використанню.

Незважаючи на критичну роль, яку платіжні системи відіграють у цифровій економіці, вони стикаються з декількома ключовими ризиками та проблемами щодо захисту даних.

Однією з найбільш важливих проблем є дедалі складніші кібератаки, які можуть бути спрямовані на вразливі місця платіжних систем і призвести до витоку даних. Платіжні системи також повинні вирішувати проблеми, пов'язані з безпекою даних, такими як підтримка точності даних, захист від несанкціонованого доступу та забезпечення цілісності даних. Крім того, вони повинні забезпечити прозорість своєї діяльності з обробки даних, надаючи чітку інформацію про те, як дані збираються, обробляються та використовуються.

Наслідки витоку даних і недотримання норм GDPR можуть бути серйозними для платіжних систем. Ці наслідки можуть включати значні фінансові втрати, шкоду репутації та юридичну відповідальність. Таким чином, платіжні системи повинні серйозно ставитися до захисту даних і вживати відповідних заходів для забезпечення відповідності нормам GDPR.

Щоб забезпечити відповідність нормам GDPR, платіжні системи повинні запровадити комплексну структуру відповідності GDPR. Структура відповідності GDPR складається з кількох ключових компонентів, включаючи відображення даних, оцінку ризиків, політики та процедури, а також навчання та обізнаність працівників [9].

Відображення даних — це процес ідентифікації та документування всіх персональних даних, які збираються, обробляються та зберігаються платіжними системами. Це включає дані, які зберігаються сторонніми постачальниками, і передачу даних до країн за межами ЄС [4]. Після відображення даних платіжні системи можуть проводити оцінку ризиків, щоб визначити потенційну вразливість, загрози та ризики для персональних даних, які вони зберігають.

На основі результатів оцінки ризиків платіжні системи повинні розробити політики та процедури, спрямовані на виявлені ризики та забезпечення відповідності GDPR. Ці політики та процедури мають включати заходи щодо захисту даних, повідомлення про порушення та права суб'єктів даних. Важливо забезпечити регулярний перегляд і оновлення цих політик і процедур, щоб відобразити зміни в нормативному середовищі або бізнес-практики [5].

Іншим важливим компонентом відповідності GDPR є навчання та обізнаність працівників. Платіжні системи повинні забезпечити, щоб співробітники пройшли навчання щодо відповідності GDPR, включаючи політики та процедури захисту даних, і усвідомлювали свої обов'язки щодо захисту персональних даних. Співробітники повинні розуміти важливість дотримання GDPR і вміти визначати ризики та порушення захисту даних і повідомляти про них.

Платіжні системи можуть застосувати рамки відповідності GDPR до своїх операцій, попередньо оцінивши свій поточний статус відповідності вимогам GDPR. Потім вони повинні розробити дорожню карту, яка окреслює кроки, необхідні для досягнення відповідності GDPR, включаючи відображення даних, оцінку ризиків, розробку політики та навчання співробітників. Важливо переконатися, що всі аспекти рамок відповідності GDPR реалізовані, і регулярні аудити проводяться для моніторингу відповідності [5].

У забезпеченні відповідності GDPR різні учасники відіграють різні ролі та відповідальність. Платіжні системи несуть відповідальність за забезпечення відповідності нормам GDPR і вжиття відповідних заходів для захисту персональних даних. Сторонні постачальники, такі як платіжні постачальники та постачальники зберігання даних, також повинні відповідати нормам GDPR і бути прозорими у своїй діяльності з обробки даних.

Органи нагляду, наприклад органи захисту даних, відіграють важливу роль у забезпеченні відповідності GDPR, надаючи вказівки, забезпечуючи дотримання норм GDPR, розслідуючи та накладаючи санкції на невідповідність. Суб'єкти даних також відіграють вирішальну роль у дотриманні GDPR, реалізуючи свої права, наприклад право на доступ до своїх особистих даних і право на їх виправлення, а також повідомляючи про будь-які порушення захисту даних контролюючим органам.

Після розуміння принципів відповідності GDPR і того, як платіжні системи можуть застосовувати їх у своїх операціях, важливо оцінити рівень відповідності платіжних систем нормам GDPR. Оцінка відповідності може допомогти платіжним системам визначити сфери, де їм потрібно вдосконалити, і розробити дорожню карту для досягнення повної відповідності GDPR.

Одним із критичних критеріїв оцінки відповідності GDPR є оцінка впливу на захист даних (DPIA). Data Protection Impact Assessment (DPIA) — це обов'язковий процес, який платіжні системи повинні виконувати, щоб виявити та мінімізувати ризики захисту даних, пов'язані з їх діяльністю. DPIA оцінює необхідність, пропорційність і законність діяльності з обробки даних і визначає потенційні ризики для захисту даних і заходи для їх зменшення. Платіжні системи повинні забезпечити проведення DPIA для всіх нових дій з обробки та регулярний перегляд для відображення змін у операційній діяльності чи нормативному середовищі [6].

Ще одним критерієм оцінки відповідності GDPR є політика конфіденційності. Платіжні системи повинні мати чітку та стислу політику конфіденційності, яка пояснює їх діяльність з обробки даних і спосіб збору, обробки та зберігання персональних даних. Політика конфіденційності також повинна містити інформацію про права суб'єкта даних, наприклад право на доступ до особистих даних і їх виправлення, а також контактні дані уповноваженого із захисту даних. Платіжні системи повинні гарантувати, що їхня політика конфіденційності є доступною, прозорою та актуальною.

Механізми згоди також мають вирішальне значення для оцінки відповідності GDPR. Платіжні системи повинні отримати чітку та інформовану згоду суб'єктів даних перед збором, обробкою або зберіганням їхніх персональних даних. Платіжні системи також повинні гарантувати, що суб'єкти даних можуть відкликати свою згоду в будь-який час і що механізми згоди є доступними, зрозумілими та стислими.

Іншими критеріями для оцінки відповідності GDPR є права суб'єктів даних і процедури сповіщення про порушення даних. Платіжні системи повинні гарантувати, що суб'єкти даних можуть реалізувати свої права, такі як право на доступ і виправлення персональних даних, а також оперативну відповідь на запити. Платіжні системи також повинні мати чіткі та ефективні процедури сповіщення про порушення даних, які дозволяють їм виявляти, повідомляти та розслідувати порушення даних протягом необхідного 72-годинного періоду.

Порівняння рівнів відповідності різних платіжних систем і визначення найкращих практик може допомогти платіжним системам навчатися одна в одної та покращити відповідність GDPR. Платіжні системи, які демонструють високий рівень відповідності GDPR, можуть слугувати взірцем для інших платіжних систем. Найкращі практики щодо відповідності GDPR включають впровадження комплексної системи відповідності GDPR, проведення регулярних аудитів та оцінок, а також забезпечення навчання та підвищення обізнаності працівників.

Невідповідність GDPR може мати серйозні наслідки для платіжних систем, включаючи штрафи, репутаційну шкоду та юридичну відповідальність. Штрафи GDPR можуть становити до 4% річного глобального доходу компанії або 20 мільйонів євро, залежно від того, що більше. Платіжні системи, які не відповідають нормам GDPR, також можуть зазнати репутаційної шкоди, оскільки клієнти можуть втратити довіру до здатності платіжної системи захистити їхні особисті дані. Невідповідність GDPR також може призвести до юридичної відповідальності, оскільки суб'єкти даних можуть вимагати компенсації за будь-яку шкоду, заподіяну внаслідок невідповідності платіжної системи [7].

Висновки

Підсумовуючи, дотримання правил GDPR має важливе значення для платіжних систем для підтримки довіри клієнтів і забезпечення довгострокової стабільності їх операцій. Оцінка відповідності GDPR на основі різних критеріїв, таких як DPIA, політика конфіденційності, механізми отримання згоди, права суб'єктів даних і процедури сповіщення про порушення даних, може допомогти платіжним системам визначити сфери для вдосконалення та розробити дорожню карту для досягнення повної відповідності GDPR. Порівняння рівнів відповідності різних платіжних систем і визначення найкращих практик також можуть допомогти платіжним системам покращити відповідність GDPR. Невідповідність GDPR може мати серйозні наслідки для платіжних систем, включаючи штрафи, репутаційну шкоду та

юридичну відповідальність. Важливо, щоб платіжні системи надавали пріоритет відповідності GDPR, щоб захистити особисті дані та зберегти довіру клієнтів.

Підсумовуючи вище сказане, аналіз відповідності платіжних систем нормам GDPR є надзвичайно важливим у сучасній цифровій економіці. Наша оцінка показала, що багатьом платіжним системам ще потрібно пройти довгий шлях, щоб досягти повної відповідності вимогам GDPR. Однак деякі платіжні системи досягли значного прогресу у відповідності цим стандартам, і їхні найкращі практики можуть слугувати керівництвом для інших.

На основі наших критеріїв оцінки ми виявили, що багато платіжних систем не повністю запровадили оцінки впливу на захист даних, політики конфіденційності та механізми отримання згоди відповідно до стандартів GDPR. Подібним чином деякі платіжні системи не мають відповідних прав суб'єктів даних і процедур сповіщення про порушення даних. Тому ми рекомендуємо всім платіжним системам застосовувати більш проактивний підхід для дотримання норм GDPR.

Крім того, недотримання GDPR може призвести до серйозних наслідків, таких як великі штрафи, репутаційні збитки та юридична відповідальність. Платіжні системи повинні визнавати важливість відповідності GDPR для підтримки довіри клієнтів і забезпечення довгострокової стабільності в галузі.

Як висновок, структура відповідності GDPR є важливим інструментом, який можуть використовувати платіжні системи, щоб переконатися, що вони відповідають необхідним стандартам захисту даних і конфіденційності. Застосовуючи найкращі практики та усуваючи прогалини у відповідності, платіжні системи можуть досягти більшої довіри та впевненості серед клієнтів, що може допомогти їм досягти успіху на конкурентному ринку. Відповідність нормам GDPR не слід розглядати як тягар, а як можливість продемонструвати відданість конфіденційності та захисту даних клієнтів.

Список використаних джерел

1. Г.В. Коваленко, І.В. Коваль. "Моделювання та аналіз інформаційно-комунікаційних систем". - К.: Видавництво "Логос", 2016. - 272 с.
2. О.О. Шумило. "Технології захисту інформації в комп'ютерних системах". - К.: Інформаційно-аналітичне агентство, 2014. - 240 с.
3. М.О. Шевченко. "Захист інформації в комп'ютерних мережах". - К.: Видавництво "Політехніка", 2016. - 292 с.
4. Офіційний портал Європейського Союзу з питань захисту персональних даних (https://ec.europa.eu/info/law/law-topic/data-protection_en)
5. Офіційний текст загального регламенту про захист персональних даних (GDPR) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679)
6. Директива Європейського Парламенту та Ради 2015/2366/ЄС щодо платіжних послуг в межах внутрішнього ринку, що змінює та визначає Закон про платіжні послуги 2009 року (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366)
7. Наказ Національного банку України "Про затвердження Типових правил забезпечення безпеки платіжних карток" від 16.11.2016 р. № 376 https://zakon.rada.gov.ua/laws/show/z2049-16
8. GDPR Compliance https://www.collidu.com/presentation-gdpr-compliance
9. Кокарча , Ю., & Лалуєва , А. (2022). ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ: ВПЛИВ ВОЄННОГО СТАНУ. Collection of Scientific Papers «SCIENTIA», (November 25, 2022; Sydney, Australia), 70–74. Retrieved from https://previous.scientia.report/index.php/archive/article/view/579

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКО Б.Т.

МОНІТОРИНГ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ

ТУРЧЕНКО Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто інформацію про важливість забезпечення інформаційної безпеки на підприємствах. Визначено сучасні засоби забезпечення інформаційної безпеки на прикладі SIEM-систем, наведені найбільш популярні виробники та постачальники послуг SIEM-систем. Описано основне призначення та особливості SIEM-систем для збору інформації та управління подіями.

The article discusses information about the importance of ensuring information security at enterprises. Modern means of ensuring information security are defined using the example of SIEM systems, the most popular manufacturers and service providers of SIEM systems are listed. The main purpose and features of SIEM systems for collecting information and managing events are described.

Актуальність. Удосконалення та забезпечення системи безпеки співробітників підприємства є одним із пріоритетних напрямів досягнення максимальної ефективності його діяльності. Від того, яким чином є сформована система безпеки співробітників на підприємстві, залежить ефективність реалізації поставлених його цілей. Результатом якісної роботи підприємства в сфері безпеки є стабільність і гармонійність її діяльності, і, як наслідок, стабільне зростання такого показника, як оптимізація прибутковості підприємства. Система моніторингу стану інформаційної безпеки є основним елементом системи безпеки підприємства, оскільки, від якості діяльності співробітників залежать сфери діяльності підприємств.

Моніторинг стану інформаційної безпеки, за допомогою дій співробітників підприємства – це результат налагодженої роботи багатьох служб, у першу чергу, служби безпеки та служби персоналу. Кожен претендент на вакансію, співробітник підприємства повинен розглядатися, як джерело ризику та потенційної загрози. Ризики можуть бути пов'язані як з умисним нанесенням шкоди, так і з необережністю. Потенційно небезпечними є працівники з низьким рівнем кваліфікації. Невідповідність рівня кваліфікації займаній посаді призводить до невдоволення працівника своєю роботою та умовами праці. На виникнення ризиків, також, впливають відсутність чітко і однозначно закріплених юридичних правовідносин, неадекватне оцінювання результатів праці. До втрат і збитків може привести низька якість прогнозування і контролювання зміни благонадійності тощо.

Метою статті є дослідження особливостей моніторингу стану інформаційної безпеки на підприємствах.

Об'єктом дослідження є процес моніторингу інформаційної безпеки.

Предмет дослідження – комп'ютерна мережа підприємства.

Аналіз попередніх досліджень. Дослідженням питань інформаційної безпеки займається ряд як вітчизняних, так і закордонних дослідників, а також значна кількість державних і недержавних наукових установ, дослідницьких та аналітичних центрів. Серед науковців, що досліджують проблеми інформаційної безпеки: А. Грамші, К. Кубечка, Р. Калюжний, Б. Кормич, В. Ліпкан, В. Макаренко, Ю. Максименко, О. Барановський та ін.

Виклад основного матеріалу. Сьогодні існує безліч загроз інформаційній безпеці підприємств, бізнесовим структурам. Серед загроз з якими стикаються підприємства – зовнішні вторгнення в корпоративні мережі і, як результат, – недоступність до корпоративних сервісів, викрадення конфіденційних даних та інформації, неможливість контролю веб-

трафіку, проникнення вірусів і, так званих, «троянських» програм, різні види внутрішніх і зовнішніх загроз підприємству та його діяльності.

Інформаційна безпека – стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз. Захист інформації передбачає систему заходів, спрямованих на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації, втрати, знищення, порушення цілісності [1, 2].

Метою реалізації інформаційної безпеки (ІБ) будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту. Для побудови та ефективної експлуатації системи забезпечення ІБ необхідно [2]:

- виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;
- врахувати вимоги національного та міжнародного законодавства;
- використовувати напрацьовані практики (стандарти, методології) побудови подібних системи забезпечення ІБ;
- визначити підрозділи, відповідальні за реалізацію та підтримку системи забезпечення ІБ;
- розподілити між підрозділами області відповідальності у здійсненні вимог системи забезпечення ІБ;
- на базі управління ризиками ІБ визначити загальні положення, технічні та організаційні вимоги, що становлять політику ІБ об'єкта захисту;
- реалізувати вимоги політики ІБ, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;
- реалізувати систему управління інформаційної безпеки (СУІБ);
- використовуючи СУІБ, організувати регулярний контроль ефективності системи забезпечення ІБ та при необхідності переглядати і коригувати системи забезпечення ІБ і СУІБ.

Для побудови політики ІБ рекомендується окремо розглядати основні напрями захисту ІБ:

- захист об'єктів ІБ;
- захист процесів, процедур і програм обробки інформації;
- захист каналів зв'язку (акустичні, інфрачервоні, провідні оптичні);
- придушення побічних електромагнітних випромінювань;
- управління системою захисту.

При цьому політика ІБ повинна описувати наступні етапи створення засобів захисту інформації:

1. Визначення інформаційних і технічних ресурсів, що підлягають захисту.
2. Виявлення повної безлічі потенційно можливих загроз і каналів витоку інформації.
3. Проведення оцінки вразливості і ризиків інформації за наявної безлічі загроз і каналів витоку.
4. Визначення вимог до системи захисту.
5. Здійснення вибору засобів захисту інформації та їх характеристик.
6. Впровадження та організація використання обраних заходів, способів та засобів захисту.
7. Здійснення контролю цілісності і керування системою захисту.

Політика ІБ оформляється у вигляді задокументованих вимог на інформаційну систему. Документи зазвичай поділяють за рівнями деталізації процесу захисту. Документи верхнього рівня політики ІБ відображають позицію організації до діяльності в галузі захисту інформації, її прагнення відповідати державним, міжнародним вимогам і стандартам у цій галузі. Подібні документи можуть називатися «Концепція ІБ», «Регламент управління ІБ», «Політика ІБ», «Технічний стандарт ІБ» тощо. Область поширення документів верхнього рівня зазвичай не обмежується, проте дані документи можуть випускатися і в двох редакціях − для зовнішнього і внутрішнього використання [1, 2].

Організаційний захист об'єктів інформаційних систем (ІС) – це регламентація виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз [1].

До основних організаційних заходів належать [1, 2]:

- організація режиму і охорони. Їх мета – виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб;
- організація роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;
- організація роботи з документами та документованою інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;
- організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;
- організація роботи з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту;
- організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв.

Засоби захисту інформації поділяються на: засоби захисту від несанкціонованого доступу (засоби авторизації, мандатне управління доступом, виборче управління доступом, управління доступом на основі ролей, аудит); системи аналізу та моделювання інформаційних потоків (CASE-системи); системи моніторингу мереж (системи виявлення й запобігання вторгнень (IDS / IPS), системи запобігання витоків конфіденційної інформації (DLP-системи); аналізатори протоколів; антивірусні засоби; міжмережеві екрани; криптографічні засоби (шифрування, цифровий підпис); системи резервування; системи безперебійного живлення; системи аутентифікації на основі пароля, ключа доступу (фізичного або електронного); біометричних даних; засоби запобігання злому корпусів і крадіжок устаткування; засоби контролю та управління доступом в приміщення; інструментальні засоби аналізу систем захисту [2].

Для забезпечення ІБ та керування інцидентами безпеки використовують SIEM-системи (Security Information and Event Management). Абревіатура SIEM означає «Система збору та кореляції подій». Як можна судити з назви, самі по собі такі системи не здатні що-небудь запобігати або захищати. Їх завдання в іншому – аналізувати інформацію, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, міжмережеві екрани, операційні системи серверів. SIEM-системи представлені додатками, приладами і послугами. SIEM-система моніторингу дозволяє звести всі події та інциденти ІБ в єдиній структурі, виконує інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи щодо ІБ мереж [1, 3, 4]. Крім цього, система моніторингу ІБ виконує реєстрацію та зберігання всіх інцидентів ІБ, що робить можливим використання отриманого матеріалу в якості доказового при виконанні розслідувань інцидентів та в судочинстві [4]. Робота цієї системи дозволяє побачити більш повну картину активності мережі і інцидентів ІБ. Але разом з тим, цю систему використовують як додатковий спосіб захисту від цілеспрямованих атак на мережу. SIEM-система повинна збирати, аналізувати, моніторити і представляти інформацію із мережевих приладів і приладів безпеки.

Функції SIEM-системи спрямовані на моніторинг основних подій і станів інформаційної безпеки всередині компанії та її діяльності. Основними функціями можна назвати [4]:

- моніторинг автентифікації та знаходження компроментуючих аккаунтів користувачів мережі та адміністраторів;

- моніторинг випадків зараження мереж;
- моніторинг підозрілого вихідного трафіку мереж і передання по мережі даних с використанням журналів веб-проксі;
- відстеження системи змін і інших адміністративних дій у внутрішніх мережах на їх відповідність дозволеного протоколу даних компанії;
- моніторинг атак на веб-додатки шляхом аналізу різних звітів;
- відстеження крадіжок даних та інших підозрілих зовнішніх підключень.

Слід приділити особливу увагу налаштуванню SIEM під клієнта, його інфраструктуру і системи безпеки. Правильно налаштовані правила використання системи дозволять спеціалісту аналізувати дійсно важливі повідомлення про інциденти порушення ІБ, фільтруючи зайві дані [3].

SIEM-системи використовують інформацію з таких джерел, як [4]:

- системи автентифікації і системи контролю і управління доступом (Access Control);
- антивірусні засоби;
- міжмережеві екрани; системи виявлення / запобігання вторгнень;
- системи проксінг доступу в інтернет і веб-фільтрації; активні мережеві пристрої;
- системні журнали подій ІБ серверів і робочих станцій користувачів;
- журнали аудиту систем управління базами даних;
- ключові корпоративні ресурси: поштові сервери, файлообмінні сервери, CRM- і ERP-системи;
- інші бізнес-додатки відповідно до вимог ІБ компаній і стандартів.

Типове рішення SIEM-системи включає в себе кілька функціональних компонентів, які зображені на Рис. 1.: агенти, що встановлюються на інформаційну систему, яка моніториться (актуально для операційних систем; агент являє собою резидентну програму (сервіс, демон, служба), яка локально збирає журнали подій і по можливості передає їх на сервер); колектори на агентах, які, по суті, являють собою модулі (бібліотеки) для розуміння конкретного журналу подій або системи; сервери-колектори, призначені для попередньої акумуляції подій від безлічі джерел; сервер-корелятор, що відповідає за збір інформації від колекторів і агентів і обробку за правилами і алгоритмами кореляції; сервер баз даних і сховища, який відповідає за зберігання журналів подій [4].

Рис. 1. Основні компоненти SIEM

Функціонування SIEM-системи доцільно деталізувати на рівні: збір лог-файлів і формування необхідних даних від різних джерел; нормалізація даних, яка полягає у приведенні подій з однаковим змістом до загального формату; кореляція подій системи, важливих для забезпечення безпеки, шляхом знаходження зв'язків між ними, наприклад, підбір паролів, зараження шкідливим кодом, аномальна активність в системі, зміна критичних

параметрів системи тощо.; організація зберігання лог-файлів; реагування на інциденти, в тому числі повідомлення про важливі події для інформаційної безпеки; візуалізація інцидентів, формування звітних документів. До типових структурних компонентів відносяться: міжмережевий екран; поштові послуги; бази даних; система виявлення вразливостей; антивірусний захист; локальний портал; файловий сервер [3, 5]

Структурно-функціональна модель системи захисту інформації (СЗІ) включає в себе перелік структурних компонентів обладнання, а також їх функціональні зв'язки і можливості при вирішенні завдання аналізу і захисту інформації (Рис. 2).

Рис. 2. Структурно-функціональна модель SIEM-системи

Отриману інформацію SIEM аналізує за допомогою правил, що містять набір умов, тригерів, лічильників і сценаріїв дій у відповідь (в сукупності складових Use Cases). SIEM не протидіє зловмисним діям порушників, однак рішення дозволяє отримати найбільш повне уявлення про виникаючі події безпеки [3, 5].

Великі підприємства, холдинги, мульти та транснаціональні компанії різних галузей – основна категорія споживачів SIEM-систем. SIEM дозволяють виявити порушення безпеки серед величезної кількості подій і оперативно відреагувати на виявлені проблеми. Крім того, SIEM-системи при необхідності беруть участь в проведенні аудитів відповідності. Все більша увага приділяється дрібним постачальникам, оскільки організації малого і середнього бізнесу шукають послуги або варіанти надання SIEM для скорочення внутрішніх ресурсів і витрат, необхідних для дотримання вимог безпеки, використовують послуги аутсорсингу [3, 5].

Сьогодні світовий ринок SIEM можна назвати зрілим і конкурентоспроможним. Постачальники в змозі задовольнити основні вимоги будь-якого клієнта, проте залишаються проблеми, пов’язані з виявленням цілеспрямованих атак і порушень в сфері інформаційної безпеки. Ситуація може бути поліпшена завдяки додатковій розвідці загроз, профілізації поведінки користувачів і додатків, ефективній аналітиці. На даний момент спостерігається активне впровадження поведінкової аналітики користувачів і сутностей (User and Entity Behavior Analytics, UEBA), що позиціонується постачальниками як доповнення до SIEM, що володіє більш високою точністю виявлення цілеспрямованих атак [3, 4].

Серед світових лідерів-постачальників SIEM систем можна назвати такі як: SolarWinds Inc. – американська компанія, яка розробляє програмне забезпечення для бізнесу, яке допомагає керувати їх мережами, системами та інфраструктурою інформаційних технологій. Netwrix – це приватна компанія, що займається інформаційною безпекою, яка дає можливість фахівцям з інформаційної безпеки та управління відновлювати контроль над чутливими, регульованими та критично важливими для бізнесу даними, незалежно від місця їх проживання. Rapid7 – лідер в розробці рішення для управління уявленнями і тестування на просування. Допомога полягає в повному представленні безпеки інформаційної інфраструктури [3, 5].

Одними з найбільш популярними SIEM-систем в Україні на теперішній час є [5]:

- QRadar Security Intelligence Platform (виробника IBM), основними перевагами є єдина платформа для всіх дій, які виконуються; гнучка архітектура; велика кількість

безкоштовних додатків, контенту і модулів. Широко застосовується до таких видів діяльності: силові структури, банківський сектор, державні організації, торговельно-комерційні підприємства;

- McAfee (від виробника ESM), основні переваги це великий обхват промислових систем управління; інтеграція зі сторонніми технологіями; постійне джерело оновлення даних. Зазначені системи дозволяють в режимі реального часу отримувати події інформаційної безпеки, аналізувати їх та реагувати на виявлені загрози, інциденти та порушення політик інформаційної безпеки;
- HP ArcSight, основні переваги це повний набір можливостей, які дають можливість використання всіх функцій системи; проведення різноманітних аналіз; наявність бази знань загроз; наявність правил і додаткових продуктів. Володіючи розширеними можливостями збагачення даних, комплексна SIEM-платформа ArcSight ESM поєднує в собі функції виявлення і аналізу загроз у реальному часі, управління процесами безпеки і забезпечення відповідності нормативним вимогам. ArcSight ESM виявляє ознаки виникнення інцидентів в реальному часі, дозволяючи швидше на них реагувати. ArcSight ESM виявляє ознаки виникнення інцидентів в реальному часі, дозволяючи швидше на них реагувати. ArcSight ESM покликана стати основою центра моніторингу інформаційної безпеки (SOC).

Висновки. Отже, ІБ сучасних підприємств та бізнес-структур є одним з найважливіших компонентів ІБ, на якому б рівні вона не розглядалась – національному, галузевому, корпоративному або персональному. У сфері забезпечення ІБ систем важливі не тільки окремі рішення, а й механізми генерації нових рішень, що дозволяють працювати і розвиватися в темпі технічного прогресу. Наявність засобів захисту інформації не є гарантією захисту всіх корпоративних ресурсів. Для забезпечення оптимального рівня захисту необхідна система моніторингу ІБ підприємства, якими є SIEM-системи, що спрямовані на моніторинг основних подій і інцидентів ІБ всередині компанії та її діяльності. В умовах сьогодення, сучасні технології програмування інформаційних систем не дозволяють створювати безпомилкові програми, що не підтримує швидкий розвиток засобів забезпечення ІБ. Важливо починати з того, що необхідно створювати надійні системи ІБ із залученням підозрілих компонентів (програм). Це стає цілком можливим, але потребує дотримання певних принципів і контролю за станом захищеності протягом усього життєвого циклу інформаційної системи.

Список використаних джерел

1. Хорошко В.А., Методи і інструмети захисту інформації. / Хорошко В.А., Чекатков А.М. // К.: Юниор, 2003. – С. 504.
2. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – Харків: ХНУРЕ, 2019. - С. 104–105.
3. Моніторинг інформаційної безпеки (SIEM). \\ Режим доступу: https://www.snt.ua/portfolio/it-resheniya/informacionnaya-bezopasnost/monitoring-informacionnoj-bezopasnosti-siem (останнє звернення: 19.03.2023р).
4. Столова, О. В. Методика порівняння ефективності сучасних SIEM-систем / О. В. Столова // XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 25-27 травня 2017 року, м. Київ. – Київ : ВПІ ВПК «ПОЛІТЕХНІКА», 2017. – С. 163-164.
5. Drew Robb, Top SIEM Products [Електронний ресурс]. \\ Режим доступу: https://www.esecurityplanet.com/products/top-siem-products.html (останнє звернення: 19.03.2023р).

Робота виконана під науковим керівництвом к.т.н., доцента
ЗВЄРЄВА В.П.

ПІДХОДИ ДО РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ UNIVERSITY DORM CAMPUS

УДОВИЦЯ О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуті питання розробки програмної платформи University Dorm Campus, як системи управління студентським житлом, описані основні компоненти системи, а саме управління проживанням студентів у гуртожитку, включаючи управління платежами, ремонтом та обслуговуванням, безпекою, спільнотою та комунікацією.

The article discusses the issues of developing the University Dorm Campus software platform as a student housing management system. The main components of the system are described, including the management of students' stay in the dormitory, which includes payment management, repair and maintenance management, security, community and communication

Актуальність. Орієнтоване на користувача проектування University Dorm Campus (UCD) і гнучка методологія розробки є двома важливими підходами до розробки програмного забезпечення, які можна застосувати до проектування та розробки програмної платформи університетського гуртожитку.

Дизайн, орієнтований на користувача, — це підхід до розробки програмного забезпечення, який орієнтований на потреби та цілі користувачів. У контексті програмної платформи кампусу університетського гуртожитку це означає розробку платформи з урахуванням потреб і переваг студентів, адміністраторів та інших зацікавлених сторін. UCD передбачає проведення дослідження користувачів, щоб зрозуміти потреби, цілі та проблемні точки цільових користувачів, а потім ітераційне проектування та тестування програмного забезпечення, щоб переконатися, що воно відповідає цим потребам.

Гнучка розробка – це гнучкий і повторюваний підхід до розробки програмного забезпечення, який наголошує на співпраці, швидкому створенні прототипів і безперервній доставці. У контексті програмної платформи університетського гуртожитку це означає розробку платформи невеликими поетапними етапами з регулярним тестуванням і відгуками від користувачів. Гнучка розробка включає розбиття процесу розробки на менші, більш керовані етапи, а потім визначення пріоритетів і планування завдань на основі відгуків користувачів і мінливих вимог.

Поєднання дизайну, орієнтованого на користувача, і гнучких методологій розробки може допомогти гарантувати, що програмна платформа кампусу університетського гуртожитку розроблена з урахуванням потреб і цілей користувачів і розробляється ефективно та результативно. Залучаючи користувачів протягом усього процесу розробки, платформу можна тестувати та вдосконалювати ітеративно, гарантуючи, що вона відповідає потребам і вподобанням користувачів у міру її розвитку.

Метою статті є опис підходів до розробки програмного забезпечення для університетських гуртожитків та аналізі їх ефективності для досягнення більш високого рівня забезпечення комфорту та безпеки студентів під час їх перебування в гуртожитках.

Об'єктом дослідження є процес розробки програмного забезпечення для університетських гуртожитків.

Предметом дослідження є різні підходи до розробки програмного забезпечення університетських гуртожитків, їх характеристики та ефективність у досягненні мети забезпечення комфорту та безпеки студентів у гуртожитках.

Аналіз попередніх досліджень Одне дослідження, проведене Гуптою та Агарвалом (2020), показало, що програмні платформи кампусу гуртожитків можуть підвищити рівень задоволеності та залучення студентів. Надаючи студентам централізовану платформу для

інформації про житло, події та спілкування, студенти можуть легко отримати доступ до важливої інформації, спілкуватися зі своїми однолітками та брати участь у заходах гуртожитку.

Інше дослідження, проведене Ваном і Джином (2021), виявило, що програмні платформи гуртожитків можуть підвищити ефективність управління університетом. Університети можуть заощадити час і ресурси, оптимізувавши такі завдання з управління житлом, як розподіл кімнат, запити на обслуговування та планування подій. Дослідження також виявило, що програмні платформи гуртожитків можуть підвищити безпеку, дозволяючи університетам контролювати та відстежувати доступ до гуртожитків і заходів.

Виклад основного матеріалу. Програмні платформи університетських гуртожитків – це цифрові рішення, які дозволяють навчальним закладам ефективно керувати повсякденною діяльністю своїх гуртожитків. Ці платформи дозволяють студентам централізовано отримувати доступ до інформації, пов'язаної з житлом, сусідами по кімнаті, приміщеннями, подіями та іншими послугами. У цьому огляді літератури ми обговоримо ключові особливості програмних платформ університетських гуртожитків та їхні переваги для студентів, університетів та інших зацікавлених сторін.

Основні особливості програмних платформ University Dorm Campus складає чотири основні компоненти: підбір сусідів по кімнаті; управління житлом; управління подіями; комунікація; керування платежами. розглянемо їх детально.

Підбір сусідів по кімнаті.

Однією з важливих функцій програмної платформи студентського містечка гуртожитків є інструмент підбору сусідів по кімнаті. Ця функція дозволяє студентам знаходити сумісних сусідів по кімнаті на основі їхніх уподобань та інтересів. Інструменти підбору сусідів по кімнаті часто включають опитування та анкети для оцінки способу життя та звичок студента. Кілька досліджень вивчали ефективність інструментів підбору сусідів по кімнаті для підвищення задоволеності учнів і зменшення конфліктів.

Одне дослідження Рінкуса та Харлоу (2017) показало, що інструменти підбору сусідів по кімнаті можуть покращити якість стосунків із сусідами по кімнаті та зменшити конфлікти. Дослідження показало, що студенти, які користувалися інструментами підбору сусідів по кімнаті, були більш задоволені своїми сусідами по кімнаті та повідомили про менше конфліктів порівняно зі студентами, яким випадково призначали сусідів по кімнаті.

Управління житлом.

Іншою ключовою особливістю програмних платформ гуртожитків є модуль управління житлом. Ця функція дозволяє університетам керувати розподілом житла, зміною кімнат і перевіркою кімнат. Це також дозволяє студентам переглядати свої призначення житла, подавати запити на зміну кімнати та повідомляти про проблеми з обслуговуванням.

Основна мета цієї складової полягає в тому, щоб спростити та забезпечити ефективну організацію житлового простору в кампусі. Для досягнення цієї мети компонент надає такі функції:

1. Реєстрація та адміністрування користувачів: користувачі можуть створювати облікові записи, вводити та змінювати свої персональні дані. Адміністратори житла можуть виконувати функції з контролю доступу та повторення.
2. Бронювання кімнати: Користувачі можуть бронювати кімнати в кампусі відповідно до їх потреб.
3. Управління оплатою: Компонента надає можливість оплати проживання, а також управління платежами.
4. Обслуговування кімнати: Адміністратор може виконувати функції розміщення з управлінням та обслуговуванням кімнати, щоб забезпечити гарні умови для користувачів.
5. Запис пропусків: Користувачі можуть зареєструвати свій в'їзд та виїзд з кампусу.

6. Інформаційні повідомлення: Компонента надає можливість для надсилання інформаційних повідомлень користувачам та адміністраторам кампусу.

Загалом, компонент «Управління житлом» платформи University Dorm Campus дозволяє забезпечити ефективне управління житловим простором у студентському кампусі, забезпечуючи комфортні умови для проживання студентів.

Управління подіями.

Програмні платформи студентського містечка гуртожитків також включають інструменти керування подіями, які дозволяють університетам організовувати та рекламувати події в гуртожитках. Ця функція дозволяє студентам переглядати майбутні події, відповідати на запрошення та отримувати нагадування про події. Кілька досліджень вивчали вплив заходів у гуртожитку на залученість і задоволеність студентів.

Одне дослідження, проведене Норберто та Салвалагліо (2018), виявило, що заходи в гуртожитку можуть підвищити залученість і задоволення студентів. Дослідження виявило, що студенти, які брали участь у заходах у гуртожитку, повідомили про вищий рівень соціальної інтеграції, академічної задоволеності та загальної задоволеності порівняно зі студентами, які не брали участі в заходах у гуртожитку.

Комунікація.

Інструменти комунікації також є важливою особливістю програмних платформ гуртожитків. Ця функція дозволяє студентам спілкуватися один з одним, а також зі своїми постійними радниками (RA) і персоналом університету. Він також надає університетам платформу для надсилання важливих оголошень, сповіщень і сповіщень.

Ефективне спілкування має важливе значення для роботи гуртожитку та задоволеності студентів. Програмні платформи студентського містечка гуртожитку включають комунікаційні засоби, які дозволяють студентам спілкуватися між собою та з персоналом університету. Кілька досліджень вивчали вплив засобів спілкування на задоволеність і залученість студентів.

Одне дослідження Плурда та Ренна (2019) виявило, що інструменти спілкування можуть покращити задоволеність і залученість студентів. Дослідження показало, що студенти, які використовували засоби спілкування для спілкування зі своїми однолітками та співробітниками університету, повідомили про вищий рівень задоволеності та залученості порівняно зі студентами, які не використовували засоби спілкування.

Програмна платформа спільноти та комунікації для гуртожитків складається з таких функцій:

1. Система повідомлень – програмна платформа може допомогти студентам і персоналу гуртожитку взаємодіяти через систему повідомлень. Це може включати повідомлення про надходження пошти, оголошення про події та активності, оголошення про ремонт тощо. Такі повідомлення можуть бути надіслані студентам через мобільний додаток, електронну пошту, SMS-повідомлення тощо.
2. Спільнота – програмна платформа може допомогти студентам створювати та приєднуватися до спільнот, де вони можуть обговорювати інші теми, знати та здобувати допомогу від інших студентів. У спільноті можуть бути створені різні тематичні групи, такі як групи для обговорення активностей, спорту, культурних заходів тощо. У програмній платформі також можуть бути функції для створення подій та запрошення членів спільноти.
3. Запитання та відповіді – програмна платформа має функцію для запитань та відповідей, де студенти можуть поставити питання персоналу гуртожитку та отримувати відповіді від них. Це може бути корисно для отримання інформації про графік роботи, правила гуртожитку, процедури оформлення тощо.
4. Дошка оголошень – програмна платформа має дошку оголошень, де студенти можуть отримувати оновлення та повідомлення від персоналу гуртожитку. Це може включати оголошення про плани ремонту, інформацію про важливі дати

та події, оголошення про вакансії або можливості волонтерства, а також іншу корисну інформацію.

5. Розклади – програмна платформа може мати розклади для різних подій та послуг, таких як години роботи їдальні, розклад занять спортивний зал, розклад транспорту до університету та інше.
6. Замовлення послуг – програмна платформа може мати функції для замовлення різних послуг, таких як замовлення прибирання кімнати, заявки на ремонт чи інші запити до персоналу гуртожитку.

Керування платіжками.

Програмна платформа University Dorm Campus може допомогти гуртожитковому персоналу відстежувати та обробляти різні типи платежів, такі як квартирна плата, комунальні послуги та додаткові послуги, наприклад послуги з пральні або внутрішньогуртожиткової кафетерії.

Програмна платформа керування платежами для гуртожитків має тикі функції:

1. Створення рахунків – програмна платформа може автоматично створювати рахунки для студентів на основі їхніх договорів оренди кімнати. Рахунки можуть бути різними типами платежів, таких як плата за кімнату, комунальні послуги та додаткові послуги.
2. Обробка платежів – програмна платформа може допомогти персоналу гуртожитку обробляти різні типи платежів, такі як готові та безготівкові платежі, онлайн-платежі та платежі з банківських карт.
3. Відстеження платежів – програмна платформа може відстежувати всі платежі, зроблені студентами, та показувати статус кожного платежу. Відстеження платежів може допомогти персоналу гуртожитку легко відслідковувати заборгованість студентів та вирішувати проблеми з платежами вчасно.
4. Генерація звітів – програмна платформа може формувати звіти про платежі, такі як звіти про заборгованість студентів, звіти про витрати на комунальні послуги та інші фінансові зв'язки

Керування ремонтом та обслуговуванням.

Програмна платформа University Dorm Campus може допомогти гуртожитковому персоналу відстежити замовлення на ремонт, провести профілактичний ремонт та забезпечити планову технічну підтримку всього гуртожитку.

Програмна платформа управління ремонтом та обслуговуванням гуртожитків має наступні функції:

1. Планування ремонту - програмна платформа може допомогти персоналу гуртожитку спланувати ремонтні роботи в кімнатах та спільних приміщеннях. Це може включати планування часу та дати ремонтних робіт, визначення потреб у матеріалах та інструментах, а також розподіл завдань між працівниками.
2. Обробка заявок на ремонт - програмна платформа може допомогти студентам відправити заявки на ремонт або послугу до персоналу гуртожитку. Після отримання заявки програмна платформа може автоматично створити ремонтне замовлення та надіслати його відповідному працівнику.
3. Стеження за станом ремонту - програмна платформа може відстежувати стан ремонтних замовлень та показувати, на якому етапі знаходиться кожне замовлення. Це дозволяє персоналу гуртожитку відстежувати стан ремонтів та забезпечити їх виконання вчасно.
4. Інвентаризація - програмна платформа може допомогти персоналу гуртожитку відстежувати та контролювати запаси матеріалів та інструментів для ремонту. Це може допомогти гарантувати кількість матеріалів та інструментів для виконання ремонтних робіт.
5. Генерація звіту – формування звітів про проведення ремонтних робіт

Керування безпекою – програмна платформа може допомогти гуртожитковому персоналу відстежувати безпеку в гуртожитку, включаючи контроль доступу, моніторинг безпеки та запобігання порушенню правил.

Програмна платформа керування безпекою для гуртожитків має такі функції:

1. Моніторинг доступу - програмна платформа може допомогти персоналу гуртожитку відслідковувати доступ студентів до різних зон гуртожитку, включаючи вхідні двері, спа, спільні приміщення тощо. Це може забезпечити безпеку для студентів, забезпечуючи, що небажані особи не мають доступу до зони, де вони не повинні перебувати.
2. Система відеоспостереження - програмна платформа може допомогти персоналу гуртожитку встановити та керувати системою відеоспостереження в гуртожитку. Це може забезпечити високий рівень безпеки для студентів, забезпечуючи, що будь-які небажані події можуть бути відстежені та зафіксовані.
3. Попередження про небезпеку - програмна платформа може допомогти персоналу гуртожитку вивести студентів про небезпеку, яка може виникнути в гуртожитку. Це може включати попередження про пожежі, повені, насильство, крадіжки тощо. Такі повідомлення можуть бути надіслані студентам через мобільний додаток, електронну пошту, SMS-повідомлення тощо

Узагальнюючи, програмна платформа University Dorm Campus надає студентам різні корисні функції для управління їхнім проживанням у гуртожитку, включаючи управління платежами, ремонтом та обслуговуванням, безпекою, спільнотою та комунікацією. Ці функції можуть забезпечити студентам зручність та ефективність в їхньому повсюдному житті, а також зменшити навантаження на персональну гуртожитку.

Переваги програмних платформ University Dorm Campus:

- Покращений досвід студентів: програмні платформи кампусу гуртожитку університету покращують досвід студентів, надаючи централізоване місце для інформації про житло, події та спілкування. Це дозволяє студентам легко отримувати доступ до інформації, спілкуватися зі своїми однолітками та співробітниками університету та брати участь у заходах гуртожитку.
- Підвищення ефективності: програмні платформи кампусу гуртожитку спрощують завдання управління житлом, наприклад розподіл кімнат і запити на технічне обслуговування, що призводить до підвищення ефективності для університетів і персоналу.
- Покращена безпека та безпека: програмні платформи гуртожитків також підвищують безпеку, дозволяючи університетам контролювати та відстежувати, хто має доступ до гуртожитків та подій.
- Збільшення залучення студентів: програмні платформи студентського містечка гуртожитків сприяють залученню студентів, надаючи студентам можливість спілкуватися один з одним і брати участь у заходах гуртожитку. Це призводить до більш активної та залученої студентської спільноти.

На ринку є кілька типів програмних платформ університетських гуртожитків, включаючи системи управління студентським житлом, платформи для спілкування та співпраці, системи безпеки та безпеки, а також віртуальні тури та орієнтації.

Системи управління студентським житлом надають університетам комплексне рішення для управління студентським житлом, включаючи розподіл кімнат, логістику вселення та виїзду, а також запити на обслуговування. Ці системи також надають студентам онлайн-доступ до інформації про житло, такої як орендна плата, переваги сусідів по кімнаті та житлова політика.

Платформи для спілкування та співпраці дозволяють студентам спілкуватися один з одним та з університетським персоналом через різні канали, такі як обмін повідомленнями, форуми та соціальні мережі. Ці платформи також дозволяють легко планувати зустрічі та події

та забезпечують централізоване розташування для обміну важливими документами та оголошеннями.

Системи безпеки та безпеки використовують передові технології, такі як відеоспостереження, контроль доступу та системи оповіщення про надзвичайні ситуації, щоб забезпечити безпеку студентів і персоналу в кампусі. Ці системи також забезпечують моніторинг у реальному часі та можливості звітування для команд безпеки кампусу.

Віртуальні тури та орієнтації пропонують майбутнім і майбутнім студентам віртуальний досвід кампусу, включаючи гуртожиток та інші об'єкти. Ці платформи дозволяють студентам досліджувати кампус, не виходячи з власного дому, і дають їм змогу краще зрозуміти середовище та культуру кампусу.

Переваги та недоліки:

- Програмні платформи студентського містечка університетського гуртожитку пропонують кілька переваг, зокрема покращене спілкування та співпрацю між студентами та персоналом, покращену безпеку та спрощені адміністративні процеси. Ці платформи також сприяють залученню студентів і надають студентам більш зручний і ефективний спосіб доступу до ресурсів кампусу.
- Однак ці платформи також мають деякі недоліки. Наприклад, деякі учні можуть віддавати перевагу очній взаємодії над онлайн-спілкуванням, і залежність від технологій може створювати додаткові перешкоди для студентів, які не мають доступу до необхідних пристроїв або підключення до Інтернету.

Вплив на університетські містечка:

- Програмні платформи кампусу гуртожитку університету мали значний вплив на життя кампусу. Ці платформи покращили загальний досвід студентів, від процесу подачі заявки до дня заїзду та далі. Вони також допомогли університетам краще керувати інвентарем житла та забезпечити безпеку своїх студентів.
- Крім того, ці платформи надали університетам цінні дані, такі як показники залученості студентів і рівень заповнюваності, які можуть стати основою для прийняття стратегічних рішень і допомогти оптимізувати роботу кампусу.

Висновок. Програмні платформи кампусу гуртожитку університету стали основними інструментами для сучасних університетів. Вони пропонують низку функцій і переваг, які покращують залучення студентів, безпеку та ефективність навчання та проживання.

Хоча ці платформи мають певні недоліки, загальний вплив був позитивним, і університети, які прийняли ці технології, краще оснащені для задоволення потреб своїх студентів і співробітників. У той час як університети продовжують використовувати цифрові рішення для управління діяльністю своїх студентських містечок, програмні платформи студентських містечок гуртожитків продовжуватимуть відігравати важливу роль у забезпеченні студентів безпечним, зручним і привабливим життям.

Список використаних джерел

1. С. О. Цибульник, К. С. Барандич. Технології розроблення програмного забезпечення : Підручник. – Київ; КПІ ім. Ігоря Сікорського 2022, – 270 с.
2. Роберт С. Мартін. Чистий код: : створення, аналіз і рефакторинг. – Харків.: Книжковий дім, 2022. – 464 с.

Робота виконана під науковим керівництвом к.т.н., доцента
РЗАЄВОЇ С.Л.

АНАЛІЗ ЗАХИСТУ ВИБОРЧОЇ СИСТЕМИ: ОСНОВНІ ВРАЗЛИВОСТІ ТА РИЗИКИ

ФЕСЮК А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У цій статті проведено аналіз захисту виборчої системи з метою визначення основних вразливостей та ризиків, пов'язаних з її функціонуванням. Розглянуто різні аспекти безпеки виборів, включаючи кібербезпеку, захист від зловживань та маніпуляцій з результатами голосування. В результаті дослідження встановлено, що виборча система є вразливою до різноманітних атак, і необхідно приділяти більше уваги заходам забезпечення її безпеки.

This article analyzes the security of the electoral system in order to identify the main vulnerabilities and risks associated with its operation. Various aspects of election security are considered, including cybersecurity, protection against abuse, and manipulation of voting results. As a result of the study, it was found that the electoral system is vulnerable to various attacks and that more attention needs to be paid to measures to ensure its security.

Актуальність. В сучасному світі, коли більшість політичних процесів відбуваються через вибори, безпека виборчих систем є критично важливою. Адже злочинці та зловживання можуть стати загрозою для цих систем.

Виборчі системи є одними з найважливіших елементів політичної стабільності та демократії в будь-якій цивілізованій країні, в тому числі, в Україні. Ці системи мають на меті забезпечити чесні та вільні вибори шляхом забезпечення безпеки голосування та збору голосів. Однак, в зв'язку зі зростаючим використанням технологій у виборчих системах, з'являється більше можливостей для порушень безпеки та злочинних дій, які можуть підривати довіру громадян до виборчої системи та її результатів.

Ця стаття присвячена аналізу основних вразливостей та ризиків, пов'язаних з захистом виборчої системи, з метою забезпечення надійного та безпечного виборчого процесу.

Метою статті є розкриття основних вразливостей та ризиків, що відносяться до захисту виборчої системи, а також розгляд можливих заходів щодо забезпечення безпеки та надійності виборчих процесів.

Об'єктом дослідження є виборча система та її компоненти, які відповідають за захист від можливих загроз та атак.

Предметом дослідження є основні вразливості та ризики, що можуть знайти вираження у виборчій системі, а також способи забезпечення безпеки та надійності виборчого процесу. Дослідження включає аналіз загроз, які можуть виникнути від різних ворогів, таких як хакери, кіберзлочинці тощо, а також оцінку ризиків, які вони можуть створити для виборчої системи.

Аналіз попередніх досліджень. Попередні дослідження в галузі захисту виборчих систем науковцями: В. Венгер, М. Ільницький, О. Токар-Остапенко, І. Павленко, Г. Задорожня, О. Ільницький - вказують на те, що технічні та організаційні вразливості можуть призвести до порушення конфіденційності, цілісності та доступності виборчих даних. Ці вразливості можуть бути використані для маніпулювання результатами виборів та злочинних дій, таких як крадіжка особистої інформації виборців тощо.

Огляд заходів забезпечення безпеки виборчих систем показує, що технічні, організаційні та юридичні заходи можуть бути використані для забезпечення безпеки виборчих систем. Такі заходи включають аудит виборчих систем, використання шифрування та контроль доступу до виборчих даних.

Виклад основного матеріалу. Якщо погянути на систему в цілому, то електронна виборча система - це система, яка використовується для збору та обробки голосів на виборах, за допомогою електронних пристроїв. Принцип роботи електронної виборчої системи полягає в наступних етапах:

- Реєстрація виборців: відбувається перед початком виборів. Виборці реєструються у виборчій системі, де їхні особисті дані перевіряються та зберігаються в базі даних.
- Голосування: виборці голосують за допомогою електронних пристроїв, які можуть бути різних типів - наприклад, комп'ютери або спеціальні термінали. Зазвичай виборці отримують картки або ключі для входу до системи та голосують, натискаючи на кнопки на екрані пристрою.
- Обробка голосів: виборча система автоматично підраховує голоси та зберігає їх в електронній формі в базі даних. Зазвичай це здійснюється за допомогою спеціального програмного забезпечення, яке встановлене на електронних пристроях. Результати голосування можуть бути показані на екрані пристрою або надруковані.
- Перевірка результатів: результати голосування можуть бути перевірені за допомогою виборчого комітету або незалежної аудиторської фірми, яка перевірить, чи були зібрані та оброблені всі голоси правильно.

Електронні виборчі системи мають свої переваги та недоліки. Основною перевагою є швидкість та точність обробки голосів, що дозволяє оголошувати результати виборів набагато швидше, ніж у випадку з традиційними паперовими голосувальними бюлетенями. Також електронні виборчі системи можуть бути менш витратними та екологічно чистими, тому що не потребують великої кількості паперус на бюлетені для голосування. [1]

Однак, електронні виборчі системи мають свої недоліки, зокрема, можуть бути вразливими до кібератак та викрадення даних, що може призвести до порушення виборчого процесу та несправедливого розподілу голосів. Також можуть виникати проблеми зі стабільністю системи та несправностями обладнання. Тому важливо використовувати ефективні методи захисту, а також проводити ретельний аудит електронної виборчої системи, щоб забезпечити її безпеку та надійність.

Виборчі системи можуть бути вразливі як через технічні проблеми, так і через людські помилки. Основні вразливості виборчих систем можуть бути наступними:

Технічні вразливості:

- Хакерські атаки - виборчі системи можуть піддаватися хакерським атакам, які можуть привести до порушення або зміни результатів голосування. Хакерські атаки можуть бути проведені через інтернет, на місці або через підключення до мережі виборчої системи.
- Віруси та зловмисний код - виборчі системи можуть бути вражені вірусними атаками та упровадженню зловмисного коду, який може порушити результати голосування або змінити їх.
- Несправність обладнання - несправність обладнання може призвести до втрати даних або знищення їх.
- Невідповідність стандартам безпеки - виборчі системи можуть піддаютися атакам через невідповідність стандартам безпеки.

Людські вразливості:

- Соціальна інженерія - атаки соціальної інженерії можуть бути використані для впливу на результати голосування шляхом зміни волевиявлення виборців або завдання іншої шкоди.
- Виборче шахрайство - виборче шахрайство може бути використано для впливу на результати голосування, включаючи підроблення голосів, зміну результатів голосування та інші маніпуляції.

- Інші людські помилки - інші людські помилки, такі як помилки введення даних або неправильне використання обладнання, можуть призвести до порушення результатів голосування.

Усі ці вразливості можуть бути небезпечними для правильного проведення голосування та порушити демократичний процес в країні. Нижче наведено деякі заходи, які можуть бути вжиті для зменшення ризиків вразливостей виборчих систем:

- Забезпечення захисту від хакерських атак і вірусних програм шляхом використання найновіших технологій та протоколів безпеки, включаючи шифрування, мережеві заходи безпеки, фірмовий та апаратний захист.
- Використання стійких паролів, двофакторної автентифікації, а також використання CAPTCHA для доступу до системи.
- Забезпечення фізичної безпеки виборчої системи, що включає обмеження доступу до обладнання та забезпечення контролю доступу до серверів та інших пристроїв.
- Проведення регулярних тестів на проникнення для виявлення можливих вразливостей та подальшого вдосконалення системи.
- Забезпечення надійності системи для зберігання та передачі голосів шляхом використання шифрування та інших заходів захисту.
- Навчання персоналу та волонтерів, які займаються обслуговуванням виборчих систем, щоб вони були усвідомлені та обізнані з технічними вразливостями та можливими загрозами виборчого процесу.
- Проведення аудиту результатів голосування для підтвердження їх правильності та уникнення можливих помилок.
- Встановлення та дотримання прозорих та стандартизованих процедур голосування, щоб запобігти можливому виборчому шахрайству та іншим формам маніпуляцій.

Загалом, зменшення вразливостей виборчих систем потребує інтегрованого підходу, що охоплює як технічні, так і людські аспекти. Необхідно забезпечити безпеку системи від зовнішніх і внутрішніх загроз, а також навчити всіх учасників виборчого процесу користуватися системою безпеки. Для цього необхідно вжити заходів на кожному етапі виборчого процесу - від розробки системи до проведення голосування та підрахунку результатів. Тільки в такому разі можна забезпечити довіру до виборчої системи та результатів голосування.

Наприклад, досягнення прозорості та довіри до виборчих систем може бути досягнуто за допомогою наступних заходів:

- Розробка та публікація документів, які описують принципи та процедури роботи виборчих систем, а також їх використання.
- Встановлення міжнародних стандартів та протоколів щодо безпеки та дотримання їх під час проведення виборів.
- Проведення досліджень та тестувань виборчих систем з метою виявлення та усунення можливих вразливостей.
- Публікація результатів голосування у відкритому доступі, що дозволяє громадськості перевіряти та аналізувати їх.
- Визначення відповідальних органів та осіб за безпеку виборчих систем та їх дії в разі виявлення вразливостей.
- Забезпечення навчання всіх учасників.

Ризики, пов'язані з вразливостями виборчих систем, можуть бути дуже серйозними та наслідки від їх реалізації можуть бути дуже шкідливими для виборців, кандидатів та результатів виборів. Давайте розглянемо кожну з цих категорій окремо:

Ризики для виборців:

- Крадіжка особистої інформації (імені, адреси, дати народження) та її використання в шахрайських схемах;
- Можливість втручання у виборчий процес та крадіжки голосів;

- Здійснення атак на виборчі системи з метою впливу на результати виборів;
- Використання соціальної інженерії та масового обману з метою впливу на результати виборів;
- Зниження довіри до виборчих систем та зменшення участі виборців через відчуття небезпеки під час голосування.

Ризики для результатів виборів:

- Можливість зламу виборчої системи та вплив на результати голосування;
- Використання соціальної інженерії та масового обману з метою впливу на результати голосування;
- Недостатня безпека виборчих систем може привести до підозри у фальсифікації результатів та зниження довіри до виборчих процесів;
- Неправильне зберігання та обробка даних може призвести до помилок та змін у результаті голосування;
- Відсутність адекватного контролю та аудиту може спричинити помилки та зловживання.

Загалом, вразливості виборчих систем можуть призвести до підозри у фальсифікації результатів виборів та зниження довіри до демократичного процесу голосування. Це може вплинути на легітимність влади та підірвати демократію. Тому, щоб запобігти цим ризикам, важливо забезпечити безпеку виборчих систем, зберігання та обробку даних, контроль та аудит процесу голосування, а також підвищення культури виборців та кандидатів у питаннях кібербезпеки. [1]

Забезпечення безпеки виборчих систем є дуже важливим завданням, особливо в контексті забезпечення права на вільні та справедливі вибори. З метою забезпечення безпеки виборчих систем застосовуються технічні, організаційні та юридичні заходи:

Технічні заходи:

- Захист від вірусів та зломів: системи повинні бути захищені від вірусів та зломів шляхом встановлення антивірусного програмного забезпечення, застосування програмного забезпечення для виявлення та запобігання злому, і використання захищеного з'єднання виборчого комп’ютерного обладнання.
- Контроль доступу: системи повинні мати ефективні засоби контролю доступу до даних та функцій системи. Наприклад, електронна система може використовувати паролі, біометричні дані або токени безпеки для забезпечення безпеки даних виборчої системи та виборця.
- Контроль та шифрування каналів передачі даних у процесі голосування, автентифікації та зарахування голосу.
- Контроль та створення дублюючих каналів зв’язку у випадку зникнення комутації, інтернету, компрометації вузла передачі чи каналу передачі, для відновлення і продовження роботи електронної виборчої системи.
- Захист від DDoS атак: для запобігання DDoS атак системи повинні мати ефективні засоби захисту, такі як використання спеціального програмного забезпечення або хмарних рішень.

Організаційні заходи:

- Організація навчання та підготовки: працівники, які мають пряме стосування до виборчої системи, повинні проходити регулярні курси навчання та підготовки з питань безпеки виборів.
- Аудит безпеки: системи повинні піддаватися аудиту безпеки для виявлення слабких місць та вразливостей.
- Мають бути описані протоколи прийняття рішень, щодо ситуацій з втручанням у електронну систему голосування, виявлення порушень та способи і засоби їх усунення.

- Захист від внутрішнього злочинця: виборчі системи повинні бути захищені від внутрішніх злочинців, тому необхідно розробити процедури контролю за доступом до системи.

Юридичні заходи, пов'язані з забезпеченням безпеки виборчих систем, включають:

- Законодавче регулювання: український законодавчий акт "Про вибори народних депутатів України" містить вимоги щодо захисту виборчих систем від несанкціонованого доступу та забезпечення захисту виборчих даних від порушень.
- Встановлення відповідальності: відповідальність за порушення безпеки виборчих систем повинна бути встановлена та передбачена згідно з законодавством України.
- Захист персональних даних: повинні бути встановлені правила захисту персональних даних, зібраних в рамках виборчого процесу, від несанкціонованого доступу та використання.
- Міжнародні стандарти: Україна має дотримуватися міжнародних стандартів забезпечення безпеки виборчих систем, таких як Кодекс практики з виборчих процесів у Європі.
- Моніторинг та контроль: урядові та недержавні організації здійснюють моніторинг та контроль за виборчим процесом з метою запобігання можливих порушень. [2]

Висновки. Безпека виборчих систем має бути забезпечена комплексним підходом, що включає технічні, організаційні та юридичні заходи. Дотримання цих заходів забезпечить довіру громадськості до виборчого процесу та збереження демократичних цінностей.

Забезпечення безпеки виборчих систем є надзвичайно важливим завданням для забезпечення демократичного процесу в країні. Огляд літератури показав, що вразливості електронних виборчих систем можуть бути технічними та людськими, а ризики можуть містити загрозу для виборців, кандидатів та результатів виборів. Для захисту виборчих систем можуть бути використані технічні, організаційні та юридичні заходи. Зокрема, до технічних заходів можуть належати захист мережі, захист бази даних, використання шифрування каналів передачі даних, організація контролю доступу до виборчих даних. До організаційних заходів можуть належати навчання та підготовка персоналу з питань кібербезпеки, аудит виборчих систем та підвищення уваги до соціального інжинірингу. До юридичних заходів можуть належати законодавчі акти, які встановлюють вимоги до захисту виборчих систем та кримінальні санкції за порушення цих вимог.

Результати дослідження показують, що захист виборчих систем є важливим завданням для забезпечення демократичного процесу в країні. Заходи забезпечення безпеки повинні бути комплексними та охоплювати як технічні, так і організаційні та юридичні заходи. Підвищення уваги до захисту виборчих систем та навчання персоналу з питань кібербезпеки можуть допомогти зменшити ризики порушення безпеки виборчих систем. Законодавчі акти, які встановлюють вимоги до захисту виборчих систем та кримінальні санкції за їхнє порушення, можуть забезпечити правовий захист для виборців, кандидатів та результатів виборів.

Список використаних джерел

1. Geneva internet voting system // Режим доступу: https://www.coe.int/t/dgap/goodgovernance/activities/e-voting/evoting_documentation/passport_evoting2010.pdf
2. Стогова О.В., Мурач Д.В. Електронне голосування: проблеми та перспективи запровадження // Юридичний науковий електронний журнал. 2021. № 3. С. 38-41. // Режим доступу: https://essuir.sumdu.edu.ua/handle/123456789/86308

Робота виконана під науковим керівництвом, ст. викладача
ШЕСТАКА Я.І.

МЕТОДИ ЗАХИСТУ ЛОКАЛЬНИХ МЕРЕЖ ВІД КІБЕРАТАК

ФІЛАТОВ О., 2м курс ФІТ ДТЕУ
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні методи захисту локальних мереж від кібератак, які пов'язані зі зростанням кіберзлочинності. Описано різні підходи до захисту локальних мереж, такі як використання брандмауерів, вірусних сканерів, систем виявлення вторгнень, їх принцип дій, переваги та недоліки. Доведено комплексний підхід до захисту локальних мереж та зменшення ризику кібератак.

The article examines methods of protecting local area networks from cyberattacks, which are associated with the growth of cybercrime. Specified various approaches to the protection of local area networks, such as firewalls, virus scanners, intrusion detection systems. Described their principles, advantages and disadvantages. A comprehensive approach to protecting local networks and reducing the risk of a cyberattack has been proven.

Актуальність. В сучасну цифрову епоху все більше підприємств, організацій і окремих осіб покладаються на локальні мережі (LAN) для підключення пристроїв і обміну інформацією. Зі збільшенням частоти та складності кібератак захист локальних мереж став критичною проблемою для всіх, хто використовує ці мережі. Локальні мережі можуть бути вразливими до різних типів кібератак, включаючи зараження зловмисним програмним забезпеченням, витік даних і атаки на відмову в обслуговуванні, що може завдати значної фінансової та репутаційної шкоди. Тому розуміння та впровадження ефективних методів захисту від кібератак має вирішальне значення для захисту даних, підтримки безвідмовної роботи локальної мережі.

Кіберзлочинці стають все більш витонченими та використовують різноманітні методи та техніки, щоб отримати доступ до локальних мереж та викрасти конфіденційну інформацію або завдати шкоди підприємств. У зв'язку з цим, питання захисту мереж стає все важливішим для бізнесу та інших підприємств. Важливо мати ефективні методи захисту, які дозволяють попереджувати та виявляти кібератаки, а також зменшувати ризики порушення безпеки мережі.

Метою статті є дослідження методів та стратегій, які можна використовувати для захисту локальних мереж від кібератак та надання практичних рекомендацій з їх застосуванням для різних типів мереж та бізнес-потреб.

Об'єктом дослідження є визначення практичних аспектів використання методів та технологій, таких як вибір та налаштування відповідних захисних засобів, аналіз та ідентифікація загроз безпеці мережі, управління ризиками та розвиток стратегій захисту мережі від кібератак.

Предмет дослідження – локальні мережі, провідні та бездротові мережі, їх характеристики та особливості, що можуть впливати на вибір та застосування певних методів захисту.

Аналіз попередніх досліджень: Закордонні науковці, такі як С. Джаджодія, Р. Пувендран, А. Ставру, А. Р. Прасад, К. Нойман, Л. Чен та інші, присвятили свої дослідження локальним мережам, методам та стратегіям захисту від кібератак.

Виклад основного матеріалу. У наш час кожна комп'ютерна система вразлива до атак, тому підприємствам важливо впровадити надійні заходи безпеки, які можуть захистити їх мережеву систему та ресурси. Щоб протистояти атакам, що походять з мережі або за її межами, адміністратори повинні ретельно вибирати та розгортати відповідні технології безпеки. Оскільки доступна велика кількість технологій безпеки, дуже важливо вибрати та

розгорнути їх у спосіб, який узгоджується із загальними цілями та політикою безпеки підприємства.

Підприємства визначають свої стратегії безпеки на основі своїх бізнес-цілей. Ці стратегії відображаються в політиці безпеки підприємства, яка являє собою набір правил, яких повинні дотримуватися співробітники та користувачі для забезпечення безпеки інформаційних і технологічних ресурсів організації. Згідно із запитом на коментарі (RFC) 2196, політика безпеки – це офіційна заява про правила, які регулюють поведінку людей, які мають доступ до технологій та інформації організації. Політика має чітко визначати вимоги щодо захисту технологій та інформаційних активів підприємства та окреслювати процедури виконання цих вимог.

Перед створенням політики безпеки слід розробити план безпеки. Цей план має визначити, що потрібно захистити та від яких загроз. Проведення аналізу ризиків є поширеним способом досягнення цього. Аналіз ризиків визначить, які дії допустимі, а які ні, і допоможе визначити, як і де будуть вирішуватися питання безпеки. Ефективна політика безпеки має охоплювати різноманітні сфери, включаючи доступ користувачів, віддалений доступ, підзвітність, автентифікацію, обробку інцидентів, доступ до Інтернету, використання електронної пошти, фізичну безпеку, обслуговування та звітування про порушення.

Політика безпеки не повинна бути надто обмежувальною, а натомість сприяти використанню ресурсів, зберігаючи певний рівень обмежень. Як правило, відповідальність за розробку політики безпеки покладається на адміністраторів мережі та вищих менеджерів підприємств.

Оскільки підприємства зазнають частих змін щодо технологій і бізнес-стратегій, ризики для їхніх ресурсів і активів також змінюються з часом. Тому вкрай важливо регулярно переглядати та вносити правки в документи політики безпеки, щоб не відставати від мінливих потреб організації в безпеці.

Сучасні системи мережевого зв'язку та спільного використання вимагають ефективних заходів безпеки, які відповідають загальній політиці безпеки підприємства, щоб захистити її мережеві активи та ресурси. Існує кілька доступних технологій безпеки для побудови системи безпеки, але вибір відповідної технології та визначення її оптимального розміщення в мережі залишається основною проблемою для адміністраторів. Доступні варіанти техніки та їх розміщення в охоронній зоні показанв на Рис. 1 [1].

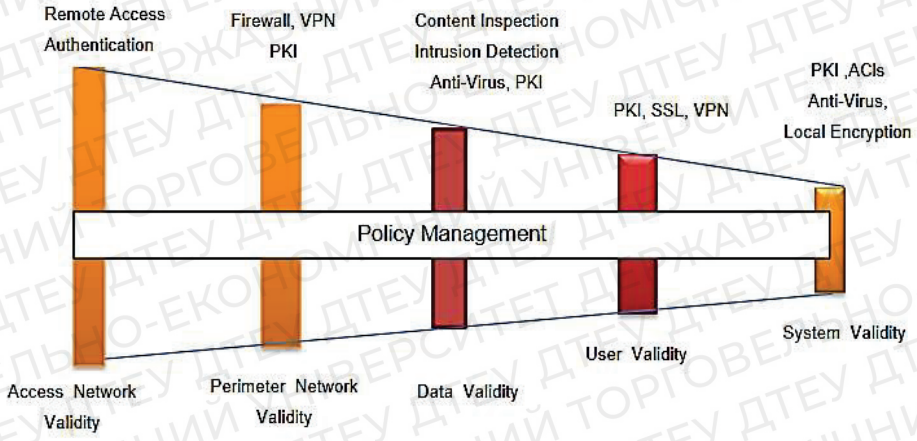


Рис. 1. Розміщення заходів безпеки на охоронній зоні

Захист від неавторизованого віддаленого доступу до мережевого ресурсу досягається за допомогою розгортання технологій автентифікації віддаленого доступу, таких як RADIUS (для захисту комутованих з'єднань), шифрування (для з'єднань по виділеній лінії) та IPsec (для з'єднання через публічну мережу). Щоб захистити пристрої рівня розподілу, зазвичай розгортають один або кілька брандмауерів і зону безпеки.

Після того, як користувач отримав доступ до мережевих ресурсів, важливо перевірити вхідні та вихідні дані на наявність шкідливих об'єктів, таких як віруси, які можуть порушити нормальне функціонування комп'ютерної системи. Одним із способів досягти цього є розгортання інспекції вмісту, виявлення вторгнень, захисту від вірусів або технологій PKI (Pre-shared Key Information). Крім того, важливо захистити систему обслуговування додатків за допомогою списків контролю доступу (ACL), шифрування даних і антивірусних програм.

Безпека Інтернет-протоколу (IPsec) − це структура безпеки, яка базується на відкритому стандарті, розробленому Інженерною робочою групою Інтернету (IETF) для забезпечення безпечного зв'язку через IP-мережі. IPsec вважається найбільш бажаною технологією для захисту наскрізного зв'язку через IP-мережі, оскільки вона забезпечує захист для протоколів і програм вищого рівня. Основною метою IPsec є забезпечення конфіденційності, цілісності та автентичності передачі даних, а також сумісності пристроїв. Для виконання цих завдань IPsec використовує два протоколи, відомі як Authentication Header (AH) і Encapsulating Security Payload (ESP), а також стандартні механізми узгодження ключів і керування.

Протокол заголовка автентифікації (AH) призначений для забезпечення цілісності даних для всієї IP-дейтаграми, що робить його ефективним у запобіганні IP-спуфінгу та викраденню сесії. З іншого боку, протокол Encapsulating Security Payload (ESP) призначений для забезпечення як цілісності даних, так і конфіденційності шляхом шифрування IP-пакетів за допомогою загального секретного ключа.

IPsec включає обмін ключами в Інтернеті (IKE), а також протокол керування ключами асоціації безпеки в Інтернеті (ISAKMP)/Oakley для обробки генерації та керування ключами, а також для встановлення асоціацій безпеки (SA). Асоціація безпеки − це угода між одноранговими пристроями, яка визначає, як відбувається обмін даними між ними. Крім того, IPsec працює в двох режимах: тунельний і транспортний. У режимі тунелю IPsec розгортається між двома шлюзами, а вихідний IP-пакет шифрується та стає корисним навантаженням нового IP-пакета. З іншого боку, у транспортному режимі IPsec використовується між хостами, а вихідна інформація заголовка (джерело та адресат) не шифрується, що робить її видимою для проміжних мережевих пристроїв.

Мережа Ethernet може бути розділена на кілька сегментів IP-маршрутизатором, що призводить до створення окремих широкомовних доменів. Це усуває можливість атак на основі ARP, STP, VLAN і таблиці MAC-адрес між цими сегментами. Однак однакові атаки можуть відбуватися в кожному сегменті, якщо замість кожного комутатора не використовується багатопортовий маршрутизатор.

Розділивши мережу Ethernet на кілька сегментів за допомогою IP-маршрутизатора, трафік між сегментами не можна перехопити або перенаправити для атаки Man-in-the-Middle (MITM). На маршрутизаторі MAC-заголовки Ethernet видаляються, а трафік спрямовується на основі IP-адрес і таблиці IP-адрес маршрутизатора. Протоколи площини керування Ethernet, такі як ARP і STP, блокуються маршрутизатором від проходження між сегментами. Якщо маршрутизатор налаштовано правильно, то він підвищує рівень безпеки, обмежуючи атаки DHCP одним сегментом та ігноруючи повідомлення протоколу маршрутизації від сегментів Ethernet.

Щоб почати атаку, зловмиснику спочатку потрібен доступ. Отже, обмеження доступу до мережі або застосування протоколів автентифікації можуть утримати ненадійних осіб на відстані. Крім того, навіть довіреним особам можна обмежити можливості доступу для подальшого пом'якшення потенційних загроз. Тож можна запропонувати декілька методів для обмеження доступу.

1. Фізичний захист мережі. Мережеве обладнання можна закріпити в шафах і стійках що замикаються, а дроти можна встановити всередині стін, щоб запобігти несанкціонованому доступу. Тим не менш, оскільки доступ є важливим для роботи мережі, фізичний захист має обмежену цінність.

2. Сегментація та VLAN. Обмеження розміру сегмента Ethernet може звести до мінімуму вразливу область для атак. Для досягнення сегментації можна використовувати

пристрій вищого рівня, наприклад маршрутизатор або брандмауер. Крім того, механізм віртуальної локальної мережі IEEE 802.1Q можна використовувати в Ethernet для обмеження трансляцій та іншого трафіку певними сегментами. Мережі VLAN функціонують як логічно окремі об'єкти у фізичній мережі та створюють у ній домени безпеки. Віртуальна локальна мережа це технологія завдяки якій пристрої у локальній мережі розділяються на мережеві сегменти логічно, а не фізично. Сегментація мережі не обмежується фізичним розташуванням її користувачів. Вона базується на таких вимогах користувачів, як групування за: розташуванням, ролями, відділами, використовуваними програмами та використовуваними протоколами. Завдяки віртуальним локальним мережам, користувачі можуть бути організовані у менші робочі групи, кожна зі своїм ідентифікатором, що обмежить трафік кожного користувача до їх відповідної віртуальної локальної мережі та обмежить зв'язок між різними групами. Перевага віртуальної локальної мережі полягає в тому що вона обмежує широкомовний діапазон.

Існує три метода поділу віртуальної локальної мережі:

- Віртуальна локальна мережа що поділена за MAC-адресою − поділ що не потребує повторної конфігурації якщо вузол був переміщений.
- Віртуальна локальна мережа що поділена за IP-адресою − поділ в якому легко додавати вузли до мережі, адже комутатор сам призначить його до віртуальної мережі відповідно до його IP-адресі. Найкращий метод для поділу, але також і складний, бо потребує налаштувань.
- Віртуальна локальна мережа що поділена за протоколом − групує мережеві пристрої на основі протоколів що вони використовують для комунікації.

Комутатори можна налаштувати для призначення VLAN 1 і 2 окремим портам (Рис. 2), використовуючи VLAN 3 як магістраль. Зв'язок між хостами в різних VLAN блокується на рівні 2. Постачальники зазвичай рекомендують VLAN для безпеки, однак правильна конфігурація комутатора має вирішальне значення, оскільки налаштування за замовчуванням часто є небезпечними та можуть спровокувати такі атаки, як VLAN hopping.

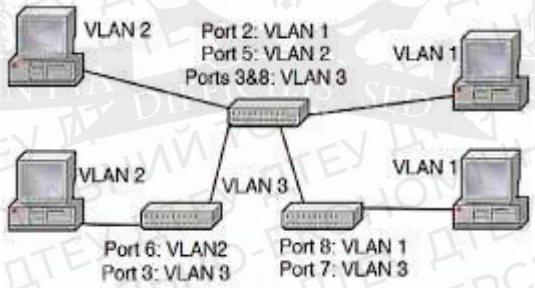


Рис. 2. Сегментація VLAN

3. Індивідуальні VLAN. Подвійне тегування IEEE 802.1ad Q-in-Q або конфігурацію комутатора Private VLAN (PVLAN), надану постачальником, можна використовувати для призначення кожному хосту в Ethernet власної VLAN. Цей підхід особливо корисний у мережах доступу на основі Ethernet, де хости спілкуються лише з одним або кількома іншими вузлами. Q-in-Q розширює простір ідентифікатора VLAN, додаючи інший тег VLAN, у той час як PVLAN використовує конфігурацію комутатора, щоб ізолювати хости та дозволяти їх трафіку проходити лише через один «безладний» порт, підключений до маршрутизатора та Інтернету. За допомогою PVLAN кожен хост може бачити лише себе та хости, підключені до безладного порту, і лише кілька ідентифікаторів VLAN потрібні на магістралях, щоб вказати трафік PVLAN.

4. Контроль доступу на основі автентифікації. Перевірка ідентичності користувача або хоста, який підключається до порту комутатора, є покращенням порівняно з базовим контролем фізичного доступу.

Автентифікація через порт IEEE 802.1X дозволяє використовувати різні облікові дані для автентифікації, наприклад пару імені користувача та пароля, або сертифікат і відповідний йому закритий ключ. Для цього методу потрібне клієнтське програмне забезпечення на кінцевому хості, програмне забезпечення на комутаторі та централізований сервер бази даних автентифікації. Рис. 3 демонструє зв'язок між хостом, комутатором і сервером бази даних автентифікації. Для автентифікації хост зв'язується з комутатором, і комутатор перевіряє облікові дані з бази даних. Розширюваний протокол автентифікації (EAP) використовується 802.1X, який підтримує різні методи та структури автентифікації.

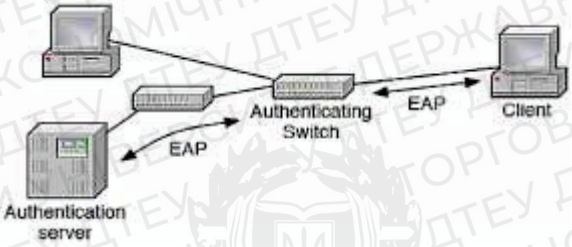


Рис. 3. Сеанс автентифікації 802.1X

На початку сеансу 802.1X автентифікує хост і пов'язує його MAC-адресу з певним портом комутатора. Якщо комутатор виявляє розрив з'єднання, асоціація розривається, і потрібна нова автентифікація. Коли хости безпосередньо підключені до комутатора, який підтримує 802.1X, то він забезпечує захист від атак підробки MAC-адрес і флуд-атак. Однак інші атаки, такі як отруєння ARP, все ще можуть бути можливими.

Зловмисник може втрутитися в концентратор або перемикнутися між комутатором автентифікації та автентифікованим хостом. Після завершення автентифікації автентифікованого хоста може від'єднати без розриву електричного з'єднання з комутатором автентифікації, дозволяючи зловмиснику ввести в мережу інший хост з такою ж MAC-адресою [2]. Щоб створити захищену внутрішню мережу та запобігти атакам імітації комутатора, між комутаторами також можна реалізувати автентифікацію.

5. Списки контролю доступу. Ethernet не має вбудованих списків контролю доступу (ACL), оскільки вони не включені до специфікації Ethernet. Тому постачальники комутаторів самостійно додали різноманітні можливості. У простому кадрі ACL Ethernet доступні атрибути обмежені за MAC-адресою відправника чи одержувача або полем Ethertype. Доступ можна обмежити на основі MAC-адрес, але зазвичай реалізовано декілька ACL для певної служби. Наступні функції можуть бути використані для забезпечення контроля доступу.

Безпека порту − це функція, яка дозволяє адміністраторам мережі обмежувати доступ до порту комутатора, контролюючи кількість MAC-адрес, які можуть до нього підключитися [3]. Це ефективно запобігає атакам переповнення MAC-адрес і несанкціонованому розширенню мережі, запобігаючи додаванню неавторизованих комутаторів. Захист портів надає можливість детального контролю, наприклад блокування нових MAC-адрес, які перевищують ліміт, блокування портів із існуючих MAC-адрес, закінчення терміну дії старих MAC-адрес через певний період або збереження MAC-адрес статичними, доки порт не буде скинуто вручну. Крім того, MAC-адреси можуть бути прив'язані до порту, до якого вони були підключені вперше, що блокує використання тієї ж адреси на інших портах, таким чином запобігаючи мобільності та підробці MAC-адрес.

Захист від шторму пакетів − це функція, яка обмежує кількість кадрів, які можна надіслати через порт комутатора протягом заданого періоду часу. Він призначений для запобігання шторму пакетів, який виникає, коли хост надсилає надмірну кількість кадрів через несправність або навмисну атаку. Якщо обмеження встановлено досить низьким, це також може запобігти атакам затоплення MAC-адрес.

Захист BPDU − це функція, яка запобігає проходженню будь-яких повідомлень STP через порт, і її можна використовувати для визначення порту, який не повинен бути частиною

сітчастої мережі. Водночас захист кореня STP ідентифікує порт, який є частиною мережі STP, але не може стати коренем STP. Ці функції також використовуються для цілей оптимізації продуктивності, наприклад, забезпечення того, що для побудови деревовидної топології мережі використовувалися лише найшвидші зв'язки [4].

6. Захист від перевантаження рівня контролю та управління. Обмеження обсягу трафіку на площинах контролю та управління може допомогти запобігти перевантаженню. Контроль площини керування (CoPP або CPP) досягає цього за допомогою набору фільтрів, які покладаються на методи та адреси обмеження швидкості, щоб уникнути перевантаження функцій площини керування. Фільтри призначені для того, щоб дозволити лише певній кількості пакетів даних рівня контролю та управління досягти центральний процесор (ЦП), а весь інший трафік блокується до того, як він досягне рівня ЦП. Цей підхід допомагає захиститися від навмисних атак, спрямованих на виснаження ЦП, хоча легітимні повідомлення також можуть бути втрачені під час атаки. Фільтри можна налаштувати, щоб дозволити окремо встановлювати різні типи контрольних кадрів.

7. Безпека локальної мережі з централізованим керуванням. Дослідницьке співтовариство запропонувало різні методи збору інформації з локальної мережі та її використання для управління безпекою. Цими методами є:

- SANE – це нова конструкція, яка використовує централізований контролер для хостів для публікації служб і запитів доступу один до одного. Його основна мета полягає в тому, щоб реалізувати орієнтовану на організацію політику безпеки на рівні локальної мережі, і він прагне забезпечити широкий захист для Ethernet.
- Ethane є розширенням підходу SANE, який усуває необхідність встановлення нового програмного забезпечення на хостах. Хоча центральний контролер все ще підтримує політики, але хости все ж повинні бути автентифіковані. Коли ініціюються нові потоки, комутатори Ethane спочатку надсилають їх до контролера, який визначає, авторизувати чи забороняти їх, і відповідно налаштовує комутатор.
- OpenFlow – це дизайн, який базується на ідеях Ethane, вводячи перемикач, який використовує таблиці потоку та зовнішній контролер замість таблиці MAC. Ці таблиці потоку враховують такі атрибути пакетів, як Ethernet, IP і транспортні рівні. Крім того, кадри можуть бути спрямовані на порти або центральний контролер, відокремлюючи запити ARP від іншого трафіку. OpenFlow представляє архітектуру, відому як програмно визначена мережа (SDN), яка відокремлює функції керування від функцій перемикання та реалізує керування лише на початку потоку [4, 5].

Обмеження доступу до цілей для зловмисників досягається за допомогою контролю доступу. Цілі також можна зробити менш доступними шляхом включення функцій безпеки в протоколи.

Одним із рішень забезпечення цілісності та конфіденційності є криптографія. MACsec, стандарт IEEE 802.1AE, що встановлює зашифровані з'єднання між комутаторами та хостами, захищаючи цілісність і конфіденційність переданих даних. Щоб реалізувати MACsec, необхідно встановити програмне забезпечення та конфігурувати автентифікацію для кожного об'єкта мережі. Хоча MACsec використовує інформацію автентифікації 802.1X, він не визначає керування ключами, що залишається на розсуд постачальників.

MACsec ефективно захищає від несанкціонованого доступу до мережі, забезпечуючи конфіденційність і цілісність даних. Однак це не гарантує захисту від авторизованих хостів, які можуть поводитися зловмисно. MACsec забезпечує безпеку лише для зовнішнього периметра, а внутрішні об'єкти залишаються вразливими до атак. Наприклад, авторизований хост може використовувати ARP для захоплення трафіку іншого хоста. Крім того, MACsec не забезпечує захист від DoS-атак і аналіз трафіку.

Архітектура Ethernet вразлива до атак через протокол розпізнавання адрес (ARP). Однак цю вразливість можна усунути, використовуючи інформацію, отриману від стеження за протоколом динамічної конфігурації хоста (DHCP), щоб пов'язати MAC-адреси з відповідними IP-адресами та портами. Тим не менш, відстеження DHCP може мати

обмежений обсяг, оскільки комутатор може не мати видимості розподілу, зробленого для хостів, які не проходять через нього для доступу до сервера DHCP.

Дослідники в основному зосереджуються на рішеннях, заснованих на криптографії, таких як S-ARP, яке містить поле автентифікації в повідомленнях ARP разом із структурою керування ключами, що використовує зв'язування криптографічного простору імен, або [6], що розширює покриття MACsec між кінцевими точками та захист багатоадресної передачі.

Щоб запобігти неправильному використанню вищих функцій комутатора, доступ до комутатора має бути контрольованим. Функції площини керування, які пов'язані з площиною користувача, можна захистити за допомогою методів, розглянутих раніше.

Один із способів захисту функцій площини керування − обмежити їх окремою фізичною або віртуальною мережею керування. Крім того, зашифровані з'єднання часто використовуються для захисту даних керування, при цьому SSH зазвичай використовується для командного рядка та TLS/SSL для веб-інтерфейсів. Механізми автентифікації можуть включати паролі або криптографічні облікові дані.

Моніторинг комутаторів зазвичай здійснюється за допомогою простого протоколу керування мережею (SNMP), який може використовувати або не використовувати захист паролем. Шифрування не підтримується у версії 1 SNMP, і навіть якщо воно доступне у версії 3 і деяких типах версії 2, воно може не використовуватися, коли SNMP використовується виключно для моніторингу.

Протоколи вищого рівня та MACsec зазвичай включають такі механізми, як мітки часу або неповторювані значення (nonces), щоб запобігти атакам відтворення, оскільки сам базовий кадр Ethernet не забезпечує захисту від них.

У попередніх абзацах були описані підходи до безпеки, які є переважно проактивними та самодостатніми, без необхідності втручання людини чи участі зовнішніх систем. Однак активні технології можуть забезпечити додаткову безпеку мережі.

Брандмауери використовуються для обмеження потоку трафіку між різними сегментами мережі, і їх можна розглядати як більш складні версії списків контролю доступу, які включають можливості відстеження стану. Крім того, брандмауери можуть використовувати глибоку перевірку пакетів (DPI) і відтворення сеансу прикладного рівня для забезпечення перевірки. Сучасні брандмауери можуть працювати на всіх мережевих рівнях, роблячи безглуздим ідею «мережевого екрану Ethernet». ACL комутаторів можна використовувати для обмеження трафіку на рівні Ethernet, у той час як стандартні брандмауери можуть контролювати вищі рівні.

Реалізація політики безпеки підприємств значною мірою залежить від брандмауера, який вважається системою або групою систем, що використовуються для контролю мережевого трафіку на основі заздалегідь визначених правил. Діючи як захисний міст, який відокремлює внутрішню мережу від зовнішньої ненадійної мережі, такої як Інтернет, брандмауер функціонує як контрольно-пропускний шлюз, який ретельно перевіряє IP-пакети, щоб визначити, дозволяти чи не пропускати їх на основі попередньо налаштованих правил. Крім того, брандмауер вирішує, яка інформація або служби доступні як зсередини, так і ззовні мережі, і хто має дозвіл на доступ до них.

Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) використовують DPI для виявлення мережевих атак, зазвичай шляхом порівняння мережевого трафіку з бібліотекою відомих сигнатур атак. Ці системи потребують доступу до мережевого трафіку, який можна отримати шляхом розміщення пристрою IDS/IPS безпосередньо між двома кінцевими точками (зазвичай використовується як брандмауер або для посилення брандмауера) або шляхом моніторингу трафіку від комутатора за допомогою функції дублювання портів. Віддзеркалення портів дублює трафік до та з вибраних портів до порту моніторингу, де розташований пристрій IDS/IPS. За потреби можна встановити окрему мережу, щоб пристрої моніторингу були відокремлені від захищеної мережі.

Комутатори мають додаткові можливості, які можуть допомогти у виявленні зловмисної поведінки. Наприклад, сповіщення про MAC-адресу може надсилати

повідомлення перехоплення SNMP, коли хост рухається в мережі. Для цілей системи виявлення вторгнень (IDS) кілька визначень інформаційної бази керування SNMP (MIB) можуть бути цінними, включаючи MIB віддаленого моніторингу мережі (RMON) та її розширення комутатора (SMON). Поряд з пасивним моніторингом для виявлення зловмисної поведінки також можна застосовувати активні заходи. Кадри з очікуваною поведінкою можуть бути введені в мережу та відстежені для виявлення атак ARP-спуфінгу [7].

Ефективне планування, налаштування та адміністрування можуть мати значний вплив на різні аспекти мережі Ethernet. Багато технічних рішень, розглянутих раніше, вимагають постійної конфігурації та коригування для адаптації до змін у топології мережі. Оскільки не існує надійного методу автоматичного розрізнення магістральної мережі від підключень до кінцевих вузлів, адміністратори мережі повинні вручну налаштувати цю інформацію на комутаторах. Розділення управлінської інформації у виділену VLAN та обмеження функціональності рівня керування та потоків даних може підвищити безпеку мережі до рівня, порівнянного з мережею на основі IP-маршрутизатора.

Існує кілька доступних систем керування мережею, які можуть допомогти в налаштуванні комутаторів у мережі. Ці системи підтримують топологію мережі та автоматизують завдання, тим самим зменшуючи помилки. Однак для використання цих систем керування комутатори мають бути сумісні з програмним забезпеченням і налаштовані для спільної роботи.

Висновки. Захист локальної мережі потребує багатостороннього підходу, який передбачає поєднання проактивних і реактивних заходів. Це включає такі методи, як VLAN, ACL, MACsec, DPI, IDS/IPS та активне сканування для виявлення вразливостей. Належні методи адміністрування мережі, такі як відокремлення управлінської інформації до виділеної VLAN та обмеження функціональності рівня керування та потоків даних, також можуть підвищити безпеку. Зрештою, ключем до захисту локальної мережі є постійний моніторинг і оновлення заходів безпеки, щоб не відставати від загроз, що розвиваються. Впроваджуючи комплексну стратегію захисту, мережеві адміністратори можуть значно знизити ризик зламу мережі та несанкціонованого доступу.

Список використаних джерел

1. Fundamentals of Network Security \\ Режим доступу: https://www.theseus.fi/bitstream/handle/10024/61830/Building%20a%20Secure%20Local%20Area%20Network_final%20-%20Copy.pdf?sequence=1 (останнє звернення 18.03.2023р.)
2. Mitigating the threats of rogue machines802.1X or IPsec? \\ Режим доступу: http://technet.microsoft.com/en-us/library/cc512611.aspx (останнє звернення 18.03.2023р.)
3. Safe layer 2 security in-depth \\ Режим доступу: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfbluwp.pdf (останнє звернення 18.03.2023р.)
4. Pushing enterprise security down the network stack \\ Режим доступу http://hdl.handle.net/1853/30782 (Останнє звернення 18.03.2023р.)
5. T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, and S. Shenker, Onix: a distributed control platform for large-scale production networks. – 2010. – с. 1 – 6.
6. K. Wahid, Rethinking the link security approach to manage large scale Ethernet network. – 2010. – с. 5 – 7.
7. N. Hubballi, S. Roopa, R. Ratti, F. A. Barbhuiya, S. Biswas, A. Sur, S. Nandi, V. Ramachandran, An active intrusion detection system for LAN specific attacks. – 2010. – с. 129 – 142.

Робота виконана під науковим керівництвом старшого викладача
КОСТЮК Ю.В.

ОНЛАЙН-СПІЛКУВАННЯ У ЦИФРОВУ ЕПОХУ: ВІД АНАЛІЗУ ПЛАТФОРМ ДО ПОТРЕБИ У СПЕЦІАЛІЗОВАНОМУ РІШЕННІ ДЛЯ ТЕМАТИЧНИХ ВЕЧІРОК

ЦІОМІК І., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглядається різноманітність сучасних платформ для організації онлайн-зустрічей, вказуючи на їх переваги та недоліки. Деякі платформи, зокрема Hopin, Houseparty, Airbnb Online Experiences, Netflix Party, Twitch та YouTube Live, надають користувачам унікальні можливості для інтерактивного спілкування, віртуальних подій та спільного перегляду контенту. Втім, не існує платформи, яка була б спеціалізована на організації тематичних онлайн вечірок. Розробка такої платформи, яка враховує потреби осіб з інвалідністю, може стати відповіддю на зростаючу потребу якісних платформ для онлайн-спілкування.

The article examines the variety of modern platforms for organizing online meetings, highlighting their advantages and disadvantages. Platforms such as Hopin, Houseparty, Airbnb Online Experiences, Netflix Party, Twitch, and YouTube Live offer users unique opportunities for interactive communication, virtual events, and shared content viewing. However, there is no platform specifically designed for thematic online parties. Developing such a platform, which takes into account the needs of people with disabilities, can be an answer to the growing demand for quality online communication platforms.

Актуальність. Зростаюча цифрова трансформація суспільства невблаганно перетворює усі аспекти нашого життя, включаючи спосіб спілкування та розваг. Останні події, пов'язані зі світовою пандемією, ще більше підкреслили необхідність в інноваційних підходах до організації подій та розважальних заходів. У контексті цього варто врахувати й вплив війни, конфліктів та непевностей, які можуть призвести до обмежень у фізичних зустрічах та спілкуванні. Становлення нової реальності, де фізична відстань не заважає спілкуванню, робить платформу для організації та проведення онлайн тематичних вечірок вкрай актуальною.

Умови, змінені пандемією, війною, природними катаклізмами та іншими геополітичними конфліктами, спонукають нас до пошуку нових способів комунікацій та розваг. Важливість такої платформи полягає в тому, що вона не лише забезпечує можливість соціального спілкування, але і дозволяє організувати нові та нетрадиційні й нетипові заходи в онлайн форматі. Вона створює можливість об'єднати людей з різних куточків світу, які мають спільні погляди, цінності, інтереси та хочуть проводити якісно час, спілкуючись разом. Разом з тим, така платформа дає можливість соціалізації людей з особливими потребами.

Різноманітність тематик та креативних концепцій для вечірок додає платформі додатковий рівень привабливості. Вона є місцем для реалізації ідей, віртуального творчого експерименту та незабутнього дозвілля. Крім того, розширені можливості взаємодії в онлайн просторі дозволяють підтримувати постійний контакт з друзями та знайомими, а також знаходити нових друзів, знайомих, бізнес-партнерів тощо, не зважаючи на віддаленість.

Все це робить тему "Платформа для організації та проведення онлайн тематичних вечірок" особливо актуальною у наш час. Вона відповідає потребам сучасного суспільства в інноваційних способах взаємодії, соціального спілкування та розваг, роблячи їх доступними в будь-який час та з будь-якого місця.

Мета дослідження: полягає в розробці та реалізації комплексної онлайн платформи, яка забезпечує організацію та проведення тематичних вечірок в віртуальному середовищі. Головною метою є створення зручного та привабливого інструменту для користувачів, що дозволить їм активно взаємодіяти, спілкуватися та відчувати радість від спільного часу, незалежно від географічного розташування.

Об'єктом дослідження є процеси організації та проведення онлайн тематичних вечірок, а також взаємодія учасників під час таких подій.

Предмет дослідження є розробка та функціонування платформи, що забезпечує можливість організації та участі в онлайн тематичних вечірках.

Виклад основного матеріалу.

Нині, коли технології продовжують швидко розвиватися, віртуальні події стають все більш популярними. Серед великої кількості різних онлайн заходів окрему нішу займають онлайн вечірки. Онлайн вечірки вцілому та тематичні онлайн вечірки зокрема, виконують низку сучасних функцій:

1.Соціальна взаємодія. Онлайн вечірки дозволяють людям зібратися, спілкуватися та провести час разом, навіть якщо вони знаходяться на великій відстані. Це може бути особливо важливим для тих, хто має друзів та рідних у різних частинах світу.

2.Креативність та розвага. Тематичні вечірки дають можливість проявити креативність, обрати певний стиль або тему, підготувати костюми чи декорації.

3.Підтримка певних інтересів. Онлайн вечірки можуть бути спрямовані на певні інтереси, хобі або захоплення. Це дає можливість знайти спільноту людей з спільними інтересами та захопленнями.

4.Доступність. Для людей з певними обмеженнями онлайн вечірки можуть бути особливо важливими, оскільки вони дозволяють взяти участь у соціальних подіях, не залишаючи дім.

5.Безпека і зручність. Онлайн вечірки можуть бути більш зручними та безпечними для деяких людей, особливо у випадках, коли їм потрібно уникати масових зібрань.

6.Подолання географічних обмежень. Онлайн вечірки дають можливість об'єднати людей з різних країн і континентів, не залежно від відстані.

Різноманітні платформи для проведення таких вечірок з'являються на просторах інтернету зі своїми унікальними можливостями та особливостями. Їх можна класифікувати таким чином: комерційні, безкоштовні та частково безкоштовні (у вільному доступі з певними обмеженими функціями); платформи загального призначення для організації онлайн зустрічей та спеціалізовані платформи для онлайн вечірок.

На сьогоднішній день існує безліч платформ, які можна використовувати для проведення онлайн вечірок та подій. У даному розділі буде проведено дефінітивний аналіз деяких найпопулярніших платформ для проведення онлайн зустрічей та організації онлайн вечірок.

Zoom - це ім'я, що стало практично синонімом для відеоконференцій і онлайн спілкування в реальному часі. Ця платформа, яка широко використовувалася під час глобальної пандемії COVID-19, стала також популярним вибором для проведення онлайн вечірок. Завдяки своїм розширеним можливостям, Zoom надає користувачам можливість створювати забавні, інтерактивні івенти, де вони можуть обмінюватися ідеями, грати в ігри та відчувати себе разом, навіть якщо вони фізично знаходяться далеко один від одного.

Переваги Zoom для проведення онлайн вечірок:

Висока якість відео та аудіо: Zoom відомий своєю стабільною роботою і гарною якістю зв'язку.

– Можливість створювати тематичні кімнати: Ви можете створювати різні кімнати для різних активностей під час вечірки.

– Екранний показ та обмін файлами: Це дає можливість демонструвати відео, графіку або інші матеріали для всіх учасників.

– Чат і реакції: Учасники можуть спілкуватися у чаті, відправляти реакції та виражати свої враження під час події.

– Велика кількість учасників: Залежно від обраного плану, Zoom може підтримувати значну кількість учасників на одній зустрічі.

Обмеження Zoom для проведення онлайн вечірок:

– Обмежений доступ до певних функцій у безкоштовному плані: Деякі продвинуті функції можуть бути доступні тільки за плату.

– Потребує встановлення програми або додатку: Учасники можуть потребувати завантажити програму або додаток Zoom, щоб приєднатися до зустрічі.

Висновок: Zoom є надійним і універсальним вибором для проведення різноманітних онлайн вечірок. Його розширені можливості сприяють створенню інтерактивного та захоплюючого досвіду для учасників.

У наступних розділах ми розглянемо інші популярні платформи для проведення онлайн вечірок та їх переваги та обмеження.

Microsoft Teams також підходить для віртуальних зібрань та вечірок. Вона має інтеграцію з іншими інструментами Microsoft та можливості для спільної роботи. При цьому вона має свої переваги та недоліки, які варто враховувати перед вибором цієї платформи.

Переваги:

– Зручна організація зустрічей: Teams має функції для планування та організації відеоконференцій. Є можливість створювати календар події, визначати учасників, встановлювати різні часові зони тощо.

– Поділ на групи (канали): можна створювати різні канали для різних тем або груп людей, що допомагає організовувати вечірку та спілкування більш структуровано.

– Безпека та конфіденційність: Microsoft Teams має високі стандарти безпеки та захисту даних, що може бути важливим, особливо якщо під час вечірки передбачено проведення конфіденційних розмови або подій.

– Microsoft 365 live events дає можливість організувати зустрічі у форматі трансляцій для 10 000 відвідувачів та менше [2].

Недоліки:

– Обмежені можливості для розваг: платформа Microsoft Teams переважно спрямована бізнес-середовище, тому її можливості для розваг, ігор або креативних заходів можуть бути обмеженими порівняно з іншими платформами.

– Складність для незнайомих користувачів: для тих, хто не має досвіду з Microsoft Teams, платформа може здаватися дещо складною та незрозумілою.

– Обмеження у безкоштовній версії: деякі функції та можливості можуть бути доступні лише за плату або в розширеній версії Microsoft Teams [2].

Discord – це безкоштовна комунікаційна програма, яка дозволяє ділитися голосовим, відео- та текстовим чатом із друзями, ігровими спільнотами та розробниками. Discord можна використовувати майже на всіх популярних платформах і пристроях, включаючи Windows, macOS, Linux, iOS, iPadOS, Android, а також через веб-браузери.

Основна мета Discord – спілкування. Кожен може безкоштовно створити сервер Discord використовувати його, щоб зібрати друзів разом у груповому текстовому чи голосовому чаті. Розробники часто використовують Discord як місце для обміну ігровими смаками зі своїми спільнотами.

Переваги:

– Спрямованість на спільноти: Discord розроблений для спільнот, і він має багато функцій, що сприяють взаємодії у спільностях, що робить його добрим варіантом для тематичних вечірок.

– Голосовий чат і тесктовий чат: Discord надає можливість створювати голосові та текстові канали, де учасники можуть спілкуватися під час вечірки.

– Багато можливостей для налаштувань: можна створювати різні канали для різних аспектів вечірки, встановлювати ролі для учасників, обмежувати доступ до певних функцій тощо.

– Віртуальні сервери: Discord надає можливість створювати власні сервери, що може бути корисним для збереження всіх тематичних вечірок та спільнот.

– Багато інтегрованих ігор та додатків: Discord має багато ігор, які можна грати разом з учасниками вечірки, а також інші додатки, які можуть бути використані для розваг.

Недоліки:

– Неспеціалізована платформа: Оскільки Discord спрямований на геймерів, деякі функції, які можуть бути важливими для організації вечірок, можуть бути менше розвиненими порівняно з іншими платформами.

– Інтерфейс Discord не є інтуїтивно зрозумілим для тих, хто раніше не користувався платформою.

– Можливість завантаження вмісту: на платформі може з'являтися несанкціонований або небажаний вміст, який може потребувати уваги та контролю.

Загалом, Discord може бути чудовим варіантом для організації тематичних вечірок, особливо якщо ви бажаєте залучити учасників, які спільно ділять певні інтереси та хочуть взаємодіяти під час вечірки.

Gather.town є інтерактивною платформою, яка дозволяє створювати віртуальні простори для різноманітних зустрічей. Вона відрізняється від традиційних платформ завдяки своєму графічному середовищу та методам взаємодії між учасниками.

Переваги:

– Інтерактивність: можливість для користувачів динамічно взаємодіяти між собою в віртуальному середовищі.

– Спрощене спілкування: автоматичний вхід в аудіо- та відеодзвінки при наближенні до іншого користувача.

– Групові активності: інтеграція групових ігор та інших форм розваг.

– Безпека: можливість створення приватних зон та контролю доступу.

Недоліки:

– Технічні обмеження: Потенційні проблеми для користувачів зі слабким інтернет-з'єднанням або застарілим обладнанням.

– Крива навчання: Для деяких користувачів інтерфейс може здатися складним.

– Вартість: Потенційно висока вартість при великих масштабах або потребах у додаткових функціях.

– Відсутність деяких функцій: Можливе обмеження в функціоналі порівняно з іншими платформами.

– Максимальне обмеження учасників: Обмеження кількості учасників в залежності від пакету послуг [5].

Отже, Gather.town представляє собою унікальний інструмент для організації віртуальних зустрічей, що поєднує в собі інтерактивність та гнучкість. Проте, при його використанні, необхідно враховувати потенційні технічні обмеження та особливості користувачів.

Remo є однією з платформ, яка пропонує інноваційний підхід до організації віртуальних зустрічей та конференцій. Remo створена для підвищення інтерактивності та сприяння ефективності мережевої взаємодії. Ця платформа симулює віртуальне середовище, де користувачі можуть пересуватися між різними «столами», імітуючи реальне життєве спілкування.

Переваги:

– Інтерактивність: платформа дозволяє учасникам вільно переміщуватися між столами та групами, сприяючи природній взаємодії.

– Ефективність для нетворкінгу: особливо корисно для бізнес-зустрічей та конференцій, де важлива можливість нетворкінгу.

– Гнучкість конфігурації: можливість налаштовувати віртуальні простори згідно з потребами заходу.

– Інтегровані інструменти: наявність додаткових інструментів для презентацій, обговорень тощо.

Недоліки:

– Обмеження в учасниках: залежно від пакету, може бути обмеження на максимальну кількість учасників.

– Технічні вимоги: потреба у стабільному інтернет-з'єднанні та сучасному обладнанні для оптимального досвідуК

– Вартість: вартість підписки може бути досить високою для великих масштабів або додаткових функцій [6].

Отже, Remo є високоефективним інструментом для проведення віртуальних зустрічей, особливо в контексті нетворкінгу та бізнес-заходів. Однак важливо враховувати технічні вимоги та потреби користувачів, щоб забезпечити успішний досвід використання платформи.

Висновки. У сучасному цифровому світі існує велика різноманітність платформ для організації та проведення онлайн зустрічей. Кожна платформа має свої унікальні переваги та недоліки, що робить їх ідеально підходящими для різних типів подій.

Платформи, такі як Hopin і Houseparty, надають можливість інтерактивної участі, забезпечуючи як групові, так і індивідуальні взаємодії. Airbnb Online Experiences дозволяє користувачам відкрити для себе унікальні віртуальні заходи, представлені різними культурами з усього світу. Netflix Party і Twitch акцентують увагу на спільному перегляді контенту та грах, в той час як YouTube Live дозволяє користувачам досягти величезної аудиторії завдяки стрімінгу в реальному часі.

Що стосується технічної сторони, багато платформ потребують високоякісного зєднання з Інтернетом та професійного обладнання для оптимального досвіду користувача.

Для організації тематичних онлайн вечірок важливо вибрати платформу, яка найкраще відповідає потребам та очікуванням аудиторії, але дослідження показаи, що наразі не існує спеціалізованої платформи саме для оргаізації тематичних онлайн вечірок.

Розробка платформи для онлайн організації вечірок є відповіддю на зростаючу потребу людей у якісних платформах для онлайн-спілкування. З урахуванням особливостей потреб осіб з інвалідністю, платформа матиме великий потенціал стати популярним та корисним інструментом соціалізації в онлайн просторі.

Список використаних джерел

1. https://zoom.us/pricing
2. https://news.microsoft.com
3. https://meet.google.com/
4. https://store.epicgames.com/en-US/news/what-is-discord-and-what-is-it-used-for
5. https://www.gather.town/
6. https://remo.co/solutions-for-higher-education

Робота виконана під науковим керівництвом канд. пед. наук, доцента
ЖИРОВОЇ Т.О.

ПОБУДОВА МІКРОСЕРВІСІВ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ GO

ЧЕРКАСОВ А., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови мікросервісів за допомогою мови програмування Go. Зазначено переваги використання Go та її екосистеми для побудови відмовостійкої мікросервісної архітектури хмарного середовища. Приведені приклади реалізації мікросервісів на Go.

The article discusses the main principles of building microservices using the Go programming language. The advantages of using Go and its ecosystem for building a resilient microservices architecture in a cloud environment are highlighted. Examples of implementing microservices in Go are provided.

Актуальність. Мікросервісна архітектура стала найбільш популярною архітектурою для побудови програмних систем та компонентів які можуть витримувати високі навантаження на систему, мають переваги у легкості розбудови та масштабування. Мова програмування Go, при побудові мікросервісів, зарекомендувала себе як надійний інструмент, що не дивно з урахуванням мети з якої була створена, а саме для роботи з інформаційними системами різного рівня складності, мережами та інфраструктурою, на заміну мовам програмування C++ та Java.

Метою статті є дослідження особливостей використання мови програмування Go для побудови мікросервісів.

Об'єктом дослідження є розробка мікросервісів за допомогою мови програмування Go.

Предмет дослідження: інформаційні-мікросервісні системи побудовані за допомогою мови програмування Go.

Виклад основного матеріалу. Перш ніж переходити до застосування Go в розробці мікросервісних систем потрібно визначите ключові концепції мікросервісів.

Мікросервіси це незалежно реалізовані сервіси які були спроєктований та змодельовані в рамках бізнес-моделі.

Характеризуються такими ключовими елементами [1]:

– Незалежне розгортання (Independent deployability). Незалежне розгортання — це ідея, згідно з якою ми можемо внести зміни в мікросервіс, розгорнути його та оприлюднити ці зміни нашим користувачам без необхідності розгортати будь-які інші мікросервіси.

– Змодельована навколо бізнес-моделі (Modeled around a Business Domain). Це допомагає зрозуміти та структурувати код навколо об'єктів реального світу. Якщо ми моделюємо сервіси навколо бізнес доменів, ми можемо спростити розгортання та реалізацію нових функцій та комбінувати мікросервіси різними способами, щоб надати новий функціонал кінцевому користувачу.

– Управління власним станом (Owning Their Own State). Під цим елементом мається на увазі в контексті доступу до даних сервісу, сервіс повинен володіти своїми даними та дати можливість звертатися до них іншим сервісам, замість того щоб розгортати одну базу даних для всіх наявних сервісів.

– Розмір сервісу (Size). Microservice Patterns (Manning Publications): мета мікросервісів — мати якомога менший інтерфейс. Це знову узгоджується з концепцією приховування інформації, але це спроба знайти сенс у терміні «мікросервіси», якого не було спочатку. Коли цей термін вперше використовувався для визначення цих архітектур, увага, принаймні спочатку, не була конкретно на розмірі інтерфейсів.

– Гнучкість(Flexibility). Ми не знаємо, що чекає майбутнє, тому нам потрібна архітектура, яка теоретично може допомогти нам розв'язувати будь-які проблеми, з якими ми можемо зіткнутися в майбутньому. Справжнім мистецтвом може бути знаходження балансу між можливістю пидтримки певних опцій у майбутньому і покриттям витрат на такі архітектури.

– Alignment of Architecture and Organization [1]

Спочатку мова програмування Go створювалась як внутрішній продукт у компанії Google. Вперше мова була представлена у 2009 році, а перший реліз відбувся у 2012. Основною метою створення цієї мови програмування було поєднання високої продуктивності компільованих мов з легкістю написання коду з підтримкою Garbage Collector. Мова вийшла досить лаконічна, але при цьому код залишається легким для читання і сприйняття. [2]

За допомогою Go ми можемо реалізувати всі ключеві аспекти мікросервісної архітектури, та зробити це зручніше та простіше для розробника, адже Go має такі переваги:

– Швидкість виконання: Go відома своєю високою продуктивністю та швидкістю виконання, що робить її ідеальною для великих і складних проєктів.

– Простота: Go має простий синтаксис, що робить його легким для вивчення та розуміння. Це також сприяє зменшенню кількості помилок при написанні програм.

– Конкурентність: Go підтримує паралельне виконання, що дозволяє програмістам легко створювати паралельні програми. Має дуже цікаву реалізацію перемикання потоків, чим збільшується швидкість. Go має підпрограму яка називається горутиною, за допомогою якої перемикається контекст в рамках потоку не зупиняючи при цьому сам системний та процесорний потік.

– Низький рівень складності: Go забезпечує прямий доступ до пам'яті та не використовує важкі механізми управління пам'яттю, що знижує складність програм.

– Наявність стандартної бібліотеки: Go має багату стандартну бібліотеку, яка містить багато корисних функцій та інструментів для розробки програм.

– Висока масштабованість: Go підтримує масштабованість програм, що дозволяє легко розширювати програми на більші системи.

– Має велику спільноту розробників та велику купу пакетів за межами стандартної бібліотеки.

– Великі корпорації (Amazon, Google, Uber) здійснили великий вклад в розвиток мови, та розширюють бібліотеки на Go.

Розглянемо більш детально, одну з ключових переваг застосування Go у побудові мікросервісів у порівняні з іншими серверними мовами програмування, це продуктивність.

Продуктивність мікросервісу залежить від навантаження та часу відгуку. Для досягнення найкращої продуктивності варто використовувати швидку та високоефективну мову програмування. У порівнянні з іншими мовами, які використовуються для розробки серверної частини вебсайту та мобільних додатків, Go є відмінним вибором. За даними останнього рейтингу програмної мови TIOBE [3] , Go займає 10 місце серед усіх мов програмування, що є досить високим результатом. Однією з переваг Go є те, що вона не потребує віртуальної машини, а отже, програми компілюються в машинний код. Це дозволяє виконувати програми без затримок на розминку та забезпечує високу продуктивність. Крім того, у Go є вбудований збирач сміття, що допомагає керувати пам'яттю та зменшує ризик проблем із безпекою, які можуть виникнути через інкапсуляцію коду. Це також полегшує життя розробникам, оскільки вони не повинні вручну вивільняти пам'ять після використання даних, тим самим уникнувши потенційних помилок, які можуть бути пов'язані з неправильним керуванням пам'яттю. Збирач сміття Go базується на алгоритмі "Mark and Sweep" і виконується автоматично під час роботи програми. Він слідкує за тим, які об'єкти використовуються в програмі, і вивільняє пам'ять, яка більше не потрібна. Це дозволяє підвищити продуктивність програм та полегшити розробку, оскільки розробникам не потрібно докладно керувати пам'яттю. Збирач сміття є одним із багатьох функціональних інструментів

Go, які роблять цю мову програмування досить привабливою для розробників. Слід додати, що Go відомий своєю підтримкою асинхронного програмування. Він пропонує кілька механізмів для роботи з асинхронним кодом, зокрема, горутини (goroutines) та канали (channels). Горутини - це легкі потоки, які можуть бути створені великою кількістю та виконуватися паралельно або асинхронно. Вони дозволяють запускати асинхронний код без потреби вручну створювати та керувати потоками виконання. Канали, з іншого боку, дозволяють горутинам взаємодіяти між собою задля ефективної передачі даних між різними потоками, та керувати узгодженістю виконання певних процесів де це потребується на програмному рівні. Керування горутинами здійснюється за допомогою планувальника горутин (goroutine scheduler). Планувальник відповідає за розподіл горутин між потоками та керування їх виконанням, використовуючи при цьому event-driven модель. З урахуванням наведених переваг, потрібно звернутися до практичного порівняння Go з іншими мовами програмування.

Нижче наведені дані порівняння роботи Go з популярною на сьогодні мовою програмування Java.[4]

edigits

Input: 250001

lang	code	time	stddev	peak-mem	time(user)	time(sys)	compiler/runtime
go	1.go	163ms	1.2ms	8.5MB	153ms	0ms	go 1.19.3
java	1-n.java	811ms	11ms	193.1MB	1427ms	63ms	openjdk 19
java	1-m.java	873ms	66ms	209.7MB	1583ms	97ms	openjdk 20
java	1-m.java	884ms	29ms	321.6MB	1497ms	133ms	graal/jvm 17.0.5
java	1-m.java	1069ms	67ms	457.5MB	1540ms	350ms	openjdk/zgc 19

Рис. 1. Документ «Швидкість роботи Go у порівнянні з Java»

Також слід порівняти швидкодію Go з такою мовою програмування як Python, оскільки в цьому прикладі яскраво виражені переваги Go для побудови мікросервісів.

Як ми можемо бачити з результатів таблиці, одна з головних переваг Go полягає в його швидкості та ефективності, що дозволяє зменшити час відповіді та покращити продуктивність мікросервісів.

fasta

Input: 2500000

lang	code	time	stddev	peak-mem	time(user)	time(sys)	compiler/runtime
go	3-m.go	209ms	2.4ms	4.9MB	373ms	0ms	go 1.19.3
python	1.py	3292ms	74ms	88.9MB	3257ms	20ms	pypy 3.8.13
python	5-m.py	3508ms	55ms	12.6MB	5013ms	1253ms	pyston 3.8.12
python	1.py	3949ms	15ms	7.9MB	3933ms	0ms	pyston 3.8.12
python	5-m.py	4237ms	24ms	13.8MB	6063ms	1223ms	cpython 3.11.0
python	1.py	timeout	0.0ms	0.0MB	0ms	0ms	cpython 3.11.0
python	5-m.py	timeout	0.0ms	0.0MB	0ms	0ms	pypy 3.8.13

Рис. 2. Документ «Швидкість роботи Go у порівнянні з Python»

Нижче додається приклад мікросервісної архітектури програмного додатка з використанням хмарних можливостей AWS.

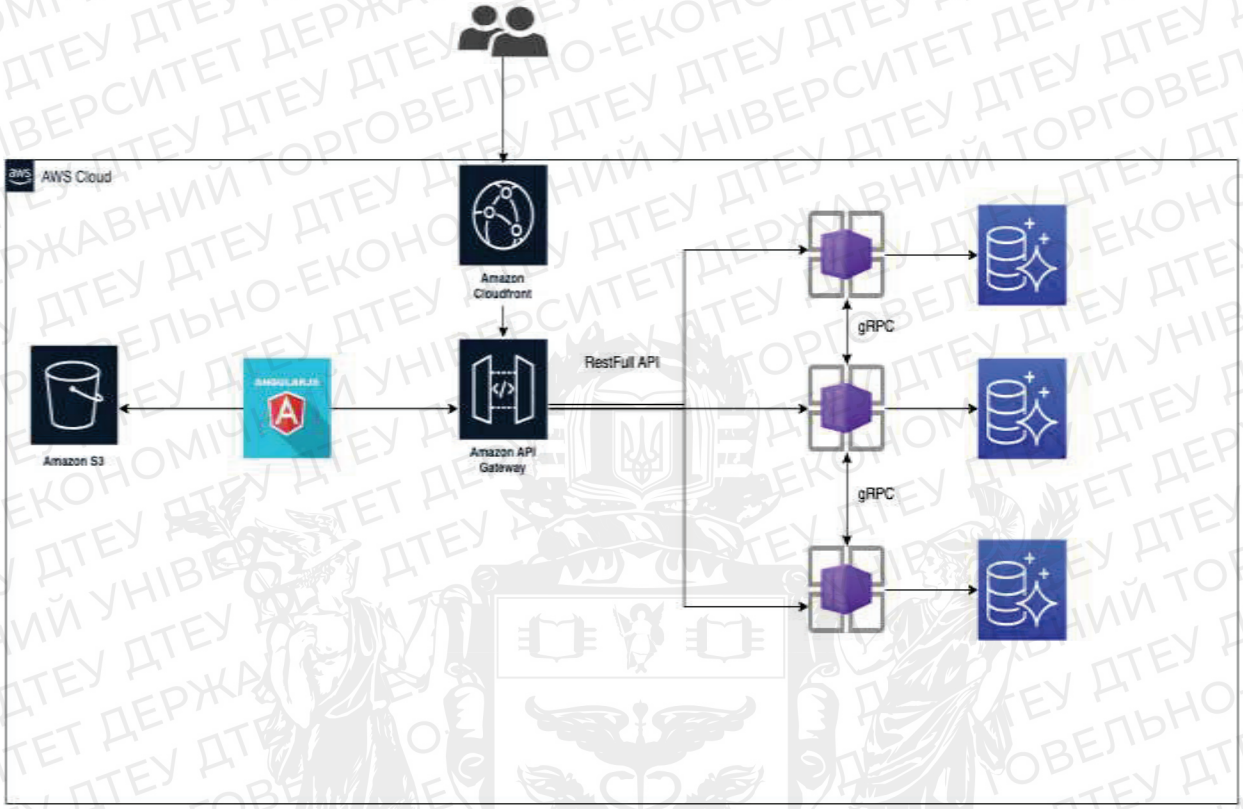


Рис. 3. Вікно Документ «Мікросервісна архітектура». Виконана автором за допомогою веб додатка draw.io

Сучасні міжсервісні системи тісно пов'язані з хмарними технологіями. Тому при розробці мікросервісної архітектури на Go, було застосовний хмарний провайдер AWS, який виділяється з поміж інших конкурентів, зручним та інтуїтивно зрозумілим інтерфейсом, а також широкою документацією. Внутрішню комунікацію між сервісами вирішено реалізувати за допомогою RPC(Remote Procedure Call), оскільки RPC більш ефективним за REST, оскільки передача даних відбувається у вигляді серіалізованих об'єктів, що зменшує розмір даних та сприяє швидкому виконанню запитів. Також RPC дозволяє розподілити логіку програми між різними сервісами, зменшуючи складність коду та покращуючи зрозумілість програми ,розширювати систему на більші обсяги, що підвищує її масштабованість, використовувати різні мови програмування для реалізації різних частин системи, що підвищує її гнучкість. Для комунікації між кліент-сервором, доречно обрати RESTful API, оскільки це дає змогу використовувати стандартні HTTP-методи, такі як GET, POST, PUT і DELETE, що дозволяє стандартизувати взаємодію з ресурсами та спрощує їх розробку та розуміння, а також дає можливість підтримки різних форматів даних, такі як JSON, XML, HTML. Також було вирішено використовувати окрему базу даних для кожного мікросервісу, оскільки це дозволяє забезпечити незалежність сервісів один від одного щодо бази даних. Кожен сервіс може використовувати той тип бази даних, який найбільше підходить для його потреб, також це полегшує масштабування системи. Якщо потрібно збільшити кількість запитів до бази даних в конкретному сервісі, можна просто масштабувати базу даних для цього сервісу, не торкаючись інших компонентів архітектури. При цьому, можемо використовувати різні бази даних. Слід зазначити, що вказаних підхід також забезпечую відмовостійкість мікросервісів , оскільки дозволяю створити зручну та безпечну реплікацію даних мікросервіса. В залежності від прогнозованого навантаження на мікросервісну систему, засовуються такі види реплікацій: Master-slave, Multi-master, Sharding, Eventual consistency, кожна з яких має свої переваги та

недоліки і потребує глибшого аналізу архітектури, тестування навантаження та бізнес вимог до даних користувача. Щодо безпековою складової, всі мікросервіси повинні бути розгорнуті в Amazon Virtual Private Cloud (VPC) це дозволяє створити ізольовану віртуальну мережу, що зменшує ризики внутрішнього доступу до систем та збільшити безпеку даних, а також контролювати доступ до ресурсів забезпечуючи можливість налаштування мережевої інфраструктури на основі потреб користувачів. VPC інтегрується з іншими сервісами AWS, такими як Amazon EC2, Amazon RDS, Amazon EMR, Amazon Redshift та інші, що дозволяє забезпечити максимальну ефективність використання ресурсів. У якості CDN було вирішено використовувати Amazon CloudFront, це дозволяє швидко та ефективно доставляти контент до користувачів в будь-якій точці світу. Це допомагає покращити швидкість завантаження веб-сайтів, відео та інших елементів контенту, захищає від DDoS-атак та забезпечує захист конфіденційної інформації, при комунікації між сервером та користувачем за рахунок можливості використання SSL та HTTPS протоколів. Amazon API Gateway є важливим компонентом мікросервісної архітектури, оскільки дозволяє створювати та керувати API для мікросервісів, що забезпечує зручний спосіб доступу до інших додатків та сервісів. Додатково, API Gateway є інструментом який забезпечує моніторинг та аналітику використання API, що дозволяє керувати продуктивністю та оптимізувати витрати, робити прогнозування навантаження на мікросервіси використовуючи аналітичні дані.

Висновки. Використання мікросервісів дозволяє розділити бізнес-логіку на окремі складові, що спрощує розробку, тестування та підтримку системи. Кожен мікросервіс може бути розроблений та підтримуватись окремо, без впливу на роботу інших компонентів системи. Крім того, мікросервісна архітектура дозволяє розгортати нові функціональність швидко та без перерв у роботі системи, що дає можливість швидко реагувати на зміни вимог бізнесу. Використання мікросервісної архітектури та мови програмування Go дозволяє розробляти ефективні та гнучкі мікросервіси, що забезпечують високу продуктивність та масштабованість. Розробка мікросервісів з використанням мови програмування Go є сучасним вибором, оскільки ця мова має високу швидкодію, підтримку паралельної та асинхронної роботи та зручні засоби для розробки мікросервісів. Також розробка на Go, дозволяє інженерам менше концентруватися на написанні програмного кода, та приділяти більше уваги бізнес логіки при розробці мікросервісів, за рахунок простоти цієї мови програмування. .Таким чином, використання мікросервісів та мови програмування Go є перспективним напрямком для розробки сучасних та ефективних веб-додатків та маштабованих систем, де швидкість виконання та обробка великих пакетів даних має важливе значення.

Список використаних джерел

1. Sam Newman. Building Microservices, 2nd Edition. O'Reilly Media, August 2021 Inc. ст. 1-20
2. Як і для чого вивчати Golang. Переваги і недоліки мови. 02.02.2023. Режим доступу: https://dou.ua/forums/topic/41933/
3. TIOBE Index for March 2023. Режим доступу: https://www.tiobe.com/tiobe-index.
4. Tuan Nguen. Golang Performance Comparison | Why is GO Fast?. Режим доступу: https://www.golinuxcloud.com/golang-performance

Робота виконана під науковим керівництвом PhD, доцента
ДЕСЯТКО А.М.

ЗАСТОСУВАННЯ СЕРВЕРНИХ СЕРВІСІВ У РОЗРОБЦІ МОБІЛЬНИХ ДОДАТКІВ

ЧЕРНЮК В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови архітектури програмних продуктів. Зазначено переваги застосування серверних сервісів у розробці мобільних додатків. Як зразок розглянуто серверний сервіс "Firebase".

The article discusses the basic principles of building the architecture of software products. The advantages of using server services in the development of mobile applications are indicated. The server service "Firebase" is considered as an example.

Актуальність. Сьогодні, для більшості із нас, використання телефону не зводиться лише до звичайних дзвінків чи відправлення SMS повідомлень. В життя людини людини тісно увійшло таке поняття як Інтернет. Його роль тяжко переоцінити, оскільки Інтернет дає нам майже безмежні можливості. Так, завдяки ньому, ми можемо вільно займатися самоосвітою маючи доступ до різноманітних наукових статей, курсів чи відеороликів. А в часи епідемії Covid-19 Інтернет взагалі кардинально вплинув на навчальний процес в закладах освіти по всьому світу, надавши можливість дистанційно здобувати знання. Більшість банківських компаній усвідомили вагомий вплив мережі на збільшення кількості потенційних клієнтів та добавили до переліку власних послуг можливість проведення онлайн-платежів, завдяки чому тепер не потрібно витрачати час у багаточасових чергах банків, що економить дорогоцінний час для більш важливих цілей. Також, завдяки мережі, стало дійсним таке поняття як “негайне спілкування” — отримання повідомлень без значних затримок у часі.

Але всі вищеперераховані можливості так чи інакше вимагають від нас комунікації із віддаленими серверами, на яких зберігається інформація про ці статті, платежі чи повідомлення. Щогодини, щохвилини та щосекунди, при використанні чи то інтернет-банку, чи то онлайн-бібліотеки, між нашими пристроями та їх серверами здійснюється дуже велика кількість обмінів пакетами із інформацією. Будь-яка втрата інформації під час їх передачі чи в момент збереження може призвести до катастрофічних наслідків. Світові відомі випадки, коли через це великі компанії втрачали шалені гроші, а деякі навіть ставали банкротами.

Саме тому збереження цієї інформації та процес її безпечної передачі є одним із найважливіших аспектів будь-якого програмного забезпечення, що направлене на роботу з мережею.

Так, ще до появи серверних сервісів, розробникам додатків, незалежно від масштаба цього додатка та бюджету, доводилося з нуля самостійно пропрацьовувати усю логіку роботи цих серверів із інформацією. Це викликало масу незручностей.

Спочатку необхідно було оприділитися із самим сервером, де мають зберігатися дані. Ця проблема мала декілька варіантів вирішення. Перший — орендувати чужий сервер, що могло бути вкрай ненадійним через можливу нестабільність зі сторони орендодавця(наприклад неякісна підтримка інфраструктури серверів, що може спричинити до втрати даних), але перевагою є відсутність у потребі обслуговування зі сторони орендаря. Другий — створення та налаштування власного серверу. Вибір цього варіанту змушував компаній робити значні витрати як на купівлю, так і на обслуговування. Але показники надійності та безпеки даних значно покращувалися.

Іще однією незручністю стала необхідність у пошуку та наймі висококваліфікованого бекенд програміста, який і буде займатися розробкою логіки роботи серверу. На процес найму та розробки уходили як фінанси, та і час.

З плином часу поступово зростав попит на пошук більш ефективного рішення проблеми із серверами, адже хоча й великі компанії могли дозволити собі ці витрати, але середні та маленькі компанії уже мали проблеми на цьому етапі через обмеженість ресурсів бюджет та часу.

Таким чином, *метою даної статті* є дослідження особливостей використання серверних сервісів під час розробки програмного забезпечення, зокрема мобільних додатків, з метою прискорення процесу розробки, зменшення фінансових витрат та спрощення підтримки у майбутньому .

Об'єктом дослідження є впровадження серверної системи "Firebase" у мобільні додатки.

Предмет дослідження — серверні сервіси.

Виклад основного матеріалу. Оскільки мова йтиме про розробку, то для повноти розуміння всієї базової архітектури доцільно буде пригадати концепцію розбиття клієнт-сервер архітектури програмного забезпечення. Вона поділяється на back-end та front-end. Схематично взаємодію клієнта та цих двох частин можна представити так (Рис. 1).

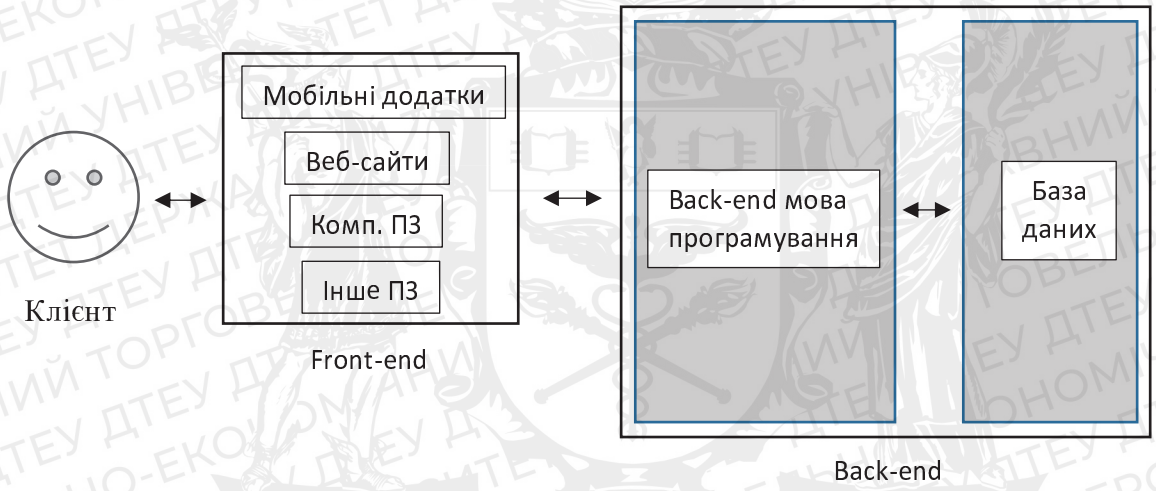


Рис. 1. Сегментація торгівлі

З рисунку вище можна зрозуміти, що користувач, не взаємодіє з сервером напряму, тобто інформація, перед тим як потрапити до клієнта, проходить процес "обробки". Цей процес відбувається в частині продукту, що зветься front-end. Інша назва front-end – сторона клієнта. Саме з нею відбувається взаємодій користувача у багатьох програмних застосунках. Основна задача front-end частини полягає у створенні зрозумілого для користувача UI (user interface), з яким, цей же користувач, матиме змогу взаємодіяти без проблем.

Якщо абстрагуватися від особливостей певних сфер бізнесу, то можна константувати, що причиною взаємодії користувача з front-end частиною є отримання інформації, її редагування, видалення чи додавання у сховище.

Згадайте будь-який сучасний мессенджер, відправляючи комусь повідомлення, Ви несвідомо добавляєте його вміст(разом з іншими метаданими) у спеціальне сховище даних. Потім пристрій одержувача цього повідомлення просто зчитує цю інформацію зі сховища. Це лише приклад із однієї галузі. Розглянемо інший – онлайн-замовлення квитка для подорожі у туроператора. Після його придбання, дані, що були вказані Вами при купівлі, добавляються в базу, після чого, по ним, в разі необхідності підтвердження, можуть зателефонувати представники компанії туроператора. І в разі підтвердження, статус(що іноді може бути навіть одним полем у таблиці сховища) зміниться. Таким чином, ці приклади демонструють, що навіть при умові великої різниці між сферами бізнесу, їх алгоритм роботи з даними, якщо, знову ж таки, звести до примітивних функцій, майже однаковий.

В ролі клієнтської сторони інтерфейсом можуть виступати веб-сайти, комп'ютерне програмне забезпечення і навіть консоль. Оскільки мова у статті йтиме про мобільну розробку, то тут роль сторони клієнта відіграють мобільні додатки, які можна вільно скачати(або придбати) у Google Play чи Apple Store, що залежності від системи.

Отже, саме завдяки стороні клієнта користувач може працювати з даними через інтерфейс. Але необхідно розуміти, що якщо є сторона, яка робить запити на отримання даних(front-end), то є і сторона, що відповідає на ці запити. За виконання цього завдання відповідає back-end.

Back-end – це внутрішня частина сервісу, що є прихованою від ока звичайного користувача і працює віддалено на сервері, незалежно від самого додатку. Тому цю частину називають "серверна сторона". Саме у бекенді основний принцип роботи заключається у своєчасному реагуванні на запити зі сторони клієнта – відправка або прийом для обробки та збереження пакетів із даними. Крім цього, у список задач серверної сторони також входить слідкування за тим, щоб ці дані завжди залишалися в безпеці та були доступними лише тим, хто має на це право.

Так, отримавши базове представлення про слої архітектури програмного продукту, перейдемо до розгляду серверних сервісів.

Як вже зазначалося – раніше, до появи серверних сервісів, серверна сторона(back-end) та логіка роботи з даними мали майже завжди розроблялася з нуля, що створювало значні фінансові та часові проблеми для представників малого та середнього бізнесу. Але після появи серверних сервісів картина змінилася на краще.

Серверні сервіси (Backend as a Service, скорочено BaaS) являють собою модель хмарного сервісу, що включає в себе певний, зазделегідь уже реалізованих комплекс рішень. Це зветься сервісом через те, що є сторонній постачальник, який надає серверні послуги, і є клієнти, які використовують ці послуги для розробки та запуску власних додатків.

Переваги використання Backend as a Service:

- Однією із головних переваг є *налаштовуваний та готовий набір функцій back-end*. Послуги серверної сторони надаються через набір API(Application Programming Interface – інтерфейс для обміну даними) та SDK(Software Developer Kit – набір готових інструментів для розробника), які можуть бути використаними у коді програмного продукту. Це означає, що більше немає необхідності в написанні власного коду для back-end, оскільки цей код уже написаний до вас так, щоб його можна було підлаштувати під усі типові потреби бізнесу. Тому розробникам і представникам бізнес сфери вдається заощадити дорогоцінні фінанси та час, разом з цим перенаправити витратити цих ресурсів на експеременти із покращенням користувальницького досвіду, на покращення клієнтської сторони(front-end) загалом;
- *Вбудовані бази даних*. Зазвичай, разом із готовим бекендом, постачальники серверних сервісів включають у перелік власних послуг і можливість створення баз даних. Доступ до них, знову ж таки, надається через API та SDK;
- *Легка масштабованість.* Якщо додаток швидко розвивається(наприклад збільшення клієнтської бази), то в такому випадку на поміч приходить масштабування, яке зроблене таким чином, щоб в будь-який момент ви могли збільшити чи то місткість баз даних, чи то набір необхідного функціоналу;
- Наявність *інструментів аналітики*, що дозволяють відслідковувати стан роботи програмного забезпечення чи поведінку користувачів у ньому;
- Постачальники BaaS також часто пропонують послуги щодо готової реалізації *аутентифікації* з широким набором можливостей. Перша за все, це створення та редагуванні облікових записів користувачів, перевірка їх електронних скриньок та забезпечення безпеки акаунту паролем;
- *Забезпечення безпеки даних*. По-перше, сервера BaaS, зокрема найбільш популярних постачальників, знаходяться в добре захищених місцях, зводячи до

мінімуму можливість витоку закритої інформації, а по-друге, сервера BaaS спрощують використання GDPR(стандарт ЄС, який вимагає від компаній встановити надійний захист персональних даних користувачів в Інтернеті), оскільки надають різноманітні попередньо створені функції для численних випадків безпеки;

Звісно що BaaS має і певний перелік мінусів:

- Використання такого рішення не буде на безкоштовній основі. Оскільки клієнт виступає в ролі орендатора, то йому, в залежності від постачальника BaaS, необхідно щотижня, щомісяця чи щотижня виконувати плату за послуги. Але тут варто зробити примітку, що ця плата все одно буде ніщо в порівнянні з платою за створення серверу з нуля;
- Бізнес з унікальною моделлю та функціоналом може не підійти BaaS через його направленість на більш типові моделі;
- Постійна прив'язаність до постачальника серверних послуг. У разі переходу з однієї платформи серверних рішень на іншу може виникнути купа проблем. В першу чергу це стосується експорту даних;
- Менший контроль за кодом. Налаштування кожної дрібниці бекенду просто не є можливим;

Завдяки усім цим перевагам та мінусам, BaaS є чудовим вибором для малого та середнього бізнесу. А особливо, через кардинальне зменшення витрат часу на розробку, в нагоді воно стане при розробці MVP(мінімально життєздатного продукту).

Серверні сервіси з'явилися відносно недавно, проте уже доволі успішно конкурують із методом написання серверної частини з нуля (іншою назвою цього методу є "Custom Back-end"). Так, відповідно до результатів досліджень ринку(Рис. 2) компанією Zion [1], станом на 2022-й рік, дохід від BaaS становив $3,0 більйон, а прогноз на 2030-й рік більше, аніж вдвічі перевищує 2022-й, що характеризує розвиток та попит на використання цієї технології як успішний та стрімкий.

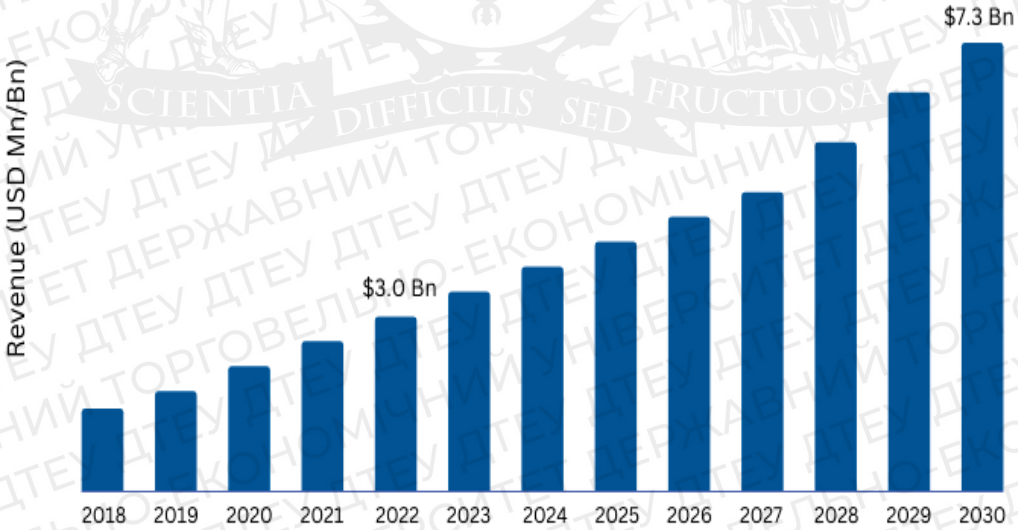


Рис. 2. Розмір ринку BaaS

Що стосується розробки саме мобільних додатків, то тут, задля економії ресурсів під час розробки серверної сторони, може бути використане більш вузьконаправлене серверне рішення – MBaaS(Mobile Back-end as a Service), хоча це не завжди є так. MBaaS дозволяє швидко інтегрувати Ваші мобільні програми з даними та функціями в захищене серверне хмарне сховище. Принцип роботи та набір інструментарію майже один і той самий що і в BaaS, проте більш орієнтований на мобільні пристрої.

Сьогодні на ринку є багато компаній, які надають Baas послуги, найбільш популярними платформами є Firebase, AWS, Supabase, Appwrite, Nhost. Але, через велику кількість

позитивних відгуків, надійності, розглянемо платформу під назвою “Firebase”. Ця платформа розпочала свій шлях у світ IT 2012-го року, надаючи спочатку послуги баз даних у реальному часі, а потім була придбана корпорацією Google. З тих пір Google став відповідальним за розвиток Firebase. Отримуючи все більше і більше функцій, ця платформа повноцінно перетворилася у постачальника серверних сервісів.

На даний момент Firebase має близько 18 функцій, що допомагають зі створення бекенду для різноманітних програм. В першу чергу це стосується мобільних додатків, але є можливість під’єднання сайтів, комп’ютерних програм і тд. Через це Firebase називають BaaS, а не MBaaS платформою.

Щодо функціоналу[2] – він доволі різноманітний та включає в себе багато корисних інструментів, тому розглянемо основні:

- *Бази даних у реальному часі (Firebase Realtime Database)*. Типова взаємодія зі звичайними базами даних заключається у відправці запитів та отримання інформації і у випадку її зміни – робити запит знову для оновлення. Але база даних у реальному часі має трохи інший спосіб взаємодій. Цей спосіб полягає в тому, що всі підключені до цієї бази клієнти, незалежно від додатку чи платформи, мають єдиний екземпляр даних, а ці дані завжди є актуальними та оновлюються автоматично у всіх клієнтів при зміні цих даних;
- *Firebase Authentication*. Вбудовані можливості для швидкого створення безпечної аутентифікації користувачів. Наявна підтримка авторизації через електронну пошту та пароль, номер телефону, Google, Twitter, Facebook і багато інших соціальних мереж;
- *Cloud Storage* – зручний інструмент для зберігання файлів користувачів. Крім цього, завдяки Firebase Authentication SDK, можна здійснювати контроль доступу до цих файлів на основі даних користувачів;
- *Cloud Functions*. Створення власних функцій для бекенду, що покликано задля розширення функціоналу Firebase платформи. Принцип їх роботи полягає в реагуванні на певні події в серверному сервісі, наприклад якщо користувач завантажить файл в Cloud Storage, то ім’я файлу запишеться в якусь окрему базу даних. Важливо, на що реагувати і як визначає сам розробник та бізнес задачі, а не платформа;
- *Hosting*. На перший погляд є звичайним хостингом для сайтів та веб-додатків, але може мати майже увесь функціонал Firebase(включаючи авторизацію, бази даних у реальному часі, функції і тд.);

Як можна помітити, практично усі функції Firebase взаємодіють один з одним. Це і робить дану платформу потужною та ефективною з точки зору економії фінансів та часу.

Щоб почати застосування BaaS сервісів, зокрема Firebase, у мобільній розробці, необхідно пройти декілька етапів. В приклад візьмемо уже реалізований додаток на операційній системі Android [3].

Проходження першого етапу зводиться до налаштування самого мобільного додатку таким чином, щоб він відповідав мінімальним вимогам Firebase, для Android – це версія 4.4, а рівень API – 19.

Переконавшись в тому, що додаток відповідає вимогам вище, необхідно перейти на сайт та створити новий проект в Firebase (Рис. 3) вказуючи ім’я в першому кроці та налаштовуючи інструменти аналітики в другому.

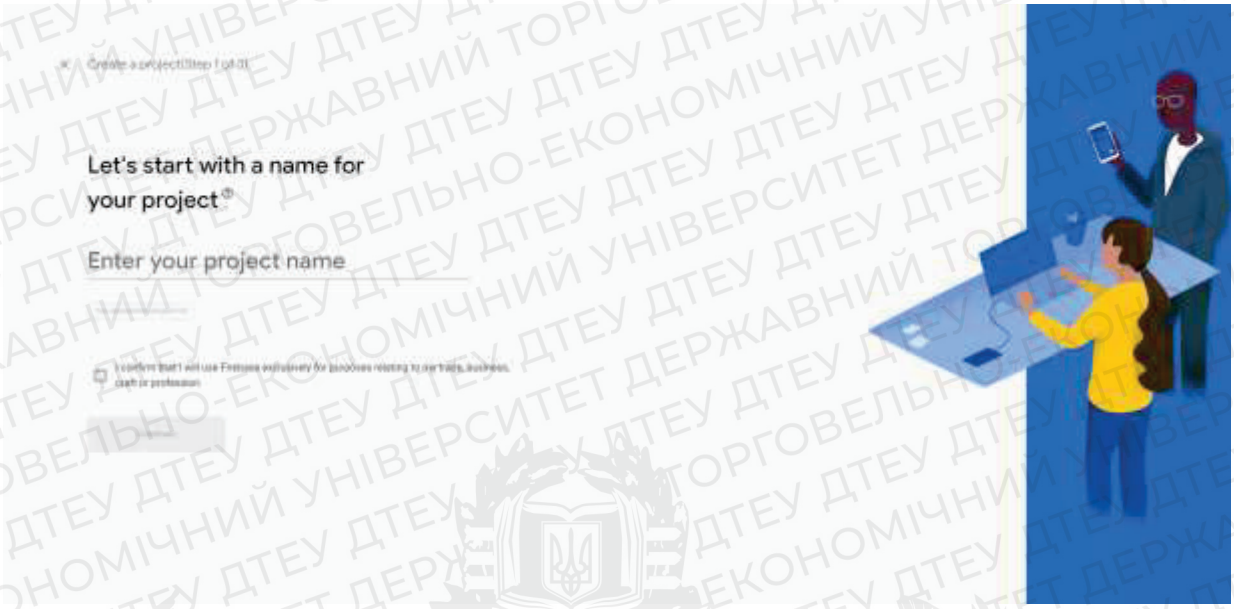


Рис. 3. Створення проекту в Firebase

Як тільки проект буде успішно створено, то за допомогою сайту та спеціального файлу налаштування, є можливість додати Android додаток в нього. В цих файлах містяться необхідні для поєднання з проектом дані. Поєднавши додаток з проектом, залишається лише додати в залежності від мобільного додатку Firebase SDK, який і дасть можливість використовувати функціонал Firebase в мобільному додатку.

Застосування серверних сервісів у розробці мобільних додатків є важливим етапом для забезпечення якості та функціональності програмного продукту. Вони дозволяють розділити логіку та оптимізувати взаємодію між клієнтом та сервером, забезпечити безпеку даних та покращити продуктивність. Незважаючи на виклики, пов'язані з впровадженням та підтримкою серверних сервісів, їхні переваги у значній мірі сприяють покращенню якості мобільних додатків та задоволенню потреб користувачів.

Висновки. Сфера розробки програмного забезпечення ніколи не стоїть на місці. Майже щодня перед розробниками постають нові виклики щодо вирішення задач по вибору найбільш зручної, а головне – ефективної архітектури для того чи іншого програмного продукту. Таким чином на світ з'явилися серверні сервіси. Завдяки набору готових рішень, час, що витрачається на розробку бекенду мобільних (і не лише) додатків, значно зменшився, що дало шанс середньому та малому сегменту бізнесу на існування та конкурування з більшим.

Список використаних джерел

1. Cloud Mobile Backend as a Service (BaaS) Market Size, Share 2030 \\ Режим доступу: https://www.zionmarketresearch.com/report/cloud-mobile-backend-as-a-service-market (останнє звернення 04.04.2023р.)
2. Firebase Products \\ Режим доступу: https://firebase.google.com/products-build (останнє звернення 04.04.2023р.)
3. Add Firebase to your Android project \\ Режим доступу: https://firebase.google.com/docs/android/setup (останнє звернення 04.04.2023р.)

Робота виконана під науковим керівництвом к.т.н., доцента
КОТЕНКО Н.О.

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

ШАБАЛІН Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто криптографічні методи захисту електронних документів, зокрема, використання електронного цифрового підпису (ЕЦП) як токену аутентифікації для захисту електронних документів. Автор статті проаналізував різноманітні методи захисту електронних документів та визначили переваги використання ЕЦП як ефективного засобу захисту.

The article discusses cryptographic methods for protecting electronic documents, including the use of an electronic digital signature (EDS) as an authentication token for securing electronic documents. The author of the article analyzed various methods of protecting electronic documents and identified the advantages of using EDS as an effective means of protection.

Актуальність. У сучасному світі все більше ділових та повсякденних операцій відбуваються в електронному вигляді, що збільшує ризики втрати даних, витоків конфіденційної інформації та крадіжки електронних документів. Захист електронних документів є надзвичайно важливою та актуальною темою, яка потребує уваги і досліджень. У зв'язку з цим, криптографічні методи захисту електронних документів є надзвичайно важливою темою досліджень в сфері інформаційної безпеки. Один з найбільш ефективних криптографічних методів захисту є використання електронного цифрового підпису (ЕЦП) як токену аутентифікації для захисту електронних документів.

Оскільки ЕЦП є ефективним засобом захисту електронних документів, наукові дослідження в цьому напрямку мають велику вагу та значення. Такі дослідження необхідні для розробки нових інноваційних методів захисту електронних документів з використанням ЕЦП, а також для удосконалення наявних методів та розробки рекомендацій з їх використання.

Однак, збільшення кількості електронних документів також призводить до збільшення кількості кібератак та крадіжок інформації. Використання ЕЦП як токену аутентифікації може допомогти забезпечити високий рівень захисту електронних документів та знизити ризики їхньої крадіжки або несанкціонованого доступу до них.

Метою статті є дослідження криптографічних методів захисту електронних документів. У статті проаналізовано сучасні методи захисту електронних документів, виявлені їхні недоліки та переваги, а також розглянуті можливості використання ЕЦП для захисту електронних документів. Дослідження базується на теоретичних аспектах криптографії та реалізації технологій захисту даних.

Об'єктом дослідження є криптографічні методи захисту електронних документів, зосередження уваги на використанні електронного цифрового підпису (ЕЦП) як токену аутентифікації для захисту електронних документів.

Предмет дослідження – криптографічних методів захисту.

Аналіз попередніх досліджень. Аналізуючи попередні дослідження з проблематики захисту електронних документів, було виявлено, що українські дослідники та експерти проявляли значний інтерес до криптографічних методів захисту електронних документів. У статтях були проаналізовані основні методи захисту даних в електронному документообігу та виявлені їх переваги та недоліки. Присвячені праці вітчизняних науковців: Я.О. Іващенка та І. В. Бубнової, О. В. Кравця та інших.

Виклад основного матеріалу. В умовах сьогодення, коли електронні документи стають все більш поширеними, захист цих документів від несанкціонованого доступу та зловживань є дуже важливим завданням. Криптографічні методи захисту є одними з найбільш ефективних

методів забезпечення безпеки електронних документів. Одним із найбільш важливих криптографічних методів захисту є електронний цифровий підпис (ЕЦП). ЕЦП використовується для аутентифікації документу та автора документу, а також для забезпечення цілісності даних, тобто захисту від їхньої модифікації без належних дозволів. Використання ЕЦП дозволяє забезпечити відповідність електронних документів законодавству та міжнародним стандартам. Щоб використовувати ЕЦП для захисту електронних документів, необхідно мати токен або смарт-карту, на яких зберігається особистий ключ підписувача. Токен або смарт-карта (рис. 1) забезпечують безпеку ключа підписувача та дозволяють уникнути несанкціонованого доступу до ключа [1].

Рис. 1. Ілюстрація цифрового підпису даних

Таким чином, необхідно враховувати те, що ЕЦП може бути підробленим, якщо ключ підписувача стає відомим зловмисникам. Тому важливо забезпечити належний захист токена або смарт-карти, на яких зберігається ключ підписувача. Загалом, використання ЕЦП є ефективним методом захисту електронних документів. Однак, для забезпечення належної безпеки, необхідно дотримуватись правил зберігання та використання токена або смарт-карти з ключем підписувача.

Розглянемо застосування ЕЦП як токену аутентифікації для захисту електронних документів. ЕЦП є цифровим підписом, який дає можливість підтверджувати автентичність та цілісність електронного документа. Для цього використовується криптографічний ключ, який є відомим лише власнику підпису та призначений для створення та перевірки підпису. Серед ключових переваг застосування ЕЦП є можливість перевірки автентичності та цілісності документа. Це забезпечує відсутність можливості зміни документа без зміни його ЕЦП. Крім того, ЕЦП може бути використаний як токен аутентифікації, що дає можливість підтверджувати автентичність власника підпису [2].

Використання ЕЦП як токену аутентифікації може бути особливо корисним в електронній комерції та банківській сфері, де важливо захистити конфіденційні дані та транзакції. В таких випадках, використання ЕЦП забезпечує високий рівень захисту даних від несанкціонованого доступу та зміни.

Для використання ЕЦП як токену аутентифікації необхідно виконати наступні кроки:

1. Створити ЕЦП для документа, що підписується.
2. Зберегти ЕЦП разом з ідентифікаційними даними власника підпису.
3. Перевірити ЕЦП при кожній спробі доступу до документа.

При цьому, необхідно використовувати безпечний канал передачі даних для збереження конфіденційності інформації. Також важливо забезпечити надійність та захист від небажаного доступу до документів під час їх зберігання на електронних носіях.
В роздрібній торгівлі застосовуються три класи інформаційно-управляючих систем.

До ефективних методів захисту електронних документів належить використання електронних цифрових підписів (ЕЦП) як токену аутентифікації. ЕЦП забезпечує ідентифікацію власника документу та його цілісність, тобто відсутність змін у документі після підписування. Крім того, ЕЦП може використовуватися для забезпечення нерепудіації, тобто неможливості відмовитися від підпису, що був накладений на документ. Для досягнення максимальної ефективності при використанні ЕЦП необхідно мати відповідні знання і навички в галузі криптографії та інформаційної безпеки. Також потрібно мати доступ до відповідної інфраструктури, яка забезпечить надійність та безпеку процесу підписування документів. Серед ключових етапів при використанні ЕЦП є генерація ключів. Для генерації ключів використовуються криптографічні алгоритми, які забезпечують надійність та безпеку ключів (рис.2). Після генерації ключів, користувач повинен зберегти їх у безпечному місці, а також забезпечити їх захист від несанкціонованого доступу [3].

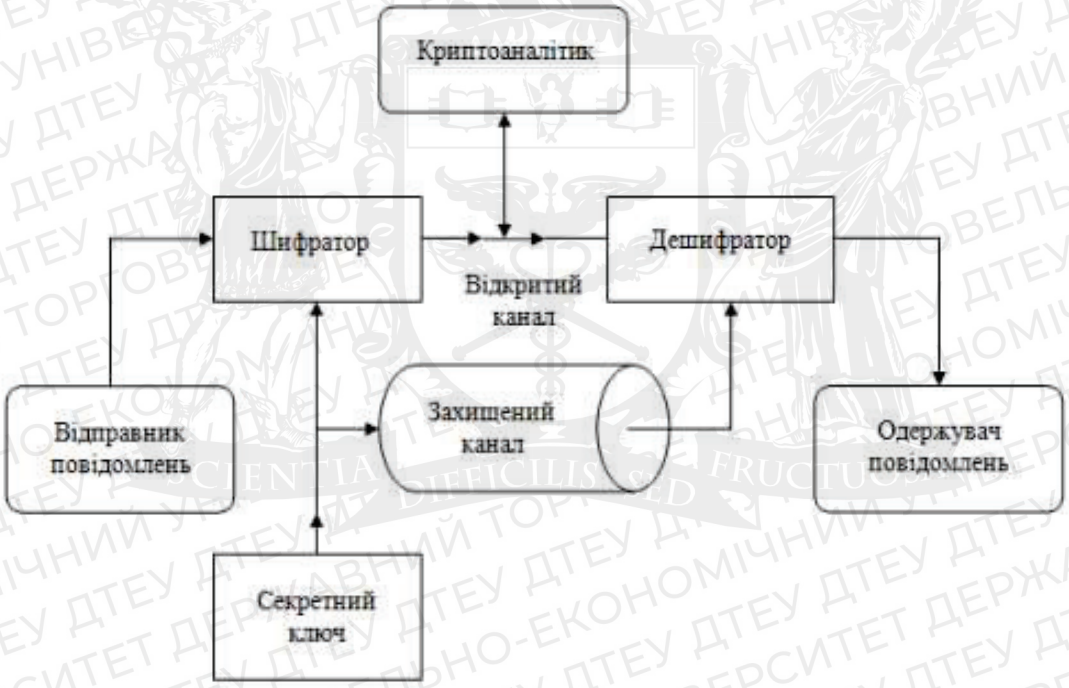


рис. 2. Схема криптосистеми з таємним ключем.

Після генерації ключів, користувач може використовувати ЕЦП для підписування електронних документів. Для цього необхідно вибрати потрібний документ та обрати опцію «підписати». Система згенерує хеш-код документу та зашифрує його за допомогою приватного ключа користувача. Далі цифровий підпис додається до документу. Із переваг використання ЕЦП для підписування документів є можливість перевірки автентичності та цілісності документу. Оскільки підпис створюється з використанням приватного ключа, який відомий лише власнику, то будь-які зміни в документі призведуть до недійсності підпису. Таким чином, використання ЕЦП забезпечує захист від будь-яких спроб підробки документа.

Наступним етапом є перевірка підпису. Для цього необхідно відкрити підписаний документ та вибрати опцію «перевірити підпис». Система автоматично розшифрує хеш-код документу за допомогою відкритого ключа користувача, який міститься у сертифікаті. Далі порівнюється розшифрований хеш-код з хеш-кодом самого документу. Якщо дані співпадають, то підпис вважається дійсним, а документ – автентичним та цілим. У зв'язку з використанням ЕЦП, як токену аутентифікації, забезпечується захист електронних документів

від несанкціонованого доступу та підробки. Проте, необхідно дотримуватись правильної процедури збереження ключів та використання безпечного каналу передачі даних для забезпечення конфіденційності.

Для забезпечення максимальної ефективності та надійності захисту електронних документів, необхідно дотримуватись правильної процедури збереження ключів. Ключі повинні зберігатись в надійному місці, що захищене від несанкціонованого доступу, наприклад, в безпечній зоні з обмеженим доступом або на криптографічному токені.

Крім того, використання безпечного каналу передачі даних є обов'язковим для забезпечення конфіденційності інформації, що передається при використанні ЕЦП. Для цього можуть використовуватись різні технології, такі як SSL / TLS або VPN, що забезпечують шифрування даних та захист від несанкціонованого доступу. Загальна ідея використання криптографічних методів захисту електронних документів полягає у забезпеченні конфіденційності, цілісності та доступності інформації, що міститься в них. Використання електронних документів зросло в останні роки, тому необхідно забезпечувати їх захист від різних загроз.

В умовах розвитку інформаційних технологій, все більше урядових структур переходять до електронної форми обміну документами. При цьому, дуже важливо забезпечити безпеку передачі і зберігання цих документів. Одним із ефективних способів є використання ЕЦП для підпису документів. Це дозволяє забезпечити конфіденційність, цілісність та автентичність даних. Переваги методу використання ЕЦП в контексті електронної адміністрації можуть включати аналіз ефективності та швидкості передачі даних з використанням ЕЦП порівняно з іншими методами захисту, а також оцінку ефективності методу в захисті від атак на систему електронної адміністрації, таких як перехоплення даних, відмова в обслуговуванні тощо.

Отже, переваги використання ЕЦП в контексті електронної адміністрації можуть бути наступними:

- *Забезпечення безпеки електронних документів:* за допомогою ЕЦП можна переконатись у тому, що електронний документ був підписаний конкретним користувачем і не був змінений після підписання.
- *Зручність та ефективність:* використання ЕЦП дозволяє зменшити час та витрати, пов'язані з підписанням паперових документів, та забезпечити більш швидке та ефективне обмін документами між учасниками.
- *Екологічність:* використання ЕЦП дозволяє зменшити кількість паперових документів, що зберігаються в офісі, та зменшити екологічний вплив на довкілля.

Прикладом успішного використання ЕЦП в контексті електронної адміністрації може служити впровадження Електронного митного декларування в Україні. За допомогою ЕЦП, митники можуть підписувати електронні митні декларації та інші документи, що забезпечує їх автентичність та недоступність для несанкціонованого доступу. Це дозволило зменшити час, витрати та помилки в процесі декларування товарів, що сприяє зростанню ефективності роботи митниці та підвищенню якості послуг, які надаються учасникам зовнішньоекономічної діяльності [4].

У порівнянні з іншими криптографічними методами, наприклад, паролями, ЕЦП має перевагу в тому, що воно не може бути відновлено або вгадано. Крім того, ЕЦП може бути використаний для автоматизації процесів, що зменшує кількість помилок, що можуть статися через людський фактор. До прикладу використання ЕЦП можна віднести систему декларування майна, яка була запроваджена в Україні в 2016 році. За допомогою ЕЦП громадяни можуть подавати декларації про своє майно та доходи онлайн, що забезпечує надійний захист даних та зменшує кількість помилок при їх заповненні. Також ця система зменшує корупцію, оскільки прозорість у веденні реєстру майна дозволяє контролювати доходи та майно посадових осіб.

У контексті електронного бізнесу використання ЕЦП має також свої переваги. Однією з них є можливість підписання електронних договорів, що дає можливість юридично оформляти угоди в онлайн-режимі. Це дозволяє економити час та зменшувати витрати на організацію зустрічей для підписання паперових документів. Крім того, використання ЕЦП забезпечує захист інтелектуальної власності, оскільки воно дозволяє встановлювати авторства електронних документів та підтверджувати їхню автентичність. За допомогою ЕЦП також можна забезпечувати безпеку платежів у електронному форматі, оскільки він гарантує, що платіжні дані не будуть змінені під час передачі та що транзакція буде здійснена від імені вірного платника [5].

Для прикладу, можна вказати, що в банківському секторі використовуються ЕЦП для забезпечення безпеки платежів та фінансової звітності [6]. Крім того, ЕЦП використовується в інтернет-магазинах для підтвердження автентичності замовлень та документів, а також для забезпечення безпеки транзакцій. Таким чином, використання ЕЦП у електронному бізнесі забезпечує безпеку та автентичність електронних документів та транзакцій, дозволяє економити час та зменшувати витрати на їхню організацію, а також сприяє захисту інтелектуальної власності.

Висновки. Запровадження ЕЦП як методу захисту електронних документів дозволяє забезпечити високий рівень безпеки та автентифікації в електронному середовищі. Цей метод має безліч переваг перед іншими криптографічними методами захисту електронних документів. Наприклад, забезпечення конфіденційності даних, підтвердження автентичності та цілісності документу, захист від несанкціонованого доступу до даних.

Крім того, використання ЕЦП має великий потенціал для застосування в електронній адміністрації. Наприклад, в Україні вже успішно використовується система ЕЦП для забезпечення автентифікації та захисту електронних документів в державних органах. Це дозволило покращити ефективність та швидкість процесів, а також зменшити кількість паперової роботи. Використання ЕЦП як методу захисту електронних документів є важливим елементом в електронній адміністрації та має безліч переваг перед іншими криптографічними методами. Його використання дозволяє забезпечити безпеку та конфіденційність даних, а також зменшити час та затрати на обробку електронних документів.

Список використаних джерел

1. Рагога Д.І. Електронний цифровий підпис у документах. – Наукові праці Донецького національного університету імені Василя Стуса. – 2021. – С. 50-56.
2. Перепелиця. Л.С. Методи та засоби автентифікації користувачів в інформаційно-телекомунікаційних системах та вироблення рекомендацій щодо підвищення їх ефективності. Наукові праці Державного університет телекомунікацій Київ. – 2022. – С. 76-80.
3. Глинчук Л.Я. Криптологія. Луцьк. Східноєвропейський національний університет імені Лесі Українки. Вежа-Друк 2014. – С. 182-186.
4. Державний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічні захист електронної інформації. Електронний цифровий підпис. Вимоги до створення, використання та перевірки.
5. Регламент ЄС 910/2014 від 23 липня 2014 року про електронний ідентифікаційний та послуги довіри для електронних транзакцій на внутрішньому ринку і відмінення директиви 1999/93/ЄС.
6. Глєбова Н. В. Електронний цифровий підпис: обліковий та податковий аспекти. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. – 2018. – С. 94-97.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т.В.

СПОСОБИ МІНІМІЗАЦІЇ РИЗИКІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ В МІЖНАРОДНІЙ ЛОГІСТИЦІ

ШАПОЧНІКОВА А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні способи зниження ризиків несанкціонованого доступу та забезпечення захисту персональних даних від витоку в міжнародній логістиці. Виокремлено Ransomwar, як найбільш розповсюджена вірусна активність в організації. Зазначено забезпечення безпеки даних і захисту в логістичній галузі від кібератак. Розглянуто як зразок морський сектор в міжнародній логістиці та найефективніший спосіб підготовки до захисту від несанкціонованого доступу.

The article examines the main ways to reduce the risks of unauthorized access and how to ensure the protection of personal data from leakage in international logistics. Ransomware is highlighted as the most viral activity in an organization. The article discusses securing data and protection in the logistics industry against cyber attacks. The maritime sector in international logistics is considered as an example, along with the most effective way to prepare for protection against unauthorized access.

Актуальність. Останні декілька років міжнародна логістика все більше страждає від кібератак. Кожна логістична компанія піддається на внутрішні та зовнішні ризики, пов'язані з перебоями в ланцюжках поставок. Найбільш кібератаки зросли після початку пандемії COVID-19 та на початку повномасштабного російського вторгнення. Логістика в Україні стала однією з перших для цілей кіберзлочинців після російського вторгнення, масштабною кібератакою на логістику, енергетику, державну владу тощо.

Про один з прикладів кібератак у логістичній галузі, в жовтні 2022 році, Microsoft повідомила про кібератаку на підприємства логістичного сектору України та Польщі. Відомо, що кіберзлочинці попередньо отримали доступ до прав адміністратора мережі. Також, Microsoft зазначає, що нове ПЗ-вимагача під назвою «Prestige» збігаються з жертвами іншої кібератаки, ця мета атаки була спрямована на знищення даних. Зазначається, що на початку повномасштабного російського вторгнення програма-вимагача Prestige ransomware, вразила сотні комп'ютерів в Україні, Литві та Латвії. Це тип шкідливого програмного забезпечення, який блокує доступ до файлів або IT-систем організації [1].

Глобальна інтеграція ланцюгів постачання призвела до надзвичайно високого рівня ризику для третіх сторін. Національний інститут стандартів і технологій (NIST), зазначає сторонні сховища є потенційними векторами атак. Зокрема, логістичні організації, щоб забезпечити безперервність роботи своїх систем, переносять робочі потужності на хмарні платформи та використовують хмарні сервіси. Наприклад, зараз транспортна галузь надає перевагу відстеженню вантажів, які вона перевозить, і зберігає дані своїх власників у хмарі за допомогою Інтернету речей.

Intel 471 зазначає, що виявив різних кіберзлочинців, які мають доступ до мережі, які продають облікові дані, належать до логістичних компаній. Це вже можлива криза кібербезпеки в ланцюжку постачання матиме дуже поганий вплив на глобальну споживчу економіку. Кіберзлочинці стверджують, що отримали облікові дані через уразливості рішень віддаленого доступу.

Метою статті є дослідити способи зниження ризиків при несанкціонованому доступі, яка допоможе захистити персональні дані в логістичному секторі.

Об'єктом дослідження є система мінімізації ризиків несанкціонованого доступу до персональних даних.

Предмет дослідження – система захисту персональних даних.

Виклад основного матеріалу. Аналізуючи світову статистику нападів, Microsoft визначає, що всього за один рік лише масштаб атак на паролі до облікових записів працівників організацій зріс на 74% — до понад 920 випадків на секунду. Як вже було зафіксовано організації стикаються із підвищенням активності вірусів-вимагачів або ж шифрувальників (англ. — Ransomware), які впливають на персональні дані. Атака може призвести до втрати своєчасного доступу до персональних даних, якщо немає відповідних резервних копій. Це завдавало шкоди логістичному сектору по всьому світу в 2022 році:

- програмне забезпечення-вимагач було використано в серії атак, націлених на сектори транспорту та логістики в Україні та Польщі. Група зберігала доступ до жовтня, Microsoft вже зазначала, що група, яка стоїть за атаками, отримала високий рівень доступу до цільових мереж досі невідомими засобами. Також, компанія «сигналізує про підвищений ризик для організацій, які безпосередньо постачають чи транспортують гуманітарну чи військову допомогу в Україну».
- лютий 2022-го року кібератака на дві логістичні компанії вплинула на системи обробки платежів сотень автозаправних станцій на півночі Німеччини;
- березень, атака на поштову службу Греції тимчасово перервала її роботу та призупинила обробку фінансових транзакцій;
- травень, напад хакерів спричинив затримки та скасування рейсів однієї з найбільших авіакомпаній Індії, перервавши поїздки сотень пасажирів.

Агентство Європейського Союзу з кібербезпеки (ENISA), зазначає про Ransomware, як головну загрозу кібербезпеки, оскільки кіберзлочинці дуже мотивуються з отримання персональних даних.

Розвиток технологій, що використовуються в операційній частині логістичного сектору, полегшує роботу працівників у віддаленій співпраці. Віддалені процеси – це сеанси, які відбуваються з незахищеним і незахищеним віддаленим з'єднанням, іноді протягом днів, іноді тижнів, залежно від тривалості міграції, і можуть зробити систему вразливою до атак програм-вимагачів.

В логістичному секторі для мінімізації витоку персональних даних потрібно забезпечити віддалений доступ і сегментація мережі, для забезпечення безпеки даних і захисту компанії від кібератак, такі як:

- програма інформування про кібербезпеку;
- принцип найменших привілеїв (POLP);
- використання багатофакторної автентифікації (MFA) та застосування політики надійних паролів;
- фізична охорона;
- підтримка програмного забезпечення в актуальному стані, щоб запобігати вразливостям системи безпеки;
- інвестувати в програми кібербезпеки та часто створювати резервні копії файлів у хмарі, щоб захистити їх від програм-вимагачів.

Програма інформування про кібербезпеку – це навчання співробітників компанії усвідомленню кіберзагроз, оскільки людський фактор в більшості випадків це і є загроза для організації. Інституції, які працюють у логістичній галузі, погоджуються, що захист критичної інфраструктури пов'язаний із безпекою систем, які безпосередньо стежать за процесами в логістиці. Люди, які працюють у секторі критичної інфраструктури, повинні бути обізнані про політику захисту даних компанії та відповідні закони та нормативні акти, тримаючись у курсі подій за допомогою тренінгів і семінарів. Співробітники в міжнародній логістичній компанії, які мають більш глибоку участь в обробці даних — наприклад, у зборі потенційних клієнтів, підтримці та зберіганні бази даних співробітників, а також передачі персональних даних

третім особам для звітності чи операцій — отримають додаткове навчання з правил захисту, що стосуються їхньої конкретної посадової функції. Той факт, що багато інцидентів із безпекою та конфіденційністю, які з'являються в новинах, пов'язані з помилками людини, щоб знизити ризики несанкціонованого доступу до персональних даних.

Визначення принципу найменших привілеїв – половина організацій мають користувачів із більшими правами доступу, ніж це необхідно для виконання їхньої роботи. Підхід POLP спрямований на регулярний аудит внутрішніх привілеїв доступу користувачів, щоб забезпечити мінімально необхідний рівень доступу до даних, систем, мереж і пристроїв, щоб особа могла виконувати свої основні обов'язки.

Багатофакторна автентифікація (Multi-factor authentication) може зупинити неавторизований доступ, що часто виникає через один зламаний пароль чи облікові дані. Наприклад, можна вгадати чи зламати пароль, проте, нелегітимний доступ важче отримати до вторинної (чи третинної) форми перевірки особи. Слід зазначити, за результатами Microsoft Multi-factor authentication допоможе запобігти 99,9% зламаних облікових записів користувачів.

Політика надійних паролів є одним із найкращих засобів захисту від несанкціонованого доступу. Це означає розробку та впровадження політики надійних паролів, яка вимагатиме від усіх користувачів дотримання встановлених найкращих практик щодо створення та регулярної зміни надійних паролів, а також забезпечення повторного використання паролів на різних пристроях, програмах чи інших облікових записах, використовуючи менеджер паролів, що являє собою зашифроване цифрове сховище, яке зберігає безпечні паролі для входу в облікові записи на пристроях, веб-сайтів та інших служб.

Фізична охорона. Незалежно від того, чи це внутрішній зловмисник, чи зовнішній зловмисник, який відвідує робоче місце, залишаючи пристрої розблокованими або записані паролі чітко видимими, є простим рецептом для несанкціонованого доступу.

Підтримка програмного забезпечення в актуальному стані. Кіберзлочинці часто отримують несанкціонований доступ через відомі вразливості. Потрібно регулярно оновлювати все програмне забезпечення, постійно оновлювати виправлення безпеки та встановлювати автоматичні оновлення безпеки, коли це можливо, щоб знизити ризик несанкціонованого доступу до персональних даних в організації.

Інвестування в програми кібербезпеки та *створення резервних копій файлів у хмарі*, щоб захистити їх від програм-вимагачів. З розвитком технологій сектору логістики кількість користувачів і додатків, які отримують доступ до даних, включених у процес закупівлі, зсередини організації та віддалено також зросла. Є доступ до хмарних даних багатьох привілейованих і адміністративних облікових записів, від допоміжного персоналу до обслуговуючого персоналу, від віддалених постачальників до корпоративних і колективних додатків, щоб підтримувати його ефективну роботу. Зростаюча кількість привілейованих облікових записів ускладнює керування цими обліковими записами та робить їхні системи керування відкритою мішенню для кіберзлочинців.

Пристрої IoT відіграють важливу роль у цифровій трансформації логістичної галузі. Програми Database Access Manager та Privilege Task Automation, можуть записувати доступ до бази даних для привілейованих облікових записів, підключених до пристроїв IoT, а також автоматизувати рутинні операції. Рівні захисту, такі як динамічний контролер паролів і двофакторна автентифікація, забезпечують безпечне керування інформацією про ідентифікацію та пароль, а також захищають облікові дані привілейованих облікових записів за допомогою складних паролів і додаткових кроків підтвердження. Таким чином, ці облікові записи захищаються від внутрішньої та зовнішньої загрози.

Міжнародна логістика інтегрується у велику галузеву інфраструктуру, наприклад, можна визначити серед них:

- морські перевізники інтегрують від простих безпекових систем оповіщення до повноцінних мереж з хмарними технологіями;

- залізничні перевізники інтегрують від мережі, до GSM-Railway.

Також, існує підхід до управління ризиками для морської логістики (рис. 1). Інтеграція управління ризиками включає такі складові:

1. Визначення ролей та обов'язків користувачів, ключового персоналу та керівництва зацікавлених сторін та оператори відповідних ланцюгів постачання.

2. Ідентифікація систем, активів, даних і можливостей, які в разі порушення можуть становити ризики для логістичні операції та безпека.

3. Реалізація технічних і процедурних заходів, а також альтернатив для захисту від кіберінцидентів для забезпечення безперервності операцій.

4. Здійснення заходів з підготовки та реагування на кіберінциденти [2].

В міжнародна морській логістиці різною мірою ці правила намагаються забезпечити дотримання мінімальних стандартів для захисту найбільш конфіденційних даних і операцій компаній, зокрема, записів клієнтів та інформації про доставку.

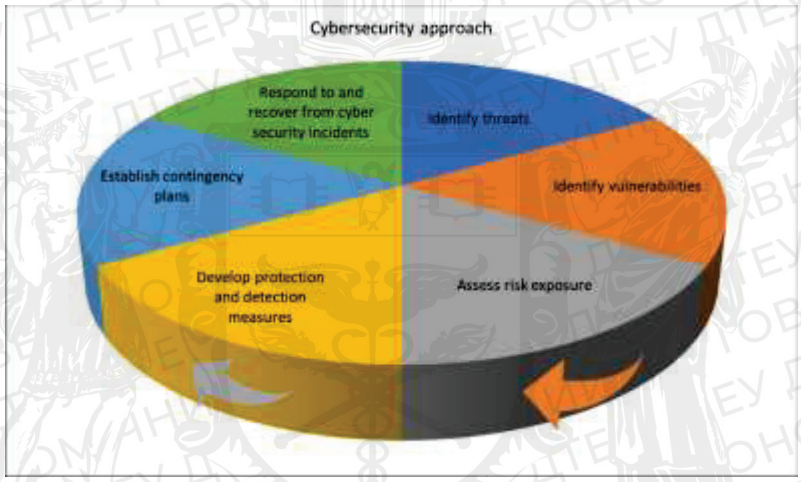


Рис. 1. Підходи до управління ризиками в морській логістиці

Слід зазначити, що ризики зростають, зокрема:

- потенційна втрата контролю над своїми персональними даними;
- стати мішенню для атак у стилі соціальної інженерії з використанням зламаних даних;
- потенційна безповоротна втрата персональних даних;
- їхні персональні дані далі зловмисно використовуються злочинцями (наприклад, для полегшення ідентифікації та фінансового шахрайства).

Інтеграція комплексного плану безпеки в мережеві системи логістики забезпечує результативний спосіб підготовки до несанкціонованого доступу. Слід провести комплексну оцінку ризиків, що допоможе розробити надійну стратегію ризиків кібербезпеки. Якщо виділяти морську галузь в логістиці, людський фактор стає ще більш складним у складній взаємопов'язаній екосистемі, подібній до тієї, яка існує. Кораблі, порти та треті сторони часто працюють зі змінними екіпажами з різним рівнем розуміння кібербезпеки, які можуть бути не повністю знайомі з безпечною роботою відповідних систем і усталеними методами кібергігієни [3].

Відсутність знання кібербезпеки може бути вигідною для будь-якого зловмисника, який хоче отримати доступ до судна та його систем, викрасти фактичну інформацію або порушити роботу судна. Системи захисту можуть брати участь у ідентифікації та пом'якшенні потенційних кібератак на кількох рівнях. Виявлення та контрзаходи, вжиті для нападу на одне судно, можуть бути передані іншим автономним суднам. В таблиці 1 наведено системи, що можуть допомогти створити стійкість до зовнішніх і внутрішніх загроз безпеці.

Таблиця 1

Системи мінімізації ризиків і стійкість до зовнішніх та внутрішніх загроз безпеці

Системи	Дії пом'якшення
Система автоматичної ідентифікації (AIS)	- вся інформація AIS повинна бути перевірена; - необхідно контролювати цілісність інформації, щоб переконатися, що ідентифікація є правильною; - слід враховувати місцеві навігаційні попередження, якщо транслюються помилкові сигнали AIS
Інформаційна система відображення електронних карт (ECDIS)	- розробники ECDIS повинні прагнути прийняти життєві цикли розробки безпеки; - регулярне документування, моніторинг і оновлення структури ECDIS; - необхідно відстежувати та реєструвати оновлення карт ECDIS, особливо оновлення вручну через компакт-диск або USB-диск; - усі файли оновлення слід сканувати антивірусним програмним забезпеченням; - слід перевірити внутрішню мережу, до якої підключено ECDIS, щоб побачити, чи можна систему ECDIS повністю ізолювати або захистити від брандмауера; - лише схвалений персонал повинен мати фізичний доступ до ECDIS та її основних компонентів
GNSS і GPS	- ідентифікація та автентифікація пристрою; - криптографічний захист
Радар	- ідентифікація та автентифікація пристрою; - криптографічний захист; - резервне копіювання інформаційної системи
Промислові системи управління (ICS)	- використовувати криптографію або інші захищені методи, щоб захистити паролі від несанкціонованого перехоплення; - щоб забезпечити безпеку систем керування, запровадити керування конфігурацією та керування виправленнями; - переконатися, що всі підключені до Інтернету пристрої ICS захищені та що паролі регулярно оновлюються; - адміністратори мережі ICS повинні використовувати сегментацію мережі та правила брандмауера, які блокують доступ до обміну файлами; - належним чином захищати файли паролів, ускладнюючи отримання хешованих паролів; - системним адміністраторам слід застосовувати надійні паролі; - використовувати конкретну політику віддаленого доступу; - аудит віддаленого доступу та пов'язаних змін; - блокувати непотрібні порти USB; - переконатися, що для всіх користувачів було проведено навчання з питань кібербезпеки
Системи керування силовими установками та механізмами та управління потужністю	- резервне копіювання інформаційної системи; - захист від відмови в обслуговуванні; - контроль фізичного доступу

Very Small Aperture Terminal (VSAT)	- слід розглянути зашифровані системи зв'язку; - необхідно ретельно розглянути механізми кіберзахисту постачальника послуг, але не слід покладатися на них виключно для захисту кожного пристрою та даних; - аутентифікація та управління контролем доступу повинні суворо дотримуватись
IT мережеві системи	- резервне копіювання інформаційної системи; - аутентифікація та контроль доступу; - забезпечити механізми захисту від загроз; - просування системи управління конфігураціями/ виправленнями / оновленнями; - переконатися, що політика BYOD діє; - переконатися, що для всіх користувачів було проведено навчання з питань кібербезпеки
Людський фактор	- сприяти розвитку кібербезпеки в організації; - переконатися, що було проведено навчання з кіберобізнаності; - оцінити ефективність навчання за допомогою вправ з кібербезпеки; - кібергігієна в рамках людського фактору

Оскільки, можливий небезпечний вплив широкомасштабної кібератаки на галузь T&L, на світову торгівлю та економічну стабільність, особливі вимоги ставлять до кращого захисту міжнародної логістики. Потрібно постійно аналізувати не тільки те, що може відбутися, але й те, що вже відбулося. Для цього здійснюється *compromise assessment*, тобто оцінювання рівня скомпрометованості інфраструктури, суть якого полягає в тому, що аналізується вся інфраструктура клієнта за великий проміжок часу, щоб пересвідчитися, що не було несанкціонованого доступу раніше.

Висновки. Одна з найбільших помилок, яку може зробити будь-яка логістична компанія, це відмова від оцінки ризиків безпеки в своїх системах. Основні способи мінімізації ризиків запобігання несанкціонованому доступу в міжнародній логістиці – це навчання співробітників організації, багатофакторна автентифікація (MFA), застосування політики надійних паролів, оновлення програмного забезпечення, періодичне створення резервних копій файлів у хмарі, щоб захистити їх від програм-вимагачів. Також, потрібно проводити комплексний інтегрований план безпеки в міжнародній логістиці, яка допоможе підготуватися до несанкціонованого доступу.

Список використаних джерел

1. Pre-ransomware activities. URL: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
2. Polatidis N/, Pavlidis M., Mouratidis H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. – Computer Standards & Interfaces, Volume 56, February 2018. – P. 74–82. https://doi.org/10.1016/j.csi.2017.09.006
3. Meland P., Bernsmed K., Wille E., Rødseth Ø., Nesheim D. A Retrospective Analysis Of Maritime Cybersecurity Incidents. – TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, 2021. –Volume 15, Issue 3. – P. 519-530. https://doi.org/10.12716/1001.15.03.04

Робота виконана під науковим керівництвом канд. техн. наук, доцента САВЧЕНКО Т.В.

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ КОРИСТУВАЧІВ ІНТЕРНЕТУ

ШАПРАН О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Роботу присвячено актуальній проблемі інформаційної безпеки в середовищі Інтернет. З розвитком технологій та підвищеним поляганням на інформаційні технології для збереження, обробки, та використання конфіденційної інформації та збільшенням обчислювальних потужностей комп'ютерних систем, традиційні методи авторизації користувачів у веб додатках потребують перегляду та оновлення для забезпечення безпеки та довіри до комп'ютерних систем. В роботі розглянуто визначення, будову, переваги та недоліки використання двофакторної автентифікації, її вплив на сучасні веб-додатки. Було розглянуто перспективи використання біометричних та інших видів підтвердження особистості (eToken) як можливий фактор захисту подальшого розвитку систем багатофакторної автентифікації.

The paper is dedicated to the pressing issue of information security in the Internet environment. With the advancement of technology and increased reliance on information technologies for the storage, processing, and utilization of confidential information, as well as the increase in computational power of computer systems, traditional methods of user authorization in web applications require review and updating to ensure security in online systems. The paper provides an overview of the definition, structure, advantages, and disadvantages of using two-factor authentication (2FA) and its impact on modern web applications. The prospects of using biometric and other types of identity verification (eToken) as a possible factor for enhancing the security of multi-factor authentication systems have been examined and analysed.

Актуальність теми: зростання кількості інтернет-шахраїв та кібератак призводить до необхідності підвищення рівня безпеки користувачів. Одним з способів забезпечення безпеки є використання двофакторної аутентифікації, яка забезпечує використання двох незалежних механізмів для підтвердження ідентичності користувача.

Метою нашої наукової статті є опис двофакторної аутентифікації як способу підвищення безпеки користувачів Інтернету та дослідити її ефективність в порівнянні з іншими методами аутентифікації.

Об'єктом нашого дослідження є безпека користувачів Інтернету.

Предмет дослідження: двофакторна аутентифікація як спосіб підвищення безпеки користувачів Інтернету.

Аналіз попередніх досліджень: попередні дослідження показують, що традиційні методи аутентифікації, такі як введення логіну та пароля, не забезпечують достатнього рівня безпеки. Також дослідження показують, що використання двофакторної аутентифікації може підвищити рівень безпеки користувачів, оскільки вона забезпечує використання двох незалежних механізмів для підтвердження ідентичності користувача. Дослідження також показують, що рівень безпеки може бути підвищений, якщо один з механізмів двофакторної аутентифікації використовує фізичні або біометричні дані, такі як відбиток пальця або обличчя.Виклад основного матеріалу.У XXI столітті Інтернет перетворився на основний спосіб зв'язку сучасного життя. Сучасний образ світу формується в кореляції з посиленням творчого потенціалу людини і можливостями цифрових технологій, мережі Інтернету, штучного інтелекту, численних медійних продуктів. Водночас образ сучасної людини формується в контексті доступу до мережі, інтернету речей, володіння і використання гаджетів, поєднання людського і штучного інтелекту тощо (Кремень В., Биков В., Ляшенко О. та ін., 2022, с. 2-3). Поява комп'ютерних технологій і активна диджиталізація суспільства

створили суспільний попит на методи автентифікації, засновані не лише на традиційних криптографічних способах (шифрування, гешування, цифровий підпис), а й на використанні декількох чинників, що забезпечують достовірність особи і активізують проблему безпеки користувачів. *Двофакторна автентифікація – це метод ідентифікації*, що вимагає від користувача надання двох даних, щоб отримати доступ і увійти у обліковий запис. Це може бути СМС на номер телефону або код з листа на адресу електронної пошти, відповідь на якесь секретне питання, або ж біометрична ідентифікація. *Отже, двофакторна автентифікація* (2FA – Two-Factor authentication) вимагає користувача підтвердити свою особу двічі, за допомогою двох різних джерел, що підвищує безпеку та захищає конфіденційні дані.

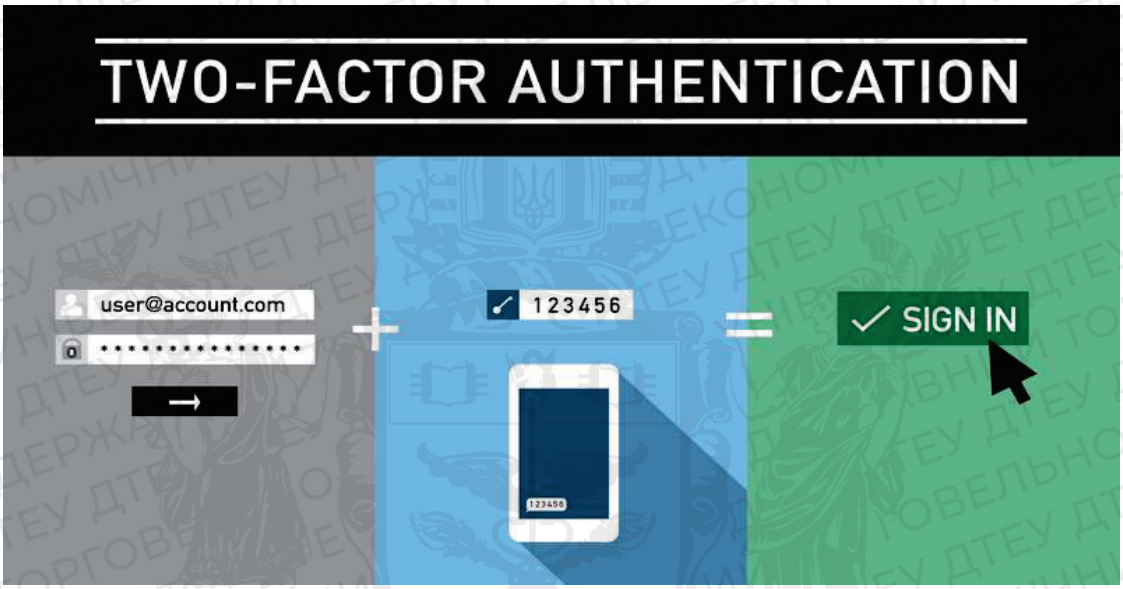


Рис. 1. Схема автентифікації з використанням 2FA, вигляд для користувача

Тобто, для того щоб увійти, наприклад, в свій електронний кабінет, користувач вводить всій логін та пароль, як прийнято на більшості веб-сервісів. Але додатково після цього проходить перевірка з іншого джерела, наприклад введення коду із СМС на номер телефону що користувач вказав при реєстрації.

Зазначений метод 2FA зазвичай різко знижує можливість крадіжки особистих даних онлайн, так як знання лише пароля недостатньо для здійснення електронного шахрайства, оскільки йде перевірка з іншого, незалежного джерела, до якого в них немає доступу.

Тим не менш, двохфакторні підходи аутентифікації залишаються уразливими для атак типу «фішинг» та «людина посередині» (Man-in-the-middle attack). На сьогоднішній день, найпопулярнішим методом реалізації 2FA є *пароль користувача та SMS із перевірочними кодами*, що генеруються за технологією OTP (One Time Password) й відправляються на смартфон користувачу. Впевненість у надійності методу 2FA обумовлюють його застосування для найвідповідальніших операцій – від авторизації в Google (*доступ до пошти, хмарного сховища, контактів і всієї інформації користувача, в тому числі конфіденційної*) до систем онлайн банкінгу та підтвердження здійснення переказу грошей.

М. Маркіна зазначає, що Національний Інститут стандартів і технологій США (The National Institute of Standards and Technology, NIST) оприлюднив влітку 2016 року попередню версію майбутнього Digital Authentication Guideline з критикою популярного підходу SMS OTP. Основні побоювання експертів Національного інституту стандартів і технологій зводилися до того, що номер телефону може бути прив'язаний до VoIP сервісу. Окрім цього, зловмисники можуть спробувати переконати постачальника послуг у зміні номеру телефону і таким чином отримати код доступу. Хоча документ рекомендує виробникам використовувати в своїх додатках токени і криптографічні ідентифікатори, автори поправок також відзначають, що «смартфон або інший мобільний пристрій завжди можуть бути вкрадені, або можуть

тимчасово перебувати в руках іншої людини» – йдеться в документі NIST. Вчені з Амстердамського університету Р. К. Конотом (R. K. Konoth), В. ван дер Вен (V. van der Veen) і Г. Бос (H. Bos) продемонстрували атаку з використанням установки уразливого додатку через Google Play. Їм вдалося успішно обійти перевірку Google Bouncer і активувати додаток для перехоплення одноразових паролів (Маркіна, 2020, с. 87-88). Отже, недоліком двофакторної аутентифікації є те, шо зловмисник може підібрати пароль користувача і перехопити SMS-повідомлення зі згенерованим кодом.

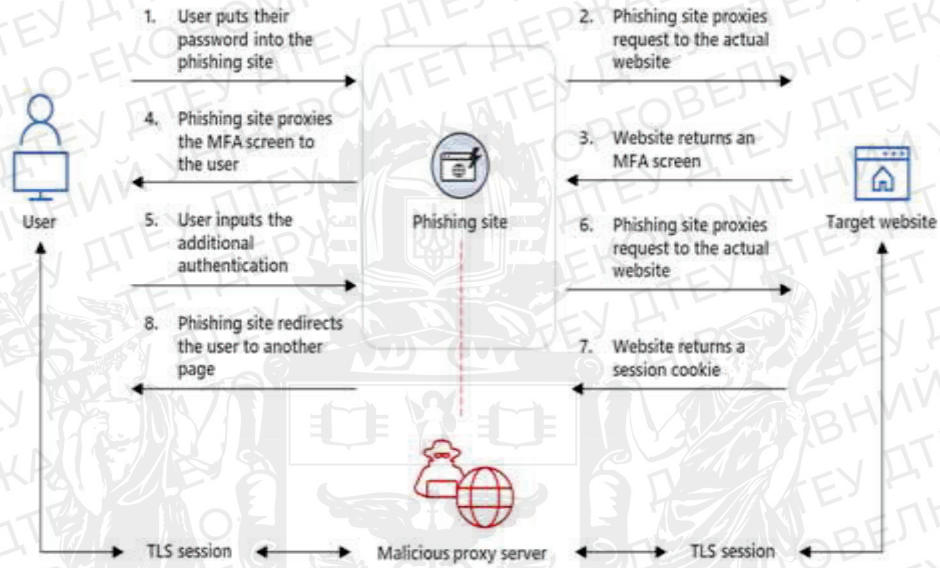


Рис.2. Схема зламу захисту 2FA за допомогою липового сайту (фішингу)

Як працює фішинг: хакери можуть розмістити липовий веб-сервіс та надіслати листа на електрону пошту користувача з проханням негайно переглянути якусь інформацію. Якщо користувач поведеться та натисне на посилання він попаде на сайт хакерів з аналогічним оформленням до справжнього. Ввівши свій пароль та логін, сайт правдоподібно попросить ввести код 2FA. Таким чином хакери ненадовго отримають все необхідні дані для автентифікації на справжньому веб-сервісі та можуть отримати доступ до профілю жертви та вкрасти гроші/інформацію.

Незважаючи на зазначені недоліки 2F-аутентифікації, погоджуємося із думкою В. Балацької, О. Полотая, А. Пузиря, що в першу чергу двофакторну автентифікацію необхідно забезпечити для облікових записів із правами адміністратора та тих, хто має доступ до конфіденційної інформації. Це є потужним кроком до запобігання крадіжці даних і можливим фінансовим втратам (Балацька В., Полотай О., Пузирь А., 2022, с. 290). Цей метод значно підвищує захист від прямих хакерських атак, як-то brute force перебирання паролей та крадіжка логіну та пароля за допомогою зараженого програмного забезпечення.

Двофакторну автентифікацію доволі легко впровадити у вже існуючі веб-сервіси, оскільки для перевірки може використовуватися вже існуюче обладнання, а нова система перевірки може бути доповненням до вже існуючого класичного «Логін+Пароль». Однак для додаткового захисту часто використовують окремі фізичні сервери.

Сервер аутентифікації 2FA генерує короткі коди, унікальні для кожного користувача. При введені коректного логіну та паролю, звичайний сервер веб-додатку дає запит на сервер автентифікації, що в свою чергу генерує унікальний код на надсилає потрібному користувачу. Дуже важливо щоб код мав обмежену кількість часу за яку він може бути використаний, це зробить неможливим крадіжку невикористаного коду для подальшої автентифікації зловмисниками. Якщо код було введено правильно – сервер автентифікації дозволяє серверу веб-додатку обслуговувати користувача та відповідати на запити на особисту інформацію. На

схемі червоними лініями описано як проводиться активація 2FA якщо користувач ще не користується нею.

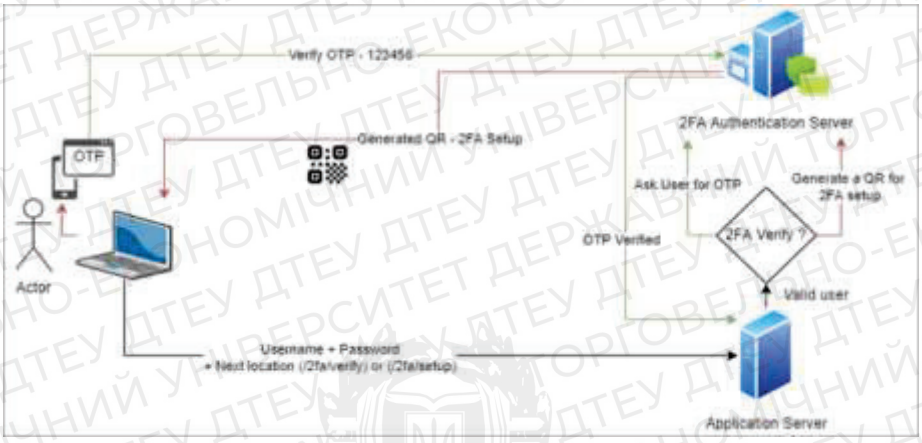


Рис. 3. Блок схема реалізації системи 2FA

Для впровадження автентифікації часто використовуються спеціальні додатки, вони є більш захищеними через неможливість перехопити СМС повідомлення, оскільки в такому випадку код для входу може генеруватися локально на пристрої користувача.

Google Authenticator – мобільний застосунок, що використовується для виконання двофакторної автентифікації, в облікових записах Google та сторонніх сервісах. Реалізований для декількох мобільних платформ, не має можливості ініціалізації на декількох пристроях. Секретний ключ можна інтегрувати в застосунок як QR-код, або ввести вручну. Налаштування в застосунку представлені лише засобами синхронізації часу з серверами Google. Автентифікатор генерує 6-ти або 8-мизначний одноразовий пароль, з використанням відкритих стандартів алгоритмів HOTP та TOTP. Дані паролі використовуються у якості другого фактору автентифікації і застосовуються після коректного введення логіну та паролю. Пароль дійсний протягом 30 секунд, що запобігає використанню його кілька разів. *Microsoft Authenticator* – мобільний застосунок, який допомагає входити в облікові записи, виконуючи двофакторну автентифікацію. Працює із будь-яким обліковим записом, який використовує двофакторну автентифікацію та підтримує одноразові паролі (TOTP). В якості генератора кодів Microsoft Authenticator обирає шестизначний пароль, який відображається під кожним доданим обліковим записом. Пароль дійсний протягом 30 секунд, що запобігає використанню коду кілька разів. Ініціалізація облікового запису проходить шляхом сканування QR-коду, або введення коду вручну. Не має можливості ініціалізувати один обліковий запис в декількох застосунках на різних пристроях одночасно (Самара Н., Бурак Н., с.55-56). Таким чином, такі компанії-гіганти як Google та Microsoft надають впевненість у коректності та стійкості обраних факторів автентифікації.

Окрім того, двофакторна автентифікація буває *різних видів*: парольна, апаратна, eToken та ін. Найбільш досконалою системою вважається *біометрична автентифікація*, тому що спирається на фізичні властивості окремого індивіда чи групи людей. Біометрична автентифікація загалом є покращеною версією парольної, тільки замість паролю чи PIN-коду користувач «вводить» свої фізичні параметри. Вона є досить легкою у використанні, але складною у побудові та затратах на неї. У *біометричній автентифікації* використовуються*:* відбитки пальців; геометрична форма кисті руки; форма і розміри особи; особливості голосу; візерунок райдужної оболонки і сітківки очей та ін. (Канівець В. , Сомов С., 2018). Найбільшого поширення набули дактилоскопічні системи автентифікації, які засновані на великих банках даних відбитків пальців і забезпечують захищений доступ до комп'ютерів, вхідних дверей, автомобілів, банкоматів тощо, а також системи автентифікації за обличчями і голосами, оскільки більшість сучасних електронних пристроїв мають відео- і аудіо засоби. Однак, технології розпізнавання рис обличчя вимагають подальшого вдосконалення, бо

залежать від коливань в освітленні, що впливає на пізнаваність особи. Системи автентифікації за голосом спираються на такі його особливості як висота, модуляція і частота звуку, що є унікальними характеристиками для кожної людини й більш піддаються верифікації.

Таким чином, інформаційна безпека знаходиться в руках користувача, який дотримується певних правил і самостійно використовує доступні рішення для захисту облікових даних. Двофакторна автентифікація (2FA) для підвищення безпеки користувачів Інтернету підходить для ресурсів, на яких зберігається менш чутлива, з точки зору конфіденційності, інформація та для віддалених ресурсів шляхом подвійного підтвердження власної особи. Для впровадження автентифікації використовуються спеціальні сервіси *(Google Authenticator, Microsoft Authenticator).* Двофакторна автентифікація буває різних видів: парольна, апаратна, eToken та ін. Найбільш досконалою системою вважається біометрична автентифікація, що можна використовувати для аутентифікації користувачів на локальних пристроях або в корпоративній мережі. Важливим фактором забезпечення захищеності інформації є своєчасне залучення новітніх інструментів і засобів безпеки

Список використаних джерел

1. Балацька В., Полотай О., Пузир А. Автентифікація, як один з механізмів забезпечення безпеки операційних систем. *Інформаційна безпека та інформаційні технології*: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. Львів: Растр-7, 2022. С. 288-290.
2. Брухнов Д. А., Азарова А. О. Забезпечення захищеної авторизації на основі двофакторної автентифікації зі змінним ключем та захистом від Brute Force. Матеріали L науково-технічної конференції підрозділів ВНТУ, (Вінниця, 10-12 березня 2021 р.). URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2021/paper/view/12495.
3. Канівець В. Г., Сомов С. В. Автентифікація користувачів комп'ютерних систем. *Новітні інформаційні системи та технології*. 2018. Вип. 9. URL: http://reposit.nupp.edu.ua/bitstream/PoltNTU/4489/1/1046-%d0%a2%d0%b5%d0%ba%d1%81%d1%82%20%d1%81%d1%82%d0%b0%d1%82%d1%82%d1%96-1983-1-10-20180721.pdf
4. Кремень В. Г., Биков В. Ю., Ляшенко О. І., Литвинова С. Г., Луговий В. І., Мальований Ю. І., Пінчук О. П., & Топузов О. М. Науково-методичне забезпечення цифровізації освіти україни: стан, проблеми, перспективи: наукова доповідь загальним зборам НАПН України «Науково-методичне забезпечення цифровізації освіти України: стан, проблеми, перспективи», 18-19 листопада 2022 р. *Вісник Національної академії педагогічних наук України*. 2022. №4(2). С. 1-49. URL: https://doi.org/10.37472/v.naes.2022.4223
5. Маркіна М.В. Використання трифакторної або двофакторної аутентифікації: переваги і недоліки, вибір оптимального варіанту. *Проблеми використання інформаційних технологій в освіті, науці та промисловості* : XIV міжнар. конф. (28-29 листоп. 2019 р.) : зб. наук. пр. / ред. кол.: Г.Г. Півняк та ін.; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». Дніпро : НТУ «ДП», 2020. № 4. С. 86-89.
6. Самара Н. М., Бурак Н. Є. Аналіз принципів реалізації методів двофакторної автентифікації в сучасних програмних додатках. *Інформаційна безпека та інформаційні технології*: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, С. 54-56.

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д.О.

МЕТОДИ ОТРИМАННЯ ЦИФРОВИХ ДОКАЗІВ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ ЗА ДОПОМОГОЮ КРИМІНАЛІСТИЧНИХ ІНСТРУМЕНТІВ

ШАЯХМЕТОВА О., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуті основні методи цифрового криміналістичного аналізу та протоколи обробки цифрових доказів. Зазначено переваги застосування певних програмних продуктів для дослідження цифрових доказів. Проведене розслідування місця злочину, на якому за допомогою певного програмного забезпечення були відновлені знищені цифрові докази.

The article discusses the main methods of digital forensic analysis and digital evidence processing protocols. The advantages of using certain software products for researching digital evidence are indicated. Conducted a crime scene investigation where destroyed digital evidence was recovered using certain software products.

Актуальність. Злочини з використанням комп'ютерів зростають стрімкими темпами. Такі злочини можуть варіюватися від злому та кібератак до крадіжок ідентичності та шахрайства. Оскільки комп’ютерні злочини досягли високого рівня, інструменти, які використовуються для боротьби з такими злочинами, розвиваються швидше. У порівнянні з іншими судово-медичними науками галузь цифрової криміналістики відносно молода, але також стала життєво важливою для розкриття комп'ютерних злочинів.

Цифрова криміналістика – це покроковий процес наукових методів і прийомів розслідування злочинів, отриманих із цифрових доказів, які можуть бути нестабільними та крихкими, і неправильне поводження з ними може змінити їх. Через свою мінливість і крихкість необхідно дотримуватися протоколів, щоб гарантувати, що дані не змінюються під час їх обробки (тобто під час доступу, збору, пакування, передачі та зберігання). Ці протоколи визначають кроки, яких слід дотримуватись під час роботи з цифровими доказами. Використання відповідних методів збору та захисту електронних доказів сприяло б цифровій криміналістиці та законодавству про інформаційні технології.

Докази для обговорення в суді часто збираються завдяки навичкам цифрових судових експертів, які можуть витягувати важливі дані з електронних пристроїв, що належать потерпілим сторонам. Для дослідження цифрових доказів та притягнення до відповідальності існує багато цифрових криміналістичних інструментів, які використовуються для розслідування цифрових злочинів шляхом ідентифікації цифрових доказів.

У цьому дослідженні основний акцент буде зроблено на процесі цифрової криміналістики, а також на програмному забезпеченні, яке використовується під час цієї процедури.

Метою статті є надати огляд комп’ютерної криміналістики та методів та вивчення протоколів, які застосовуються для отримання та обробки цифрових доказів із комп’ютерних систем для аналізу інформації, яка використовується у кримінальних розслідуваннях з метою потенціального вирішення злочину.

Об'єктом дослідження є вивчення методів отримання та протоколів обробки цифрових доказів.

Предметом дослідження є методи та протоколи обробки цифрових доказів.

Аналіз попередніх досліджень. Дослідженню методів отримання цифрових доказів, протоколів їх обробки та основних програмних продуктів присвячені праці вітчизняних та закордонних науковців: Білл Нельсон, Амелія Філліпс, Крістофер Стюарт, Майкл Бойл, Жан-Клод Вульєрме

Виклад основного матеріалу. Оскільки все більше і більше користувачів переходять на мобільні пристрої та використовують взаємопов'язані пристрої, комп'ютери часто стають центром інцидентів і розслідувань. Сучасні аналітики комп'ютерної криміналістики здатні відновлювати дані, які були видалені, зашифровані або приховані у різних пристроях; їх можна викликати для дачі свідків у суді та розповісти про докази, знайдені під час розслідування. Вони можуть брати участь у складних справах, включаючи перевірку алібі правопорушників, перевірку зловживань Інтернетом, зловживання комп'ютерними ресурсами та використання мережі для створення комп'ютерних загроз. Експертів-криміналістів можна залучити для супроводу серйозних справ, пов'язаних із витоком даних, вторгненням або будь-яким іншим типом інцидентів. Застосовуючи методи та власне програмне забезпечення для криміналістичної експертизи для дослідження системних пристроїв або платформ, вони могли б надати ключові відкриття, щоб визначити, хто був відповідальним за розслідуваний злочин.

Метою комп'ютерної криміналістичної експертизи є відновлення даних з комп'ютерів, вилучених як доказ у кримінальному розслідуванні. Експерти використовують системний підхід до дослідження доказів, які можуть бути представлені в суді під час провадження. Залучення судово-медичних експертів має бути на ранніх стадіях розслідування, оскільки вони можуть допомогти правильно зібрати технічний матеріал таким чином, щоб відновити вміст без будь-яких пошкоджень його цілісності.

Першим кроком у будь-якому криміналістичному процесі є перевірка всього апаратного та програмного забезпечення, щоб переконатися, що вони працюють належним чином. У спільноті криміналістів все ще точаться дискусії щодо того, як часто слід тестувати програмне забезпечення та обладнання. Більшість людей погоджуються з тим, що, як мінімум, організації повинні перевіряти кожен елемент програмного та апаратного забезпечення після його придбання та перед використанням. Їм також слід повторити тестування після будь-якого оновлення, виправлення або зміни конфігурації.

Криміналістичне розслідування полягає у зборі комп'ютерної криміналістичної інформації; процес можна розпочати з аналізу мережевого трафіку за допомогою аналізатора пакетів або інструменту сніфера, такого як Wireshark, який здатний перехоплювати трафік і реєструвати його для подальшого аналізу. NetworkMiner, ще один інструмент аналізу мережі (NFAT), є альтернативою Wireshark для вилучення або відновлення всіх файлів. Натомість Snort є цінним інструментом для відстеження мережевих зловмисників у реальному часі.

Програмне забезпечення NFAT також містить криміналістичні можливості, виконуючи аналіз збереженого мережевого трафіку, як випливає з його назви. Що стосується реагування на інциденти та ідентифікації, для ідентифікації видалених файлів і їх відновлення можна використовувати Forensic Toolkit або FTK; в той час, як EnCase підходить для криміналістики, кібербезпеки та електронного пошуку.

Коли платформа криміналістичної експертизи готова, спеціаліст дублює криміналістичні дані, надані в запиті, і перевіряє їх цілісність. Цей процес передбачає, що правоохоронні органи вже отримали дані за допомогою відповідного судового процесу та створили криміналістичне зображення. Криміналістичне зображення – це побітова копія даних, які існують на оригінальному носії, без будь-яких додавання чи видалення. Також передбачається, що судово-медичний експерт отримав робочу копію вилучених даних. Якщо експерти отримують оригінали доказів, вони повинні зробити робочу копію та стежити за ланцюгом зберігання оригіналу. Експерти перевіряють, чи копія, якою вони володіють, є цілою та незмінною. Зазвичай вони роблять це, перевіряючи хеш або цифровий відбиток доказів. У разі виникнення проблем екзаменатори консультуються із заявником щодо подальших дій.

Після того як експерти перевірять цілісність даних, що підлягають аналізу, розробляється план вилучення даних. Вони організовують і уточнюють судово-медичний запит на питання, які вони розуміють і на які можуть відповісти. Вибрано криміналістичні інструменти, які дозволяють їм відповісти на ці запитання. Екзаменатори, як правило, мають попередні ідеї щодо того, що шукати, на основі запиту. Вони додають їх до «Списку

пошукових запитів», який є поточним списком запитуваних елементів [2]. У моєму випадку, запит надає лід: «пошук особистих даних».

Для кожного пошукового запиту експерти виділяють відповідні дані та позначають цей пошуковий запит як «оброблений» або «готовий». Вони додають будь-що вилучене до другого списку, який називається «Список вилучених даних». Екзаменатори переслідують усі пошукові запити, додаючи результати до цього другого списку. Потім вони переходять до наступного етапу методології – ідентифікації (рис.1).

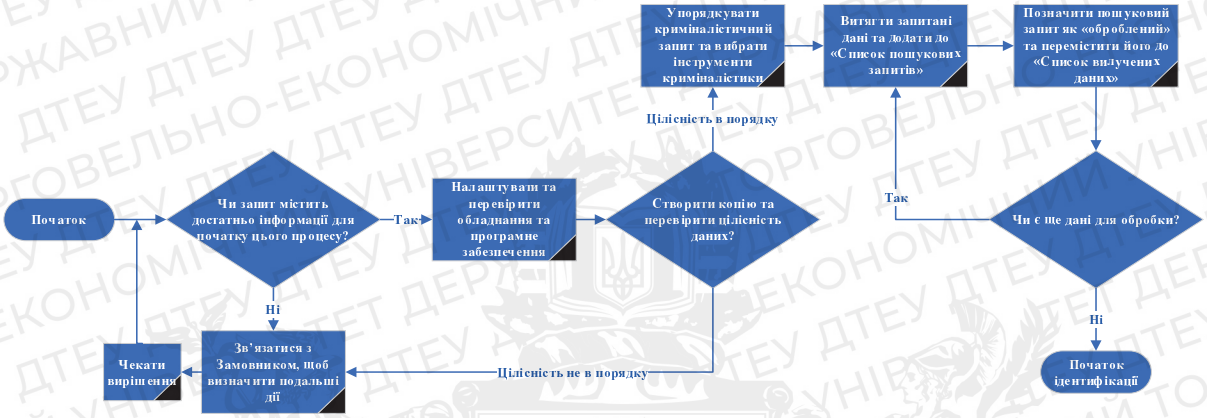


Рис. 1. Підготовка цифрових даних до їх подальшої ідентифікації

На етапі ідентифікації отримується попередня інформація про справу про кіберзлочин. Ця попередня інформація подібна до тієї, яку шукають під час традиційного кримінального розслідування. Слідчий прагне відповісти на наступні питання: Хто брав участь? Що сталося? Коли стався кіберзлочин? Де стався кіберзлочин? Як стався кіберзлочин?

Відповіді на ці запитання дадуть слідчим рекомендації щодо того, як продовжувати справу. Наприклад, відповідь на питання "де стався цей злочин?" - тобто в межах або за межами кордонів країни - інформуватиме слідчого про те, як продовжити справу (наприклад, які органи слід залучити).

Але місце злочину не обмежується фізичним розташуванням цифрових пристроїв, які використовувалися під час скоєння кіберзлочинів та які були метою кіберзлочину. Місце злочину в кіберзлочині також включає цифрові пристрої, які потенційно містять цифрові докази, і охоплює кілька цифрових пристроїв, систем і серверів. Місце злочину охороняється, коли кіберзлочин спостерігається, повідомляється та підозрюється. Користувачам не можна надавати можливість далі керувати цифровими пристроями. Слідчий проводить огляд місця злочину та виявляє докази. Перед збором доказів проводиться документування місця злочину. Документація необхідна протягом усього процесу розслідування (до, під час і після отримання доказів). Ця документація повинна містити детальну інформацію про зібрані цифрові пристрої, включаючи робочий стан пристрою – увімкнено, вимкнено, режим очікування – та його фізичні характеристики, такі як марка, модель, серійний номер, з'єднання та будь-які позначки чи інші пошкодження. Окрім письмових нотаток, для документування місця злочину та доказів також необхідні ескізи, фотографії та відеозаписи місця злочину та доказів. На етапі ідентифікації слідчі кіберзлочинів використовують багато традиційних методів розслідування, особливо щодо збору інформації та доказів. Наприклад, жертви, свідки та підозрювані в кіберзлочині опитуються для збору інформації та доказів кіберзлочину, який розслідується. Фактичний збір доказів передбачає збереження летючих доказів і відключення цифрових пристроїв.

Перш ніж розпочати збір цифрових доказів, слідчий повинен визначити типи доказів, які шукаються. Якщо вони не мають відношення до судового запиту, вони просто позначають їх як оброблений і йдуть далі. Якщо об'єкт має відношення до судово-медичного запиту, експерти документують його в третьому списку, списку відповідних даних. Цей список є набором даних, які стосуються відповіді на оригінальний судово-медичний запит. Цифрові

докази можна знайти на цифрових пристроях, таких як комп'ютери, зовнішні жорсткі диски, флеш-накопичувачі, маршрутизатори, смартфони, планшети, камери, смарт-телевізори, побутова техніка з підключенням до Інтернету (наприклад, холодильники та пральні машини) та ігрові консолі, а також загальнодоступні ресурси (наприклад, платформи соціальних медіа, веб-сайти та дискусійні форуми) і приватні ресурси (наприклад, журнали активності користувачів постачальників послуг Інтернету; бізнес-записи постачальників послуг зв'язку; записи про дії користувачів постачальників хмарних сховищ). Багато програм, веб-сайтів і цифрових пристроїв використовують служби хмарного зберігання. користувачів Таким чином, дані можуть зберігатися повністю або фрагментарно різними постачальниками на серверах у багатьох місцях. Через це отримати дані є складним завданням. Докази, які шукаються, залежатимуть від розслідуваного кіберзлочину. Якщо кіберзлочин, який розслідується, є шахрайством із ідентифікацією, тоді вилучені цифрові пристрої шукатимуть докази цього злочину (наприклад, докази шахрайських транзакцій).

У моїй справі про крадіжку особистих даних відповідні дані можуть включати номери соціального страхування, зображення фальшивих ідентифікаторів або електронні листи з обговоренням крадіжки особистих даних, серед іншого. Також можливо, що елемент генерує ще одного пошукового запиту. Електронний лист може виявити, що мета використовувала інший псевдонім. Це призведе до нового пошуку за ключовим словом для нового псевдоніма. Екзаменатори повертаються і додають цей підхід до списку пошукових запитів, щоб вони не забули його повністю дослідити.

Елемент також може вказувати на абсолютно нове потенційне джерело даних. Наприклад, екзаменатори можуть знайти новий обліковий запис електронної пошти, який використовував ціль. Після цього відкриття правоохоронні органи, можливо, захочуть отримати повістку про вміст нового облікового запису електронної пошти. Експерти також можуть знайти докази, що вказують на цільові файли, що зберігаються на знімному накопичувачі з універсальною послідовною шиною (USB), якого правоохоронні органи не знайшли під час початкового пошуку. За цих обставин правоохоронні органи можуть розглянути питання про отримання нового ордера на обшук для пошуку USB-накопичувача. Судово-медична експертиза може вказати на багато різних типів нових доказів. Деякі інші приклади включають журнали брандмауера, журнали доступу до будівлі та запис відеозапису безпеки. Експерти документують їх у четвертому списку, списку нових джерел даних.

Після обробки списку витягнутих даних експерти повертаються до будь-яких нових розроблених потенційних клієнтів. Для будь-яких нових джерел пошуку даних експерти розглядають можливість повернення до етапу вилучення для їх обробки. Подібним чином, для будь-якого нового джерела даних, яке може призвести до нових доказів, експерти розглядають можливість повернутися до процесу отримання та зображення цих нових судово-медичних даних.

На цьому етапі процесу експертам доцільно повідомити запитувача про свої початкові висновки. Це також гарний час для перевіряючих і тих, хто запитує, щоб обговорити, якою, на їхню думку, буде віддача від інвестицій для пошуку нових потенційних клієнтів. Залежно від стадії справи, витягнуті та ідентифіковані відповідні дані можуть надати запитувачу достатньо інформації для просування справи, і експертам може не знадобитися виконувати подальшу роботу (рис. 2). Але у справі про викрадення особистих даних, експерт відновлює недостатню кількість файлів в яких містяться особисті дані, тому експерти переходять до наступного кроку, аналізу.

На етапі аналізу екзаменатори з'єднують усі крапки та малюють для запитувача повну картину. Для кожного елемента в списку релевантних даних екзаменатори відповідають на такі запитання, як хто, що, коли, де та як. Вони намагаються пояснити, який користувач або програма створив, редагував, отримав або надіслав кожен елемент, і як він спочатку з'явився. Також експерти пояснюють, де його знайшли. Найголовніше, вони пояснюють, чому вся ця інформація є важливою і яке значення вона має для справи.

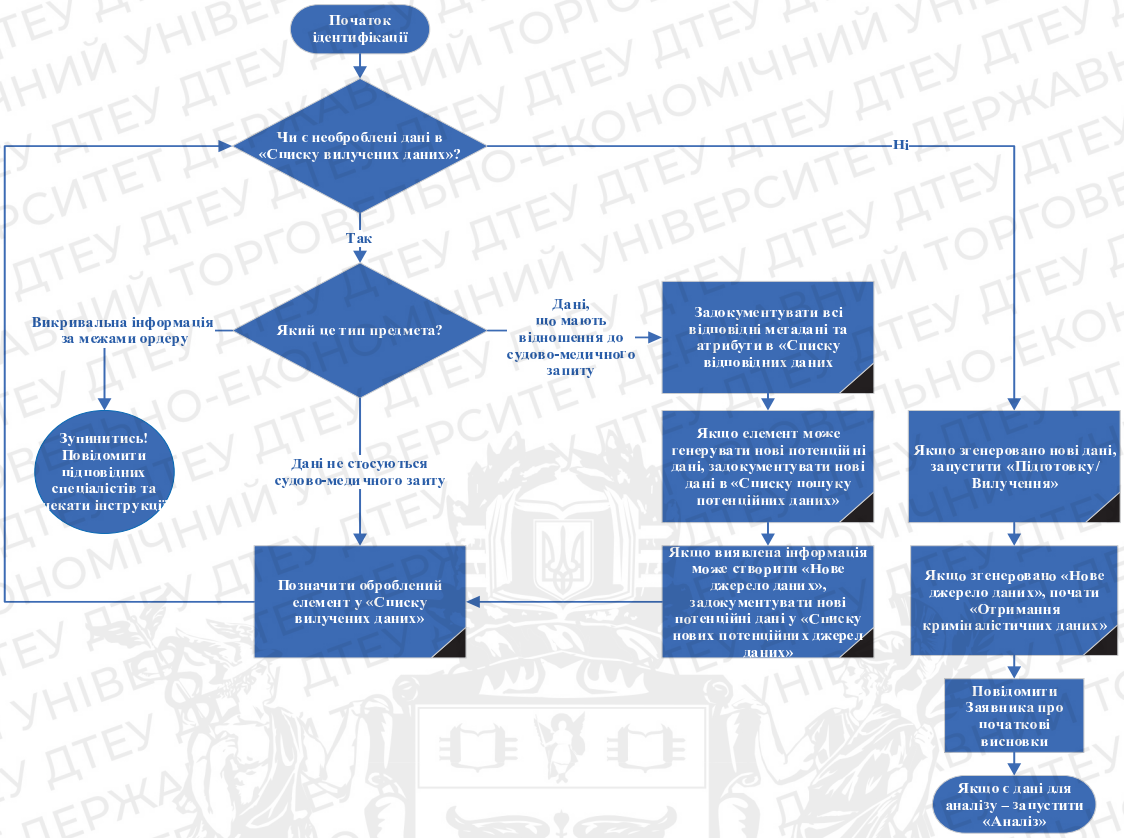


Рис. 2. Процес ідентифікації цифрових даних

Загалом існує декілька типів аналізу, які можна виконувати на комп'ютерах:

Аналіз часових рамок має на меті створити часову шкалу або часову послідовність дій за допомогою позначок часу (дата й час), які призвели до події, або визначити час і дату, коли користувач виконав певну дію. Цей аналіз виконується для приписування злочину злочинцю або принаймні дії, яка призвела до злочину, конкретній особі. Наприклад, історія веб-браузера показує відвідування сайтів і час їх відвідування. Потрібні додаткові докази, щоб показати, що особа, чиї цифрові докази використовувалися для доступу до цих веб-сайтів, була власником та/або підозрюваним користувачем пристрою.

Аналіз власності та володіння використовується для визначення особи, яка створила, отримала доступ та/або змінила файли в комп'ютерній системі. Наприклад, цей аналіз може виявити зображення матеріалів сексуального насильства над дітьми (тобто «зображення будь-якими способами дитини, яка бере участь у справжніх чи імітованих відвертих сексуальних діях, або зображення статевих частин дитини переважно з сексуальною метою»; Стаття 2 Факультативного протоколу ООН до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції та дитячої порнографії 2000 року) на пристрої підозрюваного [1]. Лише цієї інформації недостатньо, щоб підтвердити право власності на матеріали сексуального насильства над дітьми. Щоб підтвердити це, потрібні додаткові докази, наприклад ексклюзивне використання комп'ютера, де було знайдено матеріал.

Аналіз додатків і файлів виконується для перевірки додатків і файлів у комп'ютерній системі, щоб визначити знання зловмисника, намір і можливості вчинити кіберзлочин (наприклад, мітка або назва файлу може вказувати на вміст файлу; наприклад, ім'я файлу може бути ім'ям жертви кіберзлочину).

Також можна виконати аналіз приховування даних. Як випливає з назви, аналіз приховування даних шукає приховані дані в системі. Злочинці використовують кілька методів приховування даних, щоб приховати свою незаконну діяльність та ідентифікаційну інформацію, як-от використання шифрування, пристрої, що захищають паролем, і певний вміст (наприклад, файли), зміна розширень файлів і приховування розділів. Під час фази

аналізу слідчому необхідно розглянути методи приховування даних, які злочинці могли використати, щоб приховати свою особу та діяльність. Приховані дані можуть виявити «обізнаність [про злочин], право власності [контент] або намір [вчинити злочин]».

Аналіз видалених файлів. Коли файл видаляється на комп'ютері, він поміщається в корзину або кошик. Якщо кошик або сміттєвий кошик очищається (тобто шляхом видалення вмісту), видалені файли видаляються з таблиці розміщення файлів , яка архівує імена файлів і розташування на жорстких дисках. Простір, де знаходиться файл, позначається як вільний простір (тобто нерозподілений простір) після його видалення, але файл все ще перебуває в цьому просторі (принаймні до тих пір, поки він повністю або частково не буде перезаписаний новими даними).

Метою цих аналізів є реконструкція злочину (або реконструкція події). Реконструкція події має на меті визначити, хто був відповідальним за подію, що сталося, де відбулася подія, коли відбулася подія та як подія розгорталася, за допомогою ідентифікації, зіставлення та зв'язування даних (виявляючи «загальну картину» » або суть події). Реконструкція подій може включати часовий аналіз (тобто визначення часу, коли відбулися події та послідовності цих подій), реляційний аналіз (тобто визначення залучених осіб і того, що вони робили, а також асоціації та відносини між цими особами) і функціональний аналіз (тобто оцінка продуктивності та можливостей систем і пристроїв, залучених до подій).

Часто екзаменатори можуть провести найцінніший аналіз, дивлячись на те, коли все сталося, і створюючи часову шкалу, яка розповідає послідовну історію. Для кожного відповідного елемента екзаменатори намагаються пояснити, коли його було створено, доступно, змінено, отримано, надіслано, переглянуто, видалено та запущено. Вони спостерігають і пояснюють послідовність подій і відзначають, які події відбулися одночасно.

Експерти документують усі свої аналізи та іншу інформацію, що стосується судово-медичного запиту, і додають усе це до п'ятого й останнього списку, «Списку результатів аналізу». Це список усіх значущих даних, які відповідають на запитання, хто, що, коли, де, як та інші. Інформація в цьому списку відповідає вимогам судово-медичної експертизи. Навіть на цій пізній стадії процесу щось може створити нові джерела пошуку даних або джерело даних. Якщо це станеться, екзаменатори додадуть їх до відповідних списків і розглянуть можливість повернутися, щоб перевірити їх повністю.

Нарешті, після того, як експерти пройдуть ці кроки достатньо разів, вони можуть відповісти на судово-медичний запит, переходять до фази судово-медичної експертизи. Це крок, на якому експерти документують висновки, щоб заявник міг зрозуміти їх і використати у справі. Звітність судової експертизи виходить за межі цієї статті, але її важливість важко переоцінити. Остаточний звіт є найкращим способом для експертів повідомити результати запитувачу. Звіти мають бути максимально чіткими та точними. Необхідно включити демонстраційний матеріал (наприклад, малюнки, графіки, результати інструментів) і підтверджуючі документи, такі як документація про ланцюжок поставок, а також детальне пояснення використаних методів і кроків, вжитих для вивчення та вилучення даних. Висновки слід пояснювати з урахуванням цілей аналізу (тобто мети розслідування та справи, яка розслідується). Інформація про обмеження висновків також має бути включена до звіту. Після звіту запитувач проводить аналіз на рівні справи, де спеціаліст інтерпретує висновки в контексті всієї справи (рис. 3).

Отже, вивчивши методи отримання цифрових доказів комп'ютерних злочинів за допомогою криміналістичних інструментів та пройшовши всі етапи розслідування на місці злочину був вилучений ноутбук компанії HP. Ймовірно, на якому були знищені цифрові докази злочину. Попередньо, опитавши потерпілу сторону, можна припускати, що зловмисник викрав її особисті дані.

Для того, щоб знайти цифрові докази скоєного злочину потрібно за допомогою програмного забезпечення для розслідування криміналістичних процесів та живого аналізу OSForensic на ноутбуці зловмисника застосувати аналіз часу, щоб дізнатися які останні дії та в який час зловмисник робив (рис.3) [3].

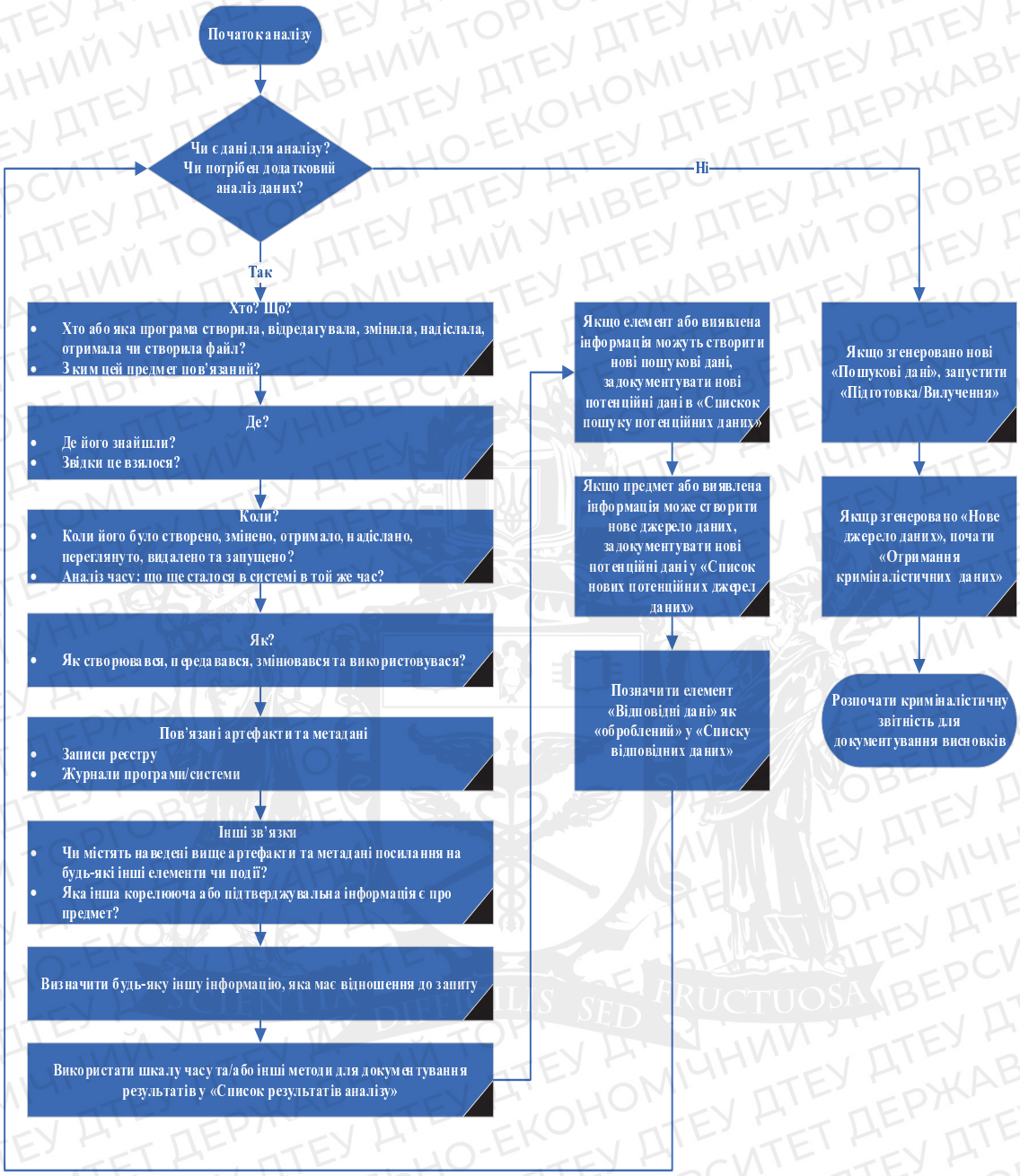


Рис. 3. Процес проведення аналізу послідовності

Перегляшувши усі показники, у видалених файлах була виявлена папка «ФІТ 1-7м паспорти», яка потенційно могла мати особисті дані потерпілих (рис.4). Після відновлення файлів папки «ФІТ 1-7м паспорти» було виявлено 19 файлів формату .docx з іменами потрепілих у яких містилися фотографії їхніх паспортів.

Отже, виявивши цифрові докази на комп'ютері зловмисника за допомогою криміналістичних інструментів та застосуванню аналізу часу та відновленню видалених файлів злочин, в якому були викрадені особисті дані був розкритий.

Висновки. Оскільки кіберзлочини (тобто будь-які кримінальні дії, пов'язані з комп'ютерами та мережами) зростають і загрожують організаційним даним, а також із збільшенням використання цифрових пристроїв широким населенням, аналіз цифрових доказів стає ключовим елементом на багатьох місцях злочину.

Судова експертиза зараз є захоплюючою професією, яка наголошує на людському факторі, але також створює проблеми через необхідність виявлення цифрових доказів у постійно мінливому середовищі. Технологічний прогрес і перехід до мережевих і хмарних

середовищ, де можуть легко вступити в дію антикриміналістичні методи, зобов'язує професіоналів у цій галузі бути в курсі подій і постійно переглядати стандартні операційні процедури.

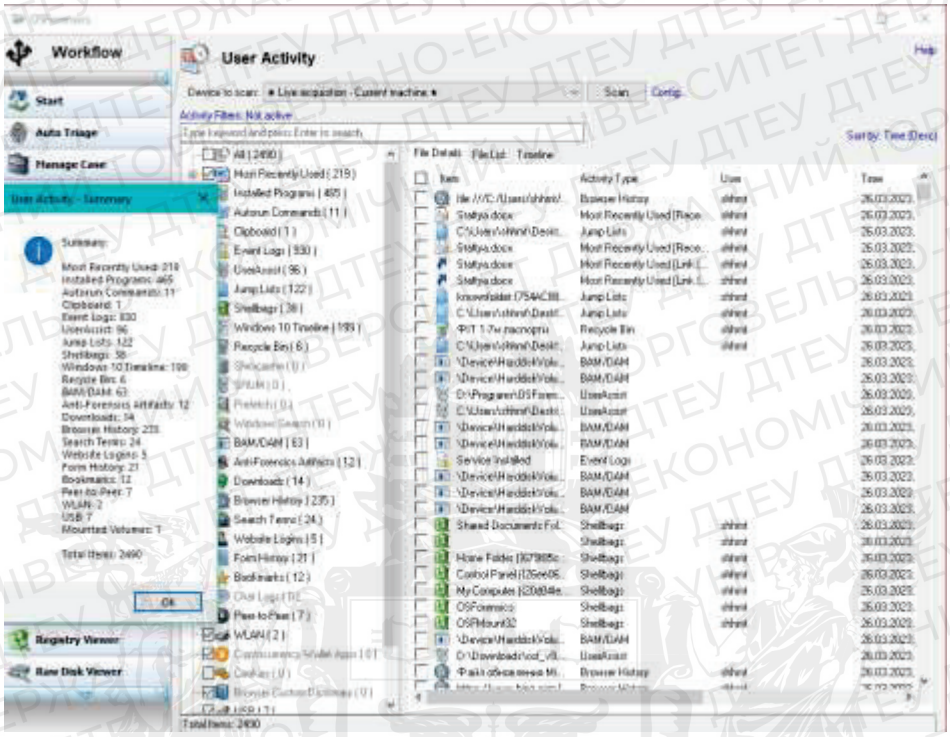


Рис.4. Аналіз часу у програмі OSForensic

Рис.5. Папка «ФІТ 1-7м паспорти»

На закінчення, отримання доказів комп'ютерних злочинів з використанням криміналістичних інструментів - це складний процес, який вимагає спеціалізованих знань та навичок. Використовуючи комбінацію методів, включаючи візуалізацію, відновлення файлів, пошук ключових слів та застосування різних типів аналізів криміналістичні слідчі можуть збирати цінні докази, які можуть бути використані для притягнення до відповідальності за комп'ютерними злочинами. Важливо, щоб криміналістичні розслідування проводилися юридично захищеними для того, щоб забезпечити допустимості докази в суді.

Список використаних джерел

1. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії \\ Режим доступу: https://zakon.rada.gov.ua/laws/show/995_b09#Text
2. Наукова робоча група з цифрових доказів (SWGDE) \\ Режим доступу: https://www.swgde.org/home
3. OSForensics \\ Режим доступу: PassMark OSForensics - Digital investigation

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

ІНФОРМАЦІЙНА СИСТЕМА ІНФРАСТРУКТУРИ ЗВО

ШЕСТАК Я., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови архітектури інформаційної системи освітнього процесу ЗВО для надання користувачам всієї необхідної інформації, а також визначено функції та завдання окремих складових інформаційної системи. Також передбачено заходи щодо захисту інформації.

The article examines the basic principles of building the information system architecture of the educational process of higher educational institutions to provide users with all the necessary information, and also defines the functions and tasks of individual components of the information system. Information protection measures are also provided.

Актуальність. Впродовж 50 років інформатизувалися заклади вищої освіти, створювалися та впроваджувалися різні інформаційні системи, які виконували певні конкретні задачі. Надалі вони модифікувалися, трансформувалися, переходили з одних платформ на інші. Наразі практично всі освітні процеси охоплені окремими інформаційними системами у єдиному освітньому просторі, мають свої задачі та є потреба у їх детальному аналізі, оптимізації та уніфікації .

Метою статті є дослідження архітектури інформаційних систем ЗВО, особливостей їх використання та ефективності функціонування.

Об'єктом дослідження є розробка моделі архітектури інформаційної системи освітнього процесу ЗВО.

Предмет дослідження – інформаційна система ЗВО.

Аналіз попередніх досліджень. Дослідженню інформаційних систем ЗВО, побудові їх архітектури присвятили свої праці вітчизняні та закордонні науковці: М. Цюцюра, О. Криворучко, В. Биков, С. Мазур, В. Співачук, А. Литвинчук, А. Пилипчук та ін.

Виклад основного матеріалу. Інформаційна система ЗВО має багато складових, які постійно удосконалюються, розширюються їх можливості та трансформуються в залежності від потреб суспільства. В процесі цифровізації держави всі процеси автоматизуються та переводяться у цифровий формат, інформація переноситься у ієрархічні та розподілені бази даних. Для ефективного використання користувачами (викладачами, адміністраторами та здобувачами вищої освіти) інформації, яка вже накопичена, зберігається і надалі акумулюється необхідно правильно розподілити ресурси інформаційних систем. Тому, за необхідності, слід побудувати зрозумілі, відкриті і доступні інтерфейси обміну інформацією за допомогою API (спеціальні проміжні таблиці, способи підключень та організація прав доступу, читання, коригування чи знищення інформації). Важливим є організація кібернетичного захисту окремих частин та в цілому інформаційної системи освітнього процесу. Архітектура інформаційної системи має передбачати способи комунікації з зовнішніми інформаційними системами смарт-міста, що дозволить полегшити отримання коректної, вивіреної інформації з її юридичними підтвердженнями, завіреної електронними підписами тощо [2]. Автором запропонована архітектура інформаційної системи освітнього процесу ЗВО зазначена на рис 1. Вона містить ряд окремих автономних інформаційних систем:

- Система освітньої діяльності ЗВО – це інформаційна система, яка виконує функції обміну інформації між всіма користувачами інфраструктури ЗВО, визначає правила та типи користувачів, в залежності від статусу: викладач, адміністратор чи здобувач – отримує певну структуровану інформацію в залежності від запиту, потреби: розклад, навантаження, тип заняття, аудиторія з певними матеріально-технічними засобами навчання, організація вибору індивідуальної траєкторії навчання, організацію заліків,

іспитів, консультацій, ознайомлення з результатами сесії, формування результуючих даних у розрізі студента, групи, груп кафедри, груп факультету, потоку чи в цілому всіх студентів ЗВО. Аналіз результатів успішності, кількісних та якісних характеристик відвідувань занять. Система включає дані щодо переведення здобувача освіти, закінчення навчання чи відрахування за неуспішність із доведенням інформації керівництву закладу засобами інформаційної системи.

- Система дистанційного навчання ЗВО – це інформаційна система, яка організовує сам процес навчання здобувачів вищої освіти в якій вони мають змогу отримувати необхідну для освіти інформацію, консультації викладачів, спілкуватись з колегами по навчанню в зручний для себе час. В системі дистанційного навчання розміщені всі необхідні методичні матеріали, електронні підручники, презентації, програми, робочі програми, методичні рекомендації для самостійної роботи здобувача вищої освіти.
- Конференц-системи для змішаного навчання, VR-системи – використовуються для розширення можливостей надання освітніх послуг та охоплення великої кількості слухачів, здобувачів та учасників конференцій і інших наукових заходів, які дають можливість очного і дистанційного навчання, чи демонстрування презентацій. Також широко почали використовувати в освітньому процесі технології віртуальної реальності VR-системи, у яких є можливість досліджувати певні процеси у віртуальному просторі.
- Система фінансово-економічної діяльності ЗВО – дає можливість у цифрому вигляді вести повний фінансовий облік матеріальних цінностей, облік всіх фінансових операцій, контролювати інформацію про фінансовий стан тощо. Система фінансово-економічної діяльності надає повну інформацію щодо прийняття управлінських рішень.
- Система кібернетичної безпеки – це система, яка забезпечує безпеку всіх інформаційних систем ЗВО, відповідно до побудованої архітектури [4].
- Системи керування серверних ресурсів – в залежності від потреби здобувачів вищої освіти, викладачів організовується розподіл ресурсів серверного обладнання, з урахуванням побудови постійного дублювання інформації, використання хмарних ресурсів – підписок Office 365(компонентів), скарб-освіти тощо – адміністратори в залежності від політики розмежування прав надають доступ до даних ресурсів.
- Система керування мережею, VPN ЗВО – для забезпечення ефективної роботи у комп'ютерній мережі, як інформаційній системі постійно ведеться моніторинг її стану, вживаються політики безпеки на різних рівнях на комутаційному керованому обладнанню за допомогою мережного програмного забезпечення. В період воєнного стану заборонено використовувати відкриті способи доступу до ресурсів елементів мережі, тільки з використанням VPN з генерацією персонального ключа користувача, для автентифікації та не допущення організаційного порушення захисту, в залежності від активності зовнішніх користувачів система моніторингу автоматично може заблокувати для забезпечення безпеки архітектури інформаційної системи ЗВО.

Така архітектура, на нашу думку, дасть можливість повного контролю інформації, можливість відповідної побудови захисту, що наразі є актуальним в період воєнного стану в Україні. Також вона дасть можливість правильно побудувати та ефективно використати інформаційні ресурси ЗВО, дозволить оптимізувати потоки інформації, підвищить надійність такої системи [3]. В процесі експлуатації це дасть можливість у повній мірі використати гібридні інформаційні системи, поєднувати роботу у локальній мережі та використати хмарні технології, а при потребі безпечно працювати віддалено у межах інформаційної системи ЗВО. Веб ресурси ЗВО необхідно розподілити на закриті і відкриті, для правильної організації освітнього процесу.

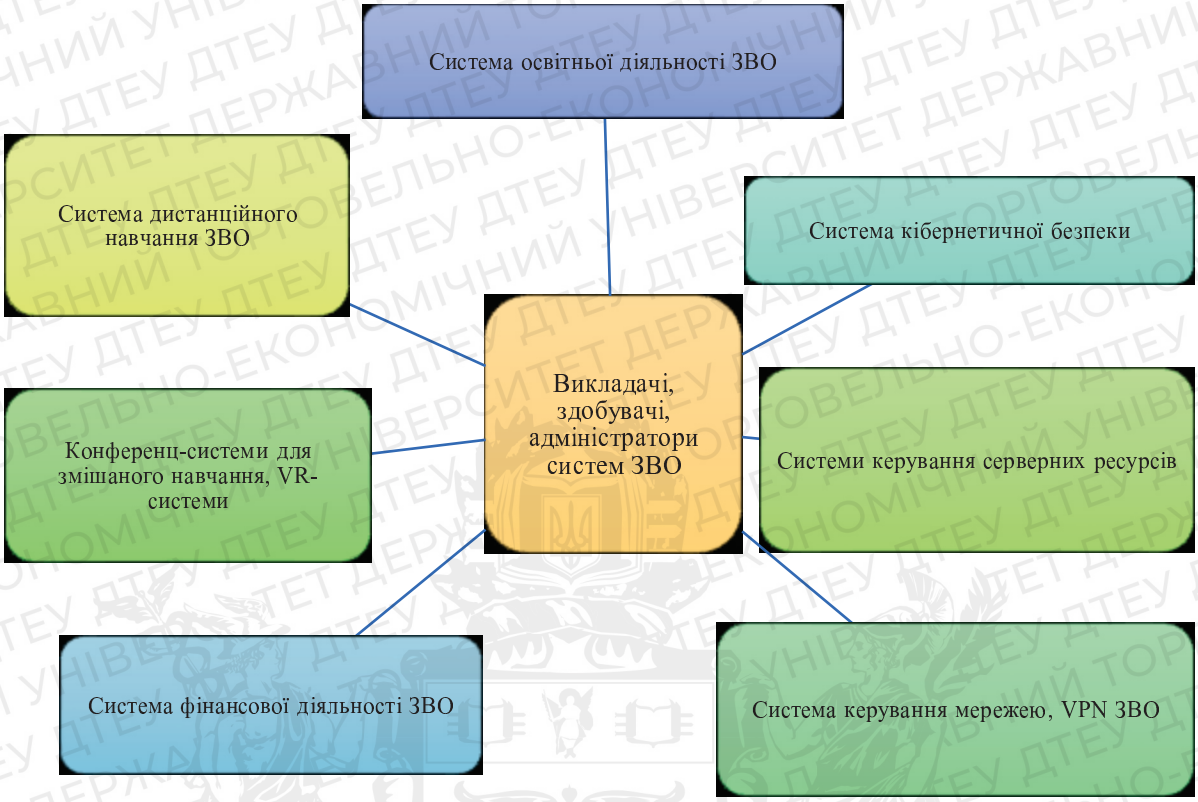


Рис. 1 Архітектура інформаційної системи освітнього процесу ЗВО.

Система освітньої діяльності ЗВО – постійно розвивається та охоплює процеси, що автоматизують введення інформації: сканування, цифрової трансформації, створення фото, відео, аудіо масивів структурованих даних, які при потребі аналізуються, відбираються та відтворюються у освітньому просторі. Цифровізовано процес навчання здобувачів вищої освіти, підготовку. Прикладом інформаційної системи керування освітнім процесом – є українська розподілена система МІА: Освіта. До функціоналу даної системи входять блоки:

- електронний кабінет,
- навантаження студента та викладача,
- створення оголошення до розкладу та тематичного плану,
- консультації,
- електронний журнал,
- графік прийому відпрацювань,
- тематичний план,
- список (академічної групи, віртуальної групи, потоку, кафедри, дисципліни за записом),
- гуртожиток (реєстрація проживаючих студентів, бронювання студентами кімнат),
- статистика успішності та відвідуваності,
- екзаменаційна відомість,
- атестації,
- стипендіальний рейтинг,
- інформатор,
- робочий план,
- ведення всього контингенту студентів (зарахування, переведення та відрахування, створення наказів на студентів),
- створення віртуальних груп, для вибіркових дисциплін,

- створення та редагування електронного розкладу для всього контингенту студентів та викладачів у розрізі студента, групи, курсу, факультету, викладача, у межах поточного тижня, поточного місяця, попереднього і наступного місяця, та заданого діапазону;
- створення переліку дисциплін освітнього закладу, спеціальності, спеціалізації, груп, викладачів на кафедрах та навчальних планів;
- розподіл навантаження кафедри, аудиторій та створення звітів навантаження по закладу освіти.
- формування потоків груп;
- формування індивідуальних карток здобувачів.

Система МІА: Освіта – є мультисистемна, працює на операційних системах з Windows XP до Windows 10, на всіх версіях Linux та IOS. Є як локальна версія для роботи в середині локальної мережі кампусу ЗВО, так і Web-версія для роботи через глобальну мережу Інтернет. Так можлива робота віддалено з любої точки, головне мати персональний доступ до ресурсу. Водночас сьогодення пропонує закладам освіти широкий вибір систем дистанційної освіти, у багатьох є всі необхідні компоненти для забезпечення освітнього процесу. Найпоширеніші наразі системи, які використовують хмарні ресурси Microsoft Office 365, застосунки Google, edx courses, рідше використовують Moodle, але вони не забезпечують увесь процес дистанційного навчання, немає повноцінної системи відеоконференцзв'язку. Найбільше вищих закладів вищої освіти визначилися і використовують Microsoft Office 365 та застосунки Google. Використовують компоненти Microsoft Office 365: Outlook, Word, Excel, PowerPoint, Power BI, OneNote, OneDrive, SharePoint, Skype для бізнесу, Teams, Sway, Forms, Stream, Flow, PowerApps, School Data Sync. Застосунки Google: Google Клас, Google Meet, Google Календар, Google Диск, Google Документи, Google Таблиці, Google Форми, Google Презентації, Google Keep, Google Сайти, Google Jamboard. У багатьох ЗВО використовують системи архівації та збереження інформації, але організаційно складно контролювати наповнення архівів, вчасне оновлення та їх зберігання. Для цього розробляють ресурси для автоматичного збереження даних, спеціальні програмні модулі збирають у визначених місцях операційної системи файли, архівують із зазначенням дати і часу та переміщують у файлове сховище через спеціальні інтерфейси захищеної передачі даних. Таким чином файли щодня зберігаються і при потребі використовуються для відновлення інформації.

Ефективним є використання конференцсистем для змішаного навчання. Всі матеріали розміщуються у системах для забезпечення дистанційного навчання, та використовуються платформи, що дозволяють забезпечити освітній процес у змішаному режимі, так Teams – дозволяє підключати віддалено студентів для отримання знань і умінь. Таким чином одночасно всі в однакових умовах можуть у онлайн режимі та очно проходити навчання.

VR-системи значною мірою використовуються для апробації з використанням віртуального середовища, середовища наближеного до реального.

Для ведення фінансово-економічної діяльності закладу вищої освіти використовують автоматизовані цифрові системи, до прикладу МІА: Облік і звітність, яка повністю забезпечує всі процеси і зв'язки з зовнішніми е-інфраструктурами: МОН, банки, фіскальні системи, урядові системи, іншими системи цифрового міста. До складу МІА: Облік і звітність входять наступні блоки:

- відтворення всіх бухгалтерських операцій фінансово-економічної діяльності,
- проведення виплат стипендії, соціальної стипендії, заробітної плати та інші платежів,
- облік матеріально-технічного забезпечення,
- прогнозування планування витрат,
- ведення обліку контингенту: студентів (зарахування, переведення та відрахування, створення наказів на студентів); працівників (викладачів та допоміжного персоналу); студентів, аспірантів – контрактників; військовозобов'язаних, а також міжнародних студентів.

МІА: Освіта та МІА: Облік і звітність є важливими інформаційними та рекомендаційними системами для прийняття ефективних рішень керівництвом закладу, за їх допомогою можна бачити стан діяльності ЗВО. Це дає змогу будувати правильну стратегію розвитку ЗВО та впливати на результати його діяльності.

Найскладнішими наразі є системи керування мережею, серверними ресурсами та контролем VPN-підключень. Ці системи забезпечують надійний зв'язок між інформаційними системами, серверами, користувачами та зовнішніми е-інфраструктурами Smart-міста. Найскладнішим є неоднорідність клієнтських підключень, багатофакторність інтерфейсів зв'язку у локальній дротовій мережі, доступ у бездротових мережах і доступність серверних ресурсів та забезпечення контролю використання хмарних ресурсів. Всі ці задачі постійно трансформуються, окремі інформаційні системи розвиваються, тому і змінюються їх канали передачі інформації, але забезпечується цілісність сукупної інформації по ЗВО в цілому.

Система кібернетичної безпеки будується на основі вивчення всіх факторів ризику інформаційних системи окремо та інформаційної системи ЗВО загалом. Розробляються організаційні заходи кіберзахисту із застосуванням апаратних та програмних засобів. По-перше для доступу до інформаційних систем використовується двохфакторна автентифікація, використання КЕП (контрольованих електронних ключів) апаратних та програмних для підтвердження особистості. Також у системах використовуються системи шифрування каналів передачі інформації, заборонено відкрито відправляти поштовими повідомленнями документацію. Таким чином забезпечуватиметься захист інформації від перехоплення. Всі бази даних шифруватимуться та додатково захищатимуться за допомогою апаратних чи програмних FireWall (рис 2). Доступ до мережі Інтернет повністю контрольований, окремо налаштовуються резидентні підключення по VPN до зовнішніх е-інфраструктур.

Так інформаційною системою інфраструктури можна визначити – сукупність апаратних і програмних засобів, котрі поєднані системами зв'язку та які мають внутрішній контроль доступу до ресурсів, а також виконують певні задачі у загальній інфраструктурі, але можуть працювати окремо, незалежно від інших систем: можуть самостійно розвиватися та не впливати на інші інформаційні системи.

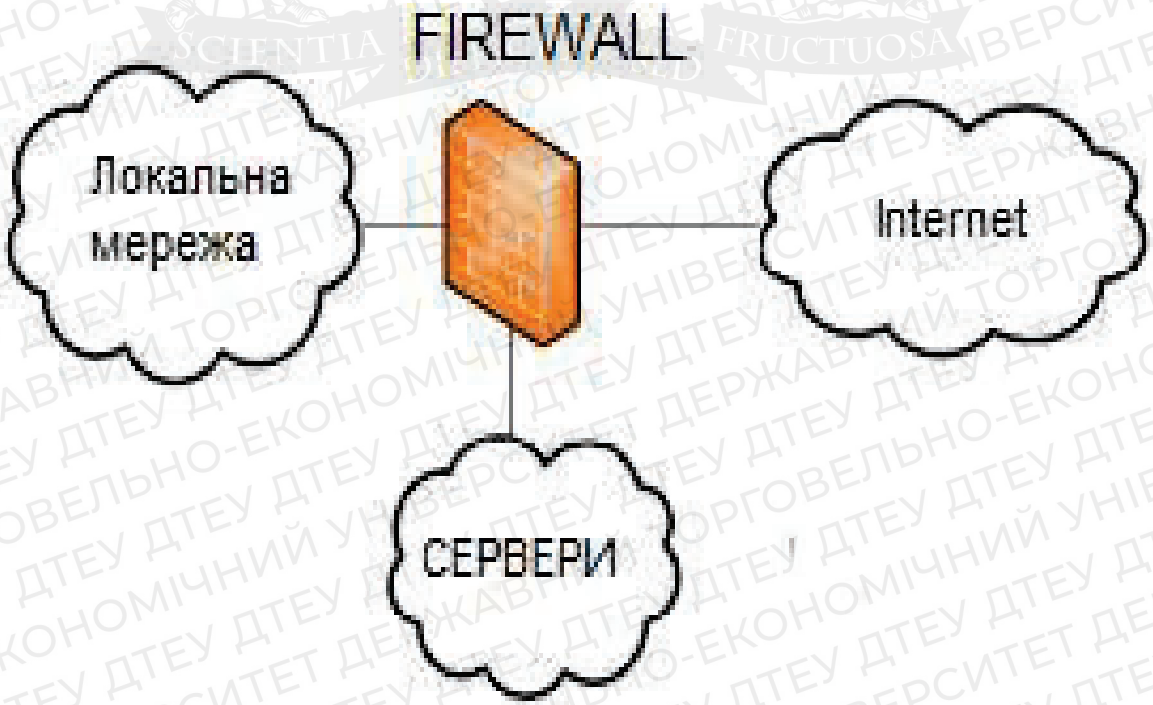


Рис. 2 Схема застосування FireWall

Постійно трансформуються технічні засоби навчання, деякі припиняють використовуватися, такі як лампові графопроектори, лампові мультимедійні проектори, бо їх замінюють на лазерні мультимедійні проектори, SmarBoard, SmartWall – які використовуються за допомогою інтерактивних застосунків, що покращує сприйняття здобувачами вищої освіти інформації. Також можливі варіанти відтворення віддаленого навчання, коли викладач знаходиться за межами закладу вищої освіти, а здобувачі у аудиторії, та завдяки відеоконференцсистемам, Інтернету забезпечується повноцінний освітній процес. З'являється можливість використання різних застосунків, участь більшої кількості здобувачів освіти в освітньому процесі. Так інформаційні системи інфраструктури ЗВО пов'язані між собою, доповнюють одна одну та дають можливість відтворювати всі можливі варіанти надання методичних матеріалів, забезпечення та контроль освітнього процесу, коригування та удосконалення при потребі навчальних матеріалів, самих систем. Керівники таких інформаційних систем отримують повну інформацію з можливістю правильного прийняття управлінських рішень для більш повного задоволення потреб суспільства та роботодавців. Сучасні інформаційні системи інфраструктури ЗВО наближаються до цифрових екосистем.

Висновки. Правильно побудувавши інформаційну систему освітнього процесу ЗВО, ми отримаємо модель системи, де можемо прогнозувати та передбачати стійкість системи. Важливим місцем у даній системі є співвідношення всіх окремих інформаційних систем, які постійно розвиваються, трансформуються, тому можна контролювати процеси підготовки і впровадження оновлень. Запропонована архітектура дає можливість побудови кіберзахисту інформаційної системи. Ефективність управління інформаційною інфраструктурою ЗВО дасть можливість покращення результатів освітнього процесу, надати більше інструментів для провадження навчання студентів, що задовольнить у більшій мірі потреби громадян і суспільства.

Список використаних джерел

1. Биков В.Ю. Проблеми та перспективи інформатизації системи освіти в України / В.Ю. Биков // Науковий часопис НПУ імені М.П. Драгоманова. Серія №2. Комп'ютерно-орієнтовані системи начання. – К.: НПУ імені М.П. Драгоманова, 2012. – № 13 (20). – С. 3-18
2. Управління розвитком складних систем:(КНУБА) УДК 004.94:378.4, Моделювання єдиного інформаційного простору закладу вищої освіти, Шестак Ярослав, ст 82-89, DOI: dx.doi.org\10.32347/2412-9933.2022.49
3. Міжнародний науково-практичний журнал «Товари і ринки»: (КНТЕУ) (№1 2021): УДК 004.7.056.5(477)(045), Кібербезпека та захист інформації під час пандемії COVID-19, Білявська Юлія, Микитенко Неля, Шестак Ярослав, ст 34-46, DOI: https://doi.org/10.31617/10.31617/tr.knute.2021(37)03
4. Міжнародний науково-практичний журнал «Товари і ринки»: (ДТЕУ) (№3 2022): УДК 004.056:004.9, Кібербезпека та кібергігієна: нова ера цифрових технологій, Білявська Юлія, Шестак Ярослав, ст 47-59, DOI: https://doi.org/10.31617/3.2022(43)04

Робота виконана під науковим керівництвом к.т.н., доцента
ХАРЧЕНКА О.А.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

ШИМОНЯ М. 2м курс ФІТ ДТЕУ
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто широке застосування новітніх інноваційних підходів і технологій, які зумовили трансформацію форм і методів діяльності суб'єктів правовідносин для збільшення їхніх функціональних можливостей, захисту даних та зменшення витрат.

This article considers the widespread use of the latest innovative approaches and technologies that have led to the transformation of the forms and methods of activities of legal entities to increase their functionality, protect data and minimize expenses.

Актуальність. З розвитком засобів інформаційних комунікацій та можливістю завдати шкоди інформації, що зберігається та передається завдяки їм, з'явилося поняття інформаційної безпеки. Інформаційна безпека допомагає захистити інформацію та інформаційну інфраструктуру від загроз.

Такі впливи можуть бути випадковими або умисними, внутрішніми або зовнішніми, і можуть призвести до втрати важливої інформації, її незаконної модифікації або використання третіми особами. Гарантувати повну та якісну інформаційну безпеку можливо лише за умови застосування системного та цілісного підходу.

Технологія блокчейн почала свій розвиток як платформа для криптовалюти Біткоїн, але згодом стала перспективною технологією задля забезпечення захисту інформації. Блокчейн пропонує широкий спектр можливостей для підтримки надійного рівня безпеки даних завдяки механізмам шифрування, цілісності даних, стійкості мережі та масштабованості. В результаті чого, перехід від традиційної системи інформаційної безпеки до системи на основі блокчейну може бути вигідним для організацій практично в будь-якій галузі.

Метою статті є дослідження особливостей використання технології блокчейн як систему захисту в різних галузях.

Об'єктом дослідження є методи та способи забезпечення інформаційної безпеки на основі технології блокчейн.

Предметом дослідження є способи захисту інформації від загрози викрадення, а також уже реалізовані системи забезпечення інформаційної безпеки на основі технології блокчейн.

Аналіз попередніх досліджень. Наукові дослідження застосування технології блокчейн у сфері публічних відносин практично відсутні. Це питання є частково розглянуто в дослідницьких роботах таких науковців 0. А. Баранова, І. В. Давидової, О. Д. Довганя, І. М. Дородіна, О. Е. Сімсон, Р. О. Стефанчука, Р. В. Чорнолуцького та ін.

Виклад основного матеріалу. Технологія блокчейну, що є основою криптовалют, таких як Bitcoin та Ethereum, здатна забезпечити надійний захист інформації. Багато компаній починають використовувати блокчейн для забезпечення безпеки своїх даних та інформації клієнтів.

Технологія блокчейн - це децентралізований або розподілений електронний реєстр достовірних та незмінних даних, що грунтується на криптографічних алгоритмах і фіксує інформацію про всі здійснені транзакції у цифровому просторі за допомогою створення блоків-транзакцій [7].

Основа технології блокчейну полягає у збереженні даних у вигляді ланцюга блоків, кожен з яких містить криптографічно захищену інформацію. Кожен блок містить у собі хеш попереднього блоку, що забезпечує надійність інформації. Таким чином, будь-які зміни в одному блоку, автоматично впливають на всі інші блоки у ланцюжку.

Однією з переваг технології блокчейну є те, що вона забезпечує безпеку за допомогою децентралізації. Інформація зберігається на кожному комп'ютері, що відповідає за обробку та підтвердження транзакцій в мережі. Це забезпечує безпеку даних усіх типів блокчейну (Таблиця 1), оскільки для того, щоб хакер взломав систему, він мусить взломати кожен комп'ютер, що приймає участь у мережі. Це зробить атаку на систему непрактичною, навіть якщо зловмисник має значні ресурси.

Таблиця 1.

Види блокчейну, які використовуються для захисту даних

Вид блокчейну	**Опис**
Публічний блокчейн	Це відкритий блокчейн, до якого можуть мати доступ всі користувачі. Він децентралізований і не підлягає контролю жодного централізованого органу або особи. Приклади: Bitcoin, Ethereum.
Приватний блокчейн	Це закритий блокчейн, до якого мають доступ лише відповідні користувачі, які мають дозвіл на доступ до системи. Він підконтрольований централізованим органом або особою, і може використовуватися для конфіденційної обробки даних. Приклади: Hyperledger Fabric, Corda.
Консорціальний блокчейн	Це гібридний блокчейн, який поєднує в собі як публічний, так і приватний блокчейн. Він використовується для спільної роботи групи організацій з різних сфер діяльності. Приклади: R3 Corda, Hyperledger.
Федеративний блокчейн	Це блокчейн, управління яким здійснюється кількома централізованими органами або особами, які мають дозвіл на доступ до системи. Приклади: Ripple, Stellar.

Всі види блокчейну можуть забезпечити захист даних. Кожен блок містить хеш попереднього блоку, який зберігає інформацію про стан системи на момент попереднього блоку. Це означає, що якщо будь-які зміни внесені в попередній блок, хеш наступного блоку автоматично стає недійсним. Це змушує зловмисників переглядати і перевіряти хеші всіх попередніх блоків для того, щоб змінити дані в останньому блоку. Це ускладнює зловмисникам атакувати систему, оскільки їм потрібно змінити кожен блок в ланцюжку. Він може забезпечувати прозорість та безпеку даних за допомогою розумного контракту. Розумний контракт - це програмний код, який автоматично виконує певні дії, коли виконуються відповідні умови. Розумний контракт може забезпечити безпеку даних, оскільки його виконання залежить від умов, які визначені у контракті, та він може автоматично виконувати дії для забезпечення безпеки даних.

Блокчейн містить базу даних про всі раніше здійснені операції та дозволяє ефективно й оперативно виконувати операції між двома сторонами в режимі онлайн, де всі транзакції перевіряються і підтримуються децентралізованою мережею комп’ютерів.

Важливо, що записи зберігаються в зашифрованому вигляді одночасно у всіх учасників системи й автоматично оновлюються з кожним внесенням змін. Користувачі виконують роль колективного нотаріуса, який підтверджує правдивість інформації в базі даних, і забезпечують захист від маніпуляцій та зловживань.

Завдяки технології блокчейн кожен договір, процес, платежі матимуть цифровий запис, який можна буде ідентифікувати, перевірити, зберегти і поділитися ним.

Система блокчейн підтримується і захищається криптографічними алгоритмами і протоколами, наприклад, цифровими підписами, хеш-функціями. Ці засоби гарантують, що транзакції, які записуються в реєстр, захищені, їх автентичність підтверджена і вони не можуть бути скасовані.

Структура мережі блокчейн складається з хешів або хеш-кодів. У системі блокчейн це унікальний числовий ідентифікатор фіксованої довжини, який генерується з даних блоку за допомогою хеш-функції (Рис. 1). Хеш служить для забезпечення цілісності та безпеки даних в блокчейні, оскільки будь-яка зміна даних в блоку призведе до зміни його хешу. При перевірці блоку на його валідність, перевіряється, чи відповідає хеш блоку відомому значенню, яке було розраховано при створенні блоку. Це дозволяє запобігти підробці даних в блокчейні.

Одним з прикладів використання хешу у блокчейні є майнінг криптовалют. Для отримання нового блоку майнер повинен розв'язати криптографічну задачу, яка включає в себе створення хешу блоку, який відповідає певному критерію складності. Це забезпечує безпеку мережі, оскільки додавання нового блоку вимагає значних обчислювальних зусиль та ресурсів.

Хеші можна використовувати для шифрування повідомлень, контролю цілісності даних, побудови індексів та багато іншого. Їх ефективність і безпека досить високі, і тому вони широко використовуються в різних галузях, включаючи блокчейн технології [10].

Рис.1. Структура мережі блокчейн

Хеш-функції - це один з найпоширеніших криптографічних алгоритмів у технології блокчейн. Це криптографічні алгоритми, призначені для забезпечення цілісності даних в технології блокчейн. Будь-який фрагмент даних може бути хешований, незалежно від його розміру або типу. У традиційному хешуванні, незалежно від розміру, типу або довжини даних, хеш, згенерований з будь-яких даних, завжди має однакову довжину.

Хеш-функція приймає початковий потік (числа, алфавіти, мультимедійні файли) будь-якої довжини і перетворює його в новий рядок фіксованої довжини. Фіксована довжина може бути різною (наприклад, 32-бітною, 64-бітною, 128-бітною або 256-бітною) залежно від типу хеш-функції, що використовується. Рядок заданої довжини називається хешем.

Технологія блокчейн є розподіленою мережею, вона потребує протоколу консенсусу, який містить в собі правила, яких повинен дотримуватися кожен учасник, щоб досягти глобальної єдиної точки зору. Протокол консенсусу є механізмом, за допомогою якого в мережі блокчейн досягається згода щодо дійсності транзакцій і відбувається підтвердження нових блоків. Він забезпечує спільне розуміння того, яка частина мережі має право на генерацію наступного блоку та як саме це має відбутися.

Існують різні види протоколів консенсусу, у кожного з яких є свої переваги та недоліки, і вибір певного протоколу залежить від конкретного застосування та потреб користувачів:

1. Proof of Work (PoW). Базується на математичних обчисленнях, які забезпечують безпеку мережі. Протокол вимагає від групи майнерів розв'язування складної криптографічної задачі, і перша особа, яка вирішує задачу, отримує можливість додати блок до ланцюжка. Bitcoin використовує протокол PoW.
2. Proof of Stake (PoS), де замість обчислень вимагає від користувачів вкладення (стейкінг) своїх монет для отримання можливості додавання блоку. У порівнянні з PoW, PoS є енергоефективнішим та менш витратним у плані обладнання.
3. Delegated Proof of Stake (DPoS). Подібний до PoS, але включає в себе вибір делегатів, які мають право на додавання блоків до ланцюжка. Делегати обираються голосуванням учасників мережі.
4. Proof of Authority (PoA) - вимагає наявності авторитету в мережі, який підтверджує дійсність блоків. Авторитетом можуть бути урядові органи, корпорації, експерти, або будь-які інші сторони, що мають довіру в мережі.
5. Proof of Elapsed Time (PoET) - заснований на виборі першого випадкового учасника мережі, який має право на додавання блоків до ланцюжка. Він працює за принципом вибіркового доступу, де обрання випадкового учасника відбувається з розрахунку його потужності та доступності.

Однак, протоколи консенсусу також мають деякі недоліки:

- Великі витрати на обчислення: деякі протоколи консенсусу можуть вимагати великих обчислювальних потужностей, що може збільшувати вартість утримання мережі.
- Проблеми з масштабованістю: деякі протоколи консенсусу можуть мати обмеження на кількість транзакцій, які можуть бути оброблені за один блок. Це може призвести до затримок у обробці транзакцій під час періодів високого навантаження.
- Ризик централізації: деякі протоколи консенсусу можуть стати дуже важкими для реалізації на великих мережах, що може призвести до концентрації влади в руках деяких груп або індивідів.

Незважаючи на ці недоліки, протоколи консенсусу є важливою складовою системи блокчейн і забезпечують її надійність та безпеку, особливо в умовах де відсутня довіра, блокчейн надає користувачам такі бажані функції, як анонімність, прозорість, незмінність, що привертає велику академічну та промислову увагу в останні кілька років. Завдяки цим перевагам технологія блокчейн привернула велику увагу науковців і підприємців в останні кілька років.

Блокчейн дозволяє побудувати довіру в інтернеті, яка може забезпечити більш прозору, безпечну та ефективну систему для всіх. Вона може збільшити інновації, знизити витрати та покращити якість життя людей у всьому світі [8, с. 78].

Блокчейн є ідеальним засобом для збереження подій у мережному середовищі, оскільки система записує і вибудовує їх у строго хронологічному порядку. У даному контексті блокчейн можна описати як послідовну структуру даних, що складається з ланцюжка блоків зв'язаних між собою за допомогою хеш-покажчиків, що містяться в заголовку кожного блоку. Ця структура є односпрямованою та без зворотного зв'язку.

Вузли блокчейна здійснюють алгоритми консенсусу, якщо кілька вузлів знаходяться в автономному режимі, інші продовжують працювати, навіть якщо вони були переведені в автономний режим внаслідок хакерської атаки. Робота відновлюється, коли вузли відновлюють зв'язок між собою, повертаються в оперативний режим і проводять пересинхронізацію вузлів, щоб забезпечити послідовність і цілісність всього ланцюжка. Ця можливість існує завдяки унікальному набору закодованих алгоритмів у системі блокчейн.

Також кожен блок в мережі блокчейн складається з двох основних частин - голови і тіла. Голова містить інформацію, яка забезпечує стабільність і непохитність мережі. Тіло містить перелік всіх транзакцій, які повинні зберігатися в цьому блоці і бути внесені в мережу блокчейн.

У класичній блокчейн мережі Head містить такі поля [2]:

- номер версії блоку (ver_block);

- хеш попереднього блоку (prev_block);
- хеш усіх транзакцій у поточному блоці (mrkl_root);
- тимчасову мітку, коли було створено блок (timestamp);
- «bits» і «nonce» параметри, що використовуються при майнінгу.

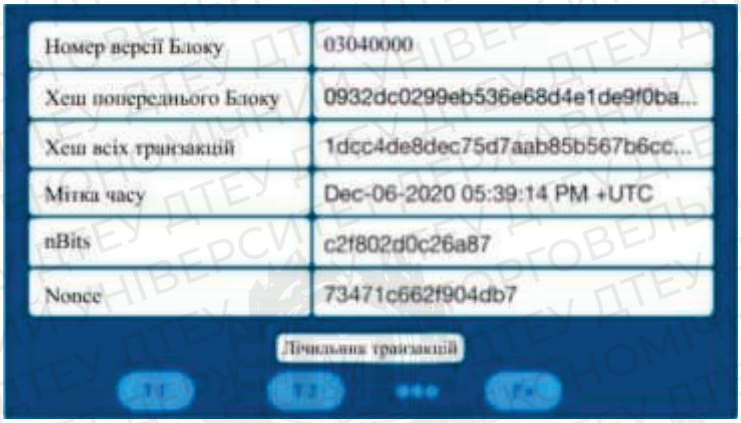


Рис. 2. Структура блоку

У системі захисту блокчейн важливу роль відіграє Payload, оскільки це дані, які передаються та зберігаються в блоках. Payload, як правило, містить дані, які потрібні для збереження в ланцюгу блоків. Ці дані можуть бути інформацією про транзакції, метаданими або будь-якою іншою корисною інформацією [9, с. 91].

Payload зашифрований та не може бути змінений після його занесення в блокчейн, що робить його даними, які не можуть бути підроблені або внесені ззовні. Payload може містити метадані, які можуть бути використані для підтвердження автентичності та джерела даних, що зберігаються в блоках. Наприклад, в цифрових платіжних системах Payload може містити інформацію про отримувача та відправника, дату та час транзакції, суму переказу.

Payload складається з лічильника транзакцій і списку всіх транзакцій, включених до існуючого блоку. Існує також максимальна кількість транзакцій, яку може вміщувати блок. Це значення залежить від розміру транзакції. Для того, щоб перевірити справжність транзакції використовується механізм асиметричної криптографії.

Цифровий підпис є невід'ємною частиною системи блокчейн і являє собою криптографічний алгоритм, який накладається особою, що використовується для перевірки справжності та цілісності документа, а також для встановлення авторства документа.

Криптографічні цифрові підписи, які базуються на асиметричній криптографії, відіграють вирішальну роль у безпеці блокчейн-мереж. Ці цифрові підписи дозволяють здійснювати безпечні та автентифіковані транзакції без необхідності використання надійного посередника. Цифрові підписи є важливим компонентом технології блокчейн, що дозволяє учасникам перевіряти автентичність і цілісність даних у мережі [11].

Криптографія з відкритим ключем та хеш-функцією надають математичні інструменти, які дозволяють ефективно використовувати цифровий підпис. Використання шифрування та цифрових підписів є важливою умовою функціонування мережі блокчейн. Хешування дозволяє кожному з учасників мережі визначити актуальний стан блокчейну, а цифрові підписи забезпечують доказ того, що всі операції були здійснені виключно справжніми користувачами.

У Лондоні 9 грудня 2014 року розпочало свою роботу Digital 5 (D5), об'єднання провідних цифрових країн (Естонії, Ізраїлю, Нової Зеландії, Південної Кореї та Великої Британії) з головна мета цього об'єднання, це розвитку цифрової економіки. Представники урядів цих країн зобов'язалися трансформувати відносини уряду з технологіями, підтримуючи використання відкритих стандартів та програмного забезпечення з відкритим кодом, а також підвищуючи ефективність роботи цифрового уряду.

Учасники Digital 5 визначили основні принципи цифрового розвитку: потреби користувачів; відкриті стандарти; відкритий код; відкриті ринки; відкритий уряд (прозорість); зв'язок; навчання дітей програмуванню; доступність цифрових послуг; обов'язок ділитися і вчитися [3]. Ці принципи можуть доповнюватися і вдосконалюватися з урахуванням нових проблем і можливостей інформаційних технологій.

Значне поширення новітніх інноваційних підходів та технологій спричинило трансформацію форм та методів діяльності юридичних осіб з метою підвищення їх функціональності, захисту даних та зменшення витрат. З кожним роком все більше юридичних осіб публічного та приватного права застосовують сучасні інформаційно-телекомунікаційні технології для покращення рівня ефективності та результативності своєї діяльності. До таких технологій відносяться: Internet of Things, Cloud Technology, Blockchain, Mobile ID, Big Data.

У січні 2018 року реалізація найкращих світових практик електронного урядування дозволила Україні увійти до переліку 14 країн, які визнані лідерами у впровадженні технології блокчейн. Технологія блокчейн в основном використовується в банківському, фінансовому та страховому секторах. Однак її можливий вплив та використання в державному управлінні ще не до кінця вивчені.

Британська науковець Мелані Свон у своїй книзі "Блокчейн: схема нової економіки (англ. Blockchain: Blueprint for a New Economy") [5], беручи до уваги поточні та потенційні технологічні аспекти блокчейну, визначила етапи еволюції даної технології: *блокчейн 1.0* - це валюта.

Криптовалюта використовується для здійснення цифрових переказів і платежів. Серед сучасних електронних валют найпоширенішою є біткойн, концепція якого була викладена у 2008 році професором Сатоші Накамото у статті "Біткойн: пірингова електронна грошова система" (Рис.3).

Рис. 3. Зображення монети Bitcoin

Блокчейн 2.0, забезпечує можливість обробки різних типів фінансових операцій, включаючи операції з цінними паперами, акціями та частками в компаніях, механізмами краудфандингу, заборгованістю, пенсійними фондами та деривативами (ф'ючерсами, облігаціями, опціонами та свопами);

Блокчейн 3.0, галузь якого виходить за межі економічної та фінансової діяльності та охоплює державне управління, охорону здоров'я, науку, освіту, культуру та мистецтво [5].

Застосування технології блокчейн має свої переваги та недоліки. Перевагами можуть бути: забезпечення високоефективних механізмів захисту цілісності та доступності інформації; створення повністю автономної системи; захищеність системи від несанкціонованого втручання та модифікації інформації, що зберігається в реєстрі; економія коштів у порівнянні зі зберіганням інформації на паперових носіях та використанням традиційних технологій зберігання даних на машинних носіях [1, с. 76]; неможливість внесення правок до реєстру даних з попередньою датою; підвищення рівня захисту державних баз даних від стороннього втручання при дотриманні певних умов.

При застосуванні технології блокчейн існують певні ризики:

- оприлюднення персональних даних та конфіденційної інформації;
- низька продуктивність та швидкість роботи бази даних;
- рівень безпеки та децентралізації системи напряму залежить від кількості його учасників та потужності обчислювальних систем;
- можливість внесення недостовірних даних; людський фактор при управлінні доступами до реєстрів;
- ідентифікація користувачів бази даних.

Не дивлячись на певні ризики при застосування цієї технології, блокчейн вважається надійно захищеною та удосконалюється з кожним роком все більше. Окрім криптографічного захисту, використання алгоритмів консенсусу та наявності децентралізованої структури, дана система має вбудовану систему автоматичної верифікації, що гарантує, що тільки правильні дані можуть бути записані в блокчейн. Це забезпечує достовірність даних та унеможливлює їхнє підроблення.

Значна популярність цієї ідеї, щодо застосування технології блокчейн для державних реєстрів, на думку І. Дороніна, передусім пов'язана із загальною недовірою суспільства до діяльності державних органів, які відповідальні за такі реєстри, дані установи навпаки повинні забезпечувати захист прав власників та зберігати інформацію в належному вигляді [1, с. 76-77]. Технологія блокчейн має значні перспективи і надає можливість якісно трансформувати сферу інтелектуальної власності у напрямку забезпечення надійними доказами авторства, полегшенням контролю за контентом та управління правами користувачів.

На сучасному етапі розвиток блокчейн технології в Україні повинен відбуватися за умов належної цифрової ідентифікації особи заявника об’єкта інтелектуальної власності та комплексного правового регулювання. Тільки за таких умов можливе створення оптимальної правової моделі захисту прав інтелектуальної власності на основі блокчейн та забезпечення повної довіри майбутніх користувачів до даної системи.

Найпершими експериментальними проєктами в Україні, які використовують систему зберігання та захисту даних блокчейн, є електронні земельні аукціони, робота Державного земельного кадастру, Державного реєстру речових прав на нерухоме майно та Системи електронних торгів арештованим майном (СЕТАМ).

16 червня відбулося підписання Меморандуму про співпрацю щодо створення новітньої цифрової системи захисту даних Державного земельного кадастру від зовнішнього втручання. Програмний продукт буде розроблений на базі технології Blockchain, яка є найбільш досконалою із існуючих на сьогодні в сфері захисту даних [6].

Попри те, що блокчейн-технології мають значний потенціал у вирішенні багатьох фінансово-економічних питань для різних секторів економіки, на практиці впровадження таких технологій має певні нюанси, що виникають при впровадженні цих технологій.

Проаналізувавши всі плюси та мінуси даної технології, можна дійти до висновку, що технологія вимагає унікального рівня організації, компанії мають бути згодні на впровадження нових ресурсоємних технічних, функціональних та юридичних механізмів. Незважаючи на це, та щорічні витрати на систему блокчейн які досягли відмітки в 1,7 мільярда доларів, багато фінансових компанії не змогли реалізувати переваги ранніх інвестицій, а низка пілотних проєктів було закрито.

На первинному етапі впровадження технології блокчейн у галузі реєстрації земельних договорів існує ймовірність виникнення складнощів з первинною ідентифікацією власників земельних ділянок, оскільки інформація, що вводиться в блокчейн-реєстри, сама по собі не є достовірною. Блокчейн забезпечує гарантію незмінності даних, а не їх правдивості, оскільки ця система може бути використана лише для перевірки або надання витягів про те, чи не є вони підробкою. Однак неможливо перевірити достовірність даних, що містяться в такому витягу [4].

В теорії і в перспективі за допомогою працюючих блокчейн-платформ можна буде просто, недорого і безпечно реєструвати юридичні особи, права на нерухоме і рухоме майно,

інтелектуальну власність, складати заповіти, здійснювати збір податків, виплачувати пенсії, видавати цивільні паспорти.

Згідно з концепцією, поєднання прозорості та захищеності блокчейна робить цю технологію привабливою для використання в електронних державних послугах (e-Government). Наприклад, громадянин оплачує адміністративний штраф або податок, а інформація про погашення миттєво з'являється і оновлюється у всіх учасників блокчейн-платформи.

Крім стабільності така система відрізняється низькими транзакційними витратами: в результаті немає необхідності утримувати велику структуру персоналу, що значно здешевлює адміністративні витрати, а головне мінімізує і виключає корупцію. Інформація про об'єкти нерухомості, угоди, реєстрацію прав власності, обтяження і стан об'єктів повинна буде заноситися в розподілені реєстри, доступ до яких можна буде отримати і з персональних комп'ютерів, і через мобільні додатки.

Таким чином, для переходу системи державного управління на технологію блокчейн важливо розробити юридично вивірений і висококонтрольований механізм передачі офлайн-даних до державних реєстрів.

Головна проблема технології наразі – це недосконалі механізми регулювання. Адже концепція регулювання прогресивної технології сама по собі є нереальною і недосяжною. Тож варто зосередитись на створенні певних світових стандартів, а також етичних принципів та принципів належного управління, оскільки вони по суті є інструментами, необхідними для росту та розвитку нової технології. Але при цьому вкрай важливо уникнути надмірного регулювання.

Ефективна робота залежить насамперед від точності формування реєстрів громадян, нерухомості та компаній. Справа в тому, що ні збереження цілісності даних у разі випадкових збоїв чи атак, ні запобігання маніпуляціям з уже введеними даними не є головними загрозами для державних IT-систем. Справжньою небезпекою є внесення до реєстрів завідомо недостовірних даних. Вочевидь, сервіс блокчейн тут виявляється безсилим. Він є лише інструментом.

В Україні здійснюються певні кроки щодо законодавчого оформлення існуючих правовідносин у сфері технології блокчейн. Так, 6 жовтня 2017 року у Верховній Раді було зареєстровано проєкт Закону "Про обіг криптовалют в Україні", який має на меті впорядкувати правовідносини щодо обігу, зберігання, володіння, використання та проведення операцій з криптовалютами в Україні. Втім, цей проєкт має загальний вигляд, містить лише термінологічні визначення та обмежено визначає статус і порядок здійснення операцій з криптовалютами, а не технологію блокчейн. В інших вітчизняних законодавчих актах щодо правового статусу криптовалют питання блокчейну взагалі не визначено.

Блокчейн все ще може бути незрілою технологією з масштабованістю і регулятивними проблемами, але він має великий потенціал для розвитку в Україні, особливо у сфері фінансів, логістики, охорони здоров'я та енергетики.

Уряд України вже взяв на озброєння деякі ініціативи щодо розвитку технології блокчейн в країні. Наприклад, у 2018 році було створено спеціальний робочий групу з блокчейн технологій, яка займається розробкою рекомендацій щодо розвитку блокчейну в Україні та сприяє створенню нових проектів у цій сфері.

Також, в Україні було створено перший блокчейн-акселератор – програму, яка надає фінансову та інфраструктурну підтримку для розвитку блокчейн-стартапів. На додаток до цього, в Україні активно досліджується використання технології блокчейн у галузі енергетики, охорони здоров'я та громадських послуг.

Висновки. Під час дослідження було виявлено що нинішні державні установи наразі є застряглими в застарілих системах і нездатними досягти нових результатів, які від них очікують сьогоднішні споживачі. Проаналізувавши приклади впровадження технології блокчейн, можна дійти до висновку, що на сьогоднішній день технологія блокчейн потребує певної роботи, щоб ефективно інтегруватися в урядовий сектор України. Масштабованість та

споживання енергії - лише деякі приклади проблем, які потрібно подолати, щоб побачити ефективні результати від блокчейну.

Блокчейн надає високоефективні засоби захисту конфіденційності та доступності інформації, а також дозволяє створювати повністю децентралізовані системи. Інтеграція блокчейн-рішень в систему електронного уряду дозволяє трансформувати, оптимізувати і навіть автоматизувати адміністративні послуги в державному і муніципальному секторах в таких сферах, як реєстрація прав власності, забезпечення функціонування реєстрацій документів, міграційний контроль, встановлення особистих даних та інші послуги електронного управління.

Проте на поточному етапі правового впорядкування потребують такі питання: юридичний статус технології блокчейн, питання щодо зберігання, володіння, застосування та інших операцій з цією технологією, правовий статус уповноважених суб'єктів, відповідальних за її функціонування, процедура доступу до інформації в системі, відносини між власниками даних та власником системи, умови обробки інформації в системі, а також забезпечення захисту інформації в системі.

Надалі широке використання технології блокчейн у сфері взаємодії з громадськістю дозволить скоротити кількість державних службовців, усунути корупційні фактори, дебюрократизувати сектор адміністративних послуг, створити сприятливі умови для покращення інвестиційного середовища для розробки та підтримки новітніх технологій, а також налагодити ефективну взаємодію між бізнесом, громадянами та владою в Україні.

Розвиток технології блокчейн в Україні має значний потенціал та може відкрити нові можливості для бізнесу та суспільства в цілому. Однак, для досягнення успіху у цій сфері потрібна активна підтримка влади та бізнесу, а також розвиток відповідної інфраструктури та правового поля.

Список використаних джерел

1. Доронін І. М. Блокчейн, суспільство і держава: проблеми правотворчості. ІТ-право: проблеми та перспективи розвитку в Україні: зб. матер. І Міжнар. наук.-практ. конф. (м. Львів, 17 листоп. 2017 р.). Львів: НУ «Львівська політехніка», 2017. С. 73-78.
2. What Is a Block in the Blockchain? — [Електронний ресурс]. – Режим доступу: https://medium.com/datadriveninvestor/what-is-ablock-in-the-blockchain-c7a420270373.
3. D5 Charter. – [Електронний ресурс]. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386290/
4. Желтухін Є. Юристи та технології: точки дотику. Юридична Газета. 2017. 14 листоп. No 46 (596). С. 26-27.
5. Melanie Swan. Blockchain: Blueprint for a New Economy, 2015.
6. Меморандум про взаєморозуміння та співробітництво між Міністерством юстиції України, Міністерством аграрної політики та продовольства України. Державним агентством з питань електронного урядування України, громадською організацією Transparency International Україна та Бітфурі ХолдінгБ. В.
7. Стефанчук Р. Інформаційні технології та право: Право України. 2018. С. 30-50.
8. Тапскотт Д., Тапскотт А. Революція блокчейнів: як технологія, що стоїть за біткойнами та іншими криптовалютами, змінює світ. 2020 рік. С. 78-79
9. Башир І. Освоєння блокчейну: пояснення технології розподіленої книги, децентралізації та розумних контрактів. 2018 рік. С. 91.
10. Колегова Д. Розумний договір як інструмент юридичного забезпечення транзакцій в мережах блокчейн: правові виклики та перспективи розвитку. 2018 рік.
11. Шин Л. Останній посібник із розуміння блокчейн-системи. 2019 рік.

Робота виконана під науковим керівництвом д.е.н., професора
ТОКАРЯ В.В.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА ПРОГРАМНОЇ ПЛАТФОРМИ BOOKIMED У РОЗВИТКУ МЕДИЧНОГО ТУРИЗМУ

ШИШКО В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Стаття присвячена ролі штучного інтелекту, медичного туризму та програмної платформи Bookimed забезпечує якісну медичну допомогу пацієнтам. Вона розглядає можливості та перспективи використання штучного інтелекту в медичному туризмі, а також роль програмної платформи Bookimed у полегшенні процесу пошуку найкращих медичних закладів та зменшенні витрат на медичний туризм. Стаття також розглядає позитивні дослідження медичного туризму, зокрема, доступ до найсучасніших технологій та процедур, які ще не є доступними в країні проживання. Висвітлення цих тем допоможе читачам зрозуміти свідомість штучного інтелекту, медичного туризму та програмної платформи Bookimed у забезпеченні високої якості медичної допомоги пацієнтам.

This article is devoted to the role of artificial intelligence, medical tourism, and the Bookimed software platform in providing quality medical care to patients. It explores the possibilities and prospects of using artificial intelligence in medical tourism, as well as the role of the Bookimed software platform in facilitating the process of finding the best medical institutions and reducing the cost of medical tourism. The article also highlights the positive consequences of medical tourism.

Актуальність. Медичний туризм є однією з найбільш швидкорозвиваючих галузей в світі туризму, і його розвиток в Україні має великий потенціал.

Україна має потужний потенціал в галузі медичного туризму, завдяки високому рівню медичної освіти та низьким цінам на медичні послуги. Проте, для того, щоб розвиток медичного туризму в Україні став успішним, необхідно мати якісні медичні послуги, а також забезпечувати високий рівень обслуговування для іноземних пацієнтів.

У цьому контексті Bookimed має важливу роль в розвитку медичного туризму в Україні, як компанія, що займається організацією та координацією медичних послуг для іноземних пацієнтів. Їхні послуги допомагають залучати іноземних клієнтів та стимулюють розвиток медичного туризму в Україні.

Також важливо зазначити, що у зв'язку з пандемією COVID-19, медичний туризм по всьому світу зазнав значних змін. Україна не стала винятком і також зазнала складнощів в розвитку медичного туризму. Однак, з поступовим покращенням ситуації, можна очікувати, що медичний туризм в Україні знову набере обертів, тому роль Bookimed у цьому процесі залишається дуже важливою.

Метою статті є показати, як можна застосувати AI технології для поліпшення якості медичних послуг та досліджень. Стаття має на меті описати, як розробники можуть використовувати AI для створення більш ефективних та персоналізованих веб-сайтів на застосунків в галузі медицини, які допомагають лікарям та пацієнтам швидше та точніше знаходити необхідну інформацію, здійснювати діагностику для лікування різних хвороб.

Об'єктом статті є штучний інтелект, що впроваджується у сферу медичних послуг.

Предметом дослідження є впровадження AI-технологій в розробку веб-сайтів як засобу поліпшення якості медичних послуг та зниження їх вартості. Розглянуться можливості використання штучного інтелекту для оптимізації процесів в галузі медицини та для розробки інноваційних медичних продуктів, що можуть допомогти пацієнтам отримувати більш якісну та доступну медичну допомогу. А також компанія Bookimed як провайдер медичних послуг для іноземних пацієнтів в Україні.

Аналіз попередніх досліджень. Наукові статті на тему аналізу ринку медичного туризму в Україні та ролі Bookimed в його розвитку досить рідкісні. Проте, деякі дослідження вже були проведені в цій області.

Наприклад, стаття "Медичний туризм в Україні: стан та перспективи" є досить інформативною і містить багато важливої інформації про медичний туризм в Україні. Автори досліджують стан медичного туризму в країні та виділяють основні переваги, недоліки та перспективи розвитку даної галузі. У статті наведені статистичні дані про розвиток медичного туризму в Україні, зокрема, про кількість іноземних туристів, які зверталися до медичних закладів країни, та про кількість медичних закладів, які пропонують послуги медичного туризму. Також автори зазначають, що недоліками медичного туризму в Україні є недостатня кількість англомовних лікарів та медичних працівників, а також низька якість медичних послуг у деяких медичних закладах. Однак, в статті зазначено, що українські медичні заклади мають висококваліфікованих лікарів та невисокі ціни на медичні послуги, що може привернути увагу іноземних туристів. Також зазначається,, що розвиток медичного туризму в Україні може стати важливим чинником для зміцнення економіки країни та збільшення кількості робочих місць у медичній галузі. Для досягнення цих цілей автори статті пропонують ряд заходів, зокрема, покращення інфраструктури медичного туризму, розвиток партнерських відносин з міжнародними партнерами, залучення іноземних інвесторів та зміцнення правового поля.

Джефрі Гінтон - відомий професор зі штучного інтелекту з університету Торонто і засновник компанії Google Brain, що займається дослідженнями глибокого навчання (deep learning). У статті "Deep learning—a technology with the potential to transform health care" він обговорює можливості глибокого навчання для трансформації галузі охорони здоров'я.У своїй статті Гінтон стверджує, що глибоке навчання може допомогти у вирішенні різноманітних проблем в галузі медицини, таких як діагностика, лікування та передбачення результатів. Він також зазначає, що технології глибокого навчання можуть бути особливо корисними в медицині, де дуже важливо збирати та аналізувати велику кількість даних, щоб зробити точні діагнози та надати ефективне лікування.У статті також згадується про використання глибокого навчання для розробки нових методів діагностики захворювань, включаючи розпізнавання зображень зі скануванням мозку та дослідження геноміки. Крім того, глибоке навчання може бути використано для передбачення результатів лікування та прогнозування ризиків захворювання.

У загальному, стаття Гінтона підтверджує важливість технологій штучного інтелекту та глибокого навчання в галузі медицини та їх потенціал для зміни підходів до діагностики та лікування різних захворювань.

В сучасному світі медичний туризм набуває все більшої популярності. Із зростанням доступності міжнародних перельотів та розвитком медичних технологій, все більше людей вирушають за кордон для отримання якісної та доступної медичної допомоги. Україна відноситься до країн, які мають великий потенціал у розвитку медичного туризму, насамперед це пов'язано з доступністю якісної медичної допомоги та відносно низькими цінами на неї (наприклад, Рис.1. порівняння лікування безпліддя в Україні та Німеччині).

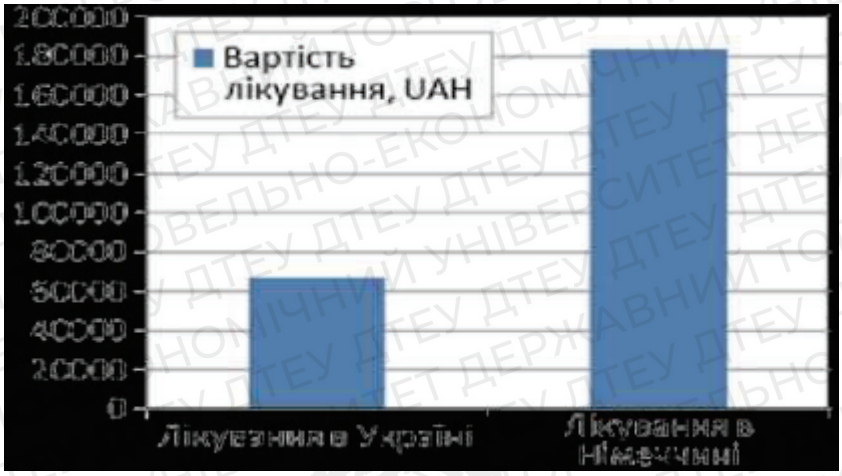


Рис. 1. Медичний туризм міста Львова: соціально-економічні можливості для розвитку

За даними Міністерства розвитку економіки, торгівлі та сільського господарства України, кількість іноземних громадян, які приїхали до України для отримання медичної допомоги, збільшилася у 2021 році на 27,6% порівняно з 2020 роком. Загалом, відсоток зростання медичного туризму в Україні становить більше 10% щорічно. З цих даних можна зробити висновок, що медичний туризм є важливою галуззю для розвитку економіки України та відіграє вагому роль у забезпеченні якісної медичної допомоги для іноземних пацієнтів.

Україна є відомою своїми унікальними природними лікувальними джерелами, курортами та сучасними клініками, що надають високоякісні медичні послуги. Серед основних напрямків медичного туризму в Україні можна виділити:

1. Лікувальні курорти. Україна має багато курортів, де можна отримати лікування за допомогою мінеральних вод, грязей, клімату та інших природних чинників;
2. Естетична медицина. Розвинена галузь естетичної медицини, де пропонуються різноманітні процедури, такі як пластична хірургія, контурна пластика, ботокс, філлери та інші;
3. Стоматологія. Стоматологія є одним з найбільш популярних напрямків медичного туризму в Україні. Багато клінік пропонують послуги з відновлення та лікування зубів, включаючи імплантацію зубів, ортодонтичні процедури, протезування;
4. Репродуктивна медицина. Україна відома своїми передовими клініками з репродуктивної медицини, де проводяться програми штучного запліднення, в тому числі, програми сурогатного материнства;
5. Нейрохірургія. Велика кількість кваліфікованих фахівців у галузі нейрохірургії та нейрології, що надають послуги з лікування різноманітних захворювань головного мозку та нервової системи;
6. Кардіологія. Високооснащені клініки та кардіоцентри, де проводяться діагностика та лікування кардіологічних захворювань;
7. Офтальмологія. Україна має клініки з передовими технологіями та професійними офтальмологами, які надають послуги з діагностики та лікування офтальмологічних захворювань, таких як катаракта, глаукома та інші.

Аналіз ринку медичного туризму в Україні відображає стан справ у галузі та дозволяє зрозуміти потенціал та перспективи розвитку. Bookimed виконує важливу роль у розвитку медичного туризму, забезпечуючи доступ до високоякісних медичних послуг для пацієнтів з різних країн світу. Дана платформа - це один з провідних сервісів медичного туризму в Україні, який активно сприяє розвитку цього напрямку в країні, забезпечує можливість обрати медичний заклад відповідно до потреб пацієнта та забезпечує підтримку та консультування на всіх етапах лікування.

Також важливо зазначити, що у зв'язку з пандемією COVID-19, медичний туризм по всьому світу зазнав значних змін. Україна не стала винятком і також зазнала складнощів в розвитку медичного туризму. Однак, з поступовим покращенням ситуації, можна очікувати, що медичний туризм в Україні знову набере обертів, тому роль Bookimed у цьому процесі залишається дуже важливою

Війна в Україні спричинила складні умови для розвитку медичного туризму. На жаль, у зоні конфлікту та прилеглих територіях, які були раніше популярними для туристів, суттєво постраждали медичні заклади та інфраструктура. Додатково, наявність зони конфлікту створює певний ризик для іноземних пацієнтів, які можуть стати свідками бойових дій або потрапити у небезпечну ситуацію. Це може відлякувати туристів від візиту до України для медичного лікування.

Крім того, економічні проблеми, які супроводжують війну, можуть суттєво позначитися на якості медичних послуг, забезпеченні медичною технікою та медикаментами. Тим не менш, в Україні діє низка медичних закладів, які надають високоякісні послуги іноземним пацієнтам, зокрема в області репродуктивної медицини та стоматології. Також існують ініціативи залучення іноземних інвесторів для розвитку медичного туризму в інших регіонах України, що не потерпають від війни.

Ключову роль у розвитку медичного туризму в Україні відіграє Bookimed. Заснована в 2014 році, компанія за майже 10 років свого існування здобула величезний досвід у цій сфері та надає високоякісні послуги своїм клієнтам. Однією з найбільших переваг Bookimed є їхній досвід та знання ринку медичного туризму в Україні. Компанія має широку мережу клінік-партнерів, з якими вони співпрацюють протягом багатьох років, тому можуть забезпечити найвищу якість медичних послуг та найбільш вигідні ціни для своїх клієнтів. Крім того, Bookimed відкриває для іноземних пацієнтів доступ до медичних послуг в Україні, які раніше були недоступні.

Основна стратегія компанії - це індивідуальний підхід до кожного клієнта та надання повного спектру послуг від підготовки до подорожі та бронювання до післяопераційної реабілітації та підтримки клієнта впродовж усього перебування в Україні. Компанія має власний медичний перекладач та координатора, які забезпечують підтримку клієнта під час усіх етапів лікування.

Bookimed дбає про те, щоб клієнти отримували найкращі медичні послуги від провідних клінік України та забезпечує повний спектр медичних послуг у таких галузях, як кардіологія, онкологія, репродуктивна медицина, стоматологія та інші. Однією з найбільших переваг Bookimed є їхній досвід та знання ринку медичного туризму в Україні. Компанія має широку мережу клінік-партнерів, з якими вони співпрацюють протягом багатьох років, тому можуть забезпечити найвищу якість медичних послуг та найбільш вигідні ціни для своїх клієнтів. Крім того, Bookimed відкриває для іноземних пацієнтів доступ до медичних послуг в Україні, які раніше були недоступні.

Алгоритми штучного інтелекту використовуються для аналізу медичних даних, таких як записи пацієнтів, геномні дані, медичні зображення та інші джерела даних, щоб забезпечити більш точну діагностику та лікування. Наприклад, AI можна використовувати для виявлення ранніх ознак захворювань шляхом аналізу медичних зображень, таких як рентгенівські знімки або МРТ. Інші приклади застосування AI в охороні здоров'я включають віддалений моніторинг пацієнтів. Системи віддаленого моніторингу з підтримкою AI дозволяють медичним працівникам віддалено збирати біометричні дані пацієнтів в режимі реального часу і швидко виявляти відхилення або ознаки проблем зі здоров'ям, що насуваються.

Процес підбору клініки за допомогою штучного інтелекту: він може відрізнятися в залежності від того, як саме був реалізований цей інструмент. Однак, загалом, процес може включати наступні кроки:

1. Збір інформації про клініки: штучний інтелект може збирати дані про клініки з різних джерел, таких як бази даних;

2. Аналіз та оцінка даних: після збору даних, система може аналізувати їх та виконувати оцінку якості клінік на основі різних параметрів, таких як відгуки пацієнтів, медичні статистики, кваліфікації медичного персоналу та інше;

3. Підбір найкращої клініки: на основі аналізу даних, штучний інтелект може вибрати декілька найкращих клінік для пацієнта;

4. Рекомендації: система може рекомендувати пацієнту найкращу клініку, враховуючи його особисті потреби та вимоги;

5. Підтримка в прийнятті рішення: штучний інтелект може надати пацієнту додаткову інформацію про клініки, щоб допомогти йому прийняти правильне рішення.

Впровадження технологій штучного інтелекту в медичні консультаційні застосунки може допомогти підвищити точність діагнозів, оптимізувати догляд за пацієнтами та підвищити ефективність роботи медичних працівників. Наприклад, поширеною проблемою є точна діагностика захворювань на основі симптомів і історії хвороби пацієнта. Алгоритми машинного навчання можна використовувати для аналізу великих обсягів медичних даних і надання рекомендацій на основі патернів. Збір та аналіз даних з електронних медичних карт, медичних журналів та інших релевантних джерел для навчання моделей штучного інтелекту. Дані повинні бути характерними для групи пацієнтів, для яких призначений застосунок. Інтеграція AI технологій в робочий процес застосунку або сайту, щоб надавати медичним працівникам рекомендації та поради в режимі реального часу, наприклад, чат-бот зі штучним інтелектом може допомогти сортувати пацієнтів і ставити початкові діагнози на основі симптомів.

AI технології можуть бути дуже корисними для пацієнтів, які шукають інформацію про лікування, перевірених лікарів та клініки. Пошукові алгоритми AI допомагають пацієнтам знайти найбільш ефективні методи лікування та найкращі клініки для отримання медичної допомоги. Щоб пошук був ефективним для пацієнтів, розробники можуть використовувати пошукові алгоритми, які ретельно аналізують дані про лікування та клініки з різних джерел, таких як медичні журнали, бази даних медичних досліджень, відгуки пацієнтів та інші джерела. Алгоритми можуть враховувати різні параметри, наприклад, типи лікування, рівень ефективності лікування, вартість, рейтинг клініки та інші фактори.

AI може бути використаний для розробки віртуальних асистентів, які допоможуть пацієнтам отримувати швидку та точну інформацію про лікування та клініки, а також можуть допомогти пацієнтам зрозуміти їх медичну історію та плани лікування.

Звичайно, точність та ефективність штучного інтелекту залежить від якості даних, які він отримує, та від того, наскільки добре він настроєний для роботи в конкретній галузі. Тому важливо ретельно перевіряти роботу системи та контролювати якість даних, щоб забезпечити максимально точні результати.

Технології AI корисні при розробці сайтів з медичного туризму бо AI може пропонувати пацієнтам медичні тури, які найкраще відповідають їхнім потребам та бюджету. Алгоритми машинного навчання можуть враховувати такі фактори, як місцезнаходження, терміни лікування, типи процедур та багато іншого. Також штучний інтелект може допомогти пацієнтам отримати консультації від лікарів дистанційно. Це корисно для тих, хто шукає допомогу від лікарів з інших країн або для тих, хто не може фізично відвідати клініку.

AI може допомогти відстежувати тенденції в галузі медичного туризму та спрогнозувати попит на різні види процедур та напрямки лікування. Це може бути корисно для розробки бізнес-стратегій та маркетингових кампаній.

На даний момент розвиток медичного туризму в Україні є перспективним напрямком. За даними Міністерства охорони здоров'я України, кількість іноземних пацієнтів, які отримують медичні послуги в Україні, зростає з кожним роком.

Уряд України активно підтримує розвиток медичного туризму, зокрема, шляхом вдосконалення законодавства, створення сприятливих умов для інвестування у медичний сектор, підвищення рівня медичної освіти та підготовки кваліфікованого медичного персоналу.

Також прогнозується збільшення кількості медичних закладів та збільшення їх обсягу фінансування, що дозволить підвищити якість медичних послуг.

Зростання популярності медичного туризму в Україні також може бути викликане збільшенням кількості спеціалізованих клінік, які спеціалізуються на наданні конкретних видів медичних послуг, та зростанням популярності альтернативної медицини.

У світлі цих факторів, прогнозується подальший розвиток медичного туризму в Україні та збільшення кількості іноземних пацієнтів, які обирають Україну як медичний туристичний напрямок.

Bookimed також відіграє важливу роль у зростанні довіри до вітчизняних лікарів серед українського населення, оскільки компанія співпрацює тільки з найкращими клініками України, які мають високу репутацію, і надають якісні послуги. Компанія пропонує своїм клієнтам консультації з висококваліфікованими медичними експертами, які можуть допомогти зрозуміти суть проблеми та призначити найкращі методи лікування. Також, завдяки своєму досвіду та знанням про медичні послуги в Україні, Bookimed допомагає іноземним пацієнтам знайти найкращі клініки та лікарів в країні. Це сприяє зростанню популярності українських медичних закладів серед іноземних пацієнтів та зміцненню довіри до вітчизняних лікарів.

Отже, Bookimed робить чималий внесок, та прикладає всі зусилля в підвищення якості та рівня медичних послуг в Україні, що в свою чергу сприяє зростанню довіри до вітчизняних лікарів та підвищенню престижу української медицини в світі.

Висновок. У статті було проведено аналіз ринку медичного туризму в Україні, зокрема зосереджено увагу на потенційних перевагах та недоліках цього ринку. На основі проведеного аналізу можна зробити висновок, що розвиток медичного туризму в Україні є перспективним напрямком і має великий потенціал для подальшого росту.

Одним із провідних гравців на ринку медичного туризму в Україні є компанія Bookimed.

Розглянуто історію створення та розвитку компанії, її стратегію та підхід до клієнтів. Виявлено, що Bookimed має декілька переваг, які дозволяють їй успішно конкурувати на ринку медичного туризму в Україні. Серед них можна виділити широку мережу партнерських клінік, високу якість обслуговування та професійність працівників.

Також було досліджено вплив Bookimed на зростання довіри до вітчизняних лікарів. Виявлено, що компанія вносить значний вклад у підвищення рівня довіри до українських медичних закладів та пропагує високі стандарти медичної практики.

Прогнозуючи розвиток медичного туризму в Україні в майбутньому, можна стверджувати, що ринок буде надалі зростати та розвиватися, що створює нові можливості для покращення якості медичної допомоги та забезпечення доступності для пацієнтів з усього світу.

Можна стверджувати, що Bookimed зіграв важливу роль в розвитку медичного туризму в Україні, зокрема в підвищенні рівня довіри

Список використаних джерел

1. Бордун О.Ю., Наука й економіка. 2016. №1(41). С.78-85. Медичний туризм міста Львова: соціально-економічні можливості для розвитку \\ https://tourlib.net/statti_ukr/bordun7.htm
2. Інформаційне управління. Опубліковано 25 березня 2016. Медичний туризм в Україні: проблеми та перспективи \\ https://www.rada.gov.ua/news/Novyny/127061.html
3. Prof. Dr. Keun Ho Ryu, Prof. Dr. Nipon Theera-Umpon, Artificial Intelligence in Healthcare \\ https://www.mdpi.com/topics/artificial_intelligence_healthcare

Робота виконана під науковим керівництвом кандидата технічних наук, доцента РЗАЄВОЇ С.Л.

ЗАХИСТ ДАНИХ У ТЕХНОЛОГІЯХ БЕЗПРОВІДНОГО ЗВ'ЯЗКУ СТАНДАРТУ IEEE 802.16

ШУЛЯЄВ Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні засади побудови системи захисту даних у технологіях безпровідного зв'язку стандарту IEEE 802.16. На теперішній час перед багатьма підприємствами постає питання швидкої та якісної організації захисту каналів зв'язку. Таким чином підвищити ефективність бізнесу – використання сучасної технології бездротової передачі даних WiMAX, яка дозволяє швидко та якісно вирішити задачі забезпечення зв'язку там, де це надзвичайно складно, або навіть неможливо зробити, використовуючи традиційні мережі.

The article discusses the basic principles of building a system for protecting a private network of a trade enterprise of the IEEE 802.16 standard. At present, many enterprises face the question of quick and high-quality organization of communication channels. In this way, to increase business efficiency - the use of modern WiMAX wireless data transmission technology, which allows you to quickly and efficiently solve the problems of providing communication where it is extremely difficult, or even impossible, to do using traditional networks.

Актуальність. Інформаційні магістралі сьогодні не поступаються по важливості транспортним, вони всюди – і на суші, і на дні океану, і в космосі. На сьогоднішній момент визначено три основних вимоги до мережевих з'єднань: висока пропускна здатність, надійність, мобільність. З'єднати всі три основних критерії може тільки покоління безпровідних технологій стандарт IEEE 802.16 − WiMAX (Worldwide Interoperability for Microwave Access).

WiMAX – це система далекої дії, що покриває кілометри простору, яка зазвичай використовує ліцензовані спектри частот (хоча можливо і використання не ліцензованих частот) для надання з'єднання із інтернетом типу точка-точка провайдером кінцевому користувачеві. Різні стандарти сімейства 802.16 забезпечують різні види доступу, від мобільного (схожий з передачею даних із мобільних телефонів) до фіксованого (альтернатива провідникового доступу, при якому бездротове обладнання користувача прив'язане до розташування). У загальному вигляді WiMAX мережі складаються з наступних основних частин – базових і абонентських станцій, а також обладнання, що зв'язує базові станції між собою, з постачальником Інтернету. Для з'єднання базової станції з абонентською використовується високочастотний діапазон радіохвиль від 1,5 до 11 ГГц. В ідеальних умовах швидкість обміну даними може досягати 70 Мбіт/с, при цьому не вимагається забезпечення прямої видимості між базовою станцією і приймачем. WiMAX застосовується як для вирішення проблеми надання доступу в Інтернет офісним та районним мережам.

При цьому, принаймні одна базова станція підключається до мережі провайдера з використанням класичних дротових з'єднань. Однак, чим більше число базових станцій (БС) підключено до мереж провайдера, тим вища швидкість передачі даних і надійність мережі в цілому. Структура мереж сімейства стандартів IEEE 802.16 схожа із традиційними GSM мережами (базові станції діють на відстанях до десятків кілометрів, для їх встановлення не обов'язково будувати вежі – допускається установка на дахах будинків при дотриманні умови прямої видимості між станціями).

Метою статті є дослідження захисту даних у технологіях безпровідного зв'язку стандарту IEEE 802.16.

Об'єктом дослідження є розробка захищеної мережі безпровідного зв'язку стандарту IEEE 802.16.

Предмет дослідження – захищена мережа безпровідного зв'язку стандарту WiMAX.

Аналіз попередніх досліджень. Дослідженню системи захисту безпровідної мережі стандарту IEEE 802.16 присвячені праці вітчизняних та закордонних науковців: А. С. Шевченка, А. В. Чунарьової, Г. В. Микитина, А. І. Ребеця, Р. І. Банаха та ін.

Виклад основного матеріалу. Безпровідні мережі забезпечують мобільність клієнта, його здатність підключатися до мережі з будь-якого місця і в будь-який час, а також можливість переміщення без втрати з'єднання Хоча безпровідна мережа використовує радіочастоти замість кабелів, вона зазвичай реалізована в комутованій мережі, а формат кадру аналогічний тому, що використовується в Ethernet. Сьогодні корпоративні мережі розвиваються швидкими темпами, забезпечуючи підтримку користувачів, які постійно перебувають в роз'їздах. Користувачі можуть підключатися, використовуючи різні пристрої, включаючи комп'ютери, ноутбуки, планшетні комп'ютери і смартфони. В рамках даної концепції мобільності користувачі можуть підключатися до мережі, перебуваючи в русі.

Безпровідний зв'язок тягне за собою безліч переваг як для корпоративних, так і для домашніх мереж. До таких переваг належать підвищені гнучкість і продуктивність, зниження витрат, можливість розвитку та адаптації до мінливих вимог Використання безпровідних мереж також дозволяє знизити витрати. У компаніях, де вже використовується безпровідна інфраструктура, економія витрат реалізується при кожній зміні або переміщенні обладнання – наприклад, при переміщенні співробітника в межах будівлі або реорганізації обладнання або лабораторії, переміщенні в тимчасові офіси або об'єкти в рамках того чи іншого проекту. Ще однією важливою перевагою бездротових мереж є здатність адаптуватися до зміни потреб і технологій. Додавання нового обладнання в бездротову мережу не викликає особливих труднощів. Користувачі за допомогою бездротового підключення в домашніх умовах можуть відвідувати веб-сайти, сидячи за кухонним столом, перебуваючи у вітальні або навіть поза приміщенням. Користувачі домашньої мережі підключають нові пристрої (наприклад смартфони, планшетні комп'ютери, ноутбуки і телевізори з інтелектуальними функціями) [1,2].

WiMAX (протокол широкосмугового радіозв'язку) – стандарт мереж IEEE 802.16, який забезпечує безпровідний широкосмуговий доступ на відстанях до 50 км (30 миль). WiMAX є альтернативою кабельному і широкосмугового DSL-підключення. У 2005 році в стандарт WiMax були додані мобільні функції, завдяки чому цей стандарт можуть використовувати оператори зв'язку для надання стільникового широкосмугового доступу.

WiMAX підходить для вирішення наступних заадач:

- З'єднання точок доступу Wi-Fi один з одним та з іншими сегментами Інтернету.
- Забезпечення безпровідного широкосмугового доступу як альтернативи виділеним лініям і DSL.
- Надання високошвидкісних сервісів передачі даних і телекомунікаційних послуг.
- Створення точок доступу, не прив'язаних до географічного положення.
- Створення систем віддаленого моніторингу системи.

WiMAX дозволяє здійснювати доступ в Інтернет на високих швидкостях, з набагато кращим покриттям, ніж у Wi-Fi-мереж. Це дозволяє використовувати технологію в якості «магістральних каналів», продовженням яких виступають традиційні DSL і виділені лінії, а також локальні мережі. В результаті подібний підхід дозволяє створювати масштабовані високошвидкісні мережі в рамках міст.

Безпровідні комп'ютерні мережі – це сучасна альтернатива традиційної провідної мережі, яка спирається на кабелі для підключення пристроїв до мережі разом. Безпровідні технології широко використовуються в домашніх і корпоративних комп'ютерних мережах. Безпровідні мережі мають безліч застосувань. В офісах на робочому місці, це полегшує спільне використання файлів, принтерів і доступ в інтернет між усіма комп'ютерами. Вдома

чи в домашньому офісі мережі дозволяє користувачам виконувати друк з ноутбука без необхідності йти до принтера і підключатися до нього.

Стандарт IEEE 802.16 описує роботу в діапазоні 10–66 ГГЦ систем з архітектурою «точка – багато точка». Це – двонаправлена система, тобто передбачені прямі і зворотні потоки. При цьому канали широкосмугові, а швидкості передачі – високі. Тракт обробки даних і формування вихідного сигналу для передачі через радіоканал у стандарті IEEE 802.16 досить звичайний для сучасних телекомунікаційних протоколів і практично однаковий для зворотних і прямих з'єднань. Вхідний потік даних скремблюється – піддається рандомізації, тобто на нього накладається псевдовипадкова послідовність, вироблювана за допомогою лінійного регістра зрушення довжини з характеристичним багаточленом і початковим заповненням. Далі скрембльовані дані кодують за допомогою завадостійких кодів. При цьому використається одна із чотирьох схем: код Рида-Соломона, код Рида-Соломона з додатковим надточним кодом (швидкість), код Рида-Соломона з додатковим контролем парності і блоковий турбокод. Розмір кодованого інформаційного блоку й число надлишкових біт не фіксовані – ці параметри можна задавати залежно від умов середовища й вимог до якості надання послуг. Перші дві схеми кодування обов'язкові для всіх пристроїв стандарту, інші два алгоритми – додаткові [1].

Побудова мережі WiMAX припускає використання трьох типів устаткування – базові станції (БС), абонентський комплект (абонентська станція – АС) і устаткування для організації зв'язку між базовими станціями – ретрансляційні станції (РС).

Кожний з модулів (або радіоінтерфейсів у двомодульних моделях) забезпечує обслуговування одного просторового сектора в межах діаграми спрямованості використовуваної антени. Типові значення зони охоплення кожного сектора 360° (один сектор), 120° (три сектори), і 60° (шість секторів). Устаткування БС не накладає певних вимог до ширини сектора, що у конкретних випадках може бути довільною, обумовленою конкретною топологією мережі, наявністю частотного ресурсу й розміщенням абонентів [1].

До складу БС входять [2]:

- Бездротові маршрутизатори R5000 – від 1 до 6, по одному на сектор. Для малопотужних БС можуть використатися двохмодульні бездротові маршрутизатори – по одному на два сектори. Односекторні БС забезпечують швидкість передачі до 54 Мбіт/с. Багатосекторні БС які забезпечують роботу зі швидкістю до 48 Мбіт/з на сектор; антенно-фідерні пристрої – по кількості секторів базової станції; ліцензії для підключення спеціалізованих абонентських станцій, на кожен сектор базової станції; програмне забезпечення для керування мережею; комутатор Ethernet; шафа для монтажу встаткування; джерела безперебійного живлення. БС розміщаються на високих будівлях або антенних опорах, на яких установлюють й інші радіосистеми, що приводить до підвищення загального рівня перешкод.
- Ретрансляційна станція (РС) призначена для підвищення дальності дії БС, обходу великих перешкод, а також для створення протяжних магістральних каналів точка-точка. Кількість підключень послідовно РС не обмежена. До кожної РС може бути підключена одна або трохи РС й/або АС До складу РС входять: двохмодульний безпровідний маршрутизатор R5000; спрямована антена для зв'язку із БС (у випадку РС без інтегрованої антени); всеспрямована, секторна або спрямована антена для підключення АС й/або РС; кабелі для підключення антен; ліцензія для підключення спеціалізованих АС до РС.
- Абонентська станція (АС) призначена для безпровідного підключення абонентів до БС або РС, а також для створення магістральних каналів «точка-точка».

Склад АС: абонентський бездротовий маршрутизатор з інтегрованою антеною або рознімання для підключення зовнішньої антени; спрямована антена й антенний кабель для моделей без інтегрованої антени.

Система керування мережею (Network Monitoring / Management System – NMS) призначена для моніторингу мережі в реальному часі з метою оперативного керування.

Специфікації стандарту WiMAX визначають передачу трафіку і сигнальний обмін тільки на радіоінтерфейсу. Що стосується з'єднання БС з Інтернетом, мережами безпровідного доступу та мережами різних операторів, рішення по архітектурі мережі приймає оператор спільно з виробником. З метою уніфікації та певної оптимізації WiMAX Forum запропонована базова архітектура мережі. NRM (Network Reference Model - базова модель мережі) WiMAX, яка є логічним поданням мережевої архітектури. NRM розділяє систему на три логічні частини:

1. Мобільні станції, використовувані абонентами для отримання доступу до мережі;

2. ASN (Access Services network) − мережа доступу до послуг, що є власністю оператора доступу до мережі (NAP − Network Access Provider); ASN складається з однієї або декількох базових станцій, якими управляє один або кілька шлюзів ASN (ASN-GW).

3. CSN (Connectivity Services Nerwork) − підмережа оператора, що забезпечує вихід на IP і інші мережі для реалізації абонентських послуг. Ця підмережа забезпечує необхідні комутаційні функції та функції безпеки. Абонента може обслуговувати оператор домашньої мережі NSP (Network Services Provider). Абонент може також перебувати в роумінгу. У цьому випадку його обслуговує оператор візитною мережі; при цьому відбувається обмін сигнальної інформацією CSN візитною і домашнього оператора.

ASN виконує наступні функції: з'єднання на рівні L2 з AC; пошук і вибір мережі на основі переваг абонента про CSN / NSP; забезпечення безпеки: передача даних про пристрої, користувачів, і послугах, серверу безпеки, тимчасове зберігання профілів користувачів; організація наскрізних IP-з'єднань між AC і CSN; управління радіоресурсу (RRM) відповідно до класу трафіку і потрібним QoS; забезпечення мобільності, тобто виконання процедур хендовера, локалізації та пейджінга. Функціонально БС забезпечує як один сектор з виділеним частотним діапазоном, підтримуючи інтерфейс IEEE 802.16e з AC.

Шлюз ASN є основним елементом мережі. Під час сеансів зв'язку шлюз організовує хендовер абонентам і пейджинг AC, управляє доступом до мережі. Для кожного приєднаного абонента в шлюзі відкрита база даних, що містить профілі абонента і ключі шифрування. На шлюз покладені завдання авторизації потоку послуг згідно з профілем абонентів і QoS. У напрямку БС шлюз підтримує тунельне з'єднання; в напрямку ядра мережі (CSN) шлюз організовує з'єднання по стандартному IP протоколу.

Питання безпеки в мережах WiMAX (стандарт IEEE 802.16), як і в мережах WiFi (стандарт IEEE 802.11), загострено легкістю підключення до мережі. Безпека WIMAX-мережі забезпечується на фізичному рівні спеціально розробленими засобами, які вбудовані в пристрої бездротового зв'язку й керують процесом передачі даних радіоканалом, запобігаючи: спробам порушення конфіденційності; порушенню цілісності даних; порушенню автентичності джерела – споживача; відмови в обслуговуванні [1].

Якість зв'язку у WiMAX вища, чим в WiFi. При підключенні декількох користувачів до точки доступу Wi-Fi виникає проблема черговості доступу до канала зв'язку. Технологія WiMAX забезпечує кожному користувачеві постійний доступ, використовуючи алгоритм установлення обмеження на число користувачів для однієї точки доступу. При наближенні базової станції WiMAX до максимуму свого потенціалу, вона автоматично розподіляє «надлишкових» користувачів на іншу базову станцію. У безпровідній передачі даних немає універсальної технології. Під кожні конкретні завдання більше підходить WiMAX або Wi-Fi. Якщо поставлено завдання надати широкосмуговий доступ до мережі для користувачів, доцільніше використовувати WiMAX, тому що ця технологія була розроблена саме із цією метою. Однак, якщо завдання − надати широкосмуговий доступ в обмеженому приміщенні, то технології Wi-Fi і WiMAX однаково добре підходять для вирішення, за умови низького рівня перешкод або їх відсутності. Для впровадження безпровідних систем безпеки або відеоспостереження доцільніше скористатися технологією Wi-Fi. Головна відмінність між провідними і безпровідними мережами пов'язано з абсолютно неконтрольованою областю між кінцевими точками мережі. У досить широкому просторі мереж безпровідне середовище ніяк не контролюється. Сучасні безпровідні технології пропонують обмежений набір засобів управління всією областю розгортання мережі. Це дозволяє атакуючим, що знаходяться в

безпосередній близькості від безпровідних структур, створювати цілий ряд нападів, які неможливі в дротовому світі [1]. Підслуховування найбільш поширена проблема відкритих і некерованих середовищ, тобто бездротових мереж − можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати дані, як показано на Рис.1.

Рис.1. Атака «підслуховування».

Обладнання, що використовується для підслуховування в мережі, може бути не складніша від того, що використовується для звичайного доступу до цієї мережі. Щоб перехопити передачу, зловмисник повинен знаходитися поблизу від передавача. Перехоплення такого типу практично неможливо зареєструвати, і ще важче їм перешкодити. Використання антен і підсилювачів дає зловмисникові можливість перебувати на значній відстані від мети в процесі перехоплення. Підслуховування ведуть для збору інформації в мережі, яку згодом передбачається атакувати. Первинна мета зловмисника − зрозуміти, хто використовує мережу, яка інформація в ній доступна, які можливості мережевого устаткування, яка територія розгортання мережі. Все це знадобиться для того, щоб організувати атаку на мережу. Багато загальнодоступних мережних протоколів передають таку важливу інформацію, як ім'я користувача та пароль, відкритим текстом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Навіть якщо передана інформація зашифрована, в руках зловмисника з’являється текст, який можна запам'ятати і розкодувати. [2, 3].

Інший спосіб підслуховування − підключитися до безпровідної мережі. Активне підслуховування в локальній бездротовій мережі зазвичай грунтується на неправильному використанні протоколу Address Resolution Protocol (ARP). Спочатку ця технологія була створена для «прослуховування» мережі. Насправді ми маємо справу з атакою типу MITM («man in the middle» – «людина посередині») на рівні зв'язку даних. Вони можуть приймати різні форми і використовуються для руйнування конфіденційності та цілісності сеансу зв'язку. Атаки MITM більш складні, ніж більшість інших атак: для їх проведення потрібно детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Коли жертва атаки ініціює з'єднання, шахрай перехоплює його і потім завершує з'єднання з необхідним ресурсом, а потім пропускає всі з'єднання з цим ресурсом через свою станцію. При цьому, атакуючий може надсилати інформацію, змінювати її або підслуховувати всі переговори і потім розшифровувати їх [4]. Таким чином, безпровідна станція може перехоплювати трафік іншого безпровідного клієнта (або провідного клієнта в локальній мережі).

Відмова в обслуговуванні (Denial of Service – DOS). Повне паралізування мережі може викликати атака типу DOS. У всій мережі, включаючи базові станції і клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися один з одним. Ця атака вимикає всі комунікації в певному районі. Атаку DOS на без мережі важко запобігти або зупинити. Більшість бездротових мережевих технологій використовує неліцензовані частоти − отже, допустима інтерференція від цілого ряду електронних пристроїв.

Глушіння в мережах відбувається тоді, коли навмисна або ненавмисна інтерференція перевищує можливості відправника або одержувача в каналі зв'язку, таким чином, виводячи цей канал з ладу. Атакуючий може використовувати різні способи глушіння [4]. Глушіння клієнтської станції дає можливість шахраєві підставити себе на місце заглушеного клієнта, як показано на Рис. 2. Також глушіння можуть використовувати для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Більш витончені атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника.

Рис. 2. Атака глушіння клієнта для перехоплення з'єднання

Глушіння базової станції надає можливість підмінити її атакуючої станцією. Таке глушіння позбавляє користувачів доступу до послуг. Більшість безпровідних мережевих технологій використовує неліцензовані частоти. Тому багато пристроїв, такі як радіотелефони, системи спостереження і мікрохвильові печі, можуть впливати на роботу бездротових мереж і глушити бездротове з'єднання.

Всі безпровідні комунікаційні мережі схильні до атак прослуховування в період контакту. А управління ключем, як правило, викликає додаткові проблеми, коли застосовується при роумінгу і в разі загального користування відкритим середовищем.

Безпровідний доступ забезпечує повну анонімність атаки. Без відповідного обладнання в мережі, що дозволяє визначати місце розташування, атакуючий може легко зберігати анонімність і ховатися де завгодно на території дії бездротової мережі [2, 3].

Системи виявлення вторгнень (Intrusion Detection System, IDS) − це пристрої за допомогою яких можна виявляти та своєчасно запобігати вторгненням в обчислювальні мережі. Вони діляться на два види: на базі мережі та на базі хоста. Мережеві системи (Network Intrusion Detection Systems, NIDS) аналізують трафік з метою виявлення відомих атак на підставі наявних у них наборів правил (експертні системи). Виняток з точки зору принципів аналізу становлять системи на базі нейронних мереж та штучного інтелекту. Підмножиною мережевих систем виявлення вторгнень є системи для спостереження тільки за одним вузлом мережі (Network Node IDS) [3].

NIDS діляться в свою чергу на дві великі категорії: на основі сигнатур і на основі бази знань. Сигнатурні IDS найбільш поширені і простіше реалізуються, але їх легко обійти і вони не здатні розпізнавати нові атаки. У таких системах події, відбуваються в мережі, порівнюються з ознаками відомих атак, які й називаються сигнатурами. Крім того, бази даних, що містять сигнатури, необхідно надійно захищати і часто оновлювати. IDS на основі бази знань стежать за мережею, збирають статистику про її поведінку в нормальних умовах, виявляють різні відхилення і позначають їх як підозрілі. Тому такі IDS ще називають заснованими на поведінці чи статистичними [4]. Гарна IDS для безпровідної мережі повинна бути одночасно сигнатурною і статистичною. Деякі інструменти для проведення атак на безпровідні мережі мають чітко виражені сигнатури. Якщо вони виявляються в базі даних, то можна піднімати тривогу. З іншого боку, у багатьох атак очевидних сигнатур немає, але на нижніх рівнях стека протоколів вони викликають відхилення від нормальної роботи мережі. При розгортанні системи необхідно чітко розуміти, що, як і навіщо ми хочемо аналізувати, і намагатися відповісти на ці питання щоб сконструювати необхідну систему IDS [1, 3, 4].

Існує безліч технологій безпеки, і всі вони пропонують рішення для найважливіших компонентів політики у сфері захисту даних: аутентифікації, підтримки цілісності даних і

активної перевірки. Ми визначаємо аутентифікацію, як аутентифікацію користувача або кінцевого пристрою і його місця розташування з подальшою авторизацією користувачів та кінцевих пристроїв [2, 3].

Цілісність даних включає такі області, як безпека мережевої інфраструктури, безпеку периметра і конфіденційність даних. Активна перевірка допомагає впевнитися в тому, що встановлена політика в галузі безпеки витримується на практиці, і відстежити всі аномальні випадки і спроби несанкціонованого доступу.

Взагалі в захищеній інформаційній системі, політика безпеки – це документ в якому визначені: мета захисту, ризики системи, основні напрямки захисту інформаційних ресурсів, методи та засоби захисту інформації, властивості захищеності в термінах, що представляють систему захисту інформації з урахуванням встановленої відповідальності за зловмисне порушення визначених вимог. Опис політики безпеки може включати або враховувати властивості порушника, моделі загроз інформаційній системі та ризики пов'язані з їх реалізацією.

Найбільш часто, розглядаються політики безпеки, що пов'язані з поняттям «доступ». Доступ категорія суб'єктно-об'єктної моделі, що описує процес виконання операцій суб'єктів на об'єктами. Політика безпеки, повинна включати: безліч можливих операцій над об'єктами; для кожної пари «суб'єкт, об'єкт», безліч дозволених операцій, що є підмножиною всієї безлічі можливих операцій.

Політика безпеки в загальному випадку являє собою нестаціонарний стан захищеності, система, що захищає властивості інформаційних ресурсів, може змінюватися, доповнюватися новими компонентами, тобто бути динамічною. Політика безпеки – сукупність керівних принципів, правил процедур і практичних прийомів в області безпеки інформації, які регулюють управління, захист і розподіл цінної інформації. Вона встановлює модель захисту для існуючої або розроблюваної мережі. Політика безпеки пропонує набір правил і стандартів для користувачів, адміністраторів та менеджерів безпровідної мережі. Для забезпечення функцій захисту мережі політика безпеки передбачає наявність посади начальника служби безпеки. Для створення політики безпеки необхідне проведення оцінки ризиків у безпровідній мережі. Оцінка ризиків передбачає визначення загроз і вразливостей в системі, а також вона обов'язкова при боротьбі з вразливостями та непередбаченими загрозами, витратами і затратами.

Засіб для забезпечення конфіденційності в безпровідних мережах має бути визначено в політиці безпеки. Шифрування має забезпечити безпечний канал зв'язку, в якому будуть циркулювати закриті дані [2, 3].

Політика безпеки передбачає введення логічних файлів та облік діяльності користувачів. Ведення логічних файлів передбачається для забезпечення: контролю за користувачами; спрощення процесу налаштування мережі в разі виникнення несправностей; спрощення винесення відповідальності за порушення правил експлуатації мережі. Політика безпеки повинна передбачати використання брандмауерів для зменшення ризику злому бездротового клієнта. За допомогою брандмауерів слід проводити реєстрацію безпровідної діяльності. Політика безпеки повинна вимагати використання антивірусного програмного забезпечення та обов'язкового відновлення антивірусних баз [3, 4].

Крім того політикою безпеки передбачається: статична ARP адресація, що підсилює захист, збільшує адміністрування; перевірка MAC адреси; статистична IP адресація; визначення схеми безпровідного мережевого ідентифікатора (SSID).

Політика безпеки може заборонити широкомовну трансляцію SSID, з метою ускладнення ідентифікації точок доступу. Рекомендується включити в політику безпеки безпровідних мереж систему виявлення вторгнень (Intrusion Detection System – IDS). Безпровідна IDS необхідна для забезпечення захисту шляхом виявлення незаконної безпровідної діяльності (нападу). Для забезпечення безпеки безпровідної мережі політика безпеки повинна включати комплекс заходів як апаратних, так і програмних. Захисту конфіденційної інформації в безпровідних мережах варто надавати особливу увагу. Сьогодні

безпровідні мережі отримали величезне розповсюдження. Вони використовуються, як у офісах, так і в домашніх умовах. Ці мережі зручні в користуванні і дозволяють незалежно від місця знаходження бути он-лайн: обмінюватися даними, відправляти і приймати пошту, знаходити потрібну інформацію в Інтернеті [3, 4].

Головними напрямками захисту будь-яких мереж, у тому числі і безпровідних є суттєві з позиції безпеки властивості інформації: конфіденційність, цілісність та доступність, які в свою чергу і уособлюють значення безпеки, графічне зображення даного факту представлене на Рис. 3.

Рис. 3. Головні напрямки безпеки безпровідної мережі приватної мережі підприємства торгівлі

Безпека мережі представляється наступними вимогами: конфіденційність особистих та інших важливих даних; цілісність і точність інформації, що зберігається і програм, які її обробляють; доступність систем, даних і служб для тих, хто має право доступу. Найбільш дієвим захистом від DoS-атак є розробка і дотримання таких правил безпеки: встановлення та оновлення брандмауерів; постійне оновлення антивірусних програмних засобів; встановлення останніх «латок» (оновлень); використання довгих паролів; від'єднання мережевих пристроїв, які не використовуються.

Висновки. Захист даних у технологіях безпровідного зв'язку стандарту IEEE 802.16 дає змогу розв'язувати проблемні задачі функціональної та інформаційної безпеки даних у комунікаціях і цифрових системах на рівні забезпеченої структури «системи – радіосигнали – радіоканали – тракти» згідно з концепцією «об'єкт – загроза – захист». У сегменті програмного забезпечення системної моделі необхідно створювати алгоритмічно-програмне забезпечення процедури шифрування даних у WiMAX-мережі на основі стандарту AES мовою програмування C#, що забезпечує конфіденційність, достовірність, цілісність даних у контексті функціональної та інформаційної безпеки технологій безпровідного зв'язку.

Список використаних джерел

1. Сайко В.Г. Мережі бездротового широкосмугового доступу. Навчальний посібник / В.Г.Сайко, В.Я. Казіміренко, Ю.М. Літвінов. – К.: ДУТ, 2015. – 196 с.
2. Довгий С.О. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання. Монографія / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв. – 2-ге вид. – К.: «Азимут Україна», 2013. – 608 с.
3. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с. (останнє звернення 10.03.2023р.).
4. Захист інформації в операційних системах, базах даних і мережах. [Електронний ресурс]. – Режим доступу: www/ URL: https://ppt-online.org/482411(останнє звернення 10.03.2023р.).

Робота виконана під науковим керівництвом к.т.н., доцента
ЧУБАЄВСЬКОГО В.І.

ОСОБЛИВОСТІ ЗАХИСТУ WEB-РЕСУРСІВ НА ОСНОВІ OAUTH 2.0

ШУНДИК А. 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто механізм захисту веб-ресурсів на основі OAuth 2.0, який є одним з найбільш поширених механізмів авторизації в сучасних веб-додатках. Розглянуто особливості та застосування механізму OAuth 2.0 для забезпечення безпеки веб-додатків, а також описано загрози, з якими він допомагає боротися. В статті наведені рекомендації для безпечної реалізації механізму OAuth 2.0. Ця стаття може бути корисна для розробників веб-додатків та тестувальників безпеки, які мають намір забезпечити надійний захист своїх веб-ресурсів.

The article discusses the mechanism for protecting web resources based on OAuth 2.0, which is one of the most common authorization mechanisms in modern web applications. The features and applications of the OAuth 2.0 mechanism for securing web applications are reviewed, and the threats it helps to combat are described. The article provides recommendations for the secure implementation of the OAuth 2.0 mechanism. This article can be useful for web application developers and security testers who want to ensure that their web resources are securely protected.

Актуальність написання даної статті полягає у тому, що з розвитком технологій та зростанням кількості користувачів інтернету все більше ресурсів вимагають аутентифікації та авторизації для доступу до персональних даних користувачів. Протокол OAuth 2.0 є одним з найбільш популярних засобів для забезпечення безпеки в таких випадках, оскільки дозволяє надавати обмежений доступ до даних користувачів іншим ресурсам, не надавши їм повного контролю над цими даними.

Однак, незважаючи на популярність і ефективність протоколу OAuth 2.0, він також має певні вразливості та можливості для атак. Ця стаття має на меті описати ці вразливості та надати рекомендації щодо їх запобігання, забезпечивши тим самим підвищення рівня безпеки web-ресурсів та захист даних користувачів від можливих загроз.

Таким чином, данна стаття є актуальною для розробників та адміністраторів web-ресурсів, які використовують протокол OAuth 2.0 для захисту даних користувачів, а також для будь-яких осіб, які цікавляться питаннями безпеки в інтернеті.

Завдання написання наукової статті на тему "Особливості захисту web-ресурсів на основі OAuth 2.0" є дуже актуальним в сучасному світі, оскільки використання web-ресурсів зростає щодня, а з ним і ризики пов'язані з безпекою даних користувачів. Одним з основних методів захисту web-ресурсів є використання протоколу авторизації та ідентифікації OAuth 2.0.

Метою статті є розглянути особливості захисту web-ресурсів на основі протоколу OAuth 2.0 та надати розробникам та адміністраторам web-ресурсів рекомендації щодо забезпечення безпеки даних користувачів під час використання цього протоколу. Крім того, стаття має на меті описати можливі вразливості протоколу OAuth 2.0 та надати поради щодо їх запобігання.

Об'єктом написання даної статті є протокол OAuth 2.0 та його застосування для забезпечення безпеки web-ресурсів. Основною метою статті є розгляд особливостей захисту web-ресурсів на основі протоколу OAuth 2.0 та надання корисної інформації розробникам та адміністраторам web-ресурсів щодо забезпечення безпеки даних користувачів.У цій статті ми розглянемо основні принципи та можливості захисту web-ресурсів на основі OAuth 2.0, а також надамо поради щодо забезпечення безпеки під час використання цього протоколу.

Предметом дослідження - механізм захисту веб-ресурсів на основі OAuth 2.0 та його застосування для забезпечення безпеки веб-додатків.

Аналіз попередніх досліджень. Аналіз попередніх досліджень показав, що механізм OAuth 2.0 є одним з найпоширеніших стандартів авторизації інтернет-ресурсів. Він дозволяє користувачам давати доступ до своїх персональних даних веб-додаткам, забезпечуючи при цьому безпеку і захист приватності.

Проте, деякі попередні дослідження показали, що механізм OAuth 2.0 має свої слабкі сторони, зокрема, недостатню захищеність від атак типу CSRF та XSS. Для розв'язання цих проблем було запропоновано різні підходи, такі як використання state параметру, захист JWT токенів, та використання захищеного cookie.

Отже, враховуючи попередні дослідження, було проведено власне дослідження щодо захисту веб-ресурсів на основі OAuth 2.0, яке дозволило показати, що правильно налаштований механізм OAuth 2.0 може забезпечувати високий рівень безпеки веб-додатків., Л.А. Птіцина, Н.М. Тюріна, О.М. Іванова, С.В. Федоренко, А.А. Максимова та ін.

Виклад основного матеріалу. В сучасному світі інформаційні технології є одним з найбільш важливих аспектів розвитку суспільства. Інтернет є найбільшою базою даних, доступну для всіх користувачів з усього світу, тому захист від несанкціонованого доступу до цієї інформації є важливим завданням для розробників веб-ресурсів.

Одним з найефективніших методів захисту веб-ресурсів є протокол OAuth 2.0. Цей протокол дозволяє користувачам дозволяти доступ до своїх даних третім сторонам без необхідності передавати свої логіни та паролі. В даній статті будуть розглянуті основні принципи роботи протоколу OAuth 2.0, його переваги та недоліки, а також можливі шляхи покращення захисту веб-ресурсів на основі цього протоколу.

Основна частина

OAuth 2.0 - це протокол авторизації, який використовується для надання доступу до ресурсів через веб-інтерфейс. Протокол базується на технології токенів доступу, що дозволяє здійснювати безпечні запити до захищених веб-ресурсів без передачі логінів та паролів.

Принцип роботи протоколу полягає у тому, що користувач аутентифікується на сторонньому веб-ресурсі, після чого він надає дозвіл на доступ до своїх даних іншому веб-ресурсу. Це здійснюється за допомогою спеціальних запитів, які передаються між веб-ресурсами з використанням токенів доступу.

Основні принципи OAuth 2.0

OAuth 2.0 базується на таких основних принципах:

Розподіл ролей. В OAuth 2.0 існує два види ролей: "клієнт" і "постачальник ідентифікації". Клієнт - це додаток або сервіс, який хоче отримати доступ до захищених ресурсів, а постачальник ідентифікації - це система, яка перевіряє, що клієнт має право на доступ до ресурсів.

Розподілення даних доступу. OAuth 2.0 використовує токени доступу для забезпечення доступу до ресурсів. Клієнт отримує токен доступу від постачальника ідентифікації, який дозволяє йому отримати доступ до ресурсів. Токени доступу можуть бути тимчасовими або постійними.

Дозвіл на доступ. Клієнт не отримує безпосередньо доступ до ресурсів. Замість цього, він отримує дозвіл на доступ до ресурсів від постачальника ідентифікації. Це дозволяє постачальнику ідентифікації контролювати, які ресурси має доступ клієнт і як він використовує ці ресурси.

Безпека протоколу. Однією з найбільш важливих принципів OAuth 2.0 є забезпечення безпеки протоколу. Для цього використовуються такі механізми, як шифрування, підписи та перевірка на ідентифікацію.

Сценарії

Веб-серверні програми. Кінцева точка Google OAuth 2.0 підтримує програми веб-сервера, які використовують такі мови та фреймворки, як PHP, Java, Python, Ruby та ASP.NET (Рис 1).

Послідовність авторизації починається, коли ваша програма перенаправляє браузер на URL-адресу Google; URL-адреса містить параметри запиту, які вказують тип запитуваного

доступу. Google здійснює автентифікацію користувача, вибір сеансу та згоду користувача. Результатом є код авторизації, який програма може обміняти на маркер доступу та маркер оновлення.

Програма має зберігати маркер оновлення для подальшого використання та використовувати маркер доступу для доступу до Google API. Після закінчення терміну дії маркера доступу програма використовує маркер оновлення для отримання нового.

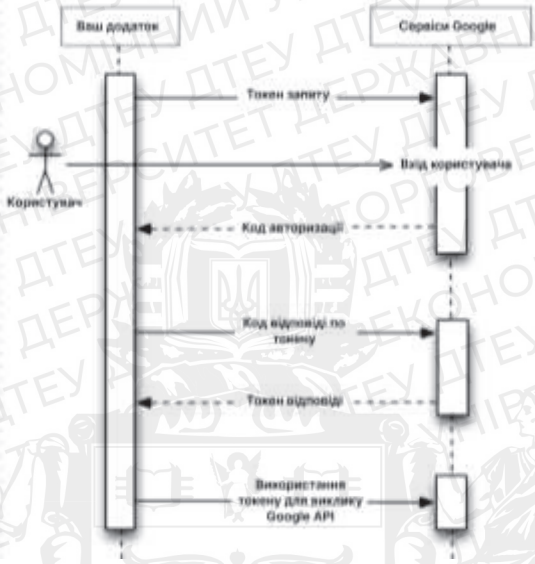


Рис. 1 Як працює Oauth2.0 з веб-серверними програмами

Клієнтські програми (JavaScript).

Кінцева точка Google OAuth 2.0 підтримує програми JavaScript, які запускаються у веб-переглядачі (Рис 2).

Послідовність авторизації починається, коли ваша програма перенаправляє браузер на URL-адресу Google; URL-адреса містить параметри запиту, які вказують тип запитуваного доступу. Google здійснює автентифікацію користувача, вибір сеансу та згоду користувача.

Результатом є маркер доступу, який клієнт повинен перевірити, перш ніж включити його в запит Google API. Коли термін дії маркера закінчується, програма повторює процес.

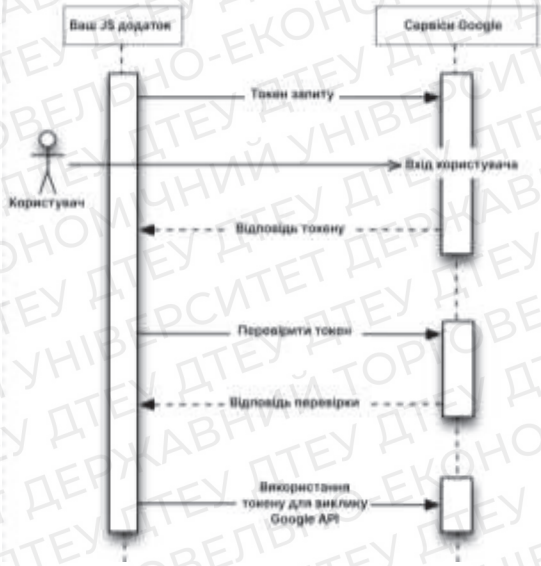


Рис. 2 Як працює Oauth2.0 з клієнтською програмою JavaScript

Програми на пристроях з обмеженим входом.

Кінцева точка Google OAuth 2.0 підтримує програми, які працюють на пристроях з обмеженим доступом, як-от ігрові консолі, відеокамери та принтери (Рис 3).

Послідовність авторизації починається з того, що програма надсилає запит веб-служби до URL-адреси Google для коду авторизації. Відповідь містить кілька параметрів, включаючи URL-адресу та код, які додаток показує користувачеві.

Користувач отримує URL-адресу та код із пристрою, а потім перемикається на окремий пристрій або комп'ютер із більшими можливостями введення. Користувач запускає браузер, переходить за вказаною URL-адресою, авторизується та вводить код.

Тим часом програма опитує URL-адресу Google через певний інтервал. Коли користувач схвалює доступ, відповідь від сервера Google містить маркер доступу та маркер оновлення. Програма має зберігати маркер оновлення для подальшого використання та використовувати маркер доступу для доступу до Google API. Після закінчення терміну дії маркера доступу програма використовує маркер оновлення для отримання нового.

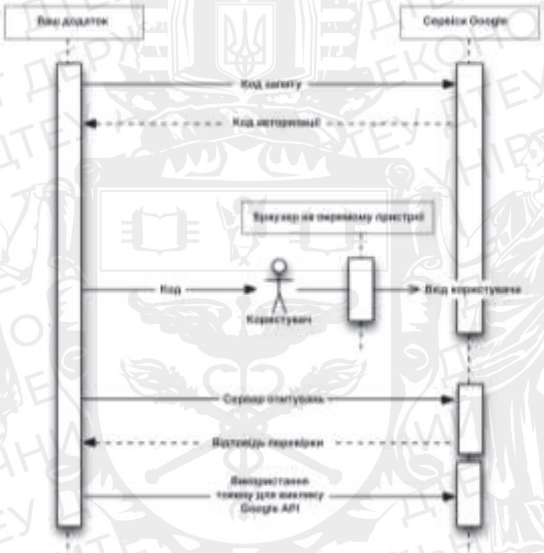


Рис. 3 Як працює Oauth2.0 з програмами на пристроях з обмеженим входом

Сервісні облікові записи.

Google API, наприклад Prediction API та Google Cloud Storage, можуть діяти від імені вашої програми без доступу до інформації користувача. У таких ситуаціях ваша програма повинна підтвердити свою власну ідентифікацію API, але згода користувача не потрібна. Подібним чином у корпоративних сценаріях ваша програма може запитувати делегований доступ до деяких ресурсів (Рис 4).

Для таких типів міжсерверної взаємодії вам потрібен обліковий запис служби , який є обліковим записом, який належить вашій програмі, а не окремому кінцевому користувачеві. Ваша програма викликає Google API від імені облікового запису служби, і згода користувача не потрібна. (У сценаріях, не пов'язаних із службовим обліковим записом, ваша програма викликає Google API від імені кінцевих користувачів, і іноді потрібна згода користувача.)

Облікові дані облікового запису служби, які ви отримуєте з Google API Console, включають згенеровану унікальну адресу електронної пошти, ідентифікатор клієнта та принаймні одну пару відкритих/приватних ключів. Ви використовуєте ідентифікатор клієнта та один закритий ключ, щоб створити підписаний JWT і створити запит маркера доступу у відповідному форматі. Потім ваша програма надсилає запит маркера на сервер авторизації Google OAuth 2.0, який повертає маркер доступу. Програма використовує маркер для доступу до Google API. Коли термін дії маркера закінчується, програма повторює процес.

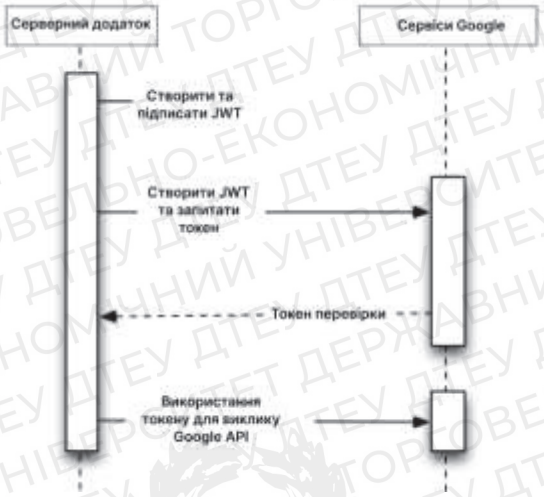


Рис. 3 Як працює Oauth2.0 з сервісними обліковими записами

Основними перевагами протоколу OAuth 2.0 є:

1. Зменшення ризику витоку паролів. Оскільки протокол використовує токени доступу, користувач не має потреби передавати свій логін та пароль сторонньому веб-ресурсу.
2. Можливість контролювання доступу до ресурсів. Протокол OAuth 2.0 дозволяє здійснювати детальний контроль над даними, до яких має доступ сторонній веб-ресурс. Користувач може обрати, які дозволи надаються тому чи іншому веб-ресурсу, а також змінювати їх в будь-який момент.
3. Спрощення розробки веб-додатків. За допомогою протоколу OAuth 2.0 розробники можуть значно спростити процес авторизації та реалізувати її за декілька кроків.

Однак, протокол OAuth 2.0 має і свої недоліки. Найбільш відомим з них є проблема безпеки, зокрема можливість атаки типу Man-in-the-middle (MITM), коли зловмисник перехоплює токен доступу та здійснює несанкціонований доступ до веб-ресурсу.

Одним із способів покращення захисту веб-ресурсів на основі протоколу OAuth 2.0 є використання двофакторної аутентифікації, яка забезпечує додатковий рівень захисту. Двофакторна аутентифікація полягає у використанні двох або більше методів для підтвердження особистості користувача, наприклад, введення пароля та використання коду, що надсилається на мобільний телефон.

Ще одним шляхом покращення захисту є використання захищеного з'єднання (SSL/TLS), яке забезпечує безпечний обмін даними між веб-ресурсами. Це зменшує ризик перехоплення токенів доступу та здійснення атак MITM.

Також можливим варіантом є використання додаткових заходів безпеки, таких як криптографічне підписання запитів та перевірка цілісності даних.

При розробці веб-додатків, які використовують протокол OAuth 2.0, необхідно дотримуватися кількох правил безпеки, щоб мінімізувати ризики несанкціонованого доступу до веб-ресурсу. Декілька рекомендацій, які можуть допомогти забезпечити безпеку веб-додатків на основі протоколу OAuth 2.0, наведені нижче.

1. Захист токенів доступу. Токени доступу мають велике значення для захисту веб-ресурсів на основі протоколу OAuth 2.0. Тому вони повинні бути зберігатися у безпечному місці та передаватися тільки по захищеному каналу. Для зменшення ризику несанкціонованого доступу до токенів доступу рекомендується використовувати їх з обмеженим терміном дії.
2. Перевірка джерела запитів. Веб-додатки на основі протоколу OAuth 2.0 повинні перевіряти джерело запиту перед тим, як надавати доступ до ресурсів. Це допомагає уникнути атак типу CSRF (Cross-Site Request Forgery), коли зловмисник намагається виконати дії в ім'я авторизованого користувача без його згоди.
3. Використання HTTPS для всіх запитів. Для забезпечення безпеки веб-додатки на основі протоколу OAuth 2.0 повинні використовувати захищене з'єднання HTTPS для всіх

запитів. Це забезпечує безпечний обмін даними між веб-ресурсами та зменшує ризик перехоплення даних або токенів доступу.

4. Моніторинг активності користувачів. Для зменшення ризиків несанкціонованого доступу до веб-ресурсів, на основі протоколу OAuth 2.0, необхідно вести моніторинг активності користувачів. Це допомагає вчасно виявляти та реагувати на підозрілу або незвичну активність.

5. Використання правильних типів авторизації. Для різних типів веб-додатків можуть використовуватися різні типи авторизації. Наприклад, для веб-додатків, які взаємодіють з API, можуть використовуватися токени доступу з обмеженими правами доступу. Для веб-додатків, які взаємодіють з користувачами, можуть використовуватися авторизаційні токени з вищим рівнем доступу.

6. Використання двофакторної аутентифікації. Для підвищення рівня безпеки веб-додатки на основі протоколу OAuth 2.0 можуть використовувати двофакторну аутентифікацію. Це допомагає зменшити ризик несанкціонованого доступу до веб-ресурсів навіть у тому випадку, якщо зловмиснику вдалося отримати доступ до користувачевого пароля.

7. Використання авторизації на основі ролей. Для керування рівнями доступу веб-додатки на основі протоколу OAuth 2.0 можуть використовувати авторизацію на основі ролей. Це дозволяє обмежити доступ до ресурсів в залежності від ролі користувача.

Усі ці рекомендації допоможуть забезпечити безпеку веб-додатків на основі протоколу OAuth 2.0 та запобігти можливим атакам. Однак, важливо пам'ятати, що безпека є постійним процесом, тому веб-додатки повинні постійно моніторитися та підтримуватися у відповідному стані.

Висновки. Отже, OAuth 2.0 є ефективним механізмом для захисту web-ресурсів, оскільки дозволяє забезпечити авторизацію користувачів і управління доступом до ресурсів за допомогою токенів доступу. Правильна реалізація механізму OAuth 2.0 може запобігти багатьом загрозам для безпеки веб-додатків, таким як атаки на міжсайтовий скриптінг, перехоплення сесії та інші. У даній статті було описано основні принципи роботи механізму OAuth 2.0, а також запропоновані практичні рекомендації щодо його безпечної реалізації. Оскільки механізм OAuth 2.0 поширено в сучасних веб-додатках, знання про його особливості та застосування в практиці може бути корисним для розробників веб-додатків.

Список використаних джерел

1. Офіційна документація OAuth 2.0 на сайті IETF (https://tools.ietf.org/html/rfc6749)
2. Стаття "OAuth 2.0 Security Best Current Practice" на сайті IETF (https://tools.ietf.org/html/draft-ietf-oauth-security-topics-16)
3. Стаття "OAuth 2.0 Threat Model and Security Considerations" на сайті IETF (https://datatracker.ietf.org/doc/html/rfc6819)
4. Офіційна документація на сайті OAuth.com (https://oauth.net/2/)
5. Стаття "OAuth" на сайті Ping Identity (https://www.pingidentity.com/en/resources/identity-fundamentals/authentication-authorization-standards/oauth.html)
6. Стаття "OpenID Connect & OAuth 2.0 API" на сайті Okta (https://developer.okta.com/docs/reference/api/oidc/)
7. Стаття "OAuth 2.0 Security Cheat Sheet" на сайті GitHub (https://github.com/koenbuyens/oauth-2.0-security-cheat-sheet)
8. Стаття "Using OAuth 2.0 to Access Google APIs" на сайті Developers.Google (https://developers.google.com/identity/protocols/oauth2)

Робота виконана під науковим керівництвом к.т.н., доцента
ВЛАСЕНКО Л.О.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КІБЕРАТАК В СИСТЕМІ СУДОУСТРОЮ

ЮНАК А., 2м курсу ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи захисту інформації від кібератак в системі судоустрою. Описано загрози, які можуть стати причиною кібератак на систему судоустрою та наслідки таких атак. Зазначено переваги застосування програмних забезпечень в судоустрою, надано опис та рекомендації щодо впровадження в практику роботи системи судоустрою. Розглянуто важливі аспекти підготовки та навчання персоналу щодо кібербезпеки та захисту інформації в системі судоустрою.

The article discusses methods for protecting information from cyber attacks in the judicial system. It describes the threats that could cause cyber attacks on the judicial system and the consequences of such attacks. The advantages of using software in the judicial system are noted, and detailed descriptions and recommendations for implementing them into the practical work of the judicial system are provided. Important aspects of preparing and training personnel in cybersecurity and information protection in the judicial system are also discussed.

Актуальність. Актуальність методів захисту інформації від кібератак в системі судоустрою надзвичайно висока в сучасних умовах. Кібератаки на системи судоустрою можуть стати причиною порушення правосуддя, втрати конфіденційної інформації, порушення прав людини та інших серйозних наслідків. У зв'язку зі зростанням кількості та складності кібератак, системи судоустрою повинні бути постійно готові до захисту від таких атак. Застосування ефективних методів захисту є надзвичайно важливим для забезпечення безпеки та надійності роботи систем судоустрою.

Крім того, залежно від країни та її політичного контексту, системи судоустрою можуть бути особливо цільовими об'єктами кібератак з боку керівництва, політичних опозиційних сил, злочинців та інших груп. Таким чином, захист інформації в системі судоустрою є дуже важливою та актуальною проблемою, яку потрібно вирішувати негайно.

Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують в прискореному темпі, кіберзлочини стають досконалішими, краще організованими і транснаціональними. Це зумовлено тим, що інтернет, цифрові послуги, інформаційно-комунікаційні технології стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайн-банкінгу до систем інтернету речей та інтелектуальних систем управління підприємствами та судоустрою.

Система кібербезпеки має працювати в інтересах громадськості як для постачальників послуг, так і для користувачів послуг.

Саме держава, як гарант прав і свобод громадян, має взяти на себе відповідальність за забезпечення доступу до стабільного безпечного цифрового простору, яким можуть скористатися всі громадяни, адже забезпечення належного рівня кібербезпеки є необхідною умовою розвитку інформаційного суспільства.

Тому, захист інформації від кібератак є однією з головних проблем в сфері інформаційної безпеки судової системи.

Метою статті є комплексний аналіз методів захисту інформації від кібератак в системі судоустрою.

Об'єктом дослідження є застосування різних методів і технологій для захисту інформації в системі судоустрою від кібератак.

Предмет дослідження - методи захисту інформації в системі судоустрою від кібератак.

Аналіз останніх досліджень. Дослідженню кібербезпеки основних характерних рис присвячені праці вітчизняних науковців: Арістова І.В., Березовської І.Р., Дзьобаня О.П., Калюжного Р.А., Кормича Б.А., Ліпкана В.А., Марущак А.І., Цимбалюка В.С., Юдіна О.К. та інших.

Виклад основного матеріалу. Існує безліч різних кібератак, які можуть бути спрямовані на систему судоустрою, такі як:

- Фішинг: атаки, які спрямовані на отримання конфіденційних даних, таких як імена користувачів та паролі, шляхом відправлення підробленої електронної пошти, яка маскується під довірену організацію.
- Сервіс-атаки (DDoS): це атаки, які призводять до перевантаження серверів або інфраструктури, що призводить до відмови в обслуговуванні, зупинки роботи системи та зниження продуктивності.
- Віруси та шкідливі програми: ці атаки спрямовані на викрадення конфіденційної інформації або руйнування системи, заражаючи її вірусами та шкідливими програмами.
- SQL-ін'єкції: це атаки, які використовують недоліки безпеки в базі даних для викрадення конфіденційної інформації або руйнування системи.
- Соціальний інжиніринг: це атаки, які спрямовані на злам системи, використовуючи маніпулювання психологією користувачів з метою отримання конфіденційної інформації або доступу до системи. Наприклад, зловмисник може надіслати електронного листа, що маскується під іншого користувача, та запросити інформацію про систему чи надати шлях для доступу.
- Розповсюдження дезінформації: це кібератака яка використовує цифрове середовище для поширення неправдивої інформації. Ці атаки можуть бути здійснені через соціальні мережі, веб-сайти, електронну пошту та інші канали комунікації.
- Ретельне перехоплення пакетів (TCP/IP Hijacking) - атака, яка полягає в перехопленні передачі даних між комп'ютерами із застосуванням програмного забезпечення.

Із за цього наслідки кібератак на систему судоустрою можуть бути дуже серйозними та мають далекосяжні наслідки для її користувачів, такі як:

- Втрата конфіденційної інформації: кібератаки можуть призвести до втрати конфіденційної інформації, такої як імена, адреси, електронні адреси та інші особисті дані. Це може стати на шляху вивчення судової справи та викликати серйозні наслідки для приватності та безпеки користувачів.
- Порушення цілісності даних: кібератаки можуть також призвести до порушення цілісності даних, що може призвести до внесення змін в судову справу або видалення важливих даних.
- Порушення доступності: атаки на доступність можуть призвести до зупинки роботи системи, що може призвести до затримок у вирішенні судових справ, збільшення термінів та зниження продуктивності.
- Підрив довіри до системи: кібератаки можуть підірвати довіру до системи, яка є ключовим елементом судової системи. Це може викликати серйозні наслідки для довіри до судової системи та вплинути на результати судових рішень.
- Фінансові наслідки: кібератаки можуть призвести до значних фінансових наслідків, таких як витрати на відновлення системи, компенсації постраждалим та збитки, пов'язані з втратою продуктивності та затримками у судових рішеннях.

Тому захист інформації є одним з ключових аспектів судової системи, якій приділяється велика увага. Кіберзлочинці можуть використовувати різні методи, щоб отримати доступ до конфіденційної інформації, яка зберігається в системі судоустрою. Далі у статті будуть приведені методи захисту інформації від кібератак в системі судоустрою [1].

Криптографічний захист один з методів захисту інформації, який використовує складні математичні алгоритми, щоб зашифрувати дані перед їх відправкою, тим самим роблячи їх

нерозбірливими для кіберзлочинців. Може включати в себе заходи, як шифрування даних, цифрові підписи, та аутентифікації, методи захисту інформації, які допомагають забезпечити конфіденційність і збереження даних у неушкодженому вихідному стані.

Простіше кажучи, є різні типи повідомлень, включаючи електронну пошту, файли, бази даних та багато інших видів інформації. Більш просунуті та ефективні методи криптографічного захисту досягаються через використання багатьох складних алгоритмів та схем шифрування, які регулярно оновлюються та модифікуються, щоб запобігти несанкціонованому доступу та забезпечити захист даних.

Для прикладу, одним з найпоширеніших криптографічних алгоритмів є алгоритм RSA, який базується на складності факторизації великих чисел. Цей алгоритм використовується для шифрування та розшифрування інформації за допомогою публічного та приватного ключів.

Інший криптографічний алгоритм, який використовується для захисту інформації від кібератак, - це алгоритм AES (Advanced Encryption Standard). Він використовується для шифрування та розшифрування інформації з використанням секретного ключа. Алгоритм AES є стандартом у багатьох сучасних криптографічних протоколах, включаючи SSL / TLS для захисту трафіку в Інтернеті [1, 3].

Судоустрої дуже ефективно використовують електрону пошту в документообігу, для цього вони використовують ключи, так кажучи для підтвердження особи або аутентифікації.

Є кілька методів які активно використовуються в судоустрої, це аутентифікація за сертифікатами, зараз кожний може отримати сертифікати, вони використовуються разом с ключами які людина може отримати навіть через такі додаткі як ПриватБанк або ОщадБанк. Сертифікат являє собою набір атрибутів, що ідентифікують власника, підписаний certificate authority (CA). CA виступає в ролі посередника, який гарантує справжність сертифікатів. Також сертифікат криптографічно пов'язаний з закритим ключем, який зберігається у власника сертифіката і дозволяє однозначно підтвердити факт володіння сертифікатом. Сертифікат може зберігатися в операціонній системі, в браузері або на окремому фізичному пристрої, такому як смарт картка або токен USB. А закритий ключ захищається, зазвичай, ще паролем. Цей спосіб є більш надійним ніж аутентифікації за паролем, але в зв'язку з важкістю розповсюдження сертифікатів, цей метод аутентифікації є менш популярним.

Аутентифікація за ключами доступу – використовується для застосунків та сервісів при їх звернені до Web-сервісів. Для аутентифікаціїї в даному методі використовюються ключі доступу, наприклад access key, API key. Ключі доступу – це довгі унікальні строки, що являють собою рандомний набір символів. Зазвичай користувачі, які хочуть отримати доступ до Web-сервісу роблять запит на створення ключа доступу і в подальшому зберігають його у клієнтському застосунку.

Цей ключ може давати не повний доступ до ресурсу після аутентифікації, це може бути задано при створенні ключа доступу. Так як ключ доступу є випадково підібраними символами, його складніше буде підібрати, на відміну від звичайного пароля. У випадку компрометації ключа, його можна анулювати і створити новий. На (Рис.1) зображено ~~самий~~ просте розуміння як проходить аутентифікація сертифіката, для чого використовується криптографічна бібліотека.

Аутентифікація за токенами – використовується зазвичай для розподілених систем Single Sign-On (SSO), де аутентифікація відбувається за рахунок іншого сервісу, наприклад здійснення аутентифікації через обліковий запис соціальних мереж. Соціальні мережі виступають в ролі сервіса аутентифікації. Токен – це структура даних, що складається з інформації: строк дії токена, відправник, можливий отримувач токену та деяка інформація про користувача, що здійснив запит на створення токену. Токен для збереження цілісності даних і захисту від несанкціонованого змінення даних додатково підписується. Одними з найрозповсюджених форматів токенів є: Simple Web Token (SWT), JSON Web Token (JWT), Security Assertion Markup Language (SAML). Для даного методу аутентифікації використовуються стандарти, що описують протокол взаємодії між клієнтами та IP і SP застосунками, також, як і формат токенів, що надсилаються. До таких стандартів належать:

стандарт SAML, стандарт WS-Trust, стандарт WS-Federation, стандарт OAuth, стандарт OpenID Connect.

Рис. 1. Схема аутентифікації сертифіката

Система судоустрою повинна бути здатна сповістити про можливі кібератаки. Наприклад, системи виявлення вторгнень можуть слідкувати за активністю в мережі, щоб мати змогу вчасно заблокувати можливість вторгнення [2].

Попередження кібератак одна з головних систем заходів, яка використовується для захисту комп'ютерної системи від потенційних кіберзагроз та атак. Безпека даних є важливою проблемою, яка потребує не тільки профілактичних заходів, таких як резервне копіювання даних, використання паролів та інших методів автентифікації, але також можливості реагування на кібератаки, які можуть відбуватися будь-якої миті. Отже система кібератак має методи виявлення спроб несанкціонованого доступу чи злому комп'ютерних систем. Вона може включати використання різних методів для моніторингу мережного трафіку і виявлення незвичайних або підозрілих дій, для цього використовують одні із популярних систем моніторингу як Zabbix або Grafana (Рис. 2, Рис. 3.).

Рис. 2. Інтерфейс "Zabbix"

Крім цього, якщо людина не розуміється в кібербезпеці для цього є заходи щодо виявлення та запобігання кібератакам, такі як використання програмного забезпечення для блокування потенційно шкідливих сайтів та більшу увагу до безпеки паролів у рамках судоустрою. Реагування на попередження кібератак може включати заходи щодо блокування вразливих вузлів мережі, перезавантаження обладнання або зміни налаштувань, оповіщення відповідних осіб про можливі загрози та багато інших дій.

Рис. 3. Інтерфейс "Grafana"

Системи моніторингу та попередження кібератак повинні забезпечувати надійний захист комп'ютерних систем від потенційних загроз та діяти у тісній співпраці з іншими системами безпеки. Вони повинні постійно оновлюватися та адаптуватися до нових видів атак, тому використання інноваційних методів та технологій − ключовий фактор у забезпеченні ефективного захисту від кібератак.

Також одним з актуальних методів виступає не тільки моніторинг ну і сам захист мережі судоустрою. Адміністратори мережі повинні використовувати захисні технології, такі як брандмауери, антивірусні програми, що допоможуть захистити мережу від кібератак.

Захист мережі являє собою процес створення та застосування заходів, які потрібні для забезпечення безпеки мережі, зокрема її хостів, даних, пристроїв і систем, пов'язаних з нею.

Захист мережі включає заходи, такі як:

- Використання безпечних паролів та методів аутентифікації, а також шифрування даних.
- Регулярне оновлення програмного забезпечення, операційних систем, маршрутизаторів та іншого обладнання.
- Встановлення та налаштування персональних та "брандмауерів".
- Шифрування даних та використання резервного копіювання для захисту даних у разі порушення безпеки.
- Використання VPN (віртуальної приватної мережі) для безпечного підключення до мережі з віддалених місць.
- Використання системи обмеження прав доступу до файлів та каталогів для забезпечення безпеки даних.
- Проведення тестування мережі на вразливість та аудиту безпеки з метою виявлення слабких місць та вдосконалення системи захисту.

Є ще один захід захисту як Wifi, але по політиці безпеки судоустрою та і взагалі із за великої ймовірності перехвату або самого взлому мережі що дасть кіберзлочинцю доступ до конфіденційної інформації, вже мало де використовується.

Отже для ефективного захисту мережі, крім вищеописаних заходів, необхідно мати систему виявлення і реагування на загрози. Це включає моніторинг мережевого трафіку на наявність аномальної активності, пошук несанкціонованих пристроїв на мережі, а також виявлення спроб злому системи захисту Важливим аспектом захисту мережі є також навчання персоналу. Всі користувачі, які мають доступ до мережі, повинні бути навчені безпеці та заходам запобігання загрозам. Вони повинні розуміти, як захистити як власні дані, так і дані, пов'язані з мережею [3]. Зрештою, захист мережі − постійний процес, що вимагає повної комбінації заходів для виявлення, запобігання та реагування на загрози.

Резервне копіювання інформації. Інформація більше за все зберігається на серверах, із за цього з'являється проблема в тому що, сервер може вийти із строю або якщо пройшла кібератака, тоді для безпеки інформації система судоустрою повинна регулярно створювати резервні копії інформації, щоб при випадку таких ситуацій була можливість відновити дані.

Існує безліч способів створення резервних копій, включаючи такі методи:

- Програмне забезпечення для резервного копіювання даних.
- Ручне копіювання даних на зовнішні жорсткі диски, USB або інші портативні пристрої для зберігання даних.
- Резервне копіювання даних у хмарних сервісах.

Крім того, важливо вибрати правильне сховище для копіювання резервних копій даних. Резервні копії можуть зберігатися на зовнішніх жорстких дисках, серверах у хмарному сховищі або інших пристроях. При виборі сховища для резервних копій слід враховувати такі фактори: місткість пристрою; тип інтерфейсу; швидкість передачі даних; ціна; надійність та безпека.

Також необхідно регулярно перевіряти резервні копії даних на наявність дефектів або помилок та стежити за їх актуальністю. важливо регулярно створювати копії даних для того, щоб мати доступ до останньої версії даних, якщо потрібно відновити інформацію.

Усі користувачі системи судоустрою повинні бути навчені засадам та правилам безпеки інформації та кібербезпеки, щоб зменшити частоту випадків людської помилки, що спричиняють кібератаки, втрати інформації або зараження вірусом саму мережу судоустрою. Навчання персоналу кібербезпеки в судоустрої є дуже важливим питанням, оскільки судові системи містять велику кількість конфіденційної інформації, яка може стати об'єктом кібератак з боку зловмисників.

Таблиця порівняння кіберзахисту (Таблиця 1) різних судових систем може бути корисною для оцінки рівня кібербезпеки:

Таблиця 1.

Порівняння типи захисту систем судоустрою.

Тип захисту	**Система А**	**Система В**	**Система С**
Рівень шифрування даних.	AES-256	AES-128	3DES
Застосування багатофакторної аутентифікації.	Так	Ні	Так
Система моніторингу та виявлення вторгнень.	Так	Так	Ні
Автоматичне оновлення програмного забезпечення.	Так	Так	Ні
Система контролю доступу до даних.	RBAC	ABAC	DAC
Наявність системи резервного копіювання.	Так	Ні	Так
Рівень відповідальності за кібербезпеку.	Кожен користувач	Ввіділ ІТ	Кожен користувач та ввіділ ІТ.

Зазначені показники можуть варіюватися в залежності від конкретної судової системи, її розміру та обсягу діяльності. Важливо зрозуміти, що жодна система кібербезпеки не є абсолютною, і завжди є ризики та потенційні вразливості. Тому необхідно постійно оновлювати заходи з кібербезпеки та забезпечувати належний рівень свідомості серед користувачів щодо правил безпеки в інформаційних системах [2, 4].

Основними аспектами навчання персоналу кібербезпеки в судоустрої можуть бути:

- Освіта і свідомість: персонал повинен розуміти, що кібербезпека є ключовою складовою судової системи і має бути усвідомлено, як відповідальність кожного працівника.
- Створення і розробка політики кібербезпеки: судова система повинна мати детальну політику кібербезпеки, яка включає в себе заходи з протидії кібератакам та забезпечення безпеки в мережі.
- Система обміну інформацією: судова система повинна мати систему обміну інформацією між співробітниками, яка буде забезпечувати безпеку в мережі.
- Захист інформації: судова система повинна мати захист інформації з допомогою шифрування, паролів, біометричних методів ідентифікації тощо.
- Перевірка безпеки: судова система повинна проводити перевірки безпеки системи, щоб виявити потенційні проблеми та ризики та вживати заходів з їх усунення.
- Курси підвищення кваліфікації: персонал повинен бути навчений останнім методам та технологіям кібербезпеки та проходити курси підвищення кваліфікації з регулярністю.

Захист інформації від кібератак є дуже важливою задачею для будь-якої системи, в тому числі й системи судоустрою. У зв'язку з тим, що система містить значну кількість конфіденційної інформації, включаючи особисті дані громадян, захист цієї інформації є критично важливим [4].

Методи захисту від кібератак в системі судоустрою можуть бути різними, включаючи аутентифікацію користувачів, шифрування даних, захист мережі, оновлення програмного та апаратного забезпечення, аналіз поведінки та виявлення загроз, а також підвищення кібербезпеки користувачів. Крім того, важливим аспектом є стратегії відповідного реагування на кібератаки, такі як планування відповіді на кібератаки, резервне копіювання даних та відновлення системи, вивчення кібератак та забезпечення належного навчання співробітників щодо кібербезпеки. Застосування методів захисту від кібератак у системі судоустрою є дуже важливим для забезпечення кібербезпеки та захисту конфіденційної інформації. Тому, системи судоустрою повинні регулярно вдосконалювати свої методи захисту та забезпечувати навчання своїх співробітників щодо кібербезпеки.

Висновки. Кібератаки можуть спричинити серйозні наслідки, які відображаються в порушенні конфіденційності, цілісності та доступності інформації, тому, захист інформації від кібератак є однією з головних проблем в сфері інформаційної безпеки судової системи. Застосування методів захисту від кібератак у системі судоустрою є дуже важливим для забезпечення кібербезпеки та захисту конфіденційної інформації. Тому, системи судоустрою повинні регулярно вдосконалювати свої методи захисту та забезпечувати навчання своїх співробітників щодо кібербезпеки.

Список використаних джерел

1. Б. Толубка Інформаційна та кібербезпека: соціотехнічний аспект / Б. Толубка // Кіберпростір, кібербезпека та кібертероризм: зб. наук. праць “ДУТ” – 2015р., с. 7 – 63.
2. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019., с.164.
3. How to Protect Your Data from Unauthorized Access, Retrieved from \\ Режим доступу: https://cypressdatadefense.com/blog/unauthorized-data-access. (останнє звернення 07.04.2023р.)
4. Матеріали Української софтверної IT компанія "TQM systems" \\ Режим доступу: https://tqm.com.ua/ua/company/about (останнє звернення 07.04.2023р.)

Робота виконана під науковим керівництвом к.п.н. доцента
ЧУБАЄВСЬКОГО В.І.

ПОРІВНЯННЯ НАТИВНОГО ТА ВЕБ-ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБМІНУ ЗАХИЩЕНИМИ ДАНИМИ

ЮРЧЕНКО В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У цій статті детально розглянуто порівняння між нативним та веб-програмним забезпеченням для обміну захищеними даними. Розглянуто переваги та недоліки кожного типу програмного забезпечення, різницю між ними, зокрема щодо швидкості та продуктивності, доступності та зручності використання, вартості та складності розробки та підтримки. У статті також розглянуто поняття безпеки даних, захисту персональних даних та технології шифрування даних.

This article provides a detailed comparison between native and web-based software for exchanging secure data. It examines the advantages and disadvantages of each type of software, the differences between them, including speed and productivity, accessibility and usability, cost and complexity of development and maintenance. The article also discusses data security concepts, personal data protection, and data encryption technologies.

Актуальність. Ця стаття є актуальною в контексті епохи цифрових технологій та інформаційного суспільства, оскільки безпека обміну захищеними даними є важливою проблемою для мільйонів користувачів Інтернету. Вибір оптимального програмного забезпечення є ключовим аспектом для забезпечення безпеки та захищеності цих даних. Розуміння переваг та недоліків різних типів програмного забезпечення, а також технологій шифрування, може допомогти забезпечити захист від зловмисників, які можуть намагатися зламати доступ до цієї інформації. Дана стаття допоможе користувачам розібратися з перевагами та недоліками різних типів програмного забезпечення для обміну захищеними даними.

Метою статті є порівняння нативного та веб-програмного забезпечення для обміну захищеними даними, з метою визначення переваг та недоліків кожного з них, а також надання рекомендацій щодо вибору відповідного програмного забезпечення за тими чи іншими потребами користувача.

Об'єктом дослідження є програмне забезпечення для обміну захищеними даними.

Завдання статті полягає в наступному:

–аналіз технічних характеристик та функціональних можливостей нативного та веб-програмного забезпечення для обміну захищеними даними;

–порівняння переваг та недоліків кожного типу програмного забезпечення для обміну захищеними даними;

–оцінка рівня безпеки нативного та веб-програмного забезпечення для обміну захищеними даними;

–рекомендації щодо вибору відповідного програмного забезпечення за тими чи іншими потребами користувача.

У сучасному світі, захист персональних даних стає все більш актуальним питанням, обмін даними зберігається як один з ключових елементів бізнес-процесів. Наявні різні способи забезпечення безпеки обміну даними, одним з яких є використання нативного та веб-програмного забезпечення, котрі можуть бути використані для забезпечення цього процесу, проте кожен з них має свої переваги та недоліки.

Нативне програмне забезпечення, як правило, розробляється для конкретної платформи та встановлюється безпосередньо на комп'ютер користувача та працює з локальними даними, має прямий доступ до ресурсів операційної системи. Це дає користувачу повний контроль над

даними та забезпечує високий рівень безпеки. Проте, встановлення та підтримка нативного програмного забезпечення потребує доволі багато часу та може бути дорогим. Прикладами нативного програмного забезпечення для обміну захищеними даними є PGP (Pretty Good Privacy) і GnuPG (GNU Privacy Guard) [1].

Веб-програмне забезпечення працює через веб-браузер та може бути використане на будь-якому пристрої з доступом до Інтернету. Це забезпечує зручність використання та швидкий доступ до даних. Однак, воно може бути менш безпечним порівняно з нативним програмним забезпеченням, оскільки відкрите з'єднання з Інтернетом може бути легше скомпрометовано. Прикладами веб-програмного забезпечення для обміну захищеними даними є ProtonMail, Tutanota та Mega.

Одним з найбільш важливих аспектів обміну захищеними даними є захист від несанкціонованого доступу. Обидва види програмного забезпечення можуть забезпечити цей захист, проте вони роблять це по-різному. Нативне програмне забезпечення може використовувати механізми шифрування та аутентифікації для захисту даних, таких як AES (Advanced Encryption Standard) та RSA (Rivest-Shamir-Adleman). Ці механізми забезпечують конфіденційність даних надаючи тільки верифікованим користувач доступ до даних. Веб-програмне забезпечення може використовувати протоколи шифрування та сертифікації безпеки, такі як SSL (Secure Sockets Layer) або TLS (Transport Layer Security) [2]. Ці протоколи застосовуються для захисту даних, які передаються через Інтернет, від прослуховування та зміни під час передачі. Це забезпечує конфіденційність даних, що передаються між веб-браузером та веб-сайтом, та їх відповідність, забезпечуючи, що веб-сайт, з яким взаємодіє користувач, є дійсно тим, за яким він видає себе. Оскільки веб-програмне забезпечення працює через мережу Інтернет, воно може бути доступним з будь-якого пристрою з підключенням до Інтернету, що робить його відмінним від нативного програмного забезпечення.

Нативне програмне забезпечення - це програмне забезпечення, що встановлюється безпосередньо на операційну систему і виконується на комп'ютері або мобільному пристрої. До переваг нативного програмного забезпечення відносяться швидкість виконання, можливість доступу до апаратних ресурсів та можливість використання системних бібліотек.

Веб-програмне забезпечення - це програмне забезпечення, яке запускається у веб-браузері та взаємодіє з сервером через Інтернет. До переваг веб-програмного забезпечення відносяться можливість використання на будь-якому пристрої, що має доступ до Інтернету, відсутність необхідності встановлення на кожному пристрої та можливість оновлення програмного забезпечення на сервері, що дає можливість швидко внести зміни до протоколів без необхідності оновлення на кожному пристрої.

Однак, веб-програмне забезпечення може мати проблеми зі швидкістю виконання та надійністю, так як воно залежить від швидкості та надійності Інтернет-з'єднання. Також, веб-програмне забезпечення може бути більш вразливим до атак, так як воно працює через відкрите Інтернет-з'єднання.

При порівнянні нативного та веб-програмного забезпечення для обміну захищеними даними, слід враховувати різні фактори, такі як швидкість виконання, доступність, надійність та безпека.

Щодо швидкості виконання, нативне програмне забезпечення має перевагу, так як воно працює безпосередньо на пристрої. Однак, веб-програмне забезпечення може бути більш доступним, оскільки воно працює на будь-якому пристрої з доступом до Інтернету.

Щодо надійності та безпеки, обидва типи програмного забезпечення мають свої переваги та недоліки. Нативне програмне забезпечення може бути менш вразливим до атак та забезпечувати більшу контрольованість над даними, однак, наявність програмного забезпечення на кожному пристрої може бути проблемою. Веб-програмне забезпечення може бути більш вразливим до атак, але воно забезпечує більшу безпеку відносно доступності та можливості оновлення протоколів на сервері.

При використанні веб-програмного забезпечення для обміну захищеними даними слід враховувати ризики, пов'язані з безпекою Інтернет-з'єднання та вразливостями веб-додатків.

Необхідно використовувати шифрування даних та ідентифікацію користувача для забезпечення безпеки даних.

Однак, використання нативного програмного забезпечення для обміну захищеними даними також має свої ризики. Наприклад, віруси та шкідливі програми можуть надходити через зовнішні пристрої, такі як флеш-накопичувачі або зовнішні жорсткі диски.

Отже, при виборі між нативним та веб-програмним забезпеченням для обміну захищеними даними слід враховувати різні фактори та ризики. В залежності від конкретних потреб та вимог, один тип програмного забезпечення може бути більш підходящим за іншого.

Нативне програмне забезпечення може бути більш вразливим для кібератак, оскільки воно може бути встановлене на кількох пристроях, які поєднані в локальну мережу, можуть бути менш безпечними. Натомість, веб-програмне забезпечення запущене на сервері та підтримується командою розробників, що може знизити ризик порушення безпеки. Однак, якщо веб-програмне забезпечення не належним чином налаштоване та забезпечене, воно також може бути вразливим для кібератак.

Незалежно від того, яке програмне забезпечення буде використане, необхідно забезпечити дотримання відповідних стандартів безпеки та захисту даних, таких як GDPR (Загальний регламент про захист даних), HIPAA (Закон про портативні електронні засоби зберігання медичної інформації) та інші [3].

Також важливо враховувати, що розвиток технологій та зміни в правовому середовищі можуть вплинути на вибір програмного забезпечення для обміну захищеними даними в майбутньому. Тому рекомендується регулярно оцінювати потреби та забезпечення безпеки при використанні програмного забезпечення для обміну захищеними даними та адаптувати підходи до вибору відповідно до змін у відповідних вимогах та контексті використання.

Нативне програмне забезпечення може бути більш безпечним, оскільки воно може бути написане мовами програмування з високим рівнем контролю та має прямий доступ до апаратного забезпечення. Крім того, воно може бути відключене від Інтернету, що додає ще більше рівня безпеки.

З іншого боку, веб-програмне забезпечення може мати перевагу в безпеці, оскільки веб-сайти та програми можуть оновлюватись в режимі реального часу, що дозволяє швидко виправляти помилки та додавати нові функції з точки зору безпеки. Крім того, веб-програмне забезпечення може мати вбудовані заходи безпеки, такі як механізми перевірки валідності введених даних та відстеження випадків зламу.

Важливим фактором є підтримка та обслуговування програмного забезпечення. Нативне програмне забезпечення може вимагати більшої кількості технічної підтримки та обслуговування, оскільки воно повинне бути встановлене та підтримуватися на кожному пристрої, на якому воно використовується. У випадку веб-програмного забезпечення, підтримка та обслуговування можуть бути більш централізованими, оскільки воно запущене на серверах та може бути підтримуване централізованою командою розробників.

Окрім цього, важливо враховувати вартість програмного забезпечення та витрати на його встановлення та підтримку. Нативне програмне забезпечення може вимагати значних витрат на його розробку та встановлення на кожному пристрої, на якому воно використовується. У випадку веб-програмного забезпечення, витрати можуть бути меншими, оскільки його можна запустити на серверах та користуватися ним з будь-якого пристрою з доступом до Інтернету [4].

Для обміну захищеними даними важливо також враховувати додаткові функції, такі як шифрування та аутентифікація користувачів. Нативне програмне забезпечення може бути складніше для реалізації цих функцій, оскільки вони повинні бути реалізовані на кожному пристрої окремо. У випадку веб-програмного забезпечення, ці функції можуть бути більш централізовані та легше реалізовані.

Для того, щоб зробити найбільш обґрунтований вибір програмного забезпечення, необхідно враховувати технічні характеристики, такі як швидкість та продуктивність, а також інші аспекти, наприклад, доступність на різних платформах та мобільних пристроях,

можливості розширення та модифікації функцій та інтеграцію з іншими програмними продуктами. Нативне програмне забезпечення може бути більш продуктивним за рахунок того, що воно взаємодіє з операційною системою безпосередньо, але менш масштабованим, тоді як веб-програмне забезпечення може бути більш масштабованим, але менш продуктивним. Крім того, веб-програмне забезпечення може бути розроблене для будь-якої платформи та може бути доступним через браузер, що робить його більш гнучким у використанні та забезпечує більшу доступність.

Слід враховувати, що розробка та підтримка нативного програмного забезпечення може бути дорожчою, оскільки вона вимагає спеціальних знань та досвіду у розробці програмного забезпечення для конкретної платформи. У той же час, розробка веб-програмного забезпечення може бути менш витратною, оскільки вона може бути розроблена з використанням відкритих стандартів та бібліотек. Витрати на підтримку програмного забезпечення можуть бути значними в майбутньому. При розробці нативного програмного забезпечення, оновлення та підтримка можуть вимагати багато ресурсів, оскільки доводиться забезпечувати сумісність з різними версіями операційних систем та платформ [5]. З іншого боку, розробка веб-програмного забезпечення може забезпечувати більш простий процес оновлення та підтримки, оскільки можна змінювати функції та оновлювати програмне забезпечення на сервері, а не на кожному пристрої користувача. Таким чином, при виборі між нативним та веб-програмним забезпеченням слід враховувати не лише вартість розробки, але й витрати на майбутню підтримку та оновлення.

Важливим фактором є зручність використання програмного забезпечення. Нативне програмне забезпечення може бути більш зручним у використанні, оскільки воно розроблене спеціально для конкретної платформи та може використовувати всі її можливості. У той же час, веб-програмне забезпечення може бути більш універсальним та зручним у використанні на різних платформах, таких як комп'ютери, планшети та мобільні пристрої.

Окрім цього, треба враховувати технічні можливості та обмеження кожного типу програмного забезпечення. Наприклад, нативне програмне забезпечення може бути більш потужним у виконанні складних операцій, таких як обробка великої кількості даних або виконання графічних ресурсів з високою якістю.

Останнім чинником, який слід враховувати, є можливість масштабування програмного забезпечення. Веб-програмне забезпечення може бути більш масштабованим, оскільки воно може працювати на різних серверах та використовувати хмарні технології. Це може дозволити обміну даними зберігати та обробляти більшу кількість інформації та забезпечити доступ користувачам з різних регіонів світу, масштабування нативного програмного забезпечення може бути складним завданням, оскільки воно зазвичай розробляється для конкретної платформи та обмежується обчислювальними ресурсами на локальному комп'ютері. Однак, в нативному програмному забезпеченні може бути більша продуктивність, ніж у веб-програмному забезпеченні, оскільки воно може працювати безпосередньо з обчислювальними ресурсами на локальному комп'ютері. Також, нативне програмне забезпечення може бути більш надійним та захищеним від зломів, оскільки воно працює локально та не піддається впливу мережі.

Веб-програмне забезпечення може бути оновлене централізовано на серверному рівні, що дозволяє вирішувати потенційні проблеми безпеки та недоліків в програмному забезпеченні усіх користувачів одночасно. Це зменшує ризик виникнення проблем безпеки, які можуть виникнути через неправильну конфігурацію або застарілість програмного забезпечення.

У разі нативного програмного забезпечення кожен користувач мусить вручну встановлювати оновлення і налаштовувати на своєму пристрої. Це може створити проблеми з безпекою, якщо користувачі забувають оновлювати своє програмне забезпечення або не знають, як правильно налаштувати його для забезпечення максимального рівня безпеки.

Крім того, веб-програмне забезпечення зазвичай працює на багатьох платформах, в той час як нативне програмне забезпечення зазвичай працює лише на одній платформі. Це може

бути корисним для користувачів, які працюють на різних операційних системах або мають доступ до різних типів пристроїв.

Однак, веб-програмне забезпечення може бути повільніше в порівнянні з нативним програмним забезпеченням, оскільки воно працює в середовищі браузера та може бути обмежене можливостями браузера та мережевої пропускної здатності. Крім того, веб-програмне забезпечення зазвичай залежить від доступності мережі, що може бути проблемою в разі обміну захищеними даними в умовах обмеженого чи відсутнього Інтернет-з'єднання.

Обидва види програмного забезпечення мають свої переваги та недоліки, і вибір між ними залежить від конкретних потреб та вимог користувачів. Нативне програмне забезпечення може бути кращим вибором для використання в обмеженому колі користувачів, які працюють на певній платформі, тоді як веб-програмне забезпечення може бути більш підходящим для більш широкого кола користувачів, які працюють на різних пристроях та платформах.

Висновки. Зважаючи на розглянуті аспекти, можна зробити наступні висновки щодо порівняння нативного та веб-програмного забезпечення для обміну захищеними даними.

Нативне програмне забезпечення зазвичай забезпечує вищу швидкість та продуктивність, а також має більшу можливість керування обладнанням, яке використовується для збереження даних.

Веб-програмне забезпечення, незважаючи на те, що воно може бути менш продуктивним, надає перевагу у доступності та масштабованості. Крім того, веб-програмне забезпечення не вимагає установки на локальному комп'ютері, що полегшує процес розгортання та встановлення.

На підставі цього, якщо користувачі мають вимоги до продуктивності та мають достатньо ресурсів для установки та керування нативним програмним забезпеченням, вони можуть зробити вибір на користь нативного програмного забезпечення. У разі, якщо користувачі шукають зручність, доступність та масштабованість, вони можуть звернутися до веб-програмного забезпечення.

З іншого боку, веб-програмне забезпечення зазвичай має менші витрати на розробку та підтримку, може бути доступним з будь-якого пристрою та операційної системи та має високу міру масштабованості. Однак, веб-програмне забезпечення може бути менш безпечним та менш ефективним у роботі з великими об'ємами даних.

Отже, при виборі між нативним та веб-програмним забезпеченням для обміну захищеними даними, необхідно зважати на різні фактори, такі як безпека, вартість, доступність, ефективність та масштабованість.

Список використаних джерел

1. Герасимик І. Розробка мобільних додатків і їх види. – 2023. [Електронний ресурс]. – Режим доступу: – http://apeps.kpi.ua/rozrobka-mobilnykh-dodatkiv-i-yii-vidy
2. Kinsta – 2023. [Електронний ресурс]. – Режим доступу: https://kinsta.com/knowledgebase/tls-vs-ssl/
3. HHS.gov. Health Information Privacy. – 2023. [Електронний ресурс]. – Режим доступу: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
4. WebFX. Native App vs. Mobile Web App: A Quick Comparison. – 2023. [Електронний ресурс]. – Режим доступу: https://www.webfx.com/blog/web-design/native-app-vs-mobile-web-app-comparison/
5. Science soft. Software Maintenance Costs. – 2023. [Електронний ресурс]. – Режим доступу: https://www.scnsoft.com/services/software-development/software-support-and-maintenance/costs

Робота виконана під науковим керівництвом к.е.н, старшого викладача
ФРАНЧУК Т. М.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ КРИВИХ ГІЛЬБЕРТА В КОМП'ЮТЕРНИХ СИСТЕМАХ

ЮРЧЕНКО С., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Ця стаття досліджує багато застосувань кривої Гільберта в комп'ютерних системах, включаючи стиснення даних, криптографію та обробку зображень. Ми розглянемо унікальні властивості кривої Гільберта та те, як її можна використовувати для оптимізації алгоритмів комп'ютерів та апаратної реалізації. Дослідивши останні дослідження та розвиток у цій галузі, ми можемо отримати уявлення про майбутнє комп'ютерної технології та про те, яку роль може відігравати крива Гільберта у її формуванні.

This article explores the many applications of the Hilbert curve in computer systems, including data compression, cryptography, and image processing. We will examine the unique properties of the Hilbert curve and how it can be utilized to optimize computer algorithms and hardware implementations. By examining the latest research and developments in this field, we can gain insights into the future of computer technology and the role that the Hilbert curve may play in shaping it.

Актуальність. Криві Гілберта – це універсальний математичний об'єкт, який залишається важливим у комп'ютерних технологіях протягом понад століття. Однією з причин цього є їх здатність ефективно представляти просторову інформацію. Криві Гілберта є кривими, які заповнюють простір, що означає, що вони можуть заповнити двовимірний простір за допомогою однієї неперервної лінії. Ця властивість робить їх корисними для різних застосувань, які пов'язані з представленням або аналізом просторових даних, таких як комп'ютерна графіка, географічні інформаційні системи та обробка зображень.

Іншою причиною актуальності кривих Гілберта є їх самоподібність та фрактальна природа. Самоподібність означає, що крива виглядає схоже на різних масштабах, а фрактальна природа означає, що крива має нецілі розміри. Ці властивості зробили криві Гілберта цікавою областю досліджень у таких галузях, як теорія хаосу, динамічні системи та складні системи. У комп'ютерних технологіях ці властивості використовуються в застосуваннях, таких як стиснення даних та криптографія.

Метою статті є дослідження особливостей використання кривих Гілберта в комп'ютерних системах та продемонструвати їхню важливість і актуальність у різноманітних застосуваннях.

Об'єктом дослідження є особливості використання кривих Гілберта в комп'ютерних системах

Предмет дослідження – криві Гілберта.

Аналіз попередніх досліджень. Дослідженню кривих Гілберта в комп'ютерних системах присвячені праці закордонних науковців: Девіда Гілберта, Бенуа Мандельброта, Мартіна Гарднера, Джона Халтона, Кена Перлін та ін.

Виклад основного матеріалу. Використання кривих Гілберта (рис.1) можна поділити на такі сегменти:

1. Представлення та аналіз даних:
- Географічні інформаційні системи
- Просторові бази даних
- Застосування в машинному навчанні

2. Обробка зображень та графіка:

- Створення фрактальних ландшафтів та місцевостей
- Сегментація зображень
- Алгоритми виявлення контуру

3. Стиснення даних та криптографія:
- Стиснення даних
- Генерація ключів шифрування
- Безпечні канали зв'язку:

4. Апаратна реалізація
- Просторове індексування
- Пошук даних

5. Квантові обчислення та ДНК-обчислення:
- Представлення та маніпулювання квантовими станами
- Кодування та декодування інформації

Розглянемо кожен з них більш детально.

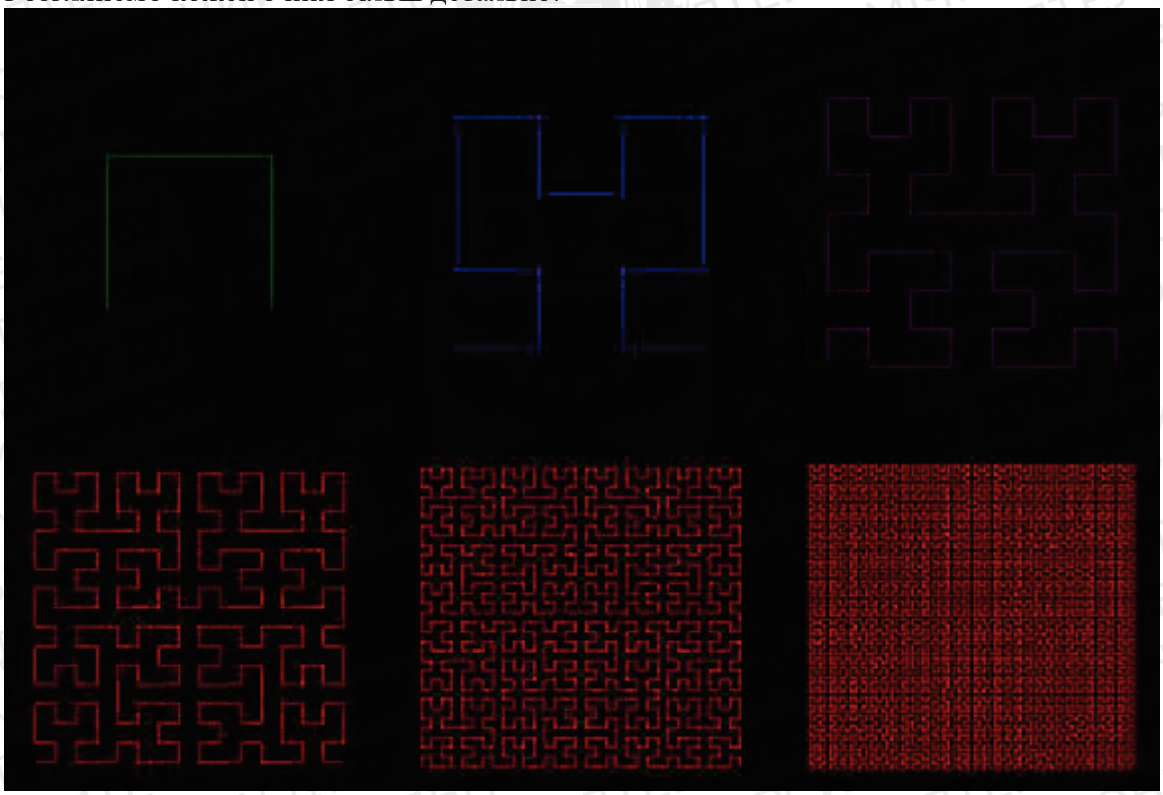


Рис.1. Криві Гілберта

Криві Гілберта використовуються в геоінформаційних системах для ефективного зберігання та отримання просторових даних. Вони забезпечують криву, яка заповнює простір, зберігаючи локальність, що означає, що близькі точки в двовимірному просторі відображаються н близьких точках на кривій. Ця властивість дозволяє швидкий та ефективний запит та отримання даних, а також просторове індексування та кластеризацію.

Подібно до ГІС. Криві Гілберта можуть бути використані в просторових базах даних для представлення та запиту просторових даних. Вони дозволяють ефективну індексацію та запит даних, а також швидкий пошук найближчіх сусідів. Криві Гілберта також можуть використовуватися для зберігання та запиту багатовимірних даних, що робить їх корисними в застосуваннях машинного навчання.

В застосуваннях машинного навчання криві Гілберта використовуються для представлення та аналізу даних. Вони можуть бути використані для зменшення розмірності багатовимірних даних, що спрощує їх аналіз та обробку. Криві Гілберта також надають спосіб

відображення даних в одновимірному просторі, що може бути корисним у кластеризаційних та класифікаційних алгоритмах.

Щодо обробки зображень та графіки, криві Гілберта використовуються для генераціх фрактальних ландшафтів та місцевостей. Для цього квадрат рекурсивно ділять на чотири менших квадрати, а отримані вершини відображають на кривій Гілберта. Цей процес повторюється, щоб створити більш складні особливості місцевості, що в результаті дає візуально привабливий та натуральних вигляд місцевості.

Також криві Гілберта використовують в алгоритмах сегментації зображень для розділення зображення на регіони на основі їх візуальних властивостей. Для цього зображення пікселі відображають на кривій Гілберта, яка зберігає просторову локальність пікселів. Це дозволяє ефективно кластеризувати пікселі на основі їх положення на кривій.

Криві Гілберта також використовуються в алгоритмах виявлення граней, які ідентифікують межі між регіонами на зображенні. Для цього зображення пікселі відображають на кривій Гілберта, після чого обчислюється локальний градієнт по кривій. Це надає змогу ідентифікувати переходи між різними регіонами на зображенні.

Не менш важливим є використання кривих Гілберта в стисненні даних та криптографії. Криві Гілберта можуть бути використані в методах стиснення даних для зменшення їх розміру. Один зі способів полягає у застосуванні кривої Гілберта до зображення, що переставляє значення пікселів у більш ефективний спосіб. Ця перестановка дозволяє краще стиснення через можливість використання просторової згуртованості зображення, що означає, що близькі пікселі мають тенденцію мати подібні значення. За допомогою перестановки значень пікселів з використанням кривої Гілберта, алгоритм стиснення може ефективніше групувати подібні значення, що призводить до меншого розміру файлу.

Криві Гілберта можуть бути використані для генерації безпечних ключів шифрування. Процес полягає у використанні кривої Гілберта для створення двовимірної мапи точок. Криптографічна функція застосовується до кожної точки для генерації послідовності випадкових чисел. Ці випадкові числа можуть бути використані для генерації ключа шифрування, який може бути використаний для шифрування даних. Використання крифої Гілберта для генерації ключів шифрування забезпечує більш високий рівень безпеки, оскільки послідовність точок на кривій є детермінованою і не може бути легко вгадана зловмисниками.

Криві Гілберта також можуть бути використані для створення безпечних комунікаційних каналів між двома сторонами. Один з методів полягає в використанні кривої Гілберта для генерації послідовності випадкових чисел, які потім використовуються для шифрування повідомлень, відправлених між сторонами. Цей процес створює безпечний комунікаційний канал, оскільки ключі шифрування є унікальними і не можуть бути легко вгадані зловмисником. Крім того, оскільки крива Гілберта є детермінованою, обидві сторони можуть згенерувати однакову послідовність точок і використовувати їх для дешифрування повідомлень, що забезпечує надійність комунікації.

Криві Гілберта також можуть бути використані для швидкого отримання інформації з великих наборів даних. Індексуючи дані за допомогою кривої Гілберта, отримання даних можна виконувати за допомогою простого пошукового алгоритму, який слідує кривій. Цей алгоритм відомий як Hilbert R-tree та є варіантом традиційного алгоритму індексування R-tree.

Використовуючи Hilbert R-tree, відновлення даних може бути виконано ефективніше, навіть для великих наборів даних.

У квантовій механіці квантовий стан представляється як комплексний вектор в багатовимірному просторі, відомому як гілбертів простір. Гілбертові криві можуть використовуватись для представлення та маніпулювання квантовими станами більш ефективним способом.

Одне з застосувань гілбертових кривих у квантовій механіці – це симуляція квантових систем. Квантові симуляції вимагають обчислення еволюції квантової системи з часом. Використовуючи криву Гілберта для представлення квантового стану, симуляцію можна

виконувати більш ефективно, оскільки крива може зафіксувати просторову узгодженість квантового стану.

У комп'ютерній науці з ДНК, молекули ДНК використовуються для представлення та обробки інформації, а виклик полягаж в тому, зоб ефективно шукати та маніпулювати великими наборами послідовностей ДНК. Криві Гілберта можуть бути використані для відображення послідовностей ДНК в двовимірному просторі, де просторове розташування послідовностей відображає їх подібність або відмінність. Це може бути корисно для кластеризації та класифікації великих наборів послідовностей ДНК та для проектування ефективних алгоритмів для вирішення проблем в обчисленні ДНК, таких як задачі оптимізації.

Крім того, криві Гілберта можуть бути використані для зберігання та відновлення даних в обчисленні ДНК. Відображаючи послідовності ДНК на криву Гілберта, просторова близкість послідовностей може бути збережена, що може бути корисно для ефективного відновлення послідовностей, які подібні або пов'язані між собою. Використання кривих Гілберта в обчисленні ДНК є перспективним підходом для вирішення деяких проблем, пов'язаних з маніпулюванням та обробкою великих послідовностей ДНК.

Апаратні реалізації кривої Гільберта є областю активних досліджень та розробок. Ці реалізації можуть мати різні форми, такі як цифрові кола, програмовані логічні матриці (FPGA) та спеціалізовані інтегральні мікросхеми (ASIC). Однією з основних мотивацій для реалізації кривої Гільберта у апаратурі є прискорення обчислень, що потребують просторової індексації або пошуку даних.

Один з підходів до апаратної реалізації полягає у використанні рекурсивного алгоритму для побудови кривої Гільберта, який може бути реалізований за допомогою цифрових кол. Цей підхід передбачає поділ двовимірного простору на чотири квадранти та рекурсивне застосування алгоритму до кожного квадранту для побудови кривої. Такі реалізації можуть бути використані для застосувань, таких як обробка сигналів, стиснення зображень та кодування відео, та демонструють значні прискорення порівняно з програмними реалізаціями.

Іншим підходом до апаратної реалізації є використання програмованих логічних матриць (FPGAs), які можуть бути програмовані для реалізації спеціалізованих апаратних архітектур. Цей підхід використовується для застосувань, таких як розпізнавання образів, кластеризація даних та відновлення даних, де крива Гільберта використовується для відображення даних в двовимірному просторі. Реалізації на базі FPGA мають перевагу гнучкості, що дозволяє перепрограмовувати апаратне забезпечення для різних застосувань та наборів даних.

Реалізації на базі ASIC кривої Гільберта пропонують потенційні переваги в забезпеченні ще більшої швидкодії, оскільки вони проектуються спеціально для конкретного застосування. Ці реалізації включають проектування спеціалізованих схем, які оптимізовані для алгоритму кривої Гільберта, і можуть надавати значні переваги в термінах швидкості та споживання енергії. Однак реалізації на базі ASIC зазвичай є більш дорогими та витратними на розробку, ніж інші апаратні реалізації, і тому використовуються в основному для застосувань, де важлива швидкість, таких як обробка сигналів в реальному часі або високопродуктивні обчислення.

Для застосувань, які вимагають просторового індексування чи пошуку даних, апаратні реалізації кривої Гільберта надають значних переваг. Вибір конкретної реалізації залежить від таких факторів, як конкретне застосування, бажаний рівень продуктивності та доступні ресурси. Оскільки технології апаратних засобів продовжують розвиватися, ймовірно, що використання кривих Гільберта в апаратних реалізаціях стане ще більш поширеним та ефективним.

Використання кривих Гільберта в комп'ютерних технологіях відкрило нові можливості для досліджень та розробок. Є кілька областей, де можна розширити використання кривих Гільберта, що приведе до нових застосувань та технологій. Одна з областей майбутніх досліджень - використання кривих Гільберта в квантових обчисленнях. При поширенні квантових комп'ютерів стає ще важливішим ефективне просторове індексування та

відновлення даних. Криві Гільберта можуть потенційно використовуватися для оптимізації цих операцій в квантових обчисленнях, що призведе до швидших та більш ефективних обчислень.

Інша область майбутніх досліджень - використання кривих Гільберта в машинному навчанні та штучному інтелекті. Алгоритми машинного навчання часто включають маніпулювання та аналіз великих обсягів даних, а просторове індексування та відновлення даних є важливими компонентами багатьох з цих алгоритмів. Криві Гільберта можуть потенційно використовуватися для оптимізації цих операцій, що призведе до більш ефективних та ефективних алгоритмів машинного навчання.

Крім того, використання кривих Гільберта в апаратному забезпеченні є галуззю, де потрібні додаткові дослідження. Розробка нових апаратних технологій, таких як нейроморфне обчислення, може потенційно отримати користь від використання кривих Гільберта в архітектурі апаратного забезпечення. Крім того, розробка нових алгоритмів та технік для конструювання та маніпулювання кривими Гільберта в апаратному забезпеченні може призвести до ще більш ефективних реалізацій.

В цілому використання кривих Гільберта в комп'ютерних технологіях є перспективним напрямком досліджень та розробки з багатьма потенційними застосуваннями та можливостями для майбутнього зростання. При тому, як дослідники продовжують досліджувати можливості кривих Гільберта та розробляти нові алгоритми та техніки для їх використання, ми можемо очікувати ще більш інноваційних та ефективних застосувань цієї технології у майбутньому.

Висновки. Крива Гільберта - захоплюючий та багатофункціональний інструмент, який знайшов широке застосування в комп'ютерних технологіях. Від стиснення даних та криптографії до обробки зображень та ДНК-обчислень, унікальні властивості кривої Гільберта зробили її цінним інструментом для представлення та обробки даних у різних галузях.

Особливо обіцяними результатами використання кривих Гільберта є застосування їх у просторовому індексуванні та отриманні даних, обробці зображень та комп'ютерній графіці, а також в ДНК-обчисленнях. Крім того, дослідження продовжують вивчати потенційні застосування кривих Гільберта у квантових обчисленнях та представленні квантових станів.

Оскільки комп'ютерні технології продовжують еволюціонувати та розширюватися, корисність та багатогранність кривих Гільберта, ймовірно, продовжуватимуть зростати. Тому вивчення та застосування кривих Гільберта залишатимуться важливою областю дослідження та розвитку ще протягом багатьох років.

Список використаних джерел

1. "Hilbert Curve Indexing for High-Dimensional Similarity Search": https://www.researchgate.net/publication/220838655_Hilbert_Curve_Indexing_for_High-Dimensional_Similarity_Search

2. "Hilbert curves and their applications in computer graphics": https://www.sciencedirect.com/science/article/pii/S0097849306000892

3. "Hilbert Curves: A Tutorial": http://www.dgp.toronto.edu/people/mooncake/papers/hilbert-tutorial.pdf

4. "Hilbert Curves in Data Science": https://www.linkedin.com/pulse/hilbert-curves-data-science-sudheendra-chilappagari

5. "Spatial Indexing Using the Hilbert Space-Filling Curve": https://www.sciencedirect.com/science/article/pii/S0306437906000416

Робота виконана під науковим керівництвом к.е.н., доцента
ТИЩЕНКА Д.О.

ПРИНЦИПИ ТА ОСОБЛИВОСТІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ЮЩЕНКО О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто передумови виникнення, основні принципи та особливості мікросервісної архітектури програмного забезпечення, її переваги, недоліки та область використання, порівняння із монолітної архітектурою.

This article considers reasons of appearance and development, main principles and traits of microservice software architecture, it's advantages, disadvantages and usage sphere, comparison with monolithic architecture.

Актуальність. Інформаційні технології та програмне забезпечення відіграють дуже важливу роль у житті суспільства. Банківська справа, торгівля, медицина, освіта та безліч інших сфер діяльності людини – все це спирається на спеціалізоване програмне забезпечення, що призначене для полегшення та підвищення ефективності праці. Умовами правильного та безперебійного функціонування такого програмного забезпечення є якість та «чистота» програмного коду, що в першу чергу залежить від проаналізованих вимог та правильно підібраної архітектури додатку.

Метою статті є дослідження особливостей мікросервісної архітектури, її розвитку, переваги та недоліки, область використання.

Об'єктом дослідження є архітектура програмного забезпечення.

Предмет дослідження – мікросервісна архітектура та її застосування при розробці програмного забезпечення.

Виклад основного матеріалу. Архітектура програмного забезпечення – це набір правил та вимог до внутрішньої структури програми та того, як її компоненти та модулі взаємодіють між собою. Основною задачею архітектури програмного забезпечення є аналіз вимог до системи та вироблення стратегії, що позволить правильно відобразити та реалізувати предметну область задачі через код. Правильно розроблена архітектура ПЗ допомагає вирішувати такі проблеми як: надійність, відмовостійкість, розширюваність, супроводжуваність, безпека, доступність тощо.

Розвиток архітектури програмного забезпечення тісно пов'язаний із розвитком інформаційних технологій у цілому. Перше спеціалізоване програмне забезпечення не було дуже вибагливим та складним, проте разом із розвитком та ускладненням задач, що потрібно було вирішувати, почали зазнавати розвитку і мови програмування, парадигми та шаблони проектування.

Першим популярним видом архітектури, що дав передумови та причини до виникнення мікросервісної архітектури, прийнято вважити **монолітну** (monolithic) архітектуру. Головною особливістю цього виду архітектури було те, що весь додаток побудований за даним принципом був неподільним та самодостатнім. Монолітний додаток містив у собі абсолютно всю логіку, що потрібна для його роботи, він не залежив від інших додатків та розповсюджувався у вигляді одної єдиної програми.

Такий підхід містить набагато більше недоліків, ніж переваг. Головною перевагою даної архітектури є легкість її реалізації. Монолітний додаток – це те, що зазвичай виходить неявно, природньо, оскільки для реалізації такої архітектури не потрібно витрачати багато зусиль – додаток розростається, новий код просто додається до існуючого, функціонал та область використання змішуються.

Вартість впровадження та легкість розгортання теж є сильними сторонами монолітної архітектури, оскільки для запуску однієї програми на сервері не потрібна велика кількість

налаштувань та інфраструктури. Вартість інфраструктури що потрібна для розгортання такого додатку буде мінімальною у порівнянні з іншими видами архітектур. Наявність лише одного виконуваного файлу також полегшує процеси тестування та налагодження (debug).

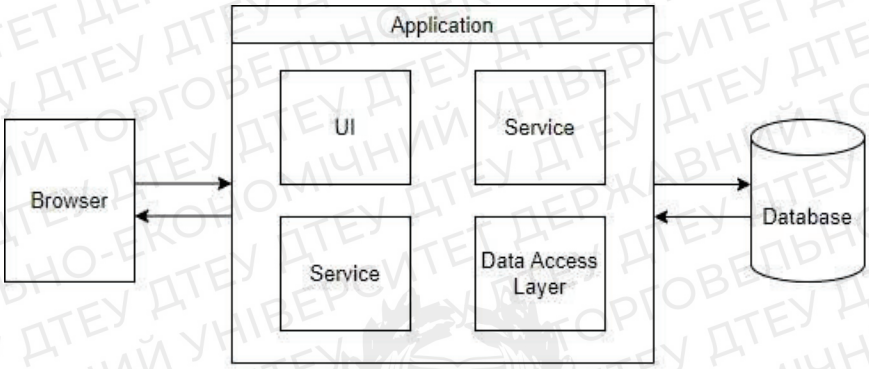


Рис. 1. Приклад монолітної архітектури додатку

Головним недоліком монолітної архітектури є її непідтримуваність протягом довгого часу. Оскільки монолітний додаток є неподільним, це означає що він розростається дуже швидко разом із впровадженням нового функціоналу. Вихідний код додатку стає незрозумілим та заплутаним, впровадження нових ідей стає тільки важче, все частіше стає у нагоді «рефакторинг», що тільки збільшує вартість підтримки та розробки нового програмного коду.

Іншим важливим недоліком монолітної архітектури є її ненадійність та немасштабованість. Через неподільність монолітного додатку, неможливо масштабувати тільки ту його частину, яка зазнає найбільшого навантаження, можливо масштабувати лише весь додаток уцілому, шляхом запуску додаткових екземплярів додатку (горизонтальне масштабування). З цієї самої причини, необроблена помилка під час виконання монолітної програми ставить під загрозу весь додаток одразу - одна така помилка може «покласти» весь додаток. Таким чином, можна виділити наступні передумови виникнення мікросервісної архітектури:

- *Ускладнення вимог та постійний розвиток*. Додавати новий функціонал потрібно все частіше, це повинно бути легко та відносно недорого. Програмний код повинен бути підтримуваним.
- *Доступність*. Із постійним розвитком інформаційних технологій все більше людей мають доступ до комп'ютерів, смартфонів та інтернету, отже програми повинні витримувати велике навантаження.
- *Відмовостійкість*. Чим більше система, тим складніше стають зв'язки між її частинами, збільшується можливість помилок. Система не повинна припиняти свою роботу, навіть у випадку коли якась її частина відмовила.
- *Розповсюдження таких практик як Agile та DevOps*.

Мікросервісна архітектура – це підхід до розробки програмного забезпечення як сукупності окремих незалежних сервісів, що взаємодіють між собою. Кожний такий сервіс відповідає за конкретну функціональність додатку, взаємодіє з іншими сервісами за допомогою HTTP запитів або подій, та може бути розгорнутий та масштабований окремо від інших. Сервіс – це структурна одиниця мікросервісної архітектури, саме це є її головною особливістю.

Принципи та переваги мікросервісної архітектури

1. *Сервіси є малими та сфокусованими на конкретній задачі*. У кожного сервісу у системі є своє конкретне призначення, що відображає окремий аспект предметної області додатку. Сервіс повинен містити у собі лише той функціонал та логіку, які безпосередньо стосується тієї задачі, що він призначений вирішувати.

За допомогою ділення додатку на множину сервісів можна уникнути заплутаності та змішування програмного коду, адже відтепер вихідний код буде логічно розділений у залежності від бізнес-вимог. Додавання нового функціоналу також стає легше, оскільки зміні зазнається не увесь додаток одразу, а лише його мала частина.

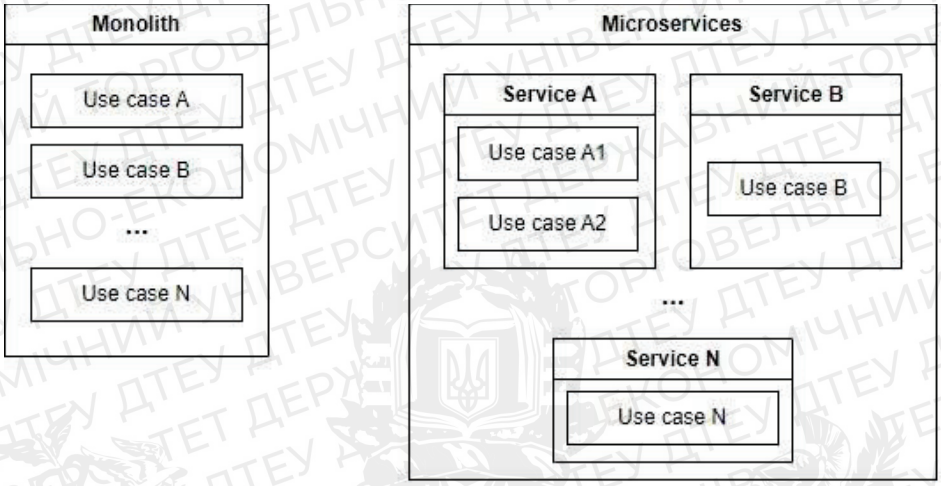


Рис. 2. Порівняння монолітної та мікросервісної архітектури

2. *Автономність та ізольованість*. Кожний сервіс є окремою незалежною сутністю, що запускається як окремий процес операційної системи або додаток у хмарі. Сервіси не знають про внутрішню реалізацію один одного та взаємодіють тільки за допомого API (Application Programming Interface), що вони надають. Зміни, що відбуваються в одному сервісі, не повинні вплинути на роботу інших сервісів та клієнтів, за умови що існуючий програмний інтерфейс сервісу залишився без змін. Така «розв'язаність» (decoupling) сприяє зменшенню залежностей частин додатку одна від одної, надає можливість змінювати реалізацію сервісів без впливу на всю систему та краще перевикористовувати існуючий функціонал.

Іншою вагомою перевагою є зручність розгортання сервісів. Оновлення декількох рядків коду у монолітному додатку вимагає повного перерозгортання всієї системи, що завжди є повільним, сповненим ризику, процесом. Це також означає, що випуск релізів та оновлень стається рідше, адже малі зміни вигідніше групувати та випускати разом. Внесення та випуск змін у мікросервіси є набагато легшим та безпечнішим процесом, оскільки зміні зазнається лише один конкретний сервіс.

3. *Організованість навколо бізнес-вимог*. Відповідно до закону Конвея (Melvin Conway, 1968), «будь-яка організація що проєктує систему, створить дизайн зі структурою, яка буде копією структури комунікації в цій організації». Це означає, що структура великих систем часто залежить від структури та організації зв'язків у середині самої компанії, що буде використовувати цю систему. Якщо у компанії є суворе розподілення на команди спеціалістів із front-end, back-end, спеціалістів із баз даних тощо, то кінцева система скоріш за все буде мати точно таке саме розподілення по модулям. Проблема закладається у тому, що при впроваджені нових ідей та функціоналу може виникнути питання, який саме підрозділ має впроваджувати ці зміни. Через суворе розподілення спеціалістів на команди, ці зміни часто погано обговорюються або впроваджуються не в ту частину системи, куди вони належать, що у свою чергу призводить до змішування та укладення програмного коду.

Мікросервісна архітектура допомагає вирішити цю проблему за допомогою організованості навколо вимог, не навколо ролей. Команда, що працює над конкретним сервісом, може мати спеціалістів з різних областей, що у свою чергу допомагає правильно оцінити та реалізувати зміни. Також, така команда не отримає завдання на впровадження змін, що її не стосуються, адже за такою структурою можна легко зрозуміти, яка команда відповідальна за конкретну частину додатку.

4. *Незалежність від технологій*. На відміну від монолітної архітектури, де обраний стек технологій майже не змінюється протягом всього часу, мікросервісна архітектура цілковито заохочує використання різних технологій для різних сервісів. Кожний сервіс у праві користуватися саме такими інструментами, які найкраще підходять для реалізації поставленої задачі.

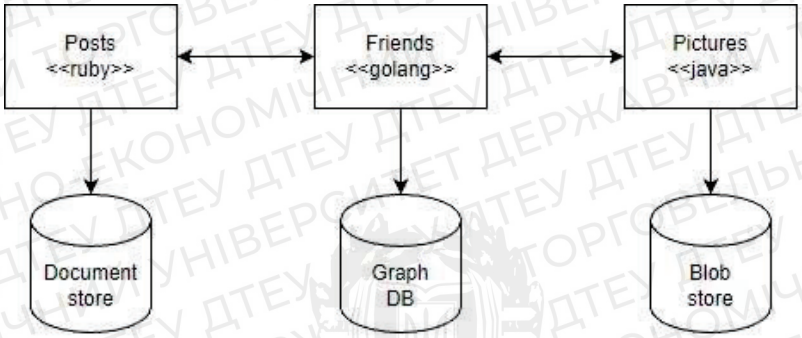


Рис. 3. Приклад сервісів, створених із використанням різних технологій

5. *Пристосованість до збоїв*. Впровадження мікросервісної архітектури дозволяє значним чином підвищити відмовостійкість додатку, адже при виході із ладу одного із сервісів, додаток не завершується аварійно, а лише втрачає частину відповідного функціоналу. Альтернативно, окремі сервіси можна вимикати усвідомлено, наприклад у випадку витоку даних або ключів доступу.

6. *Автоматизація інфраструктури*. Мікросервісну архітектуру дуже зручно використовувати у купі із такими практиками як DevOps та Agile, головними принципами яких є гнучкість, швидкість розробки та розгортання, випуску продукту на ринок. Для кожного сервісу додатку зручно створювати процеси автоматизації (CI/CD pipeline), що є відповідальними за збирання коду, забезпечення необхідної інфраструктури та розгортання. Наявність таких процесів значно підвищує ефективність розробки та зменшує час, який розробники витрачають на непов'язані із розробкою активності. Процес виписку нових версій продукту також стає значно простішим та менш ризикованим, оскільки можливість людської помилки стає менше: все що необхідно зробити – це запустити необхідний процес.

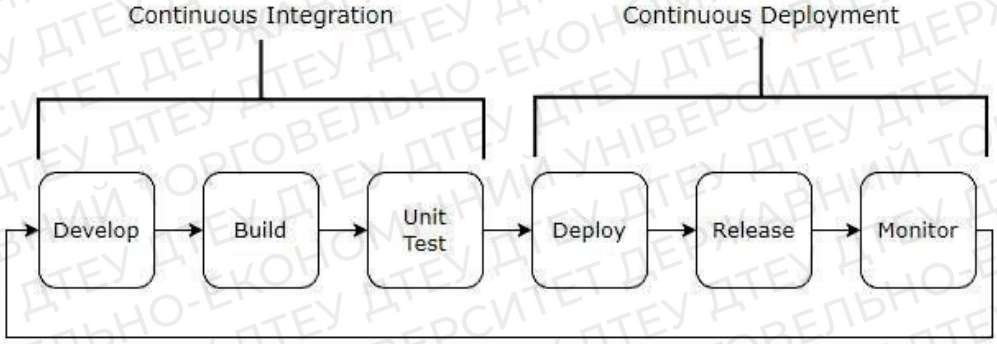


Рис. 4. Приклад автоматизації процесу збирання та розгортання коду

Через свої переваги, мікросервісна архітектура отримала визнання розробників та широке поширення. Першою великою компанією, що почала активно застосовувати та сприяти розвитку мікросервісної архітектури прийнято вважати Netflix. Netflix почали міграцію від монолітної архітектури у 2009 році, через швидке зростання кількості активних користувачів та інформації, що потрібно зберігати та оброблювати, і на кінець 2011 року перенесли весь свій функціонал на мікросервіси у хмарі. Безліч інших великих компаній, таких

як Amazon, Microsoft, Uber, Spotify, Twitter, також використовують мікросервіси у своїх додатках.

Сьогодні мікросервісну архітектуру можна використовувати при розробці широкого спектру застосунків, особливо якщо вони мають підтримувати високе навантаження або оброблювати велику кількість інформації у режимі реального часу. Інтернет магазини, соціальні мережі, фінансові додатки, IoT та багато іншого – все це може ефективно використовувати переваги мікросервісної архітектури. Проте, незважаючи на велику кількість переваг, мікросервіси не позбавлені недоліків.

Недоліки мікросервісної архітектури.

1. *Вартість інфраструктури*. Через те, що кожний сервіс хоститься окремо від інших, кількість необхідної інфраструктури, а отже її кінцева вартість зростає. Різні сервіси можуть потребувати різні операційні системи, різні бази даних, різні обчислювальні потужності тощо. Якщо додаток розрахований на велику кількість користувачів, окремої уваги потребує налаштування мережі та розподілення трафіку, що теж потребує додаткових ресурсів та витрат. Також, через те, що кожний сервіс користується власним набором технологій, кількість різноманітних ліцензій зростає.

2. *Важкість тестування.* З одної сторони, мікросервіси полегшують тестування, оскільки перевірці зазнається окремий сервіс за раз; тестування окремого, конкретного функціоналу стає легше, оскільки за нього відповідає один сервіс. З іншої сторони, у випадку коли необхідно протестувати велику частину функціоналу, що може потребувати взаємодії великої кількості сервісів, важкість тестування значно зростає. У випадку, коли такий сценарій не проходить тестування, може бути абсолютно неочевидно, який саме із сервісів викликав помилку, тому кожний з них зазнає повторного тестування. Тестування взаємодії сервісів один з одним також не є простою задачею, адже в залежності від виду комунікації між сервісами, команді тестувальників можуть знадобитися різні навички та інструменти.

3. *Вибагливість до експертизи.* Через велику кількість технологій, що можуть використовуватись під час розробки додатку, що використовує мікросервісну архітектуру, нерідко одному розробнику потрібно мати навички із декількох технологій або інструментів. DevOps інженери, що відповідають за розгортання інфраструктури, налаштування мережі, автоматизацію процесів, також мають володіти широким спектром навичок, щоб можна було виконати всі поставлені вимоги. Все це тільки підвищує складність пошуку необхідних спеціалістів та витрати на них.

У статті було розглянуто поняття архітектури програмного забезпечення, мікросервісної архітектури, умови її виникнення та порівняння із монолітною архітектурою, головні принципи, переваги, недоліки та область застосування мікросервісної архітектури.

Список використаних джерел

1. Fowler M. Microservices: a definition of this new architectural term [Електронний ресурс] / Martin Fowler // martinfowler.com. – 2014. – Режим доступу до ресурсу: https://martinfowler.com/articles/microservices.html.
2. Richards M. Fundamentals of Software Architecture / M. Richards, F. Neal., 2020. – 265 с. – (O'Reilly Media, Inc).
3. Newman S. Building Microservices / Sam Newman., 2015. – 265 с. – (O'Reilly Media, Inc.).
4. Evans E. Domain-Driven Design: Tackling Complexity in the Heart of Software / Eric Evans., 2003. – 560 с. – (Addison Wesley).

Робота виконана під науковим керівництвом к.пед.н, доцента
ЖИРОВОЇ Т.О.

КОМУНІКАТИВНИЙ ОНЛАЙН-СЕРВІС СОЦІАЛЬНОЇ СПІЛЬНОТИ

ЯНУТА В., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуті питання створення комунікативного онлайн-сервісу соціальної спільноти з фокусом на мову програмування C#. Обґрунтовується важливість таких сервісів в сучасному інтернет-ландшафті та описуються наявні програмні платформи, які можуть бути використані для розробки таких сервісів. Також досліджується перевага використання архітектури ASP.NET для програмування на мові C# та те, як вона може бути використана для створення комунікативного онлайн-сервісу соціальної спільноти. Загалом, стаття відзначається важливість технічних вимог та умов, які необхідні для успішної розробки онлайн-сервісу соціальної спільноти та може служити корисним джерелом інформації для розробників, які планують зайнятися таким проектом.

This article provides an overview of the creation of a communicative online social community service, with a focus on programming language C#. The article examines the importance of such services in today's internet landscape and discusses the existing software platforms that can be used to develop such services. The article also explores the benefits of using the Model-View-Controller (MVC) architecture for C# programming and how it can be utilized in creating a communicative online social community service. Overall, the article highlights the technical requirements and considerations involved in developing a successful online social community service and can serve as a helpful resource for developers looking to embark on such a project.

Актуальність. Комунікативні онлайн-сервіси соціальної спільноти стають все більш популярними серед користувачів Інтернету. Завдяки таким сервісам, люди можуть швидко та зручно зв'язуватися один з одним, обмінюватися інформацією, ділитися своїми думками та враженнями. Проте, для ефективного використання комунікативних сервісів соціальної спільноти необхідні відповідні програмні рішення, які дозволяють забезпечити якість та безпеку обміну даними. У цій статті розглядаються різні програмні платформи, що використовуються для створення комунікативних онлайн-сервісів соціальної спільноти, а також описано процес їх створення з використанням мови програмування C#. Враховуючи широке використання таких сервісів в сучасному світі, стаття є актуальною для розробників, які прагнуть створити високоякісні та безпечні комунікативні онлайн-сервіси соціальної спільноти.

Метою даної статті є дослідження та аналіз програмних рішень, які можна використовувати при створенні комунікативного онлайн-сервісу соціальної спільноти з використанням мови програмування C#. В статті розглянуто архітектурний шаблон MVC, веб-фреймворк ASP.NET, бази даних та їх використання у проекті, а також інші програмні засоби, які дозволяють створити функціональний та ефективний онлайн-сервіс соціальної спільноти. Результатом цієї роботи буде огляд та порівняння програмних платформ з метою вибору оптимального рішення для розробки даного проекту.

Об'єктом дослідження є комунікативний онлайн-сервіс соціальної спільноти, який розробляється з використанням мови програмування C#.

Предметом дослідження є програмні рішення та технології, що використовуються для розробки комунікативного онлайн-сервісу соціальної спільноти з використанням мови програмування C#.

Аналіз попередніх досліджень. З огляду на актуальність теми комунікативних онлайн-сервісів соціальних спільнот, було проведено аналіз попередніх досліджень у цьому напрямку, зокрема статтю «Розробка соціальної мережі для бібліотек на основі .NET технологій» автора Н.С. Гайдука, де він детально описує процес розробки, зокрема, серед переваг використання .NET технологій автор зазначає високу продуктивність, безпеку та простоту розробки завдяки

вбудованим функціям мови програмування C#. Крім того, використання платформи ASP.NET дозволяє розробляти веб-додатки з високим рівнем масштабованості та забезпечувати швидкий доступ до баз даних. Однак, автор також зазначає недоліки використання .NET технологій, зокрема, високу вартість ліцензування та обмеження у підтримці інших мов програмування. Також можуть виникнути проблеми зі сумісністю між різними версіями платформи .NET.

З комунікативними онлайн-сервісами соціальної спільноти ми можемо легко знаходити старих друзів та знайомитися з новими, обмінюватися фотографіями, відеороликами та іншими медіа-контентами, створювати групи та спільноти за інтересами, та навіть здійснювати бізнес-взаємодію. Такі сервіси стали не тільки місцем для розваги та дозвілля, але й невід'ємною частиною нашого соціального життя, де ми ділимося важливими подіями, поглядами, та сприймаємо світ через призму інших користувачів.

Водночас у статті «Програмна реалізація агрегатора соціальних мереж» за авторством М.Яковенка, А.Охрименка, С.Кузніченко аналізується наступне: серед переваг автори зазначають використання платформи ASP.NET для розробки соціальних мереж, де є можливість швидкої розробки веб-додатків завдяки вбудованому фреймворку MVC та багатому інструментарію .NET. Крім того, з використанням Entity Framework, розробники можуть легко працювати з базою даних та забезпечити її ефективну роботу. Однак, на думку авторів статті, недоліком використання платформи ASP.NET є потреба у великій кількості коду для розробки веб-додатків, а також необхідність високої кваліфікації розробника для ефективної роботи з цією платформою. Крім того, у статті було зазначено, що платформа має високі вимоги до обладнання сервера, що може стати проблемою для невеликих компаній з обмеженим бюджетом.

Виклад основного матеріалу. Комунікативний онлайн-сервіс соціальної спільноти є інтернет-платформою, яка надає користувачам можливість спілкуватися між собою, обмінюватися інформацією, фотографіями та відео з іншими учасниками спільноти. Онлайн-сервіси соціальних мереж вже давно займають головне місце серед інтернет-платформ. Їх популярність зростає з кожним роком, і це створює значні можливості для бізнесу та комерційних проектів.

C# є об'єктно-орієнтованою мовою програмування, розробленою компанією Microsoft. Вона має багатий функціонал та підтримує сучасні технології програмування, такі як:

- Мультипоточність - можливість програми виконувати кілька потоків одночасно для збільшення швидкості та продуктивності виконання завдань. Це означає, що програма може виконувати декілька операцій одночасно, якщо є відповідні потоки. В C# мультипоточність можна реалізувати за допомогою потоків (Thread) або задач (Task), які дають можливість розподілити завдання між потоками та виконувати їх паралельно.
- Асинхронність - дозволяє програмі виконувати багато задач одночасно, зменшуючи час очікування на виконання окремих завдань та підвищуючи продуктивність програми. Зокрема, в C# для роботи з асинхронним кодом використовують ключові слова async та await, які дозволяють забезпечувати продовження виконання програми в той час, коли відбувається очікування відповіді від зовнішнього сервісу, бази даних чи іншої операції, що може зайняти значний час. Асинхронність є важливим аспектом розробки комунікативних онлайн-сервісів соціальної спільноти, оскільки такі сервіси повинні забезпечувати швидкий та ефективний доступ до великих обсягів даних та надавати користувачам зручний та комфортний досвід взаємодії.
- Паралельність - це здатність виконувати декілька завдань одночасно на різних процесорах або ядрах в рамках одного процесу. Він дозволяє розподіляти обчислювальні завдання на декілька потоків, що прискорює їх виконання та забезпечує більш ефективне використання ресурсів обчислювальної системи. У C# для досягнення паралельної роботи використовуються бібліотеки Parallel і PLINQ. Бібліотека Parallel містить класи, що дозволяють виконувати паралельні операції з масивами даних,

циклами, послідовностями та іншими операціями. PLINQ (Parallel LINQ) є розширенням LINQ і дозволяє розподіляти обчислення на кілька ядер процесора.

Також, C# має велику кількість вбудованих засобів та бібліотек, що дозволяє забезпечувати високу продуктивність та надійність програмних рішень, проте ця мова програмування є компільованою мовою програмування, що дозволяє виявляти помилки на етапі компіляції та зменшує ймовірність виникнення помилок в рантаймі. Присутність підтримки об'єктно-орієнтованої парадигми програмування, що дозволяє забезпечити високий рівень модульності та розширюваності проекту.

Оскільки комунікативний онлайн-сервіс соціальної спільноти часто має велику кількість користувачів та обробляє великі обсяги даних, важливо використовувати мову програмування, яка забезпечує ефективну роботу з великими обсягами даних та швидкий відгук на запити користувачів. C# має вбудовані засоби для роботи з базами даних та збереження даних у форматах XML та JSON. Крім того, C# має підтримку платформи .NET, що дозволяє розробникам використовувати багато функцій та бібліотек, що надаються цією платформою, а також, дана мова програмування має велику спільноту розробників, що дозволяє отримувати підтримку та поради від інших спеціалістів.

Однією з ключових складових будь-якого онлайн-сервісу соціальної спільноти є можливість взаємодії між користувачами. Спілкування може відбуватися в різних форматах, таких як приватні повідомлення, коментарі та відгуки на пости, фото або відео. Для створення такого сервісу важливо розробити ефективний механізм взаємодії між користувачами. Крім взаємодії, сервіс соціальної спільноти повинен мати такі складові, як профілі користувачів, створення та редагування постів, можливість підписуватися на сторінки інших користувачів, рейтинги та відгуки. Для реалізації цих функцій необхідно використовувати відповідні програмні рішення, що дозволяють забезпечувати комфортну та безпечну взаємодію між користувачами. Одним з таких рішень є мова програмування C#, яка дозволяє створювати потужні та ефективні онлайн-сервіси з використанням .NET-фреймворку.

Один з найважливіших аспектів при створенні онлайн-сервісу соціальної спільноти - це його безпека. Користувачі повинні бути захищені від шахрайства, крадіжки даних та інших загроз. Тому важливо використовувати захист даних, двофакторну автентифікацію та інші заходи безпеки. Для цього в C# є вбудовані засоби та бібліотеки, які дозволяють забезпечити надійний рівень захисту:

- Криптографічні бібліотеки - дозволяють шифрувати та розшифровувати дані, створювати та перевіряти цифрові підписи, а також генерувати випадкові числа, які можуть бути використані для створення паролів та ключів шифрування.
- Бібліотека безпеки - містить класи для роботи з безпекою, такі як безпека мережі, безпека додатку, керування даними, керування доступом, керування ідентифікацією та автентифікацією, а також класи для роботи з різними типами захисту, такими як кодування та шифрування.
- Механізми автентифікації та авторизації - дозволяють перевіряти, чи має користувач достатньо прав для виконання певної дії, та перевіряти його ідентифікацію, щоб забезпечити безпеку даних та системи в цілому.
- Засоби обробки винятків - дозволяють програмістам обробляти помилки та виключення, що виникають у процесі роботи програми, та запобігати їх негативному впливу на безпеку даних та системи.

Для розробки онлайн-сервісу соціальної спільноти на мові програмування C# можна використовувати такі платформи, як ASP.NET, MVC та інші. Ці платформи дозволяють створювати потужні та складні сервіси з використанням різних технологій та підходів:

ASP.NET - це фреймворк, який використовується для створення веб-додатків та сервісів. Дана платформа є високопродуктивною для розробки, вона дозволяє швидко створювати динамічні веб-сторінки та веб-додатки з використанням мов програмування C#, Visual Basic і інших мов, що підтримують .NET Framework. Фреймворк має безліч переваг для розробки комунікативного онлайн-сервісу соціальної спільноти, починаючи з переваг

забезпечення безпеки, також має багато функціональних можливостей, таких як вбудована підтримка для аутентифікації та авторизації, підтримку HTTPS, яка забезпечує шифрування даних між сервером та клієнтом. Щодо продуктивності, ASP.NET забезпечує велику швидкість роботи веб-додатків, завдяки розширеному кешуванню даних та оптимізації коду. Крім того, на цій платформі можна використовувати мультипоточність, асинхронність та паралельність для оптимізації продуктивності. Щодо масштабованості, ASP.NET має вбудовану підтримку для віддаленого керування, що дозволяє легко масштабувати веб-додатки до великої кількості користувачів та маштабувати їх згідно з потребами.

ASP.NET є однією з найбільш популярних платформ для розробки веб-додатків на мові C#. Розробниками цієї платформи є компанія Microsoft, яка постійно підтримує та оновлює цей інструмент. За даними сайту W3Techs, який вивчає статистику використання технологій у веб-розробці, на початку 2021 року платформа ASP.NET використовувалась більше ніж на 18% веб-сайтів у всьому світі. Також, згідно з даними порталу StackOverflow, ASP.NET є однією з найпопулярніших платформ для розробки веб-додатків.

Одним із переваг ASP.NET є можливість використання багатофункціональних бібліотек та фреймворків, що значно спрощує розробку веб-додатків. Наприклад, платформа містить вбудовану бібліотеку Entity Framework для роботи з базами даних, а також фреймворки для створення користувацьких інтерфейсів, такі як Angular та React.

Окрім того, платформа ASP.NET надійна та безпечна, оскільки містить вбудовані засоби для захисту від різних видів атак, таких як внедрення SQL-запитів, перетин сайтів та інші.

MVC - це архітектурний шаблон, який дозволяє розділити додаток на компоненти, що забезпечує більш просту та ефективну розробку. Даний шаблон можна використовувати в C# для створення веб-додатків та сервісів, що дозволяє розробникам більш ефективно керувати кодом та забезпечити його більшу повторюваність та легкість супроводу. MVC став популярним в програмному забезпеченні, особливо в розробці веб-додатків, завдяки своїй здатності до розширення, тестування та підтримки. Він дозволяє розробникам зосередитися на різних аспектах додатку та забезпечити кращу підтримку його функцій.

MVC затребуваний серед розробників та має велику кількість прикладів використання у веб-додатках, таких як ASP.NET, Ruby on Rails, Django та інших. За даними статистики веб-сайту BuiltWith.com, майже 8% веб-сайтів використовують фреймворки на основі MVC, з найбільш популярними з них є ASP.NET. Особливою перевагою використання MVC є його здатність до розширення та підтримки, що дозволяє забезпечити кращу підтримку функцій додатку та зменшити ризики при розробці нових функцій. Крім того, MVC забезпечує більш високу продуктивність, так як він дозволяє розробникам зосередитися на різних аспектах додатку та забезпечити їх оптимізацію.

Для розробки також можна використовувати інші програмні засоби, такі як:

- Apache Cassandra - розподілена база даних, яка дозволяє зберігати великі обсяги даних зі швидкістю та масштабованістю, що є важливим для сервісу соціальної мережі.
- Elasticsearch - пошукова система, яка дозволяє швидко і ефективно знаходити та індексувати великі обсяги даних, що допомагає поліпшити швидкість пошуку та аналізу даних у соціальній мережі.
- Redis - розподілена база даних, яка дозволяє зберігати дані в оперативній пам'яті, що забезпечує високу швидкість доступу до даних та можливість кешування даних для поліпшення продуктивності сервісу.
- RabbitMQ - програмний брокер повідомлень, який дозволяє передавати повідомлення між різними компонентами сервісу, що забезпечує більш ефективну та масштабовану комунікацію в сервісі соціальної мережі.
- Amazon Web Services або Google Cloud Platform - хмарні платформи, які дозволяють розгортати та масштабувати сервіс соціальної мережі, забезпечуючи високу доступність та швидкість роботи.

Ці програмні засоби можуть бути використані для покращення функціональності та продуктивності комунікативного онлайн-сервісу соціальної спільноти.

Користувацький інтерфейс є важливою частиною будь-якого програмного забезпечення, оскільки саме через нього користувачі взаємодіють з програмою. Розробка користувацького інтерфейсу може бути виконана з використанням різноманітних інструментів, таких як Windows Presentation Foundation (WPF), що є частиною платформи .NET.WPF надає розширені можливості для розробки графічного інтерфейсу та дозволяє використовувати різні елементи управління, такі як кнопки, тексти, зображення та інші. Також існують сторонні бібліотеки, наприклад, Xamarin.Forms, які дозволяють створювати мультиплатформові мобільні додатки з користувацьким інтерфейсом.

REST (Representational State Transfer) - архітектурний стиль для побудови додатків, що працюють у мережевому середовищі, в основі якого лежить принцип передачі даних за запитом-відповіддю. REST API - це інтерфейс, що забезпечує доступ до ресурсів в мережевому середовищі за допомогою HTTP-протоколу, а також простоту та ефективність комунікації між різними додатками в Інтернеті, зокрема, між клієнтськими та серверними додатками. Для передачі даних REST API використовує HTTP-методи, такі як GET, POST, PUT, DELETE, що дозволяє взаємодіяти з ресурсами, що зберігаються на сервері.

У своїй роботі програмісти використовують цей інтерфейс для створення додатків, що працюють в мережевому середовищі, забезпечуючи їх користувачам зручний та швидкий доступ до необхідної інформації, також він дозволяє використовувати різноманітні мови програмування та платформи, що робить його універсальним інструментом для створення додатків різного рівня складності.

База даних - це один з найважливіших компонентів будь-якого онлайн-сервісу соціальної спільноти, оскільки вона забезпечує зберігання та організацію великої кількості даних, що включають профілі користувачів, повідомлення, фотографії, відео, коментарі тощо.

Для розробки комунікативного онлайн-сервісу соціальної спільноти, можна використовувати різні типи баз даних:

- MySQL - система управління реляційними базами даних, яка дозволяє зберігати, організовувати та керувати великими обсягами даних.
- NoSQL - це підхід до управління даними, що відрізняється від традиційних реляційних баз даних. У системах NoSQL дані зберігаються у вигляді документів, графів, ключ-значення або колонок, залежно від обраної моделі даних.
- Microsoft SQL Server (MS SQL Server або просто SQL Server) - це система управління базами даних, розроблена компанією Microsoft. Вона використовує мову запитів Transact-SQL (T-SQL) для взаємодії з базою даних. MS SQL Server має багато функціональних можливостей, таких як підтримка транзакцій, реплікація даних, аналітика та багато іншого.
- MongoDB - це документо-орієнтована база даних, яка зберігає дані у вигляді документів у форматі BSON (Binary JSON). Вона розроблена з орієнтацією на обробку великих обсягів даних та високі швидкості операцій з ними. MongoDB підтримує гнучкий формат даних, дозволяючи зберігати дані без встановленої схеми та змінювати її в процесі роботи з базою даних.

При проектуванні бази даних для комунікативного онлайн-сервісу потрібно враховувати такі фактори, як швидкість доступу до даних, масштабованість та безпеку. Наприклад, для забезпечення швидкого доступу до даних, можна використовувати кешування даних на рівні додатку або бази даних. Для забезпечення безпеки даних, можна використовувати різні методи шифрування даних та захисту від несанкціонованого доступу.

Також варто враховувати те, що онлайн-сервіс соціальної спільноти має бути доступним для користувачів з різних країн та мов і має підтримувати міжнародну локалізацію. Це означає, що інтерфейс користувача та контент на сайті повинні бути перекладені на мови різних країн. Для забезпечення міжнародної локалізації слід використовувати спеціальні

засоби, такі як міжнародні фреймворки локалізації, які дозволяють перекладати контент на різні мови та налаштовувати вигляд інтерфейсу користувача в залежності від мови.

Крім того, з метою забезпечення міжнародної доступності та швидкості роботи сайту, можна використовувати розподілені системи зберігання даних та міжнародні CDN (Content Delivery Network), що дозволяють ефективно розподіляти контент по всьому світу та зменшувати час завантаження сторінок сайту для користувачів з різних країн.

Застосування бази даних дозволяє зберігати значну кількість даних про користувачів та їх взаємодії, що дозволяє аналізувати ці дані та отримувати корисну інформацію щодо популярності сервісу, поведінки користувачів та інших важливих аспектів. База даних є необхідним компонентом будь-якого сервісу соціальної спільноти та важливою складовою успішної розробки імітатора соціальної спільноти.

Портування (англ. porting) — це процес перенесення програмного забезпечення з одного середовища на інше. В залежності від того, на яких платформах планується акористовувати свій онлайн-сервіс соціальної спільноти, можна розглянути портування його на Android та iOS.

Для перенесення на мобільні платформи можна використовувати інструменти, такі як Xamarin або React Native:

Xamarin - це платформа для розробки мобільних додатків, яка дозволяє розробляти кросплатформні додатки для iOS, Android і Windows Phone за допомогою мови програмування C#. За даними різних досліджень, популярність Xamarin зростає з року в рік, оскільки вона дозволяє зменшити час розробки і підтримки додатків, забезпечуючи високу якість і функціональність. Згідно з даними Stack Overflow Developer Survey за 2021 рік, Xamarin займає друге місце серед платформ для розробки мобільних додатків після React Native. Також, за даними Microsoft, більше 2 мільйонів розробників використовують Xamarin для розробки мобільних додатків. Основні переваги використання Xamarin полягають у тому, що розробники можуть використовувати мову C# для створення кросплатформних додатків, що дозволяє зменшити час розробки і підтримки. Крім того, Xamarin надає можливість використовувати переваги нативного коду для кожної платформи, що забезпечує оптимальну продуктивність додатку. Також важливо зазначити, що Xamarin має велику спільноту розробників та підтримку від Microsoft, що забезпечує регулярне оновлення платформи та надання різноманітних інструментів для розробників.

React Native - це відкрите програмне забезпечення для розробки мобільних додатків, що базується на ReactJS - бібліотеці JavaScript для створення інтерфейсів користувача. За допомогою нього розробники можуть створювати мобільні додатки для iOS та Android з використанням одного коду на JavaScript. Дане програмне забезпечення набуло значної популярності серед розробників мобільних додатків. За даними State of JS 2020, React Native стала другою за популярністю бібліотекою для розробки мобільних додатків після Flutter. У 2020 році вона була використана понад 42% респондентів дослідження для створення мобільних додатків.

React Native є популярним вибором для розробки мобільних додатків у випадку, коли потрібна швидкість розробки та висока продуктивність додатків. Програма надає можливість швидко створювати прототипи мобільних додатків та дозволяє ефективно використовувати переносимий код між платформами. Більшість розробників знаходять в ній легким для вивчення та швидким у розробці. Однією з переваг React Native є підтримка гарячого перезавантаження, що дозволяє розробникам швидко бачити зміни, які вони роблять в коді, на мобільних пристроях без необхідності перезавантаження додатку.

Створення комунікативних онлайн-сервісів соціальної спільноти - це завдання, яке потребує високої кваліфікації розробників. Оскільки такі сервіси дозволяють взаємодіяти з користувачами в режимі реального часу та обмінюватися великим обсягом даних, тестування такого програмного забезпечення є невід'ємною складовою процесу його розробки.

Аналіз проекту є необхідним етапом розробки будь-якого програмного забезпечення, оскільки воно дозволяє виявити помилки та недоліки в роботі програми та виправити їх до випуску продукту в експлуатацію.

У разі комунікативних онлайн-сервісів соціальної спільноти, тестування включає проведення тестів на функціональність, відповідність стандартам безпеки, тестування навантаження та інших параметрів, що впливають на якість та ефективність роботи сервісу. Такі тести дозволяють виявити проблеми, що виникають під час використання сервісу реальними користувачами та виправити їх до випуску продукту в експлуатацію.

Кількість користувачів та обсяги даних, що обробляються комунікативними онлайн-сервісами соціальної спільноти, можуть бути величезними. Це ставить перед розробниками завдання забезпечити не тільки надійну роботу сервісу, але й забезпечити безпеку та захист приватності користувачів. На жаль, навіть найкращі комунікативні сервіси не є ідеальними, тому тестування стає невід'ємною складовою в процесі розробки таких сервісів.

Одним з основних видів тестування є функціональне тестування, яке включає у себе перевірку функцій та можливостей сервісу. Наприклад, тестування може включати перевірку можливості додавання друзів, обмін повідомленнями, відправку та отримання файлів тощо. Важливо перевірити, що всі ці функції працюють правильно та коректно взаємодіють з іншими функціями сервісу.

Окрім функціонального тестування, важливим є також тестування на масштаб. Це означає, що необхідно перевірити, як сервіс працює при великому навантаженні та великій кількості запитів одночасно. Тестування на масштаб може допомогти виявити проблеми з продуктивністю та оптимізувати роботу сервісу.

Також важливим є тестування безпеки. Комунікативні онлайн-сервіси соціальної спільноти містять велику кількість особистих даних користувачів, тому захист цих даних є надзвичайно важливим. Тестування безпеки може допомогти виявити проблеми з захистом даних, такі як уразливості в мережевих протоколах, управлінням ідентифікацією та авторизацією, та інші проблеми, пов'язані з безпекою. Важливо проводити тестування на різних етапах розробки сервісу, включаючи тестування на ранніх етапах, коли сервіс розробляється, а також після випуску на продакшн, коли користувачі починають активно використовувати сервіс.

Тестування програмного забезпечення також може допомогти виявити проблеми з функціональністю сервісу, такі як помилки в роботі функцій, неправильні дані, невірна поведінка та інші проблеми, які можуть призвести до негативного впливу на користувачів та їхній досвід використання сервісу.

Для забезпечення якості тестування ПЗ, необхідно використовувати різні види тестів, такі як модульні тести, інтеграційні тести, тести на прийняття та інші. Крім того, необхідно використовувати автоматизоване тестування, яке може забезпечити більшу швидкість та ефективність тестування, а також підвищити його точність та надійність.

У світі, де цифрові технології стали неодмінною складовою сучасного життя, комунікативні онлайн-сервіси соціальної спільноти відіграють ключову роль у спілкуванні, обміні інформацією та побудові зв'язків. Цей розділ підбиває короткі висновки стосовно комунікативних онлайн-сервісів соціальної спільноти.

Комунікативні онлайн-сервіси соціальної спільноти забезпечують учасникам можливість обміну ідеями, думками та враженнями без обмежень простору та часу. Це створює сприятливе середовище для віртуального спілкування, побудови особистих та професійних відносин, а також сприяє розширенню кругу спільноти.

Комунікативні онлайн-сервіси соціальної спільноти включають в себе багато функціональних можливостей, таких як чати, відеодзвінки, спільні новини, групові дискусії тощо. Це дозволяє користувачам обирати способи взаємодії, які найкраще відповідають їхнім потребам та вподобанням.

Незважаючи на всі переваги, комунікативні онлайн-сервіси соціальної спільноти також стикаються з викликами, пов'язаними зі збереженням приватності та безпекою даних

користувачів. Необхідно розробляти ефективні механізми захисту та забезпечення конфіденційності даних.

Висновки. У цій статті розглянута мова C#, яка є доцільною для розробки комунікативного онлайн-сервісу соціальної спільноти з великою кількістю користувачів та потребою у високій продуктивності, ефективності та модульності, крім того проаналізовані різні програмні платформи, що використовуються для створення комунікативних онлайн-сервісів. Також було вказано, що для ефективного використання необхідні відповідні програмні рішення, які дозволяють забезпечити якість та безпеку обміну даними. Важливо проводити тестування на різних етапах розробки сервісу, включаючи тестування безпеки, щоб запобігти можливим проблемам. Також були розглянуті різні типи баз даних, такі як реляційні та нереляційні, та їх використання для зберігання та обробки даних, що використовуються в комунікативних онлайн-сервісах.

Комунікативні онлайн-сервіси соціальної спільноти є потужним інструментом для побудови зв'язків, обміну інформацією та взаємодії у віртуальному просторі. Їхній успіх полягає у здатності надати різноманітні можливості взаємодії, зберігаючи при цьому захист і приватність користувачів. Незважаючи на виклики, з якими вони стикаються, ці сервіси впливають на спосіб, яким ми спілкуємося та співпрацюємо, розширюючи границі віртуальної соціальної спільноти.

В цілому, створення комунікативного онлайн-сервісу соціальної спільноти є складним процесом, який вимагає від розробників високої кваліфікації та уваги до деталей.

Список використаних джерел

1. Microsoft «Документація по ASP.NET» \\ Режим доступу: https://learn.microsoft.com/ru-ru/aspnet/core/?view=aspnetcore-7.0
2. Microsoft «Початок роботи з ASP.NET MVC 5 \\ Режим доступу: https://learn.microsoft.com/ru-ru/aspnet/mvc/overview/getting-started/introduction/getting-started
3. Ендрю Троелсен та Філіп Джепікс «Мова програмування C# 7 і платформи .NET і .NET Core»
4. Microsoft «Документація по C#» \\ Режим доступу: https://learn.microsoft.com/ru-ru/dotnet/csharp/
5. MySQL «MySQL Documentation» \\ Режим доступу: https://dev.mysql.com/doc/
6. Microsoft «Документація по Xamarin» \\ Режим доступу: https://learn.microsoft.com/ru-ru/xamarin/
7. Н.С. Гайдук «Розробка соціальної мережі для бібліотек на основі .NET технологій» \\ Режим доступу: https://elartu.tntu.edu.ua/handle/lib/30701
8. М.Яковенко, А.Охрименко, С.Кузніченко «Програмна реалізація агрегатора соціальних мереж» \\ Режим доступу: http://mdu.edu.ua/wp-content/uploads/gmit7-16.pdf
9. React Native «Introduction» \\ Режим доступу: https://reactnative.dev/docs/getting-started
10. «Керівництво по програмуванню для Xamarin Forms» \\ Режим доступу: https://metanit.com/sharp/xamarin/
11. «Welcome to Apache Cassandra`s documentation!» \\ Режим доступу: https://cassandra.apache.org/doc/latest/
12. «Керівництво по Elasticsearch» \\ Режим доступу: https://coderlessons.com/tutorials/noveishie-tekhnologii/izuchite-uprugii-poisk/elasticsearch-kratkoe-rukovodstvo

Робота виконана під науковим курівництвом кандидата технічник наук, доцента кафедри інженерії програмного забезпечення та кібербезпеки
РЗАЄВОЇ С.Л.

СПОСОБИ ПРОТИДІЇ ВПЛИВУ СПАМУ НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

ЯЦИК М., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто поняття спаму та його види, оскільки різні види спаму вимагають різних підходів до їх боротьби. технічні, математичні та правові методи боротьби зі спамом. Описано принципи роботи кожного з цих методів, їх переваги та недоліки. Зазначено принципи та переваги застосування математичних методів боротьби зі спамом, зокрема, методів машинного навчання та статистичного аналізу. Висвітлено актуальність проблеми боротьби зі спамом, ризики, що він несе для інформаційно-комунікаційних систем, та постійно зростаюча складність боротьби з цією загрозою.

The article discusses the concept of spam and its types, as different types of spam require different approaches to combat them. It covers technical, mathematical, and legal methods for fighting spam. The principles of operation, advantages, and disadvantages of each of these methods are described. The article highlights the relevance of the problem of spam, the risks it poses to information and communication systems, and the constantly increasing complexity of combating this threat. The principles and advantages of using mathematical methods for combating spam, including machine learning and statistical analysis methods, are emphasized.

Актуальність. Всебічна інформатизація суспільства, збільшення обсягів створюваної, одержуваної і накопичуваної інформації ведуть до зростання актуальності питань, пов'язаних з поширенням спаму, його впливу на інформаційне середовище підприємств і фізичних осіб, ефективність їх діяльності; рівень інформаційної безпеки. Спам є серйозною загрозою для інформаційно-комунікаційних систем, оскільки він може призвести до перевантаження систем, зменшення продуктивності, витрат на зберігання даних та інших негативних наслідків. Крім того, спам може бути використаний зловмисниками для здійснення фішингових атак та інших видів кіберзлочинності.

У зв'язку з цим, розробка та вдосконалення методів боротьби зі спамом є одним з найважливіших завдань в галузі кібербезпеки. Компанії, що надають послуги електронної пошти та інші ІКС-провайдери, активно використовують спеціальні програми та алгоритми для виявлення та блокування спаму. Однак, зловмисники постійно розробляють нові способи обхіду захисту від спаму, що вимагає постійного вдосконалення методів боротьби з ним. Крім того, виникають нові види спаму, такі як соціальний спам, що використовується для поширення недостовірної інформації в соціальних мережах.

Актуальність способів протидії впливу спаму на інформаційно-комунікаційні системи полягає в тому, що спам є однією з найбільш поширених проблем в Інтернеті, яка може негативно вплинути на роботу інформаційно-комунікаційних систем, заважаючи користувачам отримувати та обробляти корисну інформацію. У зв'язку з цим, розробка та впровадження ефективних методів боротьби зі спамом є важливим завданням для підтримки безпеки та ефективності функціонування ІКС. Отже, актуальність способів протидії впливу спаму на ІКС буде залишатися високою в майбутньому, і провайдери інформаційно-комунікаційних систем та кібербезпеки мають постійно вдосконалювати свої методи боротьби зі спамом.

Метою статті є дослідження різних способів протидії впливу спаму на інформаційно-комунікаційні системи.

Об'єктом дослідження є процес боротьби зі спамом в інформаційно-комунікаційних системах, який включає в себе різноманітні технології та методи, спрямовані на захист

користувачів та інформаційно-комунікаційні системи від негативних наслідків, які можуть виникнути через спам.

Предмет дослідження – інформаційно-комунікаційні системи, які можуть бути піддані впливу спаму, а також технології та методи, які використовуються для захисту інформаційно-комунікаційних системах від спаму.

Аналіз попередніх досліджень. Тема протидії впливу спаму на інформаційно-комунікаційні системи є предметом досліджень багатьох українських та закордонних вчених. Зокрема, в Україні в цій галузі працюють науковці Національної академії наук України, Національного технічного університету України «Київський політехнічний інститут», Національного університету «Львівська політехніка» та інших вітчизняних університетів.

У світі науковими центрами, які досліджують протидію спаму на інформаційно-комунікаційні системи, є, зокрема, Інститут інформаційної безпеки в Університеті Флориди, Інститут комп'ютерних наук Массачусетського технологічного інституту, Лабораторія комп'ютерних наук корпорації Microsoft, Лабораторія з безпеки Інтернету у Вірджинському університеті та багато інших. Результати досліджень вказують на те, що застосування різноманітних технологій та методів захисту ІКС від спаму є ефективним. Наприклад, застосування фільтрів спаму здатне знизити кількість небажаних повідомлень до 99,9%. В той же час, існують нові технології штучного інтелекту, які забезпечують ще більш ефективний захист від спаму.

Отже, дослідження українських та закордонних вчених є важливим кроком у розробці нових технологій та методів протидії впливу спаму на ІКС, які забезпечують високу якість і безпеку роботи цих систем.

Виклад основного матеріалу. У сучасному світі, коли інформація стала найважливішим ресурсом, проблема спаму стала надзвичайно актуальною. Спам може мати шкідливий вплив на інформаційно-комунікаційні системи (ІКС) через займання мережевого простору, витрати ресурсів та загрозу для безпеки. Спам – це небажані повідомлення, які надсилаються без згоди отримувача, зазвичай з комерційною або шахрайською метою. Спам може завдати значних шкідливих наслідків для інформаційно-комунікаційних систем, включаючи перевантаження мережі, складність виявлення легітимних повідомлень та ризики відкриття вірусів або інших шкідливих програм [1]. Надходження спаму на поштові скриньки та інші комунікаційні канали може призвести до наступних наслідків:

1. Вірусні атаки: спамові повідомлення можуть містити віруси та інші шкідливі програми, що можуть пошкодити систему та зламати безпеку інформації. Віруси можуть поширюватися через електронні повідомлення та встановлюватися на комп'ютери користувачів, що відкриють спамове повідомлення.
2. Фішингові атаки: спамові повідомлення можуть містити фішингові ланки або приховані запити на введення особистих даних, таких як паролі або номери банківських карток. Фішингові атаки можуть використовуватися для викрадення особистої інформації користувачів та зламу їхніх акаунтів.
3. Соціальний інжиніринг: спамові повідомлення можуть містити запити на переказ грошей або інші шахрайські схеми, які можуть бути використані для шахрайства користувачів. Злочинці можуть використовувати соціальний інжиніринг, щоб переконати користувачів у необхідності здійснити переказ коштів або надати особисту інформацію.
4. Завантаження небезпечного контенту: спамові повідомлення можуть містити посилання на небезпечний контент, такий як порнографія або насильство. Клікнувши на посилання, користувач може завантажити шкідливий вміст на свій комп'ютер.
5. Перевантаження системи є ще однією серйозною загрозою, пов'язаною зі спамом. Частість спамових повідомлень може відправлятися великою кількістю користувачів одночасно, що може призвести до перевантаження інформаційної системи. Якщо спам-атака великої масштабності, то вона може спричинити перевантаження серверів, що може призвести до тимчасового або повного відключення веб-сайту або інших інформаційних систем.

Протидія впливу спаму на інформаційно-комунікаційні системи (ІКС) − це важлива задача, яка полягає в тому, щоб запобігти надходженню небажаних повідомлень на електронну пошту, соціальні мережі та інші інтернет-сервіси [1].

Основні методи протидії спаму на сьогоднішній день включають в себе:

- Встановлення антивірусного програмного забезпечення, яке може виявляти та блокувати спам-повідомлення, фішингові листи, віруси та інші загрози для безпеки користувачів. Також антивірусні програми можуть бути налаштовані на автоматичне видалення спаму зі скриньки електронної пошти.
- Встановлення спеціальних програм (антиспам-фільтри), які перевіряють вхідну пошту на наявність спаму та блокують його. Фільтри спаму − це програми, які автоматично відсікають небажані повідомлення на підставі певних критеріїв. Вони можуть бути настроєні на блокування спаму за ключовими словами, IP-адресами, доменними іменами та іншими параметрами. Фільтри спаму зазвичай використовуються в електронній пошті, але їх також можна застосувати до інших ІКС, таких як соціальні мережі та месенджери.
- Використання CAPTCHA. Це системи перевірки, що вимагають від користувача виконати певне завдання, щоб довести, що він є людиною, а не роботом. CAPTCHA може бути використана для захисту від автоматизованих спам-ботів, які розсилають великі обсяги спаму.
- Блокування IP-адрес використовуються для блокування повідомлень від спамерів з певних IP-адрес. Електронний поштовий сервер може перевіряти IP-адреси відправників та порівнювати їх з блеклістами, щоб блокувати повідомлення від відомих спамерів.
- Використання криптографічних методів для підтвердження відправника листа і перевірки на його автентичність.
- Системи автентифікації можуть бути використані для визначення того, що пошта, яка надходить до поштової скриньки користувача, є легітимною. Найпоширенішою системою автентифікації є SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting and Conformance). Ці системи дозволяють перевірити, що пошта була надіслана відправником, який має право відправляти листи від імені даного домену.
- Встановлення обмежень на кількість листів, які можна відправити з певної IP-адреси за певний час.
- Навчання користувачів правилам безпеки в Інтернеті. Користувачі повинні бути обізнані з тим, як розпізнавати спам, не відкривати невідомі повідомлення та не відповідати на них.
- Обмеження спаму: деякі веб-сайти та соціальні мережі використовують методи обмеження спаму, наприклад, обмеження частоти відправки повідомлень, обмеження кількості отримувачів тощо.
- Боротьба з ботнетами. Ботнети − мережа комп'ютерів, які контролюються зловмисниками, зазвичай з метою злочинної діяльності, такої як розсилання спаму, здійснення DDoS-атак, крадіжка конфіденційних даних та іншого шкідливого впливу на користувачів Інтернету. Один з найбільш ефективних методів − виявлення та відключення злочинних серверів, які контролюють ботнет. Це можна зробити шляхом спостереження за трафіком, що пересилається між злочинним сервером та інфікованими комп'ютерами, та ідентифікації вузлів мережі, які приймають та відправляють цей трафік. Після виявлення злочинного сервера, його можна відключити від Інтернету.

Протидія впливу спаму на інформаційно-комунікаційні системи включає в себе різні заходи, які повинні бути реалізовані на кількох рівнях: технічному, правовому та освітньому.

На технічному рівні протидія спаму може включати в себе такі заходи, як блокування IP-адрес, які відомі як джерело спаму, використання спеціальних програм для виявлення та

блокування спаму, та обмеження обсягу відправлення листів на конкретний домен. Також можуть використовуватися методи евристичного аналізу, такі як аналіз заголовків та тексту повідомлення, для виявлення спаму та блокування його вхідного потоку (Рис. 1). Наприклад, відповідні програми можуть розпізнавати та відфільтровувати спамові повідомлення, а також визначати IP-адреси, з яких вони надходять. Крім того, використання антивірусних програм та систем захисту може допомогти уникнути проблем з безпекою при отриманні спаму.

Рис. 1. Технічні методи боротьби із спамом

На правовому рівні протидія спаму може включати в себе прийняття законодавчих норм, що обмежують розсилку спаму. Наприклад, в Україні такі заходи регулюються Законом про електронні комунікації, який встановлює правила для відправників електронних повідомлень та визначає відповідальність за незаконну розсилку спаму.

Освітні заходи можуть допомогти в боротьбі зі спамом, допомагаючи користувачам розуміти, як розпізнавати спам та які дії потрібно вжити, щоб захистити себе від спаму. Освітні кампанії можуть проводитися на різних рівнях, включаючи школи, коледжі, університети та в мас-медіа.

Математичні технології боротьби зі спамом полягають у використанні різних математичних методів та алгоритмів для виявлення та фільтрації спамових повідомлень. Основні математичних технологій, які використовуються для боротьби зі спамом:

1. Байєсівський фільтр − математичний алгоритм, який використовується для визначення ймовірності того, що повідомлення є спамом або не спамом. Байєсівський фільтр працює на основі аналізу вмісту повідомлень та статистичних даних про спам та не спам. Алгоритм вивчає, які слова та фрази в спамових повідомленнях є найбільш ймовірними, а потім використовує цю інформацію для виявлення спаму. Байесівський фільтр спаму є досить ефективним методом, оскільки він може навчитися розпізнавати нові форми спаму [2, 3].

Байєсівський фільтр є одним з найпоширеніших методів боротьби зі спамом. Байєсівський фільтр − це математичний алгоритм, який може бути використаний для боротьби зі спамом. Він оснований на теорії ймовірності та використовується для класифікації повідомлень на спам і не-спам. Робота Байєсівського фільтра полягає у створенні моделі ймовірності, яка використовується для класифікації повідомлень. Напочатку роботи алгоритму необхідно побудувати базову модель, використовуючи набір тренувальних даних. Тренувальні дані містять набір повідомлень, які вже були класифіковані як спам або не-спам. Байєсівський фільтр аналізує ці повідомлення та знаходить зв'язок між словами, які з'являються в спамі та не-спамі. На основі цього алгоритм створює базову модель, яка допоможе в подальшій класифікації повідомлень. Кожне нове повідомлення відображується у вигляді набору слів та використовується для обчислення ймовірності, що це повідомлення є

спамом. Для цього використовується формула Байєса, яка враховує ймовірності того, що слова з'являються в спамі та не-спамі.

Одним з головних переваг Байєсівського фільтра є те, що він вимагає досить мало обчислень, тому є досить швидким та ефективним. Крім того, Байєсівський фільтр може навчатися на нових данних та оновлювати свою статистику, що дозволяє йому бути ефективним і в актуальній ситуації.

2. Лінійний дискримінантний аналіз (ЛДА) – метод, який використовується для відокремлення спамових повідомлень від легітимних електронних листів на основі визначених характеристик. Алгоритм використовує статистичний аналіз для визначення, які змінні є найбільш корисними для відокремлення спаму від легітимних повідомлень [2, 4].

Лінійний дискримінантний аналіз (ЛДА) є методом машинного навчання, який може бути використаний для боротьби зі спамом. В контексті боротьби зі спамом, ЛДА може бути використаний для класифікації повідомлень на спам і не-спам на основі набору ознак, таких як слова, фрази, символи і т.д. ЛДА працює шляхом знаходження оптимальної границі розділення між спамом і не-спамом у просторі ознак. В результаті, ЛДА може дати високу точність при класифікації повідомлень на спам і не-спам, особливо якщо використовується комплексна система класифікації, що включає в себе багато ознак та алгоритмів. Одним з головних переваг ЛДА є те, що він працює швидко з великими наборами даних, а також він є легким у використанні та розумінні. Крім того, ЛДА може працювати з даними високої розмірності. Однак, ЛДА також має свої обмеження. Наприклад, він може бути менш ефективним у випадках, коли вхідні дані мають складну структуру або коли вони не можуть бути легко розділені границею. Загалом, ЛДА може бути ефективним методом для боротьби зі спамом, якщо він використовується в комплексі з іншими методами, такими як фільтри на основі правил, евристичні методи та інші.

3. Метод опорних векторів (SVM) − метод машинного навчання, який використовується для розпізнавання спамових повідомлень. Алгоритм використовується для виявлення лінійних та не лінійних залежностей між вхідними характеристиками повідомлень та їх класифікацією як спаму або легітимних повідомлень [2].

У контексті боротьби зі спамом, SVM може бути використаний для класифікації повідомлень на спам і не-спам на основі ряду ознак (features), таких як наявність певних слів, фраз, символів тощо. SVM навчається розпізнавати спамові повідомлення на основі прикладів, що містять як спам, так і не спам. В результаті навчання SVM будує математичну модель, яка може передбачити, чи є нове повідомлення спамом чи ні. SVM може вивчити границю прийняття рішень, яка дозволяє розділити вхідні дані на два класи: спам і не-спам. Ця границя може бути дуже ефективною, особливо якщо використовувати комплексну систему класифікації, яка включає в себе багато ознак та алгоритмів. Одним з найбільших переваг SVM є те, що він працює дуже швидко, навіть з великими наборами даних. Також, SVM є дуже ефективним для роботи з даними високої розмірності. Однак, SVM також має свої обмеження. Він може мати проблеми з використанням даних, які не можуть бути легко розділені границею, або які мають складну структуру. Крім того, SVM може потребувати попередньої підготовки даних, такої як видалення зайвої інформації або перетворення даних в інший формат.

Загалом, SVM може бути ефективним методом для боротьби зі спамом, якщо він використовується в комплексі з іншими методами, такими як фільтри на основі правил, евристичні методи та інші.

4. Співставлення хеш-сум − метод, який використовується для порівняння хеш-сум спамових повідомлень зі списком відомих спамових повідомлень. Хеш-сума − це математичне значення, яке використовується для ідентифікації повідомлення. Якщо хеш-сума спамового повідомлення співпадає з хеш-сумою зі списку відомих спамових повідомлень, то повідомлення відхиляється [2, 4].

Співставлення хеш-сум (або хешування) є одним з методів боротьби зі спамом. Цей метод полягає в тому, щоб створити унікальну цифрову підпис (хеш-суму) для кожного повідомлення і порівняти його з відомими хеш-сумами відомих спамових повідомлень. Хеш-сума − це невелика послідовність цифр, створена з текстового повідомлення за допомогою функції хешування. Кожне повідомлення має свою власну унікальну хеш-суму, яка може бути використана для ідентифікації повідомлення. Якщо хеш-сума вхідного повідомлення співпадає з хеш-сумою, що відома як спам, то повідомлення вважається спамом і може бути відкинуте або помічене як спам. Цей метод може бути ефективним для боротьби з відомими типами спаму, але він може бути легко пропущений спамерами, які використовують нові методи або змінюють вміст повідомлень, щоб уникнути виявлення. Крім того, співставлення хеш-сум вимагає збереження бази даних відомих хеш-сум, що може бути дуже великим завданням при великій кількості спаму. Тому цей метод може бути дорогим у плані зберігання і обробки даних. У загальному, хеш-суми можуть бути використані як один з елементів комплексної системи боротьби зі спамом, яка включає в себе також інші методи, такі як фільтри на основі правил, машинне навчання, евристичні методи та інші [1].

5. Машинне навчання − метод, який використовується для розпізнавання спаму на основі аналізу великої кількості даних. За допомогою машинного навчання можна навчити комп'ютер розпізнавати спамові повідомлення на основі визначених характеристик, таких як адреса відправника, вміст повідомлення та інші параметри.

Інший підхід до машинного навчання для боротьби зі спамом - це використання навчальних алгоритмів класифікації, таких як метод опорних векторів (SVM) або дерева рішень. Ці алгоритми навчаються на великому наборі даних, які включають спамові та неспамові повідомлення, і використовують ці дані для класифікації нових повідомлень [1, 4].

У будь-якому випадку, машинне навчання є потужним інструментом для боротьби зі спамом. Однак, ефективність будь-якого методу машинного навчання залежить від якості вхідних даних та правильного налаштування алгоритмів.

6. Нейронні мережі є потужним інструментом для боротьби зі спамом, оскільки вони можуть навчатись на великій кількості даних і виявляти складні зв'язки між різними аспектами повідомлень [4].

Для цього використовуються різні типи нейронних мереж, такі як згорткові нейронні мережі, рекурентні нейронні мережі та мережі довготривалої пам'яті. Вони можуть використовуватись для розпізнавання спаму в текстових повідомленнях, зображеннях, аудіо та відео. Одним з найбільш ефективних методів використання нейронних мереж для боротьби зі спамом є глибоке навчання. Глибокі нейронні мережі, такі як рекурентні нейронні мережі (RNN) та згорткові нейронні мережі (CNN), можуть використовуватись для аналізу текстового повідомлення та визначення його категорії (спам або не спам). Наприклад, можна навчити рекурентну нейронну мережу на великому наборі даних, які містять текстові повідомлення, які вже були класифіковані як спам або не спам. Потім цю мережу можна застосувати до нових повідомлень, щоб визначити, чи вони є спамом чи ні. Іншим методом використання нейронних мереж для боротьби зі спамом є використання глибоких мереж для визначення аномалій в поведінці користувачів. Наприклад, можна використовувати глибокі нейронні мережі для аналізу великого обсягу даних, щоб виявити незвичайну активність на електронній пошті, таку як відправлення великої кількості повідомлень за короткий час. Згорткові нейронні мережі можуть бути використані для аналізу тексту повідомлень та виявлення ключових ознак, що вказують на його спамовий характер. Рекурентні нейронні мережі та мережі довготривалої пам'яті можуть використовуватись для аналізу поведінки користувачів та виявлення аномальної активності, що може вказувати на надсилання спаму [1, 3].

Однак, використання нейронних мереж для боротьби зі спамом також має свої виклики та обмеження. Наприклад, для успішного навчання нейронної мережі необхідно мати велику кількість даних, а також збалансований набір даних, що містить як спам, так і не-спам повідомлення. Також важливо враховувати, що спамери постійно розвивають свої методи, тому необхідно постійно оновлювати та покращувати систему захисту від спаму.

Більшість з існуючих програм для боротьби зі спамом фільтрують повідомлення, що приходять в поштову скриньку. Це зручно з двох причин. Поперше, за допомогою цих програм можна не перекачувати з сервера непотрібні листи. По-друге, вони дозволяють організувати сортування решти кореспонденції.

Існує безліч програмних рішень для виявлення спаму, які використовують різні методи і технології [4]. Деякі з найпопулярніших програмних рішень для виявлення спаму включають:

1. SpamAssassin – це безкоштовний відкритий програмний продукт, який використовує різні методики, такі як Байєсівський фільтр, співставлення хеш-сум, евристики та інші, для виявлення спаму в електронних листах. SpamAssassin може бути інтегрований з поштовими серверами та клієнтами електронної пошти.
2. Barracuda Spam Firewall – це апаратний або програмний продукт, який використовує різні методики, включаючи Байєсівський фільтр, для виявлення спаму в пошті та інших мережевих протоколах. Він також використовує технології машинного навчання, такі як нейронні мережі, для покращення точності виявлення спаму.
3. Symantec Messaging Gateway – це програмне рішення, яке використовує різні методики, включаючи Байєсівський фільтр та метод опорних векторів, для виявлення спаму в електронній пошті та інших мережевих протоколах. Symantec Messaging Gateway також використовує технології машинного навчання для покращення точності виявлення спаму та зменшення кількості неправильно класифікованих повідомлень.
4. MailWasher – це програмний продукт для перегляду та управління електронною поштою, який використовує різні методики, такі як Байєсівський фільтр та евристики, для виявлення спаму. Він може бути інтегрований з більшістю поштових клієнтів та серверів.

Ці програмні рішення дозволяють знизити кількість спаму, який надходить на поштові

Висновки. Усі методи боротьби зі спамом, які були розглянуті, мають свої переваги та недоліки, тому їх застосування залежить від конкретних умов та потреб користувачів. Наприклад, технічні методи (фільтри) є досить ефективними, але можуть блокувати корисні повідомлення. Математичні методи дають можливість визначити ймовірність того, що повідомлення є спамом, але не дають абсолютної гарантії. Дослідження українських та закордонних вчених показують, що проблема спаму не є локальною, а має глобальний характер. Крім того, недостатня увага до проблеми може призвести до серйозних наслідків для користувачів ІКТ, таких як вірусні атаки, крадіжки особистих даних та інші. Отже, вирішення проблеми спаму потребує комплексного підходу, який включає в себе не тільки технічні та математичні методи, але й підвищення свідомості користувачів щодо безпеки в ІКТ, а також співпрацю провайдерів та державних органів у сфері боротьби зі спамом.

Список використаних джерел

1. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. An evaluation of naïve bayesian anti-spam filtering techniques // Utah State University [Електронний ресурс] // Режим доступу: http://digital.cs.usu.edu/~erbacher/publications/Bayes-Vikas2.pdf (останнє звернення 22.03.2023р.).
3. Bayesian poisoning // Wikipedia The Free Encyclopedia [Електронний ресурс] // Режим доступу: https://en.wikipedia.org/wiki/Bayesian_poisoning (останнє звернення 22.03.2023р.)
4. Єрьоменко М. О. Аналіз існуючих програмних рішень для виявлення спаму // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVIII міжнародної науково-практичної конференції MicroCAD-2020. – Харків: НТУ «ХПІ» С. 118.

Робота виконана під науковим керівництвом старшого викладача
КОСТЮК Ю.В.