Державний торговельно-економічний університет
Кафедра інженерії програмного забезпечення
та кібербезпеки

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

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

Частина 1

Київ 2023

УДК 004.056.5
П 78

Програмування та захист інформації [Електронний ресурс] :
П 78 у 3 ч. Ч. 1 : зб. наук. ст. студентів / відп. ред. Т. О. Жирова. – Київ : Держ. торг.-екон. ун-т, 2023. – 211 с.

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

Матеріали подано в авторській редакції. Відповідальність за зміст статей несуть автори.

УДК 004.056.5

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

Видається за рекомендацією вченої ради факультету інформаційних технологій ДТЕУ
(протокол № 12 від 28.06.2023)

ЗМІСТ

ВСТУП

На глобальному рівні відбуваються значні трансформації в сфері обробки та захисту інформації, викликані інтенсивним зростанням 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.

Важливість інформаційних технологій створює нові виклики, пов'язані з кібербезпекою та захистом інформації. Оскільки інформаційні технології стають не просто складовою частиною, але й активним каталізатором розвитку інформаційного суспільства, з'являється необхідність у забезпеченні надійності та безпеки цих технологій та відповідної інформації.

Нині одним з пріоритетних завдань 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 для сучасного цифрового світу, де дані та системи стають вразливими перед кіберзагрозами.

На сьогодні актуальними є завдання 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. Слід зауважити, що кіберзагрози стають все більш поширеним явищем. Саме тому дедалі більше уваги приділяється підготовці фахівців у галузі кібербезпеки та захисту інформації, які мають 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 вирішення, включаючи складні ситуації. Крім того, вони відіграють важливу роль у підтримці сталого розвитку IT-компаній щодо якості процесів і результатів розробки програмного забезпечення.

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

Збірник наукових статей студентів, які здобувають освітній ступінь «магістр» за спеціальностями «Інженерія програмного забезпечення», «Кібербезпека та захист інформації», містить матеріали досліджень, отриманих під час виконання їхніх 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 artic – le 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).

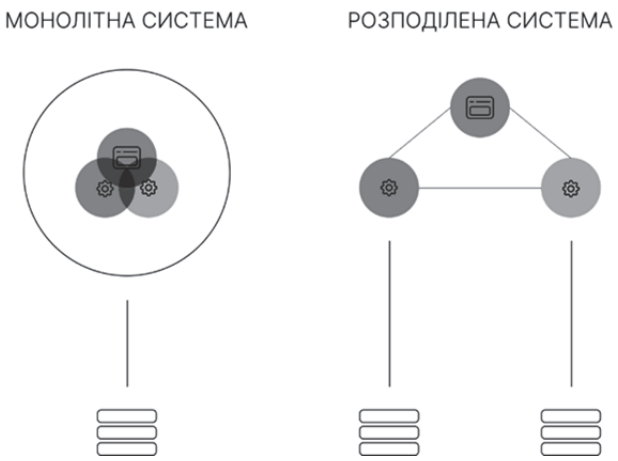


Рис. 1. Порівняння монолітної та розподіленої архітектури програмної системи

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).

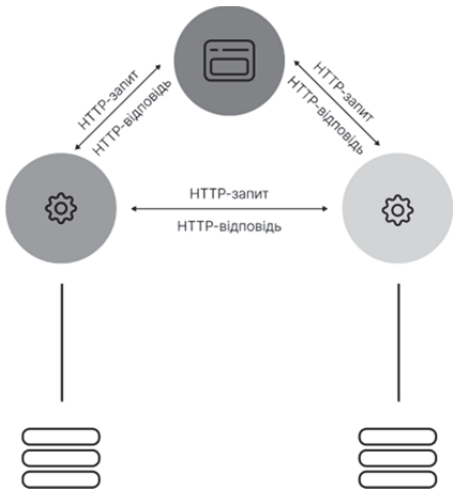


Рис. 2. Використання протоколу HTTP для комунікації в розподіленій системі

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 18.03.2023 р.).
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 «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:

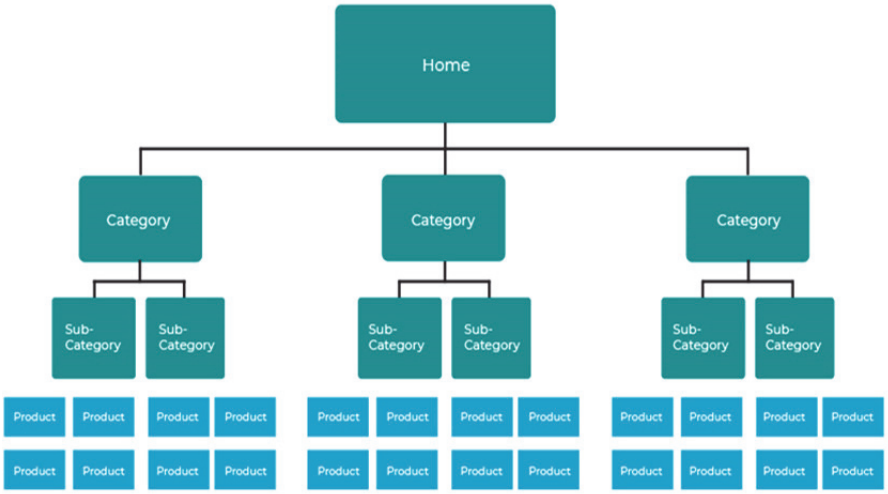


Рис. 1. Ефективна структура даних на сайті електронної комерції [3]

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

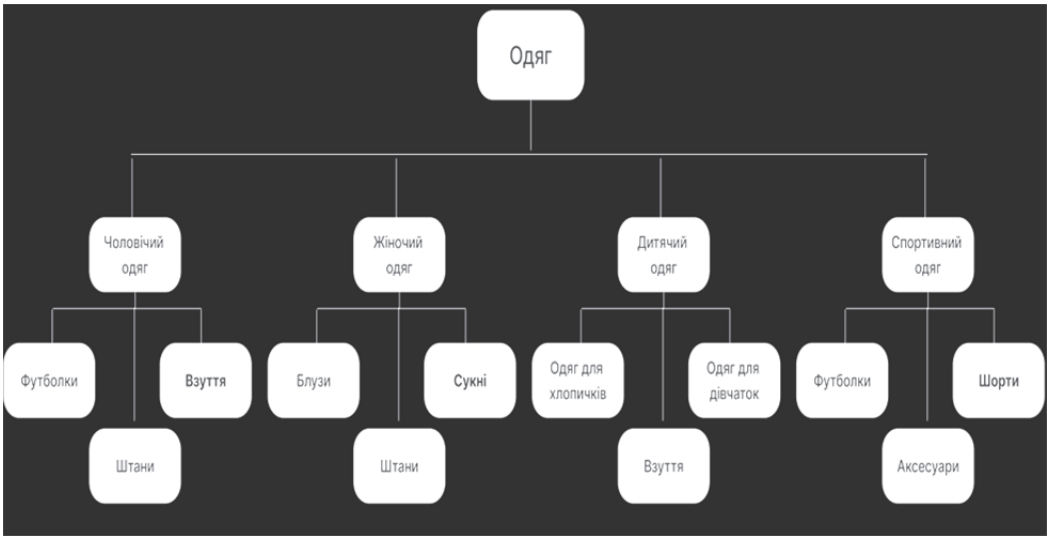


Рис. 2. Приклад ефективної структури даних на сайті магазину одягу

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.

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.

Рис. 1. Сфери використання мови Python

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 перейматочись 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.

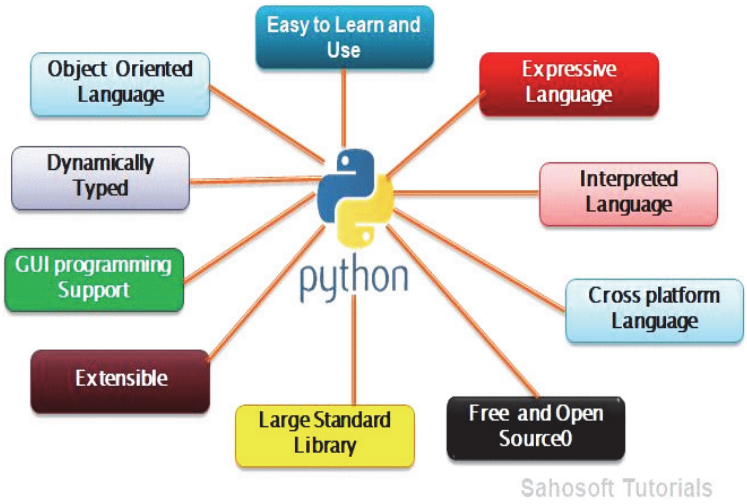


Рис. 2. Особливості мови програмування Python

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 канд. екон. наук, доцента
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].

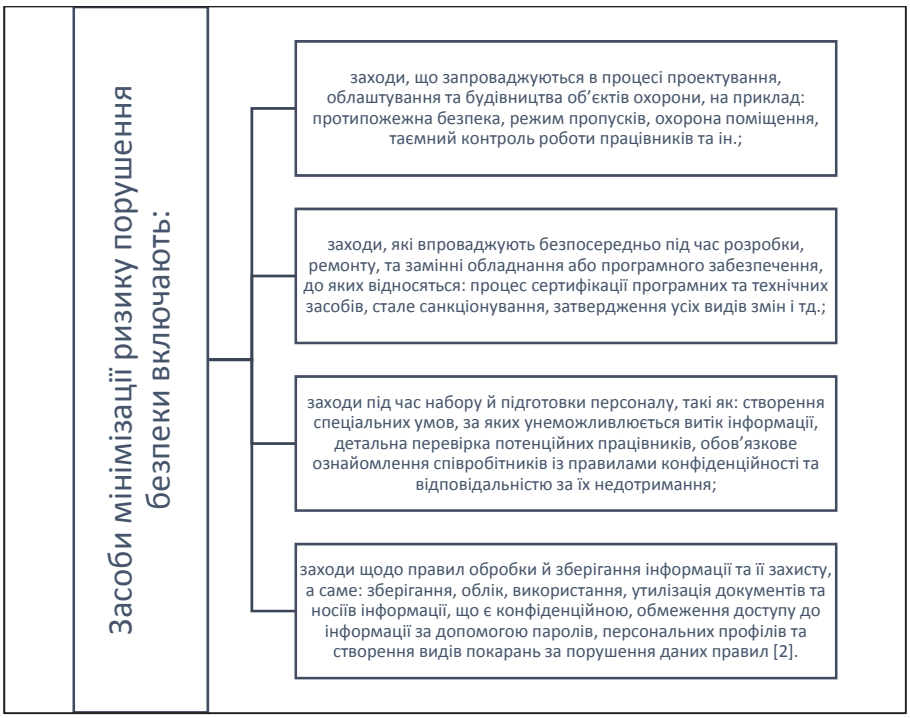


Рис. 1. Засоби мінімізації ризику порушення безпеки

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 старшого 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 вебплатформи 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:

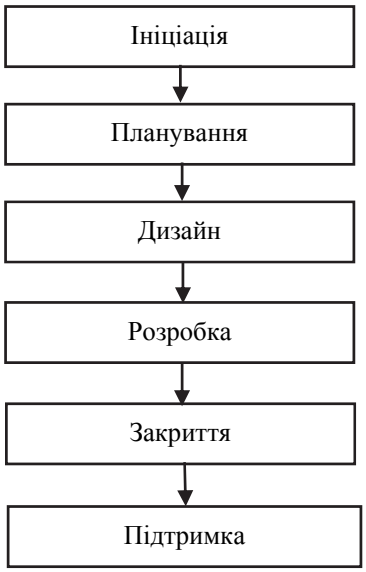


Рис. 1. Етапи впровадження доступності при створені проєкту

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 наративами 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%)

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».

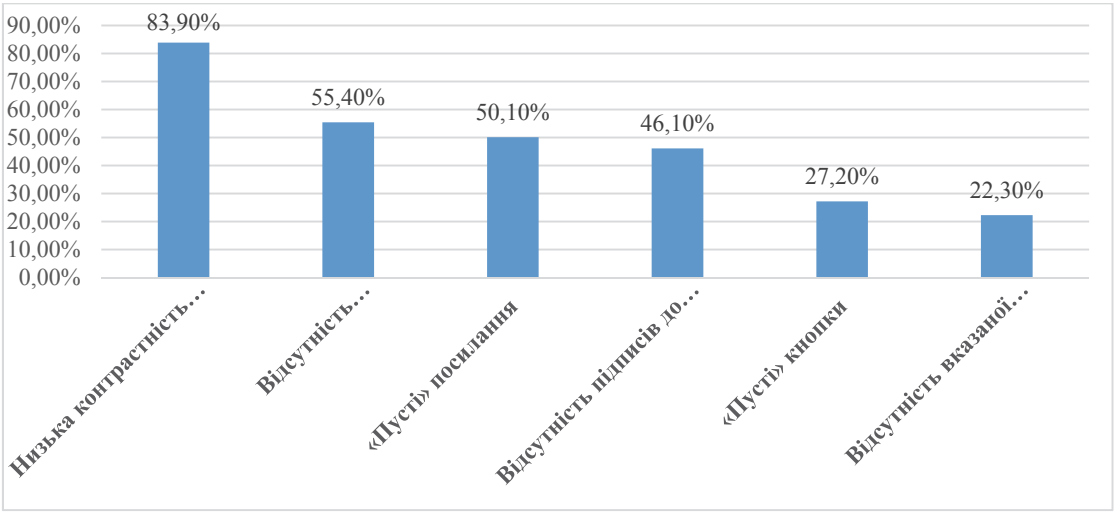


Рис. 2. Найчастіші невідповідності з нативами WCAG серед домашніх сторінок у 2022 р.

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 канд. пед. 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.

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

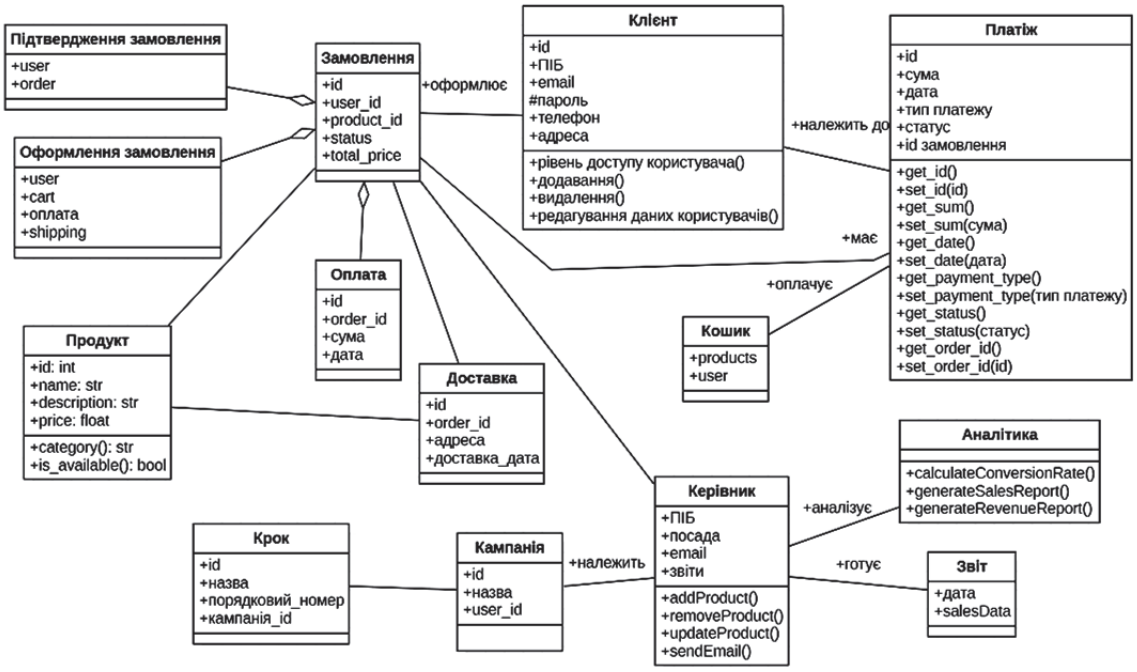


Рис. 1. Модель класів програмного забезпечення воронки продажів

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 канд. техн. наук, 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).

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;

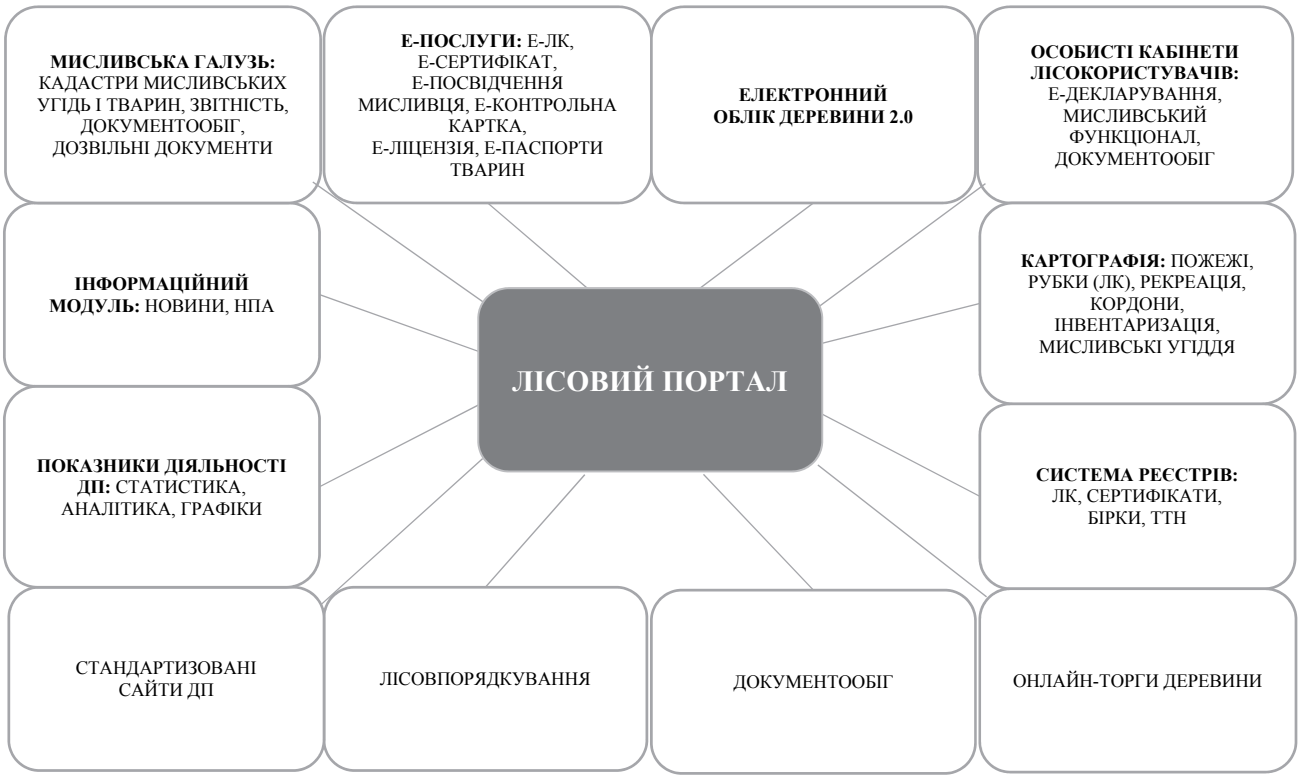


Рис. 1. Структура «Лісового порталу»

– 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).

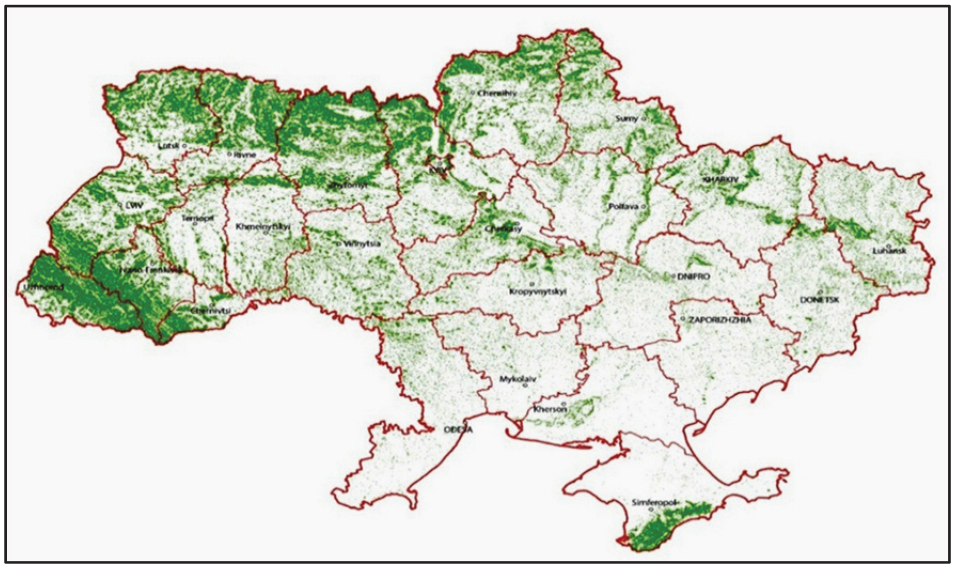


Рис.2 Маска лісів України станом на 2020 рік

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).

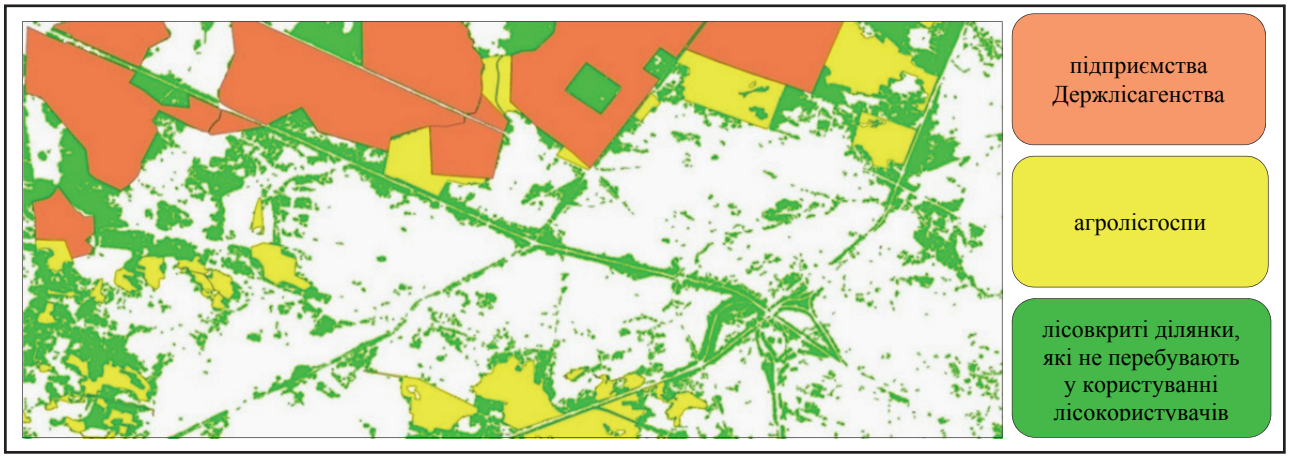


Рис. 3. Встановлення актуальної площі лісів в межах лісокористувасів

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).

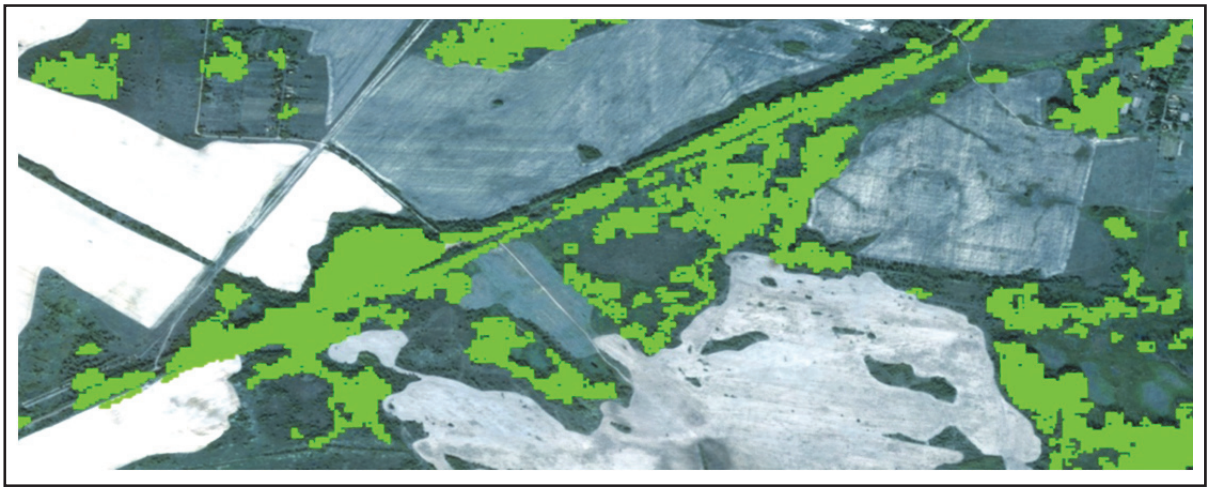


Рис. 4. Ідентифікація самосійних лісів

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

№ пор	Паперовий лісорубний квиток	Електронний лісорубний квиток
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
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, доцента
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].

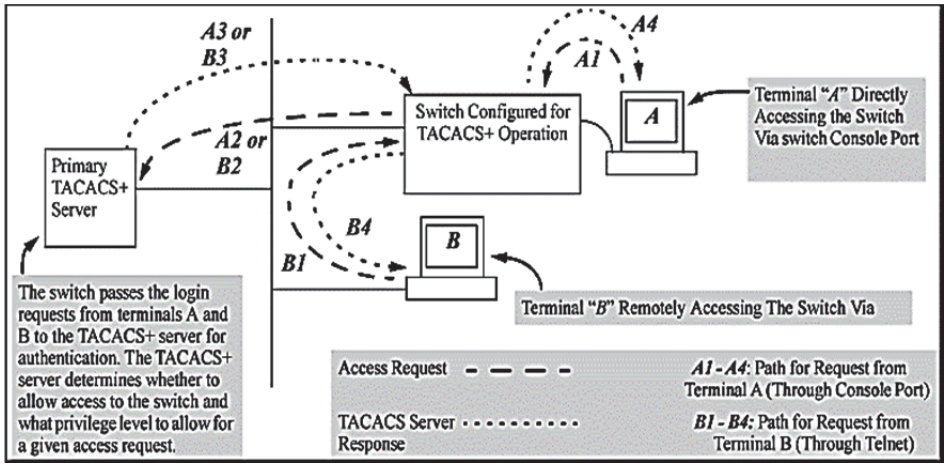


Рис. 1. Приклад роботи TACACS+

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].

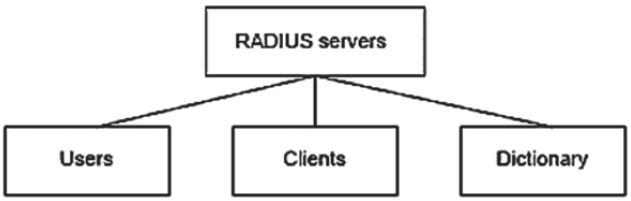


Рис. 2. Бази даних, що підтримуються RADIUS-сервером

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.

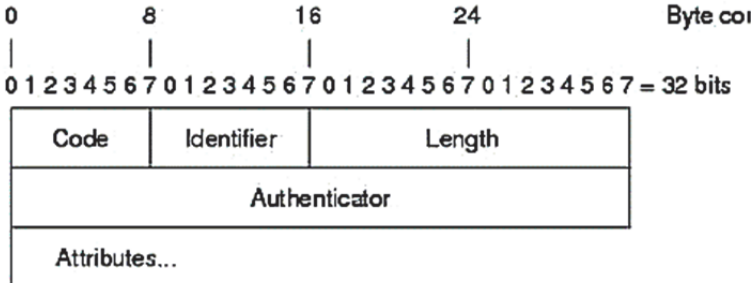


Рис. 3. Формат пакету RADIUS

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).

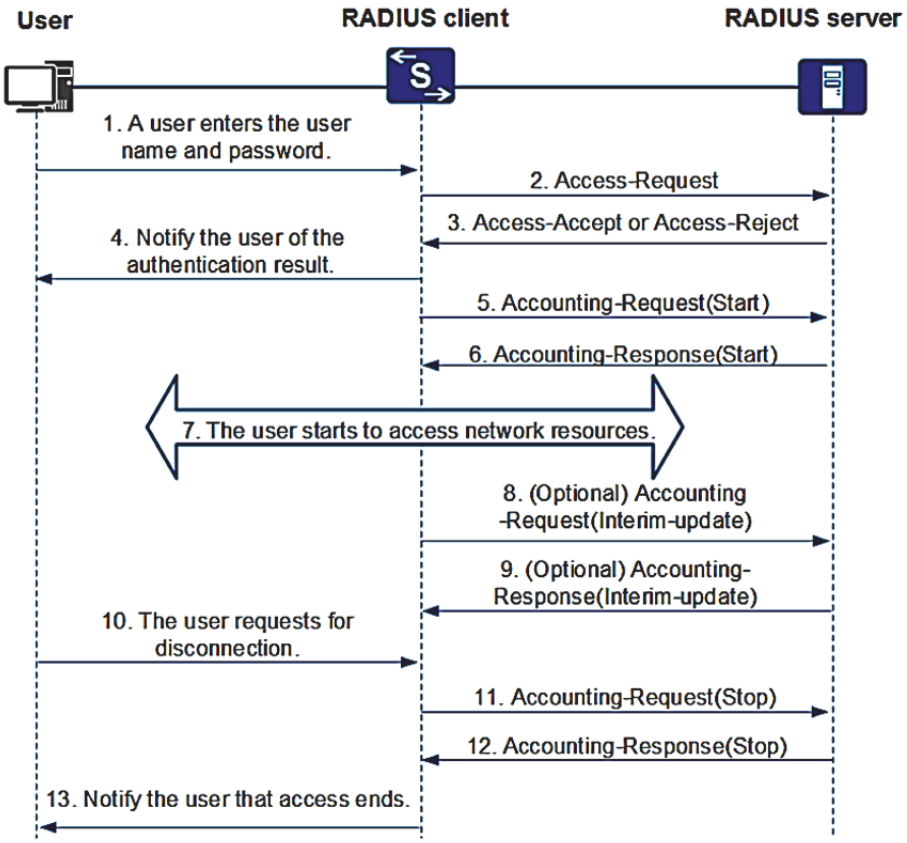


Рис. 4. Процес автентифікації, авторизації та обліку RADIUS

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).

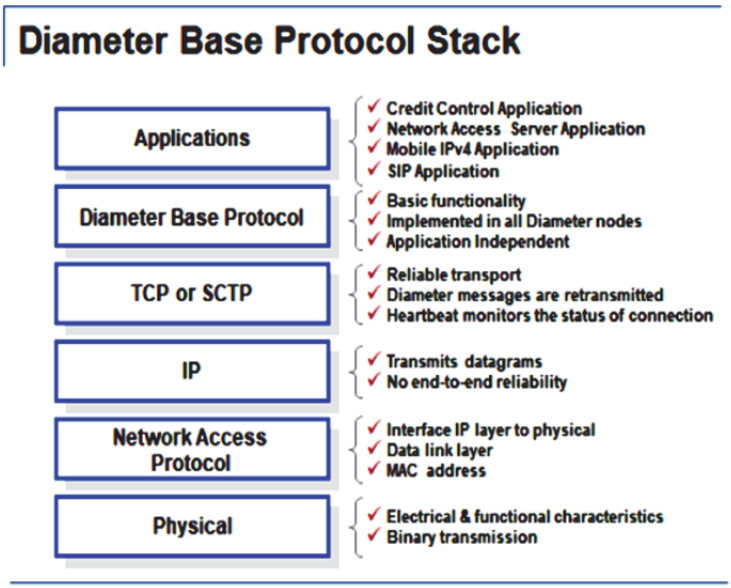


Рис. 5. Стек базових протоколів діаметру

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.

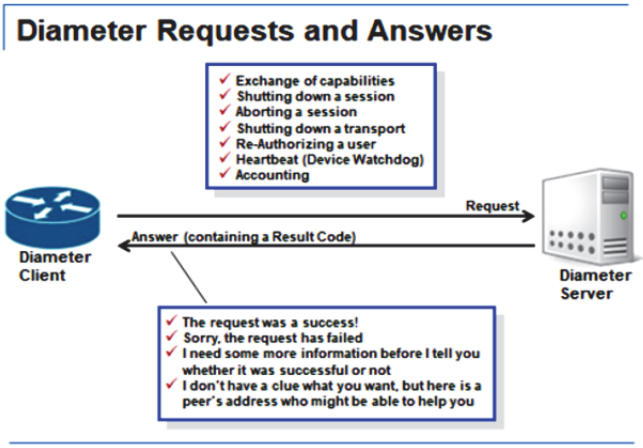


Рис. 6. Запити і відповіді Diameter

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].

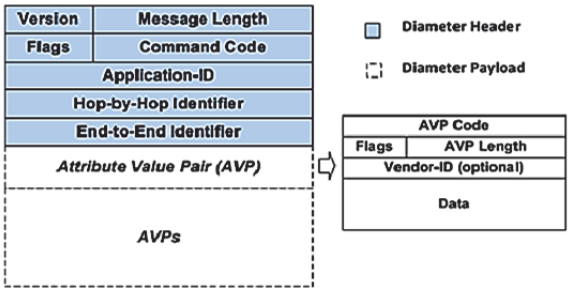


Рис. 7. Формат пакету протоколу Diameter

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 20.03.2023 р.)
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, доцента
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.

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.

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%

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.

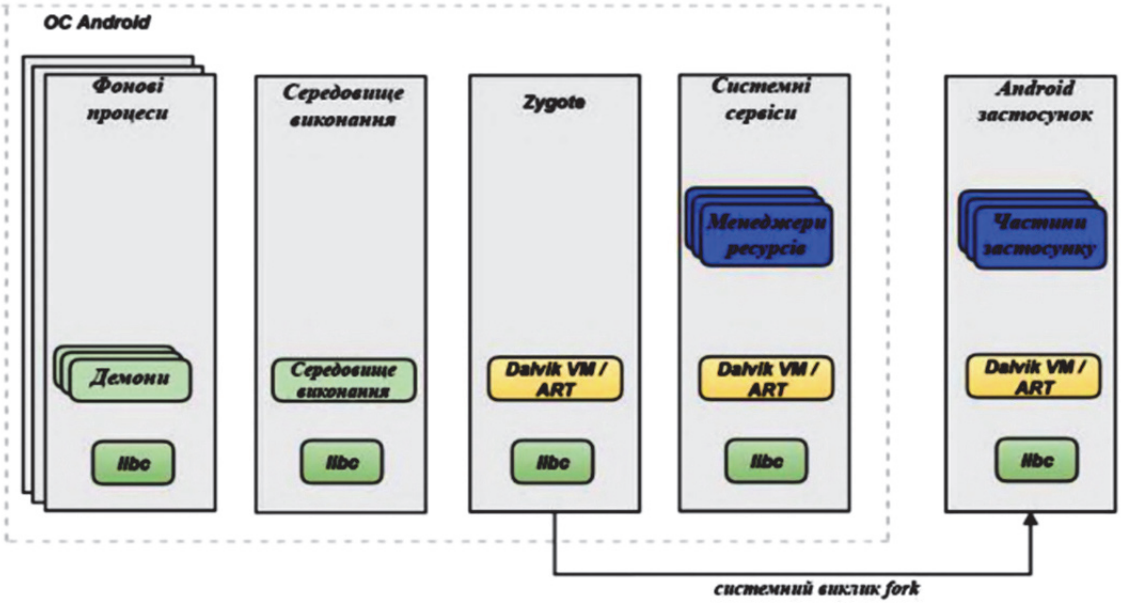


Рис. 1. Схема роботи операційної системи Android із застосунками

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.

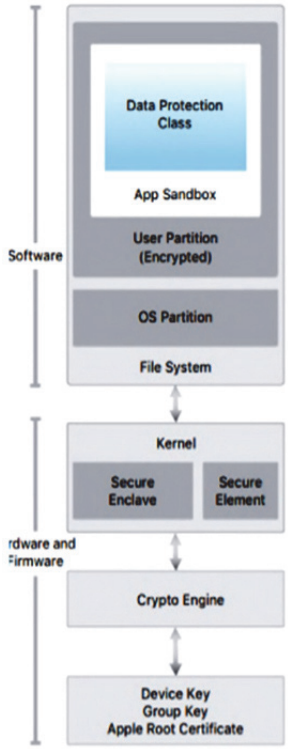


Рис. 2. Архітектура безпеки операційної системи IOS

- 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 03.20.2023 р.).
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 03.20.2023 р.).
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 03.20.2023 р.).
4. Mobile App Security Best Practices: A Checklist – PreEmptive Solutions \\ Режим доступу: https:// www.preemptive.com/top-10-app-protection-practices/ (останнє звернення 03.25.2023 р.).
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 03.25.2023 р.).
6. Android Security: Guide to Android OS – Veracode \\ Режим доступу: https://www.veracode.com/security/android-security (останнє звернення 03.25.2023 р.).
7. Application Protection: Achieve application protection with cloud-based testing tools – Veracode \\ Режим доступу: https://www.veracode.com/security/application-protection (останнє звернення 03.31.2023 р.).
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 03.31.2023 р.).
9. Захист мобільних застосунків на основі систем з нульовим знанням \\ Режим доступу: https://core.ac.uk/download/pdf/323525655.pdf (останнє звернення 04.01.2023 р.).

10. Smartphone Market Share \\ Режим доступу: https://www.idc.com/promo/smartphone-market-share (останнє звернення 04.01.2023 р.).
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 04.01.2023 р.).

Робота виконана під науковим керівництвом старшого 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.

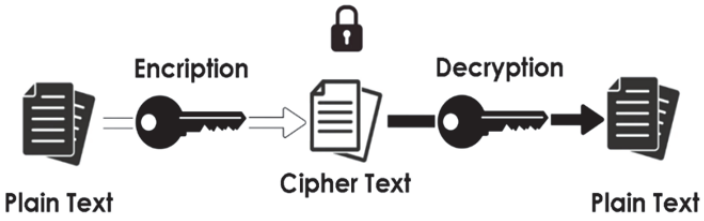


Рис. 1. Приклад роботи шифрування

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.

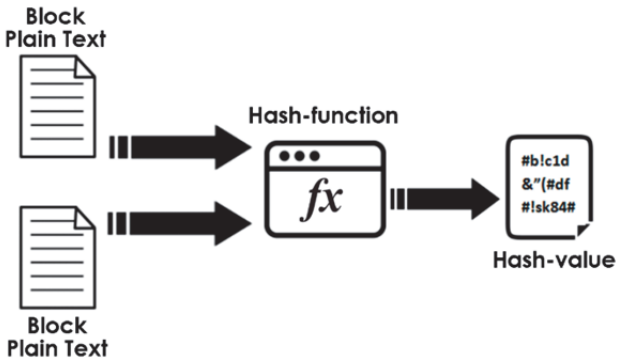


Рис. 2. Приклад роботи будь-якої хеш-функції

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.

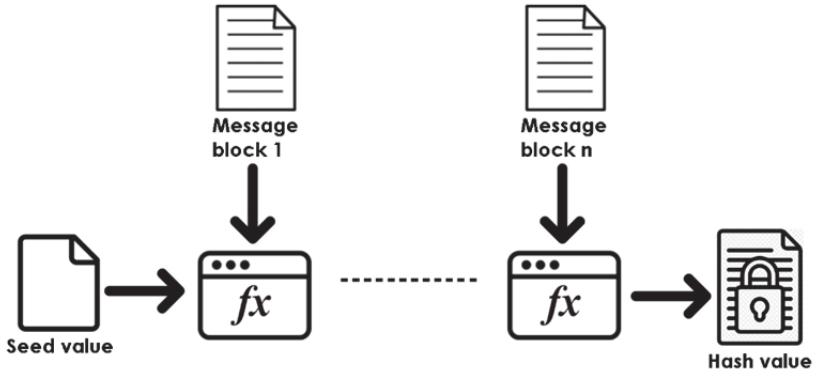


Рис. 3. Схема алгоритму хешування

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).

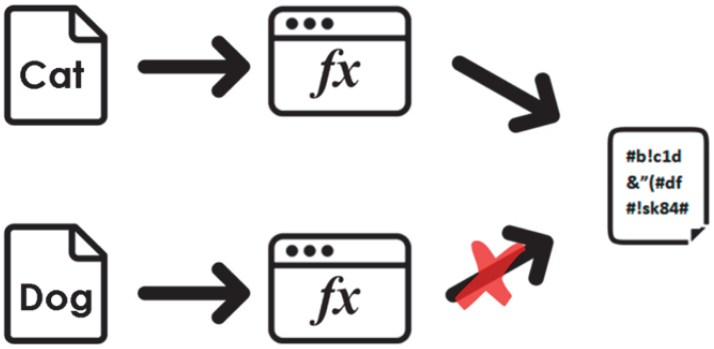


Рис. 4. Collision resistant

- 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).

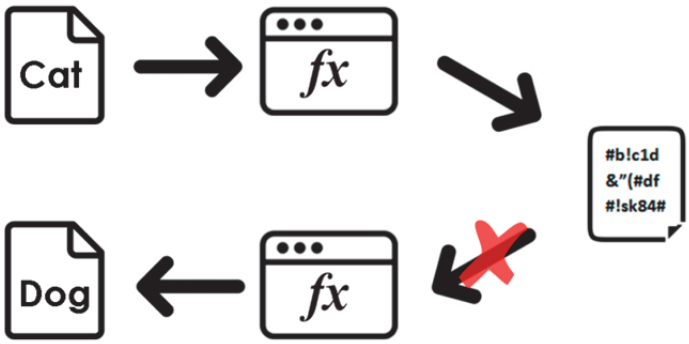


Рис. 6. Second pre-image resistance

- 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 2256 = 1, 1579209*1077 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.

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.

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)

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).

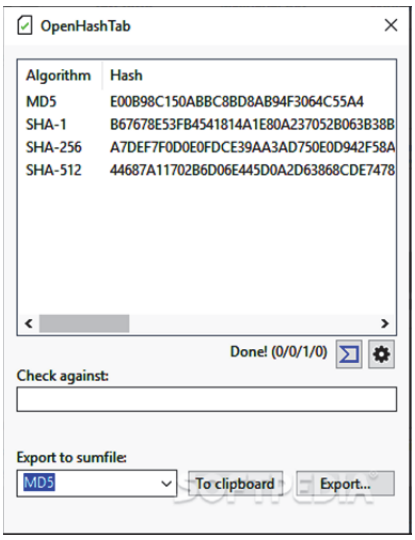


Рис. 7. Головне вікно програми OpenHashTab

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).

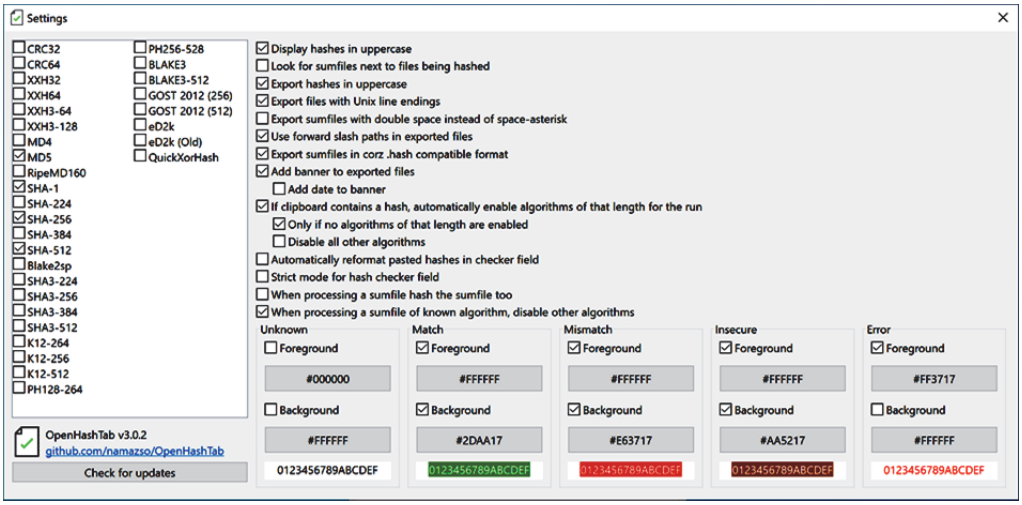


Рис. 8. Вікно налаштувань для хеш-функції

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 01.03.2023 р.).
2. Universal classes of hash functions (Extended Abstract) \\ Режим доступу: https://dl.acm.org/doi/abs/10.1145/800105.803400 (останнє звернення 01.03.2023 р.).
3. Analysis and improvement of a chaos-based Hash function construction \\ Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1007570409003426 (останнє звернення 02.03.2023 р.).
4. Cryptographic Hash Functions: A Review \\ Режим доступу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=85abc4805adb741b0f8c962794d2ab4dac975c5f (останнє звернення 03.03.2023 р.).
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 05.03.2023 р.).
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 05.03.2023 р.).
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 канд. техн. наук, 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].

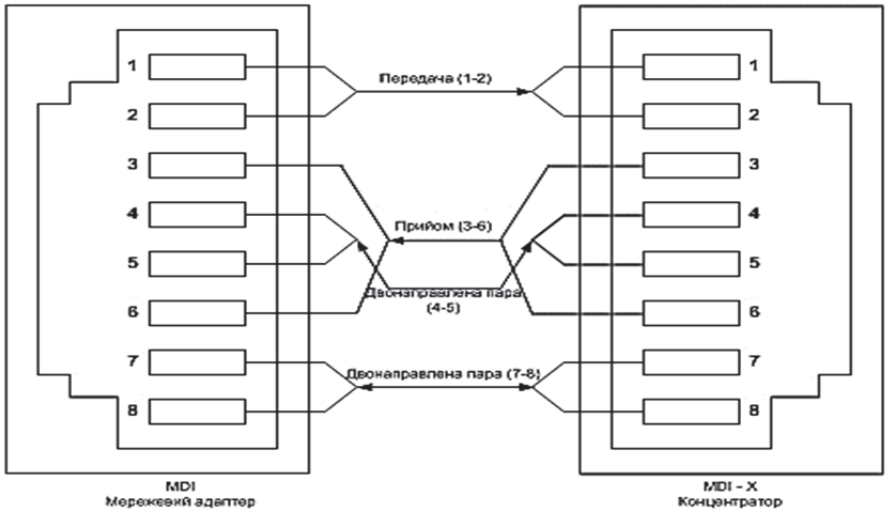


Рис. 1. З'єднання порту MDI мережного адаптера 100Base-T4 з портом MDI-X концентратора.

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 канд. політ. наук, 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).

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.

Рис. 1. Робота AJAX-запиту до бази даних

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 ІЗ 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.

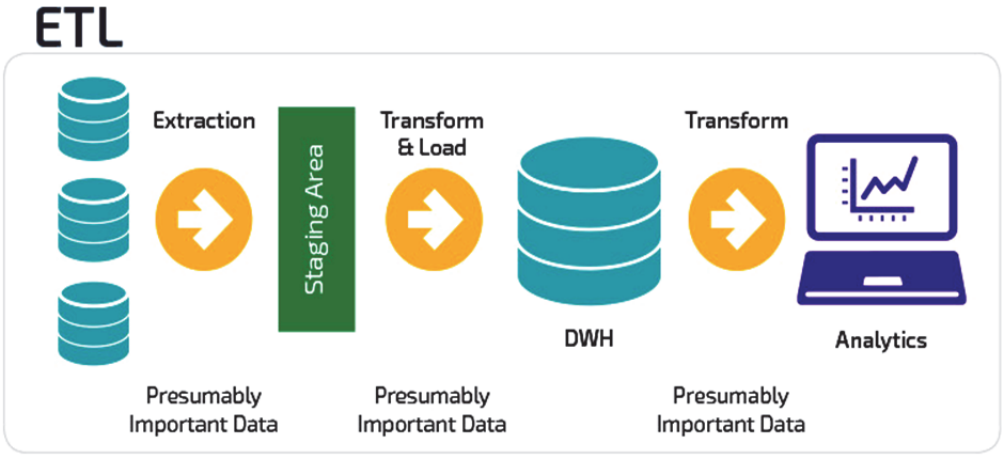


Рис. 1. Приклад концепції збору, обробки та зберігання даних

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. — 2020 р. 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 02.03.2023 р.).
4. Cryptographic Hash Functions: A Review \\ Режим доступу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=85abc4805adb741b0f8c962794d2ab4dac975c5f (останнє звернення 03.03.2023 р.).
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 05.03.2023 р.).
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 05.03.2023 р.).
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 05.03.2023 р.).
8. Big data storage and analytics. 2013 у. URL: https://www.techtarget.com/searchstorage/feature/Big-data-storage-and-analytics

Робота виконана під науковим керівництвом канд. пед. наук, 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.

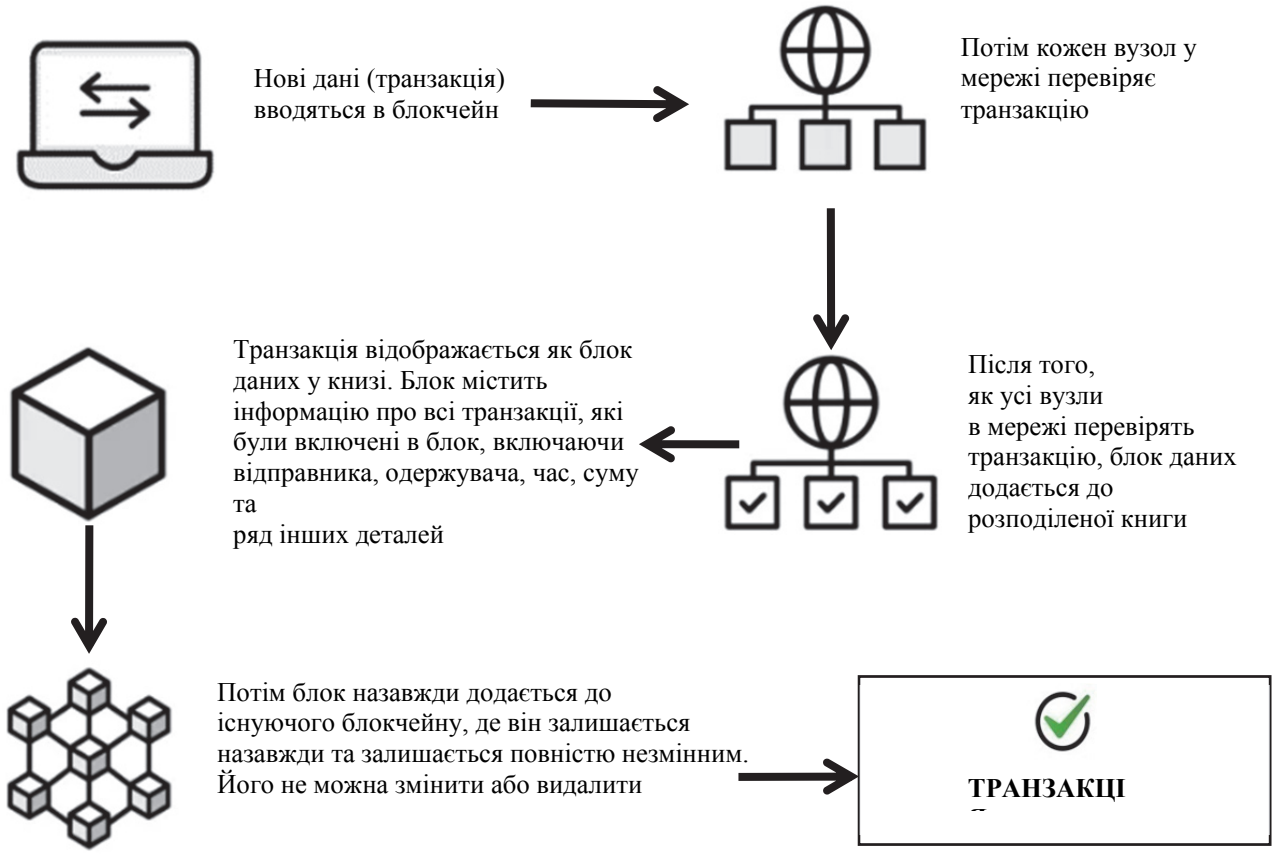


Рис. 1. Принцип роботи технології blockchain

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 масштабова-ність
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 27.02.2023 р.).
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 27.02.2023 р.).
3. The benefits and threats of blockchain technology \\ Режим доступу: https://www.sciencedirect.com/science/article/pii/S138650562030154433 (останнє звернення 01.03.2023 р.)

Робота виконана під науковим керівництвом канд. техн. наук, 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 04.04.2023 р.).
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 04.04.2023 р.).
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.pratsev lashtuvannya-2022-02-03.pdf. (останнє звернення 04.04.2023 р.).

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 04.04.2023 р.).
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 04.04.2023 р.).
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 04.04.2023 р.).

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ВЛАСЕНКО Л. О.

ТЕХНОЛОГІЇ ДЛЯ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ 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.
5. 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 канд. техн. наук, доцента
КОТЕНКО Н. О.

СИСТЕМА ОЦІНКИ РИЗИКІВ ТА ЇЇ ВПЛИВ НА ПІДВИЩЕННЯ 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 конфіден-ційності	Оцінка доступності	Рівень ризику
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
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
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 звернення 31.03.2023 р.).
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 звернення 31.03.2023 р.).
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 04.04.2023 р.).
7. International Organization for Standardization. (2018, Febr. 15). ISO 31000. Risk management. Guidelines. Режим доступу: https://www.iso.org/standard/65694.html. (останнє звернення 31.03.2023 р.).

Робота виконана під науковим керівництвом канд. техн. наук, 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 канд. пед. наук, доцента
ЖИРОВОЇ 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.

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.

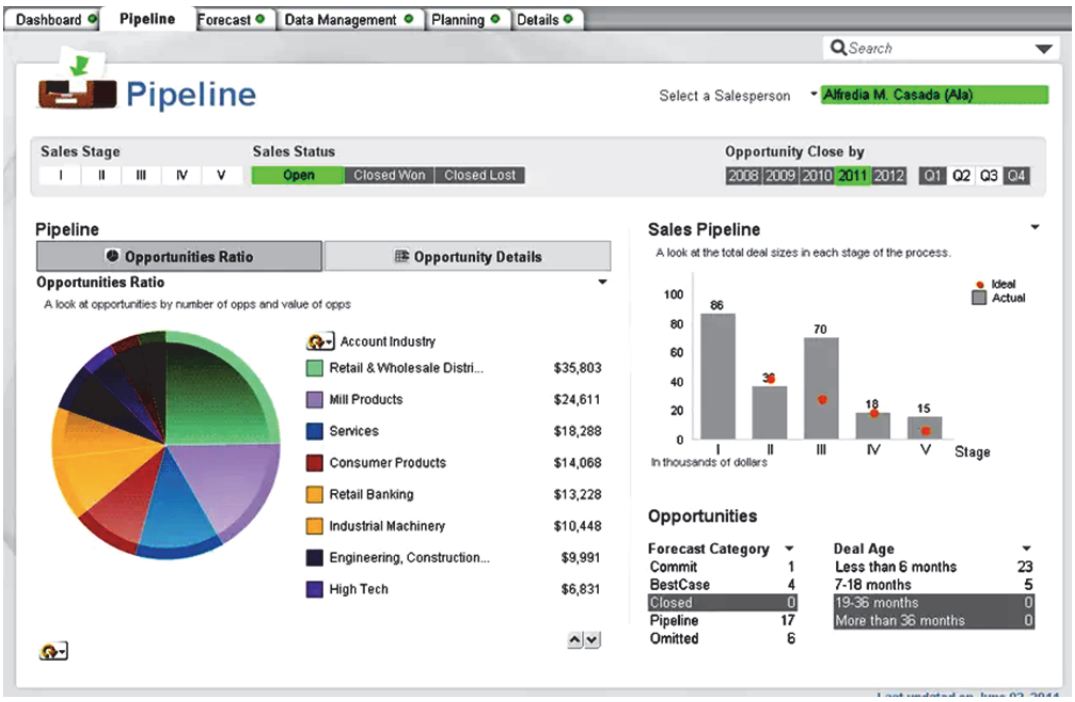


Рис. 3. Перегляд інформаційної панелі даних по продажам

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.

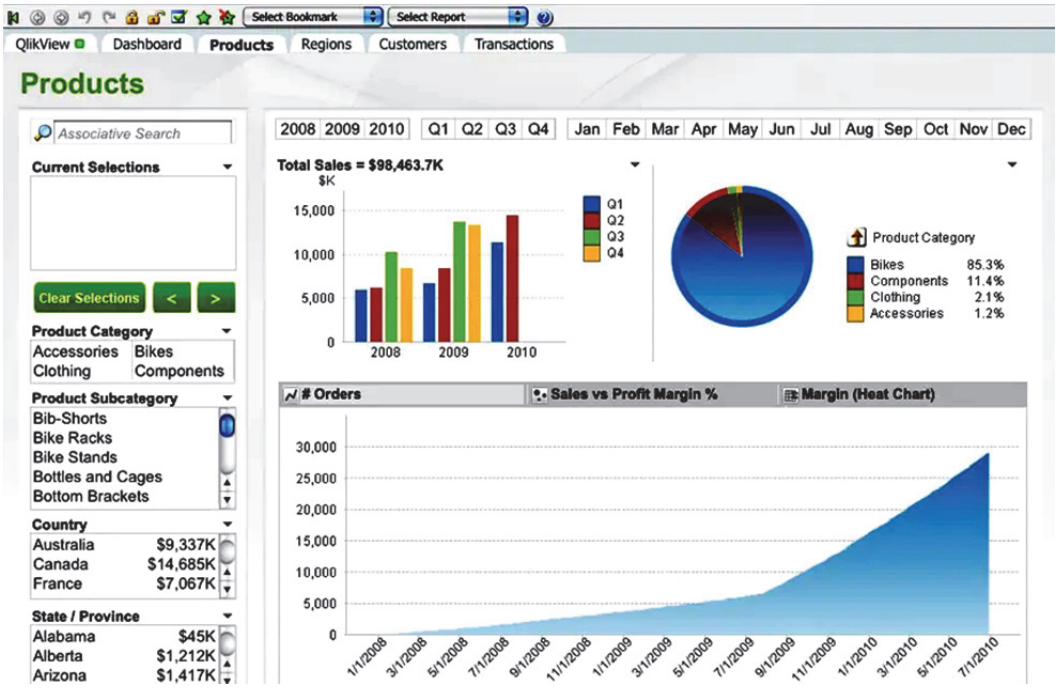


Рис. 5. Аналіз товарної інформації

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 обґрунтовані 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.

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.

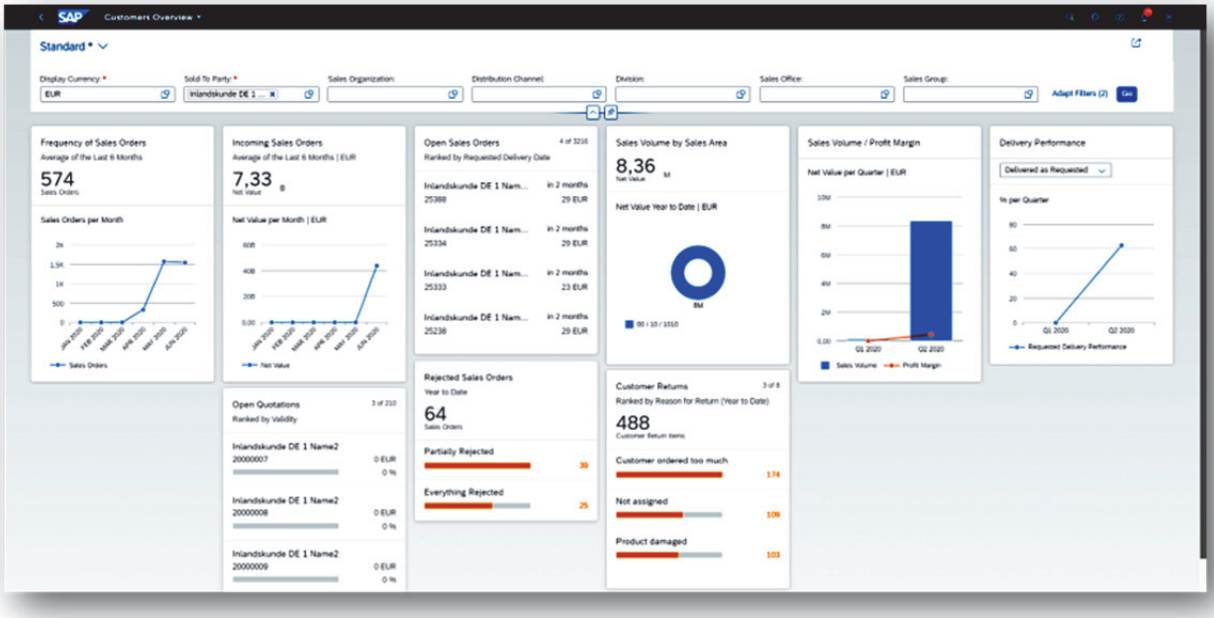


Рис. 6. Інтерфейс програми SAP S/4HANA

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.

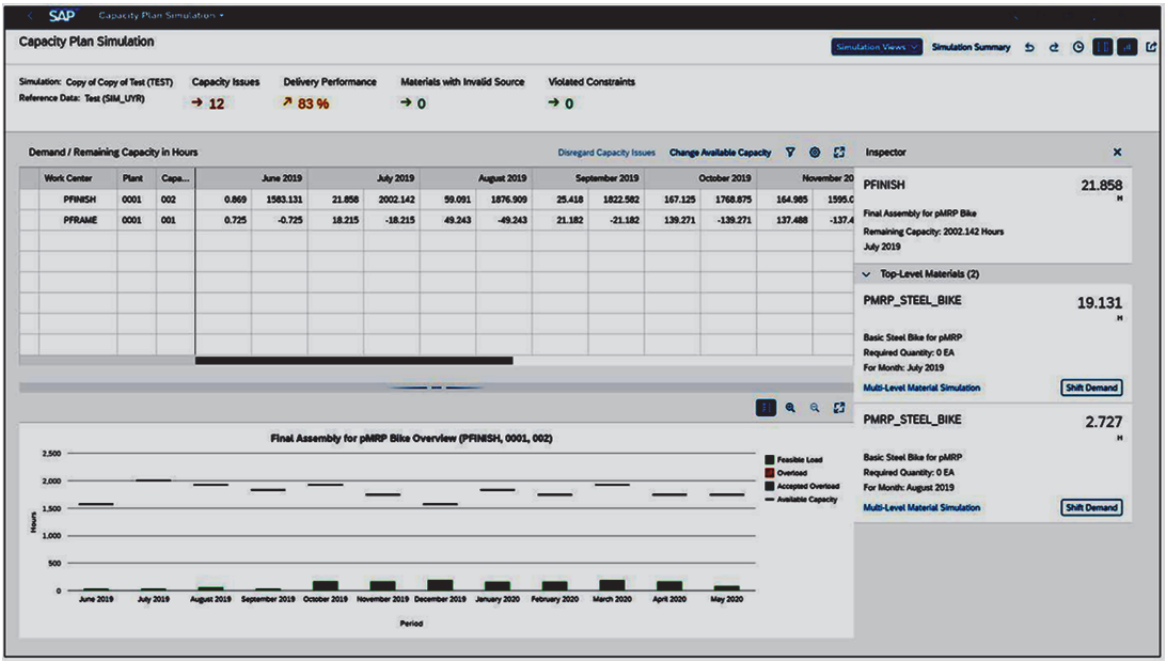


Рис. 7. Моделювання плану потужності

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.

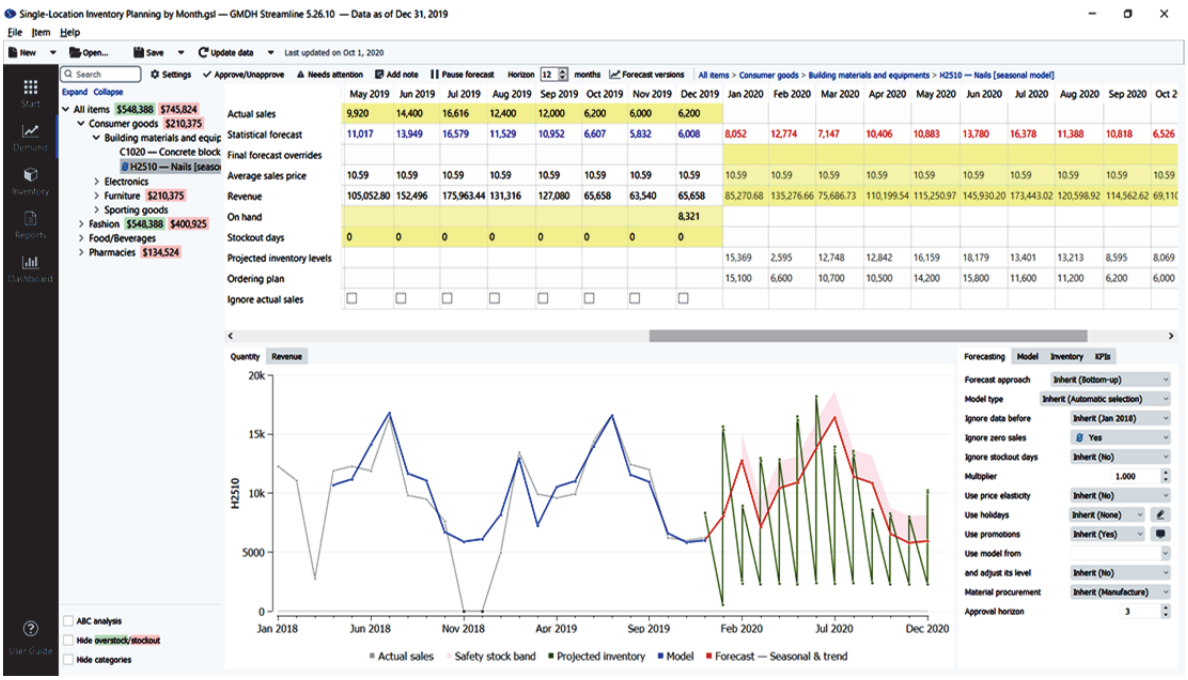


Рис. 8. Інтерфейс системи прогнозування Streamline з використанням машинного навчання

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.

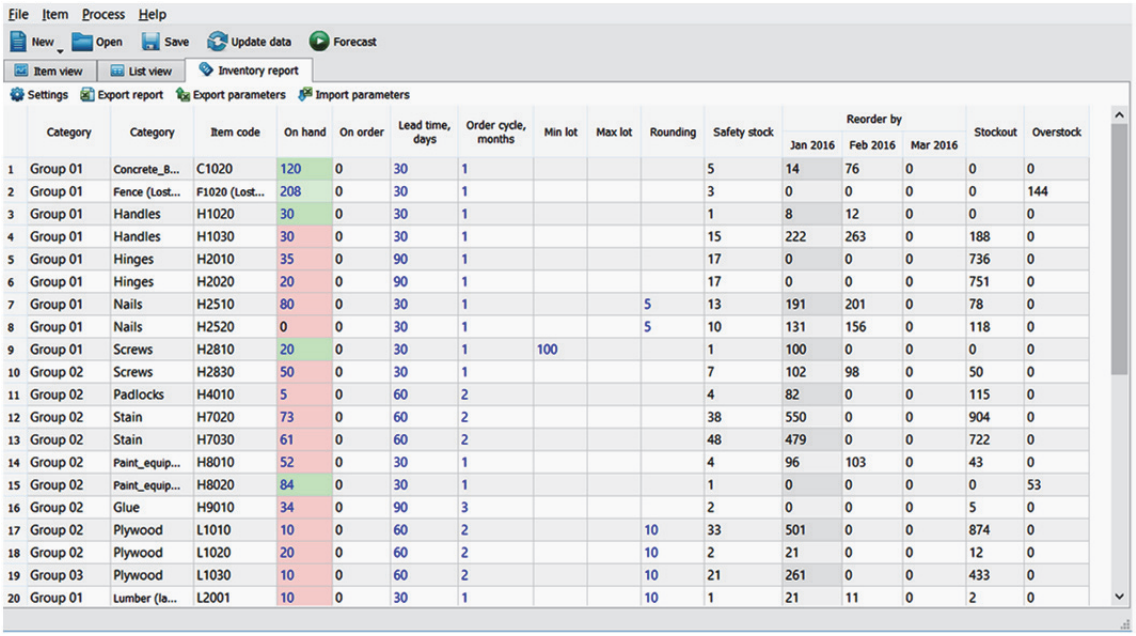
Усі компоненти архітектури Streamline працюють разом та забезпечують швидке та ефективне аналізування даних в реальному часі. Використання цієї технології дозволяє підприємствам отримувати корисну інформацію про свій бізнес швидко та ефективно, що допомагає в прийнятті важливих рішень та побудові ефективних 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.


File Item Process Help

New Open Save Update data Forecast

Item view List view Inventory report

Settings Export report Export parameters Import parameters

	Category	Category	Item code	On hand	On order	Lead time, days	Order cycle, months	Min lot	Max lot	Rounding	Safety stock	Reorder by			Stockout	Overstock
												Jan 2016	Feb 2016	Mar 2016		
1	Group 01	Concrete_B...	C1020	120	0	30	1				5	14	76	0	0	0
2	Group 01	Fence (Lost...	F1020 (Lost...	208	0	30	1				3	0	0	0	0	144
3	Group 01	Handles	H1020	30	0	30	1				1	8	12	0	0	0
4	Group 01	Handles	H1030	30	0	30	1				15	222	263	0	188	0
5	Group 01	Hinges	H2010	35	0	90	1				17	0	0	0	736	0
6	Group 01	Hinges	H2020	20	0	90	1				17	0	0	0	751	0
7	Group 01	Nails	H2510	80	0	30	1			5	13	191	201	0	78	0
8	Group 01	Nails	H2520	0	0	30	1			5	10	131	156	0	118	0
9	Group 01	Screws	H2810	20	0	30	1	100			1	100	0	0	0	0
10	Group 02	Screws	H2830	50	0	30	1				7	102	98	0	50	0
11	Group 02	Padlocks	H4010	5	0	60	2				4	82	0	0	115	0
12	Group 02	Stain	H7020	73	0	60	2				38	550	0	0	904	0
13	Group 02	Stain	H7030	61	0	60	2				48	479	0	0	722	0
14	Group 02	Paint_equip...	H8010	52	0	30	1				4	96	103	0	43	0
15	Group 02	Paint_equip...	H8020	84	0	30	1				1	0	0	0	0	53
16	Group 02	Glue	H9010	34	0	90	3				2	0	0	0	5	0
17	Group 02	Plywood	L1010	10	0	60	2			10	33	501	0	0	874	0
18	Group 02	Plywood	L1020	20	0	60	2			10	2	21	0	0	12	0
19	Group 03	Plywood	L1030	10	0	60	2			10	21	261	0	0	433	0
20	Group 01	Lumber (la...	L2001	10	0	30	1			10	1	21	11	0	2	0

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 29.03.2023 р.).
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 31.03.2023 р.).
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 02.04.2023 р.).

Робота виконана під науковим керівництвом канд. техн. наук, 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).

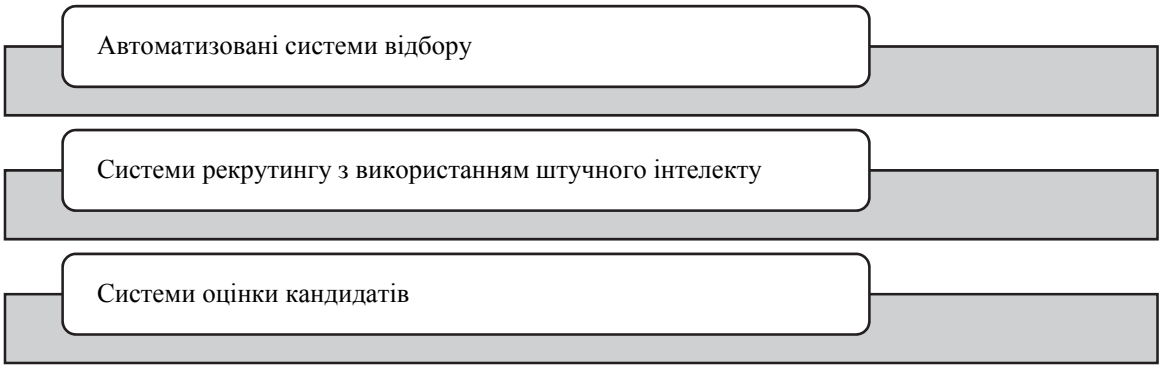


Рис. 1. Класифікація систем підбору персоналу

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 канд. техн. наук, 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):

$$K = B + B_M + O_W \quad (1)$$

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)*:

$$K\,\alpha = n/p \qquad (2)$$

де $\boldsymbol{n}$ – кількість правильно виконаних завдань тесту, $\boldsymbol{p}$ – 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].

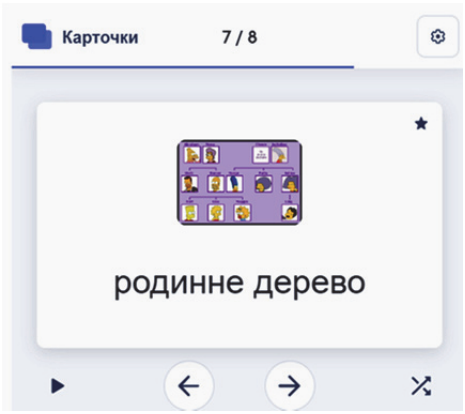


Рис. 1. Приклад тесту в програмі Quizlet

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.

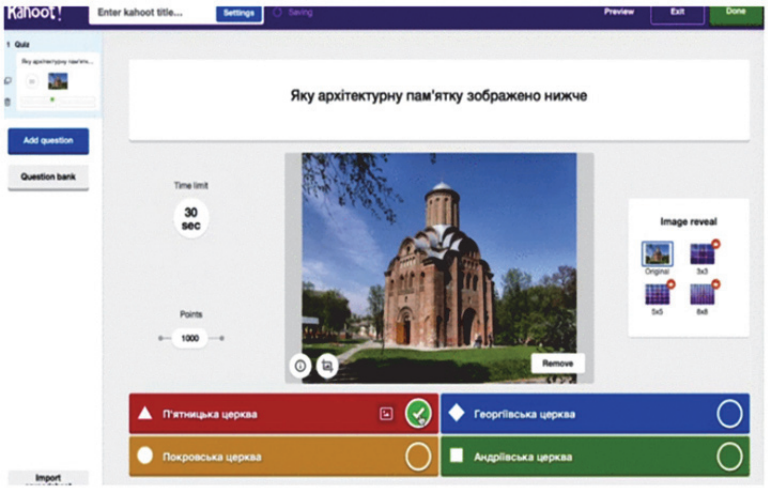


Рис. 2. Приклад тесту в програмі Kahoot!

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].

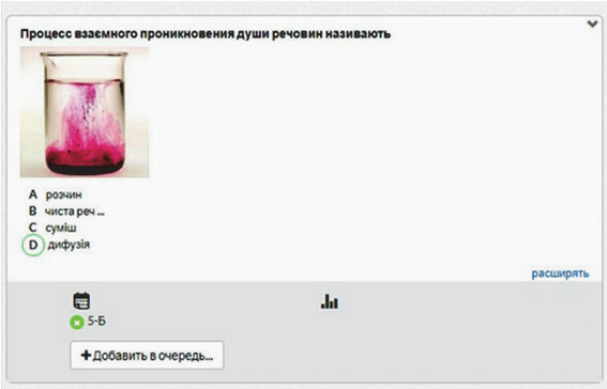


Рис. 3. Приклад тесту в програмі Plickers

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 09.03.2023 р.).
2. В. Бойко «Програмні засоби для проведення тестового контролю знань». // Режим доступу: http://oldconf.neasmo.org.ua/node/1821 (останнє звернення 09.03.2023 р.).
3. О. Корж «Додаток Quizlet ». \\ Режим доступу: https://what.com.ua/dodatok-quizlet-iak-koristyva/ (останнє звернення 13.03.2023 р.).
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 13.03.2023 р.).
5. «Plickers». // Режим доступу: https://sites.google.com/view/it-teachers/plickers (останнє звернення 26.03.2023 р.).

Робота виконана під науковим керівництвом д-ра пед. наук, 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 канд. пед. наук, 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 винагородженні 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

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC press.
2. Collberg, C., & Nagra, J. (2009). Surreptitious software: Obfuscation, watermarking, and tamperproofing for software protection. Addison-Wesley.
3. Chandra, P., & Arora, R. (2018). A Comprehensive Survey on Software Protection and Licensing Techniques. International Journal of Computer Applications, 181(47), 8–15.
4. Zhou, L., Deng, H., & Varadharajan, V. (2015). Software protection and licensing: A survey. Journal of Systems and Software, 107, 166–185.
5. 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.
6. License4J \\ Режим доступу: https://www.license4j.com/ (останнє звернення 29.03.2023 р.).

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 канд. пед. наук, 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 вебсайті, 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.

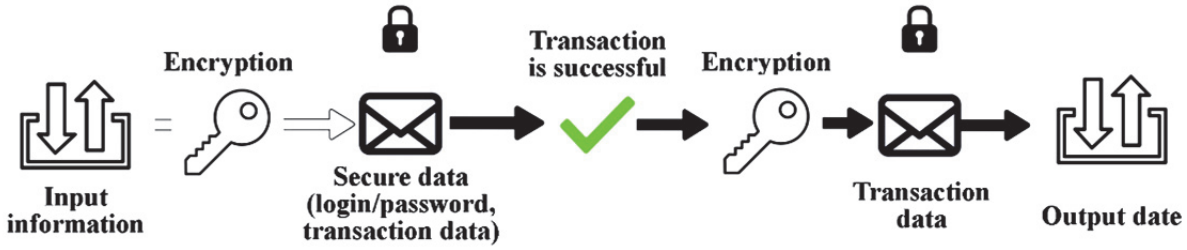


Рис. 2. Приклад шифрування інформації онлайн-гаманця

- 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.

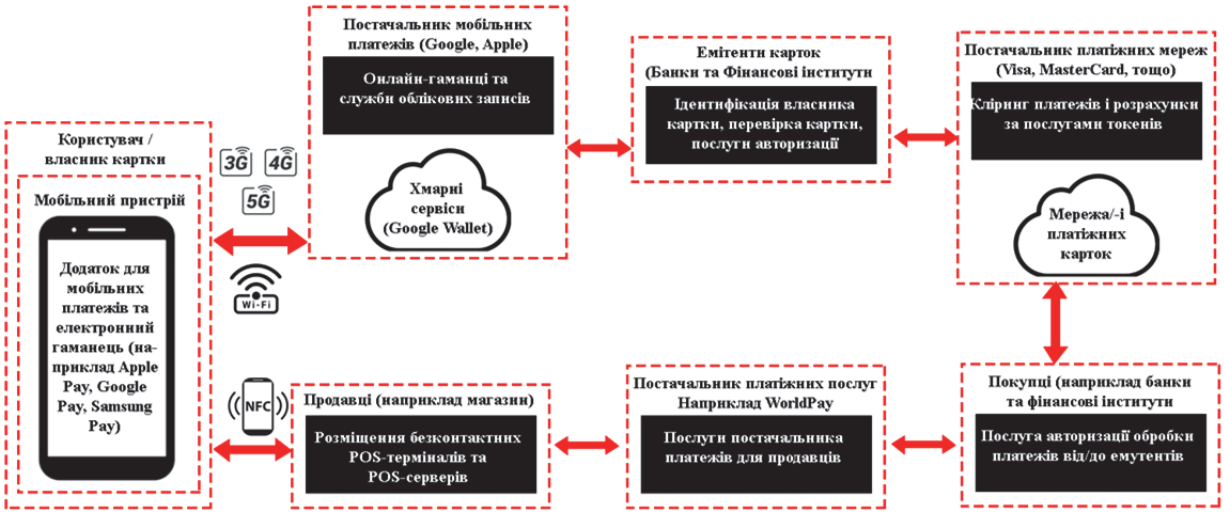


Рис. 3. Модель загроз

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.

Закінчення табл. 1

Компонент	Загроза та вектор атаки	Опис
	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

1. Survey on Online Electronic Paymentss Security // Режим доступу: https://ieeexplore.ieee.org/abstract/document/8701353/authors#authors (останнє звернення 19.03.2023 р.).
2. 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 19.03.2023 р.).
3. Основи інформаційної безпеки\\ Режим доступу: https://naurok.com.ua/informaciyna-bezpeka-247508.html (останнє звернення 19.03.2023 р.).
4. How to Secure Your Digital Wallet \\ Режим доступу: https://www.mcafee.com/blogs/internet-security/how-to-secure-your-digital-wallet/ (останнє звернення 20.03.2023 р.).
5. How safe are eWallets? How to Protect Your eWallet // Режим доступу: https://www.kaspersky.com/resource-center/threats/is-your-ewallet-safe (останнє звернення 20.03.2023 р.)
6. 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 20.03.2023 р.).
7. 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 20.03.2023 р.).

Робота виконана під науковим керівництвом д-ра екон. наук, професора
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.

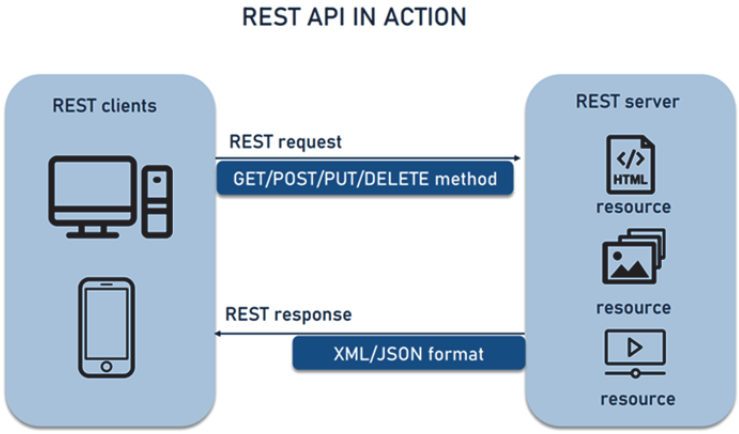


Рис. 2. Принцип роботи протоколу REST

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.

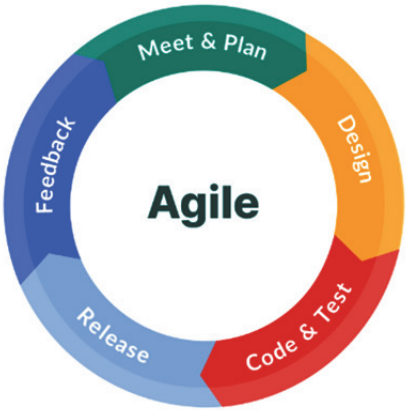


Рис. 3. Підходи методології Agile

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 канд. пед. наук, 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.

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».

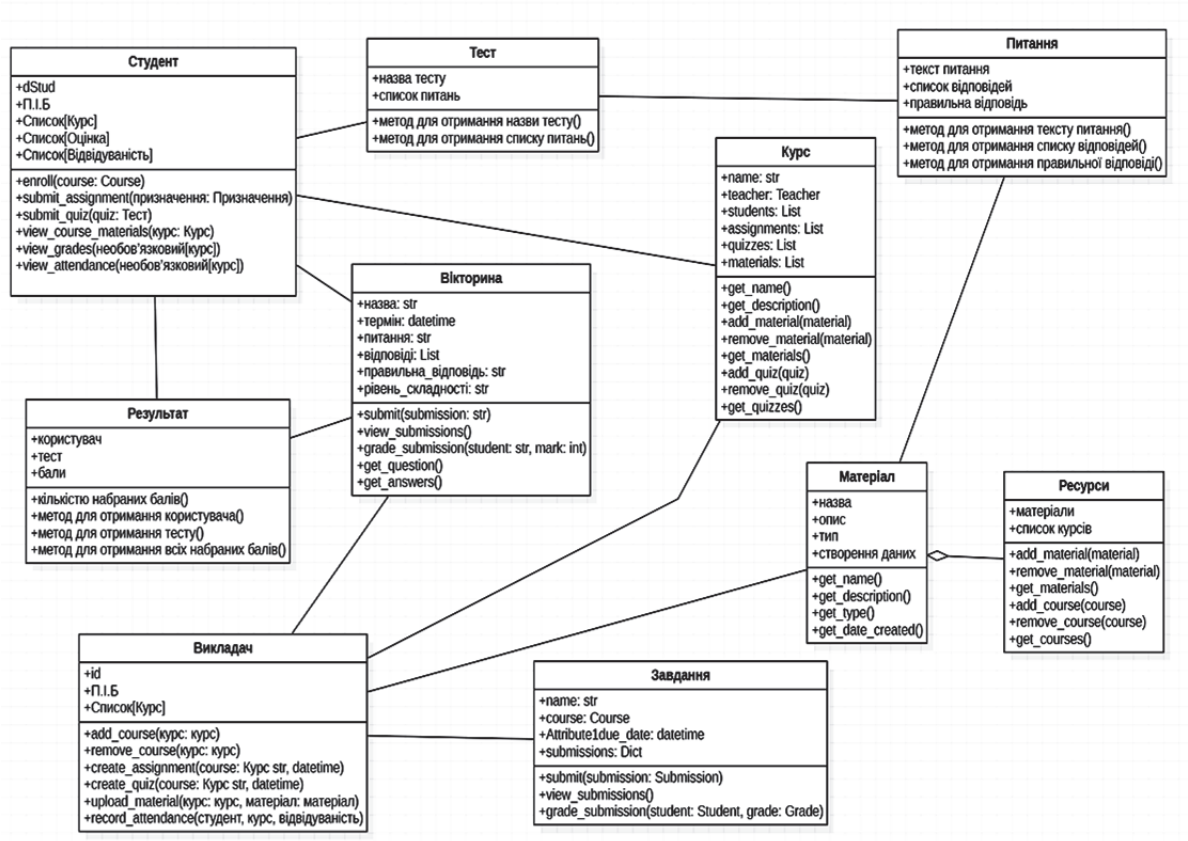


Рис. 1. Модель класів нативного мобільного додатку

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 навчаль-

ному 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/s 10639-018-9764-8
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, доцента
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 інфор-

мацію 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).

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.

Рис. 2. Порівняння складності механізмів перших та сучасних квест кімнат

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 реалізувувати 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 28.03.2023 р.).
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 28.03.2023 р.).
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 28.03.2023 р.).

Робота виконана під науковим керівництвом д-ра техн. наук, 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].

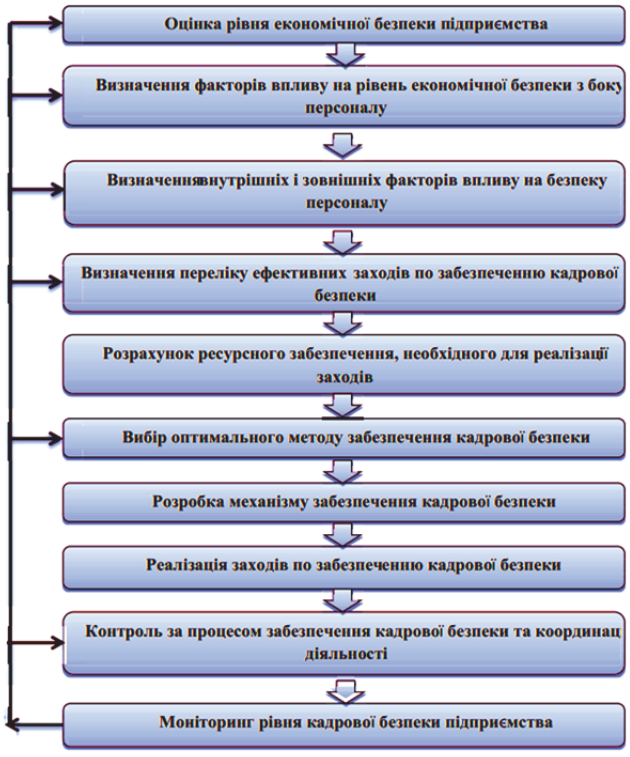


Рис. 1. Алгоритм формування системи кадрової безпеки підприємства

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 дотри-

мують 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, викори-

стання 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 зв рнення 20.03.2023 р.).
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 канд. техн. наук, 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 використо-

вується 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 відтво-

рення 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 III 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.

Наукове електронне видання

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

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

Частина 1

Видавець і виготовлювач
Державний торговельно-економічний університет
вул. Кіото, 19, м. Київ-156, Україна, 02156
Тел. (044) 513 74 18
Електронна пошта knute@knute.edu.ua
280-1Е-2023