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 3

Київ 2023

УДК 004.056.5
П 78

Програмування та захист інформації [Електронний ресурс] : у 3 ч. Ч. 3 : зб. наук. ст. студентів / відп. ред. Т. О. Жирова. – Київ : Держ. торг.-екон. ун-т, 2023. – 224 с.

П 78

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.

СУЧАСНІ ТЕНДЕНЦІЇ АВТОМАТИЗАЦІЇ УПРАВЛІНСЬКОГО Й ОСВІТНЬОГО ПРОЦЕСІВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

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

Стаття присвячена дослідженню тенденцій застосування інформаційних технологій у сфері управління та навчання в закладах вищої освіти. Основна увага приділяється автоматизації процесів управління та навчання, опису сучасних тенденцій та переваг, недоліків та перспектив розвитку в даній сфері.

Article is dedicated to the study of trends in the use of information technology in the management and education in higher education institutions. The main focus is on the automation of management and learning processes, describing current trends and advantages, disadvantages, and prospects for development in this field.

Актуальність. У світі інформаційних технологій дедалі більше уваги приділяється автоматизації процесів в усіх сферах, включаючи навчальну. Розвиток нових інформаційних технологій та платформ для онлайн-навчання надає можливості для ефективнішого та більш доступного навчання. Автоматизація також має свої недоліки та виклики, такі як проблеми з кібербезпекою та приватністю, недостатня взаємодія між викладачами та студентами тощо, тому, вивчення сучасних тенденцій та перспектив розвитку автоматизації управлінських та навчальних процесів у закладах вищої освіти є важливим та актуальним.

Автоматизація управлінських та навчальних процесів є актуальною темою у сучасному світі. Вона дозволяє підвищити ефективність управління та навчання, зменшити витрати на робочу силу та матеріальні ресурси. У цій статті розглянуто сучасні тенденції автоматизації управлінського та навчального процесів у закладах вищої освіти.

Метою статті є дослідити сучасні тенденції автоматизації управлінських та навчальних процесів у закладах вищої освіти, проаналізувати переваги та недоліки використання інформаційних технологій в цій сфері, а також визначити перспективи розвитку автоматизації управління та навчання в закладах вищої освіти.

Завдання статті полягає у:

- Огляді літературних джерел та аналізі публікацій, що стосуються автоматизації управлінських та навчальних процесів у закладах вищої освіти.
- Аналізі переваг та недоліків використання інформаційних технологій в сфері управління та навчання в закладах вищої освіти.
- Визначенні перспектив розвитку автоматизації управління та навчання в закладах вищої освіти.
- Формулюванні рекомендацій щодо вдосконалення процесів автоматизації управління та навчання в закладах вищої освіти на основі результатів дослідження.

Об'єктом дослідження є тенденції застосування інформаційних технологій у сфері управління та навчання в закладах вищої освіти.

Предметом дослідження є автоматизація процесів управління та навчання, опис сучасних тенденцій та перспектив розвитку в даній сфері, а також переваги та недоліки використання інформаційних технологій у навчальному процесі.

Застосування інформаційних технологій є необхідним елементом автоматизації управлінських процесів в закладах вищої освіти. Завдяки використанню різноманітних програмних засобів та інформаційних систем, можливо автоматизувати процеси збору, обробки та збереження інформації, що дозволяє значно полегшити роботу управлінських структур та підвищити їх ефективність.

Управління в закладах вищої освіти є складним та багатогранним процесом, що вимагає відповідального підходу та використання сучасних технологій. Однією з таких технологій є автоматизація управлінських процесів. Вона дозволяє забезпечити швидку та точну обробку даних, встановити систему контролю за виконанням завдань, зменшити кількість помилок та підвищити рівень ефективності управління.

Одним із прикладів автоматизації управління є використання спеціальних програмних засобів для управління процесом навчання. Такі засоби дозволяють створювати та зберігати розклад занять, контролювати відвідуваність та успішність студентів, встановлювати дедлайни для здачі робіт та інші завдання.

Впровадження інформаційних технологій в освітній сектор може стати каталізатором для інноваційних методів викладання та навчання, підвищення залученості студентів і підвищення академічної успішності [1, с. 48].

Один із прикладів застосування інформаційних технологій у процесі управління в закладах вищої освіти – це використання систем електронного документообігу. Це дозволяє значно спростити процес обміну документами між управлінськими структурами, забезпечити швидкий доступ до необхідної інформації та підвищити рівень безпеки збереження даних.

Також інформаційні технології дозволяють автоматизувати процеси планування та контролю навчального процесу, що дозволяє ефективно використовувати ресурси закладу та забезпечити якісну підготовку студентів. Наприклад, системи електронного навчання дають можливість вчителям та студентам здійснювати навчання та контроль знань в режимі онлайн, що значно полегшує процес навчання та контролює успішність студентів.

Отже, використання інформаційних технологій є важливим елементом автоматизації управління в закладах вищої освіти, що сприяє поліпшенню якості управління та підвищенню ефективності процесів.

В сучасних умовах університети активно використовують електронні системи управління навчальним процесом. Ці системи забезпечують можливість зберігання, обробки та аналізу великих обсягів інформації, що сприяє покращенню якості навчання та оптимізації роботи викладачів.

Однією з найбільш поширених електронних систем управління навчальним процесом є Learning Management System (LMS), такою, наприклад, є «MIA: Освіта». Ця система дозволяє студентам отримувати доступ до електронних матеріалів, викладачам – контролювати навчальний процес та взаємодіяти зі студентами в онлайн-режимі, а адміністрації – контролювати виконання навчальних планів та аналізувати результати навчання.

Крім того, електронні системи управління навчальним процесом дозволяють автоматизувати процеси планування навчальних курсів, відстежування виконання навчальних завдань та оцінювання студентів. Це дозволяє покращити якість навчання, сприяє більш ефективному використанню часу викладачів та студентів, а також зменшує кількість адміністративної роботи, пов’язаної з управлінням навчальним процесом.

Використання електронних систем управління навчальним процесом дозволяє створити зручні інструменти для спілкування між викладачами та студентами, а також дозволяє відстежувати прогрес студентів та реагувати на їх потреби у реальному часі. Крім того, використання цих систем дозволяє забезпечити доступ до навчальних матеріалів з будь-якого пристрою.

Інтеграція ІКТ у сектор освіти призвела до появи нових методів викладання та навчання, таких як змішане навчання та перевернуті класи, які довели свою ефективність у підвищенні успішності учнів [2, с.31].

Автоматизація процесу планування та контролю за навчальним процесом є ще однією важливою тенденцією в управлінні вищою освітою. Застосування інформаційних технологій в цих процесах дозволяє збільшити ефективність та точність планування, зменшити кількість помилок та зайвих витрат часу. Це дозволяє викладачам та адміністраторам швидко та зручно створювати розклади занять, враховуючи наявність аудиторій, наявність викладачів, потреби студентів тощо.

Автоматизація процесу контролю за виконанням навчальних планів дозволяє вчителям швидко та ефективно відстежувати успішність студентів, виявляти проблеми та надавати необхідну допомогу. Крім того, це дозволяє студентам отримувати негайний зворотний зв'язок щодо їхньої успішності та відразу коригувати свої дії.

Контроль за навчальним процесом також може бути автоматизованим. Системи автоматичної оцінки та відстеження успішності студентів можуть використовувати алгоритми для оцінки та аналізу навчальних результатів, що дозволяє підвищити якість контролю та сприяти розвитку індивідуальних методів навчання.

Наприклад, такі програмні засоби як «Moodle» або «Microsoft Teams» дозволяють викладачам створювати та організовувати віртуальні класи, додавати в них матеріали, викладати завдання та оцінювати роботи студентів. Також ці системи можуть бути інтегровані з електронними бібліотеками та іншими базами даних для забезпечення швидкого та зручного доступу до інформації.

Такі інструменти як автоматизовані інформаційні системи, програмне забезпечення та електронні платформи дозволяють забезпечити високий рівень якості навчання та ефективність управління в закладах вищої освіти. Вони дозволяють прискорити процес навчання, забезпечити доступ до великої кількості інформації та зменшити затрати на управління навчальним процесом.

Електронні підручники та навчальні посібники є однією з основних тенденцій використання інформаційних технологій у навчальному процесі в закладах вищої освіти. Ці матеріали можуть містити різноманітні форми навчання, такі як відеоуроки, аудіозаписи, інтерактивні тести та завдання, що дозволяє студентам засвоювати матеріал на свій власний темп та з будь-якого місця з доступом до Інтернету. Крім того, електронні підручники та навчальні посібники можуть бути оновлені та доповнені в режимі онлайн, що дозволяє студентам мати доступ до актуальної та свіжої інформації. Такі матеріали можуть бути дуже корисні для дистанційного навчання, яке стало набагато популярнішим в останні роки. Також електронні підручники та навчальні посібники можуть бути інтегровані з іншими електронними системами управління навчальним процесом, такими як система електронного навчання чи система автоматизованого тестування, що забезпечує більш зручну та ефективну організацію навчального процесу для студентів та викладачів.

Ще однією з тенденцій використання інформаційних технологій у навчальному процесі є використання відеоуроків та вебінарів. Це особливо актуально у зв'язку з пандемією COVID і російсько-українською війною, через що заклади освіти були вимушені перейти на дистанційну форму навчання. Відеоуроки є корисним інструментом для вивчення нового матеріалу або поглиблення знань в певній темі. Вони можуть бути розміщені на різних платформах, таких як YouTube, або спеціалізовані платформи навчання, які надають доступ до відеоуроків від провідних фахівців у різних галузях, таких як Coursera або Prometheus. Вебінари – це живі онлайн-презентації, під час яких провідний експерт пояснює певну тему та відповідає на запитання учасників. Вони можуть бути проведені за допомогою різних платформ, таких як Zoom, Google Meeting, Microsoft Teams, або спеціалізовані платформи для вебінарів. Відеоуроки та вебінари забезпечують доступ до навчання з будь-якого місця, де є доступ до Інтернету. Крім того, вони можуть бути записані та використані в якості додаткового матеріалу для підготовки до екзаменів або інших важливих подій [3, с. 4].

Автоматизація навчальних процесів у закладах вищої освіти також є важливою тенденцією сучасності. Вона дозволяє підвищити ефективність навчання та забезпечити кращу якість знань студентів. Однією з основних переваг автоматизації навчальних процесів є можливість забезпечення індивідуального підходу до кожного студента, використовуючи різноманітні методи навчання.

Одним із прикладів автоматизації навчальних процесів є використання електронних курсів та онлайн-навчання. Це дозволяє студентам вивчати матеріал у своєму темпі та в зручний для них час, а також забезпечує доступ до багатої бази знань та матеріалів. Крім того, автоматизація дозволяє студентам брати участь у віртуальних лекціях та семінарах,

спілкуватися з викладачами та іншими студентами, що забезпечує взаємодію та обмін досвідом.

Електронні підручники також стали невід'ємною частиною у навчальному процесі. Основне його завдання на етапі отримання нових знань полягає у залученні в процес навчання інших, ніж традиційний підручник, можливостей людського мозку, зокрема, слухової та емоційної пам'яті, з метою максимального полегшення розуміння та запам'ятовування навчального матеріалу. Текстова частина супроводжується численними перехресними посиланнями, що дають змогу скоротити час пошуку необхідної інформації. Такий підручник може мати аудіо- або відеозапис лекторського викладу матеріалу. Але використання електронних підручників дозволяє формувати тільки певний рівень знань у студентів, тоді як формування практичних навичок і компетенцій в такому випадку є неможливим [3, с. 45].

Електронні системи контролю знань є ще однією тенденцією використання інформаційних технологій у навчальному процесі. Ці системи можуть бути використані для проведення онлайн тестування, оцінювання завдань, роботи з електронними тестами та іншими методами оцінювання знань студентів.

Електронні системи контролю знань дозволяють автоматизувати процес оцінювання та зберігання результатів, що полегшує роботу викладачів та адміністраторів навчального закладу. Крім того, такі системи можуть надавати додаткові можливості для аналізу даних про навчальні досягнення студентів та виявлення проблемних місць у навчанні.

Також електронні системи контролю знань можуть бути інтегровані з іншими електронними системами управління навчальним процесом, що дозволяє створювати єдину інформаційну систему для ефективного управління навчальним процесом в цілому.

Застосування інформаційних технологій управління та навчання має ряд переваг, серед яких:

- Збільшення ефективності та швидкості обробки інформації. Інформаційні технології дозволяють обробляти інформацію значно швидше, ніж людина, що забезпечує швидке та точне прийняття рішень.
- Зменшення витрат на паперову документацію та збереження даних. Інформаційні системи дозволяють зберігати та обробляти інформацію в електронному вигляді, що зменшує витрати на паперову документацію та зберігання даних.
- Забезпечення доступності інформації для користувачів. Інформаційні технології дозволяють швидко та легко забезпечити доступ до інформації користувачам, що робить процес управління та навчання більш доступним та ефективним.
- Підвищення якості навчання та забезпечення індивідуального підходу. Застосування інформаційних технологій дозволяє забезпечити індивідуальний підхід до навчання, забезпечити різноманітність форм та методів навчання, що підвищує якість навчання.
- Можливість доступу до навчального матеріалу у будь-який час та в будь-якому місці[4, с. 27]

Хоча автоматизація управлінських та навчальних процесів має багато переваг, вона також має певні недоліки, які слід враховувати:

- Високі витрати на розробку та впровадження інформаційних систем. Розробка, підтримка та оновлення програмного забезпечення можуть бути дуже витратними, особливо для закладів з обмеженим бюджетом.
- Залежність від технології. Якщо система автоматизації навчання відмовляє, це може призвести до затримок у проведенні занять та оцінюванні.
- Віддаленість від людського контакту. Деякі студенти можуть відчувати віддаленість від викладачів та інших студентів, особливо якщо навчання відбувається виключно в онлайн-форматі.
- Використання застарілих технологій. Багато закладів вищої освіти мають застарілу техніку та програмне забезпечення, що може призвести до проблем зі сумісністю та ефективністю автоматизованих систем.

Сучасні технології дозволяють значно полегшити та покращити управління та навчання в закладах вищої освіти. Автоматизація управлінських та навчальних процесів дозволяє забезпечити ефективну та точну обробку даних, зменшити кількість помилок та витрат на робочу силу, а також підвищити якість навчання та знань студентів.

Однак, разом з тим, автоматизація вимагає розробки та впровадження спеціальних програмних засобів, а також може призвести до зниження кількості робочих місць, що пов'язані з управлінням та навчанням.

Крім того, важливо враховувати етичні аспекти впровадження автоматизації в управління та навчання. Наприклад, необхідно забезпечувати конфіденційність даних студентів та викладачів, а також забезпечувати право на вільний вибір методів навчання та доступ до необхідної інформації для всіх студентів.

Загалом, можна зробити висновок, що автоматизація управлінських та навчальних процесів є важливою тенденцією сучасності в закладах вищої освіти. Вона дозволяє підвищити ефективність та точність управління, зменшити кількість помилок та витрат на робочу силу, а також підвищити якість навчання та знань студентів. Однак, важливо розробляти нові напрями роботи та навчання для спеціалістів, які займаються автоматизацією, та враховувати етичні аспекти впровадження автоматизації в управління та навчання.

Висновки. У результаті дослідження було встановлено, що автоматизація управлінських та навчальних процесів є актуальною та перспективною тенденцією в сучасній вищій освіті. Застосування інформаційних технологій дозволяє знизити витрати часу та зусиль на адміністративні та рутинні процеси, підвищити якість та ефективність управління, забезпечити доступність та якість навчання.

Проте, також було виявлено недоліки та обмеження в застосуванні інформаційних технологій, такі як можливість технічних збоїв та проблем з безпекою даних, необхідність кваліфікованого персоналу та відповідних знань та навичок користування цими технологіями.

Отже, можна стверджувати, що використання інформаційних технологій у вищій освіті є невід'ємною складовою сучасного навчально-виховного процесу, який підвищує якість та ефективність навчання, а також сприяє покращенню управління закладами вищої освіти.

Список використаних джерел

1. Осадчий В.В., Осадча К.П. Сучасні реалії і тенденції розвитку інформаційно-комунікаційних технологій в освіті. Інформаційні технології і засоби навчання, Т. 48, № 4, с. 47–57, 2015.
2. Іванова С. Застосування сучасних технологій та інноваційних методів навчання у вищих навчальних закладах. Інформаційні технології та Інтернет у навчальному процесі та наукових дослідженнях: навч. посіб. – 2018. – 295с.
3. Полянська А.С. Круглий стіл: Інноваційні методи викладання у вищій школі: обмін досвідом та кращі практики. – Івано-Франківськ: ІФНТУНГ, 2020. – 192 с.
4. Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми: збірник. наук. пр. – Вип. 42. – Київ-Вінниця: ТОВ фірма «Планер», 2015. – 471 с.

Робота виконана під науковим керівництвом канд. екон. наук, старшого викладача
ФРАНЧУК Т. М.

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ ДЛЯ ПРОГНОЗУВАННЯ ЗАПІЗНЕНЬ ГРОМАДСЬКОГО ТРАНСПОРТУ

ПОНОМАРЕНКО С., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У сучасному світі, де технології розвиваються зі швидкістю світла, застосування машинного навчання в різних галузях стає все більш поширеним. Однією з таких галузей є транспортна індустрія, де машинне навчання може бути застосоване для вдосконалення різних процесів, включаючи прогнозування запізнень громадського транспорту. У статті досліджено, як компанія Google використовує технології машинного навчання для прогнозування запізнень громадського транспорту. Розглянуто методи збору та аналізу даних про рух транспорту та алгоритми машинного навчання, які використовуються для прогнозування запізнень.

In the modern world, where technologies are developing at the speed of light, the use of machine learning in various industries is becoming increasingly widespread. One of such industries is the transportation industry, where machine learning can be applied to improve various processes, including predicting delays in public transportation. In this article, we will investigate how Google uses machine learning technologies to predict delays in public transportation. We will examine the methods of collecting and analyzing data on transportation movement and the machine learning algorithms used to predict delays.

Актуальність. У сучасному світі, технології змінюють наш спосіб життя та роботи. Застосування машинного навчання в різних галузях стає все більш поширеним і дозволяє вдосконалювати процеси та забезпечувати високу точність в прийнятті рішень. Однією з таких галузей є транспортна індустрія, де застосування машинного навчання може значно покращити якість послуг та зменшити час очікування для пасажирів громадського транспорту.

Прогнозування запізнень громадського транспорту є важливою задачею для забезпечення точності та своєчасності. Технології машинного навчання, такі як нейронні мережі, можуть допомогти вирішувати цю задачу, збираючи та аналізуючи великі обсяги даних про рух транспорту та прогнозуючи його рух у майбутньому.

Однією з компаній, яка застосовує машинне навчання для прогнозування запізнень громадського транспорту, є Google. Компанія використовує свою платформу Google Maps для збору даних про рух транспорту та аналізує їх, використовуючи алгоритми машинного навчання для прогнозування запізнень. Це дозволяє пасажирам більш точно планувати свій маршрут, а компаніям громадського транспорту покращити ефективність свого руху та забезпечити більш якісне обслуговування.

Прогнозування запізнень громадського транспорту – це лише один із прикладів того, як машинне навчання може забезпечити більш точну та швидку обробку даних у різних галузях.

Метою статті є дослідження того, як компанія Google використовує машинне навчання для прогнозування запізнень громадського транспорту, зокрема методів збору та аналізу даних про рух транспорту та алгоритмів машинного навчання, що застосовуються для прогнозування запізнень.

Об'єктом дослідження є застосування технологій машинного навчання компанією Google для прогнозування запізнень громадського транспорту.

Предмет дослідження – використання технологій машинного навчання для прогнозування запізнень громадського транспорту.

Аналіз попередніх досліджень у сфері прогнозування запізнень громадського транспорту засвідчив, що вже було проведено досить багато досліджень з використанням

різноманітних методів машинного навчання, таких як регресійна аналітика, дерева рішень, нейронні мережі тощо.

Серед таких робіт були:

- Дослідження «Real-Time Prediction of Bus Arrival Time using Automatic Vehicle Location (AVL) Data» (2011) виконане Dr. Yanfeng Ouyang, Department of Civil and Environmental Engineering, University of Illinois at Urbana-Champaign.
- «Predicting Transit Bus Arrival/Departure Times using General Transit Feed Specification Data» (2014) виконане Rongjie Yu, Alireza Khani, та Wei (David) Fan, Department of Computer Science, Florida State University.
- «Real-time estimation of public transport vehicle arrival times at a stop using GPS data» (2017) виконане Sunil Kumar Jha, Rajesh Kumar Tiwari, та Shweta Singh, Department of Electronics and Communication Engineering, Birla Institute of Technology.
- «Improving Public Transit System Performance through Real-Time Data Analysis» (2019) виконане Ashish Kumar та Upendra Kumar, Department of Electrical [2].

Ці дослідження охоплюють різні аспекти прогнозування запізнень громадського транспорту, від використання GPS-даних та дані з загальних транспортних розкладів до застосування методів машинного навчання та глибинного навчання. Результати цих досліджень можуть допомогти покращити ефективність транспортних систем та зробити їх більш доступними для користувачів.

Виклад основного матеріалу. Машинне навчання – це підхід до розв'язання задач штучного інтелекту, що дозволяє комп'ютерам вчитися з досвіду та покращувати свої результати з часом. В контексті прогнозування запізнень громадського транспорту, машинне навчання може бути використане для створення моделей, що будуть прогнозувати час прибуття транспортного засобу на зупинку на основі даних про його рух та інші фактори, такі як трафік та погодні умови.

- Навчання з учителем (supervised learning) – один зі способів машинного навчання, в ході якого випробувана система примусово навчається за допомогою наявної множини прикладів «стимул-реакція» з метою визначення «реакції» для «стимулів», які не належать до наявної множини прикладів.
- Навчання без учителя (unsupervised learning) – моделі навчаються на основі непозначених даних, у яких відомі лише вхідні дані. Цей тип навчання використовується для задач кластеризації, зменшення розмірності та виявлення аномалій, де не відомі бажані вихідні дані.
- Підсилення (reinforcement learning) – це галузь машинного навчання, натхнена біхевіористською психологією, що вивчає питання про те, які дії (англ. actions) повинні виконувати програмні агенти в певному середовищі (англ. environment) задля максимізації деякого уявлення про сукупну винагороду (англ. reward).
- Передбачення (predictive learning) – моделі навчаються на основі зіставлення вхідних даних зі збереженими прикладами, щоб передбачати результати для нових вхідних даних. Цей тип навчання використовується для задач прогнозування, де необхідно передбачити майбутні значення на основі історичних даних. [3].

У випадку прогнозування запізнень громадського руху, застосовуються моделі машинного навчання з учителем, в яких вхідними даними є інформація про попередні маршрути та дані GPS, а вихідними даними – прогнозований час прибуття транспортного засобу на зупинку. На основі цих даних моделі навчаються передбачати, наскільки може затриматися рух транспорту на наступних зупинках, що допомагає уникнути запізнень та зробити транспортну систему більш ефективною. [4, с. 3-4].

За останні кілька років прогрес у галузі штучного інтелекту та машинного навчання дозволяє застосовувати їх для покращення ефективності транспортних систем. Один з головних проблем громадського транспорту – це запізнення рейсів, що може призвести до нестачі часу та стресу для пасажирів. Google зайнялася проблемою запізнення громадського

транспорту та розробила модель прогнозування запізнення автобусів з високою точністю, що базується на машинному навчанні та статистичних методах.

Сотні мільйонів людей у всьому світі щоденно користуються громадським транспортом для своєї робочої дороги, і понад половина всіх поїздок здійснюється автобусами. При зростанні міст у всьому світі, пасажири хочуть знати, коли очікувати затримки, особливо на автобусних маршрутах, які часто зупиняються у заторах. Хоча напрямки громадського транспорту, що надає Google Maps, інформуються багатьма транспортними агентствами, які надають дані в режимі реального часу, є багато агентств, які не можуть надати ці дані через технічні та ресурсні обмеження. Сьогодні Google Maps представив систему передбачення затримок на автобусні маршрути, що включає прогнозування затримок автобусів в сотнях міст у всьому світі, починаючи від Атланти до Загреба, до Стамбула, до Маніли та інших міст. Це поліпшує точність визначення часу громадського транспорту для понад шістдесяти мільйонів людей.

Приклад поїздки автобусом в середу після обіду у Сіднеї. Фактичний рух автобуса (синій) відстає від опублікованого розкладу (чорний) на декілька хвилин. Швидкості руху автомобільного трафіку (червоний) впливають на автобус, наприклад, сповільнення на відстані 2000 метрів, але довга зупинка на відстані 800 метрів суттєво уповільнює рух автобуса порівняно з автомобілем. [1].

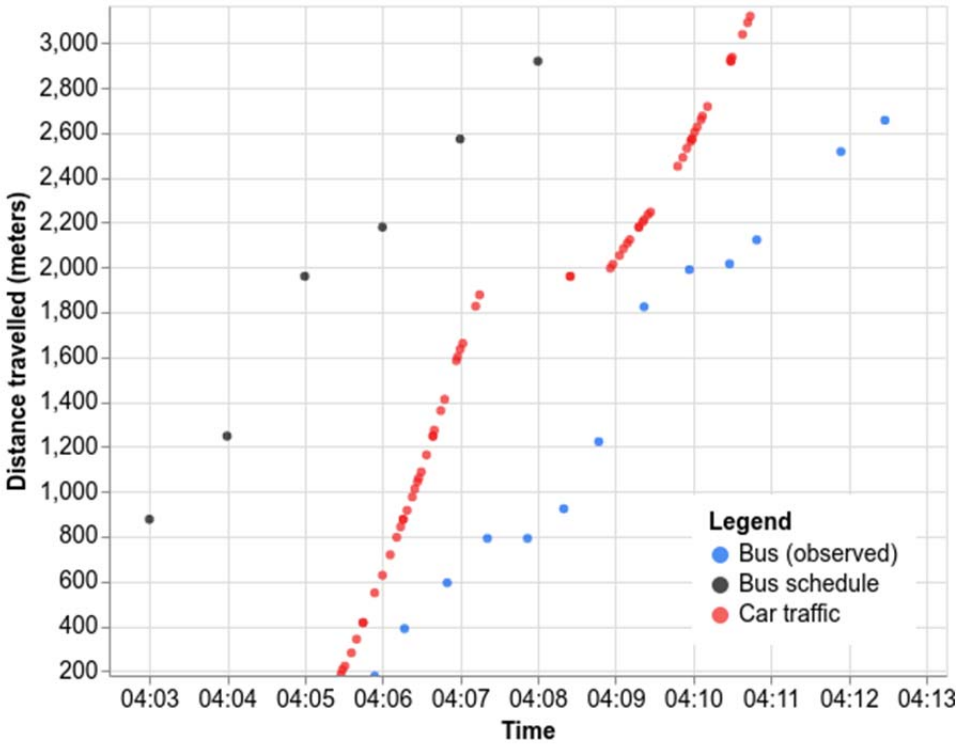

Рис. 1. Графік пройденої відстані в залежності від часу [1]

Для розробки моделі використовували тренувальні дані з послідовностей позицій автобусів в часі, які надходили з потоків реального часу транспортних агенцій, і відповідно до цього зв'язували їх зі швидкістю руху автомобільного трафіку на маршруті автобуса під час подорожі. Модель поділяється на послідовні одиниці часу, які відповідають кожному шматочку часової лінії автобуса, і кожна одиниця передбачає тривалість. Пара прилеглих спостережень зазвичай охоплює багато одиниць, через нерегулярність звітності, швидкість руху автобусів і короткі відрізки доріг і зупинок. Ця структура добре підходить для нейронних послідовних моделей, подібних до тих, що останнім часом успішно застосовуються у мовному процесінгу, машинному перекладі тощо. Ця модель є простішою.

Кожна одиниця передбачає свою тривалість незалежно, а кінцевий результат – сума передбачень для кожної одиниці. У відміну від багатьох послідовних моделей, ця модель не потребує вивчення комбінування виходів одиниць та передачі стану через послідовність одиниць. Замість цього, структура послідовності дозволяє навчити моделі тривалості окремих одиниць та оптимізувати «лінійну систему», де кожна спостережена траєкторія присвоює загальну тривалість сумі багатьох одиниць, які вона охоплює.

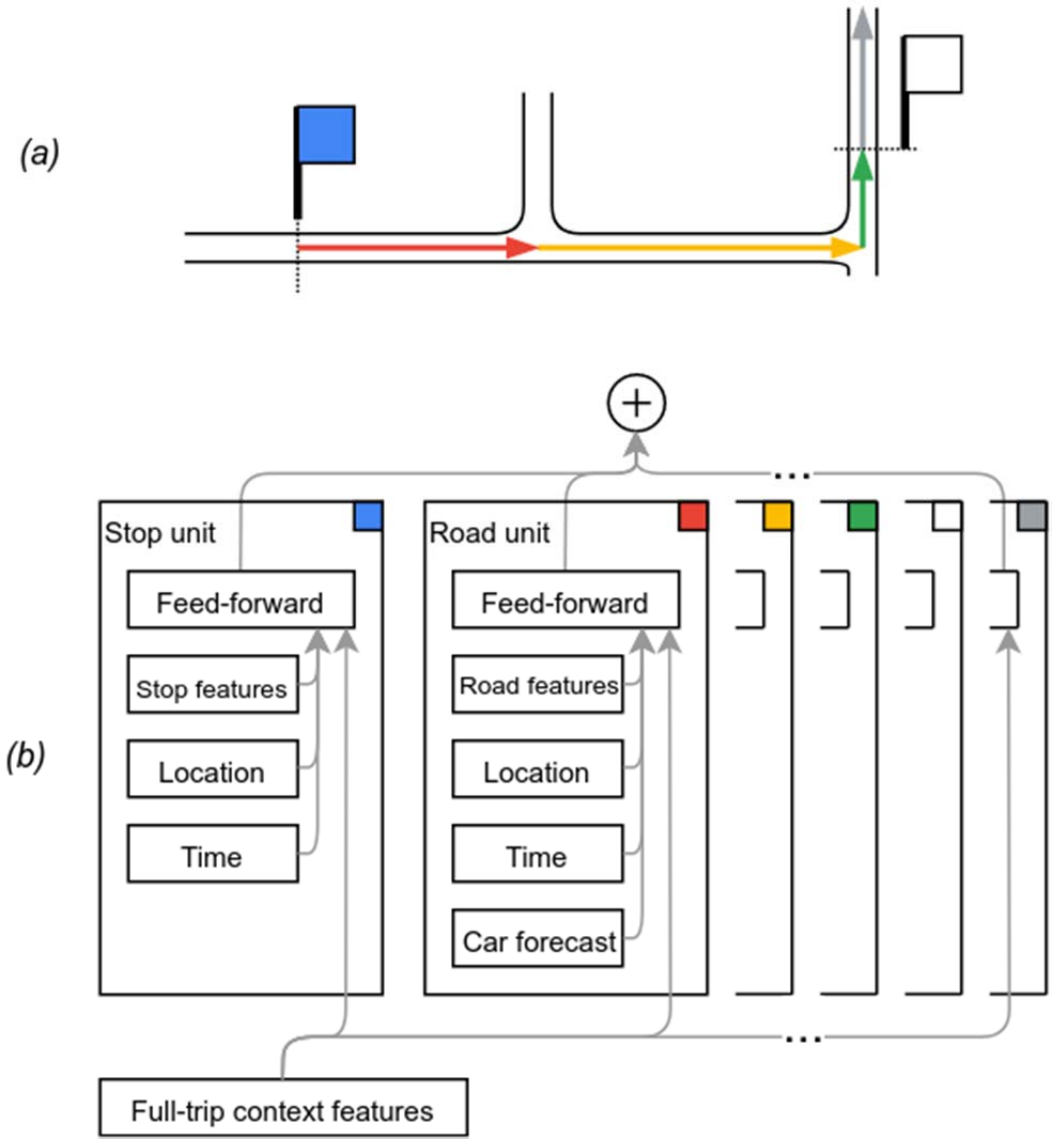

Рис. 2. Щоб змоделювати поїздку на автобусі (а), яка починається з синьої зупинки, модель (б) додає прогнози затримок з одиниці часової шкали для синьої зупинки, трьох ділянок дороги, білої зупинки тощо. [1]

З використанням комбінації даних про час, відстань та окремі події, штучний інтелект дозволяє Google надавати передбачення, не потребуючи розкладів автобусів, які надаються громадськими транспортними організаціями.

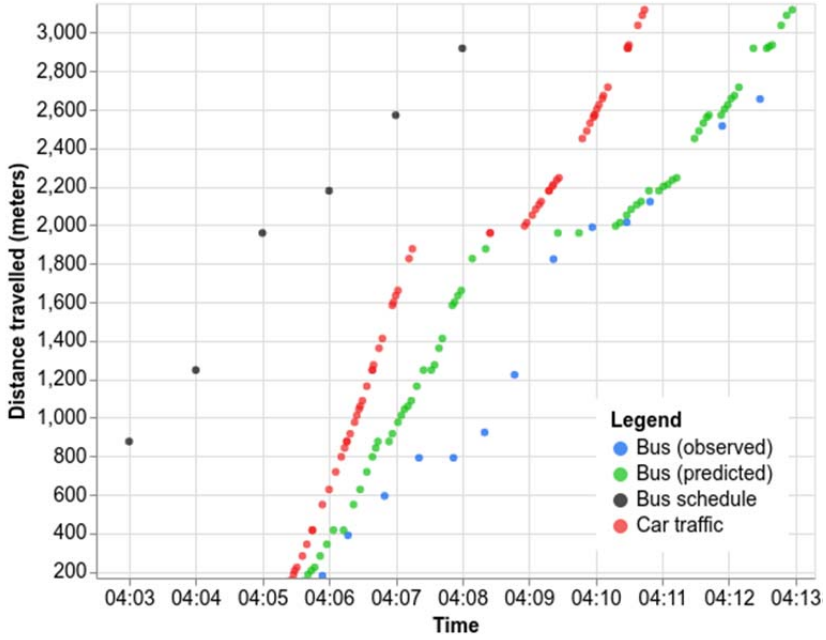

Рис. 3. Розклад автобусів(зелений колір). [1]

Для створення моделі збирається інформація про місцезнаходження автобусів від транспортних компаній для тренувальних даних, після чого вона узгоджується зі швидкістю руху автомобілів на маршруті. Потім послідовна модель враховує кожну очікувану зупинку або зниження швидкості, таку як час та відстань, необхідні для того, щоб автобус зменшив швидкість та зупинився біля зупинки.

Висновки. У цій статті машинне навчання використовується для покращення прогнозування тривалості подорожі автобусом. Розроблена модель використовує дані про позиції автобуса з часом, щоб передбачити тривалість подорожі на кожній вулиці та зупинці. Використання машинного навчання дозволило розробникам покращити точність прогнозування із залученням додаткових даних, які не були доступні раніше. Крім того, використання машинного навчання забезпечило більш гнучкий і ефективний підхід до прогнозування тривалості подорожі, що може бути корисним для підвищення якості громадського транспорту та зручності пасажирів.

Список використаних джерел

1. Google AI Blog: «Improving Public Transit Accessibility with Machine Learning»\\ Режим доступу:https://ai.googleblog.com/2019/08/improving-public-transit-accessibility.html
2. IEEE Xplore: «Enhancing the Accessibility of Public Transit with Machine Learning»\\ Режим доступу:https://ieeexplore.ieee.org/document/8683749
3. Cornell University Library: «Enhancing the Accessibility of Public Transit with Machine Learning»\\ Режим доступу: https://arxiv.org/abs/1908.02325
4. Матвійчук А., Шестопалов О. Машинне навчання. Загальний підхід. Київ: Видавництво «Ліра», 2019. ISBN 978-966-376-673-7.

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

РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗВ'ЯЗУВАННЯ ЗАДАЧ ВИЩОЇ МАТЕМАТИКИ НА ОСНОВІ АНАЛІЗУ СУЧАСНИХ ПЛАТФОРМ

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

У даній статті розглянуто сучасні платформи для розв'язання задач вищої математики. Проведено аналіз та порівняння платформ за різними критеріями, такими як доступність для мобільних пристроїв та людей з обмеженими можливостями. Було виявлено, що жодна з платформ не є ідеальною, але кожна має свої переваги та недоліки. На основі отриманих результатів, було сформульовано рекомендації щодо кращих практик розробки програмного забезпечення для розв'язування задач вищої математики. Також було проаналізовано основні функції, які повинна містити така платформа.

This article discusses modern platforms for solving higher mathematics problems. An analysis and comparison of the platforms was carried out according to various criteria, such as accessibility for mobile devices and people with disabilities. It was found that neither platform is perfect, but each has its advantages and disadvantages. Based on the obtained results, recommendations were formulated regarding the best practices of software development for solving higher mathematics problems. It also analyzed the main functions that such a platform should contain.

Актуальність. Використання програмного забезпечення для розв'язування математичних задач набуває все більшої популярності в сучасному світі. Університети та наукові установи активно використовують цей вид ПЗ для вирішення складних завдань вищої математики. Крім того, таке програмне забезпечення знайшло застосування в різних індустріях, таких як фінансові послуги, технічний дизайн та інженерія.

Отже, дана стаття є актуальною для широкого кола читачів, які зацікавлені в використанні програмного забезпечення для розв'язування математичних завдань різної складності, а також для тих, хто цікавиться розвитком технологій у цьому напрямку.

Метою статті є аналіз існуючих платформ для розв'язування задач вищої математики та визначення їхніх переваг та недоліків з урахуванням вимог щодо доступності для різних категорій користувачів, зокрема для людей з особливими потребами.

Об'єктом дослідження є платформи для розв'язування задач вищої математики.

Завдання статті полягає в наступному:

– проаналізувати різні платформи для розв'язування задач вищої математики, їх функціональні можливості, цільову аудиторію та особливості роботи з ними;

– визначити переваги та недоліки кожної платформи з урахуванням вимог щодо доступності для різних категорій користувачів;

– визначити найкращі практики для розробки програмного забезпечення для розв'язування задач вищої математики з урахуванням виявлених недоліків платформ, які використовуються на сьогоднішній день.

Математика – це наука, яка вимагає від людей великої уваги та точності. Розв'язування складних математичних задач може бути дуже важким завданням, тому багато людей звертаються до різних платформ, щоб отримати допомогу в цьому процесі. На сьогоднішній день існує багато різних інструментів, які допомагають вирішувати майже будь-яку математичну задачу.

Для початку, проаналізуємо декілька існуючих платформ для розв'язування задач з вищої математики, дослідимо їхні можливості та обмеження.

Платформа Wolfram Mathematica є однією з найбільш відомих платформ для розв'язування складних математичних задач. Вона розроблена для студентів, науковців, інженерів та інших фахівців, які працюють з математикою та комп'ютерними науками.

Wolfram Mathematica забезпечує розв'язування різних задач, включаючи чисельне та символьне розв'язування, обробку даних, графічний аналіз та візуалізацію. Це робить його одним з найпопулярніших інструментів для розв'язування математичних задач. Крім того, Wolfram Mathematica має інтегровані засоби для символьних обчислень, диференціальних рівнянь та функціонального аналізу [1].

Незважаючи на те, що Wolfram Mathematica є потужним інструментом для розв'язування складних математичних задач, він має деякі обмеження, які можуть зменшувати його ефективність і корисність для користувачів.

Одним з найбільших недоліків є висока вартість платформи, що робить її недоступною для багатьох користувачів, особливо студентів та молодих дослідників. Крім того, інтерфейс платформи може бути складним для користувачів, які не мають достатнього досвіду в роботі з програмним забезпеченням.

MATLAB – це платформа для зручної роботи з математичними обчисленнями та програмуванням, яка дозволяє розв'язувати системи рівнянь та інші математичні завдання. Ця платформа є однією з найбільш використовуваних у наукових дослідженнях, інженерному проектуванні та в інших областях, пов'язаних з математикою та комп'ютерними науками.

Однією з основних переваг MATLAB є його зручний інтерфейс, що дозволяє легко розробляти та запускати програми з математичними обчисленнями, використовуючи вбудовані функції та інструменти. Крім того, MATLAB має велику кількість додаткових пакетів та інструментів, що дозволяють розширювати його можливості та використовувати його для різних цілей, включаючи обробку сигналів, обробку зображень, моделювання та багато іншого.

MATLAB також має можливості для роботи з великими обсягами даних та високопродуктивними обчислювальними задачами, що робить його ідеальним вибором для багатьох наукових та інженерних досліджень [2].

Однак, MATLAB має деякі недоліки, включаючи високу вартість ліцензій, що може стати перешкодою для користувачів з обмеженим бюджетом. Крім того, MATLAB може бути менш ефективним для деяких видів математичних обчислень порівняно з іншими інструментами.

Mathway – це платформа для розв'язування математичних задач, яка спеціалізується на розв'язуванні алгебраїчних, геометричних та інших математичних задач. Вона має багато корисних функцій, таких як відображення кроків розв'язання задачі, що допомагає користувачам зрозуміти процес розв'язання та покращити свої знання в математиці.

Mathway доступна на комп'ютерах та мобільних пристроях, що дозволяє користувачам користуватися платформою в будь-який час та в будь-якому місці. Також, Mathway може бути корисною для людей з обмеженими можливостями, оскільки має можливість користування платформою для людей з вадами зору та іншими особливостями.

Одним з недоліків Mathway є те, що для доступу до деяких функцій потрібна платна підписка. Крім того, Mathway не має такої великої кількості функцій, які є у більш широких платформ, таких як Wolfram Mathematica або MATLAB.

GeoGebra – це додаток, який дозволяє користувачам виконувати різноманітні математичні операції та розв'язувати задачі. Додаток має широкий спектр функцій, включаючи побудову графіків, обчислення похідних та інтегралів, розв'язування рівнянь та систем рівнянь. Окрім цього, GeoGebra дозволяє створювати власні математичні об'єкти та використовувати їх для розв'язання задач. Додаток має інтуїтивний інтерфейс та може бути використаний як на комп'ютерах, так і на мобільних пристроях [3].

GeoGebra має певну адаптацію для людей з особливими потребами. На сайті платформи є можливість вибрати темний фон та збільшити розмір тексту, що полегшує

користування додатком людям з вадами зору. Крім того, GeoGebra має функцію для збільшення об’єктів на екрані, що полегшує роботу людям зі зниженою здатністю до моторики. Також, є можливість додавання аудіо та відео-коментарів до створених математичних об’єктів, що забезпечує доступність для людей зі зниженим слухом. Хоча додаток не має спеціальної адаптації для людей з особливими потребами, деякі функції додатку можуть бути корисними для покращення доступності для людей з вадами зору, слуху та моторики.

Однак, GeoGebra має деякі недоліки. Наприклад, додаток може бути менш ефективним для розв’язання деяких складних математичних задач, порівняно з іншими спеціалізованими додатками. Крім того, для користувачів без попереднього досвіду з математикою, додаток може бути складним у використанні.

Загалом, GeoGebra є корисним додатком для студентів, викладачів та інших користувачів, які займаються математикою. Додаток має великий потенціал для використання в навчанні та розв’язуванні різних математичних задач.

Symbolab є потужною та зручною платформою для розв’язування математичних задач, яка надає користувачам широкий спектр інструментів. Зокрема, на платформі можна відображати графіки, обчислювати похідні та інтеграли, розв’язувати системи рівнянь та багато іншого. Крім того, Symbolab має спеціалізовані функції для розв’язування складних математичних задач, таких як вирішення лінійних диференціальних рівнянь [4]. Платформа доступна на комп’ютерах та мобільних пристроях.

Однак, Symbolab має свої недоліки. Розв’язання деяких складних математичних задач може бути менш точним порівняно з альтернативними платформами. Також важко використовувати платформу для користувачів, які не мають попереднього досвіду з математикою та розв’язанням математичних задач. Важливо зазначити, що Symbolab не адаптована для користувачів з особливими потребами, такими як вади зору та інші обмеження.

Після дослідження різних платформ для розв’язування задач вищої математики, можна зробити висновок, що жодна з них не є ідеальною. Деякі з них забезпечують велику кількість функцій, але не є дуже зручними у використанні, інші мають простий інтерфейс, але не мають достатньої функціональності.

Також не всі проаналізовані платформи можуть бути зручними для користувачів з вадами зору або нездатністю користуватися мишкою. Для забезпечення максимальної доступності для користувачів з різними потребами, важливо враховувати їхні потреби при розробці інтерфейсів платформ.

В результаті дослідження були визначені кращі практики, які можуть бути використані для розробки ПЗ для розв’язування задач вищої математики. Основними критеріями, на які варто звернути увагу при створенні програмного забезпечення для розв’язування задач вищої математики, є:

– Зручність використання. Програмне забезпечення має бути легким у використанні та зрозумілим для користувача, незалежно від його рівня кваліфікації.

– Функціональність та можливості. Програмне забезпечення повинно мати всі необхідні можливості для розв’язування задач вищої математики.

– Доступність для мобільних гаджетів. Зважаючи на те, що все більше користувачів використовують мобільні пристрої, важливо забезпечити доступність програмного забезпечення на таких пристроях.

– Доступність для людей з особливими потребами. Програмне забезпечення повинно бути зручним у використанні для людей з різними вадами зору та здатності до користування мишкою.

Основною метою розробки програмного забезпечення є спрощення роботи з вищою математикою для користувачів різного рівня знань та кваліфікації. Пріоритетом є простота та зрозумілість інтерфейсу, які дозволять користувачам швидко та ефективно вирішувати математичні задачі. Важливими аспектами є надійність та точність отримуваних результатів,

а також підтримка користувачів та допомога у вирішенні проблем, що виникають під час використання програми [5].

Розробка майбутнього програмного забезпечення буде здійснюватися з використанням мови програмування Python. Вона є однією з найбільш популярних мов програмування для розробки програмного забезпечення, особливо в галузі математичного моделювання. Її легкість вивчення та простота використання дозволяють розробникам швидко створювати ефективне програмне забезпечення для розв'язування складних математичних задач.

Крім того, Python має велику кількість бібліотек та фреймворків, що дозволяє розробникам ефективно використовувати готові рішення для розв'язування задач з різних галузей математики та науки.

Наприклад, бібліотека NumPy дозволяє працювати з масивами даних та виконувати різні математичні операції, а бібліотека Matplotlib дозволяє візуалізувати дані та результати розрахунків у вигляді графіків та діаграм.

Також, бібліотека SciPy надає інструменти для розв'язування різноманітних наукових та інженерних задач, включаючи оптимізацію, інтерполяцію, інтегрування та обробку сигналів. Бібліотека SymPy, з іншого боку, надає можливості символьного обчислення, що дозволяє виконувати складні математичні операції з використанням символів та формул. Ці бібліотеки дозволяють розробникам ефективно використовувати готові рішення та зосередитися на розв'язуванні самої математичної задачі [6].

Забезпечення доступності для мобільних гаджетів є необхідним етапом у розробці програмного забезпечення для вирішення математичних задач. Користувачі зможуть використовувати додаток на своєму смартфоні чи планшеті в будь-який момент часу та в будь-якому місці, що дозволить їм бути більш продуктивними та ефективними.

Крім того, доступність додатку для мобільних гаджетів може збільшити його популярність та залучити нових користувачів. На сьогоднішній день, мобільні пристрої стали необхідними елементами нашого життя, і більшість людей використовують їх для доступу до різноманітних сервісів та додатків. Головною метою є забезпечення максимальної доступності та зручності для користувачів. Додаток повинен легко знаходитися та завантажуватися з мобільних магазинів додатків, а також мати інтуїтивно зрозумілий та зручний інтерфейс для користувачів.

Важливим елементом розробки програмного забезпечення є його документація та підтримка користувачів. Детальна та зрозуміла документація дозволяє користувачам ознайомитися з можливостями програмного забезпечення та швидко розв'язати свої задачі. Підтримка користувачів від розробників дозволяє швидко відповідати на запитання та проблеми користувачів, а також вдосконалювати програмне забезпечення з урахуванням їхніх вимог та пропозицій.

Розглядається можливість впровадження режиму для людей з обмеженими можливостями, що забезпечить доступність програми для користувачів з різними потребами. Наприклад, можна розробити спеціальний інтерфейс для людей з вадами зору або низькою моторикою, який дозволить користувачам взаємодіяти з програмою без перешкод. Також можна впровадити інтерфейс з голосовим керуванням для людей з вадами зору або використовувати штучний інтелект для розпізнавання голосових команд.

Крім того, конкурентні ціни на платформу сприятимуть привабливості продукту для широкого кола користувачів. Низькі витрати на використання програмного забезпечення зроблять його доступним для великої кількості людей, включаючи невеликі компанії та стартапи з обмеженим бюджетом.

Безпека та надійність програмного забезпечення буде забезпечуватися конфіденційністю користувачів. Запобігання витоку даних та забезпечення приватності користувачів – це одні з головних пріоритетів розробників програмного забезпечення, що забезпечить надійність та довіру до продукту.

Для досягнення високої продуктивності програми та зручного інтерфейсу користувача необхідно поєднати різні технології та методи, що сприятимуть оптимальним результатам та комфортній роботі користувачів з програмним забезпеченням.

Загалом, створення програмного забезпечення для розв'язування задач вищої математики – це складний та багатоаспектний процес, який вимагає від розробників глибоких знань та уваги до деталей. Проте, якщо правильно підійти до цього процесу, можна створити високоякісне програмне забезпечення, яке допоможе користувачам розв'язувати складні математичні задачі з максимальною продуктивністю та ефективністю.

Висновки. Було проведено аналіз декількох платформ для розв'язання математичних задач, і встановлено, що кожна з них має певні переваги та обмеження.

Серед найбільш популярних платформ можна виділити Wolfram Mathematica, Symbolab, Mathway та GeoGebra. Wolfram Mathematica є дуже потужним інструментом, здатним розв'язувати складні математичні задачі, проте інтерфейс платформи може бути складним для користувачів без відповідного досвіду роботи з програмним забезпеченням.

Symbolab є більш детальним та зрозумілим інструментом, проте розв'язання деяких складних математичних задач може бути менш точним порівняно з альтернативними платформами. Платформа Mathway має багато корисних функцій, таких як візуалізація кроків розв'язання задачі, проте вона має обмежену функціональність у безкоштовній версії.

GeoGebra популярна платформа, яка поєднує в собі широкий спектр функцій та інструментів для виконання різних операцій з математикою, включаючи графіки, геометрію та алгебру. Недоліком GeoGebra є обмежена потужність та функціональність порівняно з такими платформами як Wolfram Mathematica. Вона менш адаптована для розв'язання складних задач та не має такої широкої бібліотеки інструментів. Крім того, GeoGebra не підтримує такий широкий спектр типів розв'язання задач, як Symbolab або Mathway.

Для розробки програмного забезпечення щодо розв'язання математичних задач було б доцільно використати кращі практики з кожної платформи. Наприклад, користувачам потрібно бачити детальні розв'язання задач для розуміння шляху досягнення відповіді. Крім того, розробникам програмного забезпечення варто звернути увагу на важливість його доступності для людей з обмеженими можливостями. Також варто розглянути можливість створення мобільного додатку для зручності користувачів.

Отже, програмне забезпечення для розв'язання математичних задач повинно бути потужним та детальним, зрозумілим та доступним, а також забезпечувати можливість візуалізації та розв'язання різних типів задач. Крім того, його інтерфейс має бути інтуїтивно зрозумілим та простим у використанні для різних категорій користувачів.

Список використаних джерел

1. Wolfram Mathematica. – 2023. [Електронний ресурс]. – Режим доступу : https://www.wolfram.com/mathematica/index.php.en?source=footer
2. MathWorks. – 2023. [Електронний ресурс]. – Режим доступу : https://www.mathworks.com/products/matlab.html
3. GeoGebra – 2023. [Електронний ресурс]. – Режим доступу : https://www.geogebra.org/calculator
4. Symbolab – 2023. [Електронний ресурс]. – Режим доступу : https://www.symbolab.com
5. Величко В. Є. Вільне програмне забезпечення в електронному навчанні майбутніх учителів математики, фізики та інформатики. – 2021. [Електронний ресурс]. – Режим доступу : https://www.researchgate.net/publication/331469364_VILNE_PROGRAMNE_ZABEZPECENNA_V_ELEKTRONNOMU_NAVCANNI_MAJBUTNIH_UCITELIV_MATEMATIKI_FIZIKI_TA_INFORMATIKI
6. Jake VanderPlas. Python Data Science Handbook. – 2016. [Електронний ресурс]. – Режим доступу : https://jakevdp.github.io/PythonDataScienceHandbook/

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

АНАЛІЗ ТЕХНОЛОГІЙ ТА МЕТОДІВ РЕКОМЕНДАЦІЙ ВІДЕОКОНТЕНТУ

ПШЕНИШНИЙ П., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Відео контент – важлива частина нашого життя, і рекомендаційні системи допомагають нам знайти контент, який нас цікавить. Netflix – провідна компанія, що використовує машинне навчання та аналіз даних для рекомендацій відео контенту. У статті ми розглянемо, як Netflix та інші компанії використовують рекомендаційні системи відео контенту та як ці системи впливають на наші споживацькі звички.

Video content is an essential part of our lives, and recommendation systems help us find content that interests us. Netflix is a leading company that uses machine learning and data analysis for video content recommendations. In this article, we will discuss how Netflix and other companies use video content recommendation systems and how these systems affect our viewing habits.

Актуальність. З розвитком інтернету та цифрових технологій відео контент став невід'ємною частиною нашого життя. Згідно з даними, відео контент став одним з найбільш популярних форматів онлайн контенту, зокрема на YouTube щодня переглядається більше мільярда годин відео. Проте, зростає конкуренція серед компаній, які надають відео контент, і важливим є не лише створення цікавого та якісного контенту, але й залучення та утримання аудиторії.

У цьому контексті рекомендаційні системи відео контенту стають ключовим інструментом для залучення та утримання аудиторії. Вони допомагають користувачам знайти контент, який їх цікавить, та сприяють збільшенню кількості переглядів відео контенту. Компанії, які надають відео контент, активно використовують рекомендаційні системи, щоб залучити нових користувачів та зберегти існуючих.[1,с.2-3]

Однією з провідних компаній, яка використовує рекомендаційні системи відео контенту, є Netflix. Ця компанія зарекомендувала себе як лідер у своїй галузі завдяки високому рівню персоналізації та індивідуалізації рекомендаційного алгоритму. Netflix використовує машинне навчання та аналіз даних, щоб збирати та обробляти інформацію про користувачів та їх поведінку. На основі цих даних компанія створює індивідуальні рекомендації для кожного користувача, що робить досвід перегляду відео на Netflix більш приємним та зручним.

Метою статті дослідження технологій та методів, що використовуються в рекомендаційних системах відео контенту, з основним фокусом на підходах, які застосовує компанія Netflix.

Об'єктом дослідження є технології та методи рекомендації відео контенту в рекомендаційних системах, з основним фокусом на Netflix.

Предмет дослідження – аналіз технологій та методів рекомендації відео контенту, які використовуються в різних рекомендаційних системах, з урахуванням особливостей підходів, які використовує компанія Netflix.

Аналіз попередніх досліджень. Попередні дослідження показали важливість технологій та методів рекомендації відео контенту для користувачів і платформ відеострімінгу, таких як Netflix, YouTube і Amazon Prime Video. Наприклад, дослідження компанії Netflix, яке було опубліковано в 2016 році, вказує на те, що понад 75% переглянутих фільмів та серіалів на платформі були віднайдені завдяки рекомендаціям. Інше дослідження, проведене університетом Carnegie Mellon, показало, що удосконалення алгоритмів рекомендацій може покращити задоволення користувачів від контенту на 7-8%.

Виклад основного матеріалу.

Відео контент зараз є однією з провідних форм розваг і навчання. Залежно від платформи, яку вони використовують, провайдери відео контенту застосовують різні технології та методи рекомендацій для залучення користувачів. Одним із таких прикладів є Netflix, який використовує різні технології та методи рекомендацій для збільшення кількості переглядів відео контенту та покращення користувацького досвіду.

Рис. 1. Рекомендаційна система Netflix та Big data [2]

Netflix використовує комбінацію різних методів для рекомендації відео контенту; основні методи, які використовує Netflix, включають колаборативну фільтрацію, рекомендації на основі контенту, глибинне навчання та інтерактивні рекомендації.

Колаборативна фільтрація – це рекомендаційна технологія, що базується на аналізі даних про взаємодію користувачів з контентом і використовується в різних секторах, таких як електронна комерція, соціальні мережі, музика та кіноіндустрія. У випадку Netflix колаборативна фільтрація використовується для аналізу даних про взаємодію користувачів з відео контентом, таких як рейтинги, відгуки та перегляди. На основі цих даних Netflix може зрозуміти, який контент користується найбільшою популярністю серед користувачів і які фактори впливають на їхній вибір. Існує два типи спільної фільтрації: на основі користувачів і на основі об’єктів.

У випадку фільтрації на основі користувача Netflix аналізує поведінку користувача і порівнює її з поведінкою інших користувачів, які мають схожі інтереси. Наприклад, якщо поведінка користувача А і користувача В дуже схожа, ймовірно, що рекомендації, які відповідають користувачеві В, також будуть відповідати користувачеві А.

У випадку об’єктно-орієнтованого підходу Netflix аналізує схожість між різним відео контентом і рекомендує користувачам контент, схожий на той, що їм вже подобається. Наприклад, якщо користувачеві дуже подобається певний фільм, йому можуть бути рекомендовані фільми зі схожими темами, жанрами або акторами.

Колаборативна фільтрація може бути ефективним способом рекомендувати відео контент, оскільки вона враховує вподобання та інтереси кожного користувача. Однак колаборативна фільтрація також має певні обмеження. Одним з обмежень є проблема «холодного старту», яка виникає, коли користувачі є новачками на платформі і не мають достатньо даних про свою поведінку для надання точних рекомендацій. Щоб подолати цю проблему, Netflix використовує такі методи, як рекомендації на основі популярності контенту, рекомендації на основі контенту та глибинне навчання. Крім того, колаборативна фільтрація вразлива до певних типів атак, таких як атаки з несправжніми користувачами (sybil attacks) та маніпуляційні атаки, які можуть спотворювати рекомендації та впливати на поведінку користувачів. Загалом, колаборативна фільтрація є ефективним і широко використовуваним методом рекомендації відео контенту, який дозволяє Netflix надавати користувачам персоналізований і цікавий контент. Однак він має обмеження і потребує постійного вдосконалення технологій і методів аналізу даних, щоб максимізувати точність рекомендацій.

Рекомендації на основі контенту – це метод рекомендацій, який використовує Netflix. Платформа аналізує відео контент, який подобається користувачам, і рекомендує контент зі схожим змістом. Рекомендації на основі вмісту можуть враховувати такі фактори, як жанр, акторський склад, характеристики режисера та тематика відео контенту. Netflix використовує підхід рекомендацій на основі контенту, щоб рекомендувати фільми та телешоу, які можуть сподобатися користувачам. Компанія аналізує якості контенту, який користувачі переглянули або високо оцінили, і рекомендує схожий контент. Наприклад, якщо користувач дивиться багато комедійних фільмів, Netflix порекомендує йому інші комедійні фільми та телешоу. Крім того, Netflix також аналізує поведінку користувачів, наприклад, коли вони дивляться контент, і використовує цю інформацію для надання рекомендацій. Наприклад, якщо користувач дивиться фільм вночі, платформа може порекомендувати фільми або драми з нічною атмосферою. Зокрема, Netflix використовує алгоритмічну систему рекомендацій під назвою «Cinematch», яка аналізує попередні вибори та оцінки користувачів для надання рекомендацій. Система також включає машинне навчання, наприклад, технологію глибокого навчання. Загалом, рекомендації на основі контенту – це ефективний підхід до надання контенту, який користувачам може бути цікаво переглянути. Такі рекомендації дозволяють користувачам мати більш персоналізований досвід перегляду.

Глибинне навчання – це метод, який використовує Netflix для покращення рекомендацій, використовуючи інформацію про перегляд та поведінку на платформі. Netflix використовує нейронні мережі для аналізу поведінки користувачів та рекомендації відео контенту. Глибинне навчання допомагає Netflix зрозуміти, що привертає увагу користувачів і які фактори впливають на їхній вибір відео. Ця техніка може автоматично виявляти складні взаємозв’язки між вхідними та вихідними даними. У випадку з Netflix глибинне навчання використовується для аналізу великих обсягів даних відео контенту та інформації про користувачів, щоб зрозуміти, які фактори впливають на вибір користувачів. Наприклад, глибинне навчання можна використовувати для автоматичного виявлення закономірностей у поведінці користувачів, таких як перегляди відео, рейтинги та відгуки. За допомогою глибинного навчання Netflix може адаптувати рекомендації до конкретних інтересів і поведінки кожного користувача. Однією з переваг глибинне навчання є те, що воно може автоматизувати багато процесів, які раніше вимагали багато ручної роботи. Наприклад, використовуючи глибинне навчання для автоматичного відбору та категоризації великих обсягів відео контенту, Netflix може значно збільшити кількість контенту, доступного для користувачів. У світі, де обсяг доступного відео контенту стрімко зростає, глибинне навчання може дозволити Netflix залишатися конкурентоспроможним, дозволяючи швидко і ефективно аналізувати великі обсяги даних і надавати користувачам персоналізовані рекомендації щодо контенту.

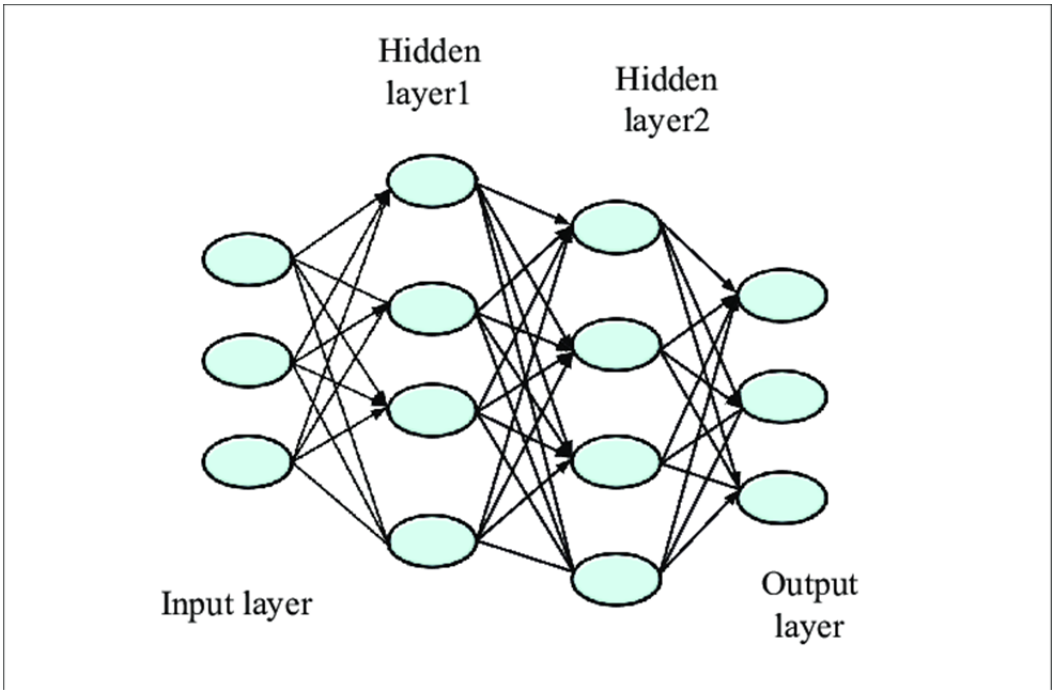

Рис. 2. Базова структура глибокої нейронної мережі [*3*]

Інтерактивні рекомендації – це новий підхід до алгоритмів рекомендацій, який дозволяє користувачам взаємодіяти з рекомендованим контентом і вказувати свої вподобання, підвищуючи точність рекомендацій і покращуючи користувацький досвід. Наприклад, Netflix може запитувати користувачів про їхній настрій та емоції і рекомендувати відео контент, який може відповісти на ці запитання. Інтерактивні рекомендації – це новий підхід до алгоритмів рекомендацій, який дозволяє користувачам взаємодіяти з рекомендованим контентом і вказувати свої вподобання, підвищуючи точність рекомендацій і покращуючи користувацький досвід. Netflix вперше представив інтерактивні рекомендації у фільмі «BlackMirror:Bandersnatch», який вийшов на екрани у 2017 році. Це був інтерактивний проект, який дозволяв глядачам впливати на історію, обираючи поведінку головного героя. На основі реакції глядачів Netflix міг запропонувати подальші варіанти сюжету та надати персоналізовані рекомендації.

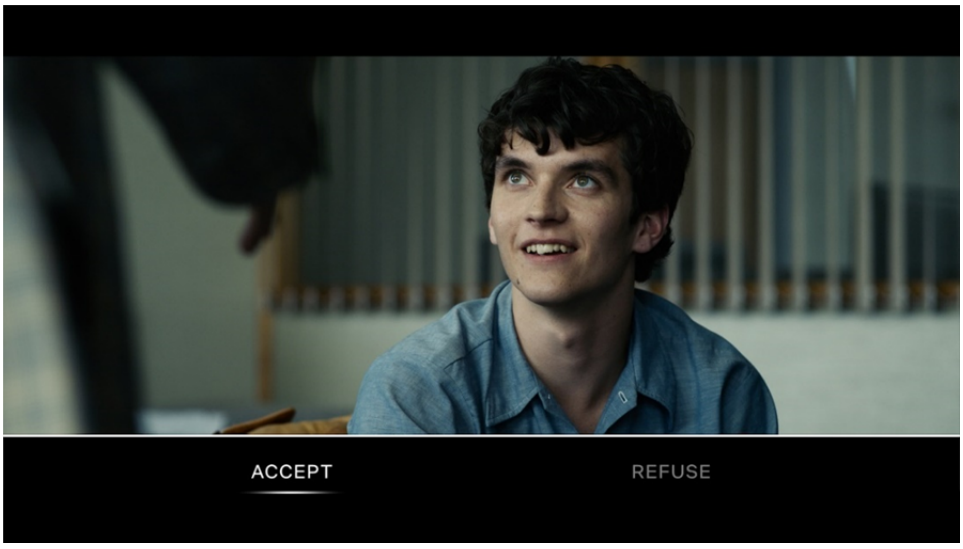

Рис. 3. Приклад інтерактивної рекомендації у фільмі.

Після успіху «Bandersnatch» Netflix продовжив поширювати інтерактивність на інші фільми та серіали, дозволяючи глядачам взаємодіяти з пропонованим контентом і обирати власну сюжетну лінію. Це дозволяє Netflix збирати більше даних про вподобання та інтереси користувачів, що дає змогу надавати більш точні та персоналізовані рекомендації. Інтерактивні рекомендації також включають елемент експериментів спільноти для моніторингу реакції користувачів на новий контент і збору відгуків, що допоможе вдосконалити алгоритми рекомендацій і надавати кращі рекомендації в майбутньому.

Окрім методів і прийомів надання рекомендацій, Netflix також використовує надану користувачем інформацію про нього для надання персоналізованих рекомендацій. Наприклад, Netflix збирає дані про вподобання користувачів, а також інформацію про вік, стать і географічне розташування для надання персоналізованих рекомендацій.

Таким чином, Netflix використовує різні технології та методи рекомендацій, щоб залучити користувачів і покращити їхній досвід. Поєднуючи такі методи рекомендацій, як спільна фільтрація, рекомендації на основі контенту, глибинне навчання та інтерактивні рекомендації, Netflix може надавати персоналізовані рекомендації щодо відео контенту для кожного користувача.

Компанія постійно вдосконалює свої технології та методи рекомендацій, щоб забезпечити найкращий користувацький досвід. Наприклад, у 2020 році Netflix запустив нову функцію Top 10, яка показує 10 найпопулярніших відео контенту на локальному ринку користувача. Це полегшує користувачам пошук нових шоу та фільмів, які користуються популярністю серед інших користувачів у їхньому регіоні. Крім того, Netflix також використовує відео аналітику та машинне навчання для аналізу відео контенту та підбору його відповідно до інтересів користувачів, аналізує зв'язок між жанрами та темами, щоб надавати користувачам персоналізовані рекомендації, аналізує користувацький досвід під час перегляду відео контенту, щоб зрозуміти, які елементи контенту приваблюють глядачів і як їх можна покращити в майбутньому [3].

Висновки. Технології та методи рекомендації відео контенту є ключовими для відеоплатформ, таких як Netflix, які стикаються з великою кількістю контенту та зростаючими очікуваннями користувачів. Рекомендаційні системи, які використовуються на таких платформах, базуються на складних алгоритмах та машинному навчанні, що дозволяє їм надавати користувачам персоналізовані рекомендації та поліпшувати загальне задоволення від контенту. Дослідження показують, що удосконалення цих технологій може покращити якість рекомендацій та задоволення користувачів від перегляду відео контенту.

Список використаних джерел

1. Bansal, R., & Saini, R. (2021). A Hybrid Recommendation Algorithm Using Association Rule Mining and Collaborative Filtering. Complexity, 2021, 1-13. c: 10.1155/2021/8875700
2. Smith, J. Building a Netflix Recommendation System. Analytics Vidhya. https://medium.com/analytics-vidhya/building-a-netflix-recommendation-system-7b1fec90f83e.
3. ResearchGate. (n.d.). The basic structure of the deep neural network (DNN). Retrieved, from https://www.researchgate.net/figure/The-basic-structure-of-the-deep-neural-network-DNN_fig1_355756076
4. Іваницький, А., Маруняк, І., & Хом'як, І. (2019). Розвиток рекомендаційних систем в онлайн-сервісах: приклад Netflix. Маркетинг і менеджмент інновацій, (4), 68-75. https://doi.org/10.21272/mmi.2019.4-06

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

АСПЕКТНО-ОРІЄНТОВАНЕ ПРОГРАМУВАННЯ ДЛЯ ПОЛІПШЕННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

РИБКІН Я., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті досліджується застосування аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури. Відзначається, що мікросервісна архітектура є потужним інструментом для розробки та підтримки програмного забезпечення. Однак, вона також може бути складною для розуміння та підтримки через велику кількість компонентів, що можуть змінюватись динамічно. Аспектно-орієнтоване програмування надає зручний спосіб для розділення перехресних аспектів в програмному забезпеченні та забезпечення їх незалежної розробки та підтримки. У статті розглядаються основні принципи аспектно-орієнтованого програмування, його застосування в мікросервісній архітектурі та приклади реалізації.

The article explores the use of aspect-oriented programming to enhance microservices architecture. Microservices architecture is a powerful tool for developing and maintaining software, but it can also be complex to understand and maintain due to the large number of components that can change dynamically. Aspect-oriented programming provides a convenient way to separate cross-cutting concerns in software and ensure their independent development and maintenance. The article discusses the basic principles of aspect-oriented programming, its application in microservices architecture, and examples of implementation.

Актуальність. У сучасному світі інформаційних технологій, мікросервісна архітектура стала ключовою стратегією для будівництва гнучких та масштабованих програмних додатків. Ця архітектурна парадигма передбачає розбиття складних додатків на невеликі, незалежні компоненти, що спрощує розробку, розгортання та обслуговування. Однак, при рості розміру та складності мікросервісних систем виникає низка викликів, пов'язаних зі збереженням їхньої ефективності, розширюваністю та управлінням.

Розробка програмного забезпечення на основі мікросервісної архітектури є однією з найбільш популярних практик в індустрії програмного забезпечення. Проте, розробка та підтримка мікросервісної архітектури може бути важкою через складність зв'язків між компонентами та змінність архітектури. Одним з підходів для зменшення складності мікросервісної архітектури є застосування аспектно-орієнтованого програмування. Цей підхід дозволяє зменшити залежності між різними частинами програмного забезпечення та забезпечити більшу гнучкість та модульність.

Метою даної статті є дослідження можливості використання аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури. Ми дослідимо, як застосування аспектно-орієнтованого програмування дозволяє зменшити складність мікросервісної архітектури та забезпечити більшу гнучкість та модульність програмного забезпечення. Ми також розглянемо основні принципи аспектно-орієнтованого програмування та приклади його застосування в мікросервісній архітектурі.

Для досягнення мети було поставлено наступні завдання:

- проаналізувати поняття аспектно-орієнтованого програмування та мікросервісної архітектури;
- розглянути можливості використання аспектно-орієнтованого програмування для зменшення залежностей між різними компонентами мікросервісної архітектури;
- дослідити застосування аспектно-орієнтованого програмування для забезпечення безпеки та моніторингу мікросервісної архітектури;

- порівняти підходи, що використовують аспектно-орієнтоване програмування, з іншими підходами, які застосовуються для поліпшення мікросервісної архітектури;
- зробити висновки щодо ефективності використання аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури.

Об'єктом дослідження є мікросервісна архітектура, яка є популярним підходом для розробки програмного забезпечення.

Предметом дослідження є застосування аспектно-орієнтованого програмування для поліпшення мікросервісної архітектури.

Аналіз попередніх досліджень. Раніше дослідження показали, що мікросервісна архітектура може бути складною в розробці та підтримці через залежності між різними компонентами. Застосування аспектно-орієнтованого програмування може допомогти зменшити ці залежності та забезпечити більшу гнучкість та модульність програмного забезпечення.

У дослідженні, проведеному Дж. Гу та його колегами (2018), автори запропонували використання аспектно-орієнтованого програмування для забезпечення моніторингу та аналізу мікросервісної архітектури. Аспекти використовувалися для збору метрик та статистики від різних компонентів системи, що дозволило покращити моніторинг та аналіз архітектури.

У дослідженні, проведеному Б. Штулецом та його колегами (2017), автори досліджували застосування аспектно-орієнтованого програмування для забезпечення безпеки в мікросервісній архітектурі. Аспекти використовувалися для виконання додаткових перевірок безпеки при виконанні різних операцій, що дозволило забезпечити більшу безпеку програмного забезпечення.

Обидва дослідження показують можливості застосування аспектно-орієнтованого програмування для поліпшення різних аспектів мікросервісної архітектури, що підтверджує актуальність нашої статті та мотивує дослідження даного підходу детальніше.

Виклад основного матеріалу. Мікросервісна архітектура є однією з найпопулярніших архітектурних підходів в програмному забезпеченні. Вона спрощує процес розробки, деплою та масштабування складних систем. Однак, при збільшенні кількості мікросервісів, архітектура може стати складною для управління та розуміння.

Аспектно-орієнтоване програмування (АОП) – це методологія програмування, що дозволяє виділяти спільні аспекти програми та використовувати їх для поліпшення якості та керованості програмного коду. Використання АОП для поліпшення мікросервісної архітектури може допомогти зменшити складність та зробити архітектуру більш модульною та керованою.

У даній статті ми розглянемо основні поняття АОП та його використання для поліпшення мікросервісної архітектури.

Першим кроком до використання АОП для поліпшення мікросервісної архітектури є розбиття мікросервісів на аспекти. Для цього можна проаналізувати функціональність кожного мікросервісу та виділити спільні аспекти, які можна використати для поліпшення керованості та якості коду.

Наприклад, мікросервіс, що відповідає за обробку замовлень, може мати спільну функціональність з мікросервісом, що відповідає за обробку платежів. Ці спільні аспекти можуть бути використані для реалізації більш керованої та якісної функціональності.

Після розбиття мікросервісів на аспекти можна використовувати поради для поліпшення їх функціональності та якості коду. Наприклад, можна використовувати передпоради для перевірки вхідних даних та забезпечення їх правильної ініціалізації. Також можна використовувати післяпоради для обробки результатів виконання та очищення даних. Навколопоради можуть використовуватись для обробки виключень та забезпечення правильної обробки даних.

Для використання АОП можна також використовувати анотації, які дозволяють позначати код для застосування певних порад. Анотації можуть бути використані для позначення методів або класів, які мають бути покриті певними порадами.

Наприклад, можна використовувати анотації для позначення методів, які мають бути покриті передпорадами для перевірки вхідних даних. Це дозволяє забезпечити правильну ініціалізацію даних та зменшити ризик помилок при виконанні методів.

Для використання АОП для поліпшення мікросервісної архітектури можна також використовувати зв'язки між аспектами. Зв'язки можуть бути використані для забезпечення правильної взаємодії між різними аспектами та їх правильного виконання.

Наприклад, можна використовувати зв'язки для забезпечення правильної взаємодії між мікросервісами, що відповідають за обробку замовлень та платежів. Це дозволяє забезпечити правильну обробку замовлень та платежів та зменшити ризик помилок.

Для кращого розуміння використання АОП для поліпшення мікросервісної архітектури, розглянемо приклад застосування АОП у мікросервісній архітектурі.

Припустимо, що ми маємо мікросервісну архітектуру, що складається з двох сервісів – сервісу обробки замовлень та сервісу оплати. Сервіс обробки замовлень отримує запити на обробку замовлень, перевіряє їх валідність та передає до сервісу оплати для здійснення оплати. Сервіс оплати отримує запит на здійснення оплати та передає результат оплати до сервісу обробки замовлень.

Ми хочемо використовувати АОП для покращення функціональності та якості коду у нашій мікросервісній архітектурі. Для цього ми використовуємо підхід, де ми використовуємо певні поради для кожного сервісу та зв'язки між ними для забезпечення правильної взаємодії між сервісами.

Необхідно забезпечити правильну обробку вхідних даних в обох сервісах. Для цього ми використовуємо передпоради, які перевіряють валідність вхідних даних перед тим, як вони будуть передані до сервісів.

У сервісі обробки замовлень ми використовуємо передпораду для перевірки валідності замовлення перед тим, як він буде переданий до сервісу оплати. Якщо замовлення не є валідним, то передпорада генерує виключення, яке повертається до клієнта.

У сервісі оплати ми також використовуємо передпораду для перевірки валідності вхідних даних. Перевіряється, чи містить запит на оплату достатньо інформації для здійснення оплати. Якщо інформація не є валідною, то передпорада генерує виключення, яке повертається до клієнта.

Помилки можуть виникати в будь-якому сервісі, і ми хочемо забезпечити правильну обробку помилок в нашій мікросервісній архітектурі. Для цього потрібно використовувати поради, які визначають правильну поведінку у випадку помилки.

У сервісі обробки замовлень ми використовуємо пораду, яка визначає правильну поведінку у випадку, якщо сервіс оплати недоступний. Якщо сервіс оплати недоступний, то сервіс обробки замовлень повертає помилку, що сервіс оплати недоступний. Це дозволяє клієнту правильно обробляти помилки та надає відповідну поведінку.

У сервісі оплати ми також використовуємо пораду, яка визначає правильну поведінку у випадку, якщо замовлення недоступне. Якщо замовлення недоступне, то сервіс оплати повертає помилку, що замовлення недоступне. Це дозволяє клієнту правильно обробляти помилки та надає відповідну поведінку.

Журналювання та моніторинг є важливим елементом мікросервісної архітектури. Потрібно забезпечити правильну реєстрацію та моніторинг наших сервісів, щоб бути впевненими у правильному функціонуванні системи.

Для журналювання ми використовуємо ELK-стек, який складається з Elasticsearch, Logstash та Kibana. Ми збираємо дані з різних сервісів та записуємо їх у Elasticsearch. Для збору даних використовується Logstash, який зчитує дані з журналів наших сервісів та пересилає їх до Elasticsearch. Кібана використовується для відображення та аналізу даних.

Для моніторингу можна використовувати Prometheus та Grafana. Prometheus збирає метрики з наших сервісів та зберігає їх у власному сховищі. Grafana використовується для відображення метрик та аналізу їх стану.

Застосування аспектно-орієнтованого програмування в нашій мікросервісній архітектурі дозволяє нам ефективно управляти різноманітними аспектами функціональності наших сервісів, забезпечувати їх взаємодію та підтримувати цілісність системи в цілому. Крім того, використання порад дозволяє нам забезпечити правильну поведінку сервісів у випадку помилок, а моніторинг та журналювання допомагають відслідковувати та аналізувати роботу нашої системи.

У майбутньому можна очікувати дальшого розвитку мікросервісної архітектури та зростання числа систем, які використовують цей підхід. Для ефективного впровадження мікросервісної архітектури необхідно використовувати інструменти, які дозволяють ефективно управляти функціональними аспектами сервісів та забезпечувати їх взаємодію. Аспектно-орієнтоване програмування може бути одним з таких інструментів, який дозволяє зосередитися на функціональних аспектах сервісів та забезпечує легкість управління їхнім поведінкою. Крім того, використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність.

Наступним кроком у розвитку мікросервісної архітектури може бути використання контейнерів та оркестраторів. Контейнери дозволяють забезпечити ізольованість сервісів та їхню мобільність, тобто можливість запуску на будь-якому сервері, що підтримує контейнеризацію. Оркестратори дозволяють автоматично керувати розгортанням та масштабуванням контейнерів, що забезпечує швидке відновлення після помилок та високу доступність системи в цілому.

Контейнеризація та оркестрація можуть бути досить складними процесами, тому необхідно використовувати ефективні інструменти для їх управління. Наприклад, Docker може бути використаний для створення контейнерів, а Kubernetes – для оркестрації їх розгортання та керування ними. Використання цих інструментів дозволяє зменшити складність розгортання та управління мікросервісами, забезпечуючи ефективну та швидку роботу системи.

У підсумку можна зробити висновок, що аспектно-орієнтоване програмування може бути ефективним інструментом для поліпшення мікросервісної архітектури. Використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність. Контейнеризація та оркестрація дозволяють забезпечити мобільність та ефективне керування мікросервісами. Використання цих технологій може допомогти зменшити складність розгортання та управління мікросервісами та забезпечити швидку відновлюваність після помилок та високу доступність системи в цілому.

Проте, важливо зазначити, що використання аспектно-орієнтованого програмування, контейнеризації та оркестрації є лише інструментами для поліпшення мікросервісної архітектури. Для успішного розгортання та ефективної роботи системи необхідно також враховувати багато інших аспектів, таких як безпека, моніторинг, тестування та інші. Крім того, важливо визначити, коли використання мікросервісної архітектури є доцільним та чи варто розгортати її в конкретному проекті.

Аспектно-орієнтоване програмування є ефективним інструментом для поліпшення мікросервісної архітектури. Використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність. Контейнеризація та оркестрація дозволяють забезпечити мобільність та ефективне керування мікросервісами.

Однак, важливо зазначити, що використання аспектно-орієнтованого програмування, контейнеризації та оркестрації є лише частинами процесу побудови ефективної мікросервісної архітектури. Для успішного розгортання та ефективної роботи системи необхідно також враховувати багато інших аспектів, таких як безпека, моніторинг, тестування та інші. Крім того, важливо визначити, коли використання мікросервісної архітектури є доцільним та чи варто розгортати її в конкретному проекті.

В цілому, аспектно-орієнтоване програмування може бути корисним інструментом для побудови ефективної мікросервісної архітектури. Використання цього підходу може допомогти зменшити складність розгортання та управління мікросервісами та забезпечити швидку відновлюваність після помилок та високу доступність системи в цілому. Однак, важливо враховувати багато інших аспектів та використовувати підходи та інструменти, які найбільше відповідають потребам конкретного проекту.

Для того, щоб успішно використовувати аспектно-орієнтоване програмування, необхідно мати достатній рівень знань та досвіду в програмуванні та мікросервісній архітектурі. Крім того, важливо розуміти, що використання цього підходу не є універсальним рішенням для всіх задач і не підходить для кожного проекту.

Особливо важливо враховувати аспекти безпеки та захисту даних під час використання мікросервісної архітектури. Кожен мікросервіс повинен мати достатній рівень захисту, а також виконувати певні стандарти щодо захисту даних. Крім того, важливо забезпечувати моніторинг та логування для швидкої виявлення та виправлення помилок.

Також важливо враховувати витрати на побудову та підтримку мікросервісної архітектури. Зазвичай це вимагає великих витрат на інфраструктуру та залучення додаткового персоналу. Тому перед розгортанням мікросервісної архітектури варто ретельно обміркувати, чи варто такі витрати та чи є можливість їх компенсувати в результаті більш ефективної роботи системи.

Усі ці фактори підтверджують, що використання мікросервісної архітектури та аспектно-орієнтованого програмування є складним завданням, яке вимагає великої кількості знань, досвіду та ретельного аналізу. Однак, якщо використання цих підходів проводиться правильно та враховується весь комплекс аспектів, то можна досягти високої ефективності та доступності системи.

Також важливе належне тестування та валідація системи перед використанням в реальних умовах. Це допоможе виявити та виправити помилки та ускладнення перед тим, як користувачі почнуть використовувати систему.

У зв’язку з розгортанням мікросервісної архітектури та використанням аспектно-орієнтованого програмування, важливо також звернути увагу на стилі програмування, які використовуються. Оскільки мікросервісна архітектура передбачає розподілення функцій між різними сервісами, кожен з яких має свою відповідальність, стилі програмування повинні бути зорієнтовані на створення зрозумілої та легко модифікуємої кодової бази.

Крім того, важливо враховувати питання масштабованості системи при використанні мікросервісної архітектури та аспектно-орієнтованого програмування. Якщо зростання обсягу даних або навантаження стає непередбачуваним, можуть виникнути проблеми з пропускною здатністю та продуктивністю. Тому важливо забезпечувати масштабованість системи та можливість розширення її функціональності при необхідності.

Аспектно-орієнтоване програмування є потужним підходом, який дозволяє розширювати функціональність програмного забезпечення, знижувати повторення коду та поліпшувати читабельність та обслуговуваність коду. Крім того, використання мікросервісної архітектури дозволяє розподілити функції системи між різними сервісами, забезпечити гнучкість та швидкість внесення змін.

Комбінування аспектно-орієнтованого програмування з мікросервісною архітектурою може принести значні переваги в розробці та підтримці програмного забезпечення. Ці підходи забезпечують можливість підтримувати чистоту коду та дозволяють зосередитись на бізнес-логіці системи, що забезпечує більш швидку та ефективну розробку та підтримку.

Однак, варто пам’ятати, що використання таких підходів також може мати свої недоліки, зокрема ускладнення підтримки системи та необхідність відповідних знань та досвіду у використанні цих технологій.

У підсумку, аспектно-орієнтоване програмування та мікросервісна архітектура є потужними інструментами у розробці програмного забезпечення. Використання цих підходів дозволяє підвищити якість та ефективність розробки та підтримки системи, забезпечуючи

гнучкість та швидкість внесення змін у відповідь на потреби користувачів та зміни бізнес-вимог. Однак, перед використанням цих технологій необхідно провести відповідну оцінку вартості та потенційних недоліків, щоб забезпечити оптимальне використання ресурсів та досягнення поставлених цілей.

Висновки. У даній статті ми розглянули важливість мікросервісної архітектури для сучасних розподілених систем. Ми дослідили проблеми, які можуть виникнути при розробці та підтримці мікросервісної архітектури та вказали на те, як аспектно-орієнтоване програмування може допомогти у вирішенні цих проблем.

Можна сказати, що мікросервісна архітектура є важливим елементом розподілених систем та дозволяє підвищити масштабованість та ефективність системи в цілому. Однак, для ефективної підтримки мікросервісної архітектури необхідно використовувати підходи, які дозволяють ефективно управляти функціональними аспектами сервісів та забезпечувати їх взаємодію.

Аспектно-орієнтоване програмування є одним з таких підходів, який може допомогти розробникам у вирішенні цих проблем. Використання порад та патернів, таких як retry, circuit breaker, bulkhead та інших, може забезпечити правильну поведінку сервісів у випадку помилок, що дозволяє зменшити час відновлення роботи системи.

Моніторинг та журналювання є також важливим елементом підтримки мікросервісної архітектури. Використання інструментів, таких як ELK-стек та Prometheus з Grafana, дозволяє ефективно збирати та аналізувати дані, що є необхідним для підтримки роботи системи в цілому.

Отже, можна зробити висновок, що аспектно-орієнтоване програмування може бути ефективним інструментом для поліпшення мікросервісної архітектури. Використання аспектів дозволяє зосередитися на функціональних аспектах сервісів, забезпечуючи легкість та гнучкість у впровадженні функціональних вимог. Поради та патерни, такі як retry, circuit breaker, bulkhead та інші, дозволяють забезпечити правильну поведінку сервісів у випадку помилок, що є важливим елементом підтримки мікросервісної архітектури.

Аспектно-орієнтоване програмування може бути ефективним інструментом для поліпшення мікросервісної архітектури. Використання патернів та порад забезпечує правильну поведінку сервісів та допомагає забезпечити їх високу доступність та ефективність. Контейнеризація та оркестрація дозволяють забезпечити мобільність та ефективне керування мікросервісами. Проте, важливо враховувати багато інших аспектів при розгортанні та управлінні мікросервісами. Використання мікросервісної архітектури повинно бути обґрунтованим та доцільним для конкретного проекту.

Список використаних джерел

1. M. Fowler, «Microservices: Decomposing Applications for Deployability and Scalability,» 2014.
2. D. Duka, A. Shtroo, «Design Patterns for Microservices Architecture,» IEEE, 2018.
3. S. Newman, «Building Microservices: Designing Fine-Grained Systems,» 2015.
4. В. Єфименко. Мікросервісна архітектура: концепції, технології, інструменти// Системні технології, -2019-№ 4 (34). – С. 38–49.
5. М. Матвєєва. Аспекти технології мікросервісів в розробці програмного забезпечення// Наукові праці Донецького національного технічного університету-2019-№ 3. – С. 105–116.
6. Ю. Данилюк. Архітектура мікросервісів як підхід до розробки високопродуктивних систем// Програмна інженерія та інформаційні технології, -2018.- № 2. – С. 83–96.

Робота виконана під науковим керівництвом канд. екон. наук, старшого викладача
ФРАНЧУК Т. М.

АВТОМАТИЗАЦІЯ ОБЛІКУ СУБ'ЄКТІВ НАДАННЯ ГУМАНІТАРНОЇ ДОПОМОГИ В УМОВАХ ВОЄННОГО ЧАСУ

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

У статті розглянуто проблематику в обліку та реалізації гуманітарних питань в умовах воєнного часу. При написанні статті були використані зауваження та пропозиції волонтерської організації «East coast aid». Розглянуто ключові моменти для створення аналітичної сисетмми обліку для обліку гуманітарної допомоги.

The article describes problems in documenting and implementing humanitarian issues in the wartime. During the writing and research process, the comments and advice of the «East Coast Aid» volunteer organization were used. Advantages of «East Coast Aid» website will be described and analyzed in the article.

Актуальність. В реаліях нинішнього світу важливу роль у допомозі армії відіграють волонтерські організації, що виконують місії в Україні та інших країнах. Будь яка допомога має бути систематизована обліком та зареєстрована для контролю її використання та мінімізації виникнення ризиків. Саме тому доречним буде впровадження новітніх ІТ-технологій при створенні та впровадженні обліку. При збільшення фондів, і використання більшої кількості ресурсів критичним стає питання доцільності використання коштів та ресурсів для максимально ефективного контролю та мінімізації ризиків. У реаліях сьогодення, люди по всьому світі почали об'єднуватись для допомоги Україні. Тому дуже важливо аби вся інформація про надання допомоги була у вільних інтернет джерелах. Таким чином, люди зі всього світу можуть приєднуватись до гуманітарної допомоги, при довірі фонду та розумінні його функціоналу. Тому критично важливе мати відкриту та інноваційну методологію системи обліку та вдалу інтернет концепцію.

Метою статті є дослідження особливостей ведення облікових систем при наданні гуманітарної допомоги з метою підвищення ефективності їх функціонування та використання.

Об'єктом дослідження є розробка системи обліку для надання гуманітарної допомоги постраждалим внаслідок російської агресії.

Предмет дослідження – аналітична система обліку суб'єктів з використанням ІТ-технологій.

Аналіз попередніх досліджень. При дослідженні проблематики систем обліку були використаний власний досвід, досвід інших гуманітарних організацій та їх досвід аналітичних систем обліку та нормативно-аналітична база аналітичних інформаційних систем.

Виклад основного матеріалу. Для початку ведення обліку, потрібно отримувати дані від користувачів для їх ідентифікації в системі та контролю повторної допомоги. Дуже багато людей зараз потребують допомоги і важливо ставити пріоритети на тих кому справді потрібна допомога і хто просто використовує волонтерів для власних потреб. Для унеможливлення зловживанням допомоги. Саме тому важливо вести облік для більш точного розуміння проблематики даного питання. У межах цієї моделі визначено пріоритетні данні для внесення у бази даних с подальшим використанням їх для обліку та аудиту системи. Адже дуже важливо своєчасний та запланований аудит, що дає більш чітке бачення проблеми. Вмілий аудит закриває питання перевірки достовірності діяльності підприємства у сфері фінансів, а й надання керівнику рекомендацій, виконуючи які можна збільшити ефективність роботи компанії.

Для ведення обліку потрібно отримувати дані з запиту для ведення списку користувачів (Рис.1). У цій формі користувач вказує свої дані, такі як ім'я та прізвище що буде ключем для реєстрації, сам запит – яка саме допомога потрібна для більш точного

розуміння необхідного. Е-мейл та телефон для контакту с користувачем та додатково вказує чи потрібна допомога спеціаліста, бо зараз виросла кількість людей які потребують роботу психолога чи юриста для узгодження своїх проблем. Таким чином ми отримуємо для реєстрації необхідні дані від користувача. Та маємо дані для обліку, що допоможе в подальшому ефективно використовувати ресурси, та унеможливить зловживання гуманітарною допомогою або крадіжок

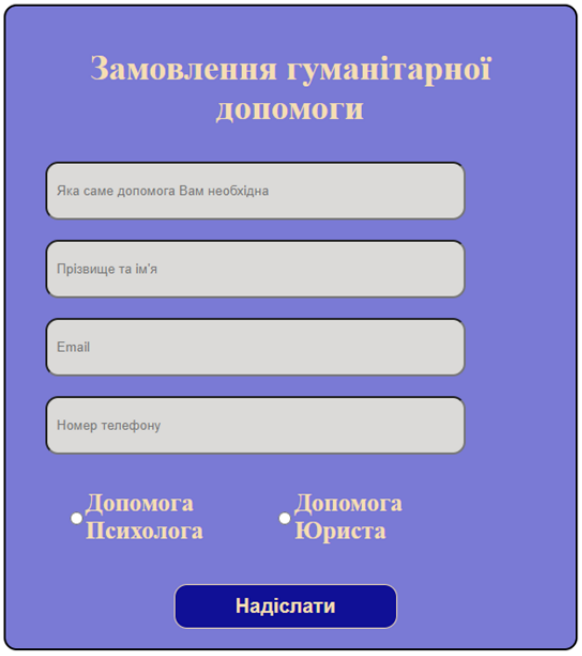

Рис. 1. Форма запиту на допомогу

Метою ведення обліку і складання фінансової звітності є надання користувачам для прийняття рішень повної, правдивої та неупередженої інформації про фінансове становище, результати діяльності та рух грошових коштів підприємства.

Основною метою обліку і складання фінансової звітності є забезпечення достовірної, повної та доступної інформації про фінансові результати, позицію та діяльність організації. Ця інформація використовується для прийняття рішень, залученні інвестицій і кредитування, а також при проведенні аудиту чи аналізу фінансової звітності. Основна мета обліку та складання фінансової звітності спрямована на забезпечення відповідності інформації корпоративним законам, вимогам і правилам організації, акціонерів та інвесторів, а також для забезпечення здатності управління приймати правильні рішення. Не слід забувати, що облік і складання фінансової звітності є невід'ємною складовою надання достовірної, повної та доступної інформації про фінансові результати, позицію та діяльність організації інвесторам та стороннім учасникам.

У рамках міжнародної гуманітарної допомоги під час війни застосовуються різні методи надання допомоги та загострення уваги на супроводжуваних осіб. Серед них можна виділити наступні ключові методи:

1. Захист прав людини: надання правової охорони та захисту людям, які переживають наслідки війни.
2. Захист життя та здоров'я: надання допомоги у лікуванні, підтримка програм щодо дотримання гігієни та профілактики болячих хвороб.
3. Освіта: надання далі доступу до освіти для дітей та дорослих на територіях, перебуваючих під впливом війни.
4. Надання безпечних притулків: створення спеціалізованих притулків для людей, які намагаються приховатися від військових дій та втратилих своє помешкання.

5. Надання матеріальної допомоги: надання харчування, одягу, житла та інших необхідних ресурсів до потреб людей, які знаходяться у ситуації примусового переселення.
6. Підтримка проектів побудови: підтримки будівництва шкіл, будівель, інфраструктури та інших об'єктів, які допомагають постраждалим та захищеним людям прийняти постійне місце проживання.

Гуманітарна допомога є різновидом благодійництва, а не видом благодійної допомоги і має спрямовуватися відповідно до обставин, об'єктивних потреб, **згоди її отримувачів** та за умови дотримання вимог Закону України «Про благодійну діяльність та благодійні організації» від 05.07.2012 р. № 5073-VI (далі – Закон № 5073 від 05.07.2012 р. № 5073-VI (далі – Закон № 5073). Про це зазначено у статті 1 Закону № 1192 (про гуманітарну допомогу). А в статті 3 Закону № 5073 мова йде лише про цілі та сфери благодійної діяльності, які повинні співпадати при отриманні гуманітарної допомоги і здійснення благодійництва. Етапи ведення обліку продемонстровано на Рис.2.

Рис. 2. Етапи ведення обліку

На першому етапі обліку слід зрозуміти що саме потрібно, яка саме допомога необхідна. Для реєстрації допомоги ми використовуємо дані отримані з форми (*Рисунок 1).* Отримані дані ми контролюємо в *Excel.* На наступному етапі ми дивимось в системі можливість допомоги в кожному випадку. На останньому етапі, якщо є можливість допомоги, надається гуманітарна допомога.

Гуманітарна допомога – добровільна, безкорислива та усвідомлена діяльність фізичних або юридичних осіб (спонсорів), що виражається через особисту та/або майнову допомогу юридичним особам, які в офіційному порядку визнані отримувачами гуманітарної допомоги, ґрунтується на принципах законності, гуманності, рівності та здійснюється із гуманних мотивів для досягнення суспільно-значимих цілей. Гуманітарна допомога має свої особливості:

- вона завжди має чітко визначений цільовий характер та передбачає кінцевого адресата;
- переслідує особливо значимі напрями здійснення благодійності;
- має у якості суб'єктів донора та юридичну особу зі спеціальним статусом отримувача гуманітарної допомоги;
- розрізняє отримувача гуманітарної допомоги та набувача (фізичну особу – кінцевого споживача);
- потребує письмової пропозиції донора про її надання;
- потребує згоди на її отримання з боку отримувача гуманітарної допомоги;

Отримувачі або набувачі гуманітарної допомоги відповідають критеріям соціальної незахищеності або матеріальної незабезпеченості. Зазначені обставини можуть бути спричинені такими подіями: важкими життєвими обставинами; стихійним лихом; значним погіршенням стану здоров'я; надзвичайним станом.

Після замовлення допомоги та реєстрації допомоги. Оператор у програмі MS Excel отримує заповнені користувачем дані.

Дані отримуються за допомогою введення користувачем даних у поля для введення та опрацьовуються закладеними функціями, методами сортування та фільтрування, розміщених у програмі Excel. Користувач може ввести дані вручну або використати інші функції для імпортування даних з інших файлів або з бази даних. Також можна використовувати функції автозаповнення, які дозволяють автоматично вводити дані в поля з наявними списками значень. Крім того, в даяких випадках можна використати макроси, які дозволяють автоматизувати процес завантаження даних з інших файлів або баз даних у форму Excel (за потреби). Введені дані генеруються в таблицю зручну для користування (Рис.3).

Ім'я та прізвище	Email	Номер телефону	Необхідна допомога	Допомога Юриста	Допомога психолога
Володимир Руденко	vldvrudenko@gmail.com	+380667161144	Необхідна допомога юриста	+	-
Гурженко Лариса	lngurszenko@gmail.com	+380667206666	Речі першої необхідності, їжа, інформація	-	-
Мостовий Андрій	mostovoi@gmail.com	+380667197865	Інформація , їжа , допомога психолога	-	+
Ткаченко Ігор	tkachenkoihor@gmail.com	+380677154521	Допомога юриста , психолога та їжа	+	+
Оксана Білик	biliuk@gmail.com	+380688171234	Інформація , речі першої необхідності	-	-
Валентина Кучерук	kucheruk@gmail.com	+380667182123	Допомога юриста , їжа	+	-

Рис. 3. Облік отриманих даних

Функціональність рішень даного типу ведення обліку гуманітарної допомоги :

- Легкість використання користувачів
- Зручність ведення обліку
- Отримання великої кількості даних користувачів
- Можливість самостійного внесення допомоги
- Реєстрація користувача
- Неможливість обману системи

Тому даний варіант отримання та використання даних є зручним, інноваційним та досить надійним для ведення обліку надання та отримання допомоги. Також важливим етапом надання допомоги є фото-фіксація для подальшої звітності перед спонсорами (Рис.4). Фото-фіксація може бути зроблена за допомогою різних методів, включаючи ручне зняття фотографії, використання планшетних пристроїв або смартфонів для зняття фотографії, а також використання відеофіксації для збору далі глибоких даних. Використовуючи ці методи, підприємства/фундації можуть зафіксувати процеси, відстежувати результати і зробити звіти для більш ефективної звітності. Якщо прийнято рішення використовувати фото-фіксацію, підприємства/фундації можуть використовувати спеціальну програму для збору, відстеження і аналізу даних. Ця програма може дозволити підприємству/фундації збирати фото-фіксацію, відстежувати її зміни і аналізувати дані, щоб отримати більш детальну інформацію про процеси і звіти про продуктивність. Система також може містити функції для відстеження процесів, визначення тривалості кожного процесу і далі генерування звітів для подальшого аналізу логістики.

Рис. 4. Приклад фото-звіту партнерами з фундації «Із покликом в серці»

Висновки. Аналітична система обліку суб'єктів надання гуманітарної допомоги в умовах воєнного часу призначена для організації та підтримки роботи з надання гуманітарної допомоги на території України та інших країн в умовах воєнного часу. Ця система має цілий спектр засобів для аналізу ситуації та подальших дій планування руху для надання гуманітарної допомоги. Система містить інструменти для збору, аналізу та обробки інформації щодо суб'єктів надання гуманітарної допомоги. Система також дозволяє збирати інформацію про тих, хто надалі хоче планувати дії для надання гуманітарної допомоги. Система ще надає можливість використання засобів аналітики, аналізу та візуалізації для отримання додаткових даних, які можуть допомогти в прийнятті оптимальних рішень. Ці дані далі використовуються для планування дій по наданню гуманітарної допомоги. Також система містить механізми для контролю доступу до інформації та можливості змінювати її. Це дозволяє збирати оновлену інформацію про суб'єкти надання гуманітарної допомоги, далі планування дій для надання гуманітарної допомоги. За допомогою цієї аналітичної системи можна підтримувати і контролювати процес надання гуманітарної допомоги в умовах воєнного часу, а також забезпечувати належне використання та планування дій для надання гуманітарної допомоги як по напрямках так і по логістиці.

Список використаних джерел

1. Косинський В.І. Сучасні інформаційні технології : навч. посіб. / В.І. Косинський, О.Ф. Швець. – Київ : Знання, 2011. – 594 с.
2. Чернишенко А. Аналітично-інтелектуальні системи обліку суб'єктів. Берлін: Springer, 2012. – 645 с.
3. Карп'юк О. Розробка аналітично-інтелектуальних систем облік ДАЛІ. Київ: Видавництво «Знання», 2009. – 326 с.
4. Карацуба Н. Програмування інтелектуальних аналітичних систем: посібник. Київ: Видавництво «Знання», 2014. – 421 с.
5. S. K. Pal and P. Mitra, Pattern Recognition Algorithms for Data Mining, Chapman & Hall CRC Press, Boca Raton, FL, May 2004, ISBN: 1-58488-457-6

Робота виконана під науковим керівництвом д-ра техн. наук, професора
КРИВОРУЧКО О. В.

ВИКОРИСТАННЯ ОНЛАЙН-ПЛАТФОРМ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ ТА ЕФЕКТИВНОСТІ НАВЧАННЯ В ОСВІТНІХ ЗАКЛАДАХ

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

У статті розглянуто використання онлайн-платформ для підвищення якості та ефективності навчання в освітніх закладах. Детально розглянуті переваги використання онлайн-платформ в освіті, різні типи онлайн-платформ для навчання, технологічні можливості онлайн-платформ, практичні приклади використання онлайн-платформ у різних освітніх закладах та їх ефективність та проблеми з безпекою даних та недостатня соціальна інтерактивність.

The article discusses the use of online platforms to improve the quality and efficiency of learning in educational institutions. The advantages of using online platforms in education, different types of online learning platforms, technological capabilities of online platforms, practical examples of using online platforms in different educational institutions and their effectiveness, as well as problems with data security and lack of social interactivity are discussed in detail.

Актуальність. Онлайн-платформи для навчання є одним з найбільш актуальних і швидко розвиваючихся напрямків у сучасній освіті. У сучасному світі навчання стає все більш цифровим і інтерактивним, а використання онлайн-платформ дозволяє учням отримувати знання та навички в більш зручному та ефективному форматі. Онлайн-платформи дозволяють учням вивчати матеріали у будь-який час та в будь-якому місці, не прив'язуючись до певного місця та часу. Це особливо важливо для тих, хто зайнятий роботою або іншими обов'язками, оскільки онлайн-платформи дозволяють організовувати навчання згідно з їх індивідуальним графіком та потребами. Крім того, використання онлайн-платформ дозволяє вчителям та учням використовувати різноманітні технологічні інструменти, такі як інтерактивні відео, аудіозаписи, тести та ігри, що сприяє більш ефективному засвоєнню матеріалу. У світлі умов, що швидко змінюються у світі, навчання на онлайн-платформах дозволяє учням отримувати актуальну інформацію та знання, оновлювати та розширювати свої навички та компетенції відповідно до потреб ринку праці, котрі постійно змінюються. В цілому, використання онлайн-платформ у навчанні є дуже актуальним та ефективним способом підвищення якості та ефективності освітнього процесу в наш час.

Використання онлайн-платформ у освіті дозволяє розширити географію навчання та участь у навчальному процесі. Особливо важливим це є для студентів, які живуть у віддалених регіонах, де доступ до якісної освіти може бути обмеженим. Онлайн-платформи дають таким студентам можливість навчатися у кращих вчителів та викладачів, брати участь у дискусіях та отримувати зворотний зв'язок на рівних умовах з іншими студентами з різних частин світу. У світлі цих переваг використання онлайн-платформ у навчанні є необхідним кроком у розвитку сучасної освіти і має бути широко прийнято в освітніх установах по всьому світу.

У даний час багато університетів і коледжів використовують онлайн-платформи для надання онлайн-курсів, які дозволяють студентам здобувати знання та навички з будь-якого місця та у зручний для них час. Такі курси можуть бути корисними для студентів з різних куточків світу, які хочуть отримати освіту в іншій країні, але не мають можливості переїхати. Крім того, використання онлайн-платформ дозволяє університетам та коледжам залучати кращих викладачів та вчених з різних країн для надання курсів та лекцій, що покращує якість освіти.

Метою статті є дослідження особливостей використання онлайн-платформ для підвищення якості та ефективності навчання в освітніх закладах.

Об'єктом дослідження є розробка онлайн-платформи дистанційного навчання.

Виклад основного матеріалу. Однією з основних переваг використання онлайн-платформ в освіті є їх зручність та доступність. Учні та викладачі можуть використовувати онлайн-платформи у будь-який час та з будь-якого місця, маючи доступ до матеріалів та інструментів, необхідних для ефективного навчання та викладання. Крім того, використання онлайн-платформ дозволяє значно зменшити часові та фінансові витрати на навчання, оскільки не потрібно відвідувати навчальні заклади та оплачувати витрати на проїзд, проживання та харчування.

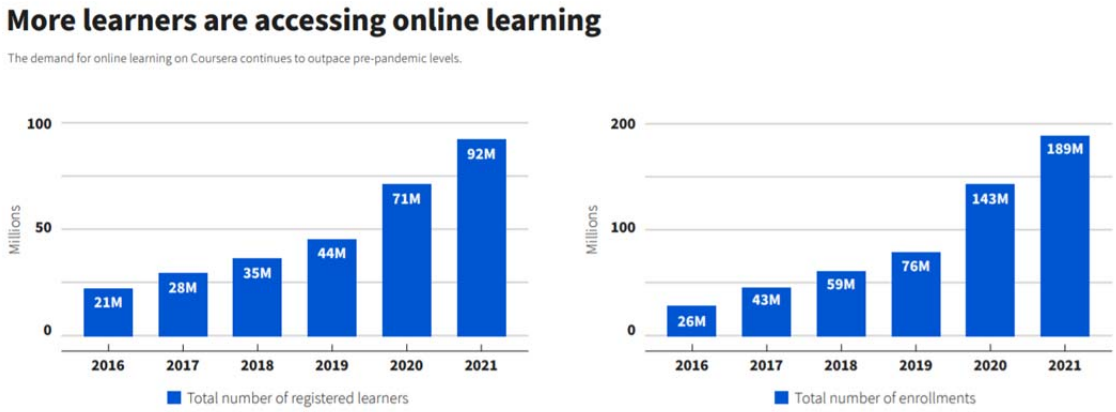

Рис. 1. Приріст нових користувачів онлайн-платформи Coursera. У 2021 році на курси зареєструвалося понад 20 мільйонів нових учнів (https://www.weforum.org/agenda/2022/01/online-learning-courses-reskill-skills-gap/)

Гнучкість – ще одна важлива перевага онлайн-платформ в освіті. Вони дозволяють учням та викладачам працювати в більш гнучкому форматі, вибираючи зручний час та місце для навчальних занять. Це особливо важливо для студентів, які мають щільні графіки або обмежений доступ до навчальних закладів. Завдяки гнучкості онлайн-платформ, учні можуть працювати за своїми індивідуальними темпами, а викладачі можуть адаптувати свій курс до потреб конкретних студентів.

Використання онлайн-платформ також сприяє підвищенню якості освіти, оскільки це дозволяє використовувати найсучасніші технології та методи навчання. Це забезпечує більш глибоке розуміння матеріалу, більш ефективний обмін знаннями та навичками між учасниками освітнього процесу, а також підвищення мотивації учнів. Крім того, використання онлайн-платформ дає можливість викладачам та студентам використовувати різні формати та методи навчання, такі як відеоуроки, онлайн-тести, форуми для дискусій та багато іншого.

Окрім того, використання онлайн-платформи в освітньому процесі також забезпечують більшу прозорість та доступність інформації. Учасники навчального процесу можуть з легкістю отримати доступ до інформації про розклад занять, вимоги до оцінювання та навчальні матеріали, що зменшує ймовірність помилок та непорозумінь.

Сучасні онлайн-платформи для навчання мають значні технологічні можливості, які можуть суттєво підвищити якість та ефективність процесу навчання. Однією з найбільш важливих є можливість створення унікальних та інтерактивних навчальних матеріалів та інструментів для саморозвитку. Вона дозволяє використовувати різноманітні мультимедійні формати, такі як відео, аудіо, графіка та інтерактивні елементи, щоб зробити навчальний матеріал більш доступним, зрозумілим та запам'ятовуваним. Це особливо важливо для студентів, які мають різні стилі навчання та потребують більш гнучкого підходу до вивчення

матеріалу. Крім того, багато платформ надають інструменти для створення власних навчальних матеріалів, що дозволяє викладачам та студентам створювати контент, який відповідає їх потребам та унікальним навчальним цілям. Це також може суттєво покращити ефективність навчання та підвищити мотивацію студентів. Наприклад, платформа Adobe Captivate надає можливість створювати інтерактивні навчальні курси, які можуть бути індивідуально налаштовані під кожного студента. Ще одним прикладом є платформа Edpuzzle, яка дозволяє викладачам створювати відеоуроки з інтерактивними питаннями та завданнями. Ці приклади демонструють, як онлайн-платформи можуть бути використані для створення унікальних та інтерактивних навчальних матеріалів та інструментів для саморозвитку.

Platform	Major Traffic Country	Traffic in Million
BYJU's	India	60-70 M
Khan Academy	United States	45-55 M
Study	United States	25-30 M
Vedantu	India	25-30 M
Duolingo	United States	12-18 M
Masterclass	United States	12-18 M
Udemy	India	10-18 M
Coursera	United States	8-12 M
Instructables	United States	8-12 M
Edx	United States	3-5 M

Рис. 2. Статистика найпопулярніших онлайн-платформ у світі. Дані станом на липень 2021 року (https://www.vdocipher.com/blog/elearning-statistics)

Існує безліч практичних прикладів успішного використання онлайн-платформ у освіті, що демонструють їх ефективність. Наприклад, Гарвардський університет використовує онлайн-платформу edX для проведення курсів, які можуть бути доступні безкоштовно для всіх бажаючих. Курс «CS50: Introduction to Computer Science» зібрав більше 2,5 мільйонів зареєстрованих студентів з усього світу, що підтверджує великий потенціал онлайн-платформ для поширення знань та доступності освіти.

Іншим прикладом є використання онлайн-платформи Coursera, яку використовують більше 200 університетів, включаючи Мічиганський університет та Каліфорнійський університет у Сан-Франциско, для проведення онлайн-курсів. Більше 77 мільйонів людей зареєструвалися на курси Coursera, що підкреслює популярність та успішність онлайн-освіти. Також варто зазначити приклад використання онлайн-платформи Khan Academy в школах США. Ця платформа надає безкоштовні відеоуроки з різних предметів, які дозволяють учням навчатися в своєму власному темпі та приділяти більше часу складним темам. Ця платформа отримала високу оцінку учнів та вчителів за її простоту використання та ефективність. Був зроблений порівняльний аналіз кількох популярних онлайн-платформ для навчання, здійснений на основі наукових досліджень та відомих відгуків:

- Google Classroom – це безкоштовна платформа, розроблена Google, яка використовується в багатьох школах та університетах для організації навчальних процесів в режимі онлайн. Вона відома своїм простим та зручним інтерфейсом, який сприяє ефективній взаємодії між вчителями та студентами. Google Classroom надає можливість створювати віртуальні класи, додавати завдання, взаємодіяти зі студентами через спеціальні функції коментування та оцінювання завдань. Вона також інтегрується з іншими продуктами Google,

такими як Google Docs, Google Drive, що дозволяє зручно організовувати та зберігати навчальні матеріали.

- Moodle – це відкрита платформа для навчання, яка використовується в багатьох навчальних установах по всьому світу. Вона відома своєю гнучкістю та можливістю налаштовувати різноманітні активності, такі як форуми, тестування, завдання та інші, що дозволяє вчителям створювати різноманітні навчальні сценарії відповідно до своїх потреб. Moodle також має велику спільноту користувачів, що надає можливість обміну досвідом та розробки нових функцій.
- Blackboard – це одна з найстаріших та відомих платформ для навчання, що використовується в багатьох університетах та вищих навчальних закладах. Вона відома своєю високою функціональністю, такою як можливість створення курсів, завдань, форумів, тестувань та інших активностей. Вона також має розширені можливості для взаємодії зі студентами, включаючи можливість надавати зворотний зв'язок та оцінювати роботи. Blackboard також надає інструменти для ведення електронного журналу та моніторингу активності студентів, що дозволяє вчителям відстежувати прогрес студентів.
- Coursera – це онлайн-платформа для навчання, яка спеціалізується на вищій освіті та пропонує віртуальні курси від провідних університетів та організацій по всьому світу. Вона відома своєю високою якістю навчання, професійними викладачами та різноманітністю курсів з різних галузей знань. Coursera надає можливість студентам проходити курси у власному темпі, має вбудовану систему оцінювання та забезпечує доступ до різноманітних навчальних ресурсів.
- EdX – це ще одна відома онлайн-платформа для навчання, яка пропонує курси від провідних університетів та організацій. Вона відома своєю відкритістю та безкоштовним доступом до багатьох курсів, а також своєю акцентом на науковій та технічній освіті. EdX також надає можливість проходити курси за власним графіком та взаємодіяти з викладачами та іншими студентами.
- Schoology – це платформа для навчання, спрямована на розподілені школи та навчальні заклади. Вона надає вчителям можливість створювати віртуальні класи, додавати матеріали, давати завдання, забезпечувати зворотній зв'язок та оцінювати роботи студентів. Особлива риса Schoology – це можливість налаштовувати процес навчання з урахуванням індивідуальних потреб студентів, розробляти персоналізовані навчальні плани та використовувати аналітику для відстеження успішності студентів.
- Edmodo – це соціальна мережа для навчання, яка забезпечує можливість створювати віртуальні класи, спілкуватися зі студентами, додавати матеріали та завдання, оцінювати роботи студентів та проводити тести. Вона також дозволяє вчителям створювати спільноти та співпрацювати з іншими вчителями, обмінюватися ресурсами та ідеями. Edmodo має також функції для забезпечення безпеки та конфіденційності даних студентів.

Імерсивні технології та їх роль у навчанні. Інклюзивне навчання, що передбачає можливості для різних типів учнів, включаючи тих, хто має особливі освітні потреби, є важливим напрямом розвитку освіти в сучасному світі. Одним з потужних інструментів, який може сприяти реалізації інклюзивного навчання, є використання імерсивних технологій. Імерсивні технології, такі як віртуальна реальність (VR), розширена реальність (AR) та змішана реальність (MR), забезпечують користувачам унікальні можливості взаємодії з віртуальним оточенням та досвідом, що може бути багатоцільовим і відповідати різним освітнім потребам.

Одним з важливих аспектів імерсивних технологій в контексті інклюзивного навчання є можливість створення доступного навчального середовища. Завдяки використанню VR, AR або MR, можна створити віртуальні класні кімнати, в яких можуть брати участь учні з різними освітніми потребами, включаючи тих, хто має фізичні обмеження, аутизм, дислексію та інші відхилення. Наприклад, віртуальна реальність може надати можливість учням з фізичними обмеженнями взаємодіяти з віртуальним оточенням, відтворюючи реальний світ, який може бути недоступним для них в реальному житті. AR може бути використана для візуалізації складних концепцій або взаємодії з навколишнім середовищем, забезпечуючи можливість взаємодії з віртуальними об'єктами в реальному часі. Змішана

реальність може забезпечити комбінацію віртуальних та реальних елементів, що може сприяти більшій взаємодії та зрозумінню матеріалу для учнів з різними типами сприйняття.

Іншим важливим аспектом використання імерсивних технологій в інклюзивному навчанні є можливість індивідуалізації навчального процесу. Завдяки інтерактивності та гнучкості імерсивних технологій, учні можуть вчитися власним темпом, відповідно до своїх потреб та рівня навчання. Віртуальні симуляції, наприклад, можуть надати можливість учням випробувати різні сценарії та вирішувати завдання, що відповідають їхнім особистим потребам та здібностям.

Крім того, імерсивні технології можуть забезпечити більш активну та залучену участь учнів у навчальному процесі. Завдяки можливості взаємодії з віртуальними об'єктами та оточенням, учні можуть відчувати більшу мотивацію до вивчення матеріалу, використовувати свої навички та розвивати критичне мислення.

Проте, варто відзначити, що використання імерсивних технологій в інклюзивному навчанні також вимагає ретельного підходу до планування та розробки навчальних матеріалів, а також врахування різноманітних освітніх потреб учнів. Додатково, важливо враховувати етичні аспекти використання імерсивних технологій в інклюзивному навчанні. Наприклад, необхідно враховувати можливість виникнення дискримінації або стереотипів у віртуальних середовищах, які можуть вплинути на деякі групи учнів. Також варто враховувати захист персональних даних учнів та забезпечення кібербезпеки в процесі використання імерсивних технологій.

Важливо забезпечити доступність імерсивних технологій для всіх учнів, включаючи тих, хто має фізичні, сенсорні або когнітивні обмеження. Наприклад, використання контролерів рухів або інших альтернативних інтерфейсів може забезпечити доступність для учнів з обмеженою рухливістю. Забезпечення адаптивності інтерфейсів, взаємодії та контенту може допомогти учням з різними особливостями в сприйнятті та сприяти їхньому повноцінному навчанню.

Безпека даних. З використанням онлайн-платформ у навчанні існують деякі проблеми, які можуть негативно впливати на якість освіти. Однією з таких проблем є безпека даних. У онлайн-середовищі, де персональні дані зберігаються та обробляються, існує ризик їх утікання та використання зловмисниками. Недавно був виявлений випадок взлому бази даних онлайн-школи Edmodo, де зловмисники отримали доступ до особистих даних учнів та вчителів, включаючи їх імена, адреси електронної пошти та хешовані паролі. Також, при використанні хмарних сервісів, дані можуть бути доступні третім особам, якщо не вживати необхідні заходи безпеки. У 2020 році, через пандемію COVID-19, були зареєстровані декілька випадків порушення безпеки на популярних платформах для дистанційного навчання, таких як Zoom та Microsoft Teams. Такі витоки можуть призвести до серйозних наслідків, таких як крадіжка особистості та шахрайство, що може негативно позначитися на довірі до онлайн-платформ в цілому.

Іншою проблемою, пов'язаною з використанням онлайн-платформ, є недостатня соціальна інтерактивність. На відміну від традиційних освітніх методів, які включають у себе спілкування в класі та співпрацю з іншими учнями, онлайн-платформи можуть створювати відчуття ізоляції та відсутності спілкування. Деякі учні можуть відчувати себе некомфортно у віртуальному середовищі та втрачати інтерес до навчання. Наприклад, у дослідженні, проведеному в Швеції, виявлено, що учні, які використовували онлайн-платформи як основний інструмент навчання, мали великі труднощі з комунікацією з іншими учнями та отримували низькі оцінки за соціальну підтримку.

Ще однією проблемою, пов'язаною з використанням онлайн-платформ, є віддаленість від викладача та відсутність можливості отримати негайну відповідь на запитання. У традиційній освіті студенти можуть задавати запитання та отримувати відповіді від викладача під час занять. Однак, на онлайн-платформах, зокрема в масових відкритих онлайн-курсах, цей процес може бути ускладненим через велику кількість студентів та відсутність особистого контакту з викладачем. Для вирішення цих проблем необхідно приймати заходи щодо підвищення безпеки даних, такі як використання сучасних технологій

шифрування та двохфакторної аутентифікації. Крім того, потрібно приділяти більше уваги соціальній інтерактивності в онлайн-навчанні, наприклад, пропонуючи можливості для спілкування з іншими учнями та організовуючи спільні проекти та дискусії. Такі заходи допоможуть створити більш комфортне та інтерактивне навчальне середовище, яке буде більш привабливим для учнів та підвищить якість освіти. Також слід враховувати, що онлайн-навчання не повинно повністю заміняти традиційні методи навчання, а повинно використовуватись як доповнення до них. Традиційні методи навчання, такі як спілкування в класі, взаємодія з вчителями та співпраця з іншими учнями, мають важливе значення для розвитку соціальних навичок та особистісного зростання учнів. Також не всі типи матеріалів можна ефективно навчати онлайн. Деякі навчальні дисципліни, такі як музика, образотворче мистецтво та фізична культура, вимагають присутності вчителя та реальної взаємодії з іншими студентами.

Висновки. У даній науковій роботі були розглянуті основні аспекти використання онлайн-платформ в освіті. Були розглянуті різні типи платформ, такі як мобільні додатки, онлайн-курси, вебінари та інші, а також технологічні можливості, які дозволяють створювати унікальні та інтерактивні навчальні матеріали та інструменти для саморозвитку.

Далі були представлені практичні приклади використання онлайн-платформ у різних освітніх установах та була показана їхня ефективність. Однак були виявлені проблеми, пов’язані з безпекою даних, недостатньою соціальною інтерактивністю та можливою заміною традиційних методів навчання. В результаті аналізу було зроблено висновок, що онлайн-навчання повинно розглядатися як доповнення до традиційних методів навчання, а не як їхня повна заміна. Використання онлайн-платформ в освіті може значно розширити можливості навчання та забезпечити доступність освіти для всіх категорій населення. Для того, щоб ефективно використовувати онлайн-платформи в освіті, необхідно вирішувати проблеми, пов’язані з безпекою даних та соціальною інтерактивністю, та стимулювати розвиток таких платформ з урахуванням індивідуальних потреб учнів. Також слід забезпечувати підтримку для традиційних методів навчання та використовувати онлайн-платформи в поєднанні з ними.

Список використаних джерел

1. The Chronicle of Higher Education. «Coursera Announces Details for Selling Certificates and Verifying Identities» \\ Режим доступу: http://chronicle.com/blogs/wiredcampus/coursera-announces-details-for-selling-certificates-and-verifying-identities/ (останнє звернення 30.03.2023)
2. «Benefits of e-learning», eLearning Industry \\ Режим доступу: https://elearningindustry.com/ benefits-of-elearning (останнє звернення 30.03.2023р.)
3. Understanding Different Types Of Online Education \\ Режим доступу: https://www. edtechreview.in/elearning/understanding-different-types-of-online-education/ (останнє звернення 30.03.2023р.)
4. 8 Reasons Your Company Should Prioritize Remote Learning \\ Режим доступу: https://www.learndash.com/8-reasons-your-company-should-prioritize-remote-learning/ (останнє звернення 30.03.2023р.)
5. The New Story of Online Education Has Yet To Be Written \\ Режим доступу: https://elearningindustry.com/the-new-story-of-online-education-has-yet-to-be-written (останнє звернення 30.03.2023р.)
6. «Top eLearning Authoring Tools», eLearning Industry \\ Режим доступу: https://elearningindustry.com/directory/software-categories/elearning-authoring-tools (останнє звернення 30.03.2023р.)
7. Udemy. «Udemy: Online Courses Anytime, Anywhere» \\ Режим доступу: https://www.udemy. com/about/ (останнє звернення 30.03.2023р.)

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ПАЛАГУТИ К. О.

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ НА ПІДПРИЄМСТВІ

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

У статті розглянуто основні принципи, методи та засоби захисту персональних даних. Розглядаються найбільш поширені загрози для безпеки персональних даних в інтернеті, такі як хакерські атаки, шахрайство та фішинг. Зазначено особливості зберігання персональних даних у безпечному місці і захист їх від несанкціонованого доступу, оскільки використання цих даних може стати причиною крадіжки особистої інформації, фінансового шахрайства та інших злочинів. Досліджено процес захисту конфіденційності, цілісності та доступності персональної інформації, що збирається та обробляється підприємствами, державними установами та іншими суб'єктами обробки персональних даних

The article discusses the basic principles and methods of protecting personal data. The most common threats to the security of personal data in the internet, such as hacking attacks, fraud, and phishing, are examined. The article highlights the peculiarities of storing personal data in a secure location and protecting it from unauthorized access, as the use of such data can lead to theft of personal information, financial fraud, and other crimes. The process of protecting the confidentiality, integrity, and availability of personal information collected and processed by businesses, government agencies, and other data processors is also explored.

Актуальність. На сьогоднішній день питання захисту персональних даних постає особливо гостро для державних установ та підприємств, які в силу своєї діяльності агрегують та використовують відомості про фізичну особу. Відповідно Закону України «Про захист персональних даних», Закону «Про захист інформації в інформаційно-телекомунікаційних системах» та багатьох підзаконних нормативних актів такі відомості повинні захищатись від несанкціонованого ознайомлення, модифікації та розповсюдження. На тлі стрімкого розвитку технологій інформація про людину стала цінним товаром, а оборот ринку, де торгують персональними даними, оцінюється мільярдами доларів. Підписавши Угоду про асоціацію з ЄС, Україна погодилась на забезпечення захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів. Тому ухвалення нового закону «Про захист персональних даних» є обов'язковим для інтеграції України в ЄС. Виходячи з євроінтеграційних прагнень України, ухвалення цього закону має особливу важливість, адже для того щоб наша держава стала повноцінним членом ЄС, ми повинні відповідати стандартам Євросоюзу в різних галузях. І одна з таких галузей – це забезпечення права на приватність, іншими словами – захист персональних даних.

Захист персональних даних є важливою темою в сучасному світі, оскільки зростає кількість зловмисників, які намагаються використовувати ці дані зі злочинними цілями. Тому необхідно дотримуватися певних правил та процедур, щоб забезпечити захист персональних даних.

Мета статті – проаналізувати механізми захисту персональних даних користувачів.

Об'єктом дослідження є аналіз методів та засобів захисту персональних даних користувачів на підприємстві.

Предмет дослідження – персональні дані користувачів на підприємстві.

Аналіз попередніх досліджень. На сьогодні саме персональні дані та інформація є знаряддям гібридної війни Російської Федерації проти нашої держави. Інформація використовується як інструмент скоєння правопорушень, також активно використовується в політиці і веденні інформаційних війн. Вивченням проблематики захисту персональних

даних займались провідні науковці О.О. Золотар, А.Ю. Нашинець-Наумова, Т.С. Перун, А.Ю. Щербіна. Проте, сьогоденний стан теоретико-практичного забезпечення адміністративно-правового режиму інформаційної безпеки в Україні, не в повній мірі відповідає вимогам ситуації, що склалася у зв'язку з веденням Російською Федерацією війни проти України.

Виклад основного матеріалу. У сучасних умовах суспільного розвитку, питання захисту персональних даних активно обговорюється не лише на національному рівні, а й на міжнародному. Це спричинено основною мірою вчинення правопорушень щодо незаконних дій щодо персональних даних осіб, що є суб'єктами певних міжнародних операцій [1].

Одним з найбільш проблемних питань в еру інформаційних технологій є захист персональних даних. До того ж у світі, поглиненому глобалізацією, дані користувача однієї країни можуть використовувати треті особи з будь-якого куточка світу (в тому числі незаконно). Проблеми захисту персональних даних можуть виникати в різних сферах життя, включаючи інтернет, медичну та фінансову галузі, державні органи, мережі соціальних мереж та інші. Персональні дані − це будь-яка інформація, що може ідентифікувати конкретну особу. Це може бути ім'я, адреса, номер телефону, адреса електронної пошти, фотографії, номери документів тощо. Відповідно до Закону України «Про захист персональних даних», персональні дані класифікуються на три категорії [2]:

1. Загальні персональні дані − це інформація про фізичну особу, яка ідентифікується або може бути ідентифікована, включаючи, наприклад, ім'я, прізвище, адресу, номер телефону, електронну адресу тощо.

2. Спеціальні категорії персональних даних − це інформація про расу, національність, політичні переконання, релігійні чи філософські переконання, стан здоров'я, статеву орієнтацію, сексуальну поведінку та інші особливо чутливі дані.

3. Біометричні персональні дані − це інформація, яка отримується в результаті біометричної ідентифікації фізичної особи, така як відбитки пальців, голос, обличчя, форма долоні та інші біометричні ознаки.

Закон України «Про захист персональних даних» встановлює спеціальні правила щодо обробки кожної з цих категорій персональних даних. Так, для обробки спеціальних категорій персональних даних потрібно отримати додаткову згоду фізичної особи або мати іншу підставу для такої обробки. А обробка біометричних персональних даних можлива лише за згодою фізичної особи або за наявності іншої підстави, встановленої законодавством.

Персональні дані можуть бути класифіковані за різними критеріями. Найбільш поширеною класифікацією є та, яка відповідає регуляторному середовищу Європейського Союзу, зокрема захищених Загальним регламентом про захист персональних даних (GDPR), який захищає конфіденційність таких даних: основна інформація про особу; веб-дані; IP-адреса; дані-cookie та теги RFID; біометричні дані тощо. Ця класифікація дозволяє розуміти, які типи персональних даних збираються та обробляються компаніями та організаціями (Рис. 1) [1, 3, 5].

Щоразу після оцінювання відповідного рівня захисту варто враховувати ризики, які спричиняє обробка, зокрема випадкове або незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних. GDPR вказує на шифрування, як на основну вимогу безпеки даних. Окрім цього, підприємствам потрібно оцінити ризики, а потім вжити заходів, що пом'якшують ризики, які вони виявляють. Оскільки жодне підприємство не може повністю визначити або передбачити всі ризики для своїх даних, і жоден підхід до периметра безпеки не є надійним, підприємства повинні шифрувати свої дані, щоб забезпечити відповідність до GDPR [4]. За допомогою шифрування, не залежно від того чи є порушення, дані будуть належно захищені. Ядром системи захисту є програмно-апаратний комплекс Keysecure, залежно від типу даних. Навколо Keysecure, залежно від типу даних, що мають захищатися, архітектури системи зберігання даних та сервісів, що беруть участь в обробці даних, можна застосовувати такі програмні продукти Gemalto:

- ProtectV – для шифрування диків віртуальних машин VMWare, AWS, Asure;
- ProtectDB – для шифрування баз даних Oracle, MS SQL, IBM DB2, Teradata;

• ProtectFile – для вибіркового шифрування папок та файлів на робочих станціях користувачів та файлових серверах Windows Linux.

Рис. 1. Вимоги до обробки персональних даних згідно GDPR

Gemalto пропонує широкий вибір продуктів для забезпечення надійної аутентифікації користувачів, що складається з аутентифікаторів на основі особистого сертифікату користувача (eToken, Smartcard MD Prime), генераторів одноразових паролів (Mobile PASS), систем (SAC, SAM, SAS, Network Logon)

Важливо зберігати персональні дані у безпечному місці і захищати їх від несанкціонованого доступу, оскільки використання цих даних може стати причиною крадіжки особистості, фінансового шахрайства та інших злочинів. Згідно з GDPR, персональні дані можуть бути класифіковані наступним чином:

1. Основні персональні дані − це дані, які можуть ідентифікувати конкретну особу, такі як ім’я, прізвище, адреса, номер телефону та ін.

2. Спеціальні категорії персональних даних − це дані, які стосуються особливих категорій осіб, таких як інформація про расову або етнічну належність, політичні переконання, релігійні переконання, громадянство, генетичні та біометричні дані, стан здоров’я та інші.

3. Дані про користувача − це дані, які збираються на основі взаємодії користувача з продуктом або послугою, такі як IP-адреса, історія перегляду, дані про використання тощо.

4. Дані про транзакції − це дані, які стосуються фінансових транзакцій, такі як дані про кредитні картки та банківські рахунки.

5. Дані про місцезнаходження − це дані, які пов’язані з місцезнаходженням користувача, такі як GPS-координати та інші дані про місцезнаходження.

За рівнем конфіденційності персональні дані можна поділити на дві категорії: загальнодоступні та конфіденційні. Загальнодоступні дані − це дані, які доступні для загального використання та не містять конфіденційної інформації, такі як ім’я, адреса електронної пошти та номер телефону. Конфіденційні дані − це дані, що містять особисту інформацію, таку як медична інформація, фінансові дані, номера соціального страхування тощо. За призначенням персональні дані можна класифікувати на декілька видів: для ідентифікації, для контактів, для відслідковування та інших цілей. Дані для ідентифікації містять інформацію, яка дозволяє ідентифікувати конкретну особу, наприклад, ім’я, прізвище та дата народження.

Витік персональних даних може бути наслідком багатьох факторів, включаючи кібератаки, недостатньо захищені мережі та пристрої, недбале ставлення до обробки даних та несанкціонований доступ до інформації. Ось деякі загрози, які пов'язані з витоком персональних даних [2, 4]:

1. Крадіжка особистої інформації: злочинці можуть використовувати викрадені персональні дані, щоб скоїти шахрайства, відкрити кредитні картки, взяти кредити чи отримати інші види фінансових послуг на ім'я потерпілого.

2. Соціальна інженерія: злочинці можуть використовувати викрадені персональні дані, щоб переконати людей поділитися іншою конфіденційною інформацією.

3. Рекламні кампанії: деякі компанії можуть збирати та продавати персональні дані, щоб показувати рекламу, яка пристосована під конкретного користувача. Однак, якщо ці дані потраплять у руки зловмисників, вони можуть бути використані для здійснення шахрайств.

4. Викрадення конфіденційної інформації: викрадені персональні дані можуть містити конфіденційну інформацію про бізнеси та їх клієнтів. Ця інформація може бути використана для здійснення крадіжок і торгівлі на чорному ринку.

Кібератаки − це одна з найбільш серйозних загроз для безпеки персональних даних. Кібератаки можуть бути спрямовані на викрадення, втручання або вивчення персональних даних. Ось деякі типи кібератак, які можуть бути спрямовані на персональні дані:

- Фішинг − атака, в якій злочинці намагаються зловити користувачів шляхом підробки веб-сайтів або електронних листів, щоб отримати доступ до їх персональних даних, таких як ім'я, адреса електронної пошти, пароль тощо.
- Віруси і шпигунське програмне забезпечення − програми можуть бути розроблені для збору персональних даних користувачів без їх знання або згоди. Віруси можуть також використовуватися для знищення або зміни персональних даних. Розповсюдження шкідливих програм − атака, при якій зловмисники використовують вразливості в програмному забезпеченні, щоб отримати доступ до персональних даних. Шкідлива програма може бути розповсюджена через електронну пошту, файлообмінні мережі, підроблені веб-сайти.
- DDoS-атаки − атаки, в яких злочинці використовують ботнет, щоб перенавантажити сервер веб-сайту, що призводить до його недоступності. Ця атака може бути використана для викрадення персональних даних з серверів веб-сайту.
- SQL-ін'єкції − атаки, в яких злочинці використовують вразливості в програмному забезпеченні веб-сайту, щоб отримати доступ до бази даних, де зберігаються персональні дані користувачів.
- Zero-day атаки − атаки, в яких злочинці використовують вразливості в програмному забезпеченні, які ще не були виявлені розробниками або ще не були виправлені.

Персональні дані потрібно захищати з багатьох причин. По-перше, такі дані містять конфіденційну інформацію про особу, що може бути використана для крадіжки особистості, злочинних дій або недобросовісної діяльності. По-друге, захист персональних даних є важливою складовою прав людини на приватність, інші конституційні та законодавчі права, що забезпечують гідність та свободу особи. Крім того, велика кількість компаній та установ збирають та зберігають персональні дані своїх клієнтів, співробітників та інших осіб. Ці дані можуть бути використані для різних цілей, наприклад, для реклами, маркетингу, аналітики, наукових досліджень тощо. Однак, це також означає, що зберігання та обробка персональних даних потребують дотримання певних стандартів та законодавчих вимог, щоб уникнути порушення приватності та інших прав особи.

Захист персональних даних – це процес захисту конфіденційності, цілісності та доступності персональної інформації, що збирається та обробляється підприємствами, державними установами та іншими суб'єктами обробки персональних даних. Це може включати будь-які дії з персональною інформацією, такі як збір, зберігання, використання, передача та видалення. Захист персональних даних є важливою проблемою в інформаційному суспільстві, оскільки все більше людей використовують Інтернет і здають свої

персональні дані на зберігання. Основні принципи захисту персональних даних включають (Рис. 2) [5]:

1. Збір та обробка персональних даних повинні здійснюватися лише за наявності згоди власника даних або на законній підставі. Обробка персональних даних має здійснюватися на законній підставі, відповідно до засад справедливості та прозорості.

2. Легальність, справедливість та прозорість – персональні дані повинні збиратися та оброблятися законно, справедливо та прозоро.

3. Обмеження фінальності – персональні дані повинні збиратися тільки для визначених, конкретних та законних цілей.

4. Точність – персональні дані повинні бути точними та актуальними.

5. Обмеження зберігання – персональні дані повинні зберігатися лише протягом необхідного часу. Збереження персональних даних повинно здійснюватися в безпечному та захищеному від несанкціонованого доступу місці.

6. Дані мають бути оброблені тільки у визначені цілях, за якими вони були зібрані. Дані мають бути достовірні, повні та актуальні.

7. Мінімізація обробки – обробка персональних даних має обмежуватись лише тими даними, які є необхідними.

8. Конфіденційність та безпека – означає, щоб персональні дані були захищені від несанкціонованого доступу, втрати, зміни або пошкодження, а також щоб вони оброблялися відповідно до вимог конфіденційності та безпеки.

Рис. 2. Основні принципи захисту персональних даних

Основні проблеми захисту персональних даних включають:

1. Втрата даних: компанії можуть втратити дані через неналежне зберігання, катастрофи або технічні проблеми. Це може призвести до втрати особистих даних та порушення приватності.

2. Крадіжка даних: хакери можуть зламати систему безпеки компанії і отримати доступ до бази даних з персональними даними користувачів. Це може стати причиною крадіжки особистих даних та ідентифікації особи.

3. Крадіжка даних: хакери можуть зламати систему безпеки компанії і отримати доступ до бази даних з персональними даними користувачів. Це може стати причиною крадіжки особистих даних та ідентифікації особи.

4. Використання даних без дозволу: деякі компанії можуть використовувати персональні дані користувачів без їхньої згоди для реклами, маркетингу або інших цілей. Це може порушувати права на приватність користувачів.

5. Недостатній захист даних: компанії можуть мати недостатній рівень захисту даних, що може стати причиною крадіжки та витоку персональних даних.

6. Спільний доступ до даних: деякі компанії можуть передавати персональний доступ користувачам.

Типові підходи аналізу, організації та забезпечення захисту персональних даних під час їх автоматизованої обробки включають в себе [3, 5]:

- класифікацію інформації в інформаційно-телекомунікаційній системі (ІТС) з визначенням окремих характеристик та технологій обробки персональних даних;
- реалізацію відповідних юридично-правових та організаційно-розпорядчих заходів щодо використання персональних даних на підприємстві;
- підготовка договорів та протоколів із фізичними особами щодо використання їх персональної інформації;
- підготовка відповідних внутрішніх розпоряджень щодо експлуатації автоматизованих систем, призначених для обробки персональних даних;
- підготовка відповідних регламентних документів щодо доступу та використання персональних даних, які збираються та накопичуються в рамках баз даних;
- виконання робіт для реєстрації бази персональних даних в рамках єдиного Державного реєстру баз персональних даних;
- створення комплексної системи захисту інформації в автоматизованих системах, призначених для обробки персональних даних відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закону «Про захист персональних даних»;
- організація та проведення державної експертизи комплексної системи захисту інформації в автоматизованих системах, призначених для обробки персональних даних.

Існує багато технологій захисту персональних даних, які можуть бути використані для захисту конфіденційної інформації: шифрування даних, хешування, маскування даних, техніки розподілу ключів, безпечний протокол передачі, безпечне зберігання даних, багаторівневий доступ до даних, контроль доступу, антивірусне програмне забезпечення, захист мереж, аутентифікація користувача, захист пристроїв [2, 6].

Шифрування даних − це процес перетворення звичайного тексту в зашифрований варіант, який може бути прочитаний лише за допомогою ключа шифрування. Шифрування може бути застосоване до різних типів даних, включаючи електронні повідомлення, файли, бази даних та інші. Криптографія використовується для забезпечення конфіденційності та цілісності даних шляхом шифрування даних, щоб зробити їх нерозбірливими для сторонніх користувачів. Два основні методи криптографії − симетричний та асиметричний [6]. Хешування: хеш-функції перетворюють вхідні дані будь-якої довжини в фіксований вихідний розмір. Це дозволяє використовувати дані, не розкриваючи їх в оригінальному форматі.

Маскування даних − метод захисту персональних даних використовується для забезпечення конфіденційності даних, замінюючи значення чутливих даних на значення, які є безпечними для публічного використання. Наприклад, можна замаскувати персональні дані, такі як ім’я та адреса, залишивши тільки першу літеру.

Техніки розподілу ключів − методи, які дозволяють безпечно розподілити ключі шифрування між декількома користувачами, що забезпечує безпеку при обміні даними. Підписи − математичний метод, що дозволяє довести автентичність даних. Підписи створюються з використанням приватного ключа і перевіряються з використанням відкритого ключа. Безпечний протокол передачі даних − такий протокол забезпечує захист від перехоплення та зміни даних під час їх передачі по мережі. Найбільш поширеними протоколами є HTTPS, SSH, SFTP та інші. Безпечне зберігання даних − це використання

спеціальних алгоритмів та методів для забезпечення безпеки даних під час їх зберігання на сервері або в базі даних. Найбільш поширеними методами є резервне копіювання даних, контроль цілісності даних та їх реплікація на різних серверах.

Багаторівневий доступ до даних − це використання різних рівнів доступу до даних залежно від рівня доступу користувача. Наприклад, для адміністраторів доступ до конфіденційної інформації може бути обмеженим, а для звичайних користувачів − обмеженим лише до відкритої інформації. Контроль доступу − це технологія, що забезпечує обмеження доступу до конфіденційної інформації лише для користувачів, які мають необхідні дозволи для цього. Контроль доступу може використовувати методи, такі як базова та двофакторна аутентифікація або ідентифікація по IP-адресі. Аутентифікація користувача − процес перевірки, що користувач, який намагається отримати доступ до системи, є тим, за кого він себе видає. Може включати в себе використання пароля, біометричних даних, токенів або інших методів ідентифікації користувача.

Антивірусне програмне забезпечення − це програмне забезпечення, що допомагає захистити комп'ютер від вірусів та шкідливих програм, які можуть призвести до витоку персональних даних. Захист мереж − це технології, які використовуються для захисту мережі від атак зовнішніх користувачів, таких як хакери. Це може включати в себе використання мережевих файрволів, систем виявлення вторгнень та інших технологій. Захист пристроїв − це технології, які використовуються для захисту пристроїв від зловмисних програм та інших загроз безпеці, що можуть використовувати вразливості операції.

Висновки. Захист персональних даних користувачів в інтернеті є надзвичайно важливим, оскільки використання цих даних без дозволу може призвести до серйозних наслідків, таких як крадіжка особистої інформації, фінансові та інші злочини. Основні методи і засоби захисту персональних даних включають криптографію, хешування, перетворення, маскування даних, сильні паролі, двофакторну автентифікацію та засоби шифрування даних для забезпечення максимального захисту особистої інформації. Для того, щоб захистити свої персональні дані, користувачам слід також звертати увагу на дотримання вимог законодавства з питань захисту персональних даних та бути обережними при наданні своєї особистої інформації в інтернеті. Для забезпечення максимального захисту персональних даних необхідно використовувати всі доступні засоби та методи захисту, щоб зменшити ризики їхньої крадіжки та зловживання.

Список використаних джерел

1. Мачуський В. Захист персональних даних на підприємстві. URL: https://www.businesslaw.org.ua/zahyst-personalnyx-danyx-na-pidpryemstvi/
2. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.
3. Щербіна А.В., Макушев П.В. Поняття персональних даних та загальні правові засади їх використання: іноземний досвід. Право і суспільство. – 2013, № 2. – С. 70-76.
4. Німченко, Т.В. Алгоритм виявлення несанкціонованого витоку персональних даних мережевими каналами. / Т.В. Німченко, І.М. Мужик, А.І. Мужик // Вісник інженерної академії України, 2014. − № 3-4. − С. 199-203.
5. Шабатура М.М., Салашник Р.О. Аналіз методів захисту персональних даних за українським законодавством і GDPR. 2021, т. 3, 2. С. 51-57.
6. Козак В. Захист персональних даних та правила приватності при дослідженнях в Інтернет. URL: http://uam.in.ua/upload/medialibrary/de7/de7199d7eeaf41d8582cbff76d2f4368.pdf

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т. В.

ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

САМОЙЛЕНКО Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто криптографічні методи та інструменти для захисту інформації, які є важливою частиною повної системи захисту інформації. Зазначено різні методи шифрування та пояснено, що таке електронні підписи. Також проаналізовано законодавчу базу для застосування криптографічних методів захисту інформації.

The article discusses cryptographic methods and tools for information protection, which are an important part of a complete information security system. Various encryption methods are mentioned and electronic signatures are explained. The legislative framework for the use of cryptographic methods for information protection is also analyzed.

Актуальність. Для повного задоволення потреб сучасного суспільства необхідне інформаційне забезпечення всіх сфер людської діяльності і, зокрема, надійний захист інформації. Особливо гостро ця проблема постає у зв'язку з масовою комп'ютеризацією, об'єднанням комп'ютерів у комп'ютерні мережі та використання Інтернету.

Теорія захисту інформації доводить, що якщо система захисту побудована з урахуванням усіх сучасних методів і засобів захисту, а також якщо на підприємстві є ретельно відібраний і навчений персонал, який не робить помилки, то дії зловмисників у такій системі неможливі. Однак це не зовсім так. З часом система захисту застаріває, змінюється персонал і втрачається пильність, зловмисники знаходять нові способи атак і способи подолання захисту, які були невідомі на момент створення системи захисту.

Отже, якщо у вас є розуміння щодо надійності вашої інформаційної безпеки, безпеки системи, все ж слід пам'ятати основне правило: жодна система захисту не може довго протистояти цілеспрямованим діям вмілого зловмисника, озброєного сучасною технікою. Це правило розроблено багаторічним досвідом фахівців з інформаційної безпеки і є універсальним. Це не залежить від рівня захисту, доброчесності користувачів і адміністраторів, апаратного та програмного забезпечення. Правило стверджує, що проблема не в тому, чи зловмисники зламають систему захисту, а в тому, коли вони це зроблять. І мета захисту інформації полягає в тому, щоб збій системи стався якомога пізніше.

Аналіз останніх досліджень і публікацій. Проблемам створення та функціонування засобів криптографічного захисту інформації присвячено достатньо публікацій у відкритих джерелах, зокрема таких науковців, як Пономаренко В.С. [1], Вербицький О.В. [2], Хорошко В. А. [3], Фаль О.М. [4].

Пономаренко В.С. у своїх працях у системній формі розглядає питання створення симетричних та асиметричних криптографічних систем захисту інформації.

Вчений Вербицький О.В. вивчає проблеми протидії та розслідування злочинів, скоєних у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж.

Вчені Хорошко В. А. та Фаль О. М. описують засоби теорії дискового шифрування, процедури управління ключами, основи розробки та впровадження криптографічних засобів. протоколи та механізм електронного цифрового підпису.

Мета статті. Визначити та опрацювати основні криптографічні методи та засоби захисту, види шифрування. Проаналізувати програмне забезпечення іноземних та українських розробників, призначене для криптографічного захисту інформації.

Об'єктом дослідження є використання різних методів криптографічного захисту інформаційних ресурсів.

Предметом дослідження є криптографічний захист.

Виклад основного матеріалу. Одним із елементів комплексної системи захисту інформації є криптографічний захист інформації. Цей вид захисту інформації реалізується шляхом перетворення інформації за допомогою ключів на основі математичних методів. Використання криптографічних методів має дві мети – приховати інформацію шляхом її шифрування та підтвердити значущість документів за допомогою електронного цифрового підпису. Іншими словами, на думку В. В. Поповського, криптографічні методи вирішують дві задачі – забезпечення конфіденційності інформації шляхом запобігання витягу зловмисником інформації з каналу зв'язку та забезпечення цілісності інформації шляхом запобігання зміні інформації та внесенню в неї неправдивого змісту [1].

Існує два розділи науки, пов'язані з криптографічними методами: криптографія і криптоаналіз, які разом утворюють криптологію.

Криптографія вивчає математичні перетворення, які дозволяють шифрувати інформацію.

Криптоаналіз вивчає методи дешифрування без знання секретного ключа [1].

Засоби криптографічного захисту інформації поділяються на:

- засоби, що реалізують криптографічні алгоритми перетворення інформації;
- засоби, системи та комплекси захисту від нав'язування неправдивої інформації з використанням криптографічних алгоритмів перетворення інформації
- засоби, системи та комплекси, призначені для виготовлення та розповсюдження ключів криптографічний захист інформації;
- системи та комплекси, що входять до комплексів захисту інформації від несанкціонованого доступу та використовують криптографічні алгоритми перетворення інформації [2].

Засоби криптографічного захисту разом із ключем та іншими видами документації, які забезпечують необхідний рівень захисту, утворюють криптографічну систему [2]. Шифрування дозволяє захистити інформацію шляхом перетворення її в незрозумілий текст (шифртекст) з можливістю подальшого розшифрування (дешифрування). Шифрувати можна як прості тексти, так і комп'ютерні файли.

Рис. 1. Алгоритм шифрування данних

Шифрування поділяється на симетричне та асиметричне.

Симетричне шифрування використовує один секретний ключ як для шифрування, так і для дешифрування. Асиметричне шифрування використовує відкритий ключ і інший секретний ключ для дешифрування, згенерований за допомогою генераторів псевдовипадкових чисел.

Асиметричне шифрування також називається шифруванням з відкритим ключем. Недоліком симетричного шифрування є необхідність передачі ключа особі адресованого тексту, що тягне за собою його розкриття та дешифрування інформації зловмисниками. Перевагою симетричного шифрування є його вища швидкість, ніж асиметричне шифрування, оскільки асиметричне шифрування використовує довші ключі, що збільшує час шифрування.

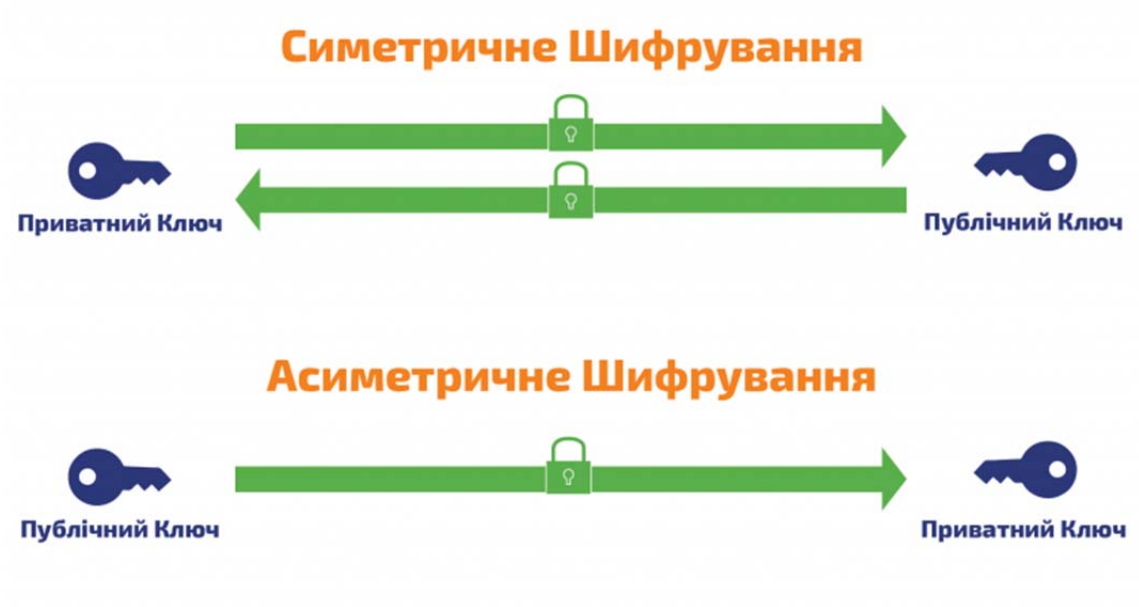

Рис. 2. Схема симетричного і асиметричного шифрування

Спосіб шифрування тексту базується на алгоритмі, і зашифрований текст можна розшифрувати лише за допомогою ключа. Для надсилання повідомлень різним одержувачам можна використовувати один алгоритм з різними ключами. Секретність визначається ключем, а не алгоритмом, оскільки більшість алгоритмів відомі широкому загалу. У зв'язку зі збільшенням продуктивності комп'ютера ймовірність знаходження ключів шляхом перебору комбінацій зростає, тому нам доводиться використовувати все довші й довші ключі, що збільшує час на шифрування [3]. Важливою характеристикою методів шифрування є їх криптостійкість, тобто для криптографічного захисту інформації в комп'ютерній мережі необхідно створити спеціальний сервіс, який генерує ключі та розповсюджує їх між користувачами мережі.

Для створення електронного підпису необхідно контрольна сума та додаткова інформація, яка шифрується за допомогою закритого ключа відправника. Щоб уникнути перехоплення та повторного використання, до підпису додається порядковий номер. Електронний підпис дозволяє підтвердити авторство документа та гарантує цілісність інформації та відсутність спроб її спотворення. Документ складається з тексту, електронного підпису та сертифіката користувача, що містить дані користувача, його ідентифікаційне ім'я та відкритий ключ дешифрування для перевірки підпису адресата документа [3].

Електронний підпис дозволяє захистити інформацію від таких злочинних дій:

– «відмова від авторства», коли автор документа відмовляється від авторства;

– «фальсифікація», коли одержувач документа його підробляє;

– «переробка», коли одержувач документа вносить зміни до нього;

– «маскування», коли користувач маскується під іншого користувача.

Для підтвердження повідомлення мають бути виконані наступні умови:

– відправник повинен поставити підпис у повідомленні, який містить додаткову інформацію, яка залежить від повідомлення та одержувача повідомлення, але відома лише відправнику;

– правильний підпис не можна зробити без додаткової інформації;

– підпис має залежати від часу, щоб старі повідомлення не могли бути використані; це відрізняє електронний підпис від рукописного;

– одержувач повинен мати можливість перевірити, що підпис належить відправнику та є правильним щодо повідомлення. Таким чином, електронний підпис – це вид пароля, який залежить від відправника, одержувача та змісту повідомлення [4].

Рис. 3. Перевірка справжності ЕЦП

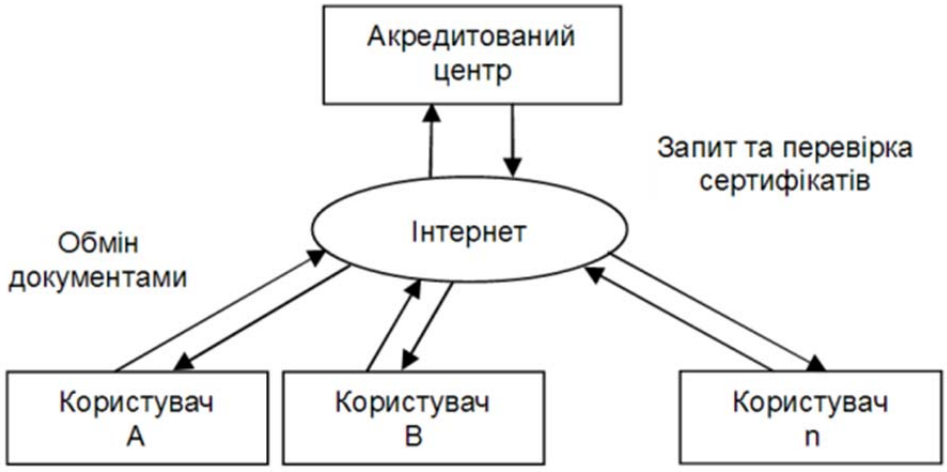

Рис. 4. Схема взаємодії користувачів електронного цифрового підпису

Відповідно до Закону України «Про електронні документи та електронний документообіг» електронний підпис є обов'язковим реквізитом електронного документу, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу та накладенням електронного підпису завершує створення електронного документа. Закон України «Про електронний цифровий підпис» визначає правовий статус електронного цифрового підпису, згідно з яким електронний цифровий підпис – це вид електронного підпису, отриманий у результаті криптографічного перетворення набору електронних даних, що додається до цього набору або логічно поєднується з ним і дозволяє підтвердити його цілісність та ідентифікацію підписувача.

Електронний цифровий підпис накладається за допомогою закритого ключа та перевіряється за допомогою відкритого ключа. Порядок криптографічного захисту інформації з обмеженим доступом, розголошення якої спричиняє (може завдати) шкоди державі, суспільству, особі в Україні визначається Положенням про порядок криптографічного захисту інформації в Україні. Згідно з цим Положенням для криптографічного захисту

інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або є власністю держави, використовуються допущені до експлуатації криптосистеми та засоби криптографічного захисту [6].

Використовуються лише засоби криптографічного захисту, які мають сертифікат відповідності [7].

Існує велика кількість програмних продуктів, призначених для криптографічного захисту інформації, як іноземних розробників, так і українських.

Однією з найкращих програм для шифрування інформації є BestCrypt від фінської компанія Jetico. Він дозволяє створити зашифрований контейнер для зберігання інформації на будь-якому типі носія і призначений для роботи як під Windows, так і під Linux. Програма може додатково використовувати один із найнадійніших алгоритмів, реалізованих із 256-бітним ключем: Rijndael (AES), Blowfish і Twofish. Новіші версії алгоритму Blowfish можуть використовувати 448-бітний ключ [8].

Також відома програма «Private Disk» від молдавської компанії «Dekart». Він дозволяє створити зашифрований віртуальний диск для зберігання інформації. Шифрування здійснюється за допомогою алгоритму AES 256. При роботі з інформацією файли на віртуальному диску мають ті ж властивості, що й незашифровані, доки користувач не заблокує доступ. Віртуальний диск захищений від вірусів, троянів і шпигунського програмного забезпечення за допомогою вбудованого Disk Firewall [9].

Є система криптографічного захисту інформації «Карма» від української компанії «NetCom Technology». Він призначений для забезпечення використання електронного цифрового підпису та шифрування, зокрема, в юридично значимому електронному документообігу. Особливістю цієї системи є можливість додавати до електронного цифрового підпису зображення власноручного підпису. В результаті електронний документ матиме вигляд паперового [10].

ТОВ «СКЗ «КриптоСофт» пропонує програмний комплекс криптографічного захисту інформації «Криптосервер» для роботи під MS Windows 8, MS Windows 10. Цей комплекс забезпечує захист даних, що передаються через незахищені публічні (Інтернет) або відкриті (наприклад, виділені лінії, MPLS) канали. Дані захищені шифруванням на основі вітчизняних алгоритмів шифрування. Максимальний рівень обмеження доступу до інформації, що захищається цим пакетом, – «конфіденційно» [11].

Висновки. Забезпечення криптографічного захисту інформаційних ресурсів є надзвичайно важливою задачею у сучасному цифровому світі. Криптографічний захист дозволяє захищати конфіденційні дані від несанкціонованого доступу та забезпечувати цілісність та автентичність інформації.

Для забезпечення криптографічного захисту використовуються різні методи, такі як симетричне та асиметричне шифрування, хеш-функції, електронні підписи та інші. Кожен з цих методів має свої переваги та недоліки, тому їх використання залежить від конкретної ситуації.

При забезпеченні криптографічного захисту необхідно враховувати різні атаки, такі як перехоплення, підроблення, внесення змін та інші. Тому важливо використовувати потужні алгоритми та ключі відповідної довжини для захисту інформації.

Забезпечення криптографічного захисту є складним процесом, який потребує високої кваліфікації фахівців та великої уваги до деталей. Однак, правильно реалізований криптографічний захист може забезпечити високий рівень безпеки інформаційних ресурсів.

Криптографія – це сукупність методів перетворення даних, спрямованих на приховування їх інформаційного змісту. Система криптографічного захисту інформації – це сукупність криптографічних алгоритмів, протоколів і процедур для формування, поширення, передачі та використання криптографічних ключів. Саме повідомлення називається відкритим текстом. Зміна зовнішнього вигляду повідомлення для приховування його суті називається шифруванням. Криптографічний захист може забезпечити умови конфіденційності та цілісності передавання даних у відкритих мережах, а також анонімність об’єкта та умови його залучення до DIR.

Криптографічний захист є необхідним елементом сучасної інформаційної безпеки. Він дозволяє зберегти конфіденційність, цілісність та доступність інформації в різних сферах діяльності, таких як банківський сектор, медицина, військова та державна сфери, торгівля та інші.

Криптографічний захист реалізується за допомогою різних методів шифрування та електронних підписів. Ці методи забезпечують захист інформації від несанкціонованого доступу, змін та втрати. Крім того, законодавча база в різних країнах визначає правила використання криптографічних методів в різних сферах діяльності.

Забезпечення криптографічного захисту вимагає комплексного підходу та регулярного оновлення заходів захисту. Крім того, важливо використовувати надійні криптографічні методи та інструменти, які відповідають сучасним вимогам безпеки. Використання криптографічних методів захисту інформації є необхідністю для забезпечення безпеки від зловмисних атак та збереження конфіденційної інформації.

Список використаних джерел

1. Пономаренко, В. С., Журавльова, І. В., і Туманов, В. В. (2003). *Основи захисту інформації: навчальний посібник*. Харків: Вид. ХДЕУ.
2. Вербицький, О. В. (2018). *Вступ до криптології.* Львів: Вид-во НТЛ.
3. Хорошко, В. А., і Чекатков А. А. (2017). *Методи і засоби захисту інформації.* Київ: Юніор.
4. Фаль, О. М. (2003). *Криптографія: основні ідеї та застосування.* Київ: ІВЦ Видавництво «Політехніка».
5. *Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV.* URL: http://zakon4.rada.gov.ua/laws/show/851-15 (станом на 26.03.2023).
6. *Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV.* URL: http://zakon4.rada.gov.ua/laws/852-15 (станом на 26.03.2023).
7. *Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 № 505/98*. URL: http://zakon4.rada.gov.ua/laws/show/505/98 (станом на 26.03.2023).
8. Private Disk – найкраща програма для шифрування файлів. URL: http://www.private-disk.net (станом на 26.03.2023).
9. *Система «KARMA». Універсальна система криптографічного захисту інформації (н.д.).* URL: http://www.eos.com.ua/eos/ua/products/carma (станом на 26.03.2023).
10. Сіра, О., і Каткова, Т. (2017). Formation of securities portfolio under conditions of uncertainty. *Eastern-European Journal of Enterprise Technologies*, 1(4 (85)), 49–55. https://doi.org/10.15587/1729-4061.2017.9228 [in English].
11. Раскін, Л., Сіра, О., і Каткова, Т. (2019). Dynamic problem of formation of securities portfolio under uncertainty conditions. *EUREKA Physics and Engineering*,6, 73–82. https://doi.org/10.21303/2461-4262.2019.00985 [in English].

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ЗВЄРЄВА В. П.

ДОСЛІДЖЕННЯ ШЛЯХІВ ІДЕНТИФІКАЦІЇ ПОРУШНИКА В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

САСІН Є., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто різні методи та технології ідентифікації порушника в IT-системах та мережах, зокрема, системи виявлення вторгнень (IDS,IPS), машинне навчання та штучний інтелект, аналізу журналів подій, відслідковування поведінки користувача тощо. Також будуть розглянуті технології захисту від DDoS-атак та інших шкідливих впливів на мережу.

The article discusses various methods and technologies for identifying intruders in IT systems and networks, including intrusion detection systems (IDS, IPS), machine learning and artificial intelligence, event log analysis, user behavior tracking, and more. The technologies for protecting against DDoS attacks and other harmful influences on the network will also be considered.

Актуальність : В сучасному світі, інформаційні технології стали невід'ємною частиною життя людей та бізнес-процесів. За останні роки кількість кібератак та інших інформаційних загроз значно збільшилась, що свідчить про необхідність підвищення рівня захисту інформації та ідентифікації порушників.

З метою захисту інформації та забезпечення безпеки користувачів, компанії та установи вкладають значні зусилля в розробку та вдосконалення методів ідентифікації порушників в інформаційно-комунікаційних системах та мережах. Це включає в себе розробку нових технологій, таких як машинне навчання, біометричні технології та аналіз мережевого трафіку, а також поєднання цих технологій для розробки комплексних систем ідентифікації порушників. Оскільки розвиток інформаційних технологій не зупиняється, а навпаки, прискорюється, проблема ідентифікації порушників в інформаційно-комуніка-ційних системах та мережах є надзвичайно актуальною і потребує постійного вдосконалення та дослідження.

Злочинці використовують різні методи, щоб отримати нелегальний доступ до конфіденційної інформації, налагоджують ботнети, проводять фішингові атаки, вимагають викуп зашифрованої інформації, та інше. Такі напади можуть призвести до серйозних наслідків, таких як втрата конфіденційної інформації, викрадення грошей, порушення роботи систем та мереж, та інше. Тому, ідентифікація порушника є надзвичайно важливою задачею, яка дозволяє вчасно виявляти та реагувати на потенційні загрози. При цьому, потрібно зазначити, що швидкість та ефективність ідентифікації порушника залежить від рівня захисту системи та мережі, та застосованих методів і технологій.

Крім того, стаття зосередить увагу на питаннях приватності та захисту персональних даних під час процесу ідентифікації порушника. Будуть розглянуті способи забезпечення конфіденційності та захисту даних користувачів.

Мета статті :Проаналізувати способи ідентифікації порушення безпеки в інформа-ційно комунікаційних системах та мережах.

Об'єктом дослідження є безпека інформаційно-комунікаційних систем та мереж.

Предмет дослідження – засоби ідентифікації порушника та забезпечення безпеки в IT-системах.

Аналіз попередніх досліджень – попередні дослідження на тему ідентифікації порушника в інформаційно-комунікаційних системах та мережах відображають актуальність даної проблеми та її складність. Нижче представлено огляд деяких з них.

Стаття «Технології захисту в інформаційно-комунікаційних системах» авторства А. В. Жилін, О. М. Шаповал, О. А. Успенський була опублікована в 2020 році [1]. У статті автори досліджують проблему оцінки ризиків виникнення кібератак на мережеві пристрої. Вони наводять приклади різних типів кібератак та їх можливі наслідки, а також описують загрози, які створюються різними типами мережевих пристроїв. Автори також пропонують методику оцінки ризиків, яка базується на підходах до аналізу вразливостей та вимог до захисту інформації. Автори проводять експерименти з оцінки ризиків виникнення кібератак на мережеві пристрої за допомогою розробленої методики. Вони порівнюють отримані результати з іншими методами оцінки ризиків та наводять приклади можливих заходів для зменшення ризиків виникнення кібератак, а також вказують на необхідність подальшого дослідження даної проблеми з урахуванням змін у технологічному середовищі.

Стаття «Аналіз ризиків безпеки інформаційної системи іт-підприємства» за авторства Карпович І.М, Гладка О.М, Наконечна Ю.А. була опублікована в 2020 році [2]. В статті досліджується проблема оцінки інформаційної безпеки корпоративних інформаційних систем (КІС). Автори розглядають підходи до визначення інформаційної безпеки та її складових елементів, а також наводять різні класифікації загроз інформаційній безпеці, а також описуються основні методи та моделі оцінки інформаційної безпеки, зокрема методології оцінки ризику, метод аналізу вразливостей, метод визначення потреби у захисті інформації тощо. В статті наводяться переваги та недоліки кожного з методів, а також порівнюються їх застосування в різних сферах.

Загалом, попередні дослідження підтверджують необхідність розробки та впровадження ефективних методів та технологій ідентифікації порушників в інформаційно-комунікаційних мережах.

Виклад основного матеріалу. Основною метою розвитку способів ідентифікації порушників в інформаційно-комунікаційних системах та мережах є забезпечення високого рівня безпеки інформації, що зберігається та передається по цих системах. Ідентифікація порушників дозволяє реалізувати наступні цілі.

1. Запобігання кібератакам: Ідентифікація порушників дозволяє швидко виявляти зловмисників, які намагаються завдати шкоди інформації, і приймати ефективні заходи для запобігання кібератакам.

2. Підвищення рівня захисту інформації: Ідентифікація порушників дозволяє забезпечити підвищений рівень захисту інформації від несанкціонованого доступу, втрати та знищення.

3. Покращення ефективності виявлення інцидентів: Ідентифікація порушників дозволяє швидко виявляти та локалізувати інциденти, що відбуваються в мережі, і вчасно приймати заходи для їх вирішення.

4. Забезпечення відповідності нормативним вимогам: В деяких секторах, наприклад, у фінансовій та медичній галузях, ідентифікація порушників є вимогою нормативно-правових актів та стандартів.

5. Зниження ризику фінансових втрат: Ідентифікація порушників дозволяє зменшити ризик фінансових втрат, які можуть виникнути в результаті кібератак.

Порушники в ІТ системах можуть мати різні цілі, в залежності від їх мотивації та потреб. Основні цілі порушників в ІТ системах можуть включати:

Отримання конфіденційної інформації: Порушники можуть бути зацікавлені в отриманні конфіденційної інформації, такої як банківські реквізити, паролі, персональні дані та інші конфіденційні дані. Вони можуть використовувати отриману інформацію для злочинних цілей, таких як крадіжка грошей, шахрайство, викрадення ідентичності та інші.

Викрадення грошей: Порушники можуть намагатися викрасти гроші з банківських рахунків, використовуючи крадіжку банківських реквізитів, фішинг та інші методи.

Навмисне завдання шкоди: Порушники можуть намагатися завдати шкоди системам та мережам, використовуючи віруси, шкідливі програми, вразливості та інші методи. Це може призвести до втрати даних, перерв у роботі систем та інших негативних наслідків.

Викрадення ідентичності: Порушники можуть намагатися викрасти ідентичність користувача, отримавши доступ до їх облікового запису та використовуючи його для злочинних цілей, таких як шахрайство, крадіжка грошей та інші.

Експлуатація комп'ютерних ресурсів: Порушники можуть намагатися використовувати комп'ютерні ресурси, такі як обчислювальна потужність та мережева пропускна здатність, для виконання своїх завдань, таких як криптовалютний майнінг.

Новітні способи та тактики протидії порушникам ІТ безпеки постійно еволюціонують, тому їх може бути багато. Ось декілька прикладів:

Машинне навчання та штучний інтелект: Використання машинного навчання та штучного інтелекту для виявлення аномальної поведінки та ідентифікації загроз може допомогти в ранньому виявленні порушників. Метод машинного навчання відіграє важливу роль у виявленні порушників в інформаційно-комунікаційних системах та мережах. Застосування методів машинного навчання може допомогти в ідентифікації зловмисних дій та зниженні ризику кібератак.

Основна ідея полягає в тому, що система машинного навчання отримує доступ до великої кількості даних про поведінку користувачів та інформаційних процесів, і на їх основі будує модель нормальної поведінки. Після цього система може виявляти незвичайні або ненормальні дії, які можуть бути індикатором зловмисних атак.

Основні методи машинного навчання, що використовуються для виявлення порушників в інформаційно-комунікаційних системах та мережах, включають:

- Навчання з учителем (supervised learning) – при цьому використовується набір даних, які містять інформацію про нормальну та аномальну поведінку. Система використовує ці дані для створення моделі, яка може виявляти ненормальну поведінку, що може бути пов'язано зі зловмисними атаками.
- Навчання без учителя (unsupervised learning) – при цьому система працює з даними, які не мають позначок про нормальну та аномальну поведінку. Система сама намагається знайти патерни та залежності в даних, що можуть бути пов'язані зі зловмисною діяльністю.
- Півнавчання (semi-supervised learning) – при цьому використовуються як дані з позначками, так і без них. Така модель дозволяє покращити якість виявлення аномальної поведінки в порівнянні з навчанням без учителя.

Багатофакторна аутентифікація: Використання більш надійної багатофакторної аутентифікації (наприклад, використання паролю та додаткового підтвердження, такого як відбиток пальця або обличчя) може зменшити ризик несанкціонованого доступу до системи.

Системи виявлення вторгнень: Використання систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS) може допомогти виявити та блокувати загрози в реальному часі. Два загальних метода виявлення, що використовуються однаково інструментами IDS та IPS, – це виявлення на основі підписів та виявлення на основі аномалії. IDS та IPS, які використовуються для визначення підписів які відповідають профілю відомих атак. Атаки виявляються за допомогою вивчення шаблонів даних, заголовків пакетів, адрес джерела та пунктів призначення. Виявлення на основі підписів є чудовим для виявлення встановлених атак. Однак виявлення на основі підписів неефективне при виявленні атак з нульовим днем, які не відповідають іншим встановленим підписам атаки.

Тестування вразливостей: Регулярне тестування вразливостей може допомогти виявити потенційні проблеми з безпекою та забезпечити швидке виправлення недоліків.

Моніторинг системи: Системний моніторинг може допомогти виявити незвичайну активність або аномальну поведінку в ІТ системі. Це може бути здійснено за допомогою спеціальних програмних засобів, які записують дії користувачів, системні події та інші параметри.

Журналізація даних: Ведення детальних журналів дій користувачів та системних подій може допомогти виявити аномальність в поведінці та діях.

Аналіз трафіку: Аналіз трафіку мережі може допомогти виявити незвичайну активність, яка може вказувати на присутність порушника в мережі.

Аудит безпеки: Аудит безпеки може допомогти виявити потенційні проблеми з безпекою в системі та допомогти зрозуміти, які заходи є необхідними для забезпечення захисту.

Кібербезпекові вправи: Проведення кібербезпекових вправ та тренувань для перевірки та підвищення рівня готовності до кібератак може допомогти компаніям та установам виявляти та захищатися від потенційних загроз.

Існує багато прикладів кібербезпекових вправ, які можуть бути проведені для перевірки та підвищення рівня готовності до кібератак. Деякі з них:

1. Соціальний інжиніринг – проведення вправ з тестування соціального інжинірингу для виявлення слабких місць у свідомості співробітників щодо кібербезпеки. Це може включати тестування співробітників на їхню готовність відповідати на підозрілі електронні повідомлення або надавати чутливу інформацію.

2. Вправи «чорного ящика» – тестування систем безпеки на можливість проникнення зловмисників. Це може включати спроби використання вразливостей в програмному забезпеченні або мережевих пристроях, щоб отримати несанкціонований доступ до системи.

3. Вправи на виявлення інцидентів – тестування реагування на кіберінциденти з метою виявлення, як швидко можна виявити та відреагувати на такі інциденти. Це може включати тестування процедур попередження, реагування та відновлення після кібератаки.

4. Вправи з кібербезпеки мереж – проведення вправ з тестування захисту мереж від кібератак. Це може включати тестування на відновлення після DoS атаки, відновлення від розриву мережі або на відстеження трафіку, що виходить з мережі.

5. Вправи на тренування співробітників – проведення вправ на тренування співробітників з кібербезпеки.

Створення культури кібербезпеки є важливим елементом забезпечення безпеки в організації. Основною метою створення культури кібербезпеки є забезпечення того, щоб кожен працівник розумів, що кібербезпека є його особистою відповідальністю та розумів, як він може допомогти у забезпеченні безпеки всієї організації. Ці заходи можуть бути використані окремо або в комбінації.

Способи виявлення та протидії кіберзагрозам на прикладі DDoS атаки.

DDoS атаки (атаки з використанням великої кількості запитів) є одними з найпоширеніших видів кібератак на сьогоднішній день. Існує безліч методів захисту від DDoS атак, ось декілька з них:

- Використання CDN (Content Delivery Network): CDN дозволяє розподіляти навантаження між різними серверами, що дозволяє зменшити вплив DDoS атак на окремий сервер.
- Використання фільтрації трафіку: Фільтрація трафіку дозволяє виділяти запити, які можуть бути пов’язані з DDoS атакою та блокувати їх.
- Використання облачних технологій: Використання хмарних технологій може допомогти забезпечити захист від DDoS атак, оскільки вони можуть забезпечити широкі канали зв’язку та високу міру масштабованості.
- Використання захисних мереж: Використання захисних мереж може допомогти забезпечити захист від DDoS атак, оскільки вони можуть блокувати небезпечний трафік та забезпечити захист від небезпечних запитів.
- Використання програмного забезпечення для захисту від DDoS атак: Існує безліч програмного забезпечення, яке може забезпечити захист від DDoS атак. Це може бути програмне забезпечення, яке забезпечує фільтрацію трафіку, блокування атак, розподіл навантаження та інше.
- Підвищення міцності інфраструктури: Підвищення міцності інфраструктури, наприклад, збільшення пропускної здатності мережі та серверів, може допомогти зменшити вплив DDoS атак.

Прикади систем ідентифікації кіберзагроз. На сьогоднішній день на ринку існує багато різних систем детекції інтранет-атак. Ось декілька прикладів:

1. Snort – це безкоштовна система детекції вторгнень (IDS) та інтранет-атак, яка працює в режимі реального часу і використовує базу даних правил для виявлення потенційно небезпечної активності в мережі.

2. Suricata – це інша відкрита система IDS та інтранет-атак, яка працює в режимі реального часу та використовує машинне навчання та інші технології для виявлення потенційно небезпечної активності в мережі.

3. Darktrace – це комерційна система детекції інтранет-атак, яка використовує технології штучного інтелекту та машинного навчання для автоматичного виявлення та реагування на кібератаки всередині корпоративної мережі.

4. Cisco Stealthwatch – це інша комерційна система детекції інтранет-атак, яка використовує машинне навчання та інші технології для виявлення потенційно небезпечної активності в мережі та забезпечення захисту мережі в реальному часі.

5. McAfee Network Security Platform – це ще одна комерційна система IDS та інтранет-атак, яка використовує різноманітні методи аналізу трафіку та машинного навчання для виявлення та блокування потенційно небезпечної активності в мережі.

6. Zeek (раніше відома як Bro) – це безкоштовна система мережевого моніторингу та виявлення вторгнень, яка використовує відкритий код та різноманітні методи аналізу трафіку для виявлення потенційно небезпечної активності в мережі.

Ці системи детекції інтранет-атак можуть бути встановлені та налаштовані на різних рівнях складності, залежно від потреб та бюджету компанії. Вони допомагають виявляти та реагувати на кібератаки всередині мережі.

Висновки. У статті було проведено дослідження шляхів ідентифікації порушника в інформаційно-комунікаційних системах та мережах. Було проаналізовано різноманітні методи та алгоритми ідентифікації. В результаті дослідження було встановлено, що ефективність методів ідентифікації порушника значно залежить від характеру нападу та використаної вразливості. Було визначено, що найбільш ефективним є комплексний підхід, який включає в себе використання різних методів ідентифікації.

Отже, на основі проведеного дослідження можна зробити висновок про необхідність постійного підвищення рівня безпеки інформаційно-комунікаційних систем та мереж. Для цього потрібно використовувати комплексний підхід до ідентифікації порушника та постійно вдосконалювати методи та алгоритми ідентифікації, щоб бути готовими до різноманітних типів нападу.

Список використаних джерел

1. Жилін А. В., Шаповал О.М., Успенський О.А. Технології захисту в інформаційно-комунікаційних системах. Режим доступу: https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf
2. Гладка І.М, Наконечна О.М. Аналіз ризиків безпеки інформаційної системи іт-підприємства Режим доступу: https://doi.org/10.32838/2663-5941/2020.5/12
3. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids.
4. Критерії захищеності інформації в комп'ютерних системах від несанаційного доступу. НД ТЗИ 2.5004-99. Режим доступу: https://tzi.com.ua/downloads/2.5-004-99.pdf

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

СОЦІАЛЬНИЙ ІНЖИНІРИНГ: СУТНІСТЬ І МЕТОДИ ПРОТИДІЇ

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

У статті розкрито сутність і методи протидії соціальному інжинірингу. Визначено генезис походження соціального інжинірингу. Сформовано взаємозв'язок між розповсюдженням вірусу COVID-19, війни Росії проти України і постійної необхідності адаптації людей до зовнішніх факторів з соціальним інжинірингом. Відокремлено низку заходів з детальним описом концепції. Зазначається, що комплексне використання методів протидії допоможе знизити рівень успішних атак за всіма методами.

The article reveals the essence and methods of combating social engineering. The genesis of the origin of social engineering is determined. The relationship between the spread of the COVID-19 virus, Russia's war against Ukraine and the constant need to adapt people to external factors with social engineering has been established. A number of measures are separated with a detailed description of the concept. It is noted that the integrated use of countermeasures will help reduce the level of successful attacks by all methods.

Актуальність. Глобальне поширення вірусу COVID-19, війна Росії проти України і постійна необхідність адаптації людей до зовнішніх факторів призвели до прискореного впровадження технологій та цифровізації, тому більшість інформації зараз зберігається у цифровому форматі. Даний факт підкреслив важливість навчання людей розпізнавати потенційні кіберзагрози та важливість навчання правильному використанню технологій з урахуванням основних критеріїв інформації: цілісність, конфіденційність та доступність. Відсутність такого навчання викликає недовіру до ролі людського фактору в інформаційній безпеці. Більше того, часто забувають про зв'язок людського фактору із інформаційною безпекою, що пов'язано з наголосом на технічних і процедурних заходах, необхідних для вирішення загальних проблем безпеки. У результаті більшість кіберзагроз виявляються за допомогою систем виявлення вторгнень, брандмауерів або антивірусного програмного забезпечення, тому соціальна інженерія є основною загрозою, оскільки з нею неможливо боротися цими звичайними засобами.

Звернення до безпеки з соціальної, технічної та когнітивної точок зору потрібне для ефективної обробки людських факторів, залучених до інформаційної безпеки. Поєднуючи людські характеристики з технологічними характеристиками, можна створити організаційну культуру, щоб мінімізувати ризики, пов'язані з атаками соціальної інженерії. Незалежно від рівня впливу, культура інформаційної безпеки є ключовим фактором уникнення потенційних небезпек, яким може бути піддана інформація. Завдяки реалізації навчання користувачі отримують необхідні знання, які сприяють гарному розумінню стратегій атак соціальної інженерії та розвитку здатності протидіяти й обмежувати потенційні наміри завдати шкоди [1]. Як наслідок, щоб досягти етапу, коли підтримка інформаційної безпеки стає діяльністю, яка виконується несвідомо та на постійній основі, необхідно впровадити організаційну культуру, встановлену через згоду та підтримку користувачів.

Мета статті. Розкрити сутність і методи протидії соціальному інжинірингу.

Об'єктом дослідження є процес протидії соціальному інжинірингу.

Предмет дослідження – соціальний інжиніринг.

Аналіз попередніх досліджень. Формулювання наукової думки в окресі соціального інжирингу є різнорідною та масштабною. У сучасній науковій площині з'являються роботи присвячені механізмам та принципам протидії соціальному інжинірингу на об'єктах господарювання.

О. Юдін, О. Матвійчук-Юдіна та О. Супрун [2] провели аналіз існуючих сучасних методів соціальної інженерії та визначено технології використання різних класів методів в інформаційно-психологічній війні, а також застосування деструктивних засобів інформаційної безпеки, як складової психологічного впливу на особистість і суспільство.

У [3] схарактеризовано основні підходи до тлумачення понять «прикладні комунікаційні технології», «соціальний інжиніринг». Авторка вдається до порівняльного вивчення методологічних систем аналізу соціальних комунікацій і комунікаційних технологій у світовій та вітчизняній науці.

Н. Баландіна, М. Василенко, В. Слатвінська та С. Сисоєнко [4] довели потребу в новому методологічному підході до побудови моделі поведінки людини в цифровій сфері, спрямованої на захист інформації в соціальному інжинірингу. Запропоновали синергійно-криптографічний підхід до побудови моделі поведінкових проявів в умовах соціального інжинірингу та в інтересах захисту інформації.

Подібні дослідження також проведено іноземними авторами, зокрема Х. Мумтаз, С. Самріна, І. Номан [5], Ф. Гассан [6], А. Очоа, А. Акеро [7], С. Врговец, І. Бернік, Б. Маркель [8], Г. Асанте [9], Ф. Рубія, Ю. Аффан, Л. Лін, В. Цзяньмін [10], Ф. Лову, Х. Нандере [11], К. Янгкен [12], К. Четіуі, Б. Бах, А. Аламі, А. Банассе [13], К. Штайнметц, Т. Холт [14]. та інші.

Однак, незважаючи на масштабність наукових досліджень за окресленою тематикою, питання розкриття сутності і методів протидії соціальному інжинірингу залишається відкритим та потребує детального опрацювання.

Виклад основного матеріалу. Примус, психологічна маніпуляція та методи індоктринації – це лише невелика частина способів, за допомогою яких уявлення, думки та переконання однієї людини порушуються або навіть замінюються уявленнями, думками та переконаннями іншої людини. Соціальний інжиніринг також відноситься до цієї категорії. Визначення терміну «соціальний інжиніринг» представляє певну складність, оскільки визначення, пов’язані з соціальним інжинірингом, відрізняються залежно від середовища, яке використовується для їх отримання. Найперша згадка про соціальний інжиніринг датується 1894 роком, у період індустріалізму, коли у своїх працях голландський радикал Дж. С. Ван Маркен наголосив на необхідності розвитку технічної експертизи в «управлінні людськими проблемами». Як визначено в онлайн-словнику Dictionary.com, соціальний інжиніринг пояснюється як «використання централізованого планування в спробі керувати соціальними змінами та регулювати майбутній розвиток і поведінку суспільства» [15]. Це визначення обмежує мету соціального інжинірингу використанням людського фактору шляхом використання комунікації та засобів, за допомогою яких він досягається. У контексті застосовності до інформаційної безпеки соціальний інжиніринг відноситься до дії обману особи з метою розкриття конфіденційної інформації, отримання несанкціонованого доступу або вчинення шахрайства шляхом спілкування з цією особою з метою завоювання її довіри [5]. Сукупність таких заходів з метою збору інформації, підробки або несанкціонованого доступу, від традиційного «шахрайства» відрізняється тим, що часто є одним із багатьох кроків у складнішій схемі доступу до інформації.

Існування кількох визначень, пов’язаних із соціальним інжинірингом, підкреслює його широку застосовність у багатьох сферах. Використовується в політичному, освітньому, релігійному чи корпоративному середовищі, соціальний інжиніринг використовується для перепланування поведінки мас. Юристи та психологи вдаються до тактики, яку використовує соціальний інжиніринг, щоб зібрати інформацію, яка інакше не була б розголошена. Уряд використовує соціальний інжиніринг через свою владу над людьми, які перебувають під його владою, при цьому людський мозок налаштований дотримуватись вказівок влади.

Продавці – це соціальні інженери, які використовують свою здатність переконувати людей звертатися до їхніх потреб і задовольняти їх за допомогою товарів або послуг, які вони комерціалізують. Приклади, звичайно, можна продовжувати, але наведених достатньо,

щоб підкреслити той факт, що соціальний інжиніринг використовується щодня людьми та установами в різних соціальних рівнях.

Незалежно від типології, до якої підпадають ініціатори соціального інжинірингу, ефективність соціального інжинірингу пояснюється використанням людських помилок, таких як: прийняття рішень під впливом емоцій, бажання допомогти, необережність у знайомих ситуаціях та ігнорування інформації, яка сприймається не вірно.

Для того, щоб застосувати соціальний інжиніринг на практиці, обов'язковим є вивчення окремих осіб та їхньої поведінки, щоб сприяти досягненню очікуваного результату, незалежно від причини, з якої використовується соціальний інжиніринг.

Теоретично атаки соціального інжинірингу можуть бути зосереджені на технологіях або на окремих особах [6]. Технологічний підхід до соціального інжинірингу полягає в підробці прикладної системи, щоб змусити користувача надати конфіденційну інформацію за допомогою спливаючих вікон, спаму, шкідливих програм, шпигунського програмного забезпечення або фішингових атак. Користувач може отримати спливаюче вікно, яке вказує на те, що комп'ютерна програма, яка зараз використовується, зіткнулася з певними проблемами, які обмежують її функціональність, доки комп'ютерна програма не зможе повторно увійти, ввівши ідентифікатор і пароль. Ввівши ці дані, хакер, який створив спливаюче вікно, зможе отримати доступ до мережі та комп'ютерної системи за допомогою облікових даних користувача. Спам-повідомлення містять вкладення, у яких троянський вірус або інша шкідлива програма впливає на системи та мережі [7]. У загальному комплексі наслідки дії таких атак варіюються від уповільнення роботи системи до знищення даних і втручання в усю комунікаційну мережу.

Поширюючи законну програму, яка містить зловмисне або шпигунське програмне забезпечення, жертву можна змусити її завантажити, вважаючи, що програма є утилітою, яка покращує продуктивність комп'ютера.

Фішингові атаки – це найпоширеніші атаки, які здійснює соціальний інжиніринг [8], під час яких до жертв звертаються за допомогою електронних листів або телефонних дзвінків. Ці атаки можна класифікувати за п'ятьма категоріями: цільовий фішинг, китобійний фішинг, вішинговий фішинг, інтерактивний фішинг із голосовою відповіддю, фішинг через невідомі корпоративні електронні листи [9]. Для отримання даних зловмисники створюють відчуття терміновості або застосовують тактику залякування. Варто зазначити, що фішингові кампанії можуть бути орієнтовані на велику кількість випадкових користувачів або конкретну особу чи групу.

Усі ці форми фішингу включають фальшиві веб-сайти, веб-сайти PayPal, програмне забезпечення для страхування, рекламу, антивірус, безкоштовні пропозиції чи призи, за допомогою яких зловмисник може дізнатися ім'я жертви, фізичну адресу, дані кредитної картки тощо.

Атаки, спрямовані на слабкі сторони поведінки людини або такі, що передбачають отримання конфіденційної інформації без використання технологічних вразливостей, ілюструють другу категорію атак соціального інжинірингу.

Видача себе за іншу особу або викрадення персональних даних особи передбачає встановлення легітимності з жертвою шляхом зв'язування та об'єднання даних, відомих про жертву. Для цього необхідно, щоб соціальний інженер, який ініціює цей тип атаки, заздалегідь мав достовірну історію, яка не викликає підозр у жертви.

Занурення спрямоване на отримання інформаційних товарів або документів. Наприклад, якщо зловмисник отримує список з іменами співробітників або список телефонних номерів, він стає бенефіціаром багатьох можливостей соціального інжинірингу: імена та номери телефонів співробітників можуть бути використані для крадіжки особистих даних або для ініціювання фішингової атаки.

Обман, на відміну від шахрайства з метою отримання фінансової чи матеріальної вигоди, часто використовується, щоб збентежити жертву або прийняти швидкі рішення.

Шпигунство та підслуховування зображують типи атак соціального інжинірингу, які здійснюються зловмисником, коли він знаходиться поблизу жертви. Ці атаки можуть призвести до отримання пароля користувача, коли він записаний на документах, доступних іншим.

Отже, незважаючи на численні форми, атака соціального інжинірингу передбачає використання соціальних навичок для отримання достатньої кількості даних для компрометації або зміни інформаційних систем організації [10].

У будь-якій успішній атаці, здійсненій у рамках соціального інжинірингу, дотримується низка етапів: збір інформації, вилучення, претекст, переконання, націлювання та розпізнавання.

Збір інформації – найретельніший етап соціального інжинірингу, який здійснюється шляхом спостереження за жертвою. Тривалість цієї стадії може варіюватися від кількох годин до кількох років, оскільки інформація не збирається відразу, а потім співвідноситься одна з одною для створення профілю жертви.

Виявлення можна визначити як здатність отримувати інформацію за допомогою логіки, тому її може бути важко виявити. По суті, проведення цієї стадії досягається проведенням дізнання. Перетекст ілюструє стадію атаки, коли соціальний інженер може прийняти фальшиву особу, яка може вплинути на прийняття жертвою певних рішень. Роль соціального інженера полягає в тому, щоб визначити спосіб мислення жертви, щоб ефективно використовувати її навички. Це здійснюється за допомогою розумових хитрощів, і, залежно від умонастрою співрозмовника, соціальний інженер вдасться до емоційної маніпуляції, зверне особливу увагу на слова, які можуть бути використані в розмові.

Коли звернення до інтересів жертви є успішним, соціальний інженер використовує переконання, щоб заставити жертву діяти від його імені, встановлюючи визначені цілі, завойовуючи довіру жертви, через взаємність або гнучкість.

Етап націлювання показує, що, на відміну від інших атак на людей, атаки соціальної інженерії сформульовані для конкретної людини.

Останній етап, розпізнавання, є формою збору інформації, за допомогою якої соціальний інженер отримує достатньо даних для планування та здійснення атаки на намічену ціль.

Стосовно України, як приклад реалізації соціального інжинірингу варто наголосити на пандемії 2019 року та війні 2022 року.

Пандемія, яка послідувала за глобальним поширенням вірусу COVID-19, а згодом і форм SARS-CoV-2, підвищила обізнаність про те, що фейкові новини можуть загрожувати загальному здоров'ю членів суспільства. Пандемія, яка розвивалася двома хвилями, перша з середини березня 2020 року, а друга – з січня 2021 року, породила нове поширене політичне, соціальне та економічне явище: інфодемію. Це явище було запроваджено Всесвітньою організацією охорони здоров'я, яка використала термін «інфодемія», щоб описати поширення дезінформації та неправдивої чи доброзичливої інформації серед великих спільнот людей одним словом. Соціальні інженери скористалися контекстом пандемії, щоб отримати допомогу від Центрів контролю та профілактики захворювань, продавати підроблені продукти (наприклад, набори тестів), звинувачувати расові групи, уряди та іммігрантів у поширенні вірусу та поширювати хаос і соціальні розбіжності, які призвели до рухів проти масок, проти вакцинації та навіть проти 5G.

Останнім і далекосяжним політично вмотивованим нападом соціальної інженерії є російсько-українська війна, яка почалася ще в лютому 2022 року. Вторгнення президента Росії Володимира Путіна в Україну також призвело до найнижчого рівня відносин між Москвою та Заходом з часів холодної війни. Російські військові та розвідувальні органи націлили на Україну через дезінформацію, намагаючись зобразити Україну та українських урядовців агресором у цьому конфлікті. Твердження російського президента мають на меті

підживити ілюзію, що Україна розпалює насильство, тому російські військові дії на українській території є необхідними, для уникнення глобального конфлікту. За словами Джо Ондрака, керівника відділу розслідувань лондонської фірми Logically, яка займається відстеженням дезінформації, російська риторика підтримується безліччю цифрових активістів, які потроюють фейкові новини про Україну.

Протидія методам соціального інжинірингу – це комплекс організаційно-режимних заходів, що включає:

– проведення перевірочних заходів при прийомі працівників на роботу, що включають всебічне вивчення особистісних якостей кандидата, його оточення, сфери інтересів та інформації про минулу трудову діяльність;

– контроль вхідної кореспонденції, що надходить в електронному вигляді до поштових скриньок співробітників, незалежно від рівня повноважень та привілейованості;

– перевірки наявності службової інформації конфіденційного характеру у відкритих інформаційних мережах;

– регулярне проведення занять із співробітниками організації щодо правил роботи з інформацією конфіденційного характеру та навчання навичкам протидії методам соціальної інженерії;

– контроль за дотриманням технології обробки інформації на технічних засобах організації;

– запис та подальший аналіз телефонних переговорів співробітників з використанням службових засобів зв'язку;

– проведення виховної роботи з метою підвищення мотивації працівників, прищеплення відданості дорученій справі;

– проведення періодичних перевірок професійної придатності співробітників організації щодо забезпечення інформаційної безпеки.

До основних методів протидії соціальному інжинірингу варто віднести:

1. Формування правильних переконань (передумов)
2. Використання дедукції (не індукції)
3. Перевірка достовірності
4. Знання логічних помилок

Формування правильних базових переконань (передумов) необхідне для формування адекватної картини світу тобто стійке переконання що Земля кругла, організація про мене подбає, моя безпека – моя відповідальність, тощо.

Дедукція (не індукція), тобто електронна пошта безпечна, зі мною такого не станеться, тощо.

Перевірка достовірності, тобто незалежне/достовірне джерело, експеримент.

Логічні помилки: «після» не означає «внаслідок», думка авторитету чи думка більшості, хибна аналогія, аргументація до традиції («у нас так заведено»).

Висновки. У роботі розкрито сутність і методи протидії соціальному інжинірингу. Враховуючи сучасний рівень геополітичної напруженості та посилення кібер-злочинів у всіх галузях господарювання, застосування соціального інжинірингу оперативно підлаштовується під поточну ситуацію і набуває ефективності особливо щодо тих користувачів, які непоінформовані про ризики та загрози цифрового середовища. Сучасний соціальний інжиніринг дає можливість коригувати соціальну реальність, використовуючи методи прогнозування, планування та програмування. Досліджено різні методи соціальної інженерії, розглянуто приклади, проведено розбір методів захисту та виведено пропозиції, комплексне використання яких допоможе знизити рівень успішних атак за всіма методами.

Перспективами подальшого дослідження є формулювання технологій протидії соціальному інжинірингу на об'єктах господарювання.

Список використаних джерел

1. Мочурад Л. І., Бойко Н. І., Яцків М. В. Моделювання стресової ситуації людини в автоматизованих системах управління технологічними процесами, Науковий вісник НЛТУ України, 2020. т. 30. № 1. С. 152-157. http://doi:10.36930/40300126
2. Інформаційно-психологічна війна та технологіх соціального інжинірингу [Електронний ресурс] / О. К. Юдін, О. В. Матвійчук-Юдіна, О. М. Супрун // Наукоємні технології. 2021. № 2. С. 130-139. – Режим доступу: http://nbuv.gov.ua/UJRN/Nt_2021_2_5
3. Бондаренко І. Прикладні комунікаційні технології у фокусі методології соціального інжинірингу. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Соціальні комунікації. 2020. Том 31 (70). № 3. Частина 3. С. 199-205.
4. Баландіна Н. М., Василенко М. Д., Слатвінська В. М., Сисоєнко С. В. Підхід до моделювання поведінкових проявів у соціальному інжинірингу в інтересах захисту інформації. Вісник Черкаського державного технологічного університету. Серія технічні науки. Вип. 4. 2020. С. 57-66. http://doi:10.24025/2306 4412.4.2020.222064 URL: http://vtn.chdtu.edu.ua/article/view/222064/225697
5. Mumtaz H., Samrina S., Noman I. (2023). Social Engineering and Data Privacy. http://doi:10.4018/978-1-6684-6581-3.ch010.
6. Hassan F. (2023). SOCIAL ENGINEERING ATTACKS TECHNIQUES. International Journal of Management Science and Engineering Management. № 03. P. 18-20.
7. Ochoa A., Acero A. (2022). The Journey of Engineering into Social Justice and Peacebuilding: A Review of the XV Conference of the International Network of Engineering, Social Justice and Peace. International Journal of Engineering Social Justice and Peace. № 9. P. 5-14. http://doi:10.24908/ijesjp.v9i1.15573.
8. Vrhovec S., Bernik I., Markelj B. (2022). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. Computers & Security. P. 125. http://doi:10.1016/j.cose.2022.103038.
9. Asante G. (2022). Social Engineering Attacks: A Clearer Perspective. International Journal of Computer Applications. № 184. P. 53-62. http://doi:10.5120/ijca2022922057.
10. Rubia F., Affan Y., Lin L., Jianmin W. (2022). Strategies for counteracting social engineering attacks. Computer Fraud & Security. 2022. http://doi:10.12968/S1361-3723(22)70583-0.
11. Lowu F., Nandere H. (2022). Simulation Model of Social Engineering Attacks in Business Enterprises. № 11. P. 2021. http://doi:10.7176/JIEA/11-2-10.
12. Youngkeun C. (2022). Workplace Violence and Social Engineering Among Korean Employees. http://doi:10.4018/978-1-6684-7464-8.ch018.
13. Chetioui K., Bah B., Alami A., Bahnasse A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science. P. 656-661. http://doi:10.1016/ j.procs.2021.12.302.
14. Steinmetz K., Holt T. (2022). Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations. Social Science Computer Review. https://journals. sagepub.com/doi/full/10.1177/08944393221117501.
15. Онлайн-словник. – Режим доступу. – https://www.wiki-data.uk-ua.nina.az/Dictionary. com.html (останнє звернення 24.03.2023р.).

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

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ WEB-САЙТІВ ТА МЕТОДІВ ЇХ УСУНЕННЯ

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

У статті розглянуто різноманітні методи та інструменти для виявлення та усунення вразливостей web-сайтів. Досліджено різні види атак, такі як SQL-ін'єкції, XSS-атаки та CSRF-атаки, а також методи їх запобігання. Описано роботу різних сканерів вразливостей, таких як OWASP ZAP, Burp Suite, Acunetix та Nessus, а також сканера вразливостей на сайти Nikto.

The article examines various methods and tools for detecting and eliminating vulnerabilities in websites. Different types of attacks such as SQL injections, XSS attacks, and CSRF attacks, as well as methods for preventing them, are investigated. The article describes the operation of various vulnerability scanners such as OWASP ZAP, Burp Suite, Acunetix, and Nessus, as well as the Nikto vulnerability scanner for websites.

Актуальність. Дослідження вразливостей web-сайтів та методів їх усунення є дуже актуальними у наш час, оскільки з кожним роком кількість web-сайтів та їх важливість для бізнесу та суспільства зростає. Із збільшенням кількості web-сайтів зростає і загроза їх вразливостей. Згідно статистики, більше 60% усіх атак в Інтернеті відбуваються через вразливості web-сайтів. Нападники використовують ці вразливості для викрадення даних користувачів, встановлення шкідливих програм або впровадження зловмисного коду на серверах web-сайтів. В разі вразливості web-сайту зловмисник може здійснювати різноманітні атаки, такі як викрадення конфіденційної інформації, редагування даних, введення шкідливого коду, відправку спаму та багато іншого. Це може призвести до серйозних наслідків для бізнесу, які можуть зазнавати фінансових втрат або втрати довіри клієнтів. Дослідження вразливостей web-сайтів та розробка методів їх усунення є важливою для забезпечення безпеки в Інтернеті. На жаль, більшість web-сайтів не забезпечують достатньої безпеки та мають вразливості, які можуть бути використані для атак.

Тому, дослідження вразливостей web-сайтів та розробка методів їх усунення має велике значення для забезпечення безпеки в Інтернеті, а також для захисту конфіденційності та безпеки користувачів web-сайтів. Тема є надзвичайно актуальною, і вона постійно вдосконалюється та розширюється відповідно до нових викликів та загроз у сфері кібербезпеки.

Метою статті є дослідження проблеми вразливостей web-сайтів та підвищення рівня свідомості про важливість захисту web-додатків від зловмисних атак та надання практичних порад щодо захисту web-сайтів від вразливостей.

Об'єктом дослідження є процес виявлення та усунення вразливостей в web-сайтах, які можуть призвести до некоректної роботи сайту, втрати конфіденційної інформації, порушення безпеки відвідувачів сайту та можливого внесення шкідливого коду.

Предмет дослідження – web-сайти та їхні вразливості, які можуть бути використані зловмисниками для здійснення різних видів кібератак, таких як SQL-ін'єкції, XSS-атаки, CSRF-атаки.

Аналіз попередніх досліджень. Дослідження вразливостей web-сайтів та методів їх усунення є актуальною темою для багатьох дослідників з усього світу. Серед українських вчених, які займалися цією темою, можна відзначити таких: В. Ю. Степанович, професор кафедри програмної інженерії та інформаційних технологій Національного авіаційного університету, який досліджує питання безпеки програмного забезпечення, включаючи вразливості web-сайтів та методи їх виявлення та усунення; К. М. Гуцало, кандидат

технічних наук, доцент кафедри інформаційних технологій та захисту інформації Львівської політехніки, який займається питанням захисту інформації, включаючи вразливості web-сайтів та методи їх усунення. Серед зарубіжних вчених, які займалися цією темою, можна відзначити таких: Джейсон Халперн (Jason Halpern), доцент кафедри інформаційної безпеки та зв'язку Нью-Йоркського технологічного інституту, який досліджує питання кібербезпеки, включаючи вразливості web-сайтів та методи їх виявлення та усунення; Хуан Хосе Перес (Juan Jose Perez), професор кафедри програмування та технологій інформаційної безпеки університету Ла-Ріоха (Іспанія), займається питанням інформаційної безпеки, включаючи вразливості web-сайтів та методи їх виявлення та усунення.

Виклад основного матеріалу. Дослідження вразливостей web-сайтів та методів їх усунення є дуже важливим процесом для забезпечення безпеки та захисту web-додатків. Це дозволяє виявляти потенційні загрози безпеці та вчасно приймати заходи для їх усунення. Існує безліч різних методів тестування web-додатків на наявність вразливостей, таких як сканування вразливостей, ручний аналіз, тестування від зловмисників та інші. Після виявлення вразливостей web-сайту необхідно прийняти заходи для їх усунення. Цей процес може включати в себе розробку патчів для web-додатків, встановлення спеціальних правил безпеки, зміну налаштувань сервера та баз даних, встановлення додаткових механізмів захисту тощо. Статистичне дослідження найбільш поширених уразливостей web-ресурсів проводять для того, щоб з'ясувати, які вразливості найчастіше зустрічаються та які заходи повинні бути прийняті для їх усунення [1].

За даними звіту OWASP, найбільш поширеними уразливостями web-додатків є: Injection − включає SQL Injection та вразливості, пов'язані з введенням даних, такі як LDAP та XML; Broken Authentication and Session Management − включає вразливості, пов'язані з недостатньою аутентифікацією та керуванням сесіями користувачів; Cross-Site Scripting (XSS) − включає вразливості, пов'язані з введенням скриптів на web-сторінки, що можуть бути виконані у web-браузері користувача; Broken Access Control − включає вразливості, пов'язані з недостатньою перевіркою доступу до ресурсів web-додатка; Security Misconfiguration − включає вразливості, пов'язані з неправильним налаштуванням безпеки web-додатка; Insecure Cryptographic Storage − включає вразливості, пов'язані з недостатньою захистом криптографічних ключів та інших конфіденційних даних; Insufficient Logging and Monitoring − включає вразливості, пов'язані з недостатнім збором та аналізом логів, які можуть бути використані для виявлення та вирішення проблем з безпекою; Insecure Communications − включає вразливості, пов'язані з використанням небезпечних протоколів зв'язку, таких як HTTP замість HTTPS; Improper Error Handling − включає вразливості, пов'язані з недостатньою обробкою помилок, які можуть призвести до розкриття конфіденційної інформації [2, 3].Додатково, для забезпечення безпеки web-додатків можна використовувати різноманітні техніки, такі як шифрування даних, контроль доступу до ресурсів, перевірку введення даних, моніторинг діяльності користувачів тощо. Дослідження вразливостей web-сайтів та методів їх усунення є важливою складовою процесу захисту web -додатків від атак та зловмисного використання. Цей процес складається з кількох етапів, таких як ідентифікація вразливостей, аналіз ризиків, виправлення вразливостей та перевірка ефективності виправлень.

Ідентифікація вразливостей зазвичай здійснюється за допомогою сканерів вразливостей для автоматичного виявлення потенційних проблем web-додатків. Сканери вразливостей можуть виявляти багато різних типів вразливостей, таких як SQL-ін'єкції, крос-сайт скриптінг (XSS), вразливості налагодження та багато інших. Однак, не завжди сканери вразливостей здатні виявити всі можливі вразливості web-сайту. Для виявлення більш складних вразливостей може знадобитися ручний аналіз коду web-сайту. Ручний аналіз дозволяє більш детально проаналізувати код web-сайту та виявити потенційні проблеми, які не можуть бути виявлені сканерами вразливостей. Після сканування web-сайту, сканер визначає потенційні вразливості та надає звіт про результати сканування. На цьому етапі можуть виявлятися різні типи вразливостей, такі як SQL ін'єкції, крос-сайт

скриптінг (XSS), аутентифікаційні та авторизаційні проблеми, ініціювання зловмисного коду та багато іншого. Після ідентифікації вразливостей важливо провести аналіз ризиків, щоб з'ясувати потенційний вплив вразливостей на безпеку web-додатку та його користувачів. Це може включати визначення потенційних наслідків використання вразливостей, оцінку ризику втрати даних або можливості витоку конфіденційної інформації. Після аналізу ризиків, наступним етапом є виправлення вразливостей. Цей процес може бути складним та включати в себе виправлення коду, встановлення нових захисних заходів та перевірку налаштувань сервера. Важливо, щоб виправлення були внесені швидко та ефективно, щоб зменшити час, протягом якого вразливість може бути використана [2].

Дослідження вразливостей web-сайтів тестуванням на проникнення (Penetration Testing або Pentesting) полягає у спробі використання потенційних вразливостей зловмисником для злому web-сайту або отримання несанкціонованого доступу до конфіденційної інформації. При проведенні тестування на проникнення використовуються різні інструменти, включаючи сканери вразливостей, експлоіти та інші програмні засоби [1, 2].

Іншим методом дослідження вразливостей є аудит безпеки web-сайту. Цей метод полягає у вивченні web-сайту та його коду з метою виявлення потенційних проблем безпеки. Аудит безпеки може бути проведений як вручну, так і за допомогою автоматичних інструментів. У разі виявлення вразливостей web-сайту, необхідно прийняти кроки для їх усунення. Це може включати в себе патчінг вразливостей, встановлення обмежень на ввід даних користувачів, налаштування прав доступу до файлів та багато іншого. Для кращої ефективності необхідно регулярно тестувати web-додатки на вразливості та виконувати вимоги безпеки, щоб захистити web-додатки від потенційних загроз.

Web-сервер − це програмне забезпечення, яке надає доступ до web-сторінок через Інтернет. Він обробляє запити від браузерів і надсилає відповіді у вигляді web-сторінок, зображень, відео та іншого контенту.

Однією з найбільш поширених вразливостей web-серверів є кросс-сайтовий скриптінг (XSS). Ця атака полягає в тому, що зловмисник вставляє в шкідливому вигляді скрипти на web-сторінку, яку відвідує жертва [2]. Коли браузер жертви завантажує web-сторінку, він виконує шкідливий скрипт із вмісту сторінки, що може призвести до злочинних дій. Ще однією вразливістю є атака SQL Injection, коли зловмисник вводить SQL-запит в поле для вводу на web-сторінці. Якщо web-сервер не перевіряє вхідні дані на валідність, це може призвести до витоку конфіденційної інформації або навіть до повного контролю над web-сайтом. Окрім того, web-сервер може стати жертвою DDoS-атаки, коли зловмисники намагаються перевантажити сервер великою кількістю запитів одночасно. Це може призвести до відмови в обслуговуванні і виключення сервера з мережі. Вразливості web-серверів та атаки на них можна класифікувати за декількома критеріями. Основні з них: за типом вразливості (кросс-сайтовий скриптінг (XSS): внедріння SQL-запитів (SQL injection); незапобіжність у разі введення великої кількості даних або завантажень (Denial of Service атаки); вразливості, пов'язані з конфігурацією web-сервера або його додатків; вразливості web-сервера, які дозволяють отримати додаткові права доступу до системи; за зонами вразливості: web-додатки, які взаємодіють з сервером; операційна система; мережевий протокол, який використовується для зв'язку між клієнтом і сервером; за характером атаки: атаки на аутентифікацію і авторизацію; атаки на мережу; атаки на програмне забезпечення; атаки на апаратне забезпечення; атаки на процеси й операційну систему [3].

Щоб зменшити ризик вразливостей web-серверів, слід використовувати оновлене програмне забезпечення і виконувати регулярні перевірки на наявність вразливостей. Також слід забезпечити доступ до web-сервера за допомогою безпечних протоколів, таких як HTTPS, і використовувати сильні паролі для адміністративних облікових записів.

Незважаючи на те, що це не повний перелік критеріїв класифікації вразливостей та атак на web-сервери, такий підхід допомагає розробникам та адміністраторам зрозуміти характер вразливостей та захистити системи від атак. Для запобігання атакам, рекомендується використовувати сучасні методи захисту, такі як WAF (Web Application Firewall),

IDS (Intrusion Detection System), IPS (Intrusion Prevention System), а також виконувати регулярні перевірки на наявність вразливостей та оновлення програмного забезпечення [2, 4].

Статистика вразливостей web-додатків є складною та змінюється з часом. Проте, деякі статистичні дослідження та звіти можуть надати загальну картину.

За даними OWASP Top 10 − це список найбільш поширених вразливостей web-додатків, який публікується організацією OWASP (Open Web Application Security Project) кожні 3 роки [2]. Останнє оновлення було зроблено в 2022 році. Згідно статистичних даних з останнього звіту маємо: 63% web-додатків мають проблеми з аутентифікацією та авторизацією; 50% web-додатків мають проблеми з введенням даних, включаючи SQL-ін'єкції та XSS; 27% web-додатків мають проблеми зі захистом конфіденційності даних, включаючи витік інформації та недостатній захист від атак типу CSRF (Cross-Site Request Forgery); 23% web-додатків мають проблеми з захистом від вразливостей, пов'язаних з бізнес-логікою додатку; 20% web-додатків мають проблеми з захистом від вразливостей, пов'язаних з мережевою інфраструктурою.

Таким чином, статистика вказує на те, що вразливості web-додатків є серйозною проблемою та потребують уваги при розробці та захисті web-додатків.

Ієрархія захисту web-серверів полягає в застосуванні різних рівнів захисту на різних рівнях інфраструктури web-сервера. Це дозволяє забезпечити більш ефективний захист від атак і зменшити ризик компрометації системи в цілому. Основні рівні ієрархії захисту web-серверів такі [1, 3, 6]:

1. Фізичний рівень захисту − розглядаються фізичні аспекти захисту web-серверів. Це можуть бути заходи забезпечення фізичної безпеки, наприклад, захист приміщення, в якому знаходиться сервер, від несанкціонованого доступу або надмірної вологості та температурних умов.

2. Мережевий рівень захисту – включає заходи забезпечення безпеки мережі, на якій працює web-сервер. Цей рівень передбачає захист сервера від мережевих атак, таких як DDoS, сканування портів, атаки на протоколи мережі та інші. На цьому рівні можуть використовуватись різні технології, такі як фільтрація трафіку, віртуальні приватні мережі (VPN), мережеві маршрутизатори, мережеві екрани (firewalls) та інші.

3. Захист програмного забезпечення − розглядаються заходи забезпечення безпеки операційної системи, на якій працює web-сервер, а також програмного забезпечення, яке використовується на web-сервері. До таких заходів можна віднести налаштування прав доступу, оновлення програмного забезпечення та встановлення антивірусного програмного забезпечення.

4. Рівень захисту від вразливостей web-додатків − це захист web-додатків, які працюють на web-сервері. Включає в себе регулярне оновлення програмного забезпечення, захист від вразливостей, пов'язаних з додатками, тестування вразливостей та контроль доступу до додатків. Це також захист web-додатків від різних видів атак, таких як SQL-ін'єкції, XSS-атаки, атаки на сесії та багато інших

5. Захист даних − забезпечує захист даних, які зберігаються на web-сервері. Включає в себе використання захисту баз даних, резервного копіювання даних, контроль доступу до даних та захист даних від втрати або крадіжки.

6. Рівень захисту операційної системи – забезпечує захист від атак, які спрямовані на операційну систему, такі як переповнення буферу, отримання некоректних даних, недопустимі параметри та інші.

7. Рівень додаткових заходів – це рівень додаткових заходів захисту, таких як захист від злому паролів, забезпечення безпеки резервного копіювання, забезпечення конфіденційності даних, захист від злому прав доступу тощо.

8. Захист мережі – налаштування мережевої інфраструктури та встановлення системи мережевої безпеки, яка забезпечує безпеку мережевого зв'язку, включаючи мережеві пристрої, такі як маршрутизатори, комутатори та файрволи.

Захист сайтів та web-проектів – це важлива задача, яка потребує системного підходу та використання різних заходів безпеки. Ось кілька порад, які можуть допомогти захистити web-проект [3, 6]:

- Використання надійного програмного забезпечення та оновлення його, встановлювати всі оновлення для операційної системи та програмного забезпечення, включаючи web-сервер, базу даних, CMS (Content Management System) тощо.
- Захист від Cross-Site Request Forgery (CSRF) – це атака, при якій зловмисник використовує web-сторінку, щоб виконати небажані дії в ім'я користувача. Для захисту від CSRF потрібно використовувати механізми токенів та перевіряти джерело запиту.
- Захист від атак на сесії – наприклад, зловмисник може вкрасти ідентифікатор сесії та використовувати його для отримання несанкціонованого доступу до web-додатку. Для захисту від таких атак необхідно використовувати безпечні механізми автентифікації та авторизації.
- Захист від DDOS атак – це атаки, при яких web-сервер отримує велику кількість запитів, що призводить до перевантаження сервера та його відмови у обслуговуванні. Для захисту від DDOS атак можна використовувати спеціальні системи захисту, наприклад, CDN (Content Delivery Network).
- Захист даних користувачів шляхом шифрування та використанням безпечних протоколів зв'язку, таких як SSL / TLS.
- Моніторинг web-проекту на предмет виявлення аномальної активності та кібератак.
- Захист від SQL-ін'єкцій та XSS атак – це дві найбільш поширені вразливості web-додатків. Щоб запобігти цим атакам, потрібно забезпечити належну обробку та валідацію введених даних на стороні сервера.
- Перевірка коду web-додатків на вразливості та недостатки з використанням спеціальних інструментів.

Деякі з поширених вразливостей web-сайтів та методи їх усунення [4, 5]:

1. SQL-ін'єкції – вразливість, при якій зловмисник може виконати SQL-запит на сервері, використовуючи введені користувачем дані. Це може призвести до витоку конфіденційної інформації або зміни даних на сервері. Дуже часто для запобігання SQL-ін'єкціям необхідно використовувати параметризовані запити та перевірку введених даних на стороні сервера.

Щоб виявити та запобігти SQL-ін'єкціям, можна використовувати наступні практики: використання параметризованих запитів є найбільш ефективним способом запобігання SQL-ін'єкціям, оскільки вони дозволяють включити користувацькі дані в запит безпечним чином; фільтрування та перевірка даних, які вводяться користувачами на web-сайті, обмеження прав доступу до бази даних, регулярне оновлення програмного забезпечення, використання відповідних інструментів для перевірки вразливостей web-додатків та баз даних.

2. XSS атаки – вразливість, при якій зловмисник може внести код на сторінку сайту, який виконується в браузері користувача. Це може призвести до виконання небажаних дій на сторінці або витоку конфіденційної інформації. Для запобігання XSS атакам необхідно валідувати та екранувати введені дані на стороні сервера та використовувати Content Security Policy (CSP).

Щоб виявити та запобігти XSS атакам, можна використовувати наступні практики: виконання валідації та екранування даних, які вводяться користувачами на web-сайті, потрібно переконатися, що введені дані відповідали очікуваному формату та не містили небезпечних символів; використання Content Security Policy (CSP), що дозволяє вказати, з яких джерел може завантажуватись вміст на web-сторінках; використання безпечних функцій для відображення даних на web-сторінці; використання HTTP заголовків, таких як Content-Security-Policy; регулярне оновлення програмного забезпечення.

3. CSRF-атаки – це атаки, при яких зловмисник використовує web-сторінку, щоб виконати небажані дії в ім'я користувача. Для усунення цієї вразливості необхідно використовувати механізми токенів та перевіряти джерело запиту.

Щоб виявити та запобігти CSRF-атаки, можна використовувати наступні практики: використання токенів CSRF – це випадкові рядки, які генеруються на сервері та передаються на сторону клієнта. Клієнт повинен включити цей токен в кожен запит до сервера, щоб сервер міг перевірити, чи є запит дійсним; використання методів POST та PUT, оскільки ці методи не можуть бути виконані з інших доменів; встановлення куків з атрибутом «HttpOnly», оскільки атрибут забороняє JavaScript доступ до кукі, що робить неможливим отримання токенів CSRF через JavaScript; встановлення заголовків безпеки дозволяють вказати браузерам, які дії можуть бути виконані на сторінці та які ресурси можуть бути завантажені; використання перевірки джерела запиту, оскільки перевірка джерела запиту дозволяє перевірити, чи є запит відповідним до домену, з якого користувач відправив запит; обмеження терміну дії сесій, якщо сесія зберігається на стороні клієнта, вона може бути вкрадена та використана зловмисником для виконання CSRF атак; використання SSL / TLS, оскільки вони забезпечують захищене з'єднання між користувачем та web-сайтом, що допомагає запобігти витоку інформації.

4. Вразливості в роботі з файлами – це вразливості, які дозволяють зловмиснику завантажувати та виконувати небажаний код на сервері. Для усунення цієї вразливості необхідно обмежувати права доступу до файлів та використовувати правильну валідацію файлових даних.

5. Недостатній захист сесій – вразливість, при якій зловмисник може перехопити ідентифікатор сесії та отримати несанкціонований доступ до облікового запису користувача. Для запобігання цьому необхідно використовувати захист сесій, такий як HTTPS та механізми автентифікації та авторизації.

6. Недостатній захист від DDOS атак – вразливість, при якій web-сервер отримує велику кількість запитів, що призводить до перевантаження сервера та його відмови у обслуговуванні. Для запобігання цьому можна використовувати зах

Сканери вразливостей для web-сайтів – це програмні інструменти, які дозволяють автоматично виявляти вразливості web-додатків. Вони працюють шляхом сканування web-сайту та його компонентів, таких як форми введення, посилання, заголовки, параметри URL тощо з метою виявлення потенційних вразливостей, які можуть бути використані зловмисниками для атак на сайт.

Існує безліч різних сканерів вразливостей для web-сайтів, деякі з яких є безкоштовними, а інші платними. До найвідоміших сканерів вразливостей для web-сайтів належать [6]:

1. OWASP ZAP (Zed Attack Proxy) – це сканер вразливостей web-додатків, який розробляється та підтримується групою волонтерів з усього світу в рамках проекту OWASP (Open Web Application Security Project). Абсолютно безкоштовний сканер вразливостей web-додатків, який може використовуватися як для ручного тестування, так і для автоматизованого сканування web-додатків.

Основні функції OWASP ZAP: активний сканер: сканує web-додатки на наявність вразливостей та допомагає знайти уразливі місця в додатках; пасивний сканер: аналізує трафік між користувачем та сервером, знаходячи можливі вразливості; Spider: сканує web-сайти, знаходячи всі доступні сторінки та ресурси; Fuzzer: автоматично тестує web-додатки на наявність вразливостей, використовуючи різні варіанти введення даних; Interception Proxy: дозволяє перехоплювати та змінювати запити та відповіді між браузером та сервером. OWASP ZAP може бути корисним інструментом для розробників web-додатків та тестувальників, що дозволяє покращити безпеку web-додатків та забезпечити захист від потенційних атак зловмисників. Проте, слід зазначити, що сканер вразливостей не є універсальним інструментом, який може знайти всі можливі вразливості в web-додатку. Він може бути використаний як допоміжний інструмент.

2. Burp Suite – це інструмент для сканування вразливостей та тестування безпеки web-додатків, який дозволяє здійснювати ручні та автоматичні тести з урахуванням специфіки web-протоколу HTTP та HTTPS.

Основні функції Burp Suite включають: сканування вразливостей: Burp Suite здійснює автоматичний аналіз web-додатків та виявляє можливі вразливості, такі як SQL-ін'єкції, XSS атаки, CSRF атаки та інші; ручне тестування: Burp Suite надає можливість проводити ручні тестування web-додатків, що дозволяє більш детально досліджувати потенційні вразливості та знайти їх експлойти; перехоплення трафіку: Burp Suite може перехоплювати трафік між клієнтом та сервером, що дозволяє досліджувати та аналізувати запити та відповіді, що відправляються на сервер; зміна трафіку: Burp Suite дозволяє змінювати запити, що відправляються на сервер, що дозволяє тестувати поведінку web-додатка в різних умовах та знайти потенційні вразливості; визначення тестових скриптів: Burp Suite дозволяє визначати тестові скрипти, що можуть бути виконані автоматично, що дозволяє збільшити ефективність процесу тестування безпеки web-додатків. Burp Suite є платним інструментом, але має безкоштовну версію з обмеженим функціоналом.

3. Acunetix – це інструмент для сканування вразливостей та тестування безпеки web-додатків. Він використовує технології сканування з високою швидкістю, що дозволяє виявляти багато різних вразливостей web-додатків.

Основні функції Acunetix включають: сканування вразливостей: Acunetix здійснює автоматичний аналіз web-додатків та виявляє можливі вразливості, такі як SQL-ін'єкції, XSS атаки, CSRF атаки та інші; перевірка безпеки web-сайту: Acunetix дозволяє перевірити безпеку web-сайту в цілому, зокрема, оцінити рівень безпеки та виявити можливі проблеми з безпекою; забезпечення відповідності з нормами безпеки: Acunetix може перевірити web-додаток на відповідність з різними нормами безпеки, такими як OWASP Top 10, PCI DSS та інші; перехоплення трафіку: Acunetix може перехоплювати трафік між клієнтом та сервером, що дозволяє досліджувати та аналізувати запити та відповіді, що відправляються на сервер; звіти та аналіз результатів: Acunetix надає звіти про виявлені вразливості та можливість аналізу результатів сканування, що дозволяє зосередитися на найбільш критичних проблемах з безпекою. Acunetix є комерційним інструментом з різними пакетами та цінами в залежності від обсягу сканування.

4. Nessus – це інструмент для сканування вразливостей та тестування безпеки web-додатків та мережевих систем. Він дозволяє здійснювати автоматичний аналіз web-додатків та мережевих систем на предмет вразливостей, таких як вразливості у програмному забезпеченні, слабкі паролі, некоректні налаштування сервера та інші.

Основні функції Nessus включають: сканування вразливостей: Nessus здійснює автоматичний аналіз мережевих систем та web-додатків та виявляє можливі вразливості; аналіз конфігурації: Nessus дозволяє аналізувати конфігурацію мережевих систем та web-додатків та виявляти некоректні налаштування, які можуть створити вразливості; розподілена архітектура: Nessus може працювати в розподіленому середовищі та сканувати мережеві системи та web-додатки з різних серверів; результати сканування: Nessus надає детальні результати сканування та допомагає розуміти важливість кожної вразливості та надає рекомендації по їх виправленню; інтеграція: Nessus може інтегруватись з іншими інструментами безпеки, такими як SIEM (Security Information and Event Management), що дозволяє краще контролювати та моніторити стан безпеки мережі. Однак Nessus є платним інструментом, але має безкоштовну версію для домашнього використання з обмеженим функціоналом.

5. Nikto – це відкрите програмне забезпечення для сканування web-сайтів на наявність вразливостей та уразливих точок. Nikto дозволяє здійснювати автоматичний аналіз web-сайтів та виявляти можливі вразливості, такі як незахищені каталоги, файлові вразливості, некоректні налаштування сервера та інші.

Основні функції Nikto включають: сканування вразливостей: Nikto дозволяє здійснювати автоматичний аналіз web-сайтів та виявляти можливі вразливості; аналіз конфігурації: Nikto дозволяє аналізувати конфігурацію web-сайтів та виявляти некоректні налаштування, які можуть створити вразливості; результати сканування: Nikto надає детальні результати сканування та допомагає розуміти важливість кожної вразливості та надає

рекомендації по їх виправленню; модульність: Nikto має модульну структуру та дозволяє користувачам додавати свої власні модулі сканування; крос-платформовість: Nikto може працювати на різних операційних системах, включаючи Windows, Linux та MacOS; налаштування: Nikto має багато налаштувань, які дозволяють користувачам налаштувати сканування відповідно до їх потреб. Nikto є безкоштовним інструментом та доступний для завантаження з офіційного сайту. Він може бути використаний для виявлення широкого спектру вразливостей на web-сайтах, але він не забезпечує повного тестування безпеки web-додатків [5, 6].

Кожен з цих сканерів має свої переваги та недоліки, і вибір конкретного інструмента залежить від конкретних потреб та вимог тестування.

Висновки. Дослідження вразливостей web-сайтів та методів їх усунення є дуже актуальною темою в сучасному світі, де web-додатки стають все більш поширеними та важливими для бізнесу та користувачів. Відсутність належного захисту може призвести до крадіжки даних, втрати конфіденційності, порушення цілісності системи та багатьох інших проблем. Виявлені вразливості web-сайтів можуть призвести до втрати конфіденційної інформації, внутрішніх атак, фішингових атак, крадіжки даних користувачів, відмови в обслуговуванні і багатьох інших негативних наслідків. Тому, для забезпечення безпеки web-додатків, необхідно використовувати різні методи захисту та регулярно перевіряти сайти на наявність вразливостей. Серед методів захисту можна виділити: захист від SQL-ін’єкцій, XSS-атак та CSRF-атак; використання сканерів вразливостей, таких як OWASP ZAP, Burp Suite, Acunetix, Nessus, Nikto; регулярне оновлення web-додатків і фіксування виявлених вразливостей. Отже, дослідження вразливостей web-додатків є надзвичайно важливим процесом, який повинен бути проводжений регулярно для забезпечення належного рівня безпеки web-сайтів та їх користувачів. Використання правильних методів та інструментів може допомогти зменшити ризики вразливостей та забезпечити належний захист web-додатків.

Список використаних джерел

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
2. Bhavani A.B. Cross-site Scripting Attacks on Android WebView / A.B. Bhavani // International Journal of Computer Science and Network. – 2013. – Vol. 2, Issue 2. – 5 p. \\ Режим доступу: http://ijcsn.org/IJCSN-2013/2- 2/IJCSN-2013-2-2-03.pdf (останнє звернення 24.03.2023р.).
3. Аналіз причин виникнення вразливостей у веб-додатках \\ Режим доступу до ресурсу: https://www.ptsecurity.com/wwen/analytics/web-vulnerabilities-2020 (останнє звернення: 24.03.2023р).
4. Захист сайтів і веб-додатків \\ Режим доступу до ресурсу: https://cybermolfar.io/services/ web-application-security/ (останнє звернення: 24.03.2023р).
5. Web Application Security Statistics \\ Режим доступу до ресурсу: http://projects. webappsec.org/f/wasc-wafec-v1.0.pdf (останнє звернення: 24.03.2023р).
6. Website Security Statistics Report: 2015. \\ Режим доступу: https://info.whitehatsec.com/ Website-StatsReport-2015.htm (останнє звернення: 24.03.2023р).

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ЗВЄРЄВА В. П.

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНИХ СИСТЕМ В ОСВІТНІЙ ПРОЦЕС

СУГАК О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто поняття інформаційної системи та визначено з яких компонентів вона складається. Наведено переваги та недоліки використання інформаційних систем у навчанні. Досліджено та розглянуто сучасні інформаційні системи, що широко використовуються в освітніх процесах.

The article defines the concept of an information system and identifies its components. The advantages and disadvantages of using information systems in education are demonstrated. The modern information systems that are widely used in educational processes are studied and considered.

Актуальність. Технології все більше впливають на нинішній світ і відмова від їх використання є неправильним вибором, що лише стоятиме на шляху до покращення. Люди переходять від застарілих методів навчання, які не забезпечують актуальністю своїх знань, можуть містити в собі застарілі дані, для зміни яких потребують багато часу та матеріалів.

Вже давно студентське суспільство активно користується інтернетом для успішного навчання, підготовки та досліджень.

Але з розвитком технологій та успіхом у дослідницьких проєктах, з урахуванням сучасних проблем, що вплинули на весь світ як пандемія та війна, переселення в інші країни – людство знайшло спосіб покращити освітній процес та зробити його максимально доступним для будь-кого. Ним стало використання інформаційних систем задля навчання.

Раніше для того, щоб керівник міг передати знання своїм підлеглим, потрібно було знаходити місце, час для зустрічі, узгоджувати купу послідовних питань. Такі ситуації витрачали багато ресурсів і були можливі та доступні не для всіх.

Для того, щоб дізнатися про сучасні методи та бібліотеки специфічних тем, необхідно було шукати книги та надзвичайно детально шукати інформацію в просторах інтернету. Щоб вивчити нові технології, потрібно було проходити дорогі курси та купувати багато літератури, оскільки вона була не розповсюдженою.

Але інтегрування інформаційних систем (ІС) стало можливістю до полегшеного процесу навчання, передачі інформації, зустрічей в онлайн-режимі. Цей процес неймовірно полегшив та скоротив етапи доступу до інформації. На момент пандемії він дав можливість не зупиняти навчальні процеси, а розширити можливості для навчання, причому зробити його набагато доступнішим, ніж будь-коли: зі сторони людини – тобто не залежно від віку, статі та інших чинників; та зі сторони технологій, тобто будь-хто, хто має вихід до мережі. Під час війни постраждало багато освітніх закладів, студенти вимушено виїхали в інші країни, проте онлайн-навчання за допомогою різних систем допомагає продовжувати освітній процес та не зупиняти прогрес поточного навчання.

Метою статті є дослідження поняття інформаційних систем, які інформаційні системи було інтегровано для освітніх процесів та визначення переваг та недоліків їх використання в освіті.

Об'єктом дослідження є інформаційна система.

Аналіз попередніх досліджень – праці по дослідженню інтеграції технологій в навчальний процес писали такі сучасні науковці як: Тюркмен Хакан, Кіммонс Ройс, Акрам Хюма, Хартман Ріта, Марло Джексон, Генота Лаурейн, Ледвіг Крістін та інші.

Предмет дослідження – взаємодія інформаційних систем з суб'єктами освітнього процесу з метою поліпшення якості навчання та результативності навчально-виховного процесу.

Завданням є дослідити наявні інформаційні системи, які використовуються в освіті та знайти приклади успішних практик використання інформаційних систем в освітніх закладах, які існують системи управління навчальним процесом, електронні бібліотеки, системи дистанційного навчання; переваги та недоліки такого формату навчання.

Виклад основного матеріалу. Ті, хто стикаються з терміном інформаційної системи, полягають, що загальне поняття інформаційної системи означає якесь програмне забезпечення та його складові. Проте вона містить в собі набагато більше. Найбільш влучно описано ІС так: інформаційна система – це набір людей, інформаційних технологій та бізнес-процесів для досягнення бізнес-мети [1]. Вона складаються з взаємопов'язаних елементів, які працюють для обробки, зберігання, збору та інших маніпуляцій з інформацією, що використовується для прийняття рішень.

Як і в будь-якій системі, можна розписати такі її компоненти (Рис.1).

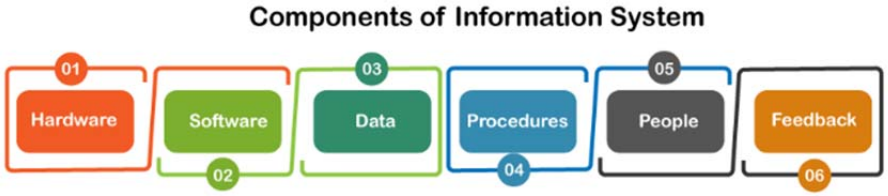

Рис. 1. Компоненти інформаційної системи [1]

Устаткування та програмне забезпечення забезпечують технічне функціонування, інформація та процедури телекомунікації визначають які дані будуть оброблятися та яким способом відбуватимуться маніпуляції даними. Люди та відгуки відповідають за частину, де необхідна людська експертиза та відгук, що покращує кінцевий продукт відповідно до певних вимог [2].

Ізабель Бозада-Джонс (координатор поглибленого навчання для міських шкіл в штаті Огайо) в своїх роздумах наголошує про те, що задля того, щоб змінити в кращу сторону життя дітей і навчити їх чомусь новому, трансформувати і поліпшити освіту, необхідно повністю дозволити старим практикам померти і створити та використовувати щось краще та прогресивніше [3].

Використання інформаційних систем у навчанні не є примхою слідування технологічним досягненням. Вони є пріоритетними, оскільки освітні заклади отримають користь від їх інтеграції:

- Студенти матимуть більшу мотивацію до навчання, поліпшуватимуть свої результати, зменшуватимуться часові затрати за рахунок використання онлайн платформ.
- Інформаційні системи допоможуть студентам управляючи бібліотекою: з можливістю перегляду доступних книг в інтернеті з будь-якого місця в будь-який час, бібліотекар відстежуватиме запити книг для кожного студента та поповнюватиме доступну літературу.
- Не лише студенти отримуватимуть користь, а й викладачі, адже впровадження нових технологій підвищує цифрову грамотність та розвиває нові їх компетенції, збільшуючи їх зону росту.
- Також до переваг необхідно додати прозору комунікацію між студентством та вчителями. ІС допоможуть співпрацювати та спілкуватися для кращого керування та організації освітнього процесу, легшого відстежування та управління академічної діяльності. Створить чесний та правильний процес іспиту шляхом автоматизації всіх етапів екзаменування, що дасть швидкий результат.

Проте, незважаючи на значний перелік переваг інтеграції інформаційних систем в освітній процес, можна виділити і такі недоліки:

- Неповна заміна традиційного навчання. Звісно для спеціальностей та програм, що тісно зв'язані з ІТ-сферою, немає необхідності фізичної присутності на лекціях, семінарах. Але студенти, що потребують практичних навичок, експериментів, дослідів – для них вона необхідна, тому ІС не зможе повністю замінити традиційне навчання.
- Технічні проблеми. У разі збоїв, недоступності сервісів, поломки серверів, освітній процес зупиниться до моменту, поки не будуть вирішені усі питання та не полагоджено обладнання.
- Залежність від технологій. Для навчання мінімально потрібен доступ до мережі інтернет та наявність технічного обладнання. В сучасних реаліях при тривалих відключеннях світла порушувався процес навчання, що негативно впливало на результати студентів.
- Неправильне використання. Якщо неправильно використовувати можливості інформаційних систем, то можна не підвищити ефективність навчання, а створити перепону до доступності матеріалів та бажання її освоєння.
- Міжнародні стандарти. Розробка інформаційних систем створюється за певних стандартів, проте не всі вони є універсальними для всіх країн. Це може завадити співпрацювати з матеріалами інших країн та визнавати дипломи і кількість кредитів матеріалу.

Наразі у світі існує величезна кількість таких систем: від платних до безкоштовних, для звичайних студентів та бізнес-користувачів. Основною їх ціллю є навчання та поліпшення навичок. Розглянемо системи, що широко відомі в суспільстві та часто використовуються в освітніх процесах.

Coursera – це платформа для онлайн-курсів, яка надає доступ до навчальних програм від провідних університетів та компаній світу [4]. Її можна охарактеризувати як ІС, оскільки забезпечує інтеграцію і обмін даними між різними компонентами платформи, такими як користувачі, курси, лекції, завдання, відео матеріали та інші ресурси.

Ця платформа має зручний інтерфейс для користувачів, щоб вони могли швидко та легко знайти необхідний курс, зареєструватись на нього та освоїти матеріал. Крім того, платформа забезпечує можливість контролю навчання шляхом здачі тестів та отримання сертифікатів про успішне завершення курсу. Вона збирає курси та матеріали з усього світу та забезпечує інтеграцію зовнішніми ІС як соцмережами, поштовими сервісами для підвищення ефективності користування платформою.

Google Workspace є однією з найпопулярніших інформаційних систем для освіти та бізнесу. Ця ІС надає безліч інструментів для ефективної співпраці, комунікації та навчання. Для освіти Google Workspace пропонує спеціальний пакет інструментів, що називається Google Workspace for Education. Він включає в себе різноманітні застосунки, такі як Google Classroom, Google Drive, Google Docs, Google Sheets та інші (Рис.2).

З їх допомогою викладачі мають можливість створювати і редагувати документи в режимі реального часу та офлайн, надавати завдання та відстежувати їх виконання, проводити онлайн-уроки. Студенти в свою чергу можуть відслідковувати свої завдання, їх виконання та оцінювання, створювати плани та організовувати свої навчальні процеси. Користувачі можуть взаємодіяти між собою за допомогою пошти, чату або ж відеоконференцій. Будь-хто може користуватися застосунками, що є великим плюсом, оскільки є доступним для всіх верств населення, більш того, Google Workspace є доступним на різних пристроях та операційних системах, що робить цю інформаційну систему універсальною [5].

Prometheus – це найбільше навчальна платформа в Україні, яка надає інструменти для створення, організації та проведення навчальних курсів та іспитів онлайн [6]. Ця інформаційна система призначена для використання в освітніх установах, компаніях та організаціях з метою забезпечення зручного та ефективного онлайн-навчання. ІС дозволяє викладачам створювати інтерактивні курси та завдання, які можуть бути доступні для учнів у будь-який зручний для них час для проходження. Платформа також надає можливість створювати тестові завдання та іспити з автоматичною перевіркою, що дозволяє викладачам ефективно та швидко оцінювати знання студентів.

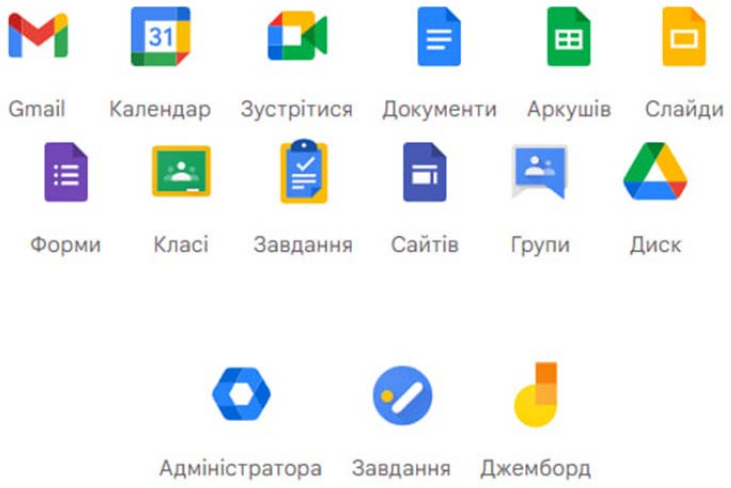

Рис. 2. Сервіси від Google Workspace [5]

Однією з головних переваг Prometheus є те, що платформа є безкоштовною та відкритою для використання, що дозволяє учасникам освітнього процесу отримувати доступ до якісної онлайн освіти незалежно від їхнього фінансового стану. Крім того, Prometheus має велику кількість інструментів для відстеження прогресу студентів, що дозволяє викладачам ефективно спілкуватися зі студентами, консультувати їх та покращувати якість навчання. Вона має два доступи до навчання: безкоштовний та Prometheus+ (Рис. 3). Такий поділ дає можливість навчатись будь-кому на безкоштовній основі та створювати й проходити ексклюзивні курси для певних категорій студентів з розширеними можливостями для навчання.

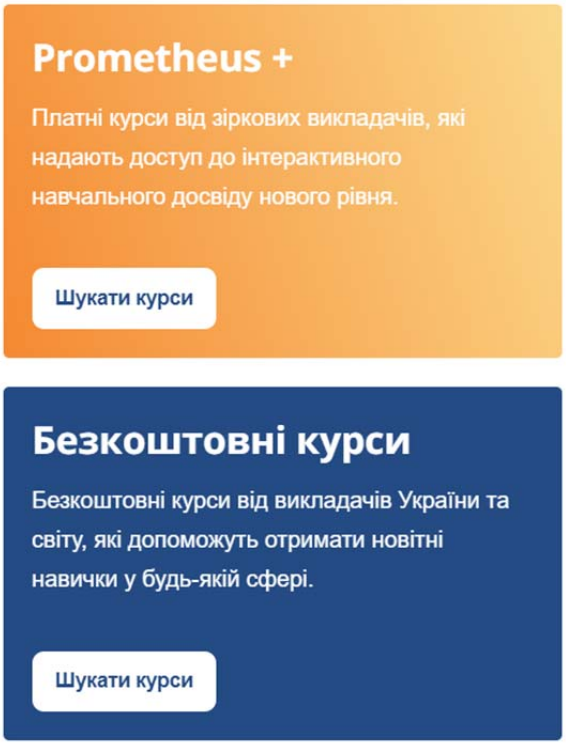

Рис. 3. Вибір каталогу до курсів Prometheus [6]

Окрім навчання студентства, потрібно враховувати і звичайних людей у повсякденному часі. Вони живуть у постійному русі технологій та навчання є стимулом до подальшого розвитку. Саме тому створили такі компанії як AcademyOcean, Docebo.

Docebo – це хмарна платформа управління навчаннями, яка дозволяє підприємствам і навчальним організаціям створювати та керувати ефективними програмами навчання для співробітників, клієнтів та партнерів [7]. Платформа має такі функції як: створення, організація та виконання онлайн-курсів, тестування та інших завдань навчання в будь-який час та з будь-якого місця, що робить її ефективною системою для дистанційного навчання (Рис.4).

Рис. 4. Навчальний цикл в Docebo [7]

Платформа має різноманітні інструменти для моніторингу та оцінювання результатів навчання, такі як звіти та аналітика і також інтегрується з багатьма іншими системами, що дозволяє легко і ефективно інтегрувати Docebo з існуючими системами управління навчаннями та іншими інформаційними системами. Крім того, потрібно додатково зазначити про забезпечення безпеки даних та конфіденційності, що є дуже важливим для бізнес та навчальних організацій.

Схожою системою за функціоналом є AcademyOcean (Рис.5). Це інформаційна система, яка також дозволяє компаніям та навчальним закладам створювати власні онлайн-курси, тренінги та іспити для своїх співробітників та студентів і відслідковувати показники виконання завдань. Для більш ефективного навчання, система пропонує різні методики та інструменти, такі як відео уроки, інтерактивні завдання та тести, відгуки та коментарі, які дозволяють користувачам взаємодіяти та ділитися своїми думками та враженнями, що покращує освітній процес [8]. AcademyOcean має досить доступну ціну та можливість безкоштовного використання для невеликих груп користувачів.

Рис. 5. Українська розумна система для бізнесу [8]

Проте недоліками останніх систем є менший поріг доступності. З широким функціоналом, вони мають лише платний доступ, тому дані ІС підходять для бізнес компаній, що хочуть розвивати своїх клієнтів та працівників.

Висновки. Аналізуючи розглянутий в статті матеріал, можна зробити висновок, що інтеграція інформаційних систем в освітній процес є надзвичайно корисним процесом. Вона матиме позитивний вплив на навчання та покращить якість освіти. Інформаційні системи можуть забезпечувати більшу доступність матеріалів для студентів, зменшувати часові затрати на пошук необхідної інформації та покращувати результати навчання. Вони оцінюватимуть чесно та швидко результати перевірок. Також, ІС зможе допомогти в управлінні бібліотекою та сприяти більш ефективній комунікації між студентами та викладачами, за рахунок збільшення можливих методів спілкування.

Проте, важливо взяти до уваги, що неправильне використання інформаційних систем може не тільки погіршити ефективність навчання, але й створити додаткові перепони до доступності матеріалів та бажання її освоєння. Крім того, повна заміна традиційного навчання, особливо для студентів, що потребують практичних навичок, може зробити інформаційні системи менш ефективними в певних випадках. Можливим виходом з цієї ситуації є використання VR та AR технологій, які зможуть наочно показати студентам необхідні практичні роботи, створювати досліди, без необхідності бути присутнім фізично на занятті.

Інтеграція інформаційних систем у освітній процес є невід'ємною частиною сучасної освіти. Вона дозволяє створити навчальне середовище, яке сприяє залученню та мотивації учнів, поліпшенню якості навчання та спрощенню взаємодії між учасниками навчального процесу. Для досягнення успіху в інтеграції інформаційних систем слід уважно розглядати переваги, виклики та кращі практики, спираючись на спільний зусилля педагогів, технологічних експертів та адміністраторів. В результатах цієї спільної праці полягає справжній потенціал технологій у трансформації навчального процесу.

Отже, висновки полягають в тому, що інформаційні системи мають великий потенціал для використання в освітньому процесі, але поки їх необхідно розглядати як допоміжні засоби та правильно використовувати, щоб досягти найбільш ефективних результатів.

Список використаних джерел

1. Information System Definition [Електронний ресурс]. – Режим доступу : https://www.javatpoint.com/information-system-definition
2. What is information systems? Definition, uses, and examples [Електронний ресурс]. – Режим доступу : https://zapier.com/blog/what-is-information-systems/
3. To Improve a Child's Education, We Must Be Willing to Let Old Practices Die [Електронний ресурс]. – Режим доступу : https://www.edsurge.com/news/2023-04-05-to-improve-a-child-s-education-we-must-be-willing-to-let-old-practices-die
4. Coursera's mission, vision [Електронний ресурс]. – Режим доступу : https://about. coursera.org/
5. Creating new possibilities in higher education [Електронний ресурс]. – Режим доступу : https://edu.google.com/intl/en_ALL/why-google/for-your-institution/higher-ed-solutions/
6. Про нас. Prometeus [Електронний ресурс]. – Режим доступу : https://prometheus. org.ua/about-us/
7. All your learning challenges, solved [Електронний ресурс]. – Режим доступу : https://www.docebo.com/
8. Розумна система для навчання [Електронний ресурс]. – Режим доступу : https://academyocean.com/ua

Робота виконана під науковим керівництвом канд. техн. наук, доцента
РЗАЄВОЇ С. Л.

АНАЛІЗ ВІДПОВІДНОСТІ ПЛАТІЖНИХ СИСТЕМ ДО НОРМ GDPR

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

Ця стаття присвячена аналізу відповідності платіжних систем до норм. Вона включає перевірку законодавчої відповідності, безпеки, зручності та вартості використання платіжних систем для користувачів та бізнесу. Детальніше буде розглянуто різноманітні питання, пов'язані з відповідністю платіжних систем до норм та їхніх можливостей у сучасному світі.

This article is dedicated to the analysis of compliance of payment systems with regulations. It includes checking the legislative compliance, security, convenience, and cost-effectiveness of using payment systems for users and businesses. Further, a variety of issues related to the compliance of payment systems with regulations and their capabilities in the modern world will be discussed.

Актуальність дослідження. Зі збільшенням використання платіжних систем у цифровій економіці захист персональних даних став гострою проблемою. Загальний регламент захисту даних (General Data Protection Regulation, GDPR) – це нормативна база, спрямована на захист персональних даних осіб у межах Європейського Союзу (ЄС) і має значний вплив на платіжні системи. Ця стаття є актуальною, оскільки містить поглиблений аналіз відповідності платіжних систем нормам GDPR.

Метою цієї статті є аналіз відповідності платіжних систем нормам GDPR. Цей аналіз має на меті визначити основні виклики та ризики, з якими стикаються платіжні системи з точки зору захисту даних, і оцінити рівень їх відповідності нормам GDPR. Крім того, ця стаття має на меті надати рекомендації платіжним системам щодо покращення відповідності GDPR та зменшення ризиків, пов'язаних із захистом даних.

Об'єктом дослідження є платіжні системи та їх відповідність нормам GDPR. Це дослідження має на меті визначити типи даних, які обробляють і зберігають платіжні системи, основні виклики та ризики, з якими стикаються платіжні системи щодо захисту даних, а також рівні відповідності платіжних систем нормам GDPR.

Предметом цього дослідження є структура відповідності GDPR та її ключові компоненти. Це дослідження має на меті надати огляд системи відповідності GDPR і того, як платіжні системи можуть застосовувати її до своїх операцій. Крім того, це дослідження роз'яснює ролі та обов'язки різних учасників у забезпеченні відповідності GDPR у платіжних системах.

Оскільки світ стає все більш цифровим, платіжні системи стали важливою частиною економіки [1]. Однак через величезну кількість особистих даних, які обробляють платіжні системи, виникає занепокоєння щодо захисту конфіденційності та даних людей. Тут вступає в дію Загальний регламент захисту даних (GDPR).

GDPR – це всеосяжний регламент захисту даних, який набув чинності в травні 2018 року і призначений для посилення захисту персональних даних і конфіденційності осіб у Європейському Союзі (ЄС). Він поширюється на всі компанії, які обробляють персональні дані громадян ЄС, незалежно від того, де розташована компанія [2]. Це означає, що платіжні системи, які збирають і обробляють величезні обсяги персональних даних, також повинні відповідати нормам GDPR.

Актуальність GDPR для платіжних систем неможливо переоцінити. Платіжні системи використовуються для обробки фінансових транзакцій, і тому вони обробляють конфіденційні особисті дані, такі як номери кредитних карток, реквізити банківського рахунку та особиста ідентифікаційна інформація [1]. Якщо ці дані не захищені належним чином, це

може призвести до серйозних фінансових і репутаційних dзбитків як для платіжних систем, так і для їх користувачів.

Основні принципи та вимоги GDPR включають отримання інформованої та чіткої згоди від осіб перед обробкою їхніх персональних даних, впровадження відповідних технічних та організаційних заходів для захисту персональних даних, надання особам права доступу та виправлення своїх персональних даних, а також повідомлення про порушення даних. до контролюючих органів протягом 72 годин [4, 5].

Рис. 1. Відповідність GDPR [8]

У цій статті ми розберемо відповідність платіжних систем нормам GDPR. Ми оглянемо платіжні системи, їх діяльності з обробки даних і рамок відповідності GDPR. Оцінимо відповідність платіжних систем нормам GDPR та визначимо найкращі практики. Ми також обговоримо наслідки невідповідності нормам GDPR для платіжних систем і надамо рекомендації щодо підвищення відповідності GDPR.

Платіжні системи є важливою частиною цифрової економіки, що дозволяє окремим особам і компаніям здійснювати електронні транзакції. Ці системи, які включають процесори кредитних і дебетових карток, мобільні платіжні програми та онлайн-платіжні шлюзи, відповідають за обробку величезних обсягів персональних даних. Однак це також означає, що вони вразливі до витоку даних, кібератак та інших ризиків захисту даних.

Щоб зрозуміти відповідність платіжних систем нормам GDPR, важливо спочатку мати розуміння про ці системи та їх діяльності з обробки даних. Платіжні системи можна визначити як платформи, які полегшують переказ грошей від однієї організації до іншої, як правило, за допомогою електронних засобів. Ці системи відіграють вирішальну роль у цифровій економіці, дозволяючи компаніям здійснювати операції з клієнтами та постачальниками по всьому світу.

Одним із основних типів даних, які платіжні системи обробляють і зберігають, є персональні дані. Це може включати таку інформацію, як імена, адреси, адреси електронної пошти та номери телефонів. Крім того, платіжні системи також обробляють конфіденційні фінансові дані, такі як номери кредитних карток, реквізити банківських рахунків та історії транзакцій [3]. Усі ці дані є дуже конфіденційними та мають бути захищені, щоб запобігти несанкціонованому доступу, крадіжці чи неправомірному використанню.

Незважаючи на критичну роль, яку платіжні системи відіграють у цифровій економіці, вони стикаються з декількома ключовими ризиками та проблемами щодо захисту даних. Однією з найбільш важливих проблем є дедалі складніші кібератаки, які можуть бути спрямовані на вразливі місця платіжних систем і призвести до витоку даних. Платіжні системи також повинні вирішувати проблеми, пов'язані з безпекою даних, такими як підтримка точності даних, захист від несанкціонованого доступу та забезпечення цілісності даних. Крім того, вони повинні забезпечити прозорість своєї діяльності з обробки даних, надаючи чітку інформацію про те, як дані збираються, обробляються та використовуються.

Наслідки витоку даних і недотримання норм GDPR можуть бути серйозними для платіжних систем. Ці наслідки можуть включати значні фінансові втрати, шкоду репутації та юридичну відповідальність. Таким чином, платіжні системи повинні серйозно ставитися до захисту даних і вживати відповідних заходів для забезпечення відповідності нормам GDPR.

Щоб забезпечити відповідність нормам GDPR, платіжні системи повинні запровадити комплексну структуру відповідності GDPR. Структура відповідності GDPR складається з кількох ключових компонентів, включаючи відображення даних, оцінку ризиків, політики та процедури, а також навчання та обізнаність працівників [9].

Відображення даних – це процес ідентифікації та документування всіх персональних даних, які збираються, обробляються та зберігаються платіжними системами. Це включає дані, які зберігаються сторонніми постачальниками, і передачу даних до країн за межами ЄС [4]. Після відображення даних платіжні системи можуть проводити оцінку ризиків, щоб визначити потенційну вразливість, загрози та ризики для персональних даних, які вони зберігають.

На основі результатів оцінки ризиків платіжні системи повинні розробити політики та процедури, спрямовані на виявлені ризики та забезпечення відповідності GDPR. Ці політики та процедури мають включати заходи щодо захисту даних, повідомлення про порушення та права суб'єктів даних. Важливо забезпечити регулярний перегляд і оновлення цих політик і процедур, щоб відобразити зміни в нормативному середовищі або бізнес-практики [5].

Іншим важливим компонентом відповідності GDPR є навчання та обізнаність працівників. Платіжні системи повинні забезпечити, щоб співробітники пройшли навчання щодо відповідності GDPR, включаючи політики та процедури захисту даних, і усвідомлювали свої обов'язки щодо захисту персональних даних. Співробітники повинні розуміти важливість дотримання GDPR і вміти визначати ризики та порушення захисту даних і повідомляти про них.

Платіжні системи можуть застосувати рамки відповідності GDPR до своїх операцій, попередньо оцінивши свій поточний статус відповідності вимогам GDPR. Потім вони повинні розробити дорожню карту, яка окреслює кроки, необхідні для досягнення відповідності GDPR, включаючи відображення даних, оцінку ризиків, розробку політики та навчання співробітників. Важливо переконатися, що всі аспекти рамок відповідності GDPR реалізовані, і регулярні аудити проводяться для моніторингу відповідності [5].

У забезпеченні відповідності GDPR різні учасники відіграють різні ролі та відповідальність. Платіжні системи несуть відповідальність за забезпечення відповідності нормам GDPR і вжиття відповідних заходів для захисту персональних даних. Сторонні постачальники, такі як платіжні постачальники та постачальники зберігання даних, також повинні відповідати нормам GDPR і бути прозорими у своїй діяльності з обробки даних.

Органи нагляду, наприклад органи захисту даних, відіграють важливу роль у забезпеченні відповідності GDPR, надаючи вказівки, забезпечуючи дотримання норм GDPR, розслідуючи та накладаючи санкції на невідповідність. Суб'єкти даних також відіграють вирішальну роль у дотриманні GDPR, реалізуючи свої права, наприклад право на доступ до своїх особистих даних і право на їх виправлення, а також повідомляючи про будь-які порушення захисту даних контролюючим органам.

Після розуміння принципів відповідності GDPR і того, як платіжні системи можуть застосовувати їх у своїх операціях, важливо оцінити рівень відповідності платіжних систем

нормам GDPR. Оцінка відповідності може допомогти платіжним системам визначити сфери, де їм потрібно вдосконалити, і розробити дорожню карту для досягнення повної відповідності GDPR.

Одним із критичних критеріїв оцінки відповідності GDPR є оцінка впливу на захист даних (DPIA). Data Protection Impact Assessment (DPIA) – це обов'язковий процес, який платіжні системи повинні виконувати, щоб виявити та мінімізувати ризики захисту даних, пов'язані з їх діяльністю. DPIA оцінює необхідність, пропорційність і законність діяльності з обробки даних і визначає потенційні ризики для захисту даних і заходи для їх зменшення. Платіжні системи повинні забезпечити проведення DPIA для всіх нових дій з обробки та регулярний перегляд для відображення змін у операційній діяльності чи нормативному середовищі [6].

Ще одним критерієм оцінки відповідності GDPR є політика конфіденційності. Платіжні системи повинні мати чітку та стислу політику конфіденційності, яка пояснює їх діяльність з обробки даних і спосіб збору, обробки та зберігання персональних даних. Політика конфіденційності також повинна містити інформацію про права суб'єкта даних, наприклад право на доступ до особистих даних і їх виправлення, а також контактні дані уповноваженого із захисту даних. Платіжні системи повинні гарантувати, що їхня політика конфіденційності є доступною, прозорою та актуальною.

Механізми згоди також мають вирішальне значення для оцінки відповідності GDPR. Платіжні системи повинні отримати чітку та інформовану згоду суб'єктів даних перед збором, обробкою або зберіганням їхніх персональних даних. Платіжні системи також повинні гарантувати, що суб'єкти даних можуть відкликати свою згоду в будь-який час і що механізми згоди є доступними, зрозумілими та стислими.

Іншими критеріями для оцінки відповідності GDPR є права суб'єктів даних і процедури сповіщення про порушення даних. Платіжні системи повинні гарантувати, що суб'єкти даних можуть реалізувати свої права, такі як право на доступ і виправлення персональних даних, а також оперативну відповідь на запити. Платіжні системи також повинні мати чіткі та ефективні процедури сповіщення про порушення даних, які дозволяють їм виявляти, повідомляти та розслідувати порушення даних протягом необхідного 72-годинного періоду.

Порівняння рівнів відповідності різних платіжних систем і визначення найкращих практик може допомогти платіжним системам навчатися одна в одної та покращити відповідність GDPR. Платіжні системи, які демонструють високий рівень відповідності GDPR, можуть слугувати взірцем для інших платіжних систем. Найкращі практики щодо відповідності GDPR включають впровадження комплексної системи відповідності GDPR, проведення регулярних аудитів та оцінок, а також забезпечення навчання та підвищення обізнаності працівників.

Невідповідність GDPR може мати серйозні наслідки для платіжних систем, включаючи штрафи, репутаційну шкоду та юридичну відповідальність. Штрафи GDPR можуть становити до 4% річного глобального доходу компанії або 20 мільйонів євро, залежно від того, що більше. Платіжні системи, які не відповідають нормам GDPR, також можуть зазнати репутаційної шкоди, оскільки клієнти можуть втратити довіру до здатності платіжної системи захистити їхні особисті дані. Невідповідність GDPR також може призвести до юридичної відповідальності, оскільки суб'єкти даних можуть вимагати компенсації за будь-яку шкоду, заподіяну внаслідок невідповідності платіжної системи [7].

Висновки

Підсумовуючи, дотримання правил GDPR має важливе значення для платіжних систем для підтримки довіри клієнтів і забезпечення довгострокової стабільності їх операцій. Оцінка відповідності GDPR на основі різних критеріїв, таких як DPIA, політика конфіденційності, механізми отримання згоди, права суб'єктів даних і процедури сповіщення про порушення даних, може допомогти платіжним системам визначити сфери для вдосконалення та розробити дорожню карту для досягнення повної відповідності GDPR. Порівняння рівнів відповідності різних платіжних систем і визначення найкращих практик також можуть

допомогти платіжним системам покращити відповідність GDPR. Невідповідність GDPR може мати серйозні наслідки для платіжних систем, включаючи штрафи, репутаційну шкоду та юридичну відповідальність. Важливо, щоб платіжні системи надавали пріоритет відповідності GDPR, щоб захистити особисті дані та зберегти довіру клієнтів.

Підсумовуючи вище сказане, аналіз відповідності платіжних систем нормам GDPR є надзвичайно важливим у сучасній цифровій економіці. Наша оцінка показала, що багатьом платіжним системам ще потрібно пройти довгий шлях, щоб досягти повної відповідності вимогам GDPR. Однак деякі платіжні системи досягли значного прогресу у відповідності цим стандартам, і їхні найкращі практики можуть слугувати керівництвом для інших.

На основі наших критеріїв оцінки ми виявили, що багато платіжних систем не повністю запровадили оцінки впливу на захист даних, політики конфіденційності та механізми отримання згоди відповідно до стандартів GDPR. Подібним чином деякі платіжні системи не мають відповідних прав суб'єктів даних і процедур сповіщення про порушення даних. Тому ми рекомендуємо всім платіжним системам застосовувати більш проактивний підхід для дотримання норм GDPR.

Крім того, недотримання GDPR може призвести до серйозних наслідків, таких як великі штрафи, репутаційні збитки та юридична відповідальність. Платіжні системи повинні визнавати важливість відповідності GDPR для підтримки довіри клієнтів і забезпечення довгострокової стабільності в галузі.

Як висновок, структура відповідності GDPR є важливим інструментом, який можуть використовувати платіжні системи, щоб переконатися, що вони відповідають необхідним стандартам захисту даних і конфіденційності. Застосовуючи найкращі практики та усуваючи прогалини у відповідності, платіжні системи можуть досягти більшої довіри та впевненості серед клієнтів, що може допомогти їм досягти успіху на конкурентному ринку. Відповідність нормам GDPR не слід розглядати як тягар, а як можливість продемонструвати відданість конфіденційності та захисту даних клієнтів.

Список використаних джерел

1. Г.В. Коваленко, І.В. Коваль. «Моделювання та аналіз інформаційно-комунікаційних систем». – К.: Видавництво «Логос», 2016. – 272 с.
2. О.О. Шумило. «Технології захисту інформації в комп'ютерних системах». – К.: Інформаційно-аналітичне агентство, 2014. – 240 с.
3. М.О. Шевченко. «Захист інформації в комп'ютерних мережах». – К.: Видавництво «Політехніка», 2016. – 292 с.
4. Офіційний портал Європейського Союзу з питань захисту персональних даних (https://ec.europa.eu/info/law/law-topic/data-protection_en)
5. Офіційний текст загального регламенту про захист персональних даних (GDPR) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679)
6. Директива Європейського Парламенту та Ради 2015/2366/ЄС щодо платіжних послуг в межах внутрішнього ринку, що змінює та визначає Закон про платіжні послуги 2009 року (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366)
7. Наказ Національного банку України «Про затвердження Типових правил забезпечення безпеки платіжних карток» від 16.11.2016 р. № 376 https://zakon.rada.gov.ua/laws/show/z2049-16
8. GDPR Compliance https://www.collidu.com/presentation-gdpr-compliance
9. Кокарча, Ю., & Лалуєва, А. (2022). ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ: ВПЛИВ ВОЄННОГО СТАНУ. Collection of Scientific Papers «SCIENTIA», (November 25, 2022; Sydney, Australia), 70–74. Retrieved from https://previous.scientia.report/index.php/archive/article/view/579

Робота виконана під науковим керівництвом старшого викладача
БЕБЕШКО Б. Т.

МОНІТОРИНГ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ

ТУРЧЕНКО Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто інформацію про важливість забезпечення інформаційної безпеки на підприємствах. Визначено сучасні засоби забезпечення інформаційної безпеки на прикладі SIEM-систем, наведені найбільш популярні виробники та постачальники послуг SIEM-систем. Описано основне призначення та особливості SIEM-систем для збору інформації та управління подіями.

The article discusses information about the importance of ensuring information security at enterprises. Modern means of ensuring information security are defined using the example of SIEM systems, the most popular manufacturers and service providers of SIEM systems are listed. The main purpose and features of SIEM systems for collecting information and managing events are described.

Актуальність. Удосконалення та забезпечення системи безпеки співробітників підприємства є одним із пріоритетних напрямів досягнення максимальної ефективності його діяльності. Від того, яким чином є сформована система безпеки співробітників на підприємстві, залежить ефективність реалізації поставлених його цілей. Результатом якісної роботи підприємства в сфері безпеки є стабільність і гармонійність її діяльності, і, як наслідок, стабільне зростання такого показника, як оптимізація прибутковості підприємства. Система моніторингу стану інформаційної безпеки є основним елементом системи безпеки підприємства, оскільки, від якості діяльності співробітників залежать сфери діяльності підприємств.

Моніторинг стану інформаційної безпеки, за допомогою дій співробітників підприємства – це результат налагодженої роботи багатьох служб, у першу чергу, служби безпеки та служби персоналу. Кожен претендент на вакансію, співробітник підприємства повинен розглядатися, як джерело ризику та потенційної загрози. Ризики можуть бути пов’язані як з умисним нанесенням шкоди, так і з необережністю. Потенційно небезпечними є працівники з низьким рівнем кваліфікації. Невідповідність рівня кваліфікації займаній посаді призводить до невдоволення працівника своєю роботою та умовами праці. На виникнення ризиків, також, впливають відсутність чітко і однозначно закріплених юридичних правовідносин, неадекватне оцінювання результатів праці. До втрат і збитків може привести низька якість прогнозування і контролювання зміни благонадійності тощо.

Метою статті є дослідження особливостей моніторингу стану інформаційної безпеки на підприємствах.

Об’єктом дослідження є процес моніторингу інформаційної безпеки.

Предмет дослідження – комп’ютерна мережа підприємства.

Аналіз попередніх досліджень. Дослідженням питань інформаційної безпеки займається ряд як вітчизняних, так і закордонних дослідників, а також значна кількість державних і недержавних наукових установ, дослідницьких та аналітичних центрів. Серед науковців, що досліджують проблеми інформаційної безпеки: А. Грамші, К. Кубечка, Р. Калюжний, Б. Кормич, В. Ліпкан, В. Макаренко, Ю. Максименко, О. Барановський та ін.

Виклад основного матеріалу. Сьогодні існує безліч загроз інформаційній безпеці підприємств, бізнесовим структурам. Серед загроз з якими стикаються підприємства − зовнішні вторгнення в корпоративні мережі і, як результат, – недоступність до корпоративних сервісів, викрадення конфіденційних даних та інформації, неможливість

контролю веб-трафіку, проникнення вірусів і, так званих, «троянських» програм, різні види внутрішніх і зовнішніх загроз підприємству та його діяльності.

Інформаційна безпека – стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз. Захист інформації передбачає систему заходів, спрямованих на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації, втрати, знищення, порушення цілісності [1, 2].

Метою реалізації інформаційної безпеки (ІБ) будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту. Для побудови та ефективної експлуатації системи забезпечення ІБ необхідно [2]:

- виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;
- врахувати вимоги національного та міжнародного законодавства;
- використовувати напрацьовані практики (стандарти, методології) побудови подібних системи забезпечення ІБ;
- визначити підрозділи, відповідальні за реалізацію та підтримку системи забезпечення ІБ;
- розподілити між підрозділами області відповідальності у здійсненні вимог системи забезпечення ІБ;
- на базі управління ризиками ІБ визначити загальні положення, технічні та організаційні вимоги, що становлять політику ІБ об'єкта захисту;
- реалізувати вимоги політики ІБ, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;
- реалізувати систему управління інформаційної безпеки (СУІБ);
- використовуючи СУІБ, організувати регулярний контроль ефективності системи забезпечення ІБ та при необхідності переглядати і коригувати системи забезпечення ІБ і СУІБ.

Для побудови політики ІБ рекомендується окремо розглядати основні напрями захисту ІБ:

- захист об'єктів ІБ;
- захист процесів, процедур і програм обробки інформації;
- захист каналів зв'язку (акустичні, інфрачервоні, провідні оптичні);
- придушення побічних електромагнітних випромінювань;
- управління системою захисту.

При цьому політика ІБ повинна описувати наступні етапи створення засобів захисту інформації:

1. Визначення інформаційних і технічних ресурсів, що підлягають захисту.
2. Виявлення повної безлічі потенційно можливих загроз і каналів витоку інформації.
3. Проведення оцінки вразливості і ризиків інформації за наявної безлічі загроз і каналів витоку.
4. Визначення вимог до системи захисту.
5. Здійснення вибору засобів захисту інформації та їх характеристик.
6. Впровадження та організація використання обраних заходів, способів та засобів захисту.
7. Здійснення контролю цілісності і керування системою захисту.

Політика ІБ оформляється у вигляді задокументованих вимог на інформаційну систему. Документи зазвичай поділяють за рівнями деталізації процесу захисту. Документи верхнього рівня політики ІБ відображають позицію організації до діяльності в галузі захисту інформації, її прагнення відповідати державним, міжнародним вимогам і стандартам у цій галузі. Подібні документи можуть називатися «Концепція ІБ», «Регламент управління ІБ», «Політика ІБ», «Технічний стандарт ІБ» тощо. Область поширення документів верхнього рівня зазвичай не обмежується, проте дані документи можуть випускатися і в двох редакціях − для зовнішнього і внутрішнього використання [1, 2].

Організаційний захист об’єктів інформаційних систем (ІС) − це регламентація виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз [1].

До основних організаційних заходів належать [1, 2]:

- організація режиму і охорони. Їх мета − виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб;
- організація роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;
- організація роботи з документами та документованою інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;
- організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;
- організація роботи з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту;
- організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв.

Засоби захисту інформації поділяються на: засоби захисту від несанкціонованого доступу (засоби авторизації, мандатне управління доступом, виборче управління доступом, управління доступом на основі ролей, аудит); системи аналізу та моделювання інформаційних потоків (CASE-системи); системи моніторингу мереж (системи виявлення й запобігання вторгнень (IDS / IPS), системи запобігання витоків конфіденційної інформації (DLP-системи); аналізатори протоколів; антивірусні засоби; міжмережеві екрани; криптографічні засоби (шифрування, цифровий підпис); системи резервування; системи безперебійного живлення; системи аутентифікації на основі пароля, ключа доступу (фізичного або електронного); біометричних даних; засоби запобігання злому корпусів і крадіжок устаткування; засоби контролю та управління доступом в приміщення; інструментальні засоби аналізу систем захисту [2].

Для забезпечення ІБ та керування інцидентами безпеки використовують SIEM-системи (Security Information and Event Management). Абревіатура SIEM означає «Система збору та кореляції подій». Як можна судити з назви, самі по собі такі системи не здатні що-небудь запобігати або захищати. Їх завдання в іншому – аналізувати інформацію, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, міжмережеві екрани, операційні системи серверів. SIEM-системи представлені додатками, приладами і послугами. SIEM-система моніторингу дозволяє звести всі події та інциденти ІБ в єдиній структурі, виконує інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи щодо ІБ мереж [1, 3, 4]. Крім цього, система моніторингу ІБ виконує реєстрацію та зберігання всіх інцидентів ІБ, що робить можливим використання отриманого матеріалу в якості доказового при виконанні розслідувань інцидентів та в судочинстві [4]. Робота цієї системи дозволяє побачити більш повну картину активності мережі і інцидентів ІБ. Але разом з тим, цю систему використовують як додатковий спосіб захисту від цілеспрямованих атак на мережу. SIEM-система повинна збирати, аналізувати, моніторити і представляти інформацію із мережевих приладів і приладів безпеки.

Функції SIEM-системи спрямовані на моніторинг основних подій і станів інформаційної безпеки всередині компанії та її діяльності. Основними функціями можна назвати [4]:

- моніторинг автентифікації та знаходження компроментуючих аккаунтів користувачів мережі та адміністраторів;

- моніторинг випадків зараження мереж;
- моніторинг підозрілого вихідного трафіку мереж і передання по мережі даних с використанням журналів веб-проксі;
- відстеження системи змін і інших адміністративних дій у внутрішніх мережах на їх відповідність дозволеного протоколу даних компанії;
- моніторинг атак на веб-додатки шляхом аналізу різних звітів;
- відстеження крадіжок даних та інших підозрілих зовнішніх підключень.

Слід приділити особливу увагу налаштуванню SIEM під клієнта, його інфраструктуру і системи безпеки. Правильно налаштовані правила використання системи дозволять спеціалісту аналізувати дійсно важливі повідомлення про інциденти порушення ІБ, фільтруючи зайві дані [3].

SIEM-системи використовують інформацію з таких джерел, як [4]:

- системи автентифікації і системи контролю і управління доступом (Access Control);
- антивірусні засоби;
- міжмережеві екрани; системи виявлення / запобігання вторгнень;
- системи проксінг доступу в інтернет і веб-фільтрації; активні мережеві пристрої;
- системні журнали подій ІБ серверів і робочих станцій користувачів;
- журнали аудиту систем управління базами даних;
- ключові корпоративні ресурси: поштові сервери, файлообмінні сервери, CRM- і ERP-системи;
- інші бізнес-додатки відповідно до вимог ІБ компаній і стандартів.

Типове рішення SIEM-системи включає в себе кілька функціональних компонентів, які зображені на Рис. 1.: агенти, що встановлюються на інформаційну систему, яка моніториться (актуально для операційних систем; агент являє собою резидентну програму (сервіс, демон, служба), яка локально збирає журнали подій і по можливості передає їх на сервер); колектори на агентах, які, по суті, являють собою модулі (бібліотеки) для розуміння конкретного журналу подій або системи; сервери-колектори, призначені для попередньої акумуляції подій від безлічі джерел; сервер-корелятор, що відповідає за збір інформації від колекторів і агентів і обробку за правилами і алгоритмами кореляції; сервер баз даних і сховища, який відповідає за зберігання журналів подій [4].

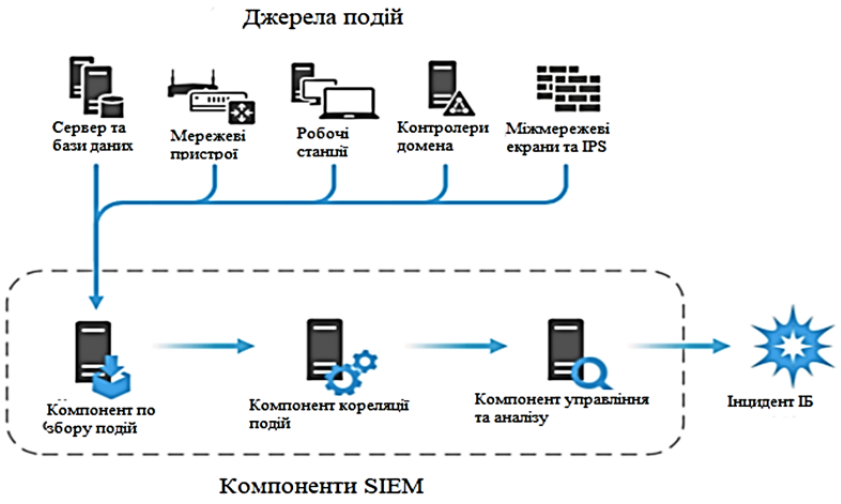

Рис. 1. Основні компоненти SIEM

Функціонування SIEM-системи доцільно деталізувати на рівні: збір лог-файлів і формування необхідних даних від різних джерел; нормалізація даних, яка полягає у приведенні подій з однаковим змістом до загального формату; кореляція подій системи, важливих для забезпечення безпеки, шляхом знаходження зв'язків між ними, наприклад, підбір паролів, зараження шкідливим кодом, аномальна активність в системі, зміна

критичних параметрів системи тощо.; організація зберігання лог-файлів; реагування на інциденти, в тому числі повідомлення про важливі події для інформаційної безпеки; візуалізація інцидентів, формування звітних документів. До типових структурних компонентів відносяться: міжмережевий екран; поштові послуги; бази даних; система виявлення вразливостей; антивірусний захист; локальний портал; файловий сервер [3, 5]

Структурно-функціональна модель системи захисту інформації (СЗІ) включає в себе перелік структурних компонентів обладнання, а також їх функціональні зв'язки і можливості при вирішенні завдання аналізу і захисту інформації (Рис. 2).

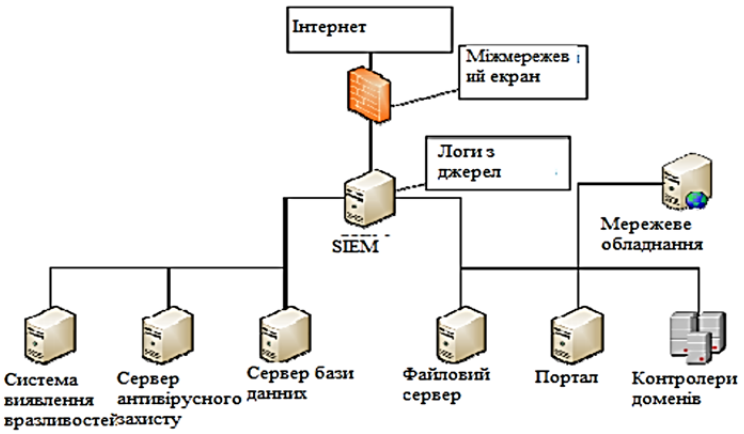

Рис. 2. Структурно-функціональна модель SIEM-системи

Отриману інформацію SIEM аналізує за допомогою правил, що містять набір умов, тригерів, лічильників і сценаріїв дій у відповідь (в сукупності складових Use Cases). SIEM не протидіє зловмисним діям порушників, однак рішення дозволяє отримати найбільш повне уявлення про виникаючі події безпеки [3, 5].

Великі підприємства, холдинги, мульти та транснаціональні компанії різних галузей – основна категорія споживачів SIEM-систем. SIEM дозволяють виявити порушення безпеки серед величезної кількості подій і оперативно відреагувати на виявлені проблеми. Крім того, SIEM-системи при необхідності беруть участь в проведенні аудитів відповідності. Все більша увага приділяється дрібним постачальникам, оскільки організації малого і середнього бізнесу шукають послуги або варіанти надання SIEM для скорочення внутрішніх ресурсів і витрат, необхідних для дотримання вимог безпеки, використовують послуги аутсорсингу [3, 5].

Сьогодні світовий ринок SIEM можна назвати зрілим і конкурентоспроможним. Постачальники в змозі задовольнити основні вимоги будь-якого клієнта, проте залишаються проблеми, пов'язані з виявленням цілеспрямованих атак і порушень в сфері інформаційної безпеки. Ситуація може бути поліпшена завдяки додатковій розвідці загроз, профілізації поведінки користувачів і додатків, ефективній аналітиці. На даний момент спостерігається активне впровадження поведінкової аналітики користувачів і сутностей (User and Entity Behavior Analytics, UEBA), що позиціонується постачальниками як доповнення до SIEM, що володіє більш високою точністю виявлення цілеспрямованих атак [3, 4].

Серед світових лідерів-постачальників SIEM систем можна назвати такі як: SolarWinds Inc. – американська компанія, яка розробляє програмне забезпечення для бізнесу, яке допомагає керувати їх мережами, системами та інфраструктурою інформаційних технологій. Netwrix – це приватна компанія, що займається інформаційною безпекою, яка дає можливість фахівцям з інформаційної безпеки та управління відновлювати контроль над чутливими, регульованими та критично важливими для бізнесу даними, незалежно від місця їх проживання. Rapid7 – лідер в розробці рішення для управління уявленнями і тестування на просування. Допомога полягає в повному представленні безпеки інформаційної інфраструктури [3, 5].

Одними з найбільш популярними SIEM-систем в Україні на теперішній час є [5]:

- QRadar Security Intelligence Platform (виробника IBM), основними перевагами є єдина платформа для всіх дій, які виконуються; гнучка архітектура; велика кількість безкоштовних додатків, контенту і модулів. Широко застосовується до таких видів діяльності: силові структури, банківський сектор, державні організації, торговельно-комерційні підприємства;
- McAfee (від виробника ESM), основні переваги це великий обхват промислових систем управління; інтеграція зі сторонніми технологіями; постійне джерело оновлення даних. Зазначені системи дозволяють в режимі реального часу отримувати події інформаційної безпеки, аналізувати їх та реагувати на виявлені загрози, інциденти та порушення політик інформаційної безпеки;
- HP ArcSight, основні переваги це повний набір можливостей, які дають можливість використання всіх функцій системи; проведення різноманітних аналіз; наявність бази знань загроз; наявність правил і додаткових продуктів. Володіючи розширеними можливостями збагачення даних, комплексна SIEM-платформа ArcSight ESM поєднує в собі функції виявлення і аналізу загроз у реальному часі, управління процесами безпеки і забезпечення відповідності нормативним вимогам. ArcSight ESM виявляє ознаки виникнення інцидентів в реальному часі, дозволяючи швидше на них реагувати. ArcSight ESM виявляє ознаки виникнення інцидентів в реальному часі, дозволяючи швидше на них реагувати. ArcSight ESM покликана стати основою центра моніторингу інформаційної безпеки (SOC).

Висновки. Отже, ІБ сучасних підприємств та бізнес-структур є одним з найважливіших компонентів ІБ, на якому б рівні вона не розглядалась – національному, галузевому, корпоративному або персональному. У сфері забезпечення ІБ систем важливі не тільки окремі рішення, а й механізми генерації нових рішень, що дозволяють працювати і розвиватися в темпі технічного прогресу. Наявність засобів захисту інформації не є гарантією захисту всіх корпоративних ресурсів. Для забезпечення оптимального рівня захисту необхідна система моніторингу ІБ підприємства, якими є SIEM-системи, що спрямовані на моніторинг основних подій і інцидентів ІБ всередині компанії та її діяльності. В умовах сьогодення, сучасні технології програмування інформаційних систем не дозволяють створювати безпомилкові програми, що не підтримує швидкий розвиток засобів забезпечення ІБ. Важливо починати з того, що необхідно створювати надійні системи ІБ із залученням підозрілих компонентів (програм). Це стає цілком можливим, але потребує дотримання певних принципів і контролю за станом захищеності протягом усього життєвого циклу інформаційної системи.

Список використаних джерел

1. Хорошко В.А., Методи і інструмети захисту інформації. / Хорошко В.А., Чекатков А.М. // К.: Юниор, 2003. – С. 504.
2. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – Харків: ХНУРЕ, 2019. – С. 104–105.
3. Моніторинг інформаційної безпеки (SIEM). \\ Режим доступу: https://www.snt.ua/portfolio/it-resheniya/informacionnaya-bezopasnost/monitoring-informacionnoj-bezopasnosti-siem (останнє звернення: 19.03.2023р).
4. Столова, О. В. Методика порівняння ефективності сучасних SIEM-систем / О. В. Столова // XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 25-27 травня 2017 року, м. Київ. – Київ : ВПІ ВПК «ПОЛІТЕХНІКА», 2017. – С. 163-164.
5. Drew Robb, Top SIEM Products [Електронний ресурс]. \\ Режим доступу: https://www.esecurityplanet.com/products/top-siem-products.html (останнє звернення: 19.03.2023р).

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ЗВЄРЄВА В. П.

ПІДХОДИ ДО РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ UNIVERSITY DORM CAMPUS

УДОВИЦЯ О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуті питання розробки програмної платформи University Dorm Campus, як системи управління студентським житлом, описані основні компоненти системи, а саме управління проживанням студентів у гуртожитку, включаючи управління платежами, ремонтом та обслуговуванням, безпекою, спільнотою та комунікацією.

The article discusses the issues of developing the University Dorm Campus software platform as a student housing management system. The main components of the system are described, including the management of students' stay in the dormitory, which includes payment management, repair and maintenance management, security, community and communication

Актуальність. Орієнтоване на користувача проектування University Dorm Campus (UCD) і гнучка методологія розробки є двома важливими підходами до розробки програмного забезпечення, які можна застосувати до проектування та розробки програмної платформи університетського гуртожитку.

Дизайн, орієнтований на користувача, – це підхід до розробки програмного забезпечення, який орієнтований на потреби та цілі користувачів. У контексті програмної платформи кампусу університетського гуртожитку це означає розробку платформи з урахуванням потреб і переваг студентів, адміністраторів та інших зацікавлених сторін. UCD передбачає проведення дослідження користувачів, щоб зрозуміти потреби, цілі та проблемні точки цільових користувачів, а потім ітераційне проектування та тестування програмного забезпечення, щоб переконатися, що воно відповідає цим потребам.

Гнучка розробка – це гнучкий і повторюваний підхід до розробки програмного забезпечення, який наголошує на співпраці, швидкому створенні прототипів і безперервній доставці. У контексті програмної платформи університетського гуртожитку це означає розробку платформи невеликими поетапними етапами з регулярним тестуванням і відгуками від користувачів. Гнучка розробка включає розбиття процесу розробки на менші, більш керовані етапи, а потім визначення пріоритетів і планування завдань на основі відгуків користувачів і мінливих вимог.

Поєднання дизайну, орієнтованого на користувача, і гнучких методологій розробки може допомогти гарантувати, що програмна платформа кампусу університетського гуртожитку розроблена з урахуванням потреб і цілей користувачів і розробляється ефективно та результативно. Залучаючи користувачів протягом усього процесу розробки, платформу можна тестувати та вдосконалювати ітеративно, гарантуючи, що вона відповідає потребам і вподобанням користувачів у міру її розвитку.

Метою статті є опис підходів до розробки програмного забезпечення для університетських гуртожитків та аналізі їх ефективності для досягнення більш високого рівня забезпечення комфорту та безпеки студентів під час їх перебування в гуртожитках.

Об'єктом дослідження є процес розробки програмного забезпечення для університетських гуртожитків.

Предметом дослідження є різні підходи до розробки програмного забезпечення університетських гуртожитків, їх характеристики та ефективність у досягненні мети забезпечення комфорту та безпеки студентів у гуртожитках.

Аналіз попередніх досліджень Одне дослідження, проведене Гуптою та Агарвалом (2020), показало, що програмні платформи кампусу гуртожитків можуть підвищити рівень задоволеності та залучення студентів. Надаючи студентам централізовану платформу для

інформації про житло, події та спілкування, студенти можуть легко отримати доступ до важливої інформації, спілкуватися зі своїми однолітками та брати участь у заходах гуртожитку.

Інше дослідження, проведене Ваном і Джином (2021), виявило, що програмні платформи гуртожитків можуть підвищити ефективність управління університетом. Університети можуть заощадити час і ресурси, оптимізувавши такі завдання з управління житлом, як розподіл кімнат, запити на обслуговування та планування подій. Дослідження також виявило, що програмні платформи гуртожитків можуть підвищити безпеку, дозволяючи університетам контролювати та відстежувати доступ до гуртожитків і заходів.

Виклад основного матеріалу. Програмні платформи університетських гуртожитків – це цифрові рішення, які дозволяють навчальним закладам ефективно керувати повсякденною діяльністю своїх гуртожитків. Ці платформи дозволяють студентам централізовано отримувати доступ до інформації, пов'язаної з житлом, сусідами по кімнаті, приміщеннями, подіями та іншими послугами. У цьому огляді літератури ми обговоримо ключові особливості програмних платформ університетських гуртожитків та їхні переваги для студентів, університетів та інших зацікавлених сторін.

Основні особливості програмних платформ University Dorm Campus складає чотири основні компоненти: підбір сусідів по кімнаті; управління житлом; управління подіями; комунікація; керування платежами. розглянемо їх детально.

Підбір сусідів по кімнаті.

Однією з важливих функцій програмної платформи студентського містечка гуртожитків є інструмент підбору сусідів по кімнаті. Ця функція дозволяє студентам знаходити сумісних сусідів по кімнаті на основі їхніх уподобань та інтересів. Інструменти підбору сусідів по кімнаті часто включають опитування та анкети для оцінки способу життя та звичок студента. Кілька досліджень вивчали ефективність інструментів підбору сусідів по кімнаті для підвищення задоволеності учнів і зменшення конфліктів.

Одне дослідження Рінкуса та Харлоу (2017) показало, що інструменти підбору сусідів по кімнаті можуть покращити якість стосунків із сусідами по кімнаті та зменшити конфлікти. Дослідження показало, що студенти, які користувалися інструментами підбору сусідів по кімнаті, були більш задоволені своїми сусідами по кімнаті та повідомили про менше конфліктів порівняно зі студентами, яким випадково призначали сусідів по кімнаті.

Управління житлом.

Іншою ключовою особливістю програмних платформ гуртожитків є модуль управління житлом. Ця функція дозволяє університетам керувати розподілом житла, зміною кімнат і перевіркою кімнат. Це також дозволяє студентам переглядати свої призначення житла, подавати запити на зміну кімнати та повідомляти про проблеми з обслуговуванням.

Основна мета цієї складової полягає в тому, щоб спростити та забезпечити ефективну організацію житлового простору в кампусі. Для досягнення цієї мети компонент надає такі функції:

1. Реєстрація та адміністрування користувачів: користувачі можуть створювати облікові записи, вводити та змінювати свої персональні дані. Адміністратори житла можуть виконувати функції з контролю доступу та повторення.

2. Бронювання кімнати: Користувачі можуть бронювати кімнати в кампусі відповідно до їх потреб.

3. Управління оплатою: Компонента надає можливість оплати проживання, а також управління платежами.

4. Обслуговування кімнати: Адміністратор може виконувати функції розміщення з управлінням та обслуговуванням кімнати, щоб забезпечити гарні умови для користувачів.

5. Запис пропусків: Користувачі можуть зареєструвати свій в'їзд та виїзд з кампусу.

6. Інформаційні повідомлення: Компонента надає можливість для надсилання інформаційних повідомлень користувачам та адміністраторам кампусу.

Загалом, компонент «Управління житлом» платформи University Dorm Campus дозволяє забезпечити ефективне управління житловим простором у студентському кампусі, забезпечуючи комфортні умови для проживання студентів.

Управління подіями.

Програмні платформи студентського містечка гуртожитків також включають інструменти керування подіями, які дозволяють університетам організовувати та рекламувати події в гуртожитках. Ця функція дозволяє студентам переглядати майбутні події, відповідати на запрошення та отримувати нагадування про події. Кілька досліджень вивчали вплив заходів у гуртожитку на залученість і задоволеність студентів.

Одне дослідження, проведене Норберто та Салвалагліо (2018), виявило, що заходи в гуртожитку можуть підвищити залученість і задоволення студентів. Дослідження виявило, що студенти, які брали участь у заходах у гуртожитку, повідомили про вищий рівень соціальної інтеграції, академічної задоволеності та загальної задоволеності порівняно зі студентами, які не брали участі в заходах у гуртожитку.

Комунікація.

Інструменти комунікації також є важливою особливістю програмних платформ гуртожитків. Ця функція дозволяє студентам спілкуватися один з одним, а також зі своїми постійними радниками (RA) і персоналом університету. Він також надає університетам платформу для надсилання важливих оголошень, сповіщень і сповіщень.

Ефективне спілкування має важливе значення для роботи гуртожитку та задоволеності студентів. Програмні платформи студентського містечка гуртожитку включають комунікаційні засоби, які дозволяють студентам спілкуватися між собою та з персоналом університету. Кілька досліджень вивчали вплив засобів спілкування на задоволеність і залученість студентів.

Одне дослідження Плурда та Ренна (2019) виявило, що інструменти спілкування можуть покращити задоволеність і залученість студентів. Дослідження показало, що студенти, які використовували засоби спілкування для спілкування зі своїми однолітками та співробітниками університету, повідомили про вищий рівень задоволеності та залученості порівняно зі студентами, які не використовували засоби спілкування.

Програмна платформа спільноти та комунікації для гуртожитків складається з таких функцій:

1. Система повідомлень – програмна платформа може допомогти студентам і персоналу гуртожитку взаємодіяти через систему повідомлень. Це може включати повідомлення про надходження пошти, оголошення про події та активності, оголошення про ремонт тощо. Такі повідомлення можуть бути надіслані студентам через мобільний додаток, електронну пошту, SMS-повідомлення тощо.

2. Спільнота – програмна платформа може допомогти студентам створювати та приєднуватися до спільнот, де вони можуть обговорювати інші теми, знати та здобувати допомогу від інших студентів. У спільноті можуть бути створені різні тематичні групи, такі як групи для обговорення активностей, спорту, культурних заходів тощо. У програмній платформі також можуть бути функції для створення подій та запрошення членів спільноти.

3. Запитання та відповіді – програмна платформа має функцію для запитань та відповідей, де студенти можуть поставити питання персоналу гуртожитку та отримувати відповіді від них. Це може бути корисно для отримання інформації про графік роботи, правила гуртожитку, процедури оформлення тощо.

4. Дошка оголошень – програмна платформа має дошку оголошень, де студенти можуть отримувати оновлення та повідомлення від персоналу гуртожитку. Це може включати оголошення про плани ремонту, інформацію про важливі дати та події, оголошення про вакансії або можливості волонтерства, а також іншу корисну інформацію.

5. Розклади – програмна платформа може мати розклади для різних подій та послуг, таких як години роботи їдальні, розклад занять спортивний зал, розклад транспорту до університету та інше.

6. Замовлення послуг – програмна платформа може мати функції для замовлення різних послуг, таких як замовлення прибирання кімнати, заявки на ремонт чи інші запити до персоналу гуртожитку.

Керування платіжками.

Програмна платформа University Dorm Campus може допомогти гуртожитковому персоналу відстежувати та обробляти різні типи платежів, такі як квартирна плата, комунальні послуги та додаткові послуги, наприклад послуги з пральні або внутріш-ньогуртожиткової кафетерії.

Програмна платформа керування платежами для гуртожитків має тикі функції:

1. Створення рахунків – програмна платформа може автоматично створювати рахунки для студентів на основі їхніх договорів оренди кімнати. Рахунки можуть бути різними типами платежів, таких як плата за кімнату, комунальні послуги та додаткові послуги.

2. Обробка платежів – програмна платформа може допомогти персоналу гуртожитку обробляти різні типи платежів, такі як готові та безготівкові платежі, онлайн-платежі та платежі з банківських карт.

3. Відстеження платежів – програмна платформа може відстежувати всі платежі, зроблені студентами, та показувати статус кожного платежу. Відстеження платежів може допомогти персоналу гуртожитку легко відслідковувати заборгованість студентів та вирішувати проблеми з платежами вчасно.

4. Генерація звітів – програмна платформа може формувати звіти про платежі, такі як звіти про заборгованість студентів, звіти про витрати на комунальні послуги та інші фінансові зв’язки

Керування ремонтом та обслуговуванням.

Програмна платформа University Dorm Campus може допомогти гуртожитковому персоналу відстежити замовлення на ремонт, провести профілактичний ремонт та забез-печити планову технічну підтримку всього гуртожитку.

Програмна платформа управління ремонтом та обслуговуванням гуртожитків має наступні функції:

1. Планування ремонту – програмна платформа може допомогти персоналу гуртожитку спланувати ремонтні роботи в кімнатах та спільних приміщеннях. Це може включати планування часу та дати ремонтних робіт, визначення потреб у матеріалах та інструментах, а також розподіл завдань між працівниками.

2. Обробка заявок на ремонт – програмна платформа може допомогти студентам відправити заявки на ремонт або послугу до персоналу гуртожитку. Після отримання заявки програмна платформа може автоматично створити ремонтне замовлення та надіслати його відповідному працівнику.

3. Стеження за станом ремонту – програмна платформа може відстежувати стан ремонтних замовлень та показувати, на якому етапі знаходиться кожне замовлення. Це дозволяє персоналу гуртожитку відстежувати стан ремонтів та забезпечити їх виконання вчасно.

4. Інвентаризація – програмна платформа може допомогти персоналу гуртожитку відстежувати та контролювати запаси матеріалів та інструментів для ремонту. Це може допомогти гарантувати кількість матеріалів та інструментів для виконання ремонтних робіт.

5. Генерація звіту – формування звітів про проведення ремонтних робіт

Керування безпекою – програмна платформа може допомогти гуртожитковому персоналу відстежувати безпеку в гуртожитку, включаючи контроль доступу, моніторинг безпеки та запобігання порушенню правил.

Програмна платформа керування безпекою для гуртожитків має такі функції:

1. Моніторинг доступу – програмна платформа може допомогти персоналу гуртожитку відслідковувати доступ студентів до різних зон гуртожитку, включаючи вхідні

двері, спа, спільні приміщення тощо. Це може забезпечити безпеку для студентів, забезпечуючи, що небажані особи не мають доступу до зони, де вони не повинні перебувати.

2. Система відеоспостереження – програмна платформа може допомогти персоналу гуртожитку встановити та керувати системою відеоспостереження в гуртожитку. Це може забезпечити високий рівень безпеки для студентів, забезпечуючи, що будь-які небажані події можуть бути відстежені та зафіксовані.

3. Попередження про небезпеку – програмна платформа може допомогти персоналу гуртожитку вивести студентів про небезпеку, яка може виникнути в гуртожитку. Це може включати попередження про пожежі, повені, насильство, крадіжки тощо. Такі повідомлення можуть бути надіслані студентам через мобільний додаток, електронну пошту, SMS-повідомлення тощо

Узагальнюючи, програмна платформа University Dorm Campus надає студентам різні корисні функції для управління їхнім проживанням у гуртожитку, включаючи управління платежами, ремонтом та обслуговуванням, безпекою, спільнотою та комунікацією. Ці функції можуть забезпечити студентам зручність та ефективність в їхньому повсюдному житті, а також зменшити навантаження на персональну гуртожитку.

Переваги програмних платформ University Dorm Campus:

- Покращений досвід студентів: програмні платформи кампусу гуртожитку університету покращують досвід студентів, надаючи централізоване місце для інформації про житло, події та спілкування. Це дозволяє студентам легко отримувати доступ до інформації, спілкуватися зі своїми однолітками та співробітниками університету та брати участь у заходах гуртожитку.
- Підвищення ефективності: програмні платформи кампусу гуртожитку спрощують завдання управління житлом, наприклад розподіл кімнат і запити на технічне обслуговування, що призводить до підвищення ефективності для університетів і персоналу.
- Покращена безпека та безпека: програмні платформи гуртожитків також підвищують безпеку, дозволяючи університетам контролювати та відстежувати, хто має доступ до гуртожитків та подій.
- Збільшення залучення студентів: програмні платформи студентського містечка гуртожитків сприяють залученню студентів, надаючи студентам можливість спілкуватися один з одним і брати участь у заходах гуртожитку. Це призводить до більш активної та залученої студентської спільноти.

На ринку є кілька типів програмних платформ університетських гуртожитків, включаючи системи управління студентським житлом, платформи для спілкування та співпраці, системи безпеки та безпеки, а також віртуальні тури та орієнтації.

Системи управління студентським житлом надають університетам комплексне рішення для управління студентським житлом, включаючи розподіл кімнат, логістику вселення та виїзду, а також запити на обслуговування. Ці системи також надають студентам онлайн-доступ до інформації про житло, такої як орендна плата, переваги сусідів по кімнаті та житлова політика.

Платформи для спілкування та співпраці дозволяють студентам спілкуватися один з одним та з університетським персоналом через різні канали, такі як обмін повідомленнями, форуми та соціальні мережі. Ці платформи також дозволяють легко планувати зустрічі та події та забезпечують централізоване розташування для обміну важливими документами та оголошеннями.

Системи безпеки та безпеки використовують передові технології, такі як відеоспостереження, контроль доступу та системи оповіщення про надзвичайні ситуації, щоб забезпечити безпеку студентів і персоналу в кампусі. Ці системи також забезпечують моніторинг у реальному часі та можливості звітування для команд безпеки кампусу.

Віртуальні тури та орієнтації пропонують майбутнім і майбутнім студентам віртуальний досвід кампусу, включаючи гуртожиток та інші об’єкти. Ці платформи

дозволяють студентам досліджувати кампус, не виходячи з власного дому, і дають їм змогу краще зрозуміти середовище та культуру кампусу.

Переваги та недоліки:

- Програмні платформи студентського містечка університетського гуртожитку пропонують кілька переваг, зокрема покращене спілкування та співпрацю між студентами та персоналом, покращену безпеку та спрощені адміністративні процеси. Ці платформи також сприяють залученню студентів і надають студентам більш зручний і ефективний спосіб доступу до ресурсів кампусу.
- Однак ці платформи також мають деякі недоліки. Наприклад, деякі учні можуть віддавати перевагу очній взаємодії над онлайн-спілкуванням, і залежність від технологій може створювати додаткові перешкоди для студентів, які не мають доступу до необхідних пристроїв або підключення до Інтернету.

Вплив на університетські містечка:

- Програмні платформи кампусу гуртожитку університету мали значний вплив на життя кампусу. Ці платформи покращили загальний досвід студентів, від процесу подачі заявки до дня заїзду та далі. Вони також допомогли університетам краще керувати інвентарем житла та забезпечити безпеку своїх студентів.
- Крім того, ці платформи надали університетам цінні дані, такі як показники залученості студентів і рівень заповнюваності, які можуть стати основою для прийняття стратегічних рішень і допомогти оптимізувати роботу кампусу.

Висновок. Програмні платформи кампусу гуртожитку університету стали основними інструментами для сучасних університетів. Вони пропонують низку функцій і переваг, які покращують залучення студентів, безпеку та ефективність навчання та проживання.

Хоча ці платформи мають певні недоліки, загальний вплив був позитивним, і університети, які прийняли ці технології, краще оснащені для задоволення потреб своїх студентів і співробітників. У той час як університети продовжують використовувати цифрові рішення для управління діяльністю своїх студентських містечок, програмні платформи студентських містечок гуртожитків продовжуватимуть відігравати важливу роль у забезпеченні студентів безпечним, зручним і привабливим життям.

Список використаних джерел

1. С. О. Цибульник, К. С. Барандич. Технології розроблення програмного забезпечення : Підручник. – Київю; КПІ ім. Ігоря Сікорського 2022, – 270 с.
2. Роберт С. Мартін. Чистий код: : створення, аналіз і рефакторинг. – Харків.: Книжковий дім, 2022. – 464 с.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
РЗАЄВОЇ С. Л.

АНАЛІЗ ЗАХИСТУ ВИБОРЧОЇ СИСТЕМИ: ОСНОВНІ ВРАЗЛИВОСТІ ТА РИЗИКИ

ФЕСЮК А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У цій статті проведено аналіз захисту виборчої системи з метою визначення основних вразливостей та ризиків, пов'язаних з її функціонуванням. Розглянуто різні аспекти безпеки виборів, включаючи кібербезпеку, захист від зловживань та маніпуляцій з результатами голосування. В результаті дослідження встановлено, що виборча система є вразливою до різноманітних атак, і необхідно приділяти більше уваги заходам забезпечення її безпеки.

This article analyzes the security of the electoral system in order to identify the main vulnerabilities and risks associated with its operation. Various aspects of election security are considered, including cybersecurity, protection against abuse, and manipulation of voting results. As a result of the study, it was found that the electoral system is vulnerable to various attacks and that more attention needs to be paid to measures to ensure its security.

Актуальність. В сучасному світі, коли більшість політичних процесів відбуваються через вибори, безпека виборчих систем є критично важливою. Адже злочинці та зловживання можуть стати загрозою для цих систем.

Виборчі системи є одними з найважливіших елементів політичної стабільності та демократії в будь-якій цивілізованій країні, в тому числі, в Україні. Ці системи мають на меті забезпечити чесні та вільні вибори шляхом забезпечення безпеки голосування та збору голосів. Однак, в зв'язку зі зростаючим використанням технологій у виборчих системах, з'являється більше можливостей для порушень безпеки та злочинних дій, які можуть підривати довіру громадян до виборчої системи та її результатів.

Ця стаття присвячена аналізу основних вразливостей та ризиків, пов'язаних з захистом виборчої системи, з метою забезпечення надійного та безпечного виборчого процесу.

Метою статті є розкриття основних вразливостей та ризиків, що відносяться до захисту виборчої системи, а також розгляд можливих заходів щодо забезпечення безпеки та надійності виборчих процесів.

Об'єктом дослідження є виборча система та її компоненти, які відповідають за захист від можливих загроз та атак.

Предметом дослідження є основні вразливості та ризики, що можуть знайти вираження у виборчій системі, а також способи забезпечення безпеки та надійності виборчого процесу. Дослідження включає аналіз загроз, які можуть виникнути від різних ворогів, таких як хакери, кіберзлочинці тощо, а також оцінку ризиків, які вони можуть створити для виборчої системи.

Аналіз попередніх досліджень. Попередні дослідження в галузі захисту виборчих систем науковцями: В. Венгер, М. Ільницький, О. Токар-Остапенко, І. Павленко, Г. Задорожня, О. Ільницький – вказують на те, що технічні та організаційні вразливості можуть призвести до порушення конфіденційності, цілісності та доступності виборчих даних. Ці вразливості можуть бути використані для маніпулювання результатами виборів та злочинних дій, таких як крадіжка особистої інформації виборців тощо.

Огляд заходів забезпечення безпеки виборчих систем показує, що технічні, організаційні та юридичні заходи можуть бути використані для забезпечення безпеки виборчих систем. Такі заходи включають аудит виборчих систем, використання шифрування та контроль доступу до виборчих даних.

Виклад основного матеріалу. Якщо погянути на систему в цілому, то електронна виборча система – це система, яка використовується для збору та обробки голосів на виборах, за допомогою електронних пристроїв. Принцип роботи електронної виборчої системи полягає в наступних етапах:

- Реєстрація виборців: відбувається перед початком виборів. Виборці реєструються у виборчій системі, де їхні особисті дані перевіряються та зберігаються в базі даних.
- Голосування: виборці голосують за допомогою електронних пристроїв, які можуть бути різних типів – наприклад, комп'ютери або спеціальні термінали. Зазвичай виборці отримують картки або ключі для входу до системи та голосують, натискаючи на кнопки на екрані пристрою.
- Обробка голосів: виборча система автоматично підраховує голоси та зберігає їх в електронній формі в базі даних. Зазвичай це здійснюється за допомогою спеціального програмного забезпечення, яке встановлене на електронних пристроях. Результати голосування можуть бути показані на екрані пристрою або надруковані.
- Перевірка результатів: результати голосування можуть бути перевірені за допомогою виборчого комітету або незалежної аудиторської фірми, яка перевірить, чи були зібрані та оброблені всі голоси правильно.

Електронні виборчі системи мають свої переваги та недоліки. Основною перевагою є швидкість та точність обробки голосів, що дозволяє оголошувати результати виборів набагато швидше, ніж у випадку з традиційними паперовими голосувальними бюлетенями. Також електронні виборчі системи можуть бути менш витратними та екологічно чистими, тому що не потребують великої кількості паперус на бюлетені для голосування. [1]

Однак, електронні виборчі системи мають свої недоліки, зокрема, можуть бути вразливими до кібератак та викрадення даних, що може призвести до порушення виборчого процесу та несправедливого розподілу голосів. Також можуть виникати проблеми зі стабільністю системи та несправностями обладнання. Тому важливо використовувати ефективні методи захисту, а також проводити ретельний аудит електронної виборчої системи, щоб забезпечити її безпеку та надійність.

Виборчі системи можуть бути вразливі як через технічні проблеми, так і через людські помилки. Основні вразливості виборчих систем можуть бути наступними:

Технічні вразливості:

- Хакерські атаки – виборчі системи можуть піддаватися хакерським атакам, які можуть привести до порушення або зміни результатів голосування. Хакерські атаки можуть бути проведені через інтернет, на місці або через підключення до мережі виборчої системи.
- Віруси та зловмисний код – виборчі системи можуть бути вражені вірусними атаками та упровадженню зловмисного коду, який може порушити результати голосування або змінити їх.
- Несправність обладнання – несправність обладнання може призвести до втрати даних або знищення їх.
- Невідповідність стандартам безпеки – виборчі системи можуть піддаютися атакам через невідповідність стандартам безпеки.

Людські вразливості:

- Соціальна інженерія – атаки соціальної інженерії можуть бути використані для впливу на результати голосування шляхом зміни волевиявлення виборців або завдання іншої шкоди.
- Виборче шахрайство – виборче шахрайство може бути використано для впливу на результати голосування, включаючи підроблення голосів, зміну результатів голосування та інші маніпуляції.
- Інші людські помилки – інші людські помилки, такі як помилки введення даних або неправильне використання обладнання, можуть призвести до порушення результатів голосування.

Усі ці вразливості можуть бути небезпечними для правильного проведення голосування та порушити демократичний процес в країні. Нижче наведено деякі заходи, які можуть бути вжиті для зменшення ризиків вразливостей виборчих систем:

- Забезпечення захисту від хакерських атак і вірусних програм шляхом використання найновіших технологій та протоколів безпеки, включаючи шифрування, мережеві заходи безпеки, фірмовий та апаратний захист.
- Використання стійких паролів, двофакторної автентифікації, а також використання CAPTCHA для доступу до системи.
- Забезпечення фізичної безпеки виборчої системи, що включає обмеження доступу до обладнання та забезпечення контролю доступу до серверів та інших пристроїв.
- Проведення регулярних тестів на проникнення для виявлення можливих вразливостей та подальшого вдосконалення системи.
- Забезпечення надійності системи для зберігання та передачі голосів шляхом використання шифрування та інших заходів захисту.
- Навчання персоналу та волонтерів, які займаються обслуговуванням виборчих систем, щоб вони були усвідомлені та обізнані з технічними вразливостями та можливими загрозами виборчого процесу.
- Проведення аудиту результатів голосування для підтвердження їх правильності та уникнення можливих помилок.
- Встановлення та дотримання прозорих та стандартизованих процедур голосування, щоб запобігти можливому виборчому шахрайству та іншим формам маніпуляцій.

Загалом, зменшення вразливостей виборчих систем потребує інтегрованого підходу, що охоплює як технічні, так і людські аспекти. Необхідно забезпечити безпеку системи від зовнішніх і внутрішніх загроз, а також навчити всіх учасників виборчого процесу користуватися системою безпеки. Для цього необхідно вжити заходів на кожному етапі виборчого процесу – від розробки системи до проведення голосування та підрахунку результатів. Тільки в такому разі можна забезпечити довіру до виборчої системи та результатів голосування.

Наприклад, досягнення прозорості та довіри до виборчих систем може бути досягнуто за допомогою наступних заходів:

- Розробка та публікація документів, які описують принципи та процедури роботи виборчих систем, а також їх використання.
- Встановлення міжнародних стандартів та протоколів щодо безпеки та дотримання їх під час проведення виборів.
- Проведення досліджень та тестувань виборчих систем з метою виявлення та усунення можливих вразливостей.
- Публікація результатів голосування у відкритому доступі, що дозволяє громадськості перевіряти та аналізувати їх.
- Визначення відповідальних органів та осіб за безпеку виборчих систем та їх дії в разі виявлення вразливостей.
- Забезпечення навчання всіх учасників.

Ризики, пов’язані з вразливостями виборчих систем, можуть бути дуже серйозними та наслідки від їх реалізації можуть бути дуже шкідливими для виборців, кандидатів та результатів виборів. Давайте розглянемо кожну з цих категорій окремо:

Ризики для виборців:

- Крадіжка особистої інформації (імені, адреси, дати народження) та її використання в шахрайських схемах;
- Можливість втручання у виборчий процес та крадіжки голосів;
- Здійснення атак на виборчі системи з метою впливу на результати виборів;
- Використання соціальної інженерії та масового обману з метою впливу на результати виборів;

- Зниження довіри до виборчих систем та зменшення участі виборців через відчуття небезпеки під час голосування.

Ризики для результатів виборів:

- Можливість зламу виборчої системи та вплив на результати голосування;
- Використання соціальної інженерії та масового обману з метою впливу на результати голосування;
- Недостатня безпека виборчих систем може привести до підозри у фальсифікації результатів та зниження довіри до виборчих процесів;
- Неправильне зберігання та обробка даних може призвести до помилок та змін у результаті голосування;
- Відсутність адекватного контролю та аудиту може спричинити помилки та зловживання.

Загалом, вразливості виборчих систем можуть призвести до підозри у фальсифікації результатів виборів та зниження довіри до демократичного процесу голосування. Це може вплинути на легітимність влади та підірвати демократію. Тому, щоб запобігти цим ризикам, важливо забезпечити безпеку виборчих систем, зберігання та обробку даних, контроль та аудит процесу голосування, а також підвищення культури виборців та кандидатів у питаннях кібербезпеки. [1]

Забезпечення безпеки виборчих систем є дуже важливим завданням, особливо в контексті забезпечення права на вільні та справедливі вибори. З метою забезпечення безпеки виборчих систем застосовуються технічні, організаційні та юридичні заходи:

Технічні заходи:

- Захист від вірусів та зломів: системи повинні бути захищені від вірусів та зломів шляхом встановлення антивірусного програмного забезпечення, застосування програмного забезпечення для виявлення та запобігання злому, і використання захищеного з’єднання виборчого комп’ютерного обладнання.
- Контроль доступу: системи повинні мати ефективні засоби контролю доступу до даних та функцій системи. Наприклад, електронна система може використовувати паролі, біометричні дані або токени безпеки для забезпечення безпеки даних виборчої системи та виборця.
- Контроль та шифрування каналів передачі даних у процесі голосування, автентифікації та зарахування голосу.
- Контроль та створення дублюючих каналів зв’язку у випадку зникнення комутації, інтернету, компрометації вузла передачі чи каналу передачі, для відновлення і продовження роботи електронної виборчої системи.
- Захист від DDoS атак: для запобігання DDoS атак системи повинні мати ефективні засоби захисту, такі як використання спеціального програмного забезпечення або хмарних рішень.

Організаційні заходи:

- Організація навчання та підготовки: працівники, які мають пряме стосування до виборчої системи, повинні проходити регулярні курси навчання та підготовки з питань безпеки виборів.
- Аудит безпеки: системи повинні піддаватися аудиту безпеки для виявлення слабких місць та вразливостей.
- Мають бути описані протоколи прийняття рішень, щодо ситуацій з втручанням у електронну систему голосування, виявлення порушень та способи і засоби їх усунення.
- Захист від внутрішнього злочинця: виборчі системи повинні бути захищені від внутрішніх злочинців, тому необхідно розробити процедури контролю за доступом до системи.

Юридичні заходи, пов’язані з забезпеченням безпеки виборчих систем, включають:

- Законодавче регулювання: український законодавчий акт «Про вибори народних депутатів України» містить вимоги щодо захисту виборчих систем від несанкціонованого доступу та забезпечення захисту виборчих даних від порушень.
- Встановлення відповідальності: відповідальність за порушення безпеки виборчих систем повинна бути встановлена та передбачена згідно з законодавством України.
- Захист персональних даних: повинні бути встановлені правила захисту персональних даних, зібраних в рамках виборчого процесу, від несанкціонованого доступу та використання.
- Міжнародні стандарти: Україна має дотримуватися міжнародних стандартів забезпечення безпеки виборчих систем, таких як Кодекс практики з виборчих процесів у Європі.
- Моніторинг та контроль: урядові та недержавні організації здійснюють моніторинг та контроль за виборчим процесом з метою запобігання можливих порушень. [2]

Висновки. Безпека виборчих систем має бути забезпечена комплексним підходом, що включає технічні, організаційні та юридичні заходи. Дотримання цих заходів забезпечить довіру громадськості до виборчого процесу та збереження демократичних цінностей.

Забезпечення безпеки виборчих систем є надзвичайно важливим завданням для забезпечення демократичного процесу в країні. Огляд літератури показав, що вразливості електронних виборчих систем можуть бути технічними та людськими, а ризики можуть містити загрозу для виборців, кандидатів та результатів виборів. Для захисту виборчих систем можуть бути використані технічні, організаційні та юридичні заходи. Зокрема, до технічних заходів можуть належати захист мережі, захист бази даних, використання шифрування каналів передачі даних, організація контролю доступу до виборчих даних. До організаційних заходів можуть належати навчання та підготовка персоналу з питань кібербезпеки, аудит виборчих систем та підвищення уваги до соціального інжинірингу. До юридичних заходів можуть належати законодавчі акти, які встановлюють вимоги до захисту виборчих систем та кримінальні санкції за порушення цих вимог.

Результати дослідження показують, що захист виборчих систем є важливим завданням для забезпечення демократичного процесу в країні. Заходи забезпечення безпеки повинні бути комплексними та охоплювати як технічні, так і організаційні та юридичні заходи. Підвищення уваги до захисту виборчих систем та навчання персоналу з питань кібербезпеки можуть допомогти зменшити ризики порушення безпеки виборчих систем. Законодавчі акти, які встановлюють вимоги до захисту виборчих систем та кримінальні санкції за їхнє порушення, можуть забезпечити правовий захист для виборців, кандидатів та результатів виборів.

Список використаних джерел

1. Geneva internet voting system // Режим доступу: https://www.coe.int/t/dgap/goodgovernance/activities/e-voting/evoting_documentation/passport_evoting2010.pdf
2. Стогова О.В., Мурач Д.В. Електронне голосування: проблеми та перспективи запровадження // Юридичний науковий електронний журнал. 2021. № 3. С. 38-41. // Режим доступу: https://essuir.sumdu.edu.ua/handle/123456789/86308

Робота виконана під науковим керівництвом старшого викладача
ШЕСТАКА Я. І.

МЕТОДИ ЗАХИСТУ ЛОКАЛЬНИХ МЕРЕЖ ВІД КІБЕРАТАК

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

У статті розглянуто основні методи захисту локальних мереж від кібератак, які пов'язані зі зростанням кіберзлочинності. Описано різні підходи до захисту локальних мереж, такі як використання брандмауерів, вірусних сканерів, систем виявлення вторгнень, їх принцип дій, переваги та недоліки. Доведено комплексний підхід до захисту локальних мереж та зменшення ризику кібератак.

The article examines methods of protecting local area networks from cyberattacks, which are associated with the growth of cybercrime. Specified various approaches to the protection of local area networks, such as firewalls, virus scanners, intrusion detection systems. Described their principles, advantages and disadvantages. A comprehensive approach to protecting local networks and reducing the risk of a cyberattack has been proven.

Актуальність. В сучасну цифрову епоху все більше підприємств, організацій і окремих осіб покладаються на локальні мережі (LAN) для підключення пристроїв і обміну інформацією. Зі збільшенням частоти та складності кібератак захист локальних мереж став критичною проблемою для всіх, хто використовує ці мережі. Локальні мережі можуть бути вразливими до різних типів кібератак, включаючи зараження зловмисним програмним забезпеченням, витік даних і атаки на відмову в обслуговуванні, що може завдати значної фінансової та репутаційної шкоди. Тому розуміння та впровадження ефективних методів захисту від кібератак має вирішальне значення для захисту даних, підтримки безвідмовної роботи локальної мережі.

Кіберзлочинці стають все більш витонченими та використовують різноманітні методи та техніки, щоб отримати доступ до локальних мереж та викрасти конфіденційну інформацію або завдати шкоди підприємств. У зв'язку з цим, питання захисту мереж стає все важливішим для бізнесу та інших підприємств. Важливо мати ефективні методи захисту, які дозволяють попереджувати та виявляти кібератаки, а також зменшувати ризики порушення безпеки мережі.

Метою статті є дослідження методів та стратегій, які можна використовувати для захисту локальних мереж від кібератак та надання практичних рекомендацій з їх застосуванням для різних типів мереж та бізнес-потреб.

Об'єктом дослідження є визначення практичних аспектів використання методів та технологій, таких як вибір та налаштування відповідних захисних засобів, аналіз та ідентифікація загроз безпеці мережі, управління ризиками та розвиток стратегій захисту мережі від кібератак.

Предмет дослідження − локальні мережі, провідні та бездротові мережі, їх характеристики та особливості, що можуть впливати на вибір та застосування певних методів захисту.

Аналіз попередніх досліджень: Закордонні науковці, такі як С. Джаджодія, Р. Пувендран, А. Ставру, А. Р. Прасад, К. Нойман, Л. Чен та інші, присвятили свої дослідження локальним мережам, методам та стратегіям захисту від кібератак.

Виклад основного матеріалу. У наш час кожна комп'ютерна система вразлива до атак, тому підприємствам важливо впровадити надійні заходи безпеки, які можуть захистити їх мережеву систему та ресурси. Щоб протистояти атакам, що походять з мережі або за її межами, адміністратори повинні ретельно вибирати та розгортати відповідні технології безпеки. Оскільки доступна велика кількість технологій безпеки, дуже важливо вибрати та розгорнути їх у спосіб, який узгоджується із загальними цілями та політикою безпеки підприємства.

Підприємства визначають свої стратегії безпеки на основі своїх бізнес-цілей. Ці стратегії відображаються в політиці безпеки підприємства, яка являє собою набір правил, яких повинні дотримуватися співробітники та користувачі для забезпечення безпеки інформаційних і технологічних ресурсів організації. Згідно із запитом на коментарі (RFC) 2196, політика безпеки − це офіційна заява про правила, які регулюють поведінку людей, які мають доступ до технологій та інформації організації. Політика має чітко визначати вимоги щодо захисту технологій та інформаційних активів підприємства та окреслювати процедури виконання цих вимог.

Перед створенням політики безпеки слід розробити план безпеки. Цей план має визначити, що потрібно захистити та від яких загроз. Проведення аналізу ризиків є поширеним способом досягнення цього. Аналіз ризиків визначить, які дії допустимі, а які ні, і допоможе визначити, як і де будуть вирішуватися питання безпеки. Ефективна політика безпеки має охоплювати різноманітні сфери, включаючи доступ користувачів, віддалений доступ, підзвітність, автентифікацію, обробку інцидентів, доступ до Інтернету, використання електронної пошти, фізичну безпеку, обслуговування та звітування про порушення.

Політика безпеки не повинна бути надто обмежувальною, а натомість сприяти використанню ресурсів, зберігаючи певний рівень обмежень. Як правило, відповідальність за розробку політики безпеки покладається на адміністраторів мережі та вищих менеджерів підприємств.

Оскільки підприємства зазнають частих змін щодо технологій і бізнес-стратегій, ризики для їхніх ресурсів і активів також змінюються з часом. Тому вкрай важливо регулярно переглядати та вносити правки в документи політики безпеки, щоб не відставати від мінливих потреб організації в безпеці.

Сучасні системи мережевого зв’язку та спільного використання вимагають ефективних заходів безпеки, які відповідають загальній політиці безпеки підприємства, щоб захистити її мережеві активи та ресурси. Існує кілька доступних технологій безпеки для побудови системи безпеки, але вибір відповідної технології та визначення її оптимального розміщення в мережі залишається основною проблемою для адміністраторів. Доступні варіанти техніки та їх розміщення в охоронній зоні показанв на Рис. 1 [1].

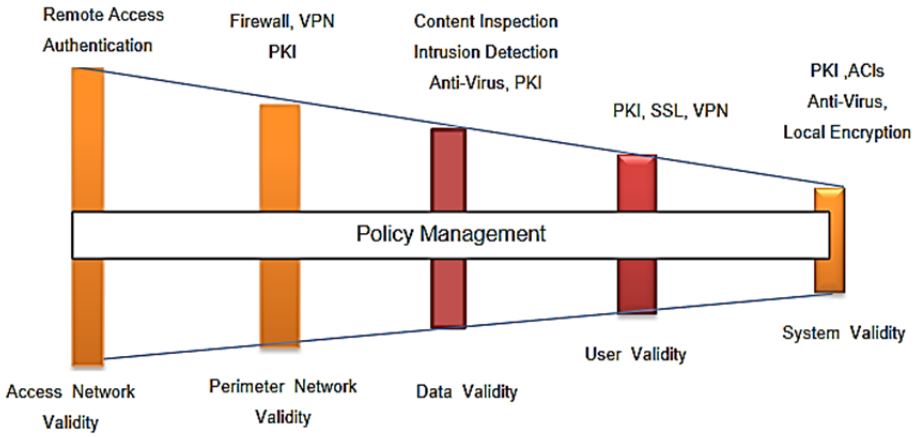

Рис. 1. Розміщення заходів безпеки на охоронній зоні

Захист від неавторизованого віддаленого доступу до мережевого ресурсу досягається за допомогою розгортання технологій автентифікації віддаленого доступу, таких як RADIUS (для захисту комутованих з’єднань), шифрування (для з’єднань по виділеній лінії) та IPsec (для з’єднання через публічну мережу). Щоб захистити пристрої рівня розподілу, зазвичай розгортають один або кілька брандмауерів і зону безпеки.

Після того, як користувач отримав доступ до мережевих ресурсів, важливо перевірити вхідні та вихідні дані на наявність шкідливих об'єктів, таких як віруси, які можуть порушити нормальне функціонування комп'ютерної системи. Одним із способів досягти цього є розгортання інспекції вмісту, виявлення вторгнень, захисту від вірусів або технологій PKI (Pre-shared Key Information). Крім того, важливо захистити систему обслуговування додатків за допомогою списків контролю доступу (ACL), шифрування даних і антивірусних програм.

Безпека Інтернет-протоколу (IPsec) − це структура безпеки, яка базується на відкритому стандарті, розробленому Інженерною робочою групою Інтернету (IETF) для забезпечення безпечного зв'язку через IP-мережі. IPsec вважається найбільш бажаною технологією для захисту наскрізного зв'язку через IP-мережі, оскільки вона забезпечує захист для протоколів і програм вищого рівня. Основною метою IPsec є забезпечення конфіденційності, цілісності та автентичності передачі даних, а також сумісності пристроїв. Для виконання цих завдань IPsec використовує два протоколи, відомі як Authentication Header (AH) і Encapsulating Security Payload (ESP), а також стандартні механізми узгодження ключів і керування.

Протокол заголовка автентифікації (AH) призначений для забезпечення цілісності даних для всієї IP-дейтаграми, що робить його ефективним у запобіганні IP-спуфінгу та викраденню сесії. З іншого боку, протокол Encapsulating Security Payload (ESP) призначений для забезпечення як цілісності даних, так і конфіденційності шляхом шифрування IP-пакетів за допомогою загального секретного ключа.

IPsec включає обмін ключами в Інтернеті (IKE), а також протокол керування ключами асоціації безпеки в Інтернеті (ISAKMP)/Oakley для обробки генерації та керування ключами, а також для встановлення асоціацій безпеки (SA). Асоціація безпеки − це угода між одноранговими пристроями, яка визначає, як відбувається обмін даними між ними. Крім того, IPsec працює в двох режимах: тунельний і транспортний. У режимі тунелю IPsec розгортається між двома шлюзами, а вихідний IP-пакет шифрується та стає корисним навантаженням нового IP-пакета. З іншого боку, у транспортному режимі IPsec використовується між хостами, а вихідна інформація заголовка (джерело та адресат) не шифрується, що робить її видимою для проміжних мережевих пристроїв.

Мережа Ethernet може бути розділена на кілька сегментів IP-маршрутизатором, що призводить до створення окремих широкомовних доменів. Це усуває можливість атак на основі ARP, STP, VLAN і таблиці MAC-адрес між цими сегментами. Однак однакові атаки можуть відбуватися в кожному сегменті, якщо замість кожного комутатора не використовується багатопортовий маршрутизатор.

Розділивши мережу Ethernet на кілька сегментів за допомогою IP-маршрутизатора, трафік між сегментами не можна перехопити або перенаправити для атаки Man-in-the-Middle (MITM). На маршрутизаторі MAC-заголовки Ethernet видаляються, а трафік спрямовується на основі IP-адрес і таблиці IP-адрес маршрутизатора. Протоколи площини керування Ethernet, такі як ARP і STP, блокуються маршрутизатором від проходження між сегментами. Якщо маршрутизатор налаштовано правильно, то він підвищує рівень безпеки, обмежуючи атаки DHCP одним сегментом та ігноруючи повідомлення протоколу маршрутизації від сегментів Ethernet.

Щоб почати атаку, зловмиснику спочатку потрібен доступ. Отже, обмеження доступу до мережі або застосування протоколів автентифікації можуть утримати ненадійних осіб на відстані. Крім того, навіть довіреним особам можна обмежити можливості доступу для подальшого пом'якшення потенційних загроз. Тож можна запропонувати декілька методів для обмеження доступу.

1. Фізичний захист мережі. Мережеве обладнання можна закріпити в шафах і стійках що замикаються, а дроти можна встановити всередині стін, щоб запобігти несанкціонованому доступу. Тим не менш, оскільки доступ є важливим для роботи мережі, фізичний захист має обмежену цінність.

2. Сегментація та VLAN. Обмеження розміру сегмента Ethernet може звести до мінімуму вразливу область для атак. Для досягнення сегментації можна використовувати пристрій вищого рівня, наприклад маршрутизатор або брандмауер. Крім того, механізм віртуальної локальної мережі IEEE 802.1Q можна використовувати в Ethernet для обмеження трансляцій та іншого трафіку певними сегментами. Мережі VLAN функціонують як логічно окремі об'єкти у фізичній мережі та створюють у ній домени безпеки. Віртуальна локальна мережа це технологія завдяки якій пристрої у локальній мережі розділяються на мережеві сегменти логічно, а не фізично. Сегментація мережі не обмежується фізичним розташуванням її користувачів. Вона базується на таких вимогах користувачів, як групування за: розташуванням, ролями, відділами, використовуваними програмами та використовуваними протоколами. Завдяки віртуальним локальним мережам, користувачі можуть бути організовані у менші робочі групи, кожна зі своїм ідентифікатором, що обмежить трафік кожного користувача до їх відповідної віртуальної локальної мережі та обмежить зв'язок між різними групами. Перевага віртуальної локальної мережі полягає в тому що вона обмежує широкомовний діапазон.

Існує три метода поділу віртуальної локальної мережі:

- Віртуальна локальна мережа що поділена за MAC-адресою − поділ що не потребує повторної конфігурації якщо вузол був переміщений.
- Віртуальна локальна мережа що поділена за IP-адресою − поділ в якому легко додавати вузли до мережі, адже комутатор сам призначить його до віртуальної мережі відповідно до його IP-адресі. Найкращий метод для поділу, але також і складний, бо потребує налаштувань.
- Віртуальна локальна мережа що поділена за протоколом − групує мережеві пристрої на основі протоколів що вони використовують для комунікації.

Комутатори можна налаштувати для призначення VLAN 1 і 2 окремим портам (Рис. 2), використовуючи VLAN 3 як магістраль. Зв'язок між хостами в різних VLAN блокується на рівні 2. Постачальники зазвичай рекомендують VLAN для безпеки, однак правильна конфігурація комутатора має вирішальне значення, оскільки налаштування за замовчуванням часто є небезпечними та можуть спровокувати такі атаки, як VLAN hopping.

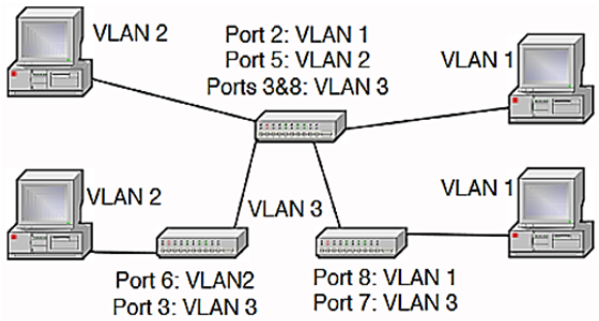

Рис. 2. Сегментація VLAN

3. Індивідуальні VLAN. Подвійне тегування IEEE 802.1ad Q-in-Q або конфігурацію комутатора Private VLAN (PVLAN), надану постачальником, можна використовувати для призначення кожному хосту в Ethernet власної VLAN. Цей підхід особливо корисний у мережах доступу на основі Ethernet, де хости спілкуються лише з одним або кількома іншими вузлами. Q-in-Q розширює простір ідентифікатора VLAN, додаючи інший тег VLAN, у той час як PVLAN використовує конфігурацію комутатора, щоб ізолювати хости та дозволяти їх трафіку проходити лише через один «безладний» порт, підключений до маршрутизатора та Інтернету. За допомогою PVLAN кожен хост може бачити лише себе та хости, підключені до безладного порту, і лише кілька ідентифікаторів VLAN потрібні на магістралях, щоб вказати трафік PVLAN.

4. Контроль доступу на основі автентифікації. Перевірка ідентичності користувача або хоста, який підключається до порту комутатора, є покращенням порівняно з базовим контролем фізичного доступу.

Автентифікація через порт IEEE 802.1X дозволяє використовувати різні облікові дані для автентифікації, наприклад пару імені користувача та пароля, або сертифікат і відповідний йому закритий ключ. Для цього методу потрібне клієнтське програмне забезпечення на кінцевому хості, програмне забезпечення на комутаторі та централізований сервер бази даних автентифікації. Рис. 3 демонструє зв'язок між хостом, комутатором і сервером бази даних автентифікації. Для автентифікації хост зв'язується з комутатором, і комутатор перевіряє облікові дані з бази даних. Розширюваний протокол автентифікації (EAP) використовується 802.1X, який підтримує різні методи та структури автентифікації.

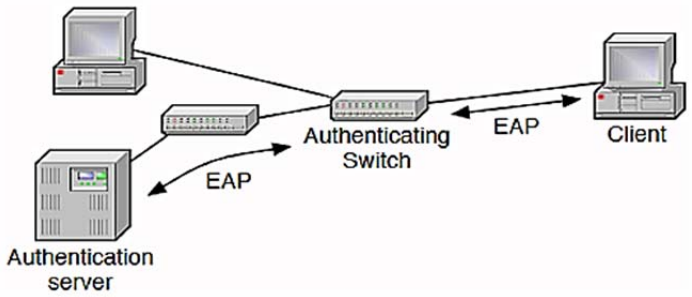

Рис. 3. Сеанс автентифікації 802.1X

На початку сеансу 802.1X автентифікує хост і пов'язує його MAC-адресу з певним портом комутатора. Якщо комутатор виявляє розрив з'єднання, асоціація розривається, і потрібна нова автентифікація. Коли хости безпосередньо підключені до комутатора, який підтримує 802.1X, то він забезпечує захист від атак підробки MAC-адрес і флуд-атак. Однак інші атаки, такі як отруєння ARP, все ще можуть бути можливими.

Зловмисник може втрутитися в концентратор або перемикнутися між комутатором автентифікації та автентифікованим хостом. Після завершення автентифікації автентифікованого хоста може від'єднати без розриву електричного з'єднання з комутатором автентифікації, дозволяючи зловмиснику ввести в мережу інший хост з такою ж MAC-адресою [2]. Щоб створити захищену внутрішню мережу та запобігти атакам імітації комутатора, між комутаторами також можна реалізувати автентифікацію.

5. Списки контролю доступу. Ethernet не має вбудованих списків контролю доступу (ACL), оскільки вони не включені до специфікації Ethernet. Тому постачальники комутаторів самостійно додали різноманітні можливості. У простому кадрі ACL Ethernet доступні атрибути обмежені за MAC-адресою відправника чи одержувача або полем Ethertype. Доступ можна обмежити на основі MAC-адрес, але зазвичай реалізовано декілька ACL для певної служби. Наступні функції можуть бути використані для забезпечення контроля доступу.

Безпека порту − це функція, яка дозволяє адміністраторам мережі обмежувати доступ до порту комутатора, контролюючи кількість MAC-адрес, які можуть до нього підключитися [3]. Це ефективно запобігає атакам переповнення MAC-адрес і несанкціонованому розширенню мережі, запобігаючи додаванню неавторизованих комутаторів. Захист портів надає можливість детального контролю, наприклад блокування нових MAC-адрес, які перевищують ліміт, блокування портів із існуючих MAC-адрес, закінчення терміну дії старих MAC-адрес через певний період або збереження MAC-адрес статичними, доки порт не буде скинуто вручну. Крім того, MAC-адреси можуть бути прив'язані до порту, до якого вони були підключені вперше, що блокує використання тієї ж адреси на інших портах, таким чином запобігаючи мобільності та підробці MAC-адрес.

Захист від шторму пакетів − це функція, яка обмежує кількість кадрів, які можна надіслати через порт комутатора протягом заданого періоду часу. Він призначений для

запобігання шторму пакетів, який виникає, коли хост надсилає надмірну кількість кадрів через несправність або навмисну атаку. Якщо обмеження встановлено досить низьким, це також може запобігти атакам затоплення MAC-адрес.

Захист BPDU − це функція, яка запобігає проходженню будь-яких повідомлень STP через порт, і її можна використовувати для визначення порту, який не повинен бути частиною сітчастої мережі. Водночас захист кореня STP ідентифікує порт, який є частиною мережі STP, але не може стати коренем STP. Ці функції також використовуються для цілей оптимізації продуктивності, наприклад, забезпечення того, що для побудови деревовидної топології мережі використовувалися лише найшвидші зв'язки [4].

6. Захист від перевантаження рівня контролю та управління. Обмеження обсягу трафіку на площинах контролю та управління може допомогти запобігти перевантаженню. Контроль площини керування (CoPP або CPP) досягає цього за допомогою набору фільтрів, які покладаються на методи та адреси обмеження швидкості, щоб уникнути перевантаження функцій площини керування. Фільтри призначені для того, щоб дозволити лише певній кількості пакетів даних рівня контролю та управління досягти центральний процесор (ЦП), а весь інший трафік блокується до того, як він досягне рівня ЦП. Цей підхід допомагає захиститися від навмисних атак, спрямованих на виснаження ЦП, хоча легітимні повідомлення також можуть бути втрачені під час атаки. Фільтри можна налаштувати, щоб дозволити окремо встановлювати різні типи контрольних кадрів.

7. Безпека локальної мережі з централізованим керуванням. Дослідницьке співтовариство запропонувало різні методи збору інформації з локальної мережі та її використання для управління безпекою. Цими методами є:

- SANE − це нова конструкція, яка використовує централізований контролер для хостів для публікації служб і запитів доступу один до одного. Його основна мета полягає в тому, щоб реалізувати орієнтовану на організацію політику безпеки на рівні локальної мережі, і він прагне забезпечити широкий захист для Ethernet.
- Ethane є розширенням підходу SANE, який усуває необхідність встановлення нового програмного забезпечення на хостах. Хоча центральний контролер все ще підтримує політики, але хости все ж повинні бути автентифіковані. Коли ініціюються нові потоки, комутатори Ethane спочатку надсилають їх до контролера, який визначає, авторизувати чи забороняти їх, і відповідно налаштовує комутатор.
- OpenFlow − це дизайн, який базується на ідеях Ethane, вводячи перемикач, який використовує таблиці потоку та зовнішній контролер замість таблиці MAC. Ці таблиці потоку враховують такі атрибути пакетів, як Ethernet, IP і транспортні рівні. Крім того, кадри можуть бути спрямовані на порти або центральний контролер, відокремлюючи запити ARP від іншого трафіку. OpenFlow представляє архітектуру, відому як програмно визначена мережа (SDN), яка відокремлює функції керування від функцій перемикання та реалізує керування лише на початку потоку [4, 5].

Обмеження доступу до цілей для зловмисників досягається за допомогою контролю доступу. Цілі також можна зробити менш доступними шляхом включення функцій безпеки в протоколи.

Одним із рішень забезпечення цілісності та конфіденційності є криптографія. MACsec, стандарт IEEE 802.1AE, що встановлює зашифровані з'єднання між комутаторами та хостами, захищаючи цілісність і конфіденційність переданих даних. Щоб реалізувати MACsec, необхідно встановити програмне забезпечення та конфігурувати автентифікацію для кожного об'єкта мережі. Хоча MACsec використовує інформацію автентифікації 802.1X, він не визначає керування ключами, що залишається на розсуд постачальників.

MACsec ефективно захищає від несанкціонованого доступу до мережі, забезпечуючи конфіденційність і цілісність даних. Однак це не гарантує захисту від авторизованих хостів, які можуть поводитися зловмисно. MACsec забезпечує безпеку лише для зовнішнього периметра, а внутрішні об'єкти залишаються вразливими до атак. Наприклад, авторизований хост може використовувати ARP для захоплення трафіку іншого хоста. Крім того, MACsec не забезпечує захист від DoS-атак і аналіз трафіку.

Архітектура Ethernet вразлива до атак через протокол розпізнавання адрес (ARP). Однак цю вразливість можна усунути, використовуючи інформацію, отриману від стеження за протоколом динамічної конфігурації хоста (DHCP), щоб пов'язати MAC-адреси з відповідними IP-адресами та портами. Тим не менш, відстеження DHCP може мати обмежений обсяг, оскільки комутатор може не мати видимості розподілу, зробленого для хостів, які не проходять через нього для доступу до сервера DHCP.

Дослідники в основному зосереджуються на рішеннях, заснованих на криптографії, таких як S-ARP, яке містить поле автентифікації в повідомленнях ARP разом із структурою керування ключами, що використовує зв'язування криптографічного простору імен, або [6], що розширює покриття MACsec між кінцевими точками та захист багатоадресної передачі.

Щоб запобігти неправильному використанню вищих функцій комутатора, доступ до комутатора має бути контрольованим. Функції площини керування, які пов'язані з площиною користувача, можна захистити за допомогою методів, розглянутих раніше.

Один із способів захисту функцій площини керування − обмежити їх окремою фізичною або віртуальною мережею керування. Крім того, зашифровані з'єднання часто використовуються для захисту даних керування, при цьому SSH зазвичай використовується для командного рядка та TLS/SSL для веб-інтерфейсів. Механізми автентифікації можуть включати паролі або криптографічні облікові дані.

Моніторинг комутаторів зазвичай здійснюється за допомогою простого протоколу керування мережею (SNMP), який може використовувати або не використовувати захист паролем. Шифрування не підтримується у версії 1 SNMP, і навіть якщо воно доступне у версії 3 і деяких типах версії 2, воно може не використовуватися, коли SNMP використовується виключно для моніторингу.

Протоколи вищого рівня та MACsec зазвичай включають такі механізми, як мітки часу або неповторювані значення (nonces), щоб запобігти атакам відтворення, оскільки сам базовий кадр Ethernet не забезпечує захисту від них.

У попередніх абзацах були описані підходи до безпеки, які є переважно проактивними та самодостатніми, без необхідності втручання людини чи участі зовнішніх систем. Однак активні технології можуть забезпечити додаткову безпеку мережі.

Брандмауери використовуються для обмеження потоку трафіку між різними сегментами мережі, і їх можна розглядати як більш складні версії списків контролю доступу, які включають можливості відстеження стану. Крім того, брандмауери можуть використовувати глибоку перевірку пакетів (DPI) і відтворення сеансу прикладного рівня для забезпечення перевірки. Сучасні брандмауери можуть працювати на всіх мережевих рівнях, роблячи безглуздим ідею «мережевого екрану Ethernet». ACL комутаторів можна використовувати для обмеження трафіку на рівні Ethernet, у той час як стандартні брандмауери можуть контролювати вищі рівні.

Реалізація політики безпеки підприємств значною мірою залежить від брандмауера, який вважається системою або групою систем, що використовуються для контролю мережевого трафіку на основі заздалегідь визначених правил. Діючи як захисний міст, який відокремлює внутрішню мережу від зовнішньої ненадійної мережі, такої як Інтернет, брандмауер функціонує як контрольно-пропускний шлюз, який ретельно перевіряє IP-пакети, щоб визначити, дозволяти чи не пропускати їх на основі попередньо налаштованих правил. Крім того, брандмауер вирішує, яка інформація або служби доступні як зсередини, так і ззовні мережі, і хто має дозвіл на доступ до них.

Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) використовують DPI для виявлення мережевих атак, зазвичай шляхом порівняння мережевого трафіку з бібліотекою відомих сигнатур атак. Ці системи потребують доступу до мережевого трафіку, який можна отримати шляхом розміщення пристрою IDS/IPS безпосередньо між двома кінцевими точками (зазвичай використовується як брандмауер або для посилення брандмауера) або шляхом моніторингу трафіку від комутатора за допомогою функції дублювання портів. Віддзеркалення портів дублює трафік до та з вибраних портів до

порту моніторингу, де розташований пристрій IDS/IPS. За потреби можна встановити окрему мережу, щоб пристрої моніторингу були відокремлені від захищеної мережі.

Комутатори мають додаткові можливості, які можуть допомогти у виявленні зловмисної поведінки. Наприклад, сповіщення про MAC-адресу може надсилати повідомлення перехоплення SNMP, коли хост рухається в мережі. Для цілей системи виявлення вторгнень (IDS) кілька визначень інформаційної бази керування SNMP (MIB) можуть бути цінними, включаючи MIB віддаленого моніторингу мережі (RMON) та її розширення комутатора (SMON). Поряд з пасивним моніторингом для виявлення зловмисної поведінки також можна застосовувати активні заходи. Кадри з очікуваною поведінкою можуть бути введені в мережу та відстежені для виявлення атак ARP-спуфінгу [7].

Ефективне планування, налаштування та адміністрування можуть мати значний вплив на різні аспекти мережі Ethernet. Багато технічних рішень, розглянутих раніше, вимагають постійної конфігурації та коригування для адаптації до змін у топології мережі. Оскільки не існує надійного методу автоматичного розрізнення магістральної мережі від підключень до кінцевих вузлів, адміністратори мережі повинні вручну налаштувати цю інформацію на комутаторах. Розділення управлінської інформації у виділену VLAN та обмеження функціональності рівня керування та потоків даних може підвищити безпеку мережі до рівня, порівнянного з мережею на основі IP-маршрутизатора.

Існує кілька доступних систем керування мережею, які можуть допомогти в налаштуванні комутаторів у мережі. Ці системи підтримують топологію мережі та автоматизують завдання, тим самим зменшуючи помилки. Однак для використання цих систем керування комутатори мають бути сумісні з програмним забезпеченням і налаштовані для спільної роботи.

Висновки. Захист локальної мережі потребує багатостороннього підходу, який передбачає поєднання проактивних і реактивних заходів. Це включає такі методи, як VLAN, ACL, MACsec, DPI, IDS/IPS та активне сканування для виявлення вразливостей. Належні методи адміністрування мережі, такі як відокремлення управлінської інформації до виділеної VLAN та обмеження функціональності рівня керування та потоків даних, також можуть підвищити безпеку. Зрештою, ключем до захисту локальної мережі є постійний моніторинг і оновлення заходів безпеки, щоб не відставати від загроз, що розвиваються. Впроваджуючи комплексну стратегію захисту, мережеві адміністратори можуть значно знизити ризик зламу мережі та несанкціонованого доступу.

Список використаних джерел

1. Fundamentals of Network Security \\ Режим доступу: https://www.theseus.fi/bitstream/handle/10024/61830/Building%20a%20Secure%20Local%20Area%20Network_final%20-%20Copy.pdf?sequence=1 (останнє звернення 18.03.2023р.)
2. Mitigating the threats of rogue machines802.1X or IPsec? \\ Режим доступу: http://technet.microsoft.com/en-us/library/cc512611.aspx (останнє звернення 18.03.2023р.)
3. Safe layer 2 security in-depth \\ Режим доступу: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfbluwp.pdf (останнє звернення 18.03.2023р.)
4. Pushing enterprise security down the network stack \\ Режим доступу http://hdl.handle.net/1853/30782 (Останнє звернення 18.03.2023р.)
5. T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, and S. Shenker, Onix: a distributed control platform for large-scale production networks. – 2010. – с. 1 – 6.
6. K. Wahid, Rethinking the link security approach to manage large scale Ethernet network. – 2010. – с. 5 – 7.
7. N. Hubballi, S. Roopa, R. Ratti, F. A. Barbhuiya, S. Biswas, A. Sur, S. Nandi, V. Ramachandran, An active intrusion detection system for LAN specific attacks. – 2010. – с. 129 – 142.

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

ОНЛАЙН-СПІЛКУВАННЯ У ЦИФРОВУ ЕПОХУ: ВІД АНАЛІЗУ ПЛАТФОРМ ДО ПОТРЕБИ У СПЕЦІАЛІЗОВАНОМУ РІШЕННІ ДЛЯ ТЕМАТИЧНИХ ВЕЧІРОК

ЦІОМІК І., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглядається різноманітність сучасних платформ для організації онлайн-зустрічей, вказуючи на їх переваги та недоліки. Деякі платформи, зокрема Hopin, Houseparty, Airbnb Online Experiences, Netflix Party, Twitch та YouTube Live, надають користувачам унікальні можливості для інтерактивного спілкування, віртуальних подій та спільного перегляду контенту. Втім, не існує платформи, яка була б спеціалізована на організації тематичних онлайн вечірок. Розробка такої платформи, яка враховує потреби осіб з інвалідністю, може стати відповіддю на зростаючу потребу якісних платформ для онлайн-спілкування.

The article examines the variety of modern platforms for organizing online meetings, highlighting their advantages and disadvantages. Platforms such as Hopin, Houseparty, Airbnb Online Experiences, Netflix Party, Twitch, and YouTube Live offer users unique opportunities for interactive communication, virtual events, and shared content viewing. However, there is no platform specifically designed for thematic online parties. Developing such a platform, which takes into account the needs of people with disabilities, can be an answer to the growing demand for quality online communication platforms.

Актуальність. Зростаюча цифрова трансформація суспільства невблаганно перетворює усі аспекти нашого життя, включаючи спосіб спілкування та розваг. Останні події, пов'язані зі світовою пандемією, ще більше підкреслили необхідність в інноваційних підходах до організації подій та розважальних заходів. У контексті цього варто врахувати й вплив війни, конфліктів та непевностей, які можуть призвести до обмежень у фізичних зустрічах та спілкуванні. Становлення нової реальності, де фізична відстань не заважає спілкуванню, робить платформу для організації та проведення онлайн тематичних вечірок вкрай актуальною.

Умови, змінені пандемією, війною, природними катаклізмами та іншими геополітичними конфліктами, спонукають нас до пошуку нових способів комунікацій та розваг. Важливість такої платформи полягає в тому, що вона не лише забезпечує можливість соціального спілкування, але і дозволяє організувати нові та нетрадиційні й нетипові заходи в онлайн форматі. Вона створює можливість об'єднати людей з різних куточків світу, які мають спільні погляди, цінності, інтереси та хочуть проводити якісно час, спілкуючись разом. Разом з тим, така платформа дає можливість соціалізації людей з особливими потребами.

Різноманітність тематик та креативних концепцій для вечірок додає платформі додатковий рівень привабливості. Вона є місцем для реалізації ідей, віртуального творчого експерименту та незабутнього дозвілля. Крім того, розширені можливості взаємодії в онлайн просторі дозволяють підтримувати постійний контакт з друзями та знайомими, а також знаходити нових друзів, знайомих, бізнес-партнерів тощо, не зважаючи на віддаленість.

Все це робить тему «Платформа для організації та проведення онлайн тематичних вечірок» особливо актуальною у наш час. Вона відповідає потребам сучасного суспільства в інноваційних способах взаємодії, соціального спілкування та розваг, роблячи їх доступними в будь-який час та з будь-якого місця.

Мета дослідження: полягає в розробці та реалізації комплексної онлайн платформи, яка забезпечує організацію та проведення тематичних вечірок в віртуальному середовищі.

Головною метою є створення зручного та привабливого інструменту для користувачів, що дозволить їм активно взаємодіяти, спілкуватися та відчувати радість від спільного часу, незалежно від географічного розташування.

Об'єктом дослідження є процеси організації та проведення онлайн тематичних вечірок, а також взаємодія учасників під час таких подій.

Предмет дослідження є розробка та функціонування платформи, що забезпечує можливість організації та участі в онлайн тематичних вечірках.

Виклад основного матеріалу.

Нині, коли технології продовжують швидко розвиватися, віртуальні події стають все більш популярними. Серед великої кількості різних онлайн заходів окрему нішу займають онлайн вечірки. Онлайн вечірки вцілому та тематичні онлайн вечірки зокрема, виконують низку сучасних функцій:

1.Соціальна взаємодія. Онлайн вечірки дозволяють людям зібратися, спілкуватися та провести час разом, навіть якщо вони знаходяться на великій відстані. Це може бути особливо важливим для тих, хто має друзів та рідних у різних частинах світу.

2.Креативність та розвага. Тематичні вечірки дають можливість проявити креативність, обрати певний стиль або тему, підготувати костюми чи декорації.

3.Підтримка певних інтересів. Онлайн вечірки можуть бути спрямовані на певні інтереси, хобі або захоплення. Це дає можливість знайти спільноту людей з спільними інтересами та захопленнями.

4.Доступність. Для людей з певними обмеженнями онлайн вечірки можуть бути особливо важливими, оскільки вони дозволяють взяти участь у соціальних подіях, не залишаючи дім.

5.Безпека і зручність. Онлайн вечірки можуть бути більш зручними та безпечними для деяких людей, особливо у випадках, коли їм потрібно уникати масових зібрань.

6.Подолання географічних обмежень. Онлайн вечірки дають можливість об'єднати людей з різних країн і континентів, не залежно від відстані.

Різноманітні платформи для проведення таких вечірок з'являються на просторах інтернету зі своїми унікальними можливостями та особливостями. Їх можна класифікувати таким чином: комерційні, безкоштовні та частково безкоштовні (у вільному доступі з певними обмеженими функціями); платформи загального призначення для організації онлайн зустрічей та спеціалізовані платформи для онлайн вечірок.

На сьогоднішній день існує безліч платформ, які можна використовувати для проведення онлайн вечірок та подій. У даному розділі буде проведено дефінітивний аналіз деяких найпопулярніших платформ для проведення онлайн зустрічей та організації онлайн вечірок.

Zoom – це ім'я, що стало практично синонімом для відеоконференцій і онлайн спілкування в реальному часі. Ця платформа, яка широко використовувалася під час глобальної пандемії COVID-19, стала також популярним вибором для проведення онлайн вечірок. Завдяки своїм розширеним можливостям, Zoom надає користувачам можливість створювати забавні, інтерактивні івенти, де вони можуть обмінюватися ідеями, грати в ігри та відчувати себе разом, навіть якщо вони фізично знаходяться далеко один від одного.

Переваги Zoom для проведення онлайн вечірок:

Висока якість відео та аудіо: Zoom відомий своєю стабільною роботою і гарною якістю зв'язку.

– Можливість створювати тематичні кімнати: Ви можете створювати різні кімнати для різних активностей під час вечірки.

– Екранний показ та обмін файлами: Це дає можливість демонструвати відео, графіку або інші матеріали для всіх учасників.

– Чат і реакції: Учасники можуть спілкуватися у чаті, відправляти реакції та виражати свої враження під час події.

– Велика кількість учасників: Залежно від обраного плану, Zoom може підтримувати значну кількість учасників на одній зустрічі.

Обмеження Zoom для проведення онлайн вечірок:

– Обмежений доступ до певних функцій у безкоштовному плані: Деякі продвинуті функції можуть бути доступні тільки за плату.

– Потребує встановлення програми або додатку: Учасники можуть потребувати завантажити програму або додаток Zoom, щоб приєднатися до зустрічі.

Висновок: Zoom є надійним і універсальним вибором для проведення різноманітних онлайн вечірок. Його розширені можливості сприяють створенню інтерактивного та захоплюючого досвіду для учасників.

У наступних розділах ми розглянемо інші популярні платформи для проведення онлайн вечірок та їх переваги та обмеження.

Microsoft Teams також підходить для віртуальних зібрань та вечірок. Вона має інтеграцію з іншими інструментами Microsoft та можливості для спільної роботи. При цьому вона має свої переваги та недоліки, які варто враховувати перед вибором цієї платформи.

Переваги:

– Зручна організація зустрічей: Teams має функції для планування та організації відеоконференцій. Є можливість створювати календар події, визначати учасників, встановлювати різні часові зони тощо.

– Поділ на групи (канали): можна створювати різні канали для різних тем або груп людей, що допомагає організовувати вечірку та спілкування більш структуровано.

– Безпека та конфіденційність: Microsoft Teams має високі стандарти безпеки та захисту даних, що може бути важливим, особливо якщо під час вечірки передбачено проведення конфіденційних розмови або подій.

– Microsoft 365 live events дає можливість організувати зустрічі у форматі трансляцій для 10 000 відвідувачів та менше [2].

Недоліки:

– Обмежені можливості для розваг: платформа Microsoft Teams переважно спрямована бізнес-середовище, тому її можливості для розваг, ігор або креативних заходів можуть бути обмеженими порівняно з іншими платформами.

– Складність для незнайомих користувачів: для тих, хто не має досвіду з Microsoft Teams, платформа може здаватися дещо складною та незрозумілою.

– Обмеження у безкоштовній версії: деякі функції та можливості можуть бути доступні лише за плату або в розширеній версії Microsoft Teams [2].

Discord – це безкоштовна комунікаційна програма, яка дозволяє ділитися голосовим, відео- та текстовим чатом із друзями, ігровими спільнотами та розробниками. Discord можна використовувати майже на всіх популярних платформах і пристроях, включаючи Windows, macOS, Linux, iOS, iPadOS, Android, а також через веб-браузери.

Основна мета Discord – спілкування. Кожен може безкоштовно створити сервер Discord використовувати його, щоб зібрати друзів разом у груповому текстовому чи голосовому чаті. Розробники часто використовують Discord як місце для обміну ігровими смаками зі своїми спільнотами.

Переваги:

– Спрямованість на спільноти: Discord розроблений для спільнот, і він має багато функцій, що сприяють взаємодії у спільностях, що робить його добрим варіантом для тематичних вечірок.

– Голосовий чат і тескстовий чат: Discord надає можливість створювати голосові та текстові канали, де учасники можуть спілкуватися під час вечірки.

– Багато можливостей для налаштувань: можна створювати різні канали для різних аспектів вечірки, встановлювати ролі для учасників, обмежувати доступ до певних функцій тощо.

– Віртуальні сервери: Discord надає можливість створювати власні сервери, що може бути корисним для збереження всіх тематичних вечірок та спільнот.

– Багато інтегрованих ігор та додатків: Discord має багато ігор, які можна грати разом з учасниками вечірки, а також інші додатки, які можуть бути використані для розваг.

Недоліки:

– Неспеціалізована платформа: Оскільки Discord спрямований на геймерів, деякі функції, які можуть бути важливими для організації вечірок, можуть бути менше розвиненими порівняно з іншими платформами.

– Інтерфейс Discord не є інтуїтивно зрозумілим для тих, хто раніше не користувався платформою.

– Можливість завантаження вмісту: на платформі може з'являтися несанкціонований або небажаний вміст, який може потребувати уваги та контролю.

Загалом, Discord може бути чудовим варіантом для організації тематичних вечірок, особливо якщо ви бажаєте залучити учасників, які спільно ділять певні інтереси та хочуть взаємодіяти під час вечірки.

Gather.town є інтерактивною платформою, яка дозволяє створювати віртуальні простори для різноманітних зустрічей. Вона відрізняється від традиційних платформ завдяки своєму графічному середовищу та методам взаємодії між учасниками.

Переваги:

– Інтерактивність: можливість для користувачів динамічно взаємодіяти між собою в віртуальному середовищі.

– Спрощене спілкування: автоматичний вхід в аудіо- та відеодзвінки при наближенні до іншого користувача.

– Групові активності: інтеграція групових ігор та інших форм розваг.

– Безпека: можливість створення приватних зон та контролю доступу.

Недоліки:

– Технічні обмеження: Потенційні проблеми для користувачів зі слабким інтернет-з'єднанням або застарілим обладнанням.

– Крива навчання: Для деяких користувачів інтерфейс може здатися складним.

– Вартість: Потенційно висока вартість при великих масштабах або потребах у додаткових функціях.

– Відсутність деяких функцій: Можливе обмеження в функціоналі порівняно з іншими платформами.

– Максимальне обмеження учасників: Обмеження кількості учасників в залежності від пакету послуг [5].

Отже, Gather.town представляє собою унікальний інструмент для організації віртуальних зустрічей, що поєднує в собі інтерактивність та гнучкість. Проте, при його використанні, необхідно враховувати потенційні технічні обмеження та особливості користувачів.

Remo є однією з платформ, яка пропонує інноваційний підхід до організації віртуальних зустрічей та конференцій. Remo створена для підвищення інтерактивності та сприяння ефективності мережевої взаємодії. Ця платформа симулює віртуальне середовище, де користувачі можуть пересуватися між різними «столами», імітуючи реальне життєве спілкування.

Переваги:

– Інтерактивність: платформа дозволяє учасникам вільно переміщуватися між столами та групами, сприяючи природній взаємодії.

– Ефективність для нетворкінгу: особливо корисно для бізнес-зустрічей та конференцій, де важлива можливість нетворкінгу.

– Гнучкість конфігурації: можливість налаштовувати віртуальні простори згідно з потребами заходу.

– Інтегровані інструменти: наявність додаткових інструментів для презентацій, обговорень тощо.

Недоліки:

– Обмеження в учасниках: залежно від пакету, може бути обмеження на максимальну кількість учасників.

– Технічні вимоги: потреба у стабільному інтернет-з'єднанні та сучасному обладнанні для оптимального досвідуК

– Вартість: вартість підписки може бути досить високою для великих масштабів або додаткових функцій [6].

Отже, Remo є високоефективним інструментом для проведення віртуальних зустрічей, особливо в контексті нетворкінгу та бізнес-заходів. Однак важливо враховувати технічні вимоги та потреби користувачів, щоб забезпечити успішний досвід використання платформи.

Висновки. У сучасному цифровому світі існує велика різноманітність платформ для організації та проведення онлайн зустрічей. Кожна платформа має свої унікальні переваги та недоліки, що робить їх ідеально підходящими для різних типів подій.

Платформи, такі як Hopin і Houseparty, надають можливість інтерактивної участі, забезпечуючи як групові, так і індивідуальні взаємодії. Airbnb Online Experiences дозволяє користувачам відкрити для себе унікальні віртуальні заходи, представлені різними культурами з усього світу. Netflix Party і Twitch акцентують увагу на спільному перегляді контенту та грах, в той час як YouTube Live дозволяє користувачам досягти величезної аудиторії завдяки стрімінгу в реальному часі.

Що стосується технічної сторони, багато платформ потребують високоякісного зєднання з Інтернетом та професійного обладнання для оптимального досвіду користувача.

Для організації тематичних онлайн вечірок важливо вибрати платформу, яка найкраще відповідає потребам та очікуванням аудиторії, але дослідження показаи, що наразі не існує спеціалізованої платформи саме для оргаізації тематичних онлайн вечірок.

Розробка платформи для онлайн організації вечірок є відповіддю на зростаючу потребу людей у якісних платформах для онлайн-спілкування. З урахуванням особливостей потреб осіб з інвалідністю, платформа матиме великий потенціал стати популярним та корисним інструментом соціалізації в онлайн просторі.

Список використаних джерел

1. https://zoom.us/pricing
2. https://news.microsoft.com
3. https://meet.google.com/
4. https://store.epicgames.com/en-US/news/what-is-discord-and-what-is-it-used-for
5. https://www.gather.town/
6. https://remo.co/solutions-for-higher-education

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

ПОБУДОВА МІКРОСЕРВІСІВ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ GO

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

У статті розглянуто основні засади побудови мікросервісів за допомогою мови програмування Go. Зазначено переваги використання Go та її екосистеми для побудови відмовостійкої мікросервісної архітектури хмарного середовища. Приведені приклади реалізації мікросервісів на Go.

The article discusses the main principles of building microservices using the Go programming language. The advantages of using Go and its ecosystem for building a resilient microservices architecture in a cloud environment are highlighted. Examples of implementing microservices in Go are provided.

Актуальність. Мікросервісна архітектура стала найбільш популярною архітектурою для побудови програмних систем та компонентів які можуть витримувати високі навантаження на систему, мають переваги у легкості розбудови та масштабування. Мова програмування Go, при побудові мікросервісів, зарекомендувала себе як надійний інструмент, що не дивно з урахуванням мети з якої була створена, а саме для роботи з інформаційними системами різного рівня складності, мережами та інфраструктурою, на заміну мовам програмування C++ та Java.

Метою статті є дослідження особливостей використання мови програмування Go для побудови мікросервісів.

Об'єктом дослідження є розробка мікросервісів за допомогою мови програмування Go.

Предмет дослідження: інформаційні-мікросервісні системи побудовані за допомогою мови програмування Go.

Виклад основного матеріалу. Перш ніж переходити до застосування Go в розробці мікросервісних систем потрібно визначите ключові концепції мікросервісів.

Мікросервіси це незалежно реалізовані сервіси які були спроєктований та змодельовані в рамках бізнес-моделі.

Характеризуються такими ключовими елементами [1]:

– Незалежне розгортання (Independent deployability). Незалежне розгортання – це ідея, згідно з якою ми можемо внести зміни в мікросервіс, розгорнути його та оприлюднити ці зміни нашим користувачам без необхідності розгортати будь-які інші мікросервіси.

– Змодельована навколо бізнес-моделі (Modeled around a Business Domain). Це допомагає зрозуміти та структурувати код навколо об'єктів реального світу. Якщо ми моделюємо сервіси навколо бізнес доменів, ми можемо спростити розгортання та реалізацію нових функцій та комбінувати мікросервіси різними способами, щоб надати новий функціонал кінцевому користувачу.

– Управління власним станом (Owning Their Own State). Під цим елементом мається на увазі в контексті доступу до даних сервісу, сервіс повинен володіти своїми даними та дати можливість звертатися до них іншим сервісам, замість того щоб розгортати одну базу даних для всіх наявних сервісів.

– Розмір сервісу (Size). Microservice Patterns (Manning Publications): мета мікросервісів – мати якомога менший інтерфейс. Це знову узгоджується з концепцією приховування інформації, але це спроба знайти сенс у терміні «мікросервіси», якого не було спочатку. Коли цей термін вперше використовувався для визначення цих архітектур, увага, принаймні спочатку, не була конкретно на розмірі інтерфейсів.

– Гнучкість(Flexibility). Ми не знаємо, що чекає майбутнє, тому нам потрібна архітектура, яка теоретично може допомогти нам розв'язувати будь-які проблеми, з якими ми можемо зіткнутися в майбутньому. Справжнім мистецтвом може бути знаходження балансу між можливістю пидтримки певних опцій у майбутньому і покриттям витрат на такі архітектури.

– Alignment of Architecture and Organization [1]

Спочатку мова програмування Go створювалась як внутрішній продукт у компанії Google. Вперше мова була представлена у 2009 році, а перший реліз відбувся у 2012. Основною метою створення цієї мови програмування було поєднання високої продуктивності компільованих мов з легкістю написання коду з підтримкою Garbage Collector. Мова вийшла досить лаконічна, але при цьому код залишається легким для читання і сприйняття. [2]

За допомогою Go ми можемо реалізувати всі ключеві аспекти мікросервісної архітектури, та зробити це зручніше та простіше для розробника, адже Go має такі переваги:

– Швидкість виконання: Go відома своєю високою продуктивністю та швидкістю виконання, що робить її ідеальною для великих і складних проєктів.

– Простота: Go має простий синтаксис, що робить його легким для вивчення та розуміння. Це також сприяє зменшенню кількості помилок при написанні програм.

– Конкурентність: Go підтримує паралельне виконання, що дозволяє програмістам легко створювати паралельні програми. Має дуже цікаву реалізацію перемикання потоків, чим збільшується швидкість. Go має підпрограму яка називається горутиною, за допомогою якої перемикається контекст в рамках потоку не зупиняючи при цьому сам системний та процесорний потік.

– Низький рівень складності: Go забезпечує прямий доступ до пам'яті та не використовує важкі механізми управління пам'яттю, що знижує складність програм.

– Наявність стандартної бібліотеки: Go має багату стандартну бібліотеку, яка містить багато корисних функцій та інструментів для розробки програм.

– Висока масштабованість: Go підтримує масштабованість програм, що дозволяє легко розширювати програми на більші системи.

– Має велику спільноту розробників та велику купу пакетів за межами стандартної бібліотеки.

– Великі корпорації (Amazon, Google, Uber) здійснили великий вклад в розвиток мови, та розширюють бібліотеки на Go.

Розглянемо більш детально, одну з ключових переваг застосування Go у побудові мікросервісів у порівняні з іншими серверними мовами програмування, це продуктивність.

Продуктивність мікросервісу залежить від навантаження та часу відгуку. Для досягнення найкращої продуктивності варто використовувати швидку та високоефективну мову програмування. У порівнянні з іншими мовами, які використовуються для розробки серверної частини вебсайту та мобільних додатків, Go є відмінним вибором. За даними останнього рейтингу програмної мови TIOBE [3], Go займає 10 місце серед усіх мов програмування, що є досить високим результатом. Однією з переваг Go є те, що вона не потребує віртуальної машини, а отже, програми компілюються в машинний код. Це дозволяє виконувати програми без затримок на розминку та забезпечує високу продуктивність. Крім того, у Go є вбудований збирач сміття, що допомагає керувати пам'яттю та зменшує ризик проблем із безпекою, які можуть виникнути через інкапсуляцію коду. Це також полегшує життя розробникам, оскільки вони не повинні вручну вивільняти пам'ять після використання даних, тим самим уникнувши потенційних помилок, які можуть бути пов'язані з неправильним керуванням пам'яттю. Збирач сміття Go базується на алгоритмі «Mark and Sweep» і виконується автоматично під час роботи програми. Він слідкує за тим, які об'єкти використовуються в програмі, і вивільняє пам'ять, яка більше не потрібна. Це дозволяє підвищити продуктивність програм та полегшити розробку, оскільки розробникам не

потрібно докладно керувати пам’яттю. Збирач сміття є одним із багатьох функціональних інструментів Go, які роблять цю мову програмування досить привабливою для розробників. Слід додати, що Go відомий своєю підтримкою асинхронного програмування. Він пропонує кілька механізмів для роботи з асинхронним кодом, зокрема, горутини (goroutines) та канали (channels). Горутини – це легкі потоки, які можуть бути створені великою кількістю та виконуватися паралельно або асинхронно. Вони дозволяють запускати асинхронний код без потреби вручну створювати та керувати потоками виконання. Канали, з іншого боку, дозволяють горутинам взаємодіяти між собою задля ефективної передачі даних між різними потоками, та керувати узгодженістю виконання певних процесів де це потребується на програмному рівні. Керування горутинами здійснюється за допомогою планувальника горутин (goroutine scheduler). Планувальник відповідає за розподіл горутин між потоками та керування їх виконанням, використовуючи при цьому event-driven модель. З урахуванням наведених переваг, потрібно звернутися до практичного порівняння Go з іншими мовами програмування.

Нижче наведені дані порівняння роботи Go з популярною на сьогодні мовою програмування Java.[4]

edigits

Input: 250001

lang	code	time	stddev	peak-mem	time(user)	time(sys)	compiler/runtime
go	1.go	163ms	1.2ms	8.5MB	153ms	0ms	go 1.19.3
java	1-m.java	811ms	11ms	193.1MB	1427ms	63ms	openjdk 19
java	1-m.java	873ms	66ms	209.7MB	1503ms	97ms	openjdk 20
java	1-m.java	884ms	29ms	321.6MB	1497ms	133ms	graal/jvm 17.0.5
java	1-m.java	1069ms	67ms	457.5MB	1540ms	350ms	openjdk/zgc 19

Рис. 1. Документ «Швидкість роботи Go у порівнянні з Java»

Також слід порівняти швидкодію Go з такою мовою програмування як Python, оскільки в цьому прикладі яскраво виражені переваги Go для побудови мікросервісів.

Як ми можемо бачити з результатів таблиці, одна з головних переваг Go полягає в його швидкості та ефективності, що дозволяє зменшити час відповіді та покращити продуктивність мікросервісів.

fasta

Input: 2500000

lang	code	time	stddev	peak-mem	time(user)	time(sys)	compiler/runtime
go	3-m.go	209ms	2.4ms	4.9MB	373ms	0ms	go 1.19.3
python	1.py	3292ms	74ms	88.9MB	3257ms	20ms	pypy 3.8.13
python	5-m.py	3508ms	55ms	12.6MB	5013ms	1253ms	pyston 3.8.12
python	1.py	3949ms	15ms	7.9MB	3933ms	0ms	pyston 3.8.12
python	5-m.py	4237ms	24ms	13.8MB	6063ms	1223ms	cpython 3.11.0
python	1.py	timeout	0.0ms	0.0MB	0ms	0ms	cpython 3.11.0
python	5-m.py	timeout	0.0ms	0.0MB	0ms	0ms	pypy 3.8.13

Рис. 2. Документ «Швидкість роботи Go у порівнянні з Python»

Нижче додається приклад мікросервісної архітектури програмного додатка з використанням хмарних можливостей AWS.

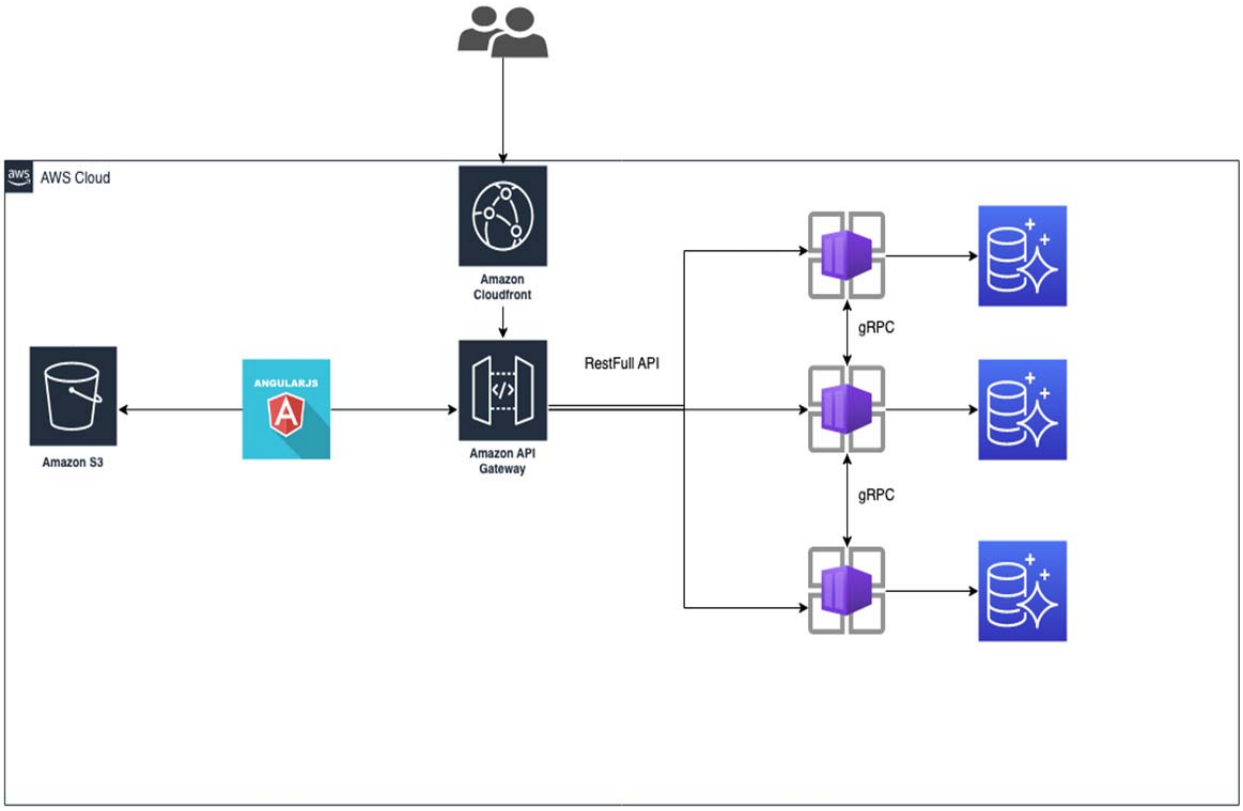

Рис. 3. Вікно Документ «Мікросервісна архітектура». Виконана автором за допомогою веб додатка draw.io

Сучасні міжсервісні системи тісно пов'язані з хмарними технологіями. Тому при розробці мікросервісної архітектури на Go, було застосовний хмарний провайдер AWS, який виділяється з поміж інших конкурентів, зручним та інтуїтивно зрозумілим інтерфейсом, а також широкою документацією. Внутрішню комунікацію між сервісами вирішено реалізувати за допомогою RPC(Remote Procedure Call), оскільки RPC більш ефективним за REST, оскільки передача даних відбувається у вигляді серіалізованих об'єктів, що зменшує розмір даних та сприяє швидкому виконанню запитів. Також RPC дозволяє розподілити логіку програми між різними сервісами, зменшуючи складність коду та покращуючи зрозумілість програми, розширювати систему на більші обсяги, що підвищує її масштабованість, використовувати різні мови програмування для реалізації різних частин системи, що підвищує її гнучкість. Для комунікації між кліент-сервором, доречно обрати RESTful API, оскільки це дає змогу використовувати стандартні HTTP-методи, такі як GET, POST, PUT і DELETE, що дозволяє стандартизувати взаємодію з ресурсами та спрощує їх розробку та розуміння, а також дає можливість підтримки різних форматів даних, такі як JSON, XML, HTML. Також було вирішено використовувати окрему базу даних для кожного мікросервісу, оскільки це дозволяє забезпечити незалежність сервісів один від одного щодо бази даних. Кожен сервіс може використовувати той тип бази даних, який найбільше підходить для його потреб, також це полегшує масштабування системи. Якщо потрібно збільшити кількість запитів до бази даних в конкретному сервісі, можна просто масштабувати базу даних для цього сервісу, не торкаючись інших компонентів архітектури. При цьому, можемо використовувати різні бази даних. Слід зазначити, що вказаних підхід також забезпечую відмовостійкість мікросервісів, оскільки дозволяю створити зручну та безпечну реплікацію даних мікросервіса. В залежності від прогнозованого навантаження на мікросервісну систему, засовуються такі види реплікацій: Master-slave, Multi-master, Sharding, Eventual consistency, кожна з яких має свої переваги та недоліки і потребує глибшого аналізу архітектури, тестування навантаження та бізнес вимог до даних користувача. Щодо

безпековою складової, всі мікросервіси повинні бути розгорнуті в Amazon Virtual Private Cloud (VPC) це дозволяє створити ізольовану віртуальну мережу, що зменшує ризики внутрішнього доступу до систем та збільшити безпеку даних, а також контролювати доступ до ресурсів забезпечуючи можливість налаштування мережевої інфраструктури на основі потреб користувачів. VPC інтегрується з іншими сервісами AWS, такими як Amazon EC2, Amazon RDS, Amazon EMR, Amazon Redshift та інші, що дозволяє забезпечити максимальну ефективність використання ресурсів. У якості CDN було вирішено використовувати Amazon CloudFront, це дозволяє швидко та ефективно доставляти контент до користувачів в будь-якій точці світу. Це допомагає покращити швидкість завантаження веб-сайтів, відео та інших елементів контенту, захищає від DDoS-атак та забезпечує захист конфіденційної інформації, при комунікації між сервером та користувачем за рахунок можливості використання SSL та HTTPS протоколів. Amazon API Gateway є важливим компонентом мікросервісної архітектури, оскільки дозволяє створювати та керувати API для мікросервісів, що забезпечує зручний спосіб доступу до інших додатків та сервісів. Додатково, API Gateway є інструментом який забезпечує моніторинг та аналітику використання API, що дозволяє керувати продуктивністю та оптимізувати витрати, робити прогнозування навантаження на мікросервіси використовуючи аналітичні дані.

Висновки. Використання мікросервісів дозволяє розділити бізнес-логіку на окремі складові, що спрощує розробку, тестування та підтримку системи. Кожен мікросервіс може бути розроблений та підтримуватись окремо, без впливу на роботу інших компонентів системи. Крім того, мікросервісна архітектура дозволяє розгортати нові функціональність швидко та без перерв у роботі системи, що дає можливість швидко реагувати на зміни вимог бізнесу. Використання мікросервісної архітектури та мови програмування Go дозволяє розробляти ефективні та гнучкі мікросервіси, що забезпечують високу продуктивність та масштабованість. Розробка мікросервісів з використанням мови програмування Go є сучасним вибором, оскільки ця мова має високу швидкодію, підтримку паралельної та асинхронної роботи та зручні засоби для розробки мікросервісів. Також розробка на Go, дозволяє інженерам менше концентруватися на написанні програмного кода, та приділяти більше уваги бізнес логіки при розробці мікросервісів, за рахунок простоти цієї мови програмування. .Таким чином, використання мікросервісів та мови програмування Go є перспективним напрямком для розробки сучасних та ефективних веб-додатків та маштабованих систем, де швидкість виконання та обробка великих пакетів даних має важливе значення.

Список використаних джерел

1. Sam Newman. Building Microservices, 2nd Edition. O'Reilly Media, August 2021 Inc. ст. 1-20
2. Як і для чого вивчати Golang. Переваги і недоліки мови. 02.02.2023. Режим доступу: https://dou.ua/forums/topic/41933/
3. TIOBE Index for March 2023. Режим доступу: https://www.tiobe.com/tiobe-index.
4. Tuan Nguen. Golang Performance Comparison | Why is GO Fast?. Режим доступу: https://www.golinuxcloud.com/golang-performance

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

ЗАСТОСУВАННЯ СЕРВЕРНИХ СЕРВІСІВ У РОЗРОБЦІ МОБІЛЬНИХ ДОДАТКІВ

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

У статті розглянуто основні засади побудови архітектури програмних продуктів. Зазначено переваги застосування серверних сервісів у розробці мобільних додатків. Як зразок розглянуто серверний сервіс «Firebase».

The article discusses the basic principles of building the architecture of software products. The advantages of using server services in the development of mobile applications are indicated. The server service «Firebase» is considered as an example.

Актуальність. Сьогодні, для більшості із нас, використання телефону не зводиться лише до звичайних дзвінків чи відправлення SMS повідомлень. В життя людини людини тісно увійшло таке поняття як Інтернет. Його роль тяжко переоцінити, оскільки Інтернет дає нам майже безмежні можливості. Так, завдяки ньому, ми можемо вільно займатися самоосвітою маючи доступ до різноманітних наукових статей, курсів чи відеороликів. А в часи епідемії Covid-19 Інтернет взагалі кардинально вплинув на навчальний процес в закладах освіти по всьому світу, надавши можливість дистанційно здобувати знання. Більшість банківських компаній усвідомили вагомий вплив мережі на збільшення кількості потенційних клієнтів та добавили до переліку власних послуг можливість проведення онлайн-платежів, завдяки чому тепер не потрібно витрачати час у багаточасових чергах банків, що економить дорогоцінний час для більш важливих цілей. Також, завдяки мережі, стало дійсним таке поняття як «негайне спілкування» – отримання повідомлень без значних затримок у часі.

Але всі вищеперераховані можливості так чи інакше вимагають від нас комунікації із віддаленими серверами, на яких зберігається інформація про ці статті, платежі чи повідомлення. Щогодини, щохвилини та щосекунди, при використанні чи то інтернет-банку, чи то онлайн-бібліотеки, між нашими пристроями та їх серверами здійснюється дуже велика кількість обмінів пакетами із інформацією. Будь-яка втрата інформації під час їх передачі чи в момент збереження може призвести до катастрофічних наслідків. Світові відомі випадки, коли через це великі компанії втрачали шалені гроші, а деякі навіть ставали банкротами.

Саме тому збереження цієї інформації та процес її безпечної передачі є одним із найважливіших аспектів будь-якого програмного забезпечення, що направлене на роботу з мережею.

Так, ще до появи серверних сервісів, розробникам додатків, незалежно від масштаба цього додатка та бюджету, доводилося з нуля самостійно пропрацьовувати усю логіку роботи цих серверів із інформацією. Це викликало масу незручностей.

Спочатку необхідно було оприділитися із самим сервером, де мають зберігатися дані. Ця проблема мала декілька варіантів вирішення. Перший – орендувати чужий сервер, що могло бути вкрай ненадійним через можливу нестабільність зі сторони орендодавця (наприклад неякісна підтримка інфраструктури серверів, що може спричинити до втрати даних), але перевагою є відсутність у потребі обслуговування зі сторони орендаря. Другий – створення та налаштування власного серверу. Вибір цього варіанту змушував компаній робити значні витрати як на купівлю, так і на обслуговування. Але показники надійності та безпеки даних значно покращувалися.

Іще однією незручністю стала необхідність у пошуку та наймі висококваліфікованого бекенд програміста, який і буде займатися розробкою логіки роботи серверу. На процес найму та розробки уходили як фінанси, та і час.

З плином часу поступово зростав попит на пошук більш ефективного рішення проблеми із серверами, адже хоча й великі компанії могли дозволити собі ці витрати, але середні та маленькі компанії уже мали проблеми на цьому етапі через обмеженість ресурсів бюджет та часу.

Таким чином, *метою даної статті* є дослідження особливостей використання серверних сервісів під час розробки програмного забезпечення, зокрема мобільних додатків, з метою прискорення процесу розробки, зменшення фінансових витрат та спрощення підтримки у майбутньому.

Об'єктом дослідження є впровадження серверної системи «Firebase» у мобільні додатки.

Предмет дослідження – серверні сервіси.

Виклад основного матеріалу. Оскільки мова йтиме про розробку, то для повноти розуміння всієї базової архітектури доцільно буде пригадати концепцію розбиття клієнт-сервер архітектури програмного забезпечення. Вона поділяється на back-end та front-end. Схематично взаємодію клієнта та цих двох частин можна представити так (Рис. 1).

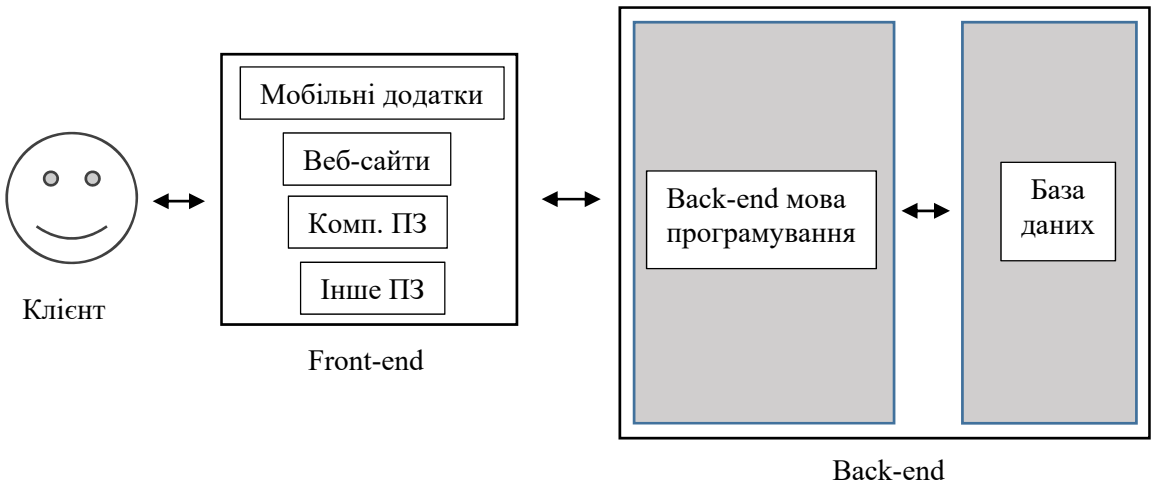

Рис. 1. Сегментація торгівлі

З рисунку вище можна зрозуміти, що користувач, не взаємодіє з сервером напряму, тобто інформація, перед тим як потрапити до клієнта, проходить процес «обробки». Цей процес відбувається в частині продукту, що зветься front-end. Інша назва front-end – сторона клієнта. Саме з нею відбувається взаємодій користувача у багатьох програмних застосунках. Основна задача front-end частини полягає у створенні зрозумілого для користувача UI (user interface), з яким, цей же користувач, матиме змогу взаємодіяти без проблем.

Якщо абстрагуватися від особливостей певних сфер бізнесу, то можна константувати, що причиною взаємодії користувача з front-end частиною є отримання інформації, її редагування, видалення чи додавання у сховище.

Згадайте будь-який сучасний мессенджер, відправляючи комусь повідомлення, Ви несвідомо добавляєте його вміст(разом з іншими метаданими) у спеціальне сховище даних. Потім пристрій одержувача цього повідомлення просто зчитує цю інформацію зі сховища. Це лише приклад із однієї галузі. Розглянемо інший – онлайн-замовлення квитка для подорожі у туроператора. Після його придбання, дані, що були вказані Вами при купівлі, добавляються в базу, після чого, по ним, в разі необхідності підтвердження, можуть

зателефонувати представники компанії туроператора. І в разі підтвердження, статус(що іноді може бути навіть одним полем у таблиці сховища) зміниться. Таким чином, ці приклади демонструють, що навіть при умові великої різниці між сферами бізнесу, їх алгоритм роботи з даними, якщо, знову ж таки, звести до примітивних функцій, майже однаковий.

В ролі клієнтської сторони інтерфейсом можуть виступати веб-сайти, комп'ютерне програмне забезпечення і навіть консоль. Оскільки мова у статті йтиме про мобільну розробку, то тут роль сторони клієнта відіграють мобільні додатки, які можна вільно скачати(або придбати) у Google Play чи Apple Store, що залежності від системи.

Отже, саме завдяки стороні клієнта користувач може працювати з даними через інтерфейс. Але необхідно розуміти, що якщо є сторона, яка робить запити на отримання даних(front-end), то є і сторона, що відповідає на ці запити. За виконання цього завдання відповідає back-end.

Back-end – це внутрішня частина сервісу, що є прихованою від ока звичайного користувача і працює віддалено на сервері, незалежно від самого додатку. Тому цю частину називають «серверна сторона». Саме у бекенді основний принцип роботи заключається у своєчасному реагуванні на запити зі сторони клієнта – відправка або прийом для обробки та збереження пакетів із даними. Крім цього, у список задач серверної сторони також входить слідкування за тим, щоб ці дані завжди залишалися в безпеці та були доступними лише тим, хто має на це право.

Так, отримавши базове представлення про слої архітектури програмного продукту, перейдемо до розгляду серверних сервісів.

Як вже зазначалося – раніше, до появи серверних сервісів, серверна сторона(back-end) та логіка роботи з даними мали майже завжди розроблялася з нуля, що створювало значні фінансові та часові проблеми для представників малого та середнього бізнесу. Але після появи серверних сервісів картина змінилася на краще.

Серверні сервіси (Backend as a Service, скорочено BaaS) являють собою модель хмарного сервісу, що включає в себе певний, зазделегідь уже реалізованих комплекс рішень. Це зветься сервісом через те, що є сторонній постачальник, який надає серверні послуги, і є клієнти, які використовують ці послуги для розробки та запуску власних додатків.

Переваги використання Backend as a Service:

- Однією із головних переваг є *налаштовуваний та готовий набір функцій back-end.* Послуги серверної сторони надаються через набір API(Application Programming Interface – інтерфейс для обміну даними) та SDK(Software Developer Kit – набір готових інструментів для розробника), які можуть бути використаними у коді програмного продукту. Це означає, що більше немає необхідності в написанні власного коду для back-end, оскільки цей код уже написаний до вас так, щоб його можна було підлаштувати під усі типові потреби бізнесу. Тому розробникам і представникам бізнес сфери вдається заощадити дорогоцінні фінанси та час, разом з цим перенаправити витратити цих ресурсів на експеременти із покращенням користувальницького досвіду, на покращення клієнтської сторони(front-end) загалом;
- *Вбудовані бази даних.* Зазвичай, разом із готовим бекендом, постачальники серверних сервісів включають у перелік власних послуг і можливість створення баз даних. Доступ до них, знову ж таки, надається через API та SDK;
- *Легка масштабованість.* Якщо додаток швидко розвивається(наприклад збільшення клієнтської бази), то в такому випадку на поміч приходить масштабування, яке зроблене таким чином, щоб в будь-який момент ви могли збільшити чи то місткість баз даних, чи то набір необхідного функціоналу;
- Наявність *інструментів аналітики*, що дозволяють відслідковувати стан роботи програмного забезпечення чи поведінку користувачів у ньому;

- Постачальники BaaS також часто пропонують послуги щодо готової реалізації *аутентифікації* з широким набором можливостей. Перша за все, це створення та редагуванні облікових записів користувачів, перевірка їх електронних скриньок та забезпечення безпеки акаунту паролем;
- *Забезпечення безпеки даних*. По-перше, сервера BaaS, зокрема найбільш популярних постачальників, знаходяться в добре захищених місцях, зводячи до мінімуму можливість витоку закритої інформації, а по-друге, сервера BaaS спрощують використання GDPR (стандарт ЄС, який вимагає від компаній встановити надійний захист персональних даних користувачів в Інтернеті), оскільки надають різноманітні попередньо створені функції для численних випадків безпеки;

Звісно що BaaS має і певний перелік мінусів:

- Використання такого рішення не буде на безкоштовній основі. Оскільки клієнт виступає в ролі орендатора, то йому, в залежності від постачальника BaaS, необхідно щотижня, щомісяця чи щотижня виконувати плату за послуги. Але тут варто зробити примітку, що ця плата все одно буде ніщо в порівнянні з платою за створення серверу з нуля;
- Бізнес з унікальною моделлю та функціоналом може не підійти BaaS через його направленість на більш типові моделі;
- Постійна прив’язаність до постачальника серверних послуг. У разі переходу з однієї платформи серверних рішень на іншу може виникнути купа проблем. В першу чергу це стосується експорту даних;
- Менший контроль за кодом. Налаштування кожної дрібниці бекенду просто не є можливим;

Завдяки усім цим перевагам та мінусам, BaaS є чудовим вибором для малого та середнього бізнесу. А особливо, через кардинальне зменшення витрат часу на розробку, в нагоді воно стане при розробці MVP(мінімально життєздатного продукту).

Серверні сервіси з’явилися відносно недавно, проте уже доволі успішно конкурують із методом написання серверної частини з нуля (іншою назвою цього методу є «Custom Back-end»). Так, відповідно до результатів досліджень ринку(Рис. 2) компанією Zion [1], станом на 2022-й рік, дохід від BaaS становив $3,0 більйон, а прогноз на 2030-й рік більше, аніж вдвічі перевищує 2022-й, що характеризує розвиток та попит на використання цієї технології як успішний та стрімкий.

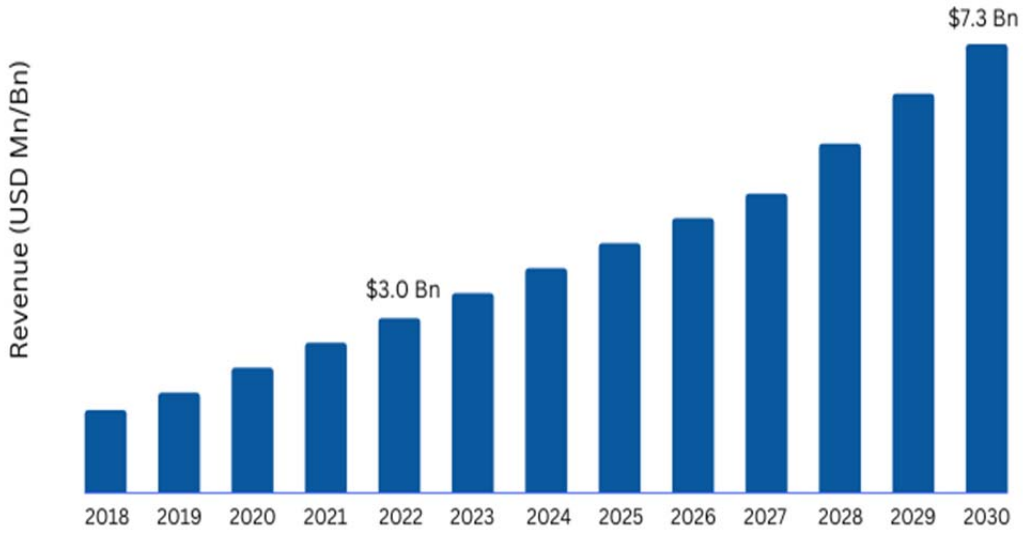

Рис. 2. Розмір ринку BaaS

Що стосується розробки саме мобільних додатків, то тут, задля економії ресурсів під час розробки серверної сторони, може бути використане більш вузьконаправлене серверне рішення – MBaaS(Mobile Back-end as a Service), хоча це не завжди є так. MBaaS дозволяє швидко інтегрувати Ваші мобільні програми з даними та функціями в захищене серверне хмарне сховище. Принцип роботи та набір інструментарію майже один і той самий що і в BaaS, проте більш орієнтований на мобільні пристрої.

Сьогодні на ринку є багато компаній, які надають Baas послуги, найбільш популярними платформами є Firebase, AWS, Supabase, Appwrite, Nhost. Але, через велику кількість позитивних відгуків, надійності, розглянемо платформу під назвою «Firebase». Ця платформа розпочала свій шлях у світ IT 2012-го року, надаючи спочатку послуги баз даних у реальному часі, а потім була придбана корпорацією Google. З тих пір Google став відповідальним за розвиток Firebase. Отримуючи все більше і більше функцій, ця платформа повноцінно перетворилася у постачальника серверних сервісів.

На даний момент Firebase має близько 18 функцій, що допомагають зі створення бекенду для різноманітних програм. В першу чергу це стосується мобільних додатків, але є можливість під'єднання сайтів, комп'ютерних програм і тд. Через це Firebase називають BaaS, а не MBaaS платформою.

Щодо функціоналу[2] – він доволі різноманітний та включає в себе багато корисних інструментів, тому розглянемо основні:

- *Бази даних у реальному часі (Firebase Realtime Database)*. Типова взаємодія зі звичайними базами даних заключається у відправці запитів та отримання інформації і у випадку її зміни – робити запит знову для оновлення. Але база даних у реальному часі має трохи інший спосіб взаємодій. Цей спосіб полягає в тому, що всі підключені до цієї бази клієнти, незалежно від додатку чи платформи, мають єдиний екземпляр даних, а ці дані завжди є актуальними та оновлюються автоматично у всіх клієнтів при зміні цих даних;
- *Firebase Authentication*. Вбудовані можливості для швидкого створення безпечної аутентифікації користувачів. Наявна підтримка авторизації через електронну пошту та пароль, номер телефону, Google, Twitter, Facebook і багато інших соціальних мереж;
- *Cloud Storage* – зручний інструмент для зберігання файлів користувачів. Крім цього, завдяки Firebase Authentication SDK, можна здійснювати контроль доступу до цих файлів на основі даних користувачів;
- *Cloud Functions*. Створення власних функцій для бекенду, що покликано задля розширення функціоналу Firebase платформи. Принцип їх роботи полягає в реагуванні на певні події в серверному сервісі, наприклад якщо користувач завантажить файл в Cloud Storage, то ім'я файлу запишеться в якусь окрему базу даних. Важливо, на що реагувати і як визначає сам розробник та бізнес задачі, а не платформа;
- *Hosting*. На перший погляд є звичайним хостингом для сайтів та веб-додатків, але може мати майже увесь функціонал Firebase(включаючи авторизацію, бази даних у реальному часі, функції і тд.);

Як можна помітити, практично усі функції Firebase взаємодіють один з одним. Це і робить дану платформу потужною та ефективною з точки зору економії фінансів та часу.

Щоб почати застосування BaaS сервісів, зокрема Firebase, у мобільній розробці, необхідно пройти декілька етапів. В приклад візьмемо уже реалізований додаток на операційній системі Android [3].

Проходження першого етапу зводиться до налаштування самого мобільного додатку таким чином, щоб він відповідав мінімальним вимогам Firebase, для Android – це версія 4.4, а рівень API – 19.

Переконавшись в тому, що додаток відповідає вимогам вище, необхідно перейти на сайт та створити новий проект в Firebase (Рис. 3) вказуючи ім'я в першому кроці та налаштовуючи інструменти аналітики в другому.

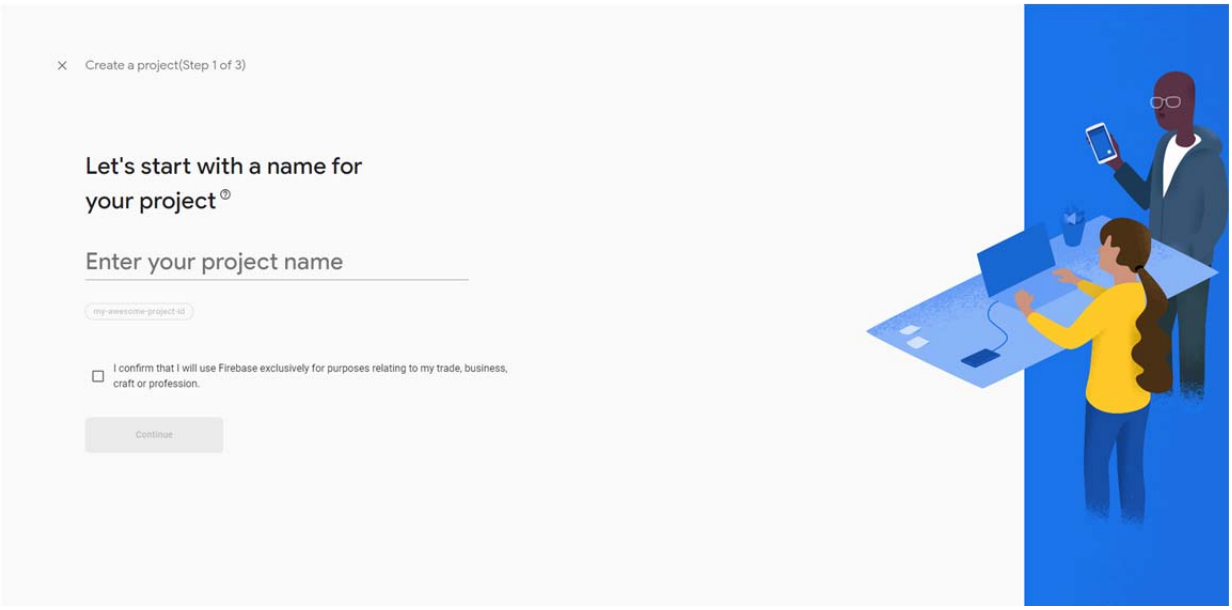

Рис. 3. Створення проекту в Firebase

Як тільки проект буде успішно створено, то за допомогою сайту та спеціального файлу налаштування, є можливість додати Android додаток в нього. В цих файлах містяться необхідні для поєднання з проектом дані. Поєднавши додаток з проектом, залишається лише додати в залежності від мобільного додатку Firebase SDK, який і дасть можливість використовувати функціонал Firebase в мобільному додатку.

Застосування серверних сервісів у розробці мобільних додатків є важливим етапом для забезпечення якості та функціональності програмного продукту. Вони дозволяють розділити логіку та оптимізувати взаємодію між клієнтом та сервером, забезпечити безпеку даних та покращити продуктивність. Незважаючи на виклики, пов’язані з впровадженням та підтримкою серверних сервісів, їхні переваги у значній мірі сприяють покращенню якості мобільних додатків та задоволенню потреб користувачів.

Висновки. Сфера розробки програмного забезпечення ніколи не стоїть на місці. Майже щодня перед розробниками постають нові виклики щодо вирішення задач по вибору найбільш зручної, а головне – ефективної архітектури для того чи іншого програмного продукту. Таким чином на світ з’явилися серверні сервіси. Завдяки набору готових рішень, час, що витрачається на розробку бекенду мобільних (і не лише) додатків, значно зменшився, що дало шанс середньому та малому сегменту бізнесу на існування та конкурування з більшим.

Список використаних джерел

1. Cloud Mobile Backend as a Service (BaaS) Market Size, Share 2030 \\ Режим доступу: https://www.zionmarketresearch.com/report/cloud-mobile-backend-as-a-service-market (останнє звернення 04.04.2023р.)
2. Firebase Products \\ Режим доступу: https://firebase.google.com/products-build (останнє звернення 04.04.2023р.)
3. Add Firebase to your Android project \\ Режим доступу: https://firebase.google.com/docs/android/setup (останнє звернення 04.04.2023р.)

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

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

ШАБАЛІН Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто криптографічні методи захисту електронних документів, зокрема, використання електронного цифрового підпису (ЕЦП) як токену аутентифікації для захисту електронних документів. Автор статті проаналізував різноманітні методи захисту електронних документів та визначили переваги використання ЕЦП як ефективного засобу захисту.

The article discusses cryptographic methods for protecting electronic documents, including the use of an electronic digital signature (EDS) as an authentication token for securing electronic documents. The author of the article analyzed various methods of protecting electronic documents and identified the advantages of using EDS as an effective means of protection.

Актуальність. У сучасному світі все більше ділових та повсякденних операцій відбуваються в електронному вигляді, що збільшує ризики втрати даних, витоків конфіденційної інформації та крадіжки електронних документів. Захист електронних документів є надзвичайно важливою та актуальною темою, яка потребує уваги і досліджень. У зв'язку з цим, криптографічні методи захисту електронних документів є надзвичайно важливою темою досліджень в сфері інформаційної безпеки. Один з найбільш ефективних криптографічних методів захисту є використання електронного цифрового підпису (ЕЦП) як токену аутентифікації для захисту електронних документів.

Оскільки ЕЦП є ефективним засобом захисту електронних документів, наукові дослідження в цьому напрямку мають велику вагу та значення. Такі дослідження необхідні для розробки нових інноваційних методів захисту електронних документів з використанням ЕЦП, а також для удосконалення наявних методів та розробки рекомендацій з їх використання.

Однак, збільшення кількості електронних документів також призводить до збільшення кількості кібератак та крадіжок інформації. Використання ЕЦП як токену аутентифікації може допомогти забезпечити високий рівень захисту електронних документів та знизити ризики їхньої крадіжки або несанкціонованого доступу до них.

Метою статті є дослідження криптографічних методів захисту електронних документів. У статті проаналізовано сучасні методи захисту електронних документів, виявлені їхні недоліки та переваги, а також розглянуті можливості використання ЕЦП для захисту електронних документів. Дослідження базується на теоретичних аспектах криптографії та реалізації технологій захисту даних.

Об'єктом дослідження є криптографічні методи захисту електронних документів, зосередження уваги на використанні електронного цифрового підпису (ЕЦП) як токену аутентифікації для захисту електронних документів.

Предмет дослідження – криптографічних методів захисту.

Аналіз попередніх досліджень. Аналізуючи попередні дослідження з проблематики захисту електронних документів, було виявлено, що українські дослідники та експерти проявляли значний інтерес до криптографічних методів захисту електронних документів. У статтях були проаналізовані основні методи захисту даних в електронному документообігу та виявлені їх переваги та недоліки. Присвячені праці вітчизняних науковців: Я.О. Іващенка та І. В. Бубнової, О. В. Кравця та інших.

Виклад основного матеріалу. В умовах сьогодення, коли електронні документи стають все більш поширеними, захист цих документів від несанкціонованого доступу та

зловживань є дуже важливим завданням. Криптографічні методи захисту є одними з найбільш ефективних методів забезпечення безпеки електронних документів. Одним із найбільш важливих криптографічних методів захисту є електронний цифровий підпис (ЕЦП). ЕЦП використовується для аутентифікації документу та автора документу, а також для забезпечення цілісності даних, тобто захисту від їхньої модифікації без належних дозволів. Використання ЕЦП дозволяє забезпечити відповідність електронних документів законодавству та міжнародним стандартам. Щоб використовувати ЕЦП для захисту електронних документів, необхідно мати токен або смарт-карту, на яких зберігається особистий ключ підписувача. Токен або смарт-карта (рис. 1) забезпечують безпеку ключа підписувача та дозволяють уникнути несанкціонованого доступу до ключа [1].

Рис. 1. Ілюстрація цифрового підпису даних

Таким чином, необхідно враховувати те, що ЕЦП може бути підробленим, якщо ключ підписувача стає відомим зловмисникам. Тому важливо забезпечити належний захист токена або смарт-карти, на яких зберігається ключ підписувача. Загалом, використання ЕЦП є ефективним методом захисту електронних документів. Однак, для забезпечення належної безпеки, необхідно дотримуватись правил зберігання та використання токена або смарт-карти з ключем підписувача.

Розглянемо застосування ЕЦП як токену аутентифікації для захисту електронних документів. ЕЦП є цифровим підписом, який дає можливість підтверджувати автентичність та цілісність електронного документа. Для цього використовується криптографічний ключ, який є відомим лише власнику підпису та призначений для створення та перевірки підпису. Серед ключових переваг застосування ЕЦП є можливість перевірки автентичності та цілісності документа. Це забезпечує відсутність можливості зміни документа без зміни його ЕЦП. Крім того, ЕЦП може бути використаний як токен аутентифікації, що дає можливість підтверджувати автентичність власника підпису [2].

Використання ЕЦП як токену аутентифікації може бути особливо корисним в електронній комерції та банківській сфері, де важливо захистити конфіденційні дані та транзакції. В таких випадках, використання ЕЦП забезпечує високий рівень захисту даних від несанкціонованого доступу та зміни.

Для використання ЕЦП як токену аутентифікації необхідно виконати наступні кроки:

1. Створити ЕЦП для документа, що підписується.

2. Зберегти ЕЦП разом з ідентифікаційними даними власника підпису.
3. Перевірити ЕЦП при кожній спробі доступу до документа.

При цьому, необхідно використовувати безпечний канал передачі даних для збереження конфіденційності інформації. Також важливо забезпечити надійність та захист від небажаного доступу до документів під час їх зберігання на електронних носіях.

В роздрібній торгівлі застосовуються три класи інформаційно-управляючих систем.

До ефективних методів захисту електронних документів належить використання електронних цифрових підписів (ЕЦП) як токену аутентифікації. ЕЦП забезпечує ідентифікацію власника документу та його цілісність, тобто відсутність змін у документі після підписування. Крім того, ЕЦП може використовуватися для забезпечення нерепудіації, тобто неможливості відмовитися від підпису, що був накладений на документ. Для досягнення максимальної ефективності при використанні ЕЦП необхідно мати відповідні знання і навички в галузі криптографії та інформаційної безпеки. Також потрібно мати доступ до відповідної інфраструктури, яка забезпечить надійність та безпеку процесу підписування документів. Серед ключових етапів при використанні ЕЦП є генерація ключів. Для генерації ключів використовуються криптографічні алгоритми, які забезпечують надійність та безпеку ключів (рис.2). Після генерації ключів, користувач повинен зберегти їх у безпечному місці, а також забезпечити їх захист від несанкціонованого доступу [3].

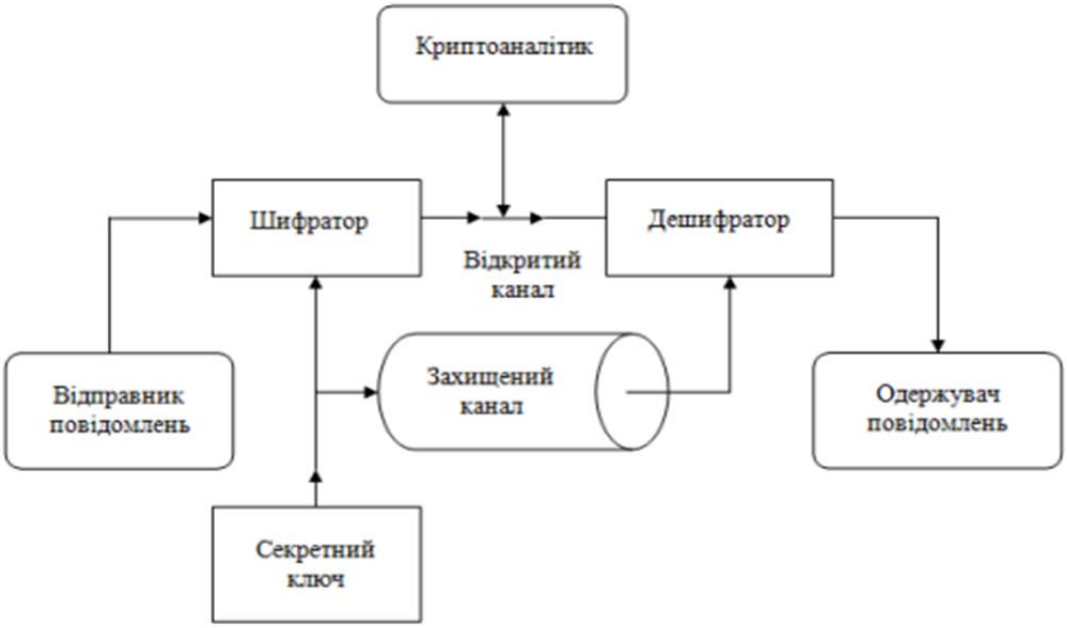

Рис. 2. Схема криптосистеми з таємним ключем

Після генерації ключів, користувач може використовувати ЕЦП для підписування електронних документів. Для цього необхідно вибрати потрібний документ та обрати опцію «підписати». Система згенерує хеш-код документу та зашифрує його за допомогою приватного ключа користувача. Далі цифровий підпис додається до документу. Із переваг використання ЕЦП для підписування документів є можливість перевірки автентичності та цілісності документу. Оскільки підпис створюється з використанням приватного ключа, який відомий лише власнику, то будь-які зміни в документі призведуть до недійсності підпису. Таким чином, використання ЕЦП забезпечує захист від будь-яких спроб підробки документа.

Наступним етапом є перевірка підпису. Для цього необхідно відкрити підписаний документ та вибрати опцію «перевірити підпис». Система автоматично розшифрує хеш-код документу за допомогою відкритого ключа користувача, який міститься у сертифікаті. Далі порівнюється розшифрований хеш-код з хеш-кодом самого документу. Якщо дані

співпадають, то підпис вважається дійсним, а документ – автентичним та цілим. У зв'язку з використанням ЕЦП, як токену аутентифікації, забезпечується захист електронних документів від несанкціонованого доступу та підробки. Проте, необхідно дотримуватись правильної процедури збереження ключів та використання безпечного каналу передачі даних для забезпечення конфіденційності.

Для забезпечення максимальної ефективності та надійності захисту електронних документів, необхідно дотримуватись правильної процедури збереження ключів. Ключі повинні зберігатись в надійному місці, що захищене від несанкціонованого доступу, наприклад, в безпечній зоні з обмеженим доступом або на криптографічному токені.

Крім того, використання безпечного каналу передачі даних є обов'язковим для забезпечення конфіденційності інформації, що передається при використанні ЕЦП. Для цього можуть використовуватись різні технології, такі як SSL / TLS або VPN, що забезпечують шифрування даних та захист від несанкціонованого доступу. Загальна ідея використання криптографічних методів захисту електронних документів полягає у забезпеченні конфіденційності, цілісності та доступності інформації, що міститься в них. Використання електронних документів зросло в останні роки, тому необхідно забезпечувати їх захист від різних загроз.

В умовах розвитку інформаційних технологій, все більше урядових структур переходять до електронної форми обміну документами. При цьому, дуже важливо забезпечити безпеку передачі і зберігання цих документів. Одним із ефективних способів є використання ЕЦП для підпису документів. Це дозволяє забезпечити конфіденційність, цілісність та автентичність даних. Переваги методу використання ЕЦП в контексті електронної адміністрації можуть включати аналіз ефективності та швидкості передачі даних з використанням ЕЦП порівняно з іншими методами захисту, а також оцінку ефективності методу в захисті від атак на систему електронної адміністрації, таких як перехоплення даних, відмова в обслуговуванні тощо.

Отже, переваги використання ЕЦП в контексті електронної адміністрації можуть бути наступними:

- *Забезпечення безпеки електронних документів:* за допомогою ЕЦП можна переконатись у тому, що електронний документ був підписаний конкретним користувачем і не був змінений після підписання.
- *Зручність та ефективність:* використання ЕЦП дозволяє зменшити час та витрати, пов'язані з підписанням паперових документів, та забезпечити більш швидке та ефективне обмін документами між учасниками.
- *Екологічність:* використання ЕЦП дозволяє зменшити кількість паперових документів, що зберігаються в офісі, та зменшити екологічний вплив на довкілля.

Прикладом успішного використання ЕЦП в контексті електронної адміністрації може служити впровадження Електронного митного декларування в Україні. За допомогою ЕЦП, митники можуть підписувати електронні митні декларації та інші документи, що забезпечує їх автентичність та недоступність для несанкціонованого доступу. Це дозволило зменшити час, витрати та помилки в процесі декларування товарів, що сприяє зростанню ефективності роботи митниці та підвищенню якості послуг, які надаються учасникам зовнішньоекономічної діяльності [4].

У порівнянні з іншими криптографічними методами, наприклад, паролями, ЕЦП має перевагу в тому, що воно не може бути відновлено або вгадано. Крім того, ЕЦП може бути використаний для автоматизації процесів, що зменшує кількість помилок, що можуть статися через людський фактор. До прикладу використання ЕЦП можна віднести систему декларування майна, яка була запроваджена в Україні в 2016 році. За допомогою ЕЦП громадяни можуть подавати декларації про своє майно та доходи онлайн, що забезпечує надійний захист даних та зменшує кількість помилок при їх заповненні. Також ця система зменшує корупцію, оскільки прозорість у веденні реєстру майна дозволяє контролювати доходи та майно посадових осіб.

У контексті електронного бізнесу використання ЕЦП має також свої переваги. Однією з них є можливість підписання електронних договорів, що дає можливість юридично оформляти угоди в онлайн-режимі. Це дозволяє економити час та зменшувати витрати на організацію зустрічей для підписання паперових документів. Крім того, використання ЕЦП забезпечує захист інтелектуальної власності, оскільки воно дозволяє встановлювати авторства електронних документів та підтверджувати їхню автентичність. За допомогою ЕЦП також можна забезпечувати безпеку платежів у електронному форматі, оскільки він гарантує, що платіжні дані не будуть змінені під час передачі та що транзакція буде здійснена від імені вірного платника [5].

Для прикладу, можна вказати, що в банківському секторі використовуються ЕЦП для забезпечення безпеки платежів та фінансової звітності [6]. Крім того, ЕЦП використовується в інтернет-магазинах для підтвердження автентичності замовлень та документів, а також для забезпечення безпеки транзакцій. Таким чином, використання ЕЦП у електронному бізнесі забезпечує безпеку та автентичність електронних документів та транзакцій, дозволяє економити час та зменшувати витрати на їхню організацію, а також сприяє захисту інтелектуальної власності.

Висновки. Запровадження ЕЦП як методу захисту електронних документів дозволяє забезпечити високий рівень безпеки та автентифікації в електронному середовищі. Цей метод має безліч переваг перед іншими криптографічними методами захисту електронних документів. Наприклад, забезпечення конфіденційності даних, підтвердження автентичності та цілісності документу, захист від несанкціонованого доступу до даних.

Крім того, використання ЕЦП має великий потенціал для застосування в електронній адміністрації. Наприклад, в Україні вже успішно використовується система ЕЦП для забезпечення автентифікації та захисту електронних документів в державних органах. Це дозволило покращити ефективність та швидкість процесів, а також зменшити кількість паперової роботи. Використання ЕЦП як методу захисту електронних документів є важливим елементом в електронній адміністрації та має безліч переваг перед іншими криптографічними методами. Його використання дозволяє забезпечити безпеку та конфіденційність даних, а також зменшити час та затрати на обробку електронних документів.

Список використаних джерел

1. Рагога Д.І. Електронний цифровий підпис у документах. – Наукові праці Донецького національного університету імені Василя Стуса. – 2021. – С. 50-56.
2. Перепелиця. Л.С. Методи та засоби автентифікації користувачів в інформаційно-телекомунікаційних системах та вироблення рекомендацій щодо підвищення їх ефективності. Наукові праці Державного університет телекомунікацій Київ. – 2022. – С. 76-80.
3. Глинчук Л.Я. Криптологія. Луцьк. Східноєвропейський національний університет імені Лесі Українки. Вежа-Друк 2014. – С. 182-186.
4. Державний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічні захист електронної інформації. Електронний цифровий підпис. Вимоги до створення, використання та перевірки.
5. Регламент ЄС 910/2014 від 23 липня 2014 року про електронний ідентифікаційний та послуги довіри для електронних транзакцій на внутрішньому ринку і відмінення директиви 1999/93/ЄС.
6. Глєбова Н. В. Електронний цифровий підпис: обліковий та податковий аспекти. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. – 2018. – С. 94-97.

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т. В.

СПОСОБИ МІНІМІЗАЦІЇ РИЗИКІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ У МІЖНАРОДНІЙ ЛОГІСТИЦІ

ШАПОЧНІКОВА А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні способи зниження ризиків несанкціонованого доступу та забезпечення захисту персональних даних від витоку в міжнародній логістиці. Виокремлено Ransomwar, як найбільш розповсюджена вірусна активність в організації. Зазначено забезпечення безпеки даних і захисту в логістичній галузі від кібератак. Розглянуто як зразок морський сектор в міжнародній логістиці та найефективніший спосіб підготовки до захисту від несанкціонованого доступу.

The article examines the main ways to reduce the risks of unauthorized access and how to ensure the protection of personal data from leakage in international logistics. Ransomware is highlighted as the most viral activity in an organization. The article discusses securing data and protection in the logistics industry against cyber attacks. The maritime sector in international logistics is considered as an example, along with the most effective way to prepare for protection against unauthorized access.

Актуальність. Останні декілька років міжнародна логістика все більше страждає від кібератак. Кожна логістична компанія піддається на внутрішні та зовнішні ризики, пов'язані з перебоями в ланцюжках поставок. Найбільш кібератаки зросли після початку пандемії COVID-19 та на початку повномасштабного російського вторгнення. Логістика в Україні стала однією з перших для цілей кіберзлочинців після російського вторгнення, масштабною кібератакою на логістику, енергетику, державну владу тощо.

Про один з прикладів кібератак у логістичній галузі, в жовтні 2022 році, Microsoft повідомила про кібератаку на підприємства логістичного сектору України та Польщі. Відомо, що кіберзлочинці попередньо отримали доступ до прав адміністратора мережі. Також, Microsoft зазначає, що нове ПЗ-вимагача під назвою «Prestige» збігаються з жертвами іншої кібератаки, ця мета атаки була спрямована на знищення даних. Зазначається, що на початку повномасштабного російського вторгнення програма-вимагача Prestige ransomware, вразила сотні комп'ютерів в Україні, Литві та Латвії. Це тип шкідливого програмного забезпечення, який блокує доступ до файлів або IT-систем організації [1].

Глобальна інтеграція ланцюгів постачання призвела до надзвичайно високого рівня ризику для третіх сторін. Національний інститут стандартів і технологій (NIST), зазначає сторонні сховища є потенційними векторами атак. Зокрема, логістичні організації, щоб забезпечити безперервність роботи своїх систем, переносять робочі потужності на хмарні платформи та використовують хмарні сервіси. Наприклад, зараз транспортна галузь надає перевагу відстеженню вантажів, які вона перевозить, і зберігає дані своїх власників у хмарі за допомогою Інтернету речей.

Intel 471 зазначає, що виявив різних кіберзлочинців, які мають доступ до мережі, які продають облікові дані, належать до логістичних компаній. Це вже можлива криза кібербезпеки в ланцюжку постачання матиме дуже поганий вплив на глобальну споживчу економіку. Кіберзлочинці стверджують, що отримали облікові дані через уразливості рішень віддаленого доступу.

Метою статті є дослідити способи зниження ризиків при несанкціонованому доступі, яка допоможе захистити персональні дані в логістичному секторі.

Об'єктом дослідження є система мінімізації ризиків несанкціонованого доступу до персональних даних.

Предмет дослідження – система захисту персональних даних.

Виклад основного матеріалу. Аналізуючи світову статистику нападів, Microsoft визначає, що всього за один рік лише масштаб атак на паролі до облікових записів працівників організацій зріс на 74% – до понад 920 випадків на секунду. Як вже було зафіксовано організації стикаються із підвищенням активності вірусів-вимагачів або ж шифрувальників (англ. – Ransomware), які впливають на персональні дані. Атака може призвести до втрати своєчасного доступу до персональних даних, якщо немає відповідних резервних копій. Це завдавало шкоди логістичному сектору по всьому світу в 2022 році:

- програмне забезпечення-вимагач було використано в серії атак, націлених на сектори транспорту та логістики в Україні та Польщі. Група зберігала доступ до жовтня, Microsoft вже зазначала, що група, яка стоїть за атаками, отримала високий рівень доступу до цільових мереж досі невідомими засобами. Також, компанія «сигналізує про підвищений ризик для організацій, які безпосередньо постачають чи транспортують гуманітарну чи військову допомогу в Україну».
- лютий 2022-го року кібератака на дві логістичні компанії вплинула на системи обробки платежів сотень автозаправних станцій на півночі Німеччини;
- березень, атака на поштову службу Греції тимчасово перервала її роботу та призупинила обробку фінансових транзакцій;
- травень, напад хакерів спричинив затримки та скасування рейсів однієї з найбільших авіакомпаній Індії, перервавши поїздки сотень пасажирів.

Агентство Європейського Союзу з кібербезпеки (ENISA), зазначає про Ransomware, як головну загрозу кібербезпеки, оскільки кіберзлочинці дуже мотивуються з отримання персональних даних.

Розвиток технологій, що використовуються в операційній частині логістичного сектору, полегшує роботу працівників у віддаленій співпраці. Віддалені процеси – це сеанси, які відбуваються з незахищеним і незахищеним віддаленим з'єднанням, іноді протягом днів, іноді тижнів, залежно від тривалості міграції, і можуть зробити систему вразливою до атак програм-вимагачів.

В логістичному секторі для мінімізації витоку персональних даних потрібно забезпечити віддалений доступ і сегментація мережі, для забезпечення безпеки даних і захисту компанії від кібератак, такі як:

- програма інформування про кібербезпеку;
- принцип найменших привілеїв (POLP);
- використання багатофакторної автентифікації (MFA) та застосування політики надійних паролів;
- фізична охорона;
- підтримка програмного забезпечення в актуальному стані, щоб запобігати вразливостям системи безпеки;
- інвестувати в програми кібербезпеки та часто створювати резервні копії файлів у хмарі, щоб захистити їх від програм-вимагачів.

Програма інформування про кібербезпеку – це навчання співробітників компанії усвідомленню кіберзагроз, оскільки людський фактор в більшості випадків це і є загроза для організації. Інституції, які працюють у логістичній галузі, погоджуються, що захист критичної інфраструктури пов'язаний із безпекою систем, які безпосередньо стежать за процесами в логістиці. Люди, які працюють у секторі критичної інфраструктури, повинні бути обізнані про політику захисту даних компанії та відповідні закони та нормативні акти, тримаючись у курсі подій за допомогою тренінгів і семінарів. Співробітники в міжнародній логістичній компанії, які мають більш глибоку участь в обробці даних – наприклад, у зборі потенційних клієнтів, підтримці та зберіганні бази даних співробітників, а також передачі

персональних даних третім особам для звітності чи операцій – отримають додаткове навчання з правил захисту, що стосуються їхньої конкретної посадової функції. Той факт, що багато інцидентів із безпекою та конфіденційністю, які з'являються в новинах, пов'язані з помилками людини, щоб знизити ризики несанкціонованого доступу до персональних даних.

Визначення принципу найменших привілеїв – половина організацій мають користувачів із більшими правами доступу, ніж це необхідно для виконання їхньої роботи. Підхід POLP спрямований на регулярний аудит внутрішніх привілеїв доступу користувачів, щоб забезпечити мінімально необхідний рівень доступу до даних, систем, мереж і пристроїв, щоб особа могла виконувати свої основні обов'язки.

Багатофакторна автентифікація (Multi-factor authentication) може зупинити неавторизований доступ, що часто виникає через один зламаний пароль чи облікові дані. Наприклад, можна вгадати чи зламати пароль, проте, нелегітимний доступ важче отримати до вторинної (чи третинної) форми перевірки особи. Слід зазначити, за результатами Microsoft Multi-factor authentication допоможе запобігти 99,9% зламаних облікових записів користувачів.

Політика надійних паролів є одним із найкращих засобів захисту від несанкціонованого доступу. Це означає розробку та впровадження політики надійних паролів, яка вимагатиме від усіх користувачів дотримання встановлених найкращих практик щодо створення та регулярної зміни надійних паролів, а також забезпечення повторного використання паролів на різних пристроях, програмах чи інших облікових записах, використовуючи менеджер паролів, що являє собою зашифроване цифрове сховище, яке зберігає безпечні паролі для входу в облікові записи на пристроях, веб-сайтів та інших служб.

Фізична охорона. Незалежно від того, чи це внутрішній зловмисник, чи зовнішній зловмисник, який відвідує робоче місце, залишаючи пристрої розблокованими або записані паролі чітко видимими, є простим рецептом для несанкціонованого доступу.

Підтримка програмного забезпечення в актуальному стані. Кіберзлочинці часто отримують несанкціонований доступ через відомі вразливості. Потрібно регулярно оновлювати все програмне забезпечення, постійно оновлювати виправлення безпеки та встановлювати автоматичні оновлення безпеки, коли це можливо, щоб знизити ризик несанкціонованого доступу до персональних даних в організації.

Інвестування в програми кібербезпеки та *створення резервних копій файлів у хмарі*, щоб захистити їх від програм-вимагачів. З розвитком технологій сектору логістики кількість користувачів і додатків, які отримують доступ до даних, включених у процес закупівлі, зсередини організації та віддалено також зросла. Є доступ до хмарних даних багатьох привілейованих і адміністративних облікових записів, від допоміжного персоналу до обслуговуючого персоналу, від віддалених постачальників до корпоративних і колективних додатків, щоб підтримувати його ефективну роботу. Зростаюча кількість привілейованих облікових записів ускладнює керування цими обліковими записами та робить їхні системи керування відкритою мішенню для кіберзлочинців.

Пристрої IoT відіграють важливу роль у цифровій трансформації логістичної галузі. Програми Database Access Manager та Privilege Task Automation, можуть записувати доступ до бази даних для привілейованих облікових записів, підключених до пристроїв IoT, а також автоматизувати рутинні операції. Рівні захисту, такі як динамічний контролер паролів і двофакторна автентифікація, забезпечують безпечне керування інформацією про ідентифікацію та пароль, а також захищають облікові дані привілейованих облікових записів за допомогою складних паролів і додаткових кроків підтвердження. Таким чином, ці облікові записи захищаються від внутрішньої та зовнішньої загрози.

Міжнародна логістика інтегрується у велику галузеву інфраструктуру, наприклад, можна визначити серед них:

- морські перевізники інтегрують від простих безпекових систем оповіщення до повноцінних мереж з хмарними технологіями;
- залізничні перевізники інтегрують від мережі, до GSM-Railway.

Також, існує підхід до управління ризиками для морської логістики (рис. 1). Інтеграція управління ризиками включає такі складові:

1. Визначення ролей та обов'язків користувачів, ключового персоналу та керівництва зацікавлених сторін та оператори відповідних ланцюгів постачання.

2. Ідентифікація систем, активів, даних і можливостей, які в разі порушення можуть становити ризики для логістичні операції та безпека.

3. Реалізація технічних і процедурних заходів, а також альтернатив для захисту від кіберінцидентів для забезпечення безперервності операцій.

4. Здійснення заходів з підготовки та реагування на кіберінциденти [2].

В міжнародна морській логістиці різною мірою ці правила намагаються забезпечити дотримання мінімальних стандартів для захисту найбільш конфіденційних даних і операцій компаній, зокрема, записів клієнтів та інформації про доставку.

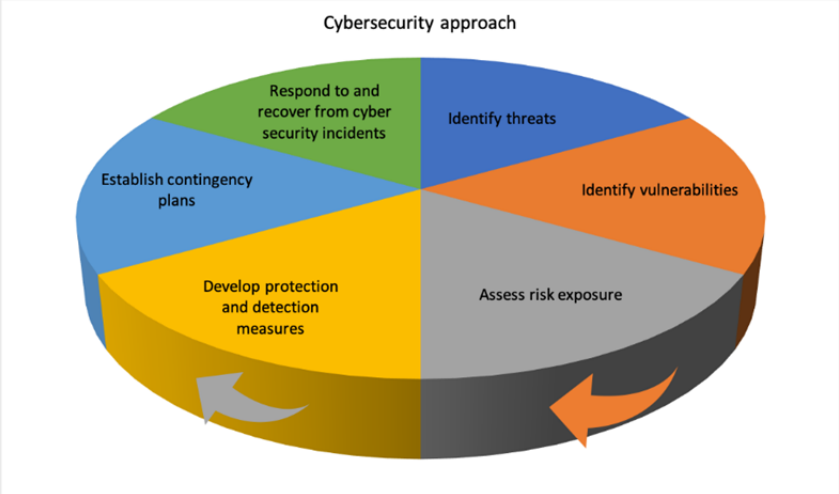

Рис. 1. Підходи до управління ризиками в морській логістиці

Слід зазначити, що ризики зростають, зокрема:

- потенційна втрата контролю над своїми персональними даними;
- стати мішенню для атак у стилі соціальної інженерії з використанням зламаних даних;
- потенційна безповоротна втрата персональних даних;
- їхні персональні дані далі зловмисно використовуються злочинцями (наприклад, для полегшення ідентифікації та фінансового шахрайства).

Інтеграція комплексного плану безпеки в мережеві системи логістики забезпечує результативний спосіб підготовки до несанкціонованого доступу. Слід провести комплексну оцінку ризиків, що допоможе розробити надійну стратегію ризиків кібербезпеки. Якщо виділяти морську галузь в логістиці, людський фактор стає ще більш складним у складній взаємопов'язаній екосистемі, подібній до тієї, яка існує. Кораблі, порти та треті сторони часто працюють зі змінними екіпажами з різним рівнем розуміння кібербезпеки, які можуть бути не повністю знайомі з безпечною роботою відповідних систем і усталеними методами кібергігієни [3].

Відсутність знання кібербезпеки може бути вигідною для будь-якого зловмисника, який хоче отримати доступ до судна та його систем, викрасти фактичну інформацію або порушити роботу судна. Системи захисту можуть брати участь у ідентифікації та пом'якшенні потенційних кібератак на кількох рівнях. Виявлення та контрзаходи, вжиті для нападу на одне судно, можуть бути передані іншим автономним суднам. В таблиці 1 наведено системи, що можуть допомогти створити стійкість до зовнішніх і внутрішніх загроз безпеці.

Таблиця 1

Системи мінімізації ризиків і стійкість до зовнішніх та внутрішніх загроз безпеці

Системи	Дії пом'якшення
Система автоматичної ідентифікації (AIS)	- вся інформація AIS повинна бути перевірена; - необхідно контролювати цілісність інформації, щоб переконатися, що ідентифікація є правильною; - слід враховувати місцеві навігаційні попередження, якщо транслюються помилкові сигнали AIS
Інформаційна система відображення електронних карт (ECDIS)	- розробники ECDIS повинні прагнути прийняти життєві цикли розробки безпеки; - регулярне документування, моніторинг і оновлення структури ECDIS; - необхідно відстежувати та реєструвати оновлення карт ECDIS, особливо оновлення вручну через компакт-диск або USB-диск; - усі файли оновлення слід сканувати антивірусним програмним забезпеченням; - слід перевірити внутрішню мережу, до якої підключено ECDIS, щоб побачити, чи можна систему ECDIS повністю ізолювати або захистити від брандмауера; - лише схвалений персонал повинен мати фізичний доступ до ECDIS та її основних компонентів
GNSS і GPS	- ідентифікація та автентифікація пристрою; - криптографічний захист
Радар	- ідентифікація та автентифікація пристрою; - криптографічний захист; - резервне копіювання інформаційної системи
Промислові системи управління (ICS)	- використовувати криптографію або інші захищені методи, щоб захистити паролі від несанкціонованого перехоплення; - щоб забезпечити безпеку систем керування, запровадити керування конфігурацією та керування виправленнями; - переконатися, що всі підключені до Інтернету пристрої ICS захищені та що паролі регулярно оновлюються; - адміністратори мережі ICS повинні використовувати сегментацію мережі та правила брандмауера, які блокують доступ до обміну файлами; - належним чином захищати файли паролів, ускладнюючи отримання хешованих паролів; - системним адміністраторам слід застосовувати надійні паролі; - використовувати конкретну політику віддаленого доступу; - аудит віддаленого доступу та пов'язаних змін; - блокувати непотрібні порти USB; - переконатися, що для всіх користувачів було проведено навчання з питань кібербезпеки
Системи керування силовими установками та механізмами та управління потужністю	- резервне копіювання інформаційної системи; - захист від відмови в обслуговуванні; - контроль фізичного доступу
Very Small Aperture Terminal (VSAT)	- слід розглянути зашифровані системи зв'язку; - необхідно ретельно розглянути механізми кіберзахисту постачальника послуг, але не слід покладатися на них виключно для захисту кожного пристрою та даних;

Системи	Дії пом'якшення
	- аутентифікація та управління контролем доступу повинні суворо дотримуватись
IT мережеві системи	- резервне копіювання інформаційної системи; - аутентифікація та контроль доступу; - забезпечити механізми захисту від загроз; - просування системи управління конфігураціями/ виправленнями / оновленнями; - переконатися, що політика BYOD діє; - переконатися, що для всіх користувачів було проведено навчання з питань кібербезпеки
Людський фактор	- сприяти розвитку кібербезпеки в організації; - переконатися, що було проведено навчання з кіберобізнаності; - оцінити ефективність навчання за допомогою вправ з кібербезпеки; - кібергігієна в рамках людського фактору

Оскільки, можливий небезпечний вплив широкомасштабної кібератаки на галузь T&L, на світову торгівлю та економічну стабільність, особливі вимоги ставлять до кращого захисту міжнародної логістики. Потрібно постійно аналізувати не тільки те, що може відбутися, але й те, що вже відбулося. Для цього здійснюється *compromise assessment*, тобто оцінювання рівня скомпрометованості інфраструктури, суть якого полягає в тому, що аналізується вся інфраструктура клієнта за великий проміжок часу, щоб пересвідчитися, що не було несанкціонованого доступу раніше.

Висновки. Одна з найбільших помилок, яку може зробити будь-яка логістична компанія, це відмова від оцінки ризиків безпеки в своїх системах. Основні способи мінімізації ризиків запобігання несанкціонованому доступу в міжнародній логістиці – це навчання співробітників організації, багатофакторна автентифікація (MFA), застосування політики надійних паролів, оновлення програмного забезпечення, періодичне створення резервних копій файлів у хмарі, щоб захистити їх від програм-вимагачів. Також, потрібно проводити комплексний інтегрований план безпеки в міжнародній логістиці, яка допоможе підготуватися до несанкціонованого доступу.

Список використаних джерел

1. Pre-ransomware activities. URL: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
2. Polatidis N/, Pavlidis M., Mouratidis H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. – Computer Standards & Interfaces, Volume 56, February 2018. – P. 74–82. https://doi.org/10.1016/j.csi.2017.09.006
3. Meland P., Bernsmed K., Wille E., Rødseth Ø., Nesheim D. A Retrospective Analysis Of Maritime Cybersecurity Incidents. – TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, 2021. –Volume 15, Issue 3. – P. 519-530. https://doi.org/10.12716/1001.15.03.04

Робота виконана під науковим керівництвом канд. техн. наук, доцента
САВЧЕНКО Т. В.

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ КОРИСТУВАЧІВ ІНТЕРНЕТУ

ШАПРАН О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Роботу присвячено актуальній проблемі інформаційної безпеки в середовищі Інтернет. З розвитком технологій та підвищеним поляганням на інформаційні технології для збереження, обробки, та використання конфіденційної інформації та збільшенням обчислювальних потужностей комп'ютерних систем, традиційні методи авторизації користувачів у веб додатках потребують перегляду та оновлення для забезпечення безпеки та довіри до комп'ютерних систем. В роботі розглянуто визначення, будову, переваги та недоліки використання двофакторної автентифікації, її вплив на сучасні веб-додатки. Було розглянуто перспективи використання біометричних та інших видів підтвердження особистості (eToken) як можливий фактор захисту подальшого розвитку систем багато-факторної автентифікації.

The paper is dedicated to the pressing issue of information security in the Internet environment. With the advancement of technology and increased reliance on information technologies for the storage, processing, and utilization of confidential information, as well as the increase in computational power of computer systems, traditional methods of user authorization in web applications require review and updating to ensure security in online systems. The paper provides an overview of the definition, structure, advantages, and disadvantages of using two-factor authentication (2FA) and its impact on modern web applications. The prospects of using biometric and other types of identity verification (eToken) as a possible factor for enhancing the security of multi-factor authentication systems have been examined and analysed.

Актуальність теми: зростання кількості інтернет-шахраїв та кібератак призводить до необхідності підвищення рівня безпеки користувачів. Одним з способів забезпечення безпеки є використання двофакторної аутентифікації, яка забезпечує використання двох незалежних механізмів для підтвердження ідентичності користувача.

Метою нашої наукової статті є опис двофакторної аутентифікації як способу підвищення безпеки користувачів Інтернету та дослідити її ефективність в порівнянні з іншими методами аутентифікації.

Об'єктом нашого дослідження є безпека користувачів Інтернету.

Предмет дослідження: двофакторна аутентифікація як спосіб підвищення безпеки користувачів Інтернету.

Аналіз попередніх досліджень: попередні дослідження показують, що традиційні методи аутентифікації, такі як введення логіну та пароля, не забезпечують достатнього рівня безпеки. Також дослідження показують, що використання двофакторної аутентифікації може підвищити рівень безпеки користувачів, оскільки вона забезпечує використання двох незалежних механізмів для підтвердження ідентичності користувача. Дослідження також показують, що рівень безпеки може бути підвищений, якщо один з механізмів двофакторної аутентифікації використовує фізичні або біометричні дані, такі як відбиток пальця або обличчя.Виклад основного матеріалу.У XXI столітті Інтернет перетворився на основний спосіб зв'язку сучасного життя. Сучасний образ світу формується в кореляції з посиленням творчого потенціалу людини і можливостями цифрових технологій, мережі Інтернету, штучного інтелекту, численних медійних продуктів. Водночас образ сучасної людини формується в контексті доступу до мережі, інтернету речей, володіння і використання гаджетів, поєднання людського і штучного інтелекту тощо (Кремень В., Биков В., Ляшенко О. та ін., 2022, с. 2-3). Поява комп'ютерних технологій і активна диджиталізація суспільства

створили суспільний попит на методи автентифікації, засновані не лише на традиційних криптографічних способах (шифрування, гешування, цифровий підпис), а й на використанні декількох чинників, що забезпечують достовірність особи і активізують проблему безпеки користувачів. *Двофакторна автентифікація – це метод ідентифікації*, що вимагає від користувача надання двох даних, щоб отримати доступ і увійти у обліковий запис. Це може бути СМС на номер телефону або код з листа на адресу електронної пошти, відповідь на якесь секретне питання, або ж біометрична ідентифікація. *Отже, двофакторна автентифікація* (2FA – Two-Factor authentication) вимагає користувача підтвердити свою особу двічі, за допомогою двох різних джерел, що підвищує безпеку та захищає конфіденційні дані.

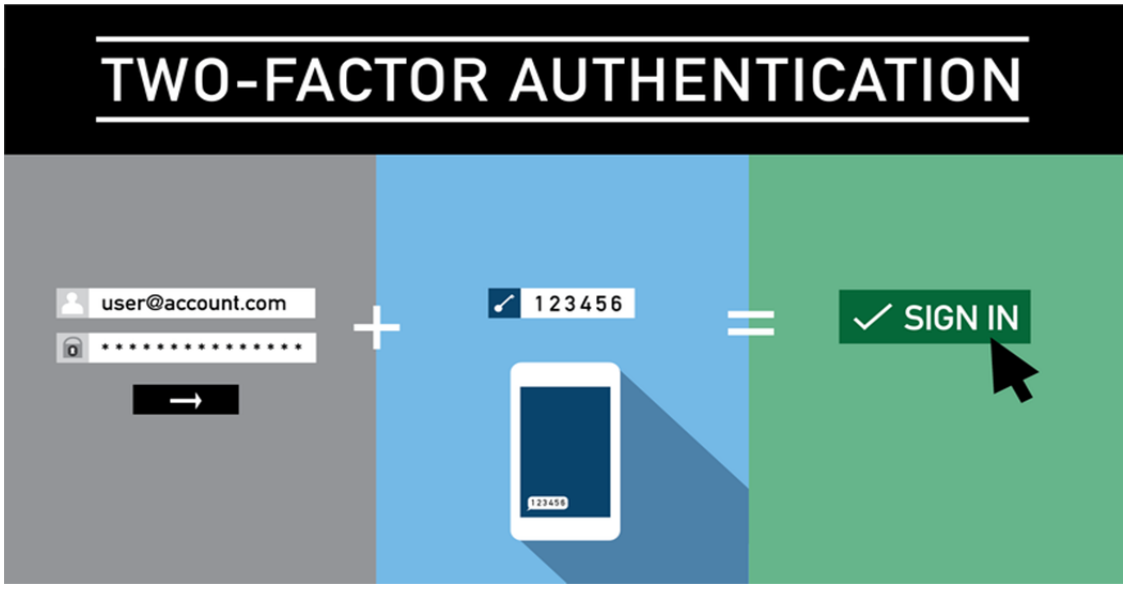

Рис. 1. Схема автентифікації з використанням 2FA, вигляд для користувача

Тобто, для того щоб увійти, наприклад, в свій електронний кабінет, користувач вводить всій логін та пароль, як прийнято на більшості веб-сервісів. Але додатково після цього проходить перевірка з іншого джерела, наприклад введення коду із СМС на номер телефону що користувач вказав при реєстрації.

Зазначений метод 2FA зазвичай різко знижує можливість крадіжки особистих даних онлайн, так як знання лише пароля недостатньо для здійснення електронного шахрайства, оскільки йде перевірка з іншого, незалежного джерела, до якого в них немає доступу.

Тим не менш, двохфакторні підходи аутентифікації залишаються уразливими для атак типу «фішинг» та «людина посередині» (Man-in-the-middle attack). На сьогоднішній день, найпопулярнішим методом реалізації 2FA є *пароль користувача та SMS із перевірочними кодами*, що генеруються за технологією OTP (One Time Password) й відправляються на смартфон користувачу. Впевненість у надійності методу 2FA обумовлюють його застосування для найвідповідальніших операцій – від авторизації в Google (*доступ до пошти, хмарного сховища, контактів і всієї інформації користувача, в тому числі конфіденційної*) до систем онлайн банкінгу та підтвердження здійснення переказу грошей.

М. Маркіна зазначає, що Національний Інститут стандартів і технологій США (The National Institute of Standards and Technology, NIST) оприлюднив влітку 2016 року попередню версію майбутнього Digital Authentication Guideline з критикою популярного підходу SMS OTP. Основні побоювання експертів Національного інституту стандартів і технологій зводилися до того, що номер телефону може бути прив'язаний до VoIP сервісу. Окрім цього, зловмисники можуть спробувати переконати постачальника послуг у зміні номеру телефону і таким чином отримати код доступу. Хоча документ рекомендує виробникам використ-

товувати в своїх додатках токени і криптографічні ідентифікатори, автори поправок також відзначають, що «смартфон або інший мобільний пристрій завжди можуть бути вкрадені, або можуть тимчасово перебувати в руках іншої людини» – йдеться в документі NIST. Вчені з Амстердамського університету Р. К. Конотом (R. K. Konoth), В. ван дер Вен (V. van der Veen) і Г. Бос (H. Bos) продемонстрували атаку з використанням установки уразливого додатку через Google Play. Їм вдалося успішно обійти перевірку Google Bouncer і активувати додаток для перехоплення одноразових паролів (Маркіна, 2020, с. 87-88). Отже, недоліком двофакторної аутентифікації є те, шо зловмисник може підібрати пароль користувача і перехопити SMS-повідомлення зі згенерованим кодом.

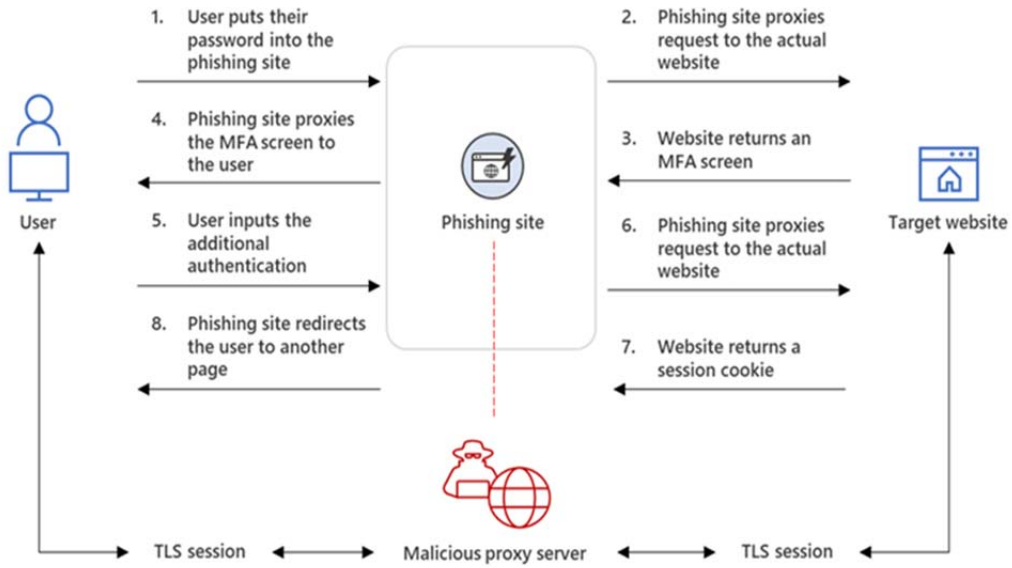

Рис. 2. Схема зламу захисту 2FA за допомогою липового сайту (фішингу)

Як працює фішинг: хакери можуть розмістити липовий веб-сервіс та надіслати листа на електрону пошту користувача з проханням негайно переглянути якусь інформацію. Якщо користувач поведеться та натисне на посилання він попаде на сайт хакерів з аналогічним оформленням до справжнього. Ввівши свій пароль та логін, сайт правдоподібно попросить ввести код 2FA. Таким чином хакери ненадовго отримають все необхідні дані для автентифікації на справжньому веб-сервісі та можуть отримати доступ до профілю жертви та вкрасти гроші/інформацію.

Незважаючи на зазначені недоліки 2F-аутентифікації, погоджуємося із думкою В. Балацької, О. Полотая, А. Пузиря, що в першу чергу двофакторну автентифікацію необхідно забезпечити для облікових записів із правами адміністратора та тих, хто має доступ до конфіденційної інформації. Це є потужним кроком до запобігання крадіжці даних і можливим фінансовим втратам (Балацька В., Полотай О., Пузирь А., 2022, с. 290). Цей метод значно підвищує захист від прямих хакерських атак, як-то brute force перебирання паролей та крадіжка логіну та пароля за допомогою зараженого програмного забезпечення.

Двофакторну автентифікацію доволі легко впровадити у вже існуючі веб-сервіси, оскільки для перевірки може використовуватися вже існуюче обладнання, а нова система перевірки може бути доповненням до вже існуючого класичного «Логін+Пароль». Однак для додаткового захисту часто використовують окремі фізичні сервери.

Сервер аутентифікації 2FA генерує короткі коди, унікальні для кожного користувача. При введені коректного логіну та паролю, звичайний сервер веб-додатку дає запит на сервер автентифікації, що в свою чергу генерує унікальний код на надсилає потрібному користувачу. Дуже важливо щоб код мав обмежену кількість часу за яку він може бути

використаний, це зробить неможливим крадіжку невикористаного коду для подальшої автентифікації зловмисниками. Якщо код було введено правильно – сервер автентифікації дозволяє серверу веб-додатку обслуговувати користувача та відповідати на запити на особисту інформацію. На схемі червоними лініями описано як проводиться активація 2FA якщо користувач ще не користується нею.

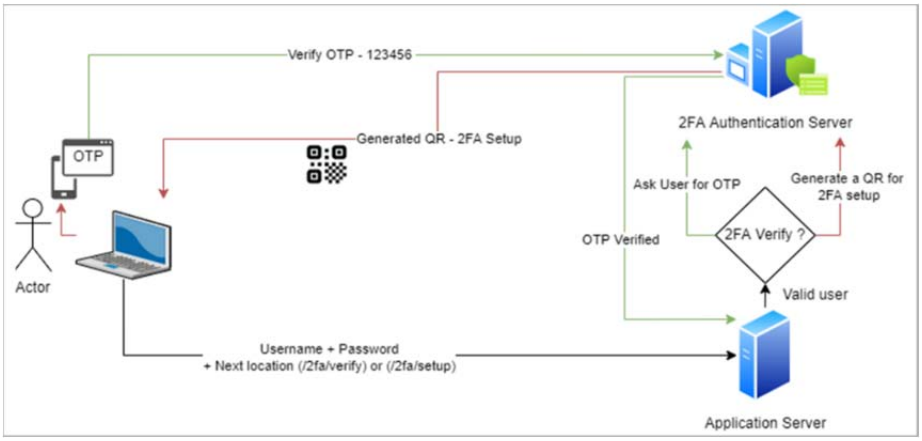

Рис. 3. Блок схема реалізації системи 2FA

Для впровадження автентифікації часто використовуються спеціальні додатки, вони є більш захищеними через неможливість перехопити СМС повідомлення, оскільки в такому випадку код для входу може генеруватися локально на пристрої користувача.

Google Authenticator – мобільний застосунок, що використовується для виконання двофакторної автентифікації, в облікових записах Google та сторонніх сервісах. Реалізований для декількох мобільних платформ, не має можливості ініціалізації на декількох пристроях. Секретний ключ можна інтегрувати в застосунок як QR-код, або ввести вручну. Налаштування в застосунку представлені лише засобами синхронізації часу з серверами Google. Автентифікатор генерує 6-ти або 8-мизначний одноразовий пароль, з використанням відкритих стандартів алгоритмів HOTP та TOTP. Дані паролі використовуються у якості другого фактору автентифікації і застосовуються після коректного введення логіну та паролю. Пароль дійсний протягом 30 секунд, що запобігає використанню його кілька разів. *Microsoft Authenticator* – мобільний застосунок, який допомагає входити в облікові записи, виконуючи двофакторну автентифікацію. Працює із будь-яким обліковим записом, який використовує двофакторну автентифікацію та підтримує одноразові паролі (TOTP). В якості генератора кодів Microsoft Authenticator обирає шестизначний пароль, який відображається під кожним доданим обліковим записом. Пароль дійсний протягом 30 секунд, що запобігає використанню коду кілька разів. Ініціалізація облікового запису проходить шляхом сканування QR-коду, або введення коду вручну. Не має можливості ініціалізувати один обліковий запис в декількох застосунках на різних пристроях одночасно (Самара Н., Бурак Н., с.55-56). Таким чином, такі компанії-гіганти як Google та Microsoft надають впевненість у коректності та стійкості обраних факторів автентифікації.

Окрім того, двофакторна автентифікація буває *різних видів*: парольна, апаратна, eToken та ін. Найбільш досконалою системою вважається *біометрична автентифікація*, тому що спирається на фізичні властивості окремого індивіда чи групи людей. Біометрична автентифікація загалом є покращеною версією парольної, тільки замість паролю чи PIN-коду користувач «вводить» свої фізичні параметри. Вона є досить легкою у використанні, але складною у побудові та затратах на неї. У *біометричній автентифікації* використовуються*:* відбитки пальців; геометрична форма кисті руки; форма і розміри особи; особливості голосу; візерунок райдужної оболонки і сітківки очей та ін. (Канівець В., Сомов С., 2018). Найбільшого поширення набули дактилоскопічні системи автентифікації, які засновані на великих банках даних відбитків пальців і забезпечують захищений доступ до комп’ютерів,

вхідних дверей, автомобілів, банкоматів тощо, а також системи автентифікації за обличчями і голосами, оскільки більшість сучасних електронних пристроїв мають відео- і аудіо засоби. Однак, технології розпізнавання рис обличчя вимагають подальшого вдосконалення, бо залежать від коливань в освітленні, що впливає на пізнаваність особи. Системи автентифікації за голосом спираються на такі його особливості як висота, модуляція і частота звуку, що є унікальними характеристиками для кожної людини й більш піддаються верифікації.

Таким чином, інформаційна безпека знаходиться в руках користувача, який дотримується певних правил і самостійно використовує доступні рішення для захисту облікових даних. Двофакторна автентифікація (2FA) для підвищення безпеки користувачів Інтернету підходить для ресурсів, на яких зберігається менш чутлива, з точки зору конфіденційності, інформація та для віддалених ресурсів шляхом подвійного підтвердження власної особи. Для впровадження автентифікації використовуються спеціальні сервіси *(Google Authenticator, Microsoft Authenticator).* Двофакторна автентифікація буває різних видів: парольна, апаратна, eToken та ін. Найбільш досконалою системою вважається біометрична автентифікація, що можна використовувати для аутентифікації користувачів на локальних пристроях або в корпоративній мережі. Важливим фактором забезпечення захищеності інформації є своєчасне залучення новітніх інструментів і засобів безпеки

Список використаних джерел

1. Балацька В., Полотай О., Пузир А. Автентифікація, як один з механізмів забезпечення безпеки операційних систем. *Інформаційна безпека та інформаційні технології*: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. Львів: Растр-7, 2022. С. 288-290.
2. Брухнов Д. А., Азарова А. О. Забезпечення захищеної авторизації на основі двофакторної автентифікації зі змінним ключем та захистом від Brute Force. Матеріали L науково-технічної конференції підрозділів ВНТУ, (Вінниця, 10-12 березня 2021 р.). URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2021/paper/view/12495.
3. Канівець В. Г., Сомов С. В. Автентифікація користувачів комп'ютерних систем. *Новітні інформаційні системи та технології*. 2018. Вип. 9. URL: http://reposit.nupp.edu.ua/bitstream/PoltNTU/4489/1/1046-96-1983-1-10-20180721.pdf
4. Кремень В. Г., Биков В. Ю., Ляшенко О. І., Литвинова С. Г., Луговий В. І., Мальований Ю. І., Пінчук О. П., & Топузов О. М. Науково-методичне забезпечення цифровізації освіти україни: стан, проблеми, перспективи: наукова доповідь загальним зборам НАПН України «Науково-методичне забезпечення цифровізації освіти України: стан, проблеми, перспективи», 18-19 листопада 2022 р. *Вісник Національної академії педагогічних наук України*. 2022. №4(2). С. 1-49. URL: https://doi.org/10.37472/v.naes.2022.4223
5. Маркіна М.В. Використання трифакторної або двофакторної аутентифікації: переваги і недоліки, вибір оптимального варіанту. *Проблеми використання інформаційних технологій в освіті, науці та промисловості* : XIV міжнар. конф. (28-29 листоп. 2019 р.) : зб. наук. пр. / ред. кол.: Г.Г. Півняк та ін.; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». Дніпро : НТУ «ДП», 2020. № 4. С. 86-89.
6. Самара Н. М., Бурак Н. Є. Аналіз принципів реалізації методів двофакторної автентифікації в сучасних програмних додатках. *Інформаційна безпека та інформаційні технології*: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, С. 54-56.

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д. О.

МЕТОДИ ОТРИМАННЯ ЦИФРОВИХ ДОКАЗІВ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ ЗА ДОПОМОГОЮ КРИМІНАЛІСТИЧНИХ ІНСТРУМЕНТІВ

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

У статті розглянуті основні методи цифрового криміналістичного аналізу та протоколи обробки цифрових доказів. Зазначено переваги застосування певних програмних продуктів для дослідження цифрових доказів. Проведене розслідування місця злочину, на якому за допомогою певного програмного забезпечення були відновлені знищені цифрові докази.

The article discusses the main methods of digital forensic analysis and digital evidence processing protocols. The advantages of using certain software products for researching digital evidence are indicated. Conducted a crime scene investigation where destroyed digital evidence was recovered using certain software products.

Актуальність. Злочини з використанням комп'ютерів зростають стрімкими темпами. Такі злочини можуть варіюватися від злому та кібератак до крадіжок ідентичності та шахрайства. Оскільки комп'ютерні злочини досягли високого рівня, інструменти, які використовуються для боротьби з такими злочинами, розвиваються швидше. У порівнянні з іншими судово-медичними науками галузь цифрової криміналістики відносно молода, але також стала життєво важливою для розкриття комп'ютерних злочинів.

Цифрова криміналістика – це покроковий процес наукових методів і прийомів розслідування злочинів, отриманих із цифрових доказів, які можуть бути нестабільними та крихкими, і неправильне поводження з ними може змінити їх. Через свою мінливість і крихкість необхідно дотримуватися протоколів, щоб гарантувати, що дані не змінюються під час їх обробки (тобто під час доступу, збору, пакування, передачі та зберігання). Ці протоколи визначають кроки, яких слід дотримуватись під час роботи з цифровими доказами. Використання відповідних методів збору та захисту електронних доказів сприяло б цифровій криміналістиці та законодавству про інформаційні технології.

Докази для обговорення в суді часто збираються завдяки навичкам цифрових судових експертів, які можуть витягувати важливі дані з електронних пристроїв, що належать потерпілим сторонам. Для дослідження цифрових доказів та притягнення до відповідальності існує багато цифрових криміналістичних інструментів, які використовуються для розслідування цифрових злочинів шляхом ідентифікації цифрових доказів.

У цьому дослідженні основний акцент буде зроблено на процесі цифрової криміналістики, а також на програмному забезпеченні, яке використовується під час цієї процедури.

Метою статті є надати огляд комп'ютерної криміналістики та методів та вивчення протоколів, які застосовуються для отримання та обробки цифрових доказів із комп'ютерних систем для аналізу інформації, яка використовується у кримінальних розслідуваннях з метою потенціального вирішення злочину.

Об'єктом дослідження є вивчення методів отримання та протоколів обробки цифрових доказів.

Предметом дослідження є методи та протоколи обробки цифрових доказів.

Аналіз попередніх досліджень. Дослідженню методів отримання цифрових доказів, протоколів їх обробки та основних програмних продуктів присвячені праці вітчизняних та закордонних науковців: Білл Нельсон, Амелія Філліпс, Крістофер Стюарт, Майкл Бойл, Жан-Клод Вульєрме

Виклад основного матеріалу. Оскільки все більше і більше користувачів переходять на мобільні пристрої та використовують взаємопов'язані пристрої, комп'ютери часто стають

центром інцидентів і розслідувань. Сучасні аналітики комп'ютерної криміналістики здатні відновлювати дані, які були видалені, зашифровані або приховані у різних пристроях; їх можна викликати для дачі свідків у суді та розповісти про докази, знайдені під час розслідування. Вони можуть брати участь у складних справах, включаючи перевірку алібі правопорушників, перевірку зловживань Інтернетом, зловживання комп'ютерними ресурсами та використання мережі для створення комп'ютерних загроз. Експертів-криміналістів можна залучити для супроводу серйозних справ, пов'язаних із витоком даних, вторгненням або будь-яким іншим типом інцидентів. Застосовуючи методи та власне програмне забезпечення для криміналістичної експертизи для дослідження системних пристроїв або платформ, вони могли б надати ключові відкриття, щоб визначити, хто був відповідальним за розслідуваний злочин.

Метою комп'ютерної криміналістичної експертизи є відновлення даних з комп'ютерів, вилучених як доказ у кримінальному розслідуванні. Експерти використовують системний підхід до дослідження доказів, які можуть бути представлені в суді під час провадження. Залучення судово-медичних експертів має бути на ранніх стадіях розслідування, оскільки вони можуть допомогти правильно зібрати технічний матеріал таким чином, щоб відновити вміст без будь-яких пошкоджень його цілісності.

Першим кроком у будь-якому криміналістичному процесі є перевірка всього апаратного та програмного забезпечення, щоб переконатися, що вони працюють належним чином. У спільноті криміналістів все ще точаться дискусії щодо того, як часто слід тестувати програмне забезпечення та обладнання. Більшість людей погоджуються з тим, що, як мінімум, організації повинні перевіряти кожен елемент програмного та апаратного забезпечення після його придбання та перед використанням. Їм також слід повторити тестування після будь-якого оновлення, виправлення або зміни конфігурації.

Криміналістичне розслідування полягає у зборі комп'ютерної криміналістичної інформації; процес можна розпочати з аналізу мережевого трафіку за допомогою аналізатора пакетів або інструменту сніфера, такого як Wireshark, який здатний перехоплювати трафік і реєструвати його для подальшого аналізу. NetworkMiner, ще один інструмент аналізу мережі (NFAT), є альтернативою Wireshark для вилучення або відновлення всіх файлів. Натомість Snort є цінним інструментом для відстеження мережевих зловмисників у реальному часі.

Програмне забезпечення NFAT також містить криміналістичні можливості, виконуючи аналіз збереженого мережевого трафіку, як випливає з його назви. Що стосується реагування на інциденти та ідентифікації, для ідентифікації видалених файлів і їх відновлення можна використовувати Forensic Toolkit або FTK; в той час, як EnCase підходить для криміналістики, кібербезпеки та електронного пошуку.

Коли платформа криміналістичної експертизи готова, спеціаліст дублює криміналістичні дані, надані в запиті, і перевіряє їх цілісність. Цей процес передбачає, що правоохоронні органи вже отримали дані за допомогою відповідного судового процесу та створили криміналістичне зображення. Криміналістичне зображення – це побітова копія даних, які існують на оригінальному носії, без будь-яких додавання чи видалення. Також передбачається, що судово-медичний експерт отримав робочу копію вилучених даних. Якщо експерти отримують оригінали доказів, вони повинні зробити робочу копію та стежити за ланцюгом зберігання оригіналу. Експерти перевіряють, чи копія, якою вони володіють, є цілою та незмінною. Зазвичай вони роблять це, перевіряючи хеш або цифровий відбиток доказів. У разі виникнення проблем екзаменатори консультуються із заявником щодо подальших дій.

Після того як експерти перевірять цілісність даних, що підлягають аналізу, розробляється план вилучення даних. Вони організовують і уточнюють судово-медичний запит на питання, які вони розуміють і на які можуть відповісти. Вибрано криміналістичні інструменти, які дозволяють їм відповісти на ці запитання. Екзаменатори, як правило, мають попередні ідеї щодо того, що шукати, на основі запиту. Вони додають їх до «Списку

пошукових запитів», який є поточним списком запитуваних елементів [2]. У моєму випадку, запит надає лід: «пошук особистих даних».

Для кожного пошукового запиту експерти виділяють відповідні дані та позначають цей пошуковий запит як «оброблений» або «готовий». Вони додають будь-що вилучене до другого списку, який називається «Список вилучених даних». Екзаменатори переслідують усі пошукові запити, додаючи результати до цього другого списку. Потім вони переходять до наступного етапу методології – ідентифікації (рис.1).

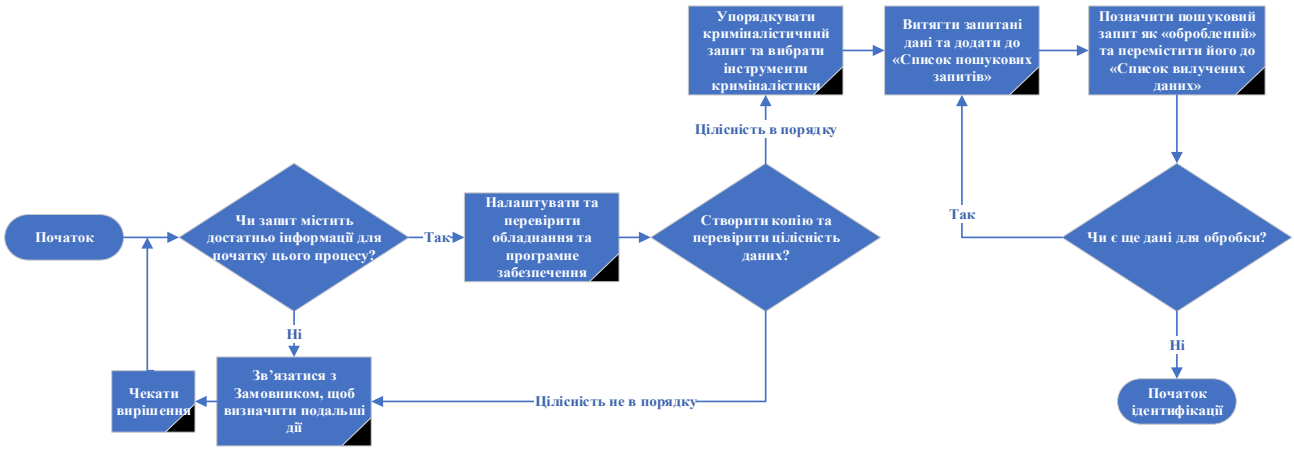

Рис. 1. Підготовка цифрових даних до їх подальшої ідентифікації

На етапі ідентифікації отримується попередня інформація про справу про кіберзлочин. Ця попередня інформація подібна до тієї, яку шукають під час традиційного кримінального розслідування. Слідчий прагне відповісти на наступні питання: Хто брав участь? Що сталося? Коли стався кіберзлочин? Де стався кіберзлочин? Як стався кіберзлочин?

Відповіді на ці запитання дадуть слідчим рекомендації щодо того, як продовжувати справу. Наприклад, відповідь на питання «де стався цей злочин?» – тобто в межах або за межами кордонів країни – інформуватиме слідчого про те, як продовжити справу (наприклад, які органи слід залучити).

Але місце злочину не обмежується фізичним розташуванням цифрових пристроїв, які використовувалися під час скоєння кіберзлочинів та які були метою кіберзлочину. Місце злочину в кіберзлочині також включає цифрові пристрої, які потенційно містять цифрові докази, і охоплює кілька цифрових пристроїв, систем і серверів. Місце злочину охороняється, коли кіберзлочин спостерігається, повідомляється та підозрюється. Користувачам не можна надавати можливість далі керувати цифровими пристроями. Слідчий проводить огляд місця злочину та виявляє докази. Перед збором доказів проводиться документування місця злочину. Документація необхідна протягом усього процесу розслідування (до, під час і після отримання доказів). Ця документація повинна містити детальну інформацію про зібрані цифрові пристрої, включаючи робочий стан пристрою – увімкнено, вимкнено, режим очікування – та його фізичні характеристики, такі як марка, модель, серійний номер, з'єднання та будь-які позначки чи інші пошкодження. Окрім письмових нотаток, для документування місця злочину та доказів також необхідні ескізи, фотографії та відеозаписи місця злочину та доказів. На етапі ідентифікації слідчі кіберзлочинів використовують багато традиційних методів розслідування, особливо щодо збору інформації та доказів. Наприклад, жертви, свідки та підозрювані в кіберзлочині опитуються для збору інформації та доказів кіберзлочину, який розслідується. Фактичний збір доказів передбачає збереження летючих доказів і відключення цифрових пристроїв.

Перш ніж розпочати збір цифрових доказів, слідчий повинен визначити типи доказів, які шукаються. Якщо вони не мають відношення до судового запиту, вони просто

позначають їх як оброблений і йдуть далі. Якщо об'єкт має відношення до судово-медичного запиту, експерти документують його в третьому списку, списку відповідних даних. Цей список є набором даних, які стосуються відповіді на оригінальний судово-медичний запит. Цифрові докази можна знайти на цифрових пристроях, таких як комп'ютери, зовнішні жорсткі диски, флеш-накопичувачі, маршрутизатори, смартфони, планшети, камери, смарт-телевізори, побутова техніка з підключенням до Інтернету (наприклад, холодильники та пральні машини) та ігрові консолі, а також загальнодоступні ресурси (наприклад, платформи соціальних медіа, веб-сайти та дискусійні форуми) і приватні ресурси (наприклад, журнали активності користувачів постачальників послуг Інтернету; бізнес-записи постачальників послуг зв'язку; записи про дії користувачів постачальників хмарних сховищ). Багато програм, веб-сайтів і цифрових пристроїв використовують служби хмарного зберігання. користувачів Таким чином, дані можуть зберігатися повністю або фрагментарно різними постачальниками на серверах у багатьох місцях. Через це отримати дані є складним завданням. Докази, які шукаються, залежатимуть від розслідуваного кіберзлочину. Якщо кіберзлочин, який розслідується, є шахрайством із ідентифікацією, тоді вилучені цифрові пристрої шукатимуть докази цього злочину (наприклад, докази шахрайських транзакцій).

У моїй справі про крадіжку особистих даних відповідні дані можуть включати номери соціального страхування, зображення фальшивих ідентифікаторів або електронні листи з обговоренням крадіжки особистих даних, серед іншого. Також можливо, що елемент генерує ще одного пошукового запиту. Електронний лист може виявити, що мета використовувала інший псевдонім. Це призведе до нового пошуку за ключовим словом для нового псевдоніма. Екзаменатори повертаються і додають цей підхід до списку пошукових запитів, щоб вони не забули його повністю дослідити.

Елемент також може вказувати на абсолютно нове потенційне джерело даних. Наприклад, екзаменатори можуть знайти новий обліковий запис електронної пошти, який використовував ціль. Після цього відкриття правоохоронні органи, можливо, захочуть отримати повістку про вміст нового облікового запису електронної пошти. Експерти також можуть знайти докази, що вказують на цільові файли, що зберігаються на знімному накопичувачі з універсальною послідовною шиною (USB), якого правоохоронні органи не знайшли під час початкового пошуку. За цих обставин правоохоронні органи можуть розглянути питання про отримання нового ордера на обшук для пошуку USB-накопичувача. Судово-медична експертиза може вказати на багато різних типів нових доказів. Деякі інші приклади включають журнали брандмауера, журнали доступу до будівлі та запис відеозапису безпеки. Експерти документують їх у четвертому списку, списку нових джерел даних.

Після обробки списку витягнутих даних експерти повертаються до будь-яких нових розроблених потенційних клієнтів. Для будь-яких нових джерел пошуку даних експерти розглядають можливість повернення до етапу вилучення для їх обробки. Подібним чином, для будь-якого нового джерела даних, яке може призвести до нових доказів, експерти розглядають можливість повернутися до процесу отримання та зображення цих нових судово-медичних даних.

На цьому етапі процесу експертам доцільно повідомити запитувача про свої початкові висновки. Це також гарний час для перевіряючих і тих, хто запитує, щоб обговорити, якою, на їхню думку, буде віддача від інвестицій для пошуку нових потенційних клієнтів. Залежно від стадії справи, витягнуті та ідентифіковані відповідні дані можуть надати запитувачу достатньо інформації для просування справи, і експертам може не знадобитися виконувати подальшу роботу (рис. 2). Але у справі про викрадення особистих даних, експерт відновлює недостатню кількість файлів в яких містяться особисті дані, тому експерти переходять до наступного кроку, аналізу.

На етапі аналізу екзаменатори з'єднують усі крапки та малюють для запитувача повну картину. Для кожного елемента в списку релевантних даних екзаменатори відповідають на такі запитання, як хто, що, коли, де та як. Вони намагаються пояснити, який користувач або

програма створив, редагував, отримав або надіслав кожен елемент, і як він спочатку з'явився. Також експерти пояснюють, де його знайшли. Найголовніше, вони пояснюють, чому вся ця інформація є важливою і яке значення вона має для справи.

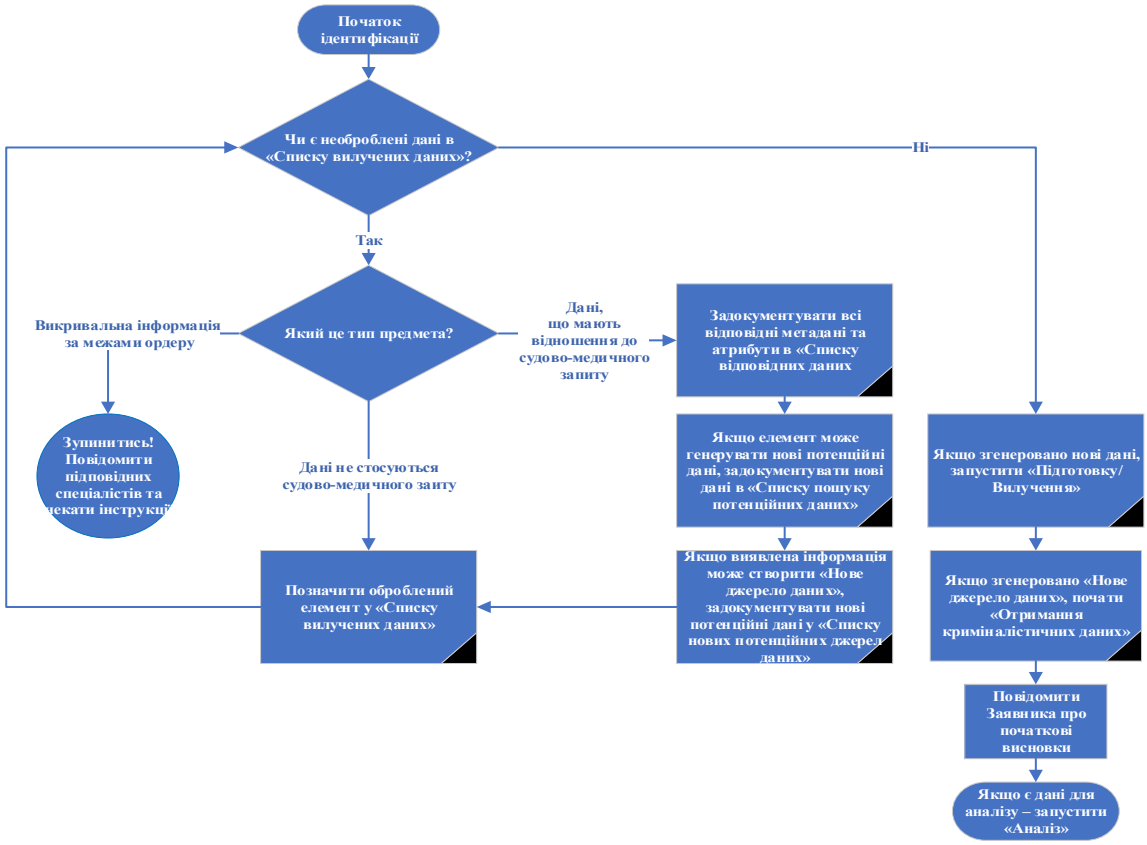

Рис. 2. Процес ідентифікації цифрових даних

Загалом існує декілька типів аналізу, які можна виконувати на комп'ютерах:

Аналіз часових рамок має на меті створити часову шкалу або часову послідовність дій за допомогою позначок часу (дата й час), які призвели до події, або визначити час і дату, коли користувач виконав певну дію. Цей аналіз виконується для приписування злочину злочинцю або принаймні дії, яка призвела до злочину, конкретній особі. Наприклад, історія веб-браузера показує відвідування сайтів і час їх відвідування. Потрібні додаткові докази, щоб показати, що особа, чиї цифрові докази використовувалися для доступу до цих веб-сайтів, була власником та/або підозрюваним користувачем пристрою.

Аналіз власності та володіння використовується для визначення особи, яка створила, отримала доступ та/або змінила файли в комп'ютерній системі. Наприклад, цей аналіз може виявити зображення матеріалів сексуального насильства над дітьми (тобто «зображення будь-якими способами дитини, яка бере участь у справжніх чи імітованих відвертих сексуальних діях, або зображення статевих частин дитини переважно з сексуальною метою»; Стаття 2 Факультативного протоколу ООН до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції та дитячої порнографії 2000 року) на пристрої підозрюваного [1]. Лише цієї інформації недостатньо, щоб підтвердити право власності на матеріали сексуального насильства над дітьми. Щоб підтвердити це, потрібні додаткові докази, наприклад ексклюзивне використання комп'ютера, де було знайдено матеріал.

Аналіз додатків і файлів виконується для перевірки додатків і файлів у комп'ютерній системі, щоб визначити знання зловмисника, намір і можливості вчинити кіберзлочин (наприклад, мітка або назва файлу може вказувати на вміст файлу; наприклад, ім'я файлу може бути ім'ям жертви кіберзлочину).

Також можна виконати аналіз приховування даних. Як випливає з назви, аналіз приховування даних шукає приховані дані в системі. Злочинці використовують кілька методів приховування даних, щоб приховати свою незаконну діяльність та ідентифікаційну інформацію, як-от використання шифрування, пристрої, що захищають паролем, і певний вміст (наприклад, файли), зміна розширень файлів і приховування розділів. Під час фази аналізу слідчому необхідно розглянути методи приховування даних, які злочинці могли використати, щоб приховати свою особу та діяльність. Приховані дані можуть виявити «обізнаність [про злочин], право власності [контент] або намір [вчинити злочин]».

Аналіз видалених файлів. Коли файл видаляється на комп'ютері, він поміщається в корзину або кошик. Якщо кошик або сміттєвий кошик очищається (тобто шляхом видалення вмісту), видалені файли видаляються з таблиці розміщення файлів, яка архівує імена файлів і розташування на жорстких дисках. Простір, де знаходиться файл, позначається як вільний простір (тобто нерозподілений простір) після його видалення, але файл все ще перебуває в цьому просторі (принаймні до тих пір, поки він повністю або частково не буде перезаписаний новими даними).

Метою цих аналізів є реконструкція злочину (або реконструкція події). Реконструкція події має на меті визначити, хто був відповідальним за подію, що сталося, де відбулася подія, коли відбулася подія та як подія розгорталася, за допомогою ідентифікації, зіставлення та зв'язування даних (виявляючи «загальну картину» « або суть події). Реконструкція подій може включати часовий аналіз (тобто визначення часу, коли відбулися події та послідовності цих подій), реляційний аналіз (тобто визначення залучених осіб і того, що вони робили, а також асоціації та відносини між цими особами) і функціональний аналіз (тобто оцінка продуктивності та можливостей систем і пристроїв, залучених до подій).

Часто екзаменатори можуть провести найцінніший аналіз, дивлячись на те, коли все сталося, і створюючи часову шкалу, яка розповідає послідовну історію. Для кожного відповідного елемента екзаменатори намагаються пояснити, коли його було створено, доступно, змінено, отримано, надіслано, переглянуто, видалено та запущено. Вони спостерігають і пояснюють послідовність подій і відзначають, які події відбулися одночасно.

Експерти документують усі свої аналізи та іншу інформацію, що стосується судово-медичного запиту, і додають усе це до п'ятого й останнього списку, «Списку результатів аналізу». Це список усіх значущих даних, які відповідають на запитання, хто, що, коли, де, як та інші. Інформація в цьому списку відповідає вимогам судово-медичної експертизи. Навіть на цій пізній стадії процесу щось може створити нові джерела пошуку даних або джерело даних. Якщо це станеться, екзаменатори додадуть їх до відповідних списків і розглянуть можливість повернутися, щоб перевірити їх повністю.

Нарешті, після того, як експерти пройдуть ці кроки достатньо разів, вони можуть відповісти на судово-медичний запит, переходять до фази судово-медичної експертизи. Це крок, на якому експерти документують висновки, щоб заявник міг зрозуміти їх і використати у справі. Звітність судової експертизи виходить за межі цієї статті, але її важливість важко переоцінити. Остаточний звіт є найкращим способом для експертів повідомити результати запитувачу. Звіти мають бути максимально чіткими та точними. Необхідно включити демонстраційний матеріал (наприклад, малюнки, графіки, результати інструментів) і підтверджуючі документи, такі як документація про ланцюжок поставок, а також детальне пояснення використаних методів і кроків, вжитих для вивчення та вилучення даних. Висновки слід пояснювати з урахуванням цілей аналізу (тобто мети розслідування та справи, яка розслідується). Інформація про обмеження висновків також має бути включена до звіту. Після звіту запитувач проводить аналіз на рівні справи, де спеціаліст інтерпретує висновки в контексті всієї справи (рис. 3).

Отже, вивчивши методи отримання цифрових доказів комп'ютерних злочинів за допомогою криміналістичних інструментів та пройшовши всі етапи розслідування на місці злочину був вилучений ноутбук компанії HP. Ймовірно, на якому були знищені цифрові докази злочину. Попередньо, опитавши потерпілу сторону, можна припускати, що зловмисник викрав її особисті дані.

Для того, щоб знайти цифрові докази скоєного злочину потрібно за допомогою програмного забезпечення для розслідування криміналістичних процесів та живого аналізу OSForensic на ноутбуці зловмисника застосувати аналіз часу, щоб дізнатися які останні дії та в який час зловмисник робив (рис.3) [3].

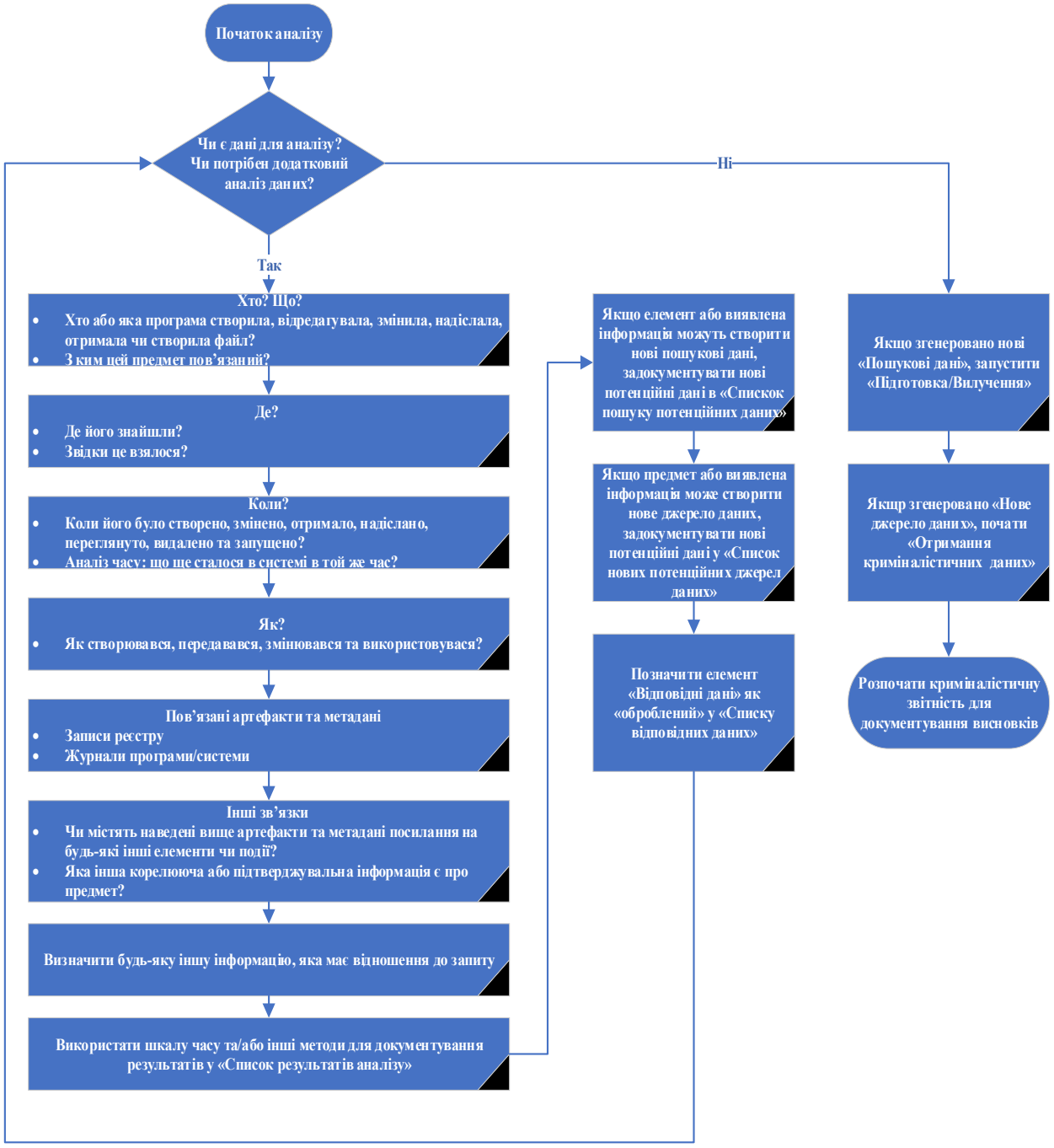

Рис. 3. Процес проведення аналізу послідовності

Перегляшувши усі показники, у видалених файлах була виявлена папка «ФІТ 1-7м паспорти», яка потенційно могла мати особисті дані потерпілих (рис.4). Після відновлення файлів папки «ФІТ 1-7м паспорти» було виявлено 19 файлів формату.docx з іменами потрепілих у яких містилися фотографії їхніх паспортів.

Отже, виявивши цифрові докази на комп'ютері зловмисника за допомогою криміналістичних інструментів та застосуванню аналізу часу та відновленню видалених файлів злочин, в якому були викрадені особисті дані був розкритий.

Висновки. Оскільки кіберзлочини (тобто будь-які кримінальні дії, пов'язані з комп'ютерами та мережами) зростають і загрожують організаційним даним, а також із збільшенням використання цифрових пристроїв широким населенням, аналіз цифрових доказів стає ключовим елементом на багатьох місцях злочину.

Судова експертиза зараз є захоплюючою професією, яка наголошує на людському факторі, але також створює проблеми через необхідність виявлення цифрових доказів у постійно мінливому середовищі. Технологічний прогрес і перехід до мережевих і хмарних середовищ, де можуть легко вступити в дію антикриміналістичні методи, зобов'язує професіоналів у цій галузі бути в курсі подій і постійно переглядати стандартні операційні процедури.

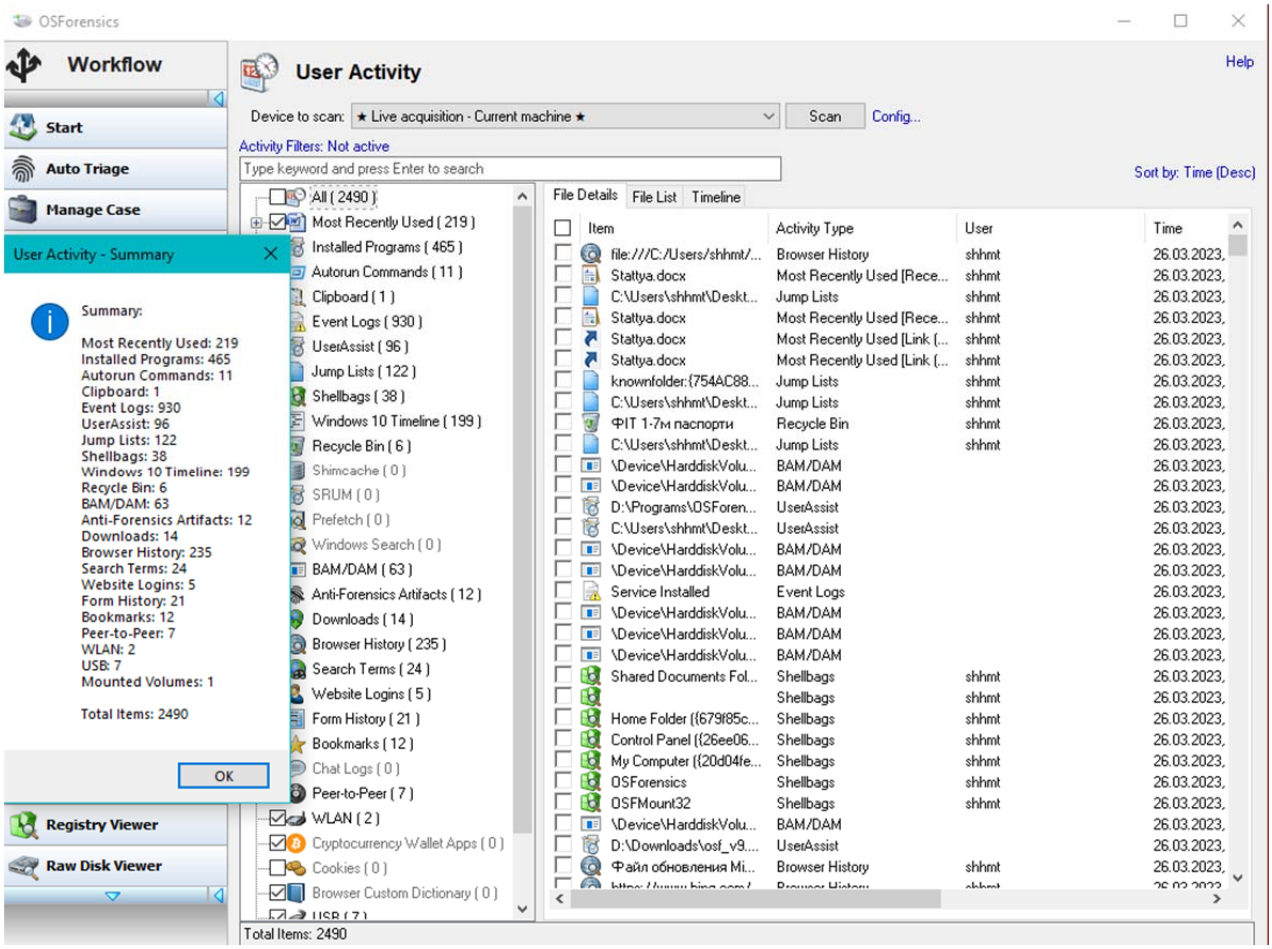

Рис. 4. Аналіз часу у програмі OSForensic

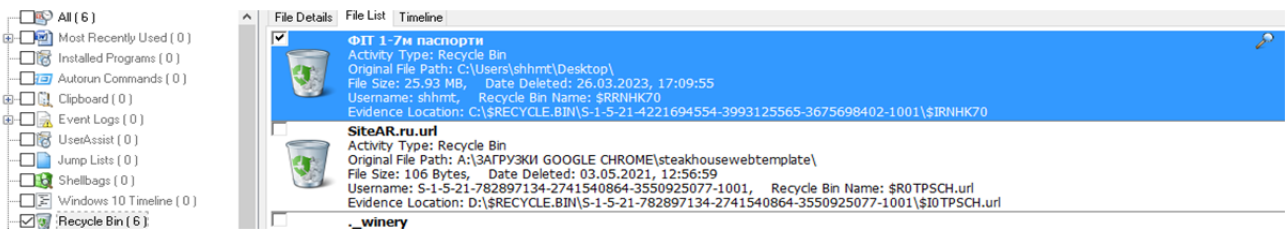

Рис. 5. Папка «ФІТ 1-7м паспорти»

На закінчення, отримання доказів комп'ютерних злочинів з використанням криміналістичних інструментів – це складний процес, який вимагає спеціалізованих знань та навичок. Використовуючи комбінацію методів, включаючи візуалізацію, відновлення файлів, пошук ключових слів та застосування різних типів аналізів криміналістичні слідчі можуть збирати цінні докази, які можуть бути використані для притягнення до відповідальності за комп'ютерними злочинами. Важливо, щоб криміналістичні розслідування проводилися юридично захищеними для того, щоб забезпечити допустимості докази в суді.

Список використаних джерел

1. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії \\ Режим доступу: https://zakon.rada.gov.ua/laws/show/995_b09#Text
2. Наукова робоча група з цифрових доказів (SWGDE) \\ Режим доступу: https://www.swgde.org/home
3. OSForensics \\ Режим доступу: PassMark OSForensics – Digital investigation

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

ІНФОРМАЦІЙНА СИСТЕМА ІНФРАСТРУКТУРИ ЗВО

ШЕСТАК Я., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто основні засади побудови архітектури інформаційної системи освітнього процесу ЗВО для надання користувачам всієї необхідної інформації, а також визначено функції та завдання окремих складових інформаційної системи. Також передбачено заходи щодо захисту інформації.

The article examines the basic principles of building the information system architecture of the educational process of higher educational institutions to provide users with all the necessary information, and also defines the functions and tasks of individual components of the information system. Information protection measures are also provided.

Актуальність. Впродовж 50 років інформатизувалися заклади вищої освіти, створювалися та впроваджувалися різні інформаційні системи, які виконували певні конкретні задачі. Надалі вони модифікувалися, трансформувалися, переходили з одних платформ на інші. Наразі практично всі освітні процеси охоплені окремими інформаційними системами у єдиному освітньому просторі, мають свої задачі та є потреба у їх детальному аналізі, оптимізації та уніфікації.

Метою статті є дослідження архітектури інформаційних систем ЗВО, особливостей їх використання та ефективності функціонування.

Об'єктом дослідження є розробка моделі архітектури інформаційної системи освітнього процесу ЗВО.

Предмет дослідження – інформаційна система ЗВО.

Аналіз попередніх досліджень. Дослідженню інформаційних систем ЗВО, побудові їх архітектури присвятили свої праці вітчизняні та закордонні науковці: М. Цюцюра, О. Криворучко, В. Биков, С. Мазур, В. Співачук, А. Литвинчук, А. Пилипчук та ін.

Виклад основного матеріалу. Інформаційна система ЗВО має багато складових, які постійно удосконалюються, розширюються їх можливості та трансформуються в залежності від потреб суспільства. В процесі цифровізації держави всі процеси автоматизуються та переводяться у цифровий формат, інформація переноситься у ієрархічні та розподілені бази даних. Для ефективного використання користувачами (викладачами, адміністраторами та здобувачами вищої освіти) інформації, яка вже накопичена, зберігається і надалі акумулюється необхідно правильно розподілити ресурси інформаційних систем. Тому, за необхідності, слід побудувати зрозумілі, відкриті і доступні інтерфейси обміну інформацією за допомогою API (спеціальні проміжні таблиці, способи підключень та організація прав доступу, читання, коригування чи знищення інформації). Важливим є організація кібернетичного захисту окремих частин та в цілому інформаційної системи освітнього процесу. Архітектура інформаційної системи має передбачати способи комунікації з зовнішніми інформаційними системами смарт-міста, що дозволить полегшити отримання коректної, вивіреної інформації з її юридичними підтвердженнями, завіреної електронними підписами тощо [2]. Автором запропонована архітектура інформаційної системи освітнього процесу ЗВО зазначена на рис 1. Вона містить ряд окремих автономних інформаційних систем:

- Система освітньої діяльності ЗВО – це інформаційна система, яка виконує функції обміну інформації між всіма користувачами інфраструктури ЗВО, визначає правила та типи користувачів, в залежності від статусу: викладач, адміністратор чи здобувач – отримує певну структуровану інформацію в залежності від запиту, потреби: розклад, навантаження, тип заняття, аудиторія з певними матеріально-технічними засобами навчання, організація вибору індивідуальної траєкторії навчання, організацію заліків, іспитів, консультацій, ознайомлення з результатами сесії, формування результуючих даних у розрізі студента, групи, груп кафедри, груп факультету, потоку чи в цілому всіх студентів ЗВО. Аналіз результатів успішності, кількісних та якісних характеристик відвідувань занять. Система включає дані щодо переведення здобувача освіти, закінчення навчання чи відрахування за неуспішність із доведенням інформації керівництву закладу засобами інформаційної системи.
- Система дистанційного навчання ЗВО – це інформаційна система, яка організовує сам процес навчання здобувачів вищої освіти в якій вони мають змогу отримувати необхідну для освіти інформацію, консультації викладачів, спілкуватись з колегами по навчанню в зручний для себе час. В системі дистанційного навчання розміщені всі необхідні методичні матеріали, електронні підручники, презентації, програми, робочі програми, методичні рекомендації для самостійної роботи здобувача вищої освіти.
- Конференц-системи для змішаного навчання, VR-системи – використовуються для розширення можливостей надання освітніх послуг та охоплення великої кількості слухачів, здобувачів та учасників конференцій і інших наукових заходів, які дають можливість очного і дистанційного навчання, чи демонстрування презентацій. Також широко почали використовувати в освітньому процесі технології віртуальної реальності VR-системи, у яких є можливість досліджувати певні процеси у віртуальному просторі.
- Система фінансово-економічної діяльності ЗВО – дає можливість у цифрому вигляді вести повний фінансовий облік матеріальних цінностей, облік всіх фінансових операцій, контролювати інформацію про фінансовий стан тощо. Система фінансово-економічної діяльності надає повну інформацію щодо прийняття управлінських рішень.
- Система кібернетичної безпеки – це система, яка забезпечує безпеку всіх інформаційних систем ЗВО, відповідно до побудованої архітектури [4].
- Системи керування серверних ресурсів – в залежності від потреби здобувачів вищої освіти, викладачів організовується розподіл ресурсів серверного обладнання, з урахуванням побудови постійного дублювання інформації, використання хмарних ресурсів – підписок Office 365(компонентів), скарб-освіти тощо – адміністратори в залежності від політики розмежування прав надають доступ до даних ресурсів.
- Система керування мережею, VPN ЗВО – для забезпечення ефективної роботи у комп'ютерній мережі, як інформаційній системі постійно ведеться моніторинг її стану,

вживаються політики безпеки на різних рівнях на комутаційному керованому обладнанню за допомогою мережного програмного забезпечення. В період воєнного стану заборонено використовувати відкриті способи доступу до ресурсів елементів мережі, тільки з використанням VPN з генерацією персонального ключа користувача, для автентифікації та не допущення організаційного порушення захисту, в залежності від активності зовнішніх користувачів система моніторингу автоматично може заблокувати для забезпечення безпеки архітектури інформаційної системи ЗВО.

Така архітектура, на нашу думку, дасть можливість повного контролю інформації, можливість відповідної побудови захисту, що наразі є актуальним в період воєнного стану в Україні. Також вона дасть можливість правильно побудувати та ефективно використати інформаційні ресурси ЗВО, дозволить оптимізувати потоки інформації, підвищить надійність такої системи [3]. В процесі експлуатації це дасть можливість у повній мірі використати гібридні інформаційні системи, поєднувати роботу у локальній мережі та використати хмарні технології, а при потребі безпечно працювати віддалено у межах інформаційної системи ЗВО. Веб ресурси ЗВО необхідно розподілити на закриті і відкриті, для правильної організації освітнього процесу.

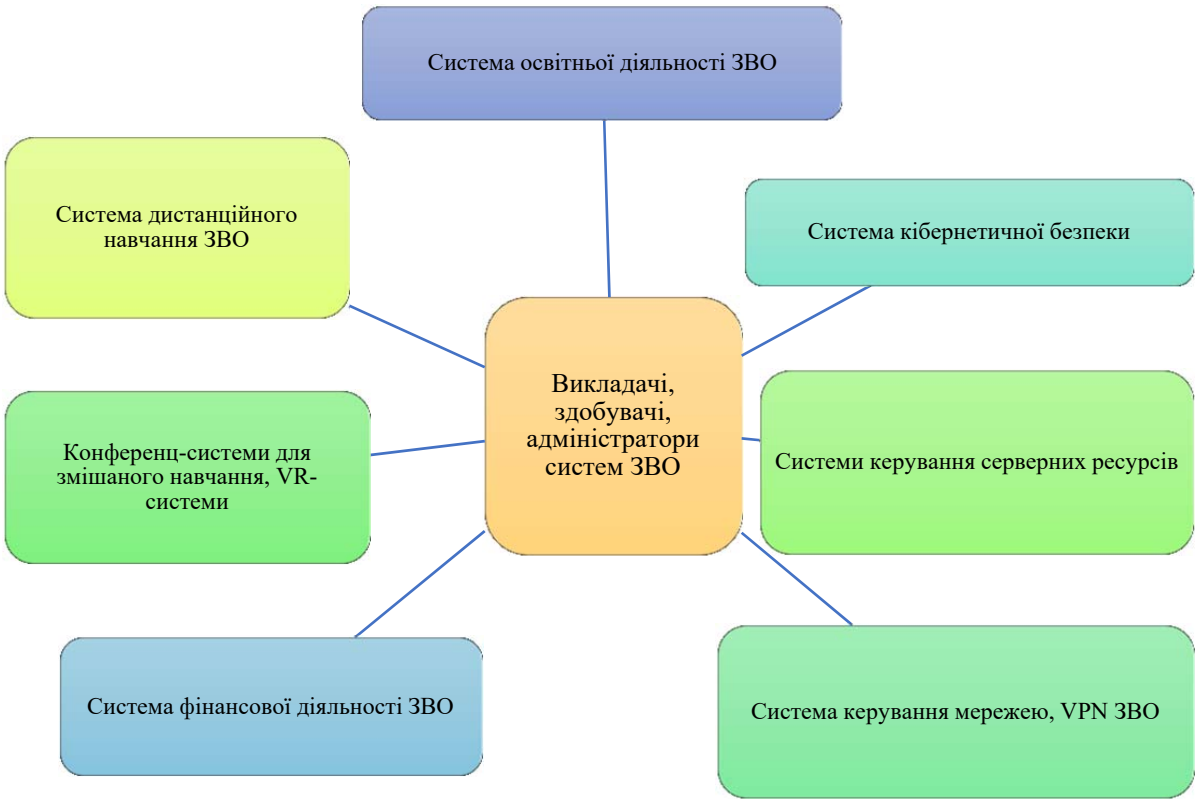

Рис. 1. Архітектура інформаційної системи освітнього процесу ЗВО.

Система освітньої діяльності ЗВО – постійно розвивається та охоплює процеси, що автоматизують введення інформації: сканування, цифрової трансформації, створення фото, відео, аудіо масивів структурованих даних, які при потребі аналізуються, відбираються та відтворюються у освітньому просторі. Цифровізовано процес навчання здобувачів вищої освіти, підготовку. Прикладом інформаційної системи керування освітнім процесом – є українська розподілена система MIA: Освіта. До функціоналу даної системи входять блоки:

- електронний кабінет,
- навантаження студента та викладача,
- створення оголошення до розкладу та тематичного плану,

- консультації,
- електронний журнал,
- графік прийому відпрацювань,
- тематичний план,
- список (академічної групи, віртуальної групи, потоку, кафедри, дисципліни за записом),
- гуртожиток (реєстрація проживаючих студентів, бронювання студентами кімнат),
- статистика успішності та відвідуваності,
- екзаменаційна відомість,
- атестації,
- стипендіальний рейтинг,
- інформатор,
- робочий план,
- ведення всього контингенту студентів (зарахування, переведення та відрахування, створення наказів на студентів),
- створення віртуальних груп, для вибіркових дисциплін,
- створення та редагування електронного розкладу для всього контингенту студентів та викладачів у розрізі студента, групи, курсу, факультету, викладача, у межах поточного тижня, поточного місяця, попереднього і наступного місяця, та заданого діапазону;
- створення переліку дисциплін освітнього закладу, спеціальності, спеціалізації, груп, викладачів на кафедрах та навчальних планів;
- розподіл навантаження кафедри, аудиторій та створення звітів навантаження по закладу освіти.
- формування потоків груп;
- формування індивідуальних карток здобувачів.

Система MIA: Освіта – є мультисистемна, працює на операційних системах з Windows XP до Windows 10, на всіх версіях Linux та IOS. Є як локальна версія для роботи в середині локальної мережі кампусу ЗВО, так і Web-версія для роботи через глобальну мережу Інтернет. Так можлива робота віддалено з любої точки, головне мати персональний доступ до ресурсу. Водночас сьогодення пропонує закладам освіти широкий вибір систем дистанційної освіти, у багатьох є всі необхідні компоненти для забезпечення освітнього процесу. Найпоширеніші наразі системи, які використовують хмарні ресурси Microsoft Office 365, застосунки Google, edx courses, рідше використовують Moodle, але вони не забезпечують увесь процес дистанційного навчання, немає повноцінної системи відеоконференцзв'язку. Найбільше вищих закладів вищої освіти визначилися і використовують Microsoft Office 365 та застосунки Google. Використовують компоненти Microsoft Office 365: Outlook, Word, Excel, PowerPoint, Power BI, OneNote, OneDrive, SharePoint, Skype для бізнесу, Teams, Sway, Forms, Stream, Flow, PowerApps, School Data Sync. Застосунки Google: Google Клас, Google Meet, Google Календар, Google Диск, Google Документи, Google Таблиці, Google Форми, Google Презентації, Google Keep, Google Сайти, Google Jamboard. У багатьох ЗВО використовують системи архівації та збереження інформації, але організаційно складно контролювати наповнення архівів, вчасне оновлення та їх зберігання. Для цього розробляють ресурси для автоматичного збереження даних, спеціальні програмні модулі збирають у визначених місцях операційної системи файли, архівують із зазначенням дати і часу та переміщують у файлове сховище через спеціальні інтерфейси захищеної передачі даних. Таким чином файли щодня зберігаються і при потребі використовуються для відновлення інформації.

Ефективним є використання конференцсистем для змішаного навчання. Всі матеріали розміщуються у системах для забезпечення дистанційного навчання, та використовуються платформи, що дозволяють забезпечити освітній процес у змішаному режимі, так Teams – дозволяє підключати віддалено студентів для отримання знань і умінь. Таким чином одночасно всі в однакових умовах можуть у онлайн режимі та очно проходити навчання.

VR-системи значною мірою використовуються для апробації з використанням віртуального середовища, середовища наближеного до реального.

Для ведення фінансово-економічної діяльності закладу вищої освіти використовують автоматизовані цифрові системи, до прикладу МІА: Облік і звітність, яка повністю забезпечує всі процеси і зв'язки з зовнішніми е-інфраструктурами: МОН, банки, фіскальні системи, урядові системи, іншими системи цифрового міста. До складу МІА: Облік і звітність входять наступні блоки:

- відтворення всіх бухгалтерських операцій фінансово-економічної діяльності,
- проведення виплат стипендії, соціальної стипендії, заробітної плати та інші платежів,
- облік матеріально-технічного забезпечення,
- прогнозування планування витрат,
- ведення обліку контингенту: студентів (зарахування, переведення та відрахування, створення наказів на студентів); працівників (викладачів та допоміжного персоналу); студентів, аспірантів – контрактників; військовозобов'язаних, а також міжнародних студентів.

МІА: Освіта та МІА: Облік і звітність є важливими інформаційними та рекомендаційними системами для прийняття ефективних рішень керівництвом закладу, за їх допомогою можна бачити стан діяльності ЗВО. Це дає змогу будувати правильну стратегію розвитку ЗВО та впливати на результати його діяльності.

Найскладнішими наразі є системи керування мережею, серверними ресурсами та контролем VPN-підключень. Ці системи забезпечують надійний зв'язок між інформаційними системами, серверами, користувачами та зовнішніми е-інфраструктурами Smart-міста. Найскладнішим є неоднорідність клієнтських підключень, багатофакторність інтерфейсів зв'язку у локальній дротовій мережі, доступ у бездротових мережах і доступність серверних ресурсів та забезпечення контролю використання хмарних ресурсів. Всі ці задачі постійно трансформуються, окремі інформаційні системи розвиваються, тому і змінюються їх канали передачі інформації, але забезпечується цілісність сукупної інформації по ЗВО в цілому.

Система кібернетичної безпеки будується на основі вивчення всіх факторів ризику інформаційних системи окремо та інформаційної системи ЗВО загалом. Розробляються організаційні заходи кіберзахисту із застосуванням апаратних та програмних засобів. По-перше для доступу до інформаційних систем використовується двохфакторна автентифікація, використання КЕП (контрольованих електронних ключів) апаратних та програмних для підтвердження особистості. Також у системах використовуються системи шифрування каналів передачі інформації, заборонено відкрито відправляти поштовими повідомленнями документацію. Таким чином забезпечуватиметься захист інформації від перехоплення. Всі бази даних шифруватимуться та додатково захищатимуться за допомогою апаратних чи програмних FireWall (рис 2). Доступ до мережі Інтернет повністю контрольований, окремо налаштовуються резидентні підключення по VPN до зовнішніх е-інфраструктур.

Так інформаційною системою інфраструктури можна визначити – сукупність апаратних і програмних засобів, котрі поєднані системами зв'язку та які мають внутрішній контроль доступу до ресурсів, а також виконують певні задачі у загальній інфраструктурі, але можуть працювати окремо, незалежно від інших систем: можуть самостійно розвиватися та не впливати на інші інформаційні системи.

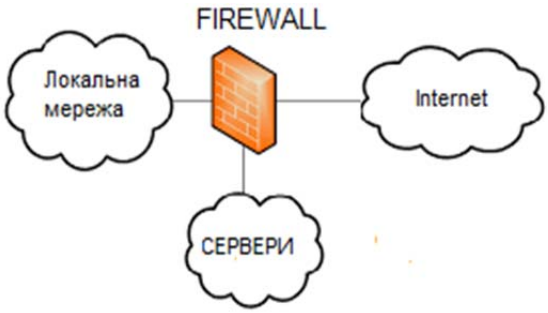

Рис. 2. Схема застосування FireWall

Постійно трансформуються технічні засоби навчання, деякі припиняють використовуватися, такі як лампові графопроектори, лампові мультимедійні проектори, бо їх замінюють на лазерні мультимедійні проектори, SmarBoard, SmartWall – які використовуються за допомогою інтерактивних застосунків, що покращує сприйняття здобувачами вищої освіти інформації. Також можливі варіанти відтворення віддаленого навчання, коли викладач знаходиться за межами закладу вищої освіти, а здобувачі у аудиторії, та завдяки відеоконференцсистемам, Інтернету забезпечується повноцінний освітній процес. З'являється можливість використання різних застосунків, участь більшої кількості здобувачів освіти в освітньому процесі. Так інформаційні системи інфраструктури ЗВО пов'язані між собою, доповнюють одна одну та дають можливість відтворювати всі можливі варіанти надання методичних матеріалів, забезпечення та контроль освітнього процесу, коригування та удосконалення при потребі навчальних матеріалів, самих систем. Керівники таких інформаційних систем отримують повну інформацію з можливістю правильного прийняття управлінських рішень для більш повного задоволення потреб суспільства та роботодавців. Сучасні інформаційні системи інфраструктури ЗВО наближаються до цифрових екосистем.

Висновки. Правильно побудувавши інформаційну систему освітнього процесу ЗВО, ми отримаємо модель системи, де можемо прогнозувати та передбачати стійкість системи. Важливим місцем у даній системі є співвідношення всіх окремих інформаційних систем, які постійно розвиваються, трансформуються, тому можна контролювати процеси підготовки і впровадження оновлень. Запропонована архітектура дає можливість побудови кіберзахисту інформаційної системи. Ефективність управління інформаційною інфраструктурою ЗВО дасть можливість покращення результатів освітнього процесу, надати більше інструментів для провадження навчання студентів, що задовольнить у більшій мірі потреби громадян і суспільства.

Список використаних джерел

1. Биков В.Ю. Проблеми та перспективи інформатизації системи освіти в України / В.Ю. Биков // Науковий часопис НПУ імені М.П. Драгоманова. Серія №2. Комп'ютерно-орієнтовані системи начання. – К.: НПУ імені М.П. Драгоманова, 2012. – № 13 (20). – С. 3-18
2. Управління розвитком складних систем:(КНУБА) УДК 004.94:378.4, Моделювання єдиного інформаційного простору закладу вищої освіти, Шестак Ярослав, ст 82-89, DOI: dx.doi.org\10.32347/2412-9933.2022.49
3. Міжнародний науково-практичний журнал «Товари і ринки»: (КНТЕУ) (№1 2021): УДК 004.7.056.5(477)(045), Кібербезпека та захист інформації під час пандемії COVID-19, Білявська Юлія, Микитенко Неля, Шестак Ярослав, ст 34-46, DOI: https://doi.org/10.31617/10.31617/tr.knute.2021(37)03
4. Міжнародний науково-практичний журнал «Товари і ринки»: (ДТЕУ) (№3 2022): УДК 004.056:004.9, Кібербезпека та кібергігієна: нова ера цифрових технологій, Білявська Юлія, Шестак Ярослав, ст 47-59, DOI: https://doi.org/10.31617/3.2022(43)04

Робота виконана під науковим керівництвом канд. техн. наук, доцента
ХАРЧЕНКА О. А.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

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

У статті розглянуто широке застосування новітніх інноваційних підходів і технологій, які зумовили трансформацію форм і методів діяльності суб'єктів правовідносин для збільшення їхніх функціональних можливостей, захисту даних та зменшення витрат.

This article considers the widespread use of the latest innovative approaches and technologies that have led to the transformation of the forms and methods of activities of legal entities to increase their functionality, protect data and minimize expenses.

Актуальність. З розвитком засобів інформаційних комунікацій та можливістю завдати шкоди інформації, що зберігається та передається завдяки їм, з'явилося поняття інформаційної безпеки. Інформаційна безпека допомагає захистити інформацію та інформаційну інфраструктуру від загроз.

Такі впливи можуть бути випадковими або умисними, внутрішніми або зовнішніми, і можуть призвести до втрати важливої інформації, її незаконної модифікації або використання третіми особами. Гарантувати повну та якісну інформаційну безпеку можливо лише за умови застосування системного та цілісного підходу.

Технологія блокчейн почала свій розвиток як платформа для криптовалюти Біткоїн, але згодом стала перспективною технологією задля забезпечення захисту інформації. Блокчейн пропонує широкий спектр можливостей для підтримки надійного рівня безпеки даних завдяки механізмам шифрування, цілісності даних, стійкості мережі та масштабованості. В результаті чого, перехід від традиційної системи інформаційної безпеки до системи на основі блокчейну може бути вигідним для організацій практично в будь-якій галузі.

Метою статті є дослідження особливостей використання технології блокчейн як систему захисту в різних галузях.

Об'єктом дослідження є методи та способи забезпечення інформаційної безпеки на основі технології блокчейн.

Предметом дослідження є способи захисту інформації від загрози викрадення, а також уже реалізовані системи забезпечення інформаційної безпеки на основі технології блокчейн.

Аналіз попередніх досліджень. Наукові дослідження застосування технології блокчейн у сфері публічних відносин практично відсутні. Це питання є частково розглянуто в дослідницьких роботах таких науковців 0. А. Баранова, І. В. Давидової, О. Д. Довганя, І. М. Дородіна, О. Е. Сімсон, Р. О. Стефанчука, Р. В. Чорнолуцького та ін.

Виклад основного матеріалу. Технологія блокчейну, що є основою криптовалют, таких як Bitcoin та Ethereum, здатна забезпечити надійний захист інформації. Багато компаній починають використовувати блокчейн для забезпечення безпеки своїх даних та інформації клієнтів.

Технологія блокчейн – це децентралізований або розподілений електронний реєстр достовірних та незмінних даних, що грунтується на криптографічних алгоритмах і фіксує інформацію про всі здійснені транзакції у цифровому просторі за допомогою створення блоків-транзакцій [7].

Основа технології блокчейну полягає у збереженні даних у вигляді ланцюга блоків, кожен з яких містить криптографічно захищену інформацію. Кожен блок містить у собі хеш

попереднього блоку, що забезпечує надійність інформації. Таким чином, будь-які зміни в одному блоку, автоматично впливають на всі інші блоки у ланцюжку.

Однією з переваг технології блокчейну є те, що вона забезпечує безпеку за допомогою децентралізації. Інформація зберігається на кожному комп'ютері, що відповідає за обробку та підтвердження транзакцій в мережі. Це забезпечує безпеку даних усіх типів блокчейну (Таблиця 1), оскільки для того, щоб хакер взломав систему, він мусить взломати кожен комп'ютер, що приймає участь у мережі. Це зробить атаку на систему непрактичною, навіть якщо зловмисник має значні ресурси.

Таблиця 1

Види блокчейну, які використовуються для захисту даних

Вид блокчейну	Опис
Публічний блокчейн	Це відкритий блокчейн, до якого можуть мати доступ всі користувачі. Він децентралізований і не підлягає контролю жодного централізованого органу або особи. Приклади: Bitcoin, Ethereum.
Приватний блокчейн	Це закритий блокчейн, до якого мають доступ лише відповідні користувачі, які мають дозвіл на доступ до системи. Він підконтрольований централізованим органом або особою, і може використовуватися для конфіденційної обробки даних. Приклади: Hyperledger Fabric, Corda.
Консорціальний блокчейн	Це гібридний блокчейн, який поєднує в собі як публічний, так і приватний блокчейн. Він використовується для спільної роботи групи організацій з різних сфер діяльності. Приклади: R3 Corda, Hyperledger.
Федеративний блокчейн	Це блокчейн, управління яким здійснюється кількома централізованими органами або особами, які мають дозвіл на доступ до системи. Приклади: Ripple, Stellar.

Всі види блокчейну можуть забезпечити захист даних. Кожен блок містить хеш попереднього блоку, який зберігає інформацію про стан системи на момент попереднього блоку. Це означає, що якщо будь-які зміни внесені в попередній блок, хеш наступного блоку автоматично стає недійсним. Це змушує зловмисників переглядати і перевіряти хеші всіх попередніх блоків для того, щоб змінити дані в останньому блоку. Це ускладнює зловмисникам атакувати систему, оскільки їм потрібно змінити кожен блок в ланцюжку. Він може забезпечувати прозорість та безпеку даних за допомогою розумного контракту. Розумний контракт – це програмний код, який автоматично виконує певні дії, коли виконуються відповідні умови. Розумний контракт може забезпечити безпеку даних, оскільки його виконання залежить від умов, які визначені у контракті, та він може автоматично виконувати дії для забезпечення безпеки даних.

Блокчейн містить базу даних про всі раніше здійснені операції та дозволяє ефективно й оперативно виконувати операції між двома сторонами в режимі онлайн, де всі транзакції перевіряються і підтримуються децентралізованою мережею комп'ютерів.

Важливо, що записи зберігаються в зашифрованому вигляді одночасно у всіх учасників системи й автоматично оновлюються з кожним внесенням змін. Користувачі виконують роль колективного нотаріуса, який підтверджує правдивість інформації в базі даних, і забезпечують захист від маніпуляцій та зловживань.

Завдяки технології блокчейн кожен договір, процес, платежі матимуть цифровий запис, який можна буде ідентифікувати, перевірити, зберегти і поділитися ним.

Система блокчейн підтримується і захищається криптографічними алгоритмами і протоколами, наприклад, цифровими підписами, хеш-функціями. Ці засоби гарантують, що транзакції, які записуються в реєстр, захищені, їх автентичність підтверджена і вони не можуть бути скасовані.

Структура мережі блокчейн складається з хешів або хеш-кодів. У системі блокчейн це унікальний числовий ідентифікатор фіксованої довжини, який генерується з даних блоку за

допомогою хеш-функції (Рис. 1). Хеш служить для забезпечення цілісності та безпеки даних в блокчейні, оскільки будь-яка зміна даних в блоку призведе до зміни його хешу. При перевірці блоку на його валідність, перевіряється, чи відповідає хеш блоку відомому значенню, яке було розраховано при створенні блоку. Це дозволяє запобігти підробці даних в блокчейні.

Одним з прикладів використання хешу у блокчейні є майнінг криптовалют. Для отримання нового блоку майнер повинен розв'язати криптографічну задачу, яка включає в себе створення хешу блоку, який відповідає певному критерію складності. Це забезпечує безпеку мережі, оскільки додавання нового блоку вимагає значних обчислювальних зусиль та ресурсів.

Хеші можна використовувати для шифрування повідомлень, контролю цілісності даних, побудови індексів та багато іншого. Їх ефективність і безпека досить високі, і тому вони широко використовуються в різних галузях, включаючи блокчейн технології [10].

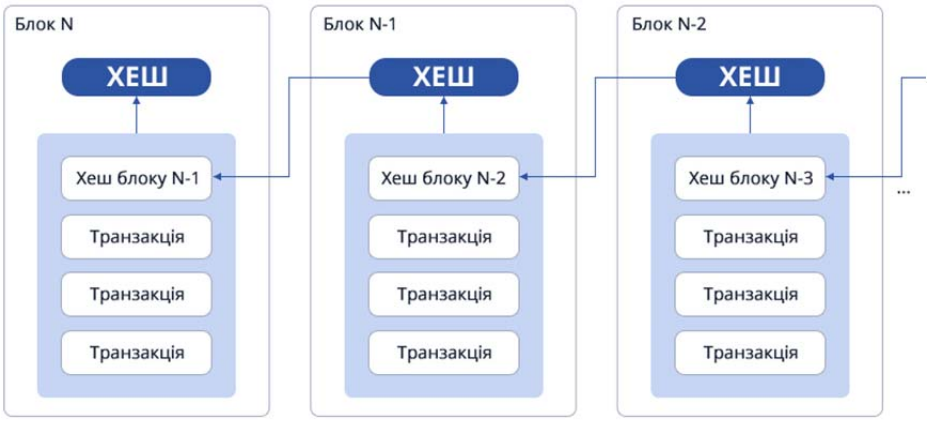

Рис. 1. Структура мережі блокчейн

Хеш-функції – це один з найпоширеніших криптографічних алгоритмів у технології блокчейн. Це криптографічні алгоритми, призначені для забезпечення цілісності даних в технології блокчейн. Будь-який фрагмент даних може бути хешований, незалежно від його розміру або типу. У традиційному хешуванні, незалежно від розміру, типу або довжини даних, хеш, згенерований з будь-яких даних, завжди має однакову довжину.

Хеш-функція приймає початковий потік (числа, алфавіти, мультимедійні файли) будь-якої довжини і перетворює його в новий рядок фіксованої довжини. Фіксована довжина може бути різною (наприклад, 32-бітною, 64-бітною, 128-бітною або 256-бітною) залежно від типу хеш-функції, що використовується. Рядок заданої довжини називається хешем.

Технологія блокчейн є розподіленою мережею, вона потребує протоколу консенсусу, який містить в собі правила, яких повинен дотримуватися кожен учасник, щоб досягти глобальної єдиної точки зору. Протокол консенсусу є механізмом, за допомогою якого в мережі блокчейн досягається згода щодо дійсності транзакцій і відбувається підтвердження нових блоків. Він забезпечує спільне розуміння того, яка частина мережі має право на генерацію наступного блоку та як саме це має відбутися.

Існують різні види протоколів консенсусу, у кожного з яких є свої переваги та недоліки, і вибір певного протоколу залежить від конкретного застосування та потреб користувачів:

1. Proof of Work (PoW). Базується на математичних обчисленнях, які забезпечують безпеку мережі. Протокол вимагає від групи майнерів розв'язування складної криптографічної задачі, і перша особа, яка вирішує задачу, отримує можливість додати блок до ланцюжка. Bitcoin використовує протокол PoW.

2. Proof of Stake (PoS), де замість обчислень вимагає від користувачів вкладення (стейкінг) своїх монет для отримання можливості додавання блоку. У порівнянні з PoW, PoS є енергоефективнішим та менш витратним у плані обладнання.

3. Delegated Proof of Stake (DPoS). Подібний до PoS, але включає в себе вибір делегатів, які мають право на додавання блоків до ланцюжка. Делегати обираються голосуванням учасників мережі.

4. Proof of Authority (PoA) – вимагає наявності авторитету в мережі, який підтверджує дійсність блоків. Авторитетом можуть бути урядові органи, корпорації, експерти, або будь-які інші сторони, що мають довіру в мережі.

5. Proof of Elapsed Time (PoET) – заснований на виборі першого випадкового учасника мережі, який має право на додавання блоків до ланцюжка. Він працює за принципом вибіркового доступу, де обрання випадкового учасника відбувається з розрахунку його потужності та доступності.

Однак, протоколи консенсусу також мають деякі недоліки:

- Великі витрати на обчислення: деякі протоколи консенсусу можуть вимагати великих обчислювальних потужностей, що може збільшувати вартість утримання мережі.
- Проблеми з масштабованістю: деякі протоколи консенсусу можуть мати обмеження на кількість транзакцій, які можуть бути оброблені за один блок. Це може призвести до затримок у обробці транзакцій під час періодів високого навантаження.
- Ризик централізації: деякі протоколи консенсусу можуть стати дуже важкими для реалізації на великих мережах, що може призвести до концентрації влади в руках деяких груп або індивідів.

Незважаючи на ці недоліки, протоколи консенсусу є важливою складовою системи блокчейн і забезпечують її надійність та безпеку, особливо в умовах де відсутня довіра, блокчейн надає користувачам такі бажані функції, як анонімність, прозорість, незмінність, що привертає велику академічну та промислову увагу в останні кілька років. Завдяки цим перевагам технологія блокчейн привернула велику увагу науковців і підприємців в останні кілька років.

Блокчейн дозволяє побудувати довіру в інтернеті, яка може забезпечити більш прозору, безпечну та ефективну систему для всіх. Вона може збільшити інновації, знизити витрати та покращити якість життя людей у всьому світі [8, с. 78].

Блокчейн є ідеальним засобом для збереження подій у мережному середовищі, оскільки система записує і вибудовує їх у строго хронологічному порядку. У даному контексті блокчейн можна описати як послідовну структуру даних, що складається з ланцюжка блоків зв’язаних між собою за допомогою хеш-покажчиків, що містяться в заголовку кожного блоку. Ця структура є односпрямованою та без зворотного зв’язку.

Вузли блокчейна здійснюють алгоритми консенсусу, якщо кілька вузлів знаходяться в автономному режимі, інші продовжують працювати, навіть якщо вони були переведені в автономний режим внаслідок хакерської атаки. Робота відновлюється, коли вузли відновлюють зв’язок між собою, повертаються в оперативний режим і проводять пересинхронізацію вузлів, щоб забезпечити послідовність і цілісність всього ланцюжка. Ця можливість існує завдяки унікальному набору закодованих алгоритмів у системі блокчейн.

Також кожен блок в мережі блокчейн складається з двох основних частин – голови і тіла. Голова містить інформацію, яка забезпечує стабільність і непохитність мережі. Тіло містить перелік всіх транзакцій, які повинні зберігатися в цьому блоці і бути внесені в мережу блокчейн.

У класичній блокчейн мережі Head містить такі поля [2]:

- номер версії блоку (ver_block);
- хеш попереднього блоку (prev_block);
- хеш усіх транзакцій у поточному блоці (mrkl_root);
- тимчасову мітку, коли було створено блок (timestamp);
- «bits» і «nonce» параметри, що використовуються при майнінгу.

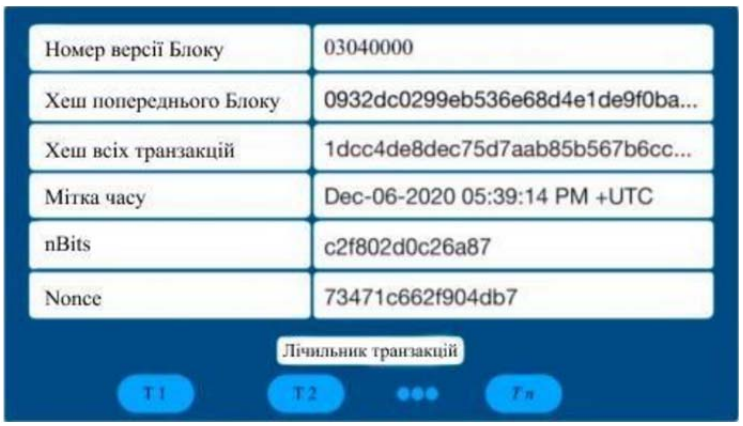

Рис. 2. Структура блоку

У системі захисту блокчейн важливу роль відіграє Payload, оскільки це дані, які передаються та зберігаються в блоках. Payload, як правило, містить дані, які потрібні для збереження в ланцюгу блоків. Ці дані можуть бути інформацією про транзакції, метаданими або будь-якою іншою корисною інформацією [9, с. 91].

Payload зашифрований та не може бути змінений після його занесення в блокчейн, що робить його даними, які не можуть бути підроблені або внесені ззовні. Payload може містити метадані, які можуть бути використані для підтвердження автентичності та джерела даних, що зберігаються в блоках. Наприклад, в цифрових платіжних системах Payload може містити інформацію про отримувача та відправника, дату та час транзакції, суму переказу.

Payload складається з лічильника транзакцій і списку всіх транзакцій, включених до існуючого блоку. Існує також максимальна кількість транзакцій, яку може вміщувати блок. Це значення залежить від розміру транзакції. Для того, щоб перевірити справжність транзакції використовується механізм асиметричної криптографії.

Цифровий підпис є невід'ємною частиною системи блокчейн і являє собою криптографічний алгоритм, який накладається особою, що використовується для перевірки справжності та цілісності документа, а також для встановлення авторства документа.

Криптографічні цифрові підписи, які базуються на асиметричній криптографії, відіграють вирішальну роль у безпеці блокчейн-мереж. Ці цифрові підписи дозволяють здійснювати безпечні та автентифіковані транзакції без необхідності використання надійного посередника. Цифрові підписи є важливим компонентом технології блокчейн, що дозволяє учасникам перевіряти автентичність і цілісність даних у мережі [11].

Криптографія з відкритим ключем та хеш-функцією надають математичні інструменти, які дозволяють ефективно використовувати цифровий підпис. Використання шифрування та цифрових підписів є важливою умовою функціонування мережі блокчейн. Хешування дозволяє кожному з учасників мережі визначити актуальний стан блокчейну, а цифрові підписи забезпечують доказ того, що всі операції були здійснені виключно справжніми користувачами.

У Лондоні 9 грудня 2014 року розпочало свою роботу Digital 5 (D5), об'єднання провідних цифрових країн (Естонії, Ізраїлю, Нової Зеландії, Південної Кореї та Великої Британії) з головна мета цього об'єднання, це розвитку цифрової економіки. Представники урядів цих країн зобов'язалися трансформувати відносини уряду з технологіями, підтримуючи використання відкритих стандартів та програмного забезпечення з відкритим кодом, а також підвищуючи ефективність роботи цифрового уряду.

Учасники Digital 5 визначили основні принципи цифрового розвитку: потреби користувачів; відкриті стандарти; відкритий код; відкриті ринки; відкритий уряд (прозорість); зв'язок; навчання дітей програмуванню; доступність цифрових послуг; обов'язок ділитися і вчитися [3]. Ці принципи можуть доповнюватися і вдосконалюватися з урахуванням нових проблем і можливостей інформаційних технологій.

Значне поширення новітніх інноваційних підходів та технологій спричинило трансформацію форм та методів діяльності юридичних осіб з метою підвищення їх функціональності, захисту даних та зменшення витрат. З кожним роком все більше юридичних осіб публічного та приватного права застосовують сучасні інформаційно-телекомунікаційні технології для покращення рівня ефективності та результативності своєї діяльності. До таких технологій відносяться: Internet of Things, Cloud Technology, Blockchain, Mobile ID, Big Data.

У січні 2018 року реалізація найкращих світових практик електронного урядування дозволила Україні увійти до переліку 14 країн, які визнані лідерами у впровадженні технології блокчейн. Технологія блокчейн в основном використовується в банківському, фінансовому та страховому секторах. Однак її можливий вплив та використання в державному управлінні ще не до кінця вивчені.

Британська науковець Мелані Свон у своїй книзі «Блокчейн: схема нової економіки (англ. Blockchain: Blueprint for a New Economy») [5], беручи до уваги поточні та потенційні технологічні аспекти блокчейну, визначила етапи еволюції даної технології: *блокчейн 1.0* – це валюта.

Криптовалюта використовується для здійснення цифрових переказів і платежів. Серед сучасних електронних валют найпоширенішою є біткойн, концепція якого була викладена у 2008 році професором Сатоші Накамото у статті «Біткойн: пірингова електронна грошова система» (Рис.3).

Рис. 3. Зображення монети Bitcoin

Блокчейн 2.0, забезпечує можливість обробки різних типів фінансових операцій, включаючи операції з цінними паперами, акціями та частками в компаніях, механізмами краудфандингу, заборгованістю, пенсійними фондами та деривативами (ф'ючерсами, облігаціями, опціонами та свопами);

Блокчейн 3.0, галузь якого виходить за межі економічної та фінансової діяльності та охоплює державне управління, охорону здоров'я, науку, освіту, культуру та мистецтво [5].

Застосування технології блокчейн має свої переваги та недоліки. Перевагами можуть бути: забезпечення високоефективних механізмів захисту цілісності та доступності інформації; створення повністю автономної системи; захищеність системи від несанкціонованого втручання та модифікації інформації, що зберігається в реєстрі; економія коштів у порівнянні зі зберіганням інформації на паперових носіях та використанням традиційних технологій зберігання даних на машинних носіях [1, с. 76]; неможливість внесення правок до реєстру даних з попередньою датою; підвищення рівня захисту державних баз даних від стороннього втручання при дотриманні певних умов.

При застосуванні технології блокчейн існують певні ризики:

- оприлюднення персональних даних та конфіденційної інформації;
- низька продуктивність та швидкість роботи бази даних;

- рівень безпеки та децентралізації системи напряму залежить від кількості його учасників та потужності обчислювальних систем;
- можливість внесення недостовірних даних; людський фактор при управлінні доступами до реєстрів;
- ідентифікація користувачів бази даних.

Не дивлячись на певні ризики при застосування цієї технології, блокчейн вважається надійно захищеною та удосконалюється з кожним роком все більше. Окрім криптографічного захисту, використання алгоритмів консенсусу та наявності децентралізованої структури, дана система має вбудовану систему автоматичної верифікації, що гарантує, що тільки правильні дані можуть бути записані в блокчейн. Це забезпечує достовірність даних та унеможливлює їхнє підроблення.

Значна популярність цієї ідеї, щодо застосування технології блокчейн для державних реєстрів, на думку І. Дороніна, передусім пов'язана із загальною недовірою суспільства до діяльності державних органів, які відповідальні за такі реєстри, дані установи навпаки повинні забезпечувати захист прав власників та зберігати інформацію в належному вигляді [1, с. 76-77]. Технологія блокчейн має значні перспективи і надає можливість якісно трансформувати сферу інтелектуальної власності у напрямку забезпечення надійними доказами авторства, полегшенням контролю за контентом та управління правами користувачів.

На сучасному етапі розвиток блокчейн технології в Україні повинен відбуватися за умов належної цифрової ідентифікації особи заявника об'єкта інтелектуальної власності та комплексного правового регулювання. Тільки за таких умов можливе створення оптимальної правової моделі захисту прав інтелектуальної власності на основі блокчейн та забезпечення повної довіри майбутніх користувачів до даної системи.

Найпершими експериментальними проєктами в Україні, які використовують систему зберігання та захисту даних блокчейн, є електронні земельні аукціони, робота Державного земельного кадастру, Державного реєстру речових прав на нерухоме майно та Системи електронних торгів арештованим майном (СЕТАМ).

16 червня відбулося підписання Меморандуму про співпрацю щодо створення новітньої цифрової системи захисту даних Державного земельного кадастру від зовнішнього втручання. Програмний продукт буде розроблений на базі технології Blockchain, яка є найбільш досконалою із існуючих на сьогодні в сфері захисту даних [6].

Попри те, що блокчейн-технології мають значний потенціал у вирішенні багатьох фінансово-економічних питань для різних секторів економіки, на практиці впровадження таких технологій має певні нюанси, що виникають при впровадженні цих технологій.

Проаналізувавши всі плюси та мінуси даної технології, можна дійти до висновку, що технологія вимагає унікального рівня організації, компанії мають бути згодні на впровадження нових ресурсоємних технічних, функціональних та юридичних механізмів. Незважаючи на це, та щорічні витрати на систему блокчейн які досягли відмітки в 1,7 мільярда доларів, багато фінансових компанії не змогли реалізувати переваги ранніх інвестицій, а низка пілотних проєктів було закрито.

На первинному етапі впровадження технології блокчейн у галузі реєстрації земельних договорів існує ймовірність виникнення складнощів з первинною ідентифікацією власників земельних ділянок, оскільки інформація, що вводиться в блокчейн-реєстри, сама по собі не є достовірною. Блокчейн забезпечує гарантію незмінності даних, а не їх правдивості, оскільки ця система може бути використана лише для перевірки або надання витягів про те, чи не є вони підробкою. Однак неможливо перевірити достовірність даних, що містяться в такому витягу [4].

В теорії і в перспективі за допомогою працюючих блокчейн-платформ можна буде просто, недорого і безпечно реєструвати юридичні особи, права на нерухоме і рухоме майно, інтелектуальну власність, складати заповіти, здійснювати збір податків, виплачувати пенсії, видавати цивільні паспорти.

Згідно з концепцією, поєднання прозорості та захищеності блокчейна робить цю технологію привабливою для використання в електронних державних послугах (e-Government). Наприклад, громадянин оплачує адміністративний штраф або податок, а інформація про погашення миттєво з'являється і оновлюється у всіх учасників блокчейн-платформи.

Крім стабільності така система відрізняється низькими транзакційними витратами: в результаті немає необхідності утримувати велику структуру персоналу, що значно здешевлює адміністративні витрати, а головне мінімізує і виключає корупцію. Інформація про об'єкти нерухомості, угоди, реєстрацію прав власності, обтяження і стан об'єктів повинна буде заноситися в розподілені реєстри, доступ до яких можна буде отримати і з персональних комп'ютерів, і через мобільні додатки.

Таким чином, для переходу системи державного управління на технологію блокчейн важливо розробити юридично вивірений і висококонтрольований механізм передачі офлайн-даних до державних реєстрів.

Головна проблема технології наразі – це недосконалі механізми регулювання. Адже концепція регулювання прогресивної технології сама по собі є нереальною і недосяжною. Тож варто зосередитись на створенні певних світових стандартів, а також етичних принципів та принципів належного управління, оскільки вони по суті є інструментами, необхідними для росту та розвитку нової технології. Але при цьому вкрай важливо уникнути надмірного регулювання.

Ефективна робота залежить насамперед від точності формування реєстрів громадян, нерухомості та компаній. Справа в тому, що ні збереження цілісності даних у разі випадкових збоїв чи атак, ні запобігання маніпуляціям з уже введеними даними не є головними загрозами для державних IT-систем. Справжньою небезпекою є внесення до реєстрів завідомо недостовірних даних. Вочевидь, сервіс блокчейн тут виявляється безсилим. Він є лише інструментом.

В Україні здійснюються певні кроки щодо законодавчого оформлення існуючих правовідносин у сфері технології блокчейн. Так, 6 жовтня 2017 року у Верховній Раді було зареєстровано проєкт Закону «Про обіг криптовалют в Україні», який має на меті впорядкувати правовідносини щодо обігу, зберігання, володіння, використання та проведення операцій з криптовалютами в Україні. Втім, цей проєкт має загальний вигляд, містить лише термінологічні визначення та обмежено визначає статус і порядок здійснення операцій з криптовалютами, а не технологію блокчейн. В інших вітчизняних законодавчих актах щодо правового статусу криптовалют питання блокчейну взагалі не визначено.

Блокчейн все ще може бути незрілою технологією з масштабованістю і регулятивними проблемами, але він має великий потенціал для розвитку в Україні, особливо у сфері фінансів, логістики, охорони здоров'я та енергетики.

Уряд України вже взяв на озброєння деякі ініціативи щодо розвитку технології блокчейн в країні. Наприклад, у 2018 році було створено спеціальний робочий групу з блокчейн технологій, яка займається розробкою рекомендацій щодо розвитку блокчейну в Україні та сприяє створенню нових проектів у цій сфері.

Також, в Україні було створено перший блокчейн-акселератор – програму, яка надає фінансову та інфраструктурну підтримку для розвитку блокчейн-стартапів. На додаток до цього, в Україні активно досліджується використання технології блокчейн у галузі енергетики, охорони здоров'я та громадських послуг.

Висновки. Під час дослідження було виявлено що нинішні державні установи наразі є застряглими в застарілих системах і нездатними досягти нових результатів, які від них очікують сьогоднішні споживачі. Проаналізувавши приклади впровадження технології блокчейн, можна дійти до висновку, що на сьогоднішній день технологія блокчейн потребує певної роботи, щоб ефективно інтегруватися в урядовий сектор України. Масштабованість та споживання енергії – лише деякі приклади проблем, які потрібно подолати, щоб побачити ефективні результати від блокчейну.

Блокчейн надає високоефективні засоби захисту конфіденційності та доступності інформації, а також дозволяє створювати повністю децентралізовані системи. Інтеграція блокчейн-рішень в систему електронного уряду дозволяє трансформувати, оптимізувати і навіть автоматизувати адміністративні послуги в державному і муніципальному секторах в таких сферах, як реєстрація прав власності, забезпечення функціонування реєстрацій документів, міграційний контроль, встановлення особистих даних та інші послуги електронного управління.

Проте на поточному етапі правового впорядкування потребують такі питання: юридичний статус технології блокчейн, питання щодо зберігання, володіння, застосування та інших операцій з цією технологією, правовий статус уповноважених суб'єктів, відповідальних за її функціонування, процедура доступу до інформації в системі, відносини між власниками даних та власником системи, умови обробки інформації в системі, а також забезпечення захисту інформації в системі.

Надалі широке використання технології блокчейн у сфері взаємодії з громадськістю дозволить скоротити кількість державних службовців, усунути корупційні фактори, дебюрократизувати сектор адміністративних послуг, створити сприятливі умови для покращення інвестиційного середовища для розробки та підтримки новітніх технологій, а також налагодити ефективну взаємодію між бізнесом, громадянами та владою в Україні.

Розвиток технології блокчейн в Україні має значний потенціал та може відкрити нові можливості для бізнесу та суспільства в цілому. Однак, для досягнення успіху у цій сфері потрібна активна підтримка влади та бізнесу, а також розвиток відповідної інфраструктури та правового поля.

Список використаних джерел

1. Доронін І. М. Блокчейн, суспільство і держава: проблеми правотворчості. ІТ-право: проблеми та перспективи розвитку в Україні: зб. матер. І Міжнар. наук.-практ. конф. (м. Львів, 17 листоп. 2017 р.). Львів: НУ «Львівська політехніка», 2017. С. 73-78.
2. What Is a Block in the Blockchain? – [Електронний ресурс]. – Режим доступу: https://medium.com/datadriveninvestor/what-is-ablock-in-the-blockchain-c7a420270373.
3. D5 Charter. – [Електронний ресурс]. https://www.gov.uk/government/uploads/ system/uploads/attachment_data/file/386290/
4. Желтухін Є. Юристи та технології: точки дотику. Юридична Газета. 2017. 14 листоп. No 46 (596). С. 26-27.
5. Melanie Swan. Blockchain: Blueprint for a New Economy, 2015.
6. Меморандум про взаєморозуміння та співробітництво між Міністерством юстиції України, Міністерством аграрної політики та продовольства України. Державним агентством з питань електронного урядування України, громадською організацією Transparency International Україна та Бітфурі ХолдінгБ. В.
7. Стефанчук Р. Інформаційні технології та право: Право України. 2018. С. 30-50.
8. Тапскотт Д., Тапскотт А. Революція блокчейнів: як технологія, що стоїть за біткойнами та іншими криптовалютами, змінює світ. 2020 рік. С. 78-79
9. Башир І. Освоєння блокчейну: пояснення технології розподіленої книги, децентралізації та розумних контрактів. 2018 рік. С. 91.
10. Колегова Д. Розумний договір як інструмент юридичного забезпечення транзакцій в мережах блокчейн: правові виклики та перспективи розвитку. 2018 рік.
11. Шин Л. Останній посібник із розуміння блокчейн-системи. 2019 рік.

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

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА ПРОГРАМНОЇ ПЛАТФОРМИ BOOKIMED У РОЗВИТКУ МЕДИЧНОГО ТУРИЗМУ

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

Стаття присвячена ролі штучного інтелекту, медичного туризму та програмної платформи Bookimed забезпечує якісну медичну допомогу пацієнтам. Вона розглядає можливості та перспективи використання штучного інтелекту в медичному туризмі, а також роль програмної платформи Bookimed у полегшенні процесу пошуку найкращих медичних закладів та зменшенні витрат на медичний туризм. Стаття також розглядає позитивні дослідження медичного туризму, зокрема, доступ до найсучасніших технологій та процедур, які ще не є доступними в країні проживання. Висвітлення цих тем допоможе читачам зрозуміти свідомість штучного інтелекту, медичного туризму та програмної платформи Bookimed у забезпеченні високої якості медичної допомоги пацієнтам.

This article is devoted to the role of artificial intelligence, medical tourism, and the Bookimed software platform in providing quality medical care to patients. It explores the possibilities and prospects of using artificial intelligence in medical tourism, as well as the role of the Bookimed software platform in facilitating the process of finding the best medical institutions and reducing the cost of medical tourism. The article also highlights the positive consequences of medical tourism.

Актуальність. Медичний туризм є однією з найбільш швидкорозвиваючих галузей в світі туризму, і його розвиток в Україні має великий потенціал.

Україна має потужний потенціал в галузі медичного туризму, завдяки високому рівню медичної освіти та низьким цінам на медичні послуги. Проте, для того, щоб розвиток медичного туризму в Україні став успішним, необхідно мати якісні медичні послуги, а також забезпечувати високий рівень обслуговування для іноземних пацієнтів.

У цьому контексті Bookimed має важливу роль в розвитку медичного туризму в Україні, як компанія, що займається організацією та координацією медичних послуг для іноземних пацієнтів. Їхні послуги допомагають залучати іноземних клієнтів та стимулюють розвиток медичного туризму в Україні.

Також важливо зазначити, що у зв'язку з пандемією COVID-19, медичний туризм по всьому світу зазнав значних змін. Україна не стала винятком і також зазнала складнощів в розвитку медичного туризму. Однак, з поступовим покращенням ситуації, можна очікувати, що медичний туризм в Україні знову набере обертів, тому роль Bookimed у цьому процесі залишається дуже важливою.

Метою статті є показати, як можна застосувати AI технології для поліпшення якості медичних послуг та досліджень. Стаття має на меті описати, як розробники можуть використовувати AI для створення більш ефективних та персоналізованих веб-сайтів на застосунків в галузі медицини, які допомагають лікарям та пацієнтам швидше та точніше знаходити необхідну інформацію, здійснювати діагностику для лікування різних хвороб.

Об'єктом статті є штучний інтелект, що впроваджується у сферу медичних послуг.

Предметом дослідження є впровадження AI-технологій в розробку веб-сайтів як засобу поліпшення якості медичних послуг та зниження їх вартості. Розглянуться можливості використання штучного інтелекту для оптимізації процесів в галузі медицини та для розробки інноваційних медичних продуктів, що можуть допомогти пацієнтам отримувати більш якісну та доступну медичну допомогу. А також компанія Bookimed як провайдер медичних послуг для іноземних пацієнтів в Україні.

Аналіз попередніх досліджень. Наукові статті на тему аналізу ринку медичного туризму в Україні та ролі Bookimed в його розвитку досить рідкісні. Проте, деякі дослідження вже були проведені в цій області.

Наприклад, стаття «Медичний туризм в Україні: стан та перспективи» є досить інформативною і містить багато важливої інформації про медичний туризм в Україні. Автори досліджують стан медичного туризму в країні та виділяють основні переваги, недоліки та перспективи розвитку даної галузі. У статті наведені статистичні дані про розвиток медичного туризму в Україні, зокрема, про кількість іноземних туристів, які зверталися до медичних закладів країни, та про кількість медичних закладів, які пропонують послуги медичного туризму. Також автори зазначають, що недоліками медичного туризму в Україні є недостатня кількість англомовних лікарів та медичних працівників, а також низька якість медичних послуг у деяких медичних закладах. Однак, в статті зазначено, що українські медичні заклади мають висококваліфікованих лікарів та невисокі ціни на медичні послуги, що може привернути увагу іноземних туристів. Також зазначається,, що розвиток медичного туризму в Україні може стати важливим чинником для зміцнення економіки країни та збільшення кількості робочих місць у медичній галузі. Для досягнення цих цілей автори статті пропонують ряд заходів, зокрема, покращення інфраструктури медичного туризму, розвиток партнерських відносин з міжнародними партнерами, залучення іноземних інвесторів та зміцнення правового поля.

Джефрі Гінтон – відомий професор зі штучного інтелекту з університету Торонто і засновник компанії Google Brain, що займається дослідженнями глибокого навчання (deep learning). У статті «Deep learning–a technology with the potential to transform health care» він обговорює можливості глибокого навчання для трансформації галузі охорони здоров'я.У своїй статті Гінтон стверджує, що глибоке навчання може допомогти у вирішенні різноманітних проблем в галузі медицини, таких як діагностика, лікування та передбачення результатів. Він також зазначає, що технології глибокого навчання можуть бути особливо корисними в медицині, де дуже важливо збирати та аналізувати велику кількість даних, щоб зробити точні діагнози та надати ефективне лікування.У статті також згадується про використання глибокого навчання для розробки нових методів діагностики захворювань, включаючи розпізнавання зображень зі скануванням мозку та дослідження геноміки. Крім того, глибоке навчання може бути використано для передбачення результатів лікування та прогнозування ризиків захворювання.

У загальному, стаття Гінтона підтверджує важливість технологій штучного інтелекту та глибокого навчання в галузі медицини та їх потенціал для зміни підходів до діагностики та лікування різних захворювань.

В сучасному світі медичний туризм набуває все більшої популярності. Із зростанням доступності міжнародних перельотів та розвитком медичних технологій, все більше людей вирушають за кордон для отримання якісної та доступної медичної допомоги. Україна відноситься до країн, які мають великий потенціал у розвитку медичного туризму, насамперед це пов'язано з доступністю якісної медичної допомоги та відносно низькими цінами на неї (наприклад, Рис.1. порівняння лікування безпліддя в Україні та Німеччині).

За даними Міністерства розвитку економіки, торгівлі та сільського господарства України, кількість іноземних громадян, які приїхали до України для отримання медичної допомоги, збільшилася у 2021 році на 27,6% порівняно з 2020 роком. Загалом, відсоток зростання медичного туризму в Україні становить більше 10% щорічно. З цих даних можна зробити висновок, що медичний туризм є важливою галуззю для розвитку економіки України та відіграє вагому роль у забезпеченні якісної медичної допомоги для іноземних пацієнтів.

Рис. 1. Медичний туризм міста Львова: соціально-економічні можливості для розвитку

Україна є відомою своїми унікальними природними лікувальними джерелами, курортами та сучасними клініками, що надають високоякісні медичні послуги. Серед основних напрямків медичного туризму в Україні можна виділити:

1. Лікувальні курорти. Україна має багато курортів, де можна отримати лікування за допомогою мінеральних вод, грязей, клімату та інших природних чинників;

2. Естетична медицина. Розвинена галузь естетичної медицини, де пропонуються різноманітні процедури, такі як пластична хірургія, контурна пластика, ботокс, філлери та інші;

3. Стоматологія. Стоматологія є одним з найбільш популярних напрямків медичного туризму в Україні. Багато клінік пропонують послуги з відновлення та лікування зубів, включаючи імплантацію зубів, ортодонтичні процедури, протезування;

4. Репродуктивна медицина. Україна відома своїми передовими клініками з репродуктивної медицини, де проводяться програми штучного запліднення, в тому числі, програми сурогатного материнства;

5. Нейрохірургія. Велика кількість кваліфікованих фахівців у галузі нейрохірургії та нейрології, що надають послуги з лікування різноманітних захворювань головного мозку та нервової системи;

6. Кардіологія. Високооснащені клініки та кардіоцентри, де проводяться діагностика та лікування кардіологічних захворювань;

7. Офтальмологія. Україна має клініки з передовими технологіями та професійними офтальмологами, які надають послуги з діагностики та лікування офтальмологічних захворювань, таких як катаракта, глаукома та інші.

Аналіз ринку медичного туризму в Україні відображає стан справ у галузі та дозволяє зрозуміти потенціал та перспективи розвитку. Bookimed виконує важливу роль у розвитку медичного туризму, забезпечуючи доступ до високоякісних медичних послуг для пацієнтів з різних країн світу. Дана платформа – це один з провідних сервісів медичного туризму в Україні, який активно сприяє розвитку цього напрямку в країні, забезпечує можливість обрати медичний заклад відповідно до потреб пацієнта та забезпечує підтримку та консультування на всіх етапах лікування.

Також важливо зазначити, що у зв’язку з пандемією COVID-19, медичний туризм по всьому світу зазнав значних змін. Україна не стала винятком і також зазнала складнощів в розвитку медичного туризму. Однак, з поступовим покращенням ситуації, можна очікувати, що медичний туризм в Україні знову набере обертів, тому роль Bookimed у цьому процесі залишається дуже важливою

Війна в Україні спричинила складні умови для розвитку медичного туризму. На жаль, у зоні конфлікту та прилеглих територіях, які були раніше популярними для туристів, суттєво постраждали медичні заклади та інфраструктура. Додатково, наявність зони конфлікту створює певний ризик для іноземних пацієнтів, які можуть стати свідками

бойових дій або потрапити у небезпечну ситуацію. Це може відлякувати туристів від візиту до України для медичного лікування.

Крім того, економічні проблеми, які супроводжують війну, можуть суттєво позначитися на якості медичних послуг, забезпеченні медичною технікою та медикаментами. Тим не менш, в Україні діє низка медичних закладів, які надають високоякісні послуги іноземним пацієнтам, зокрема в області репродуктивної медицини та стоматології. Також існують ініціативи залучення іноземних інвесторів для розвитку медичного туризму в інших регіонах України, що не потерпають від війни.

Ключову роль у розвитку медичного туризму в Україні відіграє Bookimed. Заснована в 2014 році, компанія за майже 10 років свого існування здобула величезний досвід у цій сфері та надає високоякісні послуги своїм клієнтам. Однією з найбільших переваг Bookimed є їхній досвід та знання ринку медичного туризму в Україні. Компанія має широку мережу клінік-партнерів, з якими вони співпрацюють протягом багатьох років, тому можуть забезпечити найвищу якість медичних послуг та найбільш вигідні ціни для своїх клієнтів. Крім того, Bookimed відкриває для іноземних пацієнтів доступ до медичних послуг в Україні, які раніше були недоступні.

Основна стратегія компанії – це індивідуальний підхід до кожного клієнта та надання повного спектру послуг від підготовки до подорожі та бронювання до післяопераційної реабілітації та підтримки клієнта впродовж усього перебування в Україні. Компанія має власний медичний перекладач та координатора, які забезпечують підтримку клієнта під час усіх етапів лікування.

Bookimed дбає про те, щоб клієнти отримували найкращі медичні послуги від провідних клінік України та забезпечує повний спектр медичних послуг у таких галузях, як кардіологія, онкологія, репродуктивна медицина, стоматологія та інші. Однією з найбільших переваг Bookimed є їхній досвід та знання ринку медичного туризму в Україні. Компанія має широку мережу клінік-партнерів, з якими вони співпрацюють протягом багатьох років, тому можуть забезпечити найвищу якість медичних послуг та найбільш вигідні ціни для своїх клієнтів. Крім того, Bookimed відкриває для іноземних пацієнтів доступ до медичних послуг в Україні, які раніше були недоступні.

Алгоритми штучного інтелекту використовуються для аналізу медичних даних, таких як записи пацієнтів, геномні дані, медичні зображення та інші джерела даних, щоб забезпечити більш точну діагностику та лікування. Наприклад, AI можна використовувати для виявлення ранніх ознак захворювань шляхом аналізу медичних зображень, таких як рентгенівські знімки або МРТ. Інші приклади застосування AI в охороні здоров’я включають віддалений моніторинг пацієнтів. Системи віддаленого моніторингу з підтримкою AI дозволяють медичним працівникам віддалено збирати біометричні дані пацієнтів в режимі реального часу і швидко виявляти відхилення або ознаки проблем зі здоров’ям, що насуваються.

Процес підбору клініки за допомогою штучного інтелекту: він може відрізнятися в залежності від того, як саме був реалізований цей інструмент. Однак, загалом, процес може включати наступні кроки:

1. Збір інформації про клініки: штучний інтелект може збирати дані про клініки з різних джерел, таких як бази даних;

2. Аналіз та оцінка даних: після збору даних, система може аналізувати їх та виконувати оцінку якості клінік на основі різних параметрів, таких як відгуки пацієнтів, медичні статистики, кваліфікації медичного персоналу та інше;

3. Підбір найкращої клініки: на основі аналізу даних, штучний інтелект може вибрати декілька найкращих клінік для пацієнта;

4. Рекомендації: система може рекомендувати пацієнту найкращу клініку, враховуючи його особисті потреби та вимоги;

5. Підтримка в прийнятті рішення: штучний інтелект може надати пацієнту додаткову інформацію про клініки, щоб допомогти йому прийняти правильне рішення.

Впровадження технологій штучного інтелекту в медичні консультаційні застосунки може допомогти підвищити точність діагнозів, оптимізувати догляд за пацієнтами та підвищити ефективність роботи медичних працівників. Наприклад, поширеною проблемою є точна діагностика захворювань на основі симптомів і історії хвороби пацієнта. Алгоритми машинного навчання можна використовувати для аналізу великих обсягів медичних даних і надання рекомендацій на основі патернів. Збір та аналіз даних з електронних медичних карт, медичних журналів та інших релевантних джерел для навчання моделей штучного інтелекту. Дані повинні бути характерними для групи пацієнтів, для яких призначений застосунок. Інтеграція AI технологій в робочий процес застосунку або сайту, щоб надавати медичним працівникам рекомендації та поради в режимі реального часу, наприклад, чат-бот зі штучним інтелектом може допомогти сортувати пацієнтів і ставити початкові діагнози на основі симптомів.

AI технології можуть бути дуже корисними для пацієнтів, які шукають інформацію про лікування, перевірених лікарів та клініки. Пошукові алгоритми AI допомагають пацієнтам знайти найбільш ефективні методи лікування та найкращі клініки для отримання медичної допомоги. Щоб пошук був ефективним для пацієнтів, розробники можуть використовувати пошукові алгоритми, які ретельно аналізують дані про лікування та клініки з різних джерел, таких як медичні журнали, бази даних медичних досліджень, відгуки пацієнтів та інші джерела. Алгоритми можуть враховувати різні параметри, наприклад, типи лікування, рівень ефективності лікування, вартість, рейтинг клініки та інші фактори.

AI може бути використаний для розробки віртуальних асистентів, які допоможуть пацієнтам отримувати швидку та точну інформацію про лікування та клініки, а також можуть допомогти пацієнтам зрозуміти їх медичну історію та плани лікування.

Звичайно, точність та ефективність штучного інтелекту залежить від якості даних, які він отримує, та від того, наскільки добре він настроєний для роботи в конкретній галузі. Тому важливо ретельно перевіряти роботу системи та контролювати якість даних, щоб забезпечити максимально точні результати.

Технології AI корисні при розробці сайтів з медичного туризму бо AI може пропонувати пацієнтам медичні тури, які найкраще відповідають їхнім потребам та бюджету. Алгоритми машинного навчання можуть враховувати такі фактори, як місцезнаходження, терміни лікування, типи процедур та багато іншого. Також штучний інтелект може допомогти пацієнтам отримати консультації від лікарів дистанційно. Це корисно для тих, хто шукає допомогу від лікарів з інших країн або для тих, хто не може фізично відвідати клініку.

AI може допомогти відстежувати тенденції в галузі медичного туризму та спрогнозувати попит на різні види процедур та напрямки лікування. Це може бути корисно для розробки бізнес-стратегій та маркетингових кампаній.

На даний момент розвиток медичного туризму в Україні є перспективним напрямком. За даними Міністерства охорони здоров’я України, кількість іноземних пацієнтів, які отримують медичні послуги в Україні, зростає з кожним роком.

Уряд України активно підтримує розвиток медичного туризму, зокрема, шляхом вдосконалення законодавства, створення сприятливих умов для інвестування у медичний сектор, підвищення рівня медичної освіти та підготовки кваліфікованого медичного персоналу.

Також прогнозується збільшення кількості медичних закладів та збільшення їх обсягу фінансування, що дозволить підвищити якість медичних послуг.

Зростання популярності медичного туризму в Україні також може бути викликане збільшенням кількості спеціалізованих клінік, які спеціалізуються на наданні конкретних видів медичних послуг, та зростанням популярності альтернативної медицини.

У світлі цих факторів, прогнозується подальший розвиток медичного туризму в Україні та збільшення кількості іноземних пацієнтів, які обирають Україну як медичний туристичний напрямок.

Bookimed також відіграє важливу роль у зростанні довіри до вітчизняних лікарів серед українського населення, оскільки компанія співпрацює тільки з найкращими клініками України, які мають високу репутацію, і надають якісні послуги. Компанія пропонує своїм клієнтам консультації з висококваліфікованими медичними експертами, які можуть допомогти зрозуміти суть проблеми та призначити найкращі методи лікування. Також, завдяки своєму досвіду та знанням про медичні послуги в Україні, Bookimed допомагає іноземним пацієнтам знайти найкращі клініки та лікарів в країні. Це сприяє зростанню популярності українських медичних закладів серед іноземних пацієнтів та зміцненню довіри до вітчизняних лікарів.

Отже, Bookimed робить чималий внесок, та прикладає всі зусилля в підвищення якості та рівня медичних послуг в Україні, що в свою чергу сприяє зростанню довіри до вітчизняних лікарів та підвищенню престижу української медицини в світі.

Висновок. У статті було проведено аналіз ринку медичного туризму в Україні, зокрема зосереджено увагу на потенційних перевагах та недоліках цього ринку. На основі проведеного аналізу можна зробити висновок, що розвиток медичного туризму в Україні є перспективним напрямком і має великий потенціал для подальшого росту.

Одним із провідних гравців на ринку медичного туризму в Україні є компанія Bookimed.

Розглянуто історію створення та розвитку компанії, її стратегію та підхід до клієнтів. Виявлено, що Bookimed має декілька переваг, які дозволяють їй успішно конкурувати на ринку медичного туризму в Україні. Серед них можна виділити широку мережу партнерських клінік, високу якість обслуговування та професійність працівників.

Також було досліджено вплив Bookimed на зростання довіри до вітчизняних лікарів. Виявлено, що компанія вносить значний вклад у підвищення рівня довіри до українських медичних закладів та пропагує високі стандарти медичної практики.

Прогнозуючи розвиток медичного туризму в Україні в майбутньому, можна стверджувати, що ринок буде надалі зростати та розвиватися, що створює нові можливості для покращення якості медичної допомоги та забезпечення доступності для пацієнтів з усього світу.

Можна стверджувати, що Bookimed зіграв важливу роль в розвитку медичного туризму в Україні, зокрема в підвищенні рівня довіри

Список використаних джерел

1. Бордун О.Ю., Наука й економіка. 2016. №1(41). С.78-85. Медичний туризм міста Львова: соціально-економічні можливості для розвитку \\ https://tourlib.net/statti_ukr/bordun7.htm
2. Інформаційне управління. Опубліковано 25 березня 2016. Медичний туризм в Україні: проблеми та перспективи \\ https://www.rada.gov.ua/news/Novyny/127061.html
3. Prof. Dr. Keun Ho Ryu, Prof. Dr. Nipon Theera-Umpon, Artificial Intelligence in Healthcare \\ https://www.mdpi.com/topics/artificial_intelligence_healthcare

Робота виконана під науковим керівництвом канд. техн. наук, доцента
РЗАЄВОЇ С. Л.

ЗАХИСТ ДАНИХ У ТЕХНОЛОГІЯХ БЕЗПРОВІДНОГО ЗВ'ЯЗКУ СТАНДАРТУ IEEE 802.16

ШУЛЯЄВ Д., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто основні засади побудови системи захисту даних у технологіях безпровідного зв'язку стандарту IEEE 802.16. На теперішній час перед багатьма підприємствами постає питання швидкої та якісної організації захисту каналів зв'язку. Таким чином підвищити ефективність бізнесу – використання сучасної технології бездротової передачі даних WiMAX, яка дозволяє швидко та якісно вирішити задачі забезпечення зв'язку там, де це надзвичайно складно, або навіть неможливо зробити, використовуючи традиційні мережі.

The article discusses the basic principles of building a system for protecting a private network of a trade enterprise of the IEEE 802.16 standard. At present, many enterprises face the question of quick and high-quality organization of communication channels. In this way, to increase business efficiency – the use of modern WiMAX wireless data transmission technology, which allows you to quickly and efficiently solve the problems of providing communication where it is extremely difficult, or even impossible, to do using traditional networks.

Актуальність. Інформаційні магістралі сьогодні не поступаються по важливості транспортним, вони всюди – і на суші, і на дні океану, і в космосі. На сьогоднішній момент визначено три основних вимоги до мережевих з'єднань: висока пропускна здатність, надійність, мобільність. З'єднати всі три основних критерії може тільки покоління безпровідних технологій стандарт IEEE 802.16 − WiMAX (Worldwide Interoperability for Microwave Access).

WiMAX – це система далекої дії, що покриває кілометри простору, яка зазвичай використовує ліцензовані спектри частот (хоча можливо і використання не ліцензованих частот) для надання з'єднання із інтернетом типу точка-точка провайдером кінцевому користувачеві. Різні стандарти сімейства 802.16 забезпечують різні види доступу, від мобільного (схожий з передачею даних із мобільних телефонів) до фіксованого (альтернатива провідникового доступу, при якому бездротове обладнання користувача прив'язане до розташування). У загальному вигляді WiMAX мережі складаються з наступних основних частин – базових і абонентських станцій, а також обладнання, що зв'язує базові станції між собою, з постачальником Інтернету. Для з'єднання базової станції з абонентською використовується високочастотний діапазон радіохвиль від 1,5 до 11 ГГц. В ідеальних умовах швидкість обміну даними може досягати 70 Мбіт/с, при цьому не вимагається забезпечення прямої видимості між базовою станцією і приймачем. WiMAX застосовується як для вирішення проблеми надання доступу в Інтернет офісним та районним мережам.

При цьому, принаймні одна базова станція підключається до мережі провайдера з використанням класичних дротових з'єднань. Однак, чим більше число базових станцій (БС) підключено до мереж провайдера, тим вища швидкість передачі даних і надійність мережі в цілому. Структура мереж сімейства стандартів IEEE 802.16 схожа із традиційними GSM мережами (базові станції діють на відстанях до десятків кілометрів, для їх встановлення не обов'язково будувати вежі – допускається установка на дахах будинків при дотриманні умови прямої видимості між станціями).

Метою статті є дослідження захисту даних у технологіях безпровідного зв'язку стандарту IEEE 802.16.

Об'єктом дослідження є розробка захищеної мережі безпровідного зв'язку стандарту IEEE 802.16.

Предмет дослідження – захищена мережа безпровідного зв'язку стандарту WiMAX.

Аналіз попередніх досліджень. Дослідженню системи захисту безпровідної мережі стандарту IEEE 802.16 присвячені праці вітчизняних та закордонних науковців: А. С. Шевченка, А. В. Чунарьової, Г. В. Микитина, А. І. Ребеця, Р. І. Банаха та ін.

Виклад основного матеріалу. Безпровідні мережі забезпечують мобільність клієнта, його здатність підключатися до мережі з будь-якого місця і в будь-який час, а також можливість переміщення без втрати з'єднання Хоча безпровідна мережа використовує радіочастоти замість кабелів, вона зазвичай реалізована в комутованій мережі, а формат кадру аналогічний тому, що використовується в Ethernet. Сьогодні корпоративні мережі розвиваються швидкими темпами, забезпечуючи підтримку користувачів, які постійно перебувають в роз'їздах. Користувачі можуть підключатися, використовуючи різні пристрої, включаючи комп'ютери, ноутбуки, планшетні комп'ютери і смартфони. В рамках даної концепції мобільності користувачі можуть підключатися до мережі, перебуваючи в русі.

Безпровідний зв'язок тягне за собою безліч переваг як для корпоративних, так і для домашніх мереж. До таких переваг належать підвищені гнучкість і продуктивність, зниження витрат, можливість розвитку та адаптації до мінливих вимог Використання безпровідних мереж також дозволяє знизити витрати. У компаніях, де вже використовується безпровідна інфраструктура, економія витрат реалізується при кожній зміні або переміщенні обладнання − наприклад, при переміщенні співробітника в межах будівлі або реорганізації обладнання або лабораторії, переміщенні в тимчасові офіси або об'єкти в рамках того чи іншого проекту. Ще однією важливою перевагою бездротових мереж є здатність адаптуватися до зміни потреб і технологій. Додавання нового обладнання в бездротову мережу не викликає особливих труднощів. Користувачі за допомогою бездротового підключення в домашніх умовах можуть відвідувати веб-сайти, сидячи за кухонним столом, перебуваючи у вітальні або навіть поза приміщенням. Користувачі домашньої мережі підключають нові пристрої (наприклад смартфони, планшетні комп'ютери, ноутбуки і телевізори з інтелектуальними функціями) [1,2].

WiMAX (протокол широкосмугового радіозв'язку) − стандарт мереж IEEE 802.16, який забезпечує безпровідний широкосмуговий доступ на відстанях до 50 км (30 миль). WiMAX є альтернативою кабельному і широкосмугового DSL-підключення. У 2005 році в стандарт WiMax були додані мобільні функції, завдяки чому цей стандарт можуть використовувати оператори зв'язку для надання стільникового широкосмугового доступу.

WiMAX підходить для вирішення наступних заадач:

- З'єднання точок доступу Wi-Fi один з одним та з іншими сегментами Інтернету.
- Забезпечення безпровідного широкосмугового доступу як альтернативи виділеним лініям і DSL.
- Надання високошвидкісних сервісів передачі даних і телекомунікаційних послуг.
- Створення точок доступу, не прив'язаних до географічного положення.
- Створення систем віддаленого моніторингу системи.

WiMAX дозволяє здійснювати доступ в Інтернет на високих швидкостях, з набагато кращим покриттям, ніж у Wi-Fi-мереж. Це дозволяє використовувати технологію в якості «магістральних каналів», продовженням яких виступають традиційні DSL і виділені лінії, а також локальні мережі. В результаті подібний підхід дозволяє створювати масштабовані високошвидкісні мережі в рамках міст.

Безпровідні комп'ютерні мережі − це сучасна альтернатива традиційної провідної мережі, яка спирається на кабелі для підключення пристроїв до мережі разом. Безпровідні технології широко використовуються в домашніх і корпоративних комп'ютерних мережах. Безпровідні мережі мають безліч застосувань. В офісах на робочому місці, це полегшує спільне використання файлів, принтерів і доступ в інтернет між усіма комп'ютерами. Вдома

чи в домашньому офісі мережі дозволяє користувачам виконувати друк з ноутбука без необхідності йти до принтера і підключатися до нього.

Стандарт IEEE 802.16 описує роботу в діапазоні 10–66 ГГЦ систем з архітектурою «точка – багато точка». Це – двонаправлена система, тобто передбачені прямі і зворотні потоки. При цьому канали широкосмугові, а швидкості передачі – високі. Тракт обробки даних і формування вихідного сигналу для передачі через радіоканал у стандарті IEEE 802.16 досить звичайний для сучасних телекомунікаційних протоколів і практично однаковий для зворотних і прямих з'єднань. Вхідний потік даних скремблюється – піддається рандомізації, тобто на нього накладається псевдовипадкова послідовність, вироблювана за допомогою лінійного регістра зрушення довжини з характеристичним багаточленом і початковим заповненням. Далі скрембльовані дані кодують за допомогою завадостійких кодів. При цьому використається одна із чотирьох схем: код Рида-Соломона, код Рида-Соломона з додатковим надточним кодом (швидкість), код Рида-Соломона з додатковим контролем парності і блоковий турбокод. Розмір кодованого інформаційного блоку й число надлишкових біт не фіксовані – ці параметри можна задавати залежно від умов середовища й вимог до якості надання послуг. Перші дві схеми кодування обов'язкові для всіх пристроїв стандарту, інші два алгоритми – додаткові [1].

Побудова мережі WiMAX припускає використання трьох типів устаткування – базові станції (БС), абонентський комплект (абонентська станція – АС) і устаткування для організації зв'язку між базовими станціями – ретрансляційні станції (РС).

Кожний з модулів (або радіоінтерфейсів у двомодульних моделях) забезпечує обслуговування одного просторового сектора в межах діаграми спрямованості використовуваної антени. Типові значення зони охоплення кожного сектора 360° (один сектор), 120° (три сектори), і 60° (шість секторів). Устаткування БС не накладає певних вимог до ширини сектора, що у конкретних випадках може бути довільною, обумовленою конкретною топологією мережі, наявністю частотного ресурсу й розміщенням абонентів [1].

До складу БС входять [2]:

- Бездротові маршрутизатори R5000 – від 1 до 6, по одному на сектор. Для малопотужних БС можуть використатися двохмодульні бездротові маршрутизатори – по одному на два сектори. Односекторні БС забезпечують швидкість передачі до 54 Мбіт/с. Багатосекторні БС які забезпечують роботу зі швидкістю до 48 Мбіт/з на сектор; антенно-фідерні пристрої – по кількості секторів базової станції; ліцензії для підключення спеціалізованих абонентських станцій, на кожен сектор базової станції; програмне забезпечення для керування мережею; комутатор Ethernet; шафа для монтажу встаткування; джерела безперебійного живлення. БС розміщаються на високих будівлях або антенних опорах, на яких установлюють й інші радіосистеми, що приводить до підвищення загального рівня перешкод.
- Ретрансляційна станція (РС) призначена для підвищення дальності дії БС, обходу великих перешкод, а також для створення протяжних магістральних каналів точка-точка. Кількість підключень послідовно РС не обмежена. До кожної РС може бути підключена одна або трохи РС й/або АС До складу РС входять: двохмодульний безпровідний маршрутизатор R5000; спрямована антена для зв'язку із БС (у випадку РС без інтегрованої антени); всеспрямована, секторна або спрямована антена для підключення АС й/або РС; кабелі для підключення антен; ліцензія для підключення спеціалізованих АС до РС.
- Абонентська станція (АС) призначена для безпровідного підключення абонентів до БС або РС, а також для створення магістральних каналів «точка-точка».

Склад АС: абонентський бездротовий маршрутизатор з інтегрованою антеною або рознімання для підключення зовнішньої антени; спрямована антена й антенний кабель для моделей без інтегрованої антени.

Система керування мережею (Network Monitoring / Management System – NMS) призначена для моніторингу мережі в реальному часі з метою оперативного керування. Специфікації стандарту WiMAX визначають передачу трафіку і сигнальний обмін тільки на

радіоінтерфейсу. Що стосується з'єднання БС з Інтернетом, мережами безпровідного доступу та мережами різних операторів, рішення по архітектурі мережі приймає оператор спільно з виробником. З метою уніфікації та певної оптимізації WiMAX Forum запропонована базова архітектура мережі. NRM (Network Reference Model – базова модель мережі) WiMAX, яка є логічним поданням мережевої архітектури. NRM розділяє систему на три логічні частини:

1. Мобільні станції, використовувані абонентами для отримання доступу до мережі;

2. ASN (Access Services network) − мережа доступу до послуг, що є власністю оператора доступу до мережі (NAP − Network Access Provider); ASN складається з однієї або декількох базових станцій, якими управляє один або кілька шлюзів ASN (ASN-GW).

3. CSN (Connectivity Services Nerwork) − підмережа оператора, що забезпечує вихід на IP і інші мережі для реалізації абонентських послуг. Ця підмережа забезпечує необхідні комутаційні функції та функції безпеки. Абонента може обслуговувати оператор домашньої мережі NSP (Network Services Provider). Абонент може також перебувати в роумінгу. У цьому випадку його обслуговує оператор візитною мережі; при цьому відбувається обмін сигнальної інформацією CSN візитною і домашнього оператора.

ASN виконує наступні функції: з'єднання на рівні L2 з АС; пошук і вибір мережі на основі переваг абонента про CSN / NSP; забезпечення безпеки: передача даних про пристрої, користувачів, і послугах, серверу безпеки, тимчасове зберігання профілів користувачів; організація наскрізних IP-з'єднань між АС і CSN; управління радіоресурсу (RRM) відповідно до класу трафіку і потрібним QoS; забезпечення мобільності, тобто виконання процедур хендовера, локалізації та пейджінга. Функціонально БС забезпечує як один сектор з виділеним частотним діапазоном, підтримуючи інтерфейс IEEE 802.16e з АС.

Шлюз ASN є основним елементом мережі. Під час сеансів зв'язку шлюз організовує хендовер абонентам і пейджинг АС, управляє доступом до мережі. Для кожного приєднаного абонента в шлюзі відкрита база даних, що містить профілі абонента і ключі шифрування. На шлюз покладені завдання авторизації потоку послуг згідно з профілем абонентів і QoS. У напрямку БС шлюз підтримує тунельне з'єднання; в напрямку ядра мережі (CSN) шлюз організовує з'єднання по стандартному IP протоколу.

Питання безпеки в мережах WiMAX (стандарт IEEE 802.16), як і в мережах WiFi (стандарт IEEE 802.11), загострено легкістю підключення до мережі. Безпека WIMAX-мережі забезпечується на фізичному рівні спеціально розробленими засобами, які вбудовані в пристрої бездротового зв'язку й керують процесом передачі даних радіоканалом, запобігаючи: спробам порушення конфіденційності; порушенню цілісності даних; порушенню автентичності джерела – споживача; відмови в обслуговуванні [1].

Якість зв'язку у WiMAX вища, чим в WiFi. При підключенні декількох користувачів до точки доступу Wi-Fi виникає проблема черговості доступу до канала зв'язку. Технологія WiMAX забезпечує кожному користувачеві постійний доступ, використовуючи алгоритм установлення обмеження на число користувачів для однієї точки доступу. При наближенні базової станції WiMAX до максимуму свого потенціалу, вона автоматично розподіляє «надлишкових» користувачів на іншу базову станцію. У безпровідній передачі даних немає універсальної технології. Під кожні конкретні завдання більше підходить WiMAX або Wi-Fi. Якщо поставлено завдання надати широкосмуговий доступ до мережі для користувачів, доцільніше використовувати WiMAX, тому що ця технологія була розроблена саме із цією метою. Однак, якщо завдання − надати широкосмуговий доступ в обмеженому приміщенні, то технології Wi-Fi і WiMAX однаково добре підходять для вирішення, за умови низького рівня перешкод або їх відсутності. Для впровадження безпровідних систем безпеки або відеоспостереження доцільніше скористатися технологією Wi-Fi. Головна відмінність між провідними і безпровідними мережами пов'язано з абсолютно неконтрольованою областю між кінцевими точками мережі. У досить широкому просторі мереж безпровідне середовище ніяк не контролюється. Сучасні безпровідні технології пропонують обмежений набір засобів управління всією областю розгортання мережі. Це дозволяє атакуючим, що знаходяться в

безпосередній близькості від безпровідних структур, створювати цілий ряд нападів, які неможливі в дротовому світі [1]. Підслуховування найбільш поширена проблема відкритих і некерованих середовищ, тобто бездротових мереж − можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати дані, як показано на Рис.1.

Рис. 1. Атака «підслуховування»

Обладнання, що використовується для підслуховування в мережі, може бути не складніша від того, що використовується для звичайного доступу до цієї мережі. Щоб перехопити передачу, зловмисник повинен знаходитися поблизу від передавача. Перехоплення такого типу практично неможливо зареєструвати, і ще важче їм перешкодити. Використання антен і підсилювачів дає зловмисникові можливість перебувати на значній відстані від мети в процесі перехоплення. Підслуховування ведуть для збору інформації в мережі, яку згодом передбачається атакувати. Первинна мета зловмисника − зрозуміти, хто використовує мережу, яка інформація в ній доступна, які можливості мережевого устаткування, яка територія розгортання мережі. Все це знадобиться для того, щоб організувати атаку на мережу. Багато загальнодоступних мережних протоколів передають таку важливу інформацію, як ім'я користувача та пароль, відкритим текстом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Навіть якщо передана інформація зашифрована, в руках зловмисника з'являється текст, який можна запам'ятати і розкодувати. [2, 3].

Інший спосіб підслуховування − підключитися до безпровідної мережі. Активне підслуховування в локальній бездротовій мережі зазвичай грунтується на неправильному використанні протоколу Address Resolution Protocol (ARP). Спочатку ця технологія була створена для «прослуховування» мережі. Насправді ми маємо справу з атакою типу MITM («man in the middle» – «людина посередині») на рівні зв'язку даних. Вони можуть приймати різні форми і використовуються для руйнування конфіденційності та цілісності сеансу зв'язку. Атаки MITM більш складні, ніж більшість інших атак: для їх проведення потрібно детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Коли жертва атаки ініціює з'єднання, шахрай перехоплює його і потім завершує з'єднання з необхідним ресурсом, а потім пропускає всі з'єднання з цим ресурсом через свою станцію. При цьому, атакуючий може надсилати інформацію, змінювати її або підслуховувати всі переговори і потім розшифровувати їх [4]. Таким чином, безпровідна станція може перехоплювати трафік іншого безпровідного клієнта (або провідного клієнта в локальній мережі).

Відмова в обслуговуванні (Denial of Service – DOS). Повне паралізування мережі може викликати атака типу DOS. У всій мережі, включаючи базові станції і клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися один з одним. Ця атака вимикає всі комунікації в певному районі. Атаку DOS на без мережі важко запобігти або зупинити. Більшість бездротових мережевих технологій використовує неліцензовані частоти − отже, допустима інтерференція від цілого ряду електронних пристроїв.

Глушіння в мережах відбувається тоді, коли навмисна або ненавмисна інтерференція перевищує можливості відправника або одержувача в каналі зв'язку, таким чином, виводячи цей канал з ладу. Атакуючий може використовувати різні способи глушіння [4]. Глушіння клієнтської станції дає можливість шахраєві підставити себе на місце заглушеного клієнта, як показано на Рис. 2. Також глушіння можуть використовувати для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Більш витончені атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника.

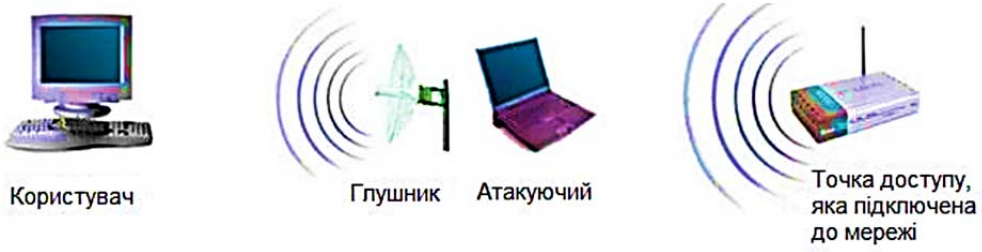

Рис. 2. Атака глушіння клієнта для перехоплення з'єднання

Глушіння базової станції надає можливість підмінити її атакуючої станцією. Таке глушіння позбавляє користувачів доступу до послуг. Більшість безпровідних мережевих технологій використовує неліцензовані частоти. Тому багато пристроїв, такі як радіотелефони, системи спостереження і мікрохвильові печі, можуть впливати на роботу бездротових мереж і глушити бездротове з'єднання.

Всі безпровідні комунікаційні мережі схильні до атак прослуховування в період контакту. А управління ключем, як правило, викликає додаткові проблеми, коли застосовується при роумінгу і в разі загального користування відкритим середовищем.

Безпровідний доступ забезпечує повну анонімність атаки. Без відповідного обладнання в мережі, що дозволяє визначати місце розташування, атакуючий може легко зберігати анонімність і ховатися де завгодно на території дії бездротової мережі [2, 3].

Системи виявлення вторгнень (Intrusion Detection System, IDS) − це пристрої за допомогою яких можна виявляти та своєчасно запобігати вторгненням в обчислювальні мережі. Вони діляться на два види: на базі мережі та на базі хоста. Мережеві системи (Network Intrusion Detection Systems, NIDS) аналізують трафік з метою виявлення відомих атак на підставі наявних у них наборів правил (експертні системи). Виняток з точки зору принципів аналізу становлять системи на базі нейронних мереж та штучного інтелекту. Підмножиною мережевих систем виявлення вторгнень є системи для спостереження тільки за одним вузлом мережі (Network Node IDS) [3].

NIDS діляться в свою чергу на дві великі категорії: на основі сигнатур і на основі бази знань. Сигнатурні IDS найбільш поширені і простіше реалізуються, але їх легко обійти і вони не здатні розпізнавати нові атаки. У таких системах події, відбуваються в мережі, порівнюються з ознаками відомих атак, які й називаються сигнатурами. Крім того, бази даних, що містять сигнатури, необхідно надійно захищати і часто оновлювати. IDS на основі бази знань стежать за мережею, збирають статистику про її поведінку в нормальних умовах, виявляють різні відхилення і позначають їх як підозрілі. Тому такі IDS ще називають заснованими на поведінці чи статистичними [4]. Гарна IDS для безпровідної мережі повинна бути одночасно сигнатурною і статистичною. Деякі інструменти для проведення атак на безпровідні мережі мають чітко виражені сигнатури. Якщо вони виявляються в базі даних, то можна піднімати тривогу. З іншого боку, у багатьох атак очевидних сигнатур немає, але на нижніх рівнях стека протоколів вони викликають відхилення від нормальної роботи мережі. При розгортанні системи необхідно чітко розуміти, що, як і навіщо ми хочемо аналізувати, і намагатися відповісти на ці питання щоб сконструювати необхідну систему IDS [1, 3, 4].

Існує безліч технологій безпеки, і всі вони пропонують рішення для найважливіших компонентів політики у сфері захисту даних: аутентифікації, підтримки цілісності даних і активної перевірки. Ми визначаємо аутентифікацію, як аутентифікацію користувача або кінцевого пристрою і його місця розташування з подальшою авторизацією користувачів та кінцевих пристроїв [2, 3].

Цілісність даних включає такі області, як безпека мережевої інфраструктури, безпеку периметра і конфіденційність даних. Активна перевірка допомагає впевнитися в тому, що встановлена політика в галузі безпеки витримується на практиці, і відстежити всі аномальні випадки і спроби несанкціонованого доступу.

Взагалі в захищеній інформаційній системі, політика безпеки – це документ в якому визначені: мета захисту, ризики системи, основні напрямки захисту інформаційних ресурсів, методи та засоби захисту інформації, властивості захищеності в термінах, що представляють систему захисту інформації з урахуванням встановленої відповідальності за зловмисне порушення визначених вимог. Опис політики безпеки може включати або враховувати властивості порушника, моделі загроз інформаційній системі та ризики пов'язані з їх реалізацією.

Найбільш часто, розглядаються політики безпеки, що пов'язані з поняттям «доступ». Доступ категорія суб'єктно-об'єктної моделі, що описує процес виконання операцій суб'єктів на об'єктами. Політика безпеки, повинна включати: безліч можливих операцій над об'єктами; для кожної пари «суб'єкт, об'єкт», безліч дозволених операцій, що є підмножиною всієї безлічі можливих операцій.

Політика безпеки в загальному випадку являє собою нестаціонарний стан захищеності, система, що захищає властивості інформаційних ресурсів, може змінюватися, доповнюватися новими компонентами, тобто бути динамічною. Політика безпеки – сукупність керівних принципів, правил процедур і практичних прийомів в області безпеки інформації, які регулюють управління, захист і розподіл цінної інформації. Вона встановлює модель захисту для існуючої або розроблюваної мережі. Політика безпеки пропонує набір правил і стандартів для користувачів, адміністраторів та менеджерів безпровідної мережі. Для забезпечення функцій захисту мережі політика безпеки передбачає наявність посади начальника служби безпеки. Для створення політики безпеки необхідне проведення оцінки ризиків у безпровідній мережі. Оцінка ризиків передбачає визначення загроз і вразливостей в системі, а також вона обов'язкова при боротьбі з вразливостями та непередбаченими загрозами, витратами і затратами.

Засіб для забезпечення конфіденційності в безпровідних мережах має бути визначено в політиці безпеки. Шифрування має забезпечити безпечний канал зв'язку, в якому будуть циркулювати закриті дані [2, 3].

Політика безпеки передбачає введення логічних файлів та облік діяльності користувачів. Ведення логічних файлів передбачається для забезпечення: контролю за користувачами; спрощення процесу налаштування мережі в разі виникнення несправностей; спрощення винесення відповідальності за порушення правил експлуатації мережі. Політика безпеки повинна передбачати використання брандмауерів для зменшення ризику злому бездротового клієнта. За допомогою брандмауерів слід проводити реєстрацію безпровідної діяльності. Політика безпеки повинна вимагати використання антивірусного програмного забезпечення та обов'язкового відновлення антивірусних баз [3, 4].

Крім того політикою безпеки передбачається: статична ARP адресація, що підсилює захист, збільшує адміністрування; перевірка MAC адреси; статистична IP адресація; визначення схеми безпровідного мережевого ідентифікатора (SSID).

Політика безпеки може заборонити широкомовну трансляцію SSID, з метою ускладнення ідентифікації точок доступу. Рекомендується включити в політику безпеки безпровідних мереж систему виявлення вторгнень (Intrusion Detection System – IDS). Безпровідна IDS необхідна для забезпечення захисту шляхом виявлення незаконної безпровідної діяльності (нападу). Для забезпечення безпеки безпровідної мережі політика безпеки

повинна включати комплекс заходів як апаратних, так і програмних. Захисту конфіденційної інформації в безпровідних мережах варто надавати особливу увагу. Сьогодні безпровідні мережі отримали величезне розповсюдження. Вони використовуються, як у офісах, так і в домашніх умовах. Ці мережі зручні в користуванні і дозволяють незалежно від місця знаходження бути он-лайн: обмінюватися даними, відправляти і приймати пошту, знаходити потрібну інформацію в Інтернеті [3, 4].

Головними напрямками захисту будь-яких мереж, у тому числі і безпровідних є суттєві з позиції безпеки властивості інформації: конфіденційність, цілісність та доступність, які в свою чергу і уособлюють значення безпеки, графічне зображення даного факту представлене на Рис. 3.

Рис. 3. Головні напрямки безпеки безпровідної мережі приватної мережі підприємства торгівлі

Безпека мережі представляється наступними вимогами: конфіденційність особистих та інших важливих даних; цілісність і точність інформації, що зберігається і програм, які її обробляють; доступність систем, даних і служб для тих, хто має право доступу. Найбільш дієвим захистом від DoS-атак є розробка і дотримання таких правил безпеки: встановлення та оновлення брандмауерів; постійне оновлення антивірусних програмних засобів; встановлення останніх «латок» (оновлень); використання довгих паролів; від'єднання мережевих пристроїв, які не використовуються.

Висновки. Захист даних у технологіях безпровідного зв'язку стандарту IEEE 802.16 дає змогу розв'язувати проблемні задачі функціональної та інформаційної безпеки даних у комунікаціях і цифрових системах на рівні забезпеченої структури «системи – радіосигнали – радіоканали – тракти» згідно з концепцією «об'єкт – загроза – захист». У сегменті програмного забезпечення системної моделі необхідно створювати алгоритмічно-програмне забезпечення процедури шифрування даних у WiMAX-мережі на основі стандарту AES мовою програмування C#, що забезпечує конфіденційність, достовірність, цілісність даних у контексті функціональної та інформаційної безпеки технологій безпровідного зв'язку.

Список використаних джерел

1. Сайко В.Г. Мережі бездротового широкосмугового доступу. Навчальний посібник / В.Г.Сайко, В.Я. Казіміренко, Ю.М. Літвінов. – К.: ДУТ, 2015. – 196 с.
2. Довгий С.О. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання. Монографія / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв. – 2-ге вид. – К.: «Азимут Україна», 2013. – 608 с.
3. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с. (останнє звернення 10.03.2023р.).
4. Захист інформації в операційних системах, базах даних і мережах. [Електронний ресурс]. – Режим доступу: www/ URL: https://ppt-online.org/482411(останнє звернення 10.03.2023р.).

Робота виконана під науковим керівництвом канд. політ. наук, доцента
ЧУБАЄВСЬКОГО В. І.

ОСОБЛИВОСТІ ЗАХИСТУ WEB-РЕСУРСІВ НА ОСНОВІ OAUTH 2.0

ШУНДИК А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто механізм захисту веб-ресурсів на основі OAuth 2.0, який є одним з найбільш поширених механізмів авторизації в сучасних веб-додатках. Розглянуто особливості та застосування механізму OAuth 2.0 для забезпечення безпеки веб-додатків, а також описано загрози, з якими він допомагає боротися. В статті наведені рекомендації для безпечної реалізації механізму OAuth 2.0. Ця стаття може бути корисна для розробників веб-додатків та тестувальників безпеки, які мають намір забезпечити надійний захист своїх веб-ресурсів.

The article discusses the mechanism for protecting web resources based on OAuth 2.0, which is one of the most common authorization mechanisms in modern web applications. The features and applications of the OAuth 2.0 mechanism for securing web applications are reviewed, and the threats it helps to combat are described. The article provides recommendations for the secure implementation of the OAuth 2.0 mechanism. This article can be useful for web application developers and security testers who want to ensure that their web resources are securely protected.

Актуальність написання даної статті полягає у тому, що з розвитком технологій та зростанням кількості користувачів інтернету все більше ресурсів вимагають аутентифікації та авторизації для доступу до персональних даних користувачів. Протокол OAuth 2.0 є одним з найбільш популярних засобів для забезпечення безпеки в таких випадках, оскільки дозволяє надавати обмежений доступ до даних користувачів іншим ресурсам, не надавши їм повного контролю над цими даними.

Однак, незважаючи на популярність і ефективність протоколу OAuth 2.0, він також має певні вразливості та можливості для атак. Ця стаття має на меті описати ці вразливості та надати рекомендації щодо їх запобігання, забезпечивши тим самим підвищення рівня безпеки web-ресурсів та захист даних користувачів від можливих загроз.

Таким чином, данна стаття є актуальною для розробників та адміністраторів web-ресурсів, які використовують протокол OAuth 2.0 для захисту даних користувачів, а також для будь-яких осіб, які цікавляться питаннями безпеки в інтернеті.

Завдання написання наукової статті на тему «Особливості захисту web-ресурсів на основі OAuth 2.0» є дуже актуальним в сучасному світі, оскільки використання web-ресурсів зростає щодня, а з ним і ризики пов’язані з безпекою даних користувачів. Одним з основних методів захисту web-ресурсів є використання протоколу авторизації та ідентифікації OAuth 2.0.

Метою статті є розглянути особливості захисту web-ресурсів на основі протоколу OAuth 2.0 та надати розробникам та адміністраторам web-ресурсів рекомендації щодо забезпечення безпеки даних користувачів під час використання цього протоколу. Крім того, стаття має на меті описати можливі вразливості протоколу OAuth 2.0 та надати поради щодо їх запобігання.

Об’єктом написання даної статті є протокол OAuth 2.0 та його застосування для забезпечення безпеки web-ресурсів. Основною метою статті є розгляд особливостей захисту web-ресурсів на основі протоколу OAuth 2.0 та надання корисної інформації розробникам та адміністраторам web-ресурсів щодо забезпечення безпеки даних користувачів.У цій статті ми розглянемо основні принципи та можливості захисту web-ресурсів на основі OAuth 2.0, а також надамо поради щодо забезпечення безпеки під час використання цього протоколу.

Предметом дослідження – механізм захисту веб-ресурсів на основі OAuth 2.0 та його застосування для забезпечення безпеки веб-додатків.

Аналіз попередніх досліджень. Аналіз попередніх досліджень показав, що механізм OAuth 2.0 є одним з найпоширеніших стандартів авторизації інтернет-ресурсів. Він дозволяє користувачам давати доступ до своїх персональних даних веб-додаткам, забезпечуючи при цьому безпеку і захист приватності.

Проте, деякі попередні дослідження показали, що механізм OAuth 2.0 має свої слабкі сторони, зокрема, недостатню захищеність від атак типу CSRF та XSS. Для розв'язання цих проблем було запропоновано різні підходи, такі як використання state параметру, захист JWT токенів, та використання захищеного cookie.

Отже, враховуючи попередні дослідження, було проведено власне дослідження щодо захисту веб-ресурсів на основі OAuth 2.0, яке дозволило показати, що правильно налаштований механізм OAuth 2.0 може забезпечувати високий рівень безпеки веб-додатків., Л.А. Птіцина, Н.М. Тюріна, О.М. Іванова, С.В. Федоренко, А.А. Максимова та ін.

Виклад основного матеріалу. В сучасному світі інформаційні технології є одним з найбільш важливих аспектів розвитку суспільства. Інтернет є найбільшою базою даних, доступну для всіх користувачів з усього світу, тому захист від несанкціонованого доступу до цієї інформації є важливим завданням для розробників веб-ресурсів.

Одним з найефективніших методів захисту веб-ресурсів є протокол OAuth 2.0. Цей протокол дозволяє користувачам дозволяти доступ до своїх даних третім сторонам без необхідності передавати свої логіни та паролі. В даній статті будуть розглянуті основні принципи роботи протоколу OAuth 2.0, його переваги та недоліки, а також можливі шляхи покращення захисту веб-ресурсів на основі цього протоколу.

Основна частина

OAuth 2.0 – це протокол авторизації, який використовується для надання доступу до ресурсів через веб-інтерфейс. Протокол базується на технології токенів доступу, що дозволяє здійснювати безпечні запити до захищених веб-ресурсів без передачі логінів та паролів.

Принцип роботи протоколу полягає у тому, що користувач аутентифікується на сторонньому веб-ресурсі, після чого він надає дозвіл на доступ до своїх даних іншому веб-ресурсу. Це здійснюється за допомогою спеціальних запитів, які передаються між веб-ресурсами з використанням токенів доступу.

Основні принципи OAuth 2.0

OAuth 2.0 базується на таких основних принципах:

Розподіл ролей. В OAuth 2.0 існує два види ролей: «клієнт» і «постачальник ідентифікації». Клієнт – це додаток або сервіс, який хоче отримати доступ до захищених ресурсів, а постачальник ідентифікації – це система, яка перевіряє, що клієнт має право на доступ до ресурсів.

Розподілення даних доступу. OAuth 2.0 використовує токени доступу для забезпечення доступу до ресурсів. Клієнт отримує токен доступу від постачальника ідентифікації, який дозволяє йому отримати доступ до ресурсів. Токени доступу можуть бути тимчасовими або постійними.

Дозвіл на доступ. Клієнт не отримує безпосередньо доступ до ресурсів. Замість цього, він отримує дозвіл на доступ до ресурсів від постачальника ідентифікації. Це дозволяє постачальнику ідентифікації контролювати, які ресурси має доступ клієнт і як він використовує ці ресурси.

Безпека протоколу. Однією з найбільш важливих принципів OAuth 2.0 є забезпечення безпеки протоколу. Для цього використовуються такі механізми, як шифрування, підписи та перевірка на ідентифікацію.

Сценарії

Веб-серверні програми. Кінцева точка Google OAuth 2.0 підтримує програми веб-сервера, які використовують такі мови та фреймворки, як PHP, Java, Python, Ruby та ASP.NET (Рис 1).

Послідовність авторизації починається, коли ваша програма перенаправляє браузер на URL-адресу Google; URL-адреса містить параметри запиту, які вказують тип запитуваного

доступу. Google здійснює автентифікацію користувача, вибір сеансу та згоду користувача. Результатом є код авторизації, який програма може обміняти на маркер доступу та маркер оновлення.

Програма має зберігати маркер оновлення для подальшого використання та використовувати маркер доступу для доступу до Google API. Після закінчення терміну дії маркера доступу програма використовує маркер оновлення для отримання нового.

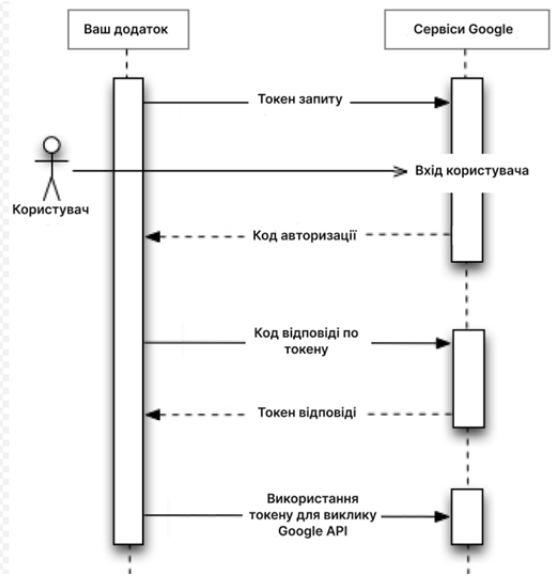

Рис. 1. Як працює Oauth2.0 з веб-серверними програмами

Клієнтські програми (JavaScript).

Кінцева точка Google OAuth 2.0 підтримує програми JavaScript, які запускаються у веб-переглядачі (Рис 2).

Послідовність авторизації починається, коли ваша програма перенаправляє браузер на URL-адресу Google; URL-адреса містить параметри запиту, які вказують тип запитуваного доступу. Google здійснює автентифікацію користувача, вибір сеансу та згоду користувача.

Результатом є маркер доступу, який клієнт повинен перевірити, перш ніж включити його в запит Google API. Коли термін дії маркера закінчується, програма повторює процес.

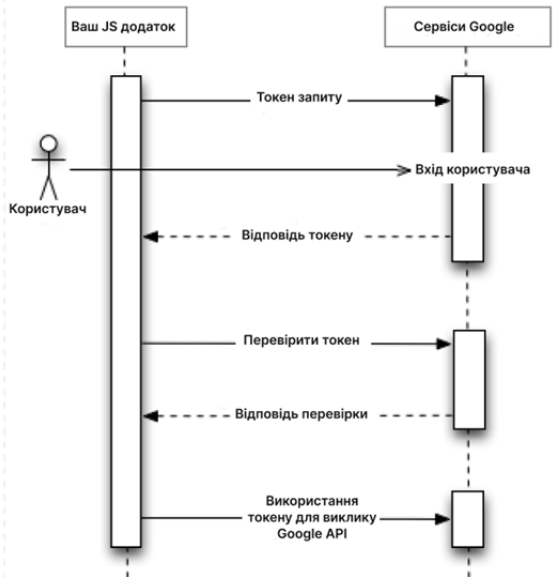

Рис. 2. Як працює Oauth2.0 з клієнтською програмою JavaScript

Програми на пристроях з обмеженим входом.

Кінцева точка Google OAuth 2.0 підтримує програми, які працюють на пристроях з обмеженим доступом, як-от ігрові консолі, відеокамери та принтери (Рис 3).

Послідовність авторизації починається з того, що програма надсилає запит веб-служби до URL-адреси Google для коду авторизації. Відповідь містить кілька параметрів, включаючи URL-адресу та код, які додаток показує користувачеві.

Користувач отримує URL-адресу та код із пристрою, а потім перемикається на окремий пристрій або комп'ютер із більшими можливостями введення. Користувач запускає браузер, переходить за вказаною URL-адресою, авторизується та вводить код.

Тим часом програма опитує URL-адресу Google через певний інтервал. Коли користувач схвалює доступ, відповідь від сервера Google містить маркер доступу та маркер оновлення. Програма має зберігати маркер оновлення для подальшого використання та використовувати маркер доступу для доступу до Google API. Після закінчення терміну дії маркера доступу програма використовує маркер оновлення для отримання нового.

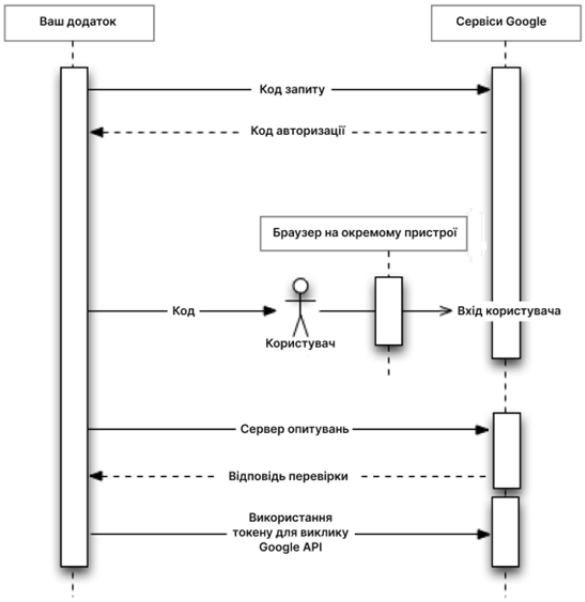

Рис. 3. Як працює Oauth2.0 з програмами на пристроях з обмеженим входом

Сервісні облікові записи.

Google API, наприклад Prediction API та Google Cloud Storage, можуть діяти від імені вашої програми без доступу до інформації користувача. У таких ситуаціях ваша програма повинна підтвердити свою власну ідентифікацію API, але згода користувача не потрібна. Подібним чином у корпоративних сценаріях ваша програма може запитувати делегований доступ до деяких ресурсів (Рис 4).

Для таких типів міжсерверної взаємодії вам потрібен обліковий запис служби, який є обліковим записом, який належить вашій програмі, а не окремому кінцевому користувачеві. Ваша програма викликає Google API від імені облікового запису служби, і згода користувача не потрібна. (У сценаріях, не пов'язаних із службовим обліковим записом, ваша програма викликає Google API від імені кінцевих користувачів, і іноді потрібна згода користувача.)

Облікові дані облікового запису служби, які ви отримуєте з Google API Console, включають згенеровану унікальну адресу електронної пошти, ідентифікатор клієнта та принаймні одну пару відкритих/приватних ключів. Ви використовуєте ідентифікатор клієнта та один закритий ключ, щоб створити підписаний JWT і створити запит маркера доступу у відповідному форматі. Потім ваша програма надсилає запит маркера на сервер авторизації Google OAuth 2.0, який повертає маркер доступу. Програма використовує маркер для доступу до Google API. Коли термін дії маркера закінчується, програма повторює процес.

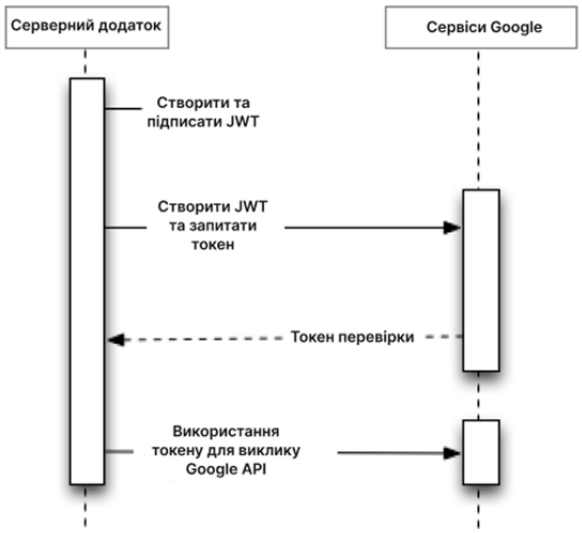

Рис. 4. Як працює Oauth2.0 з сервісними обліковими записами

Основними перевагами протоколу OAuth 2.0 є:

1. Зменшення ризику витоку паролів. Оскільки протокол використовує токени доступу, користувач не має потреби передавати свій логін та пароль сторонньому веб-ресурсу.

2. Можливість контролювання доступу до ресурсів. Протокол OAuth 2.0 дозволяє здійснювати детальний контроль над даними, до яких має доступ сторонній веб-ресурс. Користувач може обрати, які дозволи надаються тому чи іншому веб-ресурсу, а також змінювати їх в будь-який момент.

3. Спрощення розробки веб-додатків. За допомогою протоколу OAuth 2.0 розробники можуть значно спростити процес авторизації та реалізувати її за декілька кроків.

Однак, протокол OAuth 2.0 має і свої недоліки. Найбільш відомим з них є проблема безпеки, зокрема можливість атаки типу Man-in-the-middle (MITM), коли зловмисник перехоплює токен доступу та здійснює несанкціонований доступ до веб-ресурсу.

Одним із способів покращення захисту веб-ресурсів на основі протоколу OAuth 2.0 є використання двофакторної аутентифікації, яка забезпечує додатковий рівень захисту. Двофакторна аутентифікація полягає у використанні двох або більше методів для підтвердження особистості користувача, наприклад, введення пароля та використання коду, що надсилається на мобільний телефон.

Ще одним шляхом покращення захисту є використання захищеного з'єднання (SSL/TLS), яке забезпечує безпечний обмін даними між веб-ресурсами. Це зменшує ризик перехоплення токенів доступу та здійснення атак MITM.

Також можливим варіантом є використання додаткових заходів безпеки, таких як криптографічне підписання запитів та перевірка цілісності даних.

При розробці веб-додатків, які використовують протокол OAuth 2.0, необхідно дотримуватися кількох правил безпеки, щоб мінімізувати ризики несанкціонованого доступу до веб-ресурсу. Декілька рекомендацій, які можуть допомогти забезпечити безпеку веб-додатків на основі протоколу OAuth 2.0, наведені нижче.

1. Захист токенів доступу. Токени доступу мають велике значення для захисту веб-ресурсів на основі протоколу OAuth 2.0. Тому вони повинні бути зберігатися у безпечному місці та передаватися тільки по захищеному каналу. Для зменшення ризику несанкціонованого доступу до токенів доступу рекомендується використовувати їх з обмеженим терміном дії.

2. Перевірка джерела запитів. Веб-додатки на основі протоколу OAuth 2.0 повинні перевіряти джерело запиту перед тим, як надавати доступ до ресурсів. Це допомагає уникнути атак типу CSRF (Cross-Site Request Forgery), коли зловмисник намагається виконати дії в ім'я авторизованого користувача без його згоди.

3. Використання HTTPS для всіх запитів. Для забезпечення безпеки веб-додатки на основі протоколу OAuth 2.0 повинні використовувати захищене з'єднання HTTPS для всіх запитів. Це забезпечує безпечний обмін даними між веб-ресурсами та зменшує ризик перехоплення даних або токенів доступу.

4. Моніторинг активності користувачів. Для зменшення ризиків несанкціонованого доступу до веб-ресурсів, на основі протоколу OAuth 2.0, необхідно вести моніторинг активності користувачів. Це допомагає вчасно виявляти та реагувати на підозрілу або незвичну активність.

5. Використання правильних типів авторизації. Для різних типів веб-додатків можуть використовуватися різні типи авторизації. Наприклад, для веб-додатків, які взаємодіють з API, можуть використовуватися токени доступу з обмеженими правами доступу. Для веб-додатків, які взаємодіють з користувачами, можуть використовуватися авторизаційні токени з вищим рівнем доступу.

6. Використання двофакторної аутентифікації. Для підвищення рівня безпеки веб-додатки на основі протоколу OAuth 2.0 можуть використовувати двофакторну аутентифікацію. Це допомагає зменшити ризик несанкціонованого доступу до веб-ресурсів навіть у тому випадку, якщо зловмиснику вдалося отримати доступ до користувачевого пароля.

7. Використання авторизації на основі ролей. Для керування рівнями доступу веб-додатки на основі протоколу OAuth 2.0 можуть використовувати авторизацію на основі ролей. Це дозволяє обмежити доступ до ресурсів в залежності від ролі користувача.

Усі ці рекомендації допоможуть забезпечити безпеку веб-додатків на основі протоколу OAuth 2.0 та запобігти можливим атакам. Однак, важливо пам'ятати, що безпека є постійним процесом, тому веб-додатки повинні постійно моніторитися та підтримуватися у відповідному стані.

Висновки. Отже, OAuth 2.0 є ефективним механізмом для захисту web-ресурсів, оскільки дозволяє забезпечити авторизацію користувачів і управління доступом до ресурсів за допомогою токенів доступу. Правильна реалізація механізму OAuth 2.0 може запобігти багатьом загрозам для безпеки веб-додатків, таким як атаки на міжсайтовий скриптінг, перехоплення сесії та інші. У даній статті було описано основні принципи роботи механізму OAuth 2.0, а також запропоновані практичні рекомендації щодо його безпечної реалізації. Оскільки механізм OAuth 2.0 поширено в сучасних веб-додатках, знання про його особливості та застосування в практиці може бути корисним для розробників веб-додатків.

Список використаних джерел

1. Офіційна документація OAuth 2.0 на сайті IETF (https://tools.ietf.org/html/rfc6749)
2. Стаття «OAuth 2.0 Security Best Current Practice» на сайті IETF (https://tools.ietf.org/html/draft-ietf-oauth-security-topics-16)
3. Стаття «OAuth 2.0 Threat Model and Security Considerations» на сайті IETF (https://datatracker.ietf.org/doc/html/rfc6819)
4. Офіційна документація на сайті OAuth.com (https://oauth.net/2/)
5. Стаття «OAuth» на сайті Ping Identity (https://www.pingidentity.com/en/resources/identity-fundamentals/authentication-authorization-standards/oauth.html)
6. Стаття «OpenID Connect & OAuth 2.0 API» на сайті Okta (https://developer.okta.com/docs/reference/api/oidc/)
7. Стаття «OAuth 2.0 Security Cheat Sheet» на сайті GitHub (https://github.com/koenbuyens/oauth-2.0-security-cheat-sheet)
8. Стаття «Using OAuth 2.0 to Access Google APIs» на сайті Developers.Google (https://developers.google.com/identity/protocols/oauth2)

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

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КІБЕРАТАК У СИСТЕМІ СУДОУСТРОЮ

ЮНАК А., 2м курс ФІТ ДТЕУ,
спеціальність «Кібербезпека та захист інформації»

У статті розглянуто методи захисту інформації від кібератак в системі судоустрою. Описано загрози, які можуть стати причиною кібератак на систему судоустрою та наслідки таких атак. Зазначено переваги застосування програмних забезпечень в судоустрою, надано опис та рекомендації щодо впровадження в практику роботи системи судоустрою. Розглянуто важливі аспекти підготовки та навчання персоналу щодо кібербезпеки та захисту інформації в системі судоустрою.

The article discusses methods for protecting information from cyber attacks in the judicial system. It describes the threats that could cause cyber attacks on the judicial system and the consequences of such attacks. The advantages of using software in the judicial system are noted, and detailed descriptions and recommendations for implementing them into the practical work of the judicial system are provided. Important aspects of preparing and training personnel in cybersecurity and information protection in the judicial system are also discussed.

Актуальність. Актуальність методів захисту інформації від кібератак в системі судоустрою надзвичайно висока в сучасних умовах. Кібератаки на системи судоустрою можуть стати причиною порушення правосуддя, втрати конфіденційної інформації, порушення прав людини та інших серйозних наслідків. У зв'язку зі зростанням кількості та складності кібератак, системи судоустрою повинні бути постійно готові до захисту від таких атак. Застосування ефективних методів захисту є надзвичайно важливим для забезпечення безпеки та надійності роботи систем судоустрою.

Крім того, залежно від країни та її політичного контексту, системи судоустрою можуть бути особливо цільовими об'єктами кібератак з боку керівництва, політичних опозиційних сил, злочинців та інших груп. Таким чином, захист інформації в системі судоустрою є дуже важливою та актуальною проблемою, яку потрібно вирішувати негайно.

Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують в прискореному темпі, кіберзлочини стають досконалішими, краще організованими і транснаціональними. Це зумовлено тим, що інтернет, цифрові послуги, інформаційно-комунікаційні технології стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайн-банкінгу до систем інтернету речей та інтелектуальних систем управління підприємствами та судоустрою.

Система кібербезпеки має працювати в інтересах громадськості як для постачальників послуг, так і для користувачів послуг.

Саме держава, як гарант прав і свобод громадян, має взяти на себе відповідальність за забезпечення доступу до стабільного безпечного цифрового простору, яким можуть скористатися всі громадяни, адже забезпечення належного рівня кібербезпеки є необхідною умовою розвитку інформаційного суспільства.

Тому, захист інформації від кібератак є однією з головних проблем в сфері інформаційної безпеки судової системи.

Метою статті є комплексний аналіз методів захисту інформації від кібератак в системі судоустрою.

Об'єктом дослідження є застосування різних методів і технологій для захисту інформації в системі судоустрою від кібератак.

Предмет дослідження – методи захисту інформації в системі судоустрою від кібератак.

Аналіз останніх досліджень. Дослідженню кібербезпеки основних характерних рис присвячені праці вітчизняних науковців: Арістова І.В., Березовської І.Р., Дзьобаня О.П., Калюжного Р.А., Кормича Б.А., Ліпкана В.А., Марущак А.І., Цимбалюка В.С., Юдіна О.К. та інших.

Виклад основного матеріалу. Існує безліч різних кібератак, які можуть бути спрямовані на систему судоустрою, такі як:

- Фішинг: атаки, які спрямовані на отримання конфіденційних даних, таких як імена користувачів та паролі, шляхом відправлення підробленої електронної пошти, яка маскується під довірену організацію.
- Сервіс-атаки (DDoS): це атаки, які призводять до перевантаження серверів або інфраструктури, що призводить до відмови в обслуговуванні, зупинки роботи системи та зниження продуктивності.
- Віруси та шкідливі програми: ці атаки спрямовані на викрадення конфіденційної інформації або руйнування системи, заражаючи її вірусами та шкідливими програмами.
- SQL-ін'єкції: це атаки, які використовують недоліки безпеки в базі даних для викрадення конфіденційної інформації або руйнування системи.
- Соціальний інжиніринг: це атаки, які спрямовані на злам системи, використовуючи маніпулювання психологією користувачів з метою отримання конфіденційної інформації або доступу до системи. Наприклад, зловмисник може надіслати електронного листа, що маскується під іншого користувача, та запросити інформацію про систему чи надати шлях для доступу.
- Розповсюдження дезінформації: це кібератака яка використовує цифрове середовище для поширення неправдивої інформації. Ці атаки можуть бути здійснені через соціальні мережі, веб-сайти, електронну пошту та інші канали комунікації.
- Ретельне перехоплення пакетів (TCP/IP Hijacking) – атака, яка полягає в перехопленні передачі даних між комп'ютерами із застосуванням програмного забезпечення.

Із за цього наслідки кібератак на систему судоустрою можуть бути дуже серйозними та мають далекосяжні наслідки для її користувачів, такі як:

- Втрата конфіденційної інформації: кібератаки можуть призвести до втрати конфіденційної інформації, такої як імена, адреси, електронні адреси та інші особисті дані. Це може стати на шляху вивчення судової справи та викликати серйозні наслідки для приватності та безпеки користувачів.
- Порушення цілісності даних: кібератаки можуть також призвести до порушення цілісності даних, що може призвести до внесення змін в судову справу або видалення важливих даних.
- Порушення доступності: атаки на доступність можуть призвести до зупинки роботи системи, що може призвести до затримок у вирішенні судових справ, збільшення термінів та зниження продуктивності.
- Підрив довіри до системи: кібератаки можуть підірвати довіру до системи, яка є ключовим елементом судової системи. Це може викликати серйозні наслідки для довіри до судової системи та вплинути на результати судових рішень.
- Фінансові наслідки: кібератаки можуть призвести до значних фінансових наслідків, таких як витрати на відновлення системи, компенсації постраждалим та збитки, пов'язані з втратою продуктивності та затримками у судових рішеннях.

Тому захист інформації є одним з ключових аспектів судової системи, якій приділяється велика увага. Кіберзлочинці можуть використовувати різні методи, щоб отримати доступ до конфіденційної інформації, яка зберігається в системі судоустрою. Далі у статті будуть приведені методи захисту інформації від кібератак в системі судоустрою [1].

Криптографічний захист один з методів захисту інформації, який використовує складні математичні алгоритми, щоб зашифрувати дані перед їх відправкою, тим самим роблячи їх нерозбірливими для кіберзлочинців. Може включати в себе заходи, як шифрування даних, цифрові підписи, та аутентифікації, методи захисту інформації, які допомагають забезпечити конфіденційність і збереження даних у неушкодженому вихідному стані.

Простіше кажучи, є різні типи повідомлень, включаючи електронну пошту, файли, бази даних та багато інших видів інформації. Більш просунуті та ефективні методи криптографічного захисту досягаються через використання багатьох складних алгоритмів та схем шифрування, які регулярно оновлюються та модифікуються, щоб запобігти несанкціонованому доступу та забезпечити захист даних.

Для прикладу, одним з найпоширеніших криптографічних алгоритмів є алгоритм RSA, який базується на складності факторизації великих чисел. Цей алгоритм використовується для шифрування та розшифрування інформації за допомогою публічного та приватного ключів.

Інший криптографічний алгоритм, який використовується для захисту інформації від кібератак, – це алгоритм AES (Advanced Encryption Standard). Він використовується для шифрування та розшифрування інформації з використанням секретного ключа. Алгоритм AES є стандартом у багатьох сучасних криптографічних протоколах, включаючи SSL / TLS для захисту трафіку в Інтернеті [1, 3].

Судоустрої дуже ефективно використовують електрону пошту в документообігу, для цього вони використовують ключи, так кажучи для підтвердження особи або аутентифікації.

Є кілька методів які активно використовуються в судоустрої, це аутентифікація за сертифікатами, зараз кожний може отримати сертифікати, вони використовуються разом с ключами які людина може отримати навіть через такі додаткі як ПриватБанк або ОщадБанк. Сертифікат являє собою набір атрибутів, що ідентифікують власника, підписаний certificate authority (CA). CA виступає в ролі посередника, який гарантує справжність сертифікатів. Також сертифікат криптографічно пов’язаний з закритим ключем, який зберігається у власника сертифіката і дозволяє однозначно підтвердити факт володіння сертифікатом. Сертифікат може зберігатися в операціонній системі, в браузері або на окремому фізичному пристрої, такому як смарт картка або токен USB. А закритий ключ захищається, зазвичай, ще паролем. Цей спосіб є більш надійним ніж аутентифікації за паролем, але в зв’язку з важкістю розповсюдження сертифікатів, цей метод аутентифікації є менш популярним.

Аутентифікація за ключами доступу − використовується для застосунків та сервісів при їх звернені до Web-сервісів. Для аутентифікаціїї в даному методі використовюються ключі доступу, наприклад access key, API key. Ключі доступу − це довгі унікальні строки, що являють собою рандомний набір символів. Зазвичай користувачі, які хочуть отримати доступ до Web-сервісу роблять запит на створення ключа доступу і в подальшому зберігають його у клієнтському застосунку.

Цей ключ може давати не повний доступ до ресурсу після аутентифікації, це може бути задано при створенні ключа доступу. Так як ключ доступу є випадково підібраними символами, його складніше буде підібрати, на відміну від звичайного пароля. У випадку компрометації ключа, його можна анулювати і створити новий. На (Рис.1) зображено просте розуміння як проходить аутентифікація сертифіката, для чого використовується криптографічна бібліотека.

Аутентифікація за токенами − використовується зазвичай для розподілених систем Single Sign-On (SSO), де аутентифікація відбувається за рахунок іншого сервісу, наприклад здійснення аутентифікації через обліковий запис соціальних мереж. Соціальні мережі виступають в ролі сервіса аутентифікації. Токен – це структура даних, що складається з інформації: строк дії токена, відправник, можливий отримувач токену та деяка інформація про користувача, що здійснив запит на створення токену. Токен для збереження цілісності даних і захисту від несанкціонованого змінення даних додатково підписується. Одними з найрозповсюджених форматів токенів є: Simple Web Token (SWT), JSON Web Token (JWT), Security Assertion Markup Language (SAML). Для даного методу аутентифікації використовуються стандарти, що описують протокол взаємодії між клієнтами та IP і SP застосунками, також, як і формат токенів, що надсилаються. До таких стандартів належать: стандарт SAML, стандарт WS-Trust, стандарт WS-Federation, стандарт OAuth, стандарт OpenID Connect.

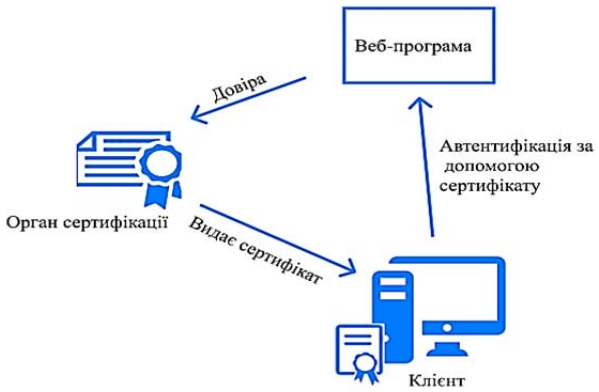

Рис. 1. Схема аутентифікації сертифіката

Система судоустрою повинна бути здатна сповістити про можливі кібератаки. Наприклад, системи виявлення вторгнень можуть слідкувати за активністю в мережі, щоб мати змогу вчасно заблокувати можливість вторгнення [2].

Попередження кібератак одна з головних систем заходів, яка використовується для захисту комп'ютерної системи від потенційних кіберзагроз та атак. Безпека даних є важливою проблемою, яка потребує не тільки профілактичних заходів, таких як резервне копіювання даних, використання паролів та інших методів автентифікації, але також можливості реагування на кібератаки, які можуть відбуватися будь-якої миті. Отже система кібератак має методи виявлення спроб несанкціонованого доступу чи злому комп'ютерних систем. Вона може включати використання різних методів для моніторингу мережного трафіку і виявлення незвичайних або підозрілих дій, для цього використовують одні із популярних систем моніторингу як Zabbix або Grafana (Рис. 2, Рис. 3.).

Рис. 2. Інтерфейс «Zabbix»

Крім цього, якщо людина не розуміється в кібербезпеці для цього є заходи щодо виявлення та запобігання кібератакам, такі як використання програмного забезпечення для блокування потенційно шкідливих сайтів та більшу увагу до безпеки паролів у рамках судоустрою. Реагування на попередження кібератак може включати заходи щодо блокування вразливих вузлів мережі, перезавантаження обладнання або зміни налаштувань, оповіщення відповідних осіб про можливі загрози та багато інших дій.

Рис. 3. Інтерфейс «Grafana»

Системи моніторингу та попередження кібератак повинні забезпечувати надійний захист комп'ютерних систем від потенційних загроз та діяти у тісній співпраці з іншими системами безпеки. Вони повинні постійно оновлюватися та адаптуватися до нових видів атак, тому використання інноваційних методів та технологій − ключовий фактор у забезпеченні ефективного захисту від кібератак.

Також одним з актуальних методів виступає не тільки моніторинг ну і сам захист мережі судоустрою. Адміністратори мережі повинні використовувати захисні технології, такі як брандмауери, антивірусні програми, що допоможуть захистити мережу від кібератак.

Захист мережі являє собою процес створення та застосування заходів, які потрібні для забезпечення безпеки мережі, зокрема її хостів, даних, пристроїв і систем, пов'язаних з нею.

Захист мережі включає заходи, такі як:

- Використання безпечних паролів та методів аутентифікації, а також шифрування даних.
- Регулярне оновлення програмного забезпечення, операційних систем, маршрутизаторів та іншого обладнання.
- Встановлення та налаштування персональних та «брандмауерів».
- Шифрування даних та використання резервного копіювання для захисту даних у разі порушення безпеки.
- Використання VPN (віртуальної приватної мережі) для безпечного підключення до мережі з віддалених місць.
- Використання системи обмеження прав доступу до файлів та каталогів для забезпечення безпеки даних.
- Проведення тестування мережі на вразливість та аудиту безпеки з метою виявлення слабких місць та вдосконалення системи захисту.

Є ще один захід захисту як Wifi, але по політиці безпеки судоустрою та і взагалі із за великої ймовірності перехвату або самого взлому мережі що дасть кіберзлочинцю доступ до конфіденційної інформації, вже мало де використовується.

Отже для ефективного захисту мережі, крім вищеописаних заходів, необхідно мати систему виявлення і реагування на загрози. Це включає моніторинг мережевого трафіку на наявність аномальної активності, пошук несанкціонованих пристроїв на мережі, а також виявлення спроб злому системи захисту Важливим аспектом захисту мережі є також навчання персоналу. Всі користувачі, які мають доступ до мережі, повинні бути навчені безпеці та заходам запобігання загрозам. Вони повинні розуміти, як захистити як власні дані, так і дані, пов'язані з мережею [3]. Зрештою, захист мережі − постійний процес, що вимагає повної комбінації заходів для виявлення, запобігання та реагування на загрози.

Резервне копіювання інформації. Інформація більше за все зберігається на серверах, із за цього з'являється проблема в тому що, сервер може вийти із строю або якщо пройшла кібератака, тоді для безпеки інформації система судоустрою повинна регулярно створювати резервні копії інформації, щоб при випадку таких ситуацій була можливість відновити дані.

Існує безліч способів створення резервних копій, включаючи такі методи:

- Програмне забезпечення для резервного копіювання даних.
- Ручне копіювання даних на зовнішні жорсткі диски, USB або інші портативні пристрої для зберігання даних.
- Резервне копіювання даних у хмарних сервісах.

Крім того, важливо вибрати правильне сховище для копіювання резервних копій даних. Резервні копії можуть зберігатися на зовнішніх жорстких дисках, серверах у хмарному сховищі або інших пристроях. При виборі сховища для резервних копій слід враховувати такі фактори: місткість пристрою; тип інтерфейсу; швидкість передачі даних; ціна; надійність та безпека.

Також необхідно регулярно перевіряти резервні копії даних на наявність дефектів або помилок та стежити за їх актуальністю. важливо регулярно створювати копії даних для того, щоб мати доступ до останньої версії даних, якщо потрібно відновити інформацію.

Усі користувачі системи судоустрою повинні бути навчені засадам та правилам безпеки інформації та кібербезпеки, щоб зменшити частоту випадків людської помилки, що спричиняють кібератаки, втрати інформації або зараження вірусом саму мережу судоустрою. Навчання персоналу кібербезпеки в судоустрої є дуже важливим питанням, оскільки судові системи містять велику кількість конфіденційної інформації, яка може стати об'єктом кібератак з боку зловмисників.

Таблиця порівняння кіберзахисту (Таблиця 1) різних судових систем може бути корисною для оцінки рівня кібербезпеки:

Таблиця 1

Порівняння типи захисту систем судоустрою

Тип захисту	Система А	Система В	Система С
Рівень шифрування даних.	AES-256	AES-128	3DES
Застосування багатофакторної аутентифікації.	Так	Ні	Так
Система моніторингу та виявлення вторгнень.	Так	Так	Ні
Автоматичне оновлення програмного забезпечення.	Так	Так	Ні
Система контролю доступу до даних.	RBAC	ABAC	DAC
Наявність системи резервного копіювання.	Так	Ні	Так
Рівень відповідальності за кібербезпеку.	Кожен користувач	Ввіділ ІТ	Кожен користувач та ввіділ ІТ.

Зазначені показники можуть варіюватися в залежності від конкретної судової системи, її розміру та обсягу діяльності. Важливо зрозуміти, що жодна система кібербезпеки не є абсолютною, і завжди є ризики та потенційні вразливості. Тому необхідно постійно оновлювати заходи з кібербезпеки та забезпечувати належний рівень свідомості серед користувачів щодо правил безпеки в інформаційних системах [2, 4].

Основними аспектами навчання персоналу кібербезпеки в судоустрої можуть бути:

- Освіта і свідомість: персонал повинен розуміти, що кібербезпека є ключовою складовою судової системи і має бути усвідомлено, як відповідальність кожного працівника.
- Створення і розробка політики кібербезпеки: судова система повинна мати детальну політику кібербезпеки, яка включає в себе заходи з протидії кібератакам та забезпечення безпеки в мережі.
- Система обміну інформацією: судова система повинна мати систему обміну інформацією між співробітниками, яка буде забезпечувати безпеку в мережі.

- Захист інформації: судова система повинна мати захист інформації з допомогою шифрування, паролів, біометричних методів ідентифікації тощо.
- Перевірка безпеки: судова система повинна проводити перевірки безпеки системи, щоб виявити потенційні проблеми та ризики та вживати заходів з їх усунення.
- Курси підвищення кваліфікації: персонал повинен бути навчений останнім методам та технологіям кібербезпеки та проходити курси підвищення кваліфікації з регулярністю.

Захист інформації від кібератак є дуже важливою задачею для будь-якої системи, в тому числі й системи судоустрою. У зв'язку з тим, що система містить значну кількість конфіденційної інформації, включаючи особисті дані громадян, захист цієї інформації є критично важливим [4].

Методи захисту від кібератак в системі судоустрою можуть бути різними, включаючи аутентифікацію користувачів, шифрування даних, захист мережі, оновлення програмного та апаратного забезпечення, аналіз поведінки та виявлення загроз, а також підвищення кібербезпеки користувачів. Крім того, важливим аспектом є стратегії відповідного реагування на кібератаки, такі як планування відповіді на кібератаки, резервне копіювання даних та відновлення системи, вивчення кібератак та забезпечення належного навчання співробітників щодо кібербезпеки. Застосування методів захисту від кібератак у системі судоустрою є дуже важливим для забезпечення кібербезпеки та захисту конфіденційної інформації. Тому, системи судоустрою повинні регулярно вдосконалювати свої методи захисту та забезпечувати навчання своїх співробітників щодо кібербезпеки.

Висновки. Кібератаки можуть спричинити серйозні наслідки, які відображаються в порушенні конфіденційності, цілісності та доступності інформації, тому, захист інформації від кібератак є однією з головних проблем в сфері інформаційної безпеки судової системи. Застосування методів захисту від кібератак у системі судоустрою є дуже важливим для забезпечення кібербезпеки та захисту конфіденційної інформації. Тому, системи судоустрою повинні регулярно вдосконалювати свої методи захисту та забезпечувати навчання своїх співробітників щодо кібербезпеки.

Список використаних джерел

1. Б. Толубка Інформаційна та кібербезпека: соціотехнічний аспект / Б. Толубка // Кіберпростір, кібербезпека та кібертероризм: зб. наук. праць «ДУТ» – 2015р., с. 7 – 63.
2. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019., с.164.
3. How to Protect Your Data from Unauthorized Access, Retrieved from \\ Режим доступу: https://cypressdatadefense.com/blog/unauthorized-data-access. (останнє звернення 07.04.2023)
4. Матеріали Української софтверної IT компанія «TQM systems» \\ Режим доступу: https://tqm.com.ua/ua/company/about (останнє звернення 07.04.2023)

Робота виконана під науковим керівництвом канд. політ. наук, доцента
ЧУБАЄВСЬКОГО В. І.

ПОРІВНЯННЯ НАТИВНОГО ТА ВЕБПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБМІНУ ЗАХИЩЕНИМИ ДАНИМИ

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

У цій статті детально розглянуто порівняння між нативним та веб-програмним забезпеченням для обміну захищеними даними. Розглянуто переваги та недоліки кожного типу програмного забезпечення, різницю між ними, зокрема щодо швидкості та продуктивності, доступності та зручності використання, вартості та складності розробки та підтримки. У статті також розглянуто поняття безпеки даних, захисту персональних даних та технології шифрування даних.

This article provides a detailed comparison between native and web-based software for exchanging secure data. It examines the advantages and disadvantages of each type of software, the differences between them, including speed and productivity, accessibility and usability, cost and complexity of development and maintenance. The article also discusses data security concepts, personal data protection, and data encryption technologies.

Актуальність. Ця стаття є актуальною в контексті епохи цифрових технологій та інформаційного суспільства, оскільки безпека обміну захищеними даними є важливою проблемою для мільйонів користувачів Інтернету. Вибір оптимального програмного забезпечення є ключовим аспектом для забезпечення безпеки та захищеності цих даних. Розуміння переваг та недоліків різних типів програмного забезпечення, а також технологій шифрування, може допомогти забезпечити захист від зловмисників, які можуть намагатися зламати доступ до цієї інформації. Дана стаття допоможе користувачам розібратися з перевагами та недоліками різних типів програмного забезпечення для обміну захищеними даними.

Метою статті є порівняння нативного та веб-програмного забезпечення для обміну захищеними даними, з метою визначення переваг та недоліків кожного з них, а також надання рекомендацій щодо вибору відповідного програмного забезпечення за тими чи іншими потребами користувача.

Об'єктом дослідження є програмне забезпечення для обміну захищеними даними.

Завдання статті полягає в наступному*:*

– аналіз технічних характеристик та функціональних можливостей нативного та веб-програмного забезпечення для обміну захищеними даними;

– порівняння переваг та недоліків кожного типу програмного забезпечення для обміну захищеними даними;

– оцінка рівня безпеки нативного та веб-програмного забезпечення для обміну захищеними даними;

– рекомендації щодо вибору відповідного програмного забезпечення за тими чи іншими потребами користувача.

У сучасному світі, захист персональних даних стає все більш актуальним питанням, обмін даними зберігається як один з ключових елементів бізнес-процесів. Наявні різні способи забезпечення безпеки обміну даними, одним з яких є використання нативного та веб-програмного забезпечення, котрі можуть бути використані для забезпечення цього процесу, проте кожен з них має свої переваги та недоліки.

Нативне програмне забезпечення, як правило, розробляється для конкретної платформи та встановлюється безпосередньо на комп'ютер користувача та працює з локальними даними, має прямий доступ до ресурсів операційної системи. Це дає користувачу повний контроль над даними та забезпечує високий рівень безпеки. Проте, встановлення та

підтримка нативного програмного забезпечення потребує доволі багато часу та може бути дорогим. Прикладами нативного програмного забезпечення для обміну захищеними даними є PGP (Pretty Good Privacy) і GnuPG (GNU Privacy Guard) [1].

Веб-програмне забезпечення працює через веб-браузер та може бути використане на будь-якому пристрої з доступом до Інтернету. Це забезпечує зручність використання та швидкий доступ до даних. Однак, воно може бути менш безпечним порівняно з нативним програмним забезпеченням, оскільки відкрите з'єднання з Інтернетом може бути легше скомпрометовано. Прикладами веб-програмного забезпечення для обміну захищеними даними є ProtonMail, Tutanota та Mega.

Одним з найбільш важливих аспектів обміну захищеними даними є захист від несанкціонованого доступу. Обидва види програмного забезпечення можуть забезпечити цей захист, проте вони роблять це по-різному. Нативне програмне забезпечення може використовувати механізми шифрування та аутентифікації для захисту даних, таких як AES (Advanced Encryption Standard) та RSA (Rivest-Shamir-Adleman). Ці механізми забезпечують конфіденційність даних надаючи тільки верифікованим користувач доступ до даних. Веб-програмне забезпечення може використовувати протоколи шифрування та сертифікації безпеки, такі як SSL (Secure Sockets Layer) або TLS (Transport Layer Security) [2]. Ці протоколи застосовуються для захисту даних, які передаються через Інтернет, від прослуховування та зміни під час передачі. Це забезпечує конфіденційність даних, що передаються між веб-браузером та веб-сайтом, та їх відповідність, забезпечуючи, що веб-сайт, з яким взаємодіє користувач, є дійсно тим, за яким він видає себе. Оскільки веб-програмне забезпечення працює через мережу Інтернет, воно може бути доступним з будь-якого пристрою з підключенням до Інтернету, що робить його відмінним від нативного програмного забезпечення.

Нативне програмне забезпечення – це програмне забезпечення, що встановлюється безпосередньо на операційну систему і виконується на комп'ютері або мобільному пристрої. До переваг нативного програмного забезпечення відносяться швидкість виконання, можливість доступу до апаратних ресурсів та можливість використання системних бібліотек.

Веб-програмне забезпечення – це програмне забезпечення, яке запускається у веб-браузері та взаємодіє з сервером через Інтернет. До переваг веб-програмного забезпечення відносяться можливість використання на будь-якому пристрої, що має доступ до Інтернету, відсутність необхідності встановлення на кожному пристрої та можливість оновлення програмного забезпечення на сервері, що дає можливість швидко внести зміни до протоколів без необхідності оновлення на кожному пристрої.

Однак, веб-програмне забезпечення може мати проблеми зі швидкістю виконання та надійністю, так як воно залежить від швидкості та надійності Інтернет-з'єднання. Також, веб-програмне забезпечення може бути більш вразливим до атак, так як воно працює через відкрите Інтернет-з'єднання.

При порівнянні нативного та веб-програмного забезпечення для обміну захищеними даними, слід враховувати різні фактори, такі як швидкість виконання, доступність, надійність та безпека.

Щодо швидкості виконання, нативне програмне забезпечення має перевагу, так як воно працює безпосередньо на пристрої. Однак, веб-програмне забезпечення може бути більш доступним, оскільки воно працює на будь-якому пристрої з доступом до Інтернету.

Щодо надійності та безпеки, обидва типи програмного забезпечення мають свої переваги та недоліки. Нативне програмне забезпечення може бути менш вразливим до атак та забезпечувати більшу контрольованість над даними, однак, наявність програмного забезпечення на кожному пристрої може бути проблемою. Веб-програмне забезпечення може бути більш вразливим до атак, але воно забезпечує більшу безпеку відносно доступності та можливості оновлення протоколів на сервері.

При використанні веб-програмного забезпечення для обміну захищеними даними слід враховувати ризики, пов'язані з безпекою Інтернет-з'єднання та вразливостями веб-додатків.

Необхідно використовувати шифрування даних та ідентифікацію користувача для забезпечення безпеки даних.

Однак, використання нативного програмного забезпечення для обміну захищеними даними також має свої ризики. Наприклад, віруси та шкідливі програми можуть надходити через зовнішні пристрої, такі як флеш-накопичувачі або зовнішні жорсткі диски.

Отже, при виборі між нативним та веб-програмним забезпеченням для обміну захищеними даними слід враховувати різні фактори та ризики. В залежності від конкретних потреб та вимог, один тип програмного забезпечення може бути більш підходящим за іншого.

Нативне програмне забезпечення може бути більш вразливим для кібератак, оскільки воно може бути встановлене на кількох пристроях, які поєднані в локальну мережу, можуть бути менш безпечними. Натомість, веб-програмне забезпечення запущене на сервері та підтримується командою розробників, що може знизити ризик порушення безпеки. Однак, якщо веб-програмне забезпечення не належним чином налаштоване та забезпечене, воно також може бути вразливим для кібератак.

Незалежно від того, яке програмне забезпечення буде використане, необхідно забезпечити дотримання відповідних стандартів безпеки та захисту даних, таких як GDPR (Загальний регламент про захист даних), HIPAA (Закон про портативні електронні засоби зберігання медичної інформації) та інші [3].

Також важливо враховувати, що розвиток технологій та зміни в правовому середовищі можуть вплинути на вибір програмного забезпечення для обміну захищеними даними в майбутньому. Тому рекомендується регулярно оцінювати потреби та забезпечення безпеки при використанні програмного забезпечення для обміну захищеними даними та адаптувати підходи до вибору відповідно до змін у відповідних вимогах та контексті використання.

Нативне програмне забезпечення може бути більш безпечним, оскільки воно може бути написане мовами програмування з високим рівнем контролю та має прямий доступ до апаратного забезпечення. Крім того, воно може бути відключене від Інтернету, що додає ще більше рівня безпеки.

З іншого боку, веб-програмне забезпечення може мати перевагу в безпеці, оскільки веб-сайти та програми можуть оновлюватись в режимі реального часу, що дозволяє швидко виправляти помилки та додавати нові функції з точки зору безпеки. Крім того, веб-програмне забезпечення може мати вбудовані заходи безпеки, такі як механізми перевірки валідності введених даних та відстеження випадків зламу.

Важливим фактором є підтримка та обслуговування програмного забезпечення. Нативне програмне забезпечення може вимагати більшої кількості технічної підтримки та обслуговування, оскільки воно повинне бути встановлене та підтримуватися на кожному пристрої, на якому воно використовується. У випадку веб-програмного забезпечення, підтримка та обслуговування можуть бути більш централізованими, оскільки воно запущене на серверах та може бути підтримуване централізованою командою розробників.

Окрім цього, важливо враховувати вартість програмного забезпечення та витрати на його встановлення та підтримку. Нативне програмне забезпечення може вимагати значних витрат на його розробку та встановлення на кожному пристрої, на якому воно використовується. У випадку веб-програмного забезпечення, витрати можуть бути меншими, оскільки його можна запустити на серверах та користуватися ним з будь-якого пристрою з доступом до Інтернету [4].

Для обміну захищеними даними важливо також враховувати додаткові функції, такі як шифрування та аутентифікація користувачів. Нативне програмне забезпечення може бути складніше для реалізації цих функцій, оскільки вони повинні бути реалізовані на кожному пристрої окремо. У випадку веб-програмного забезпечення, ці функції можуть бути більш централізовані та легше реалізовані.

Для того, щоб зробити найбільш обґрунтований вибір програмного забезпечення, необхідно враховувати технічні характеристики, такі як швидкість та продуктивність, а також інші аспекти, наприклад, доступність на різних платформах та мобільних пристроях,

можливості розширення та модифікації функцій та інтеграцію з іншими програмними продуктами. Нативне програмне забезпечення може бути більш продуктивним за рахунок того, що воно взаємодіє з операційною системою безпосередньо, але менш масштабованим, тоді як веб-програмне забезпечення може бути більш масштабованим, але менш продуктивним. Крім того, веб-програмне забезпечення може бути розроблене для будь-якої платформи та може бути доступним через браузер, що робить його більш гнучким у використанні та забезпечує більшу доступність.

Слід враховувати, що розробка та підтримка нативного програмного забезпечення може бути дорожчою, оскільки вона вимагає спеціальних знань та досвіду у розробці програмного забезпечення для конкретної платформи. У той же час, розробка веб-програмного забезпечення може бути менш витратною, оскільки вона може бути розроблена з використанням відкритих стандартів та бібліотек. Витрати на підтримку програмного забезпечення можуть бути значними в майбутньому. При розробці нативного програмного забезпечення, оновлення та підтримка можуть вимагати багато ресурсів, оскільки доводиться забезпечувати сумісність з різними версіями операційних систем та платформ [5]. З іншого боку, розробка веб-програмного забезпечення може забезпечувати більш простий процес оновлення та підтримки, оскільки можна змінювати функції та оновлювати програмне забезпечення на сервері, а не на кожному пристрої користувача. Таким чином, при виборі між нативним та веб-програмним забезпеченням слід враховувати не лише вартість розробки, але й витрати на майбутню підтримку та оновлення.

Важливим фактором є зручність використання програмного забезпечення. Нативне програмне забезпечення може бути більш зручним у використанні, оскільки воно розроблене спеціально для конкретної платформи та може використовувати всі її можливості. У той же час, веб-програмне забезпечення може бути більш універсальним та зручним у використанні на різних платформах, таких як комп’ютери, планшети та мобільні пристрої.

Окрім цього, треба враховувати технічні можливості та обмеження кожного типу програмного забезпечення. Наприклад, нативне програмне забезпечення може бути більш потужним у виконанні складних операцій, таких як обробка великої кількості даних або виконання графічних ресурсів з високою якістю.

Останнім чинником, який слід враховувати, є можливість масштабування програмного забезпечення. Веб-програмне забезпечення може бути більш масштабованим, оскільки воно може працювати на різних серверах та використовувати хмарні технології. Це може дозволити обміну даними зберігати та обробляти більшу кількість інформації та забезпечити доступ користувачам з різних регіонів світу, масштабування нативного програмного забезпечення може бути складним завданням, оскільки воно зазвичай розробляється для конкретної платформи та обмежується обчислювальними ресурсами на локальному комп’ютері. Однак, в нативному програмному забезпеченні може бути більша продуктивність, ніж у веб-програмному забезпеченні, оскільки воно може працювати безпосередньо з обчислювальними ресурсами на локальному комп’ютері. Також, нативне програмне забезпечення може бути більш надійним та захищеним від зломів, оскільки воно працює локально та не піддається впливу мережі.

Веб-програмне забезпечення може бути оновлене централізовано на серверному рівні, що дозволяє вирішувати потенційні проблеми безпеки та недоліків в програмному забезпеченні усіх користувачів одночасно. Це зменшує ризик виникнення проблем безпеки, які можуть виникнути через неправильну конфігурацію або застарілість програмного забезпечення.

У разі нативного програмного забезпечення кожен користувач мусить вручну встановлювати оновлення і налаштовувати на своєму пристрої. Це може створити проблеми з безпекою, якщо користувачі забувають оновлювати своє програмне забезпечення або не знають, як правильно налаштувати його для забезпечення максимального рівня безпеки.

Крім того, веб-програмне забезпечення зазвичай працює на багатьох платформах, в той час як нативне програмне забезпечення зазвичай працює лише на одній платформі. Це може бути корисним для користувачів, які працюють на різних операційних системах або мають доступ до різних типів пристроїв.

Однак, веб-програмне забезпечення може бути повільніше в порівнянні з нативним програмним забезпеченням, оскільки воно працює в середовищі браузера та може бути обмежене можливостями браузера та мережевої пропускної здатності. Крім того, веб-програмне забезпечення зазвичай залежить від доступності мережі, що може бути проблемою в разі обміну захищеними даними в умовах обмеженого чи відсутнього Інтернет-з'єднання.

Обидва види програмного забезпечення мають свої переваги та недоліки, і вибір між ними залежить від конкретних потреб та вимог користувачів. Нативне програмне забезпечення може бути кращим вибором для використання в обмеженому колі користувачів, які працюють на певній платформі, тоді як веб-програмне забезпечення може бути більш підходящим для більш широкого кола користувачів, які працюють на різних пристроях та платформах.

Висновки. Зважаючи на розглянуті аспекти, можна зробити наступні висновки щодо порівняння нативного та веб-програмного забезпечення для обміну захищеними даними.

Нативне програмне забезпечення зазвичай забезпечує вищу швидкість та продуктивність, а також має більшу можливість керування обладнанням, яке використовується для збереження даних.

Веб-програмне забезпечення, незважаючи на те, що воно може бути менш продуктивним, надає перевагу у доступності та масштабованості. Крім того, веб-програмне забезпечення не вимагає установки на локальному комп'ютері, що полегшує процес розгортання та встановлення.

На підставі цього, якщо користувачі мають вимоги до продуктивності та мають достатньо ресурсів для установки та керування нативним програмним забезпеченням, вони можуть зробити вибір на користь нативного програмного забезпечення. У разі, якщо користувачі шукають зручність, доступність та масштабованість, вони можуть звернутися до веб-програмного забезпечення.

З іншого боку, веб-програмне забезпечення зазвичай має менші витрати на розробку та підтримку, може бути доступним з будь-якого пристрою та операційної системи та має високу міру масштабованості. Однак, веб-програмне забезпечення може бути менш безпечним та менш ефективним у роботі з великими об'ємами даних.

Отже, при виборі між нативним та веб-програмним забезпеченням для обміну захищеними даними, необхідно зважати на різні фактори, такі як безпека, вартість, доступність, ефективність та масштабованість.

Список використаних джерел

1. Герасимик І. Розробка мобільних додатків і їх види. – 2023. [Електронний ресурс]. – Режим доступу: – http://apeps.kpi.ua/rozrobka-mobilnykh-dodatkiv-i-yii-vidy
2. Kinsta – 2023. [Електронний ресурс]. – Режим доступу: https://kinsta.com/knowledgebase/tls-vs-ssl/
3. HHS.gov. Health Information Privacy. – 2023. [Електронний ресурс]. – Режим доступу: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
4. WebFX. Native App vs. Mobile Web App: A Quick Comparison. – 2023. [Електронний ресурс]. – Режим доступу: https://www.webfx.com/blog/web-design/native-app-vs-mobile-web-app-comparison/
5. Science soft. Software Maintenance Costs. – 2023. [Електронний ресурс]. – Режим доступу: https://www.scnsoft.com/services/software-development/software-support-and-maintenance/costs

Робота виконана під науковим керівництвом канд. екон. наук, старшого викладача
ФРАНЧУК Т. М.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ КРИВИХ ГІЛБЕРТА В КОМП'ЮТЕРНИХ СИСТЕМАХ

ЮРЧЕНКО С., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

Ця стаття досліджує багато застосувань кривої Гільберта в комп'ютерних системах, включаючи стиснення даних, криптографію та обробку зображень. Ми розглянемо унікальні властивості кривої Гільберта та те, як її можна використовувати для оптимізації алгоритмів комп'ютерів та апаратної реалізації. Дослідивши останні дослідження та розвиток у цій галузі, ми можемо отримати уявлення про майбутнє комп'ютерної технології та про те, яку роль може відігравати крива Гільберта у її формуванні.

This article explores the many applications of the Hilbert curve in computer systems, including data compression, cryptography, and image processing. We will examine the unique properties of the Hilbert curve and how it can be utilized to optimize computer algorithms and hardware implementations. By examining the latest research and developments in this field, we can gain insights into the future of computer technology and the role that the Hilbert curve may play in shaping it.

Актуальність. Криві Гілберта – це універсальний математичний об'єкт, який залишається важливим у комп'ютерних технологіях протягом понад століття. Однією з причин цього є їх здатність ефективно представляти просторову інформацію. Криві Гілберта є кривими, які заповнюють простір, що означає, що вони можуть заповнити двовимірний простір за допомогою однієї неперервної лінії. Ця властивість робить їх корисними для різних застосувань, які пов'язані з представленням або аналізом просторових даних, таких як комп'ютерна графіка, географічні інформаційні системи та обробка зображень.

Іншою причиною актуальності кривих Гілберта є їх самоподібність та фрактальна природа. Самоподібність означає, що крива виглядає схоже на різних масштабах, а фрактальна природа означає, що крива має нецілі розміри. Ці властивості зробили криві Гілберта цікавою областю досліджень у таких галузях, як теорія хаосу, динамічні системи та складні системи. У комп'ютерних технологіях ці властивості використовуються в застосуваннях, таких як стиснення даних та криптографія.

Метою статті є дослідження особливостей використання кривих Гілберта в комп'ютерних системах та продемонструвати їхню важливість і актуальність у різноманітних застосуваннях.

Об'єктом дослідження є особливості використання кривих Гілберта в комп'ютерних системах

Предмет дослідження – криві Гілберта.

Аналіз попередніх досліджень. Дослідженню кривих Гілберта в комп'ютерних системах присвячені праці закордонних науковців: Девіда Гілберта, Бенуа Мандельброта, Мартіна Гарднера, Джона Халтона, Кена Перлін та ін.

Виклад основного матеріалу. Використання кривих Гілберта (рис.1) можна поділити на такі сегменти:

1. Представлення та аналіз даних:
- Географічні інформаційні системи
- Просторові бази даних
- Застосування в машинному навчанні
2. Обробка зображень та графіка:
- Створення фрактальних ландшафтів та місцевостей

- Сегментація зображень
- Алгоритми виявлення контуру

3. Стиснення даних та криптографія:

- Стиснення даних
- Генерація ключів шифрування
- Безпечні канали зв’язку:

4. Апаратна реалізація

- Просторове індексування
- Пошук даних

5. Квантові обчислення та ДНК-обчислення:

- Представлення та маніпулювання квантовими станами
- Кодування та декодування інформації

Розглянемо кожен з них більш детально.

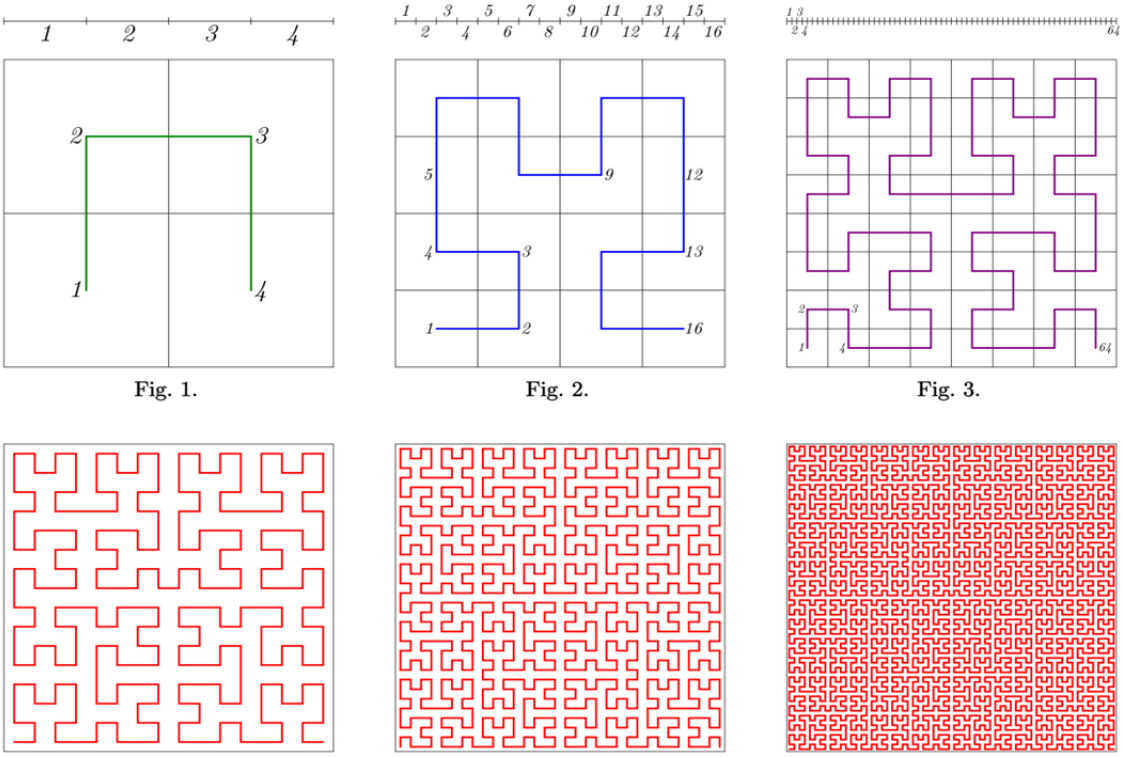

Fig. 1. Fig. 2. Fig. 3.

Рис. 1. Криві Гілберта

Криві Гілберта використовуються в геоінформаційних системах для ефективного зберігання та отримання просторових даних. Вони забезпечують криву, яка заповнює простір, зберігаючи локальність, що означає, що близькі точки в двовимірному просторі відображаються н близьких точках на кривій. Ця властивість дозволяє швидкий та ефективний запит та отримання даних, а також просторове індексування та кластеризацію.

Подібно до ГІС. Криві Гілберта можуть бути використані в просторових базах даних для представлення та запиту просторових даних. Вони дозволяють ефективну індексацію та запит даних, а також швидкий пошук найближчіх сусідів. Криві Гілберта також можуть використовуватися для зберігання та запиту багатовимірних даних, що робить їх корисними в застосуваннях машинного навчання.

В застосуваннях машинного навчання криві Гілберта використовуються для представлення та аналізу даних. Вони можуть бути використані для зменшення розмірності багатовимірних даних, що спрощує їх аналіз та обробку. Криві Гілберта також надають

спосіб відображення даних в одновимірному просторі, що може бути корисним у кластеризаційних та класифікаційних алгоритмах.

Щодо обробки зображень та графіки, криві Гілберта використовуються для генераціх фрактальних ландшафтів та місцевостей. Для цього квадрат рекурсивно ділять на чотири менших квадрати, а отримані вершини відображають на кривій Гілберта. Цей процес повторюється, щоб створити більш складні особливості місцевості, що в результаті дає візуально привабливий та натуральних вигляд місцевості.

Також криві Гілберта використовують в алгоритмах сегментації зображень для розділення зображення на регіони на основі їх візуальних властивостей. Для цього зображення пікселі відображають на кривій Гілберта, яка зберігає просторову локальність пікселів. Це дозволяє ефективно кластеризувати пікселі на основі їх положення на кривій.

Криві Гілберта також використовуються в алгоритмах виявлення граней, які ідентифікують межі між регіонами на зображенні. Для цього зображення пікселі відображають на кривій Гілберта, після чого обчислюється локальний градієнт по кривій. Це надає змогу ідентифікувати переходи між різними регіонами на зображенні.

Не менш важливим є використання кривих Гілберта в стисненні даних та криптографії. Криві Гілберта можуть бути використані в методах стиснення даних для зменшення їх розміру. Один зі способів полягає у застосуванні кривої Гілберта до зображення, що переставляє значення пікселів у більш ефективний спосіб. Ця перестановка дозволяє краще стиснення через можливість використання просторової згуртованості зображення, що означає, що близькі пікселі мають тенденцію мати подібні значення. За допомогою перестановки значень пікселів з використанням кривої Гілберта, алгоритм стиснення може ефективніше групувати подібні значення, що призводить до меншого розміру файлу.

Криві Гілберта можуть бути використані для генерації безпечних ключів шифрування. Процес полягає у використанні кривої Гілберта для створення двовимірної мапи точок. Криптографічна функція застосовується до кожної точки для генерації послідовності випадкових чисел. Ці випадкові числа можуть бути використані для генерації ключа шифрування, який може бути використаний для шифрування даних. Використання крифої Гілберта для генерації ключів шифрування забезпечує більш високий рівень безпеки, оскільки послідовність точок на кривій є детермінованою і не може бути легко вгадана зловмисниками.

Криві Гілберта також можуть бути використані для створення безпечних комунікаційних каналів між двома сторонами. Один з методів полягає в використанні кривої Гілберта для генерації послідовності випадкових чисел, які потім використовуються для шифрування повідомлень, відправлених між сторонами. Цей процес створює безпечний комунікаційний канал, оскільки ключі шифрування є унікальними і не можуть бути легко вгадані зловмисником. Крім того, оскільки крива Гілберта є детермінованою, обидві сторони можуть згенерувати однакову послідовність точок і використовувати їх для дешифрування повідомлень, що забезпечує надійність комунікації.

Криві Гілберта також можуть бути використані для швидкого отримання інформації з великих наборів даних. Індексуючи дані за допомогою кривої Гілберта, отримання даних можна виконувати за допомогою простого пошукового алгоритму, який слідує кривій. Цей алгоритм відомий як Hilbert R-tree та є варіантом традиційного алгоритму індексування R-tree.

Використовуючи Hilbert R-tree, відновлення даних може бути виконано ефективніше, навіть для великих наборів даних.

У квантовій механіці квантовий стан представляється як комплексний вектор в багатовимірному просторі, відомому як гілбертів простір. Гілбертові криві можуть використовуватись для представлення та маніпулювання квантовими станами більш ефективним способом.

Одне з застосувань гілбертових кривих у квантовій механіці – це симуляція квантових систем. Квантові симуляції вимагають обчислення еволюції квантової системи з часом. Використовуючи криву Гілберта для представлення квантового стану, симуляцію можна

виконувати більш ефективно, оскільки крива може зафіксувати просторову узгодженість квантового стану.

У комп'ютерній науці з ДНК, молекули ДНК використовуються для представлення та обробки інформації, а виклик полягаж в тому, зоб ефективно шукати та маніпулювати великими наборами послідовностей ДНК. Криві Гілберта можуть бути використані для відображення послідовностей ДНК в двовимірному просторі, де просторове розташування послідовностей відображає їх подібність або відмінність. Це може бути корисно для кластеризації та класифікації великих наборів послідовностей ДНК та для проектування ефективних алгоритмів для вирішення проблем в обчисленні ДНК, таких як задачі оптимізації.

Крім того, криві Гілберта можуть бути використані для зберігання та відновлення даних в обчисленні ДНК. Відображаючи послідовності ДНК на криву Гілберта, просторова близкість послідовностей може бути збережена, що може бути корисно для ефективного відновлення послідовностей, які подібні або пов'язані між собою. Використання кривих Гілберта в обчисленні ДНК є перспективним підходом для вирішення деяких проблем, пов'язаних з маніпулюванням та обробкою великих послідовностей ДНК.

Апаратні реалізації кривої Гільберта є областю активних досліджень та розробок. Ці реалізації можуть мати різні форми, такі як цифрові кола, програмовані логічні матриці (FPGA) та спеціалізовані інтегральні мікросхеми (ASIC). Однією з основних мотивацій для реалізації кривої Гільберта у апаратурі є прискорення обчислень, що потребують просторової індексації або пошуку даних.

Один з підходів до апаратної реалізації полягає у використанні рекурсивного алгоритму для побудови кривої Гільберта, який може бути реалізований за допомогою цифрових кол. Цей підхід передбачає поділ двовимірного простору на чотири квадранти та рекурсивне застосування алгоритму до кожного квадранту для побудови кривої. Такі реалізації можуть бути використані для застосувань, таких як обробка сигналів, стиснення зображень та кодування відео, та демонструють значні прискорення порівняно з програмними реалізаціями.

Іншим підходом до апаратної реалізації є використання програмованих логічних матриць (FPGAs), які можуть бути програмовані для реалізації спеціалізованих апаратних архітектур. Цей підхід використовується для застосувань, таких як розпізнавання образів, кластеризація даних та відновлення даних, де крива Гільберта використовується для відображення даних в двовимірному просторі. Реалізації на базі FPGA мають перевагу гнучкості, що дозволяє перепрограмовувати апаратне забезпечення для різних застосувань та наборів даних.

Реалізації на базі ASIC кривої Гільберта пропонують потенційні переваги в забезпеченні ще більшої швидкодії, оскільки вони проектуються спеціально для конкретного застосування. Ці реалізації включають проектування спеціалізованих схем, які оптимізовані для алгоритму кривої Гільберта, і можуть надавати значні переваги в термінах швидкості та споживання енергії. Однак реалізації на базі ASIC зазвичай є більш дорогими та витратними на розробку, ніж інші апаратні реалізації, і тому використовуються в основному для застосувань, де важлива швидкість, таких як обробка сигналів в реальному часі або високопродуктивні обчислення.

Для застосувань, які вимагають просторового індексування чи пошуку даних, апаратні реалізації кривої Гільберта надають значних переваг. Вибір конкретної реалізації залежить від таких факторів, як конкретне застосування, бажаний рівень продуктивності та доступні ресурси. Оскільки технології апаратних засобів продовжують розвиватися, ймовірно, що використання кривих Гільберта в апаратних реалізаціях стане ще більш поширеним та ефективним.

Використання кривих Гільберта в комп'ютерних технологіях відкрило нові можливості для досліджень та розробок. Є кілька областей, де можна розширити використання кривих Гільберта, що приведе до нових застосувань та технологій. Одна з областей

майбутніх досліджень – використання кривих Гільберта в квантових обчисленнях. При поширенні квантових комп'ютерів стає ще важливішим ефективне просторове індексування та відновлення даних. Криві Гільберта можуть потенційно використовуватися для оптимізації цих операцій в квантових обчисленнях, що призведе до швидших та більш ефективних обчислень.

Інша область майбутніх досліджень – використання кривих Гільберта в машинному навчанні та штучному інтелекті. Алгоритми машинного навчання часто включають маніпулювання та аналіз великих обсягів даних, а просторове індексування та відновлення даних є важливими компонентами багатьох з цих алгоритмів. Криві Гільберта можуть потенційно використовуватися для оптимізації цих операцій, що призведе до більш ефективних та ефективних алгоритмів машинного навчання.

Крім того, використання кривих Гільберта в апаратному забезпеченні є галуззю, де потрібні додаткові дослідження. Розробка нових апаратних технологій, таких як нейроморфне обчислення, може потенційно отримати користь від використання кривих Гільберта в архітектурі апаратного забезпечення. Крім того, розробка нових алгоритмів та технік для конструювання та маніпулювання кривими Гільберта в апаратному забезпеченні може призвести до ще більш ефективних реалізацій.

В цілому використання кривих Гільберта в комп'ютерних технологіях є перспективним напрямком досліджень та розробки з багатьма потенційними застосуваннями та можливостями для майбутнього зростання. При тому, як дослідники продовжують досліджувати можливості кривих Гільберта та розробляти нові алгоритми та техніки для їх використання, ми можемо очікувати ще більш інноваційних та ефективних застосувань цієї технології у майбутньому.

Висновки. Крива Гільберта – захоплюючий та багатофункціональний інструмент, який знайшов широке застосування в комп'ютерних технологіях. Від стиснення даних та криптографії до обробки зображень та ДНК-обчислень, унікальні властивості кривої Гільберта зробили її цінним інструментом для представлення та обробки даних у різних галузях.

Особливо обіцяними результатами використання кривих Гільберта є застосування їх у просторовому індексуванні та отриманні даних, обробці зображень та комп'ютерній графіці, а також в ДНК-обчисленнях. Крім того, дослідження продовжують вивчати потенційні застосування кривих Гільберта у квантових обчисленнях та представленні квантових станів.

Оскільки комп'ютерні технології продовжують еволюціонувати та розширюватися, корисність та багатогранність кривих Гільберта, ймовірно, продовжуватимуть зростати. Тому вивчення та застосування кривих Гільберта залишатимуться важливою областю дослідження та розвитку ще протягом багатьох років.

Список використаних джерел

1. «Hilbert Curve Indexing for High-Dimensional Similarity Search»: https://www.researchgate.net/publication/220838655_Hilbert_Curve_Indexing_for_High-Dimensional_Similarity_Search
2. «Hilbert curves and their applications in computer graphics»: https://www.sciencedirect.com/science/article/pii/S0097849306000892
3. «Hilbert Curves: A Tutorial»: http://www.dgp.toronto.edu/people/mooncake/papers/hilbert-tutorial.pdf
4. «Hilbert Curves in Data Science»: https://www.linkedin.com/pulse/hilbert-curves-data-science-sudheendra-chilappagari
5. «Spatial Indexing Using the Hilbert Space-Filling Curve»: https://www.sciencedirect.com/science/article/pii/S0306437906000416

Робота виконана під науковим керівництвом канд. екон. наук, доцента
ТИЩЕНКА Д. О.

ПРИНЦИПИ ТА ОСОБЛИВОСТІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ЮЩЕНКО О., 2м курс ФІТ ДТЕУ,
спеціальність «Інженерія програмного забезпечення»

У статті розглянуто передумови виникнення, основні принципи та особливості мікросервісної архітектури програмного забезпечення, її переваги, недоліки та область використання, порівняння із монолітної архітектурою.

This article considers reasons of appearance and development, main principles and traits of microservice software architecture, it's advantages, disadvantages and usage sphere, comparison with monolithic architecture.

Актуальність. Інформаційні технології та програмне забезпечення відіграють дуже важливу роль у житті суспільства. Банківська справа, торгівля, медицина, освіта та безліч інших сфер діяльності людини – все це спирається на спеціалізоване програмне забезпечення, що призначене для полегшення та підвищення ефективності праці. Умовами правильного та безперебійного функціонування такого програмного забезпечення є якість та «чистота» програмного коду, що в першу чергу залежить від проаналізованих вимог та правильно підібраної архітектури додатку.

Метою статті є дослідження особливостей мікросервісної архітектури, її розвитку, переваги та недоліки, область використання.

Об'єктом дослідження є архітектура програмного забезпечення.

Предмет дослідження – мікросервісна архітектура та її застосування при розробці програмного забезпечення.

Виклад основного матеріалу. Архітектура програмного забезпечення – це набір правил та вимог до внутрішньої структури програми та того, як її компоненти та модулі взаємодіють між собою. Основною задачею архітектури програмного забезпечення є аналіз вимог до системи та вироблення стратегії, що позволить правильно відобразити та реалізувати предметну область задачі через код. Правильно розроблена архітектура ПЗ допомагає вирішувати такі проблеми як: надійність, відмовостійкість, розширюваність, супроводжуваність, безпека, доступність тощо.

Розвиток архітектури програмного забезпечення тісно пов'язаний із розвитком інформаційних технологій у цілому. Перше спеціалізоване програмне забезпечення не було дуже вибагливим та складним, проте разом із розвитком та ускладненням задач, що потрібно було вирішувати, почали зазнавати розвитку і мови програмування, парадигми та шаблони проектування.

Першим популярним видом архітектури, що дав передумови та причини до виникнення мікросервісної архітектури, прийнято вважити **монолітну** (monolithic) архітектуру. Головною особливістю цього виду архітектури було те, що весь додаток побудований за даним принципом був неподільним та самодостатнім. Монолітний додаток містив у собі абсолютно всю логіку, що потрібна для його роботи, він не залежив від інших додатків та розповсюджувався у вигляді одної єдиної програми.

Такий підхід містить набагато більше недоліків, ніж переваг. Головною перевагою даної архітектури є легкість її реалізації. Монолітний додаток – це те, що зазвичай виходить неявно, природньо, оскільки для реалізації такої архітектури не потрібно витрачати багато зусиль – додаток розростається, новий код просто додається до існуючого, функціонал та область використання змішуються.

Вартість впровадження та легкість розгортання теж є сильними сторонами монолітної архітектури, оскільки для запуску однієї програми на сервері не потрібна велика кількість

налаштувань та інфраструктури. Вартість інфраструктури що потрібна для розгортання такого додатку буде мінімальною у порівнянні з іншими видами архітектур. Наявність лише одного виконуваного файлу також полегшує процеси тестування та налагодження (debug).

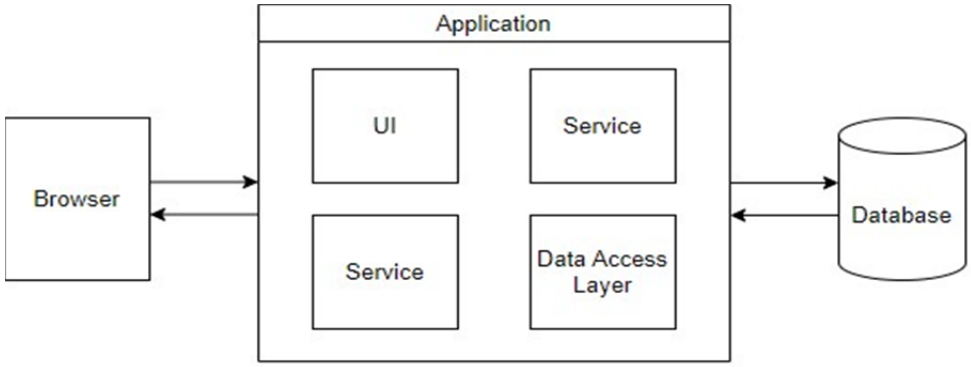

Рис. 1. Приклад монолітної архітектури додатку

Головним недоліком монолітної архітектури є її непідтримуваність протягом довгого часу. Оскільки монолітний додаток є неподільним, це означає що він розростається дуже швидко разом із впровадженням нового функціоналу. Вихідний код додатку стає незрозумілим та заплутаним, впровадження нових ідей стає тільки важче, все частіше стає у нагоді «рефакторинг», що тільки збільшує вартість підтримки та розробки нового програмного коду.

Іншим важливим недоліком монолітної архітектури є її ненадійність та немасштабованість. Через неподільність монолітного додатку, неможливо масштабувати тільки ту його частину, яка зазнає найбільшого навантаження, можливо масштабувати лише весь додаток уцілому, шляхом запуску додаткових екземплярів додатку (горизонтальне масштабування). З цієї самої причини, необроблена помилка під час виконання монолітної програми ставить під загрозу весь додаток одразу – одна така помилка може «покласти» весь додаток. Таким чином, можна виділити наступні передумови виникнення мікросервісної архітектури:

- *Ускладнення вимог та постійний розвиток*. Додавати новий функціонал потрібно все частіше, це повинно бути легко та відносно недорого. Програмний код повинен бути підтримуваним.
- *Доступність*. Із постійним розвитком інформаційних технологій все більше людей мають доступ до комп'ютерів, смартфонів та інтернету, отже програми повинні витримувати велике навантаження.
- *Відмовостійкість*. Чим більше система, тим складніше стають зв'язки між її частинами, збільшується можливість помилок. Система не повинна припиняти свою роботу, навіть у випадку коли якась її частина відмовила.
- *Розповсюдження таких практик як Agile та DevOps*.

Мікросервісна архітектура – це підхід до розробки програмного забезпечення як сукупності окремих незалежних сервісів, що взаємодіють між собою. Кожний такий сервіс відповідає за конкретну функціональність додатку, взаємодіє з іншими сервісами за допомогою HTTP запитів або подій, та може бути розгорнутий та масштабований окремо від інших. Сервіс – це структурна одиниця мікросервісної архітектури, саме це є її головною особливістю.

Принципи та переваги мікросервісної архітектури

1. *Сервіси є малими та сфокусованими на конкретній задачі*. У кожного сервісу у системі є своє конкретне призначення, що відображає окремий аспект предметної області додатку. Сервіс повинен містити у собі лише той функціонал та логіку, які безпосередньо стосується тієї задачі, що він призначений вирішувати.

За допомогою ділення додатку на множину сервісів можна уникнути заплутаності та змішування програмного коду, адже відтепер вихідний код буде логічно розділений у залежності від бізнес-вимог. Додавання нового функціоналу також стає легше, оскільки зміні зазнається не увесь додаток одразу, а лише його мала частина.

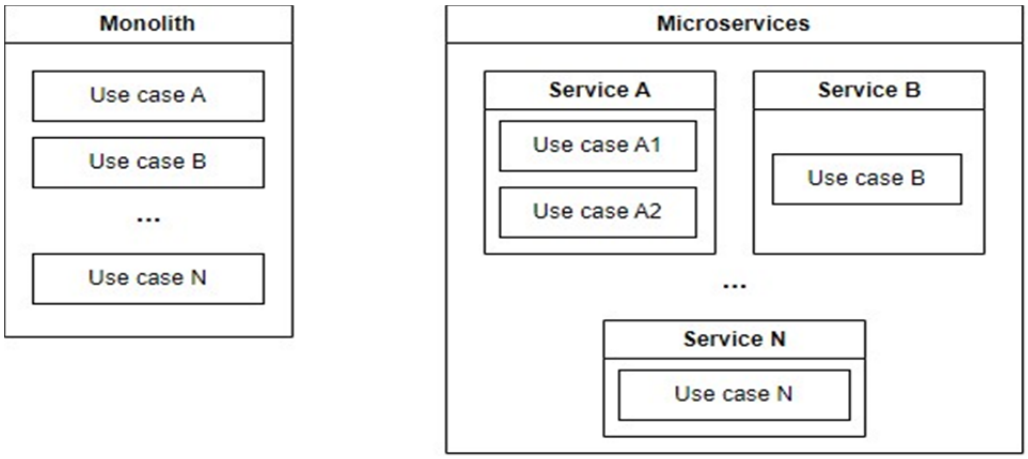

Рис. 2. Порівняння монолітної та мікросервісної архітектури

2. *Автономність та ізольованість*. Кожний сервіс є окремою незалежною сутністю, що запускається як окремий процес операційної системи або додаток у хмарі. Сервіси не знають про внутрішню реалізацію один одного та взаємодіють тільки за допомого API (Application Programming Interface), що вони надають. Зміни, що відбуваються в одному сервісі, не повинні вплинути на роботу інших сервісів та клієнтів, за умови що існуючий програмний інтерфейс сервісу залишився без змін. Така «розв'язаність» (decoupling) сприяє зменшенню залежностей частин додатку одна від одної, надає можливість змінювати реалізацію сервісів без впливу на всю систему та краще перевикористовувати існуючий функціонал.

Іншою вагомою перевагою є зручність розгортання сервісів. Оновлення декількох рядків коду у монолітному додатку вимагає повного перерозгортання всієї системи, що завжди є повільним, сповненим ризику, процесом. Це також означає, що випуск релізів та оновлень стається рідше, адже малі зміни вигідніше групувати та випускати разом. Внесення та випуск змін у мікросервіси є набагато легшим та безпечнішим процесом, оскільки зміні зазнається лише один конкретний сервіс.

3. *Організованість навколо бізнес-вимог*. Відповідно до закону Конвея (Melvin Conway, 1968), «будь-яка організація що проєктує систему, створить дизайн зі структурою, яка буде копією структури комунікації в цій організації». Це означає, що структура великих систем часто залежить від структури та організації зв'язків у середині самої компанії, що буде використовувати цю систему. Якщо у компанії є суворе розподілення на команди спеціалістів із front-end, back-end, спеціалістів із баз даних тощо, то кінцева система скоріш за все буде мати точно таке саме розподілення по модулям. Проблема закладається у тому, що при впроваджені нових ідей та функціоналу може виникнути питання, який саме підрозділ має впроваджувати ці зміни. Через суворе розподілення спеціалістів на команди, ці зміни часто погано обговорюються або впроваджуються не в ту частину системи, куди вони належать, що у свою чергу призводить до змішування та укладення програмного коду.

Мікросервісна архітектура допомагає вирішити цю проблему за допомогою організованості навколо вимог, не навколо ролей. Команда, що працює над конкретним сервісом, може мати спеціалістів з різних областей, що у свою чергу допомагає правильно оцінити та реалізувати зміни. Також, така команда не отримає завдання на впровадження змін, що її не стосуються, адже за такою структурою можна легко зрозуміти, яка команда відповідальна за конкретну частину додатку.

4. *Незалежність від технологій*. На відміну від монолітної архітектури, де обраний стек технологій майже не змінюється протягом всього часу, мікросервісна архітектура цілковито заохочує використання різних технологій для різних сервісів. Кожний сервіс у праві користуватися саме такими інструментами, які найкраще підходять для реалізації поставленої задачі.

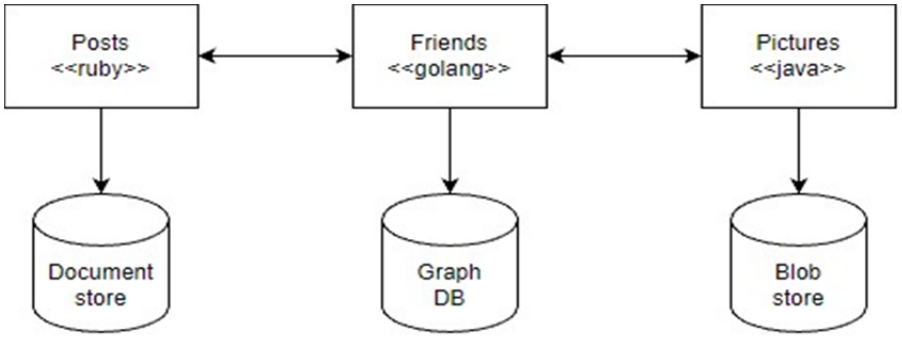

Рис. 3. Приклад сервісів, створених із використанням різних технологій

5. *Пристосованість до збоїв*. Впровадження мікросервісної архітектури дозволяє значним чином підвищити відмовостійкість додатку, адже при виході із ладу одного із сервісів, додаток не завершується аварійно, а лише втрачає частину відповідного функціоналу. Альтернативно, окремі сервіси можна вимикати усвідомлено, наприклад у випадку витоку даних або ключів доступу.

6. *Автоматизація інфраструктури*. Мікросервісну архітектуру дуже зручно використовувати у купі із такими практиками як DevOps та Agile, головними принципами яких є гнучкість, швидкість розробки та розгортання, випуску продукту на ринок. Для кожного сервісу додатку зручно створювати процеси автоматизації (CI/CD pipeline), що є відповідальними за збирання коду, забезпечення необхідної інфраструктури та розгортання. Наявність таких процесів значно підвищує ефективність розробки та зменшує час, який розробники витрачають на непов'язані із розробкою активності. Процес виписку нових версій продукту також стає значно простішим та менш ризикованим, оскільки можливість людської помилки стає менше: все що необхідно зробити – це запустити необхідний процес.

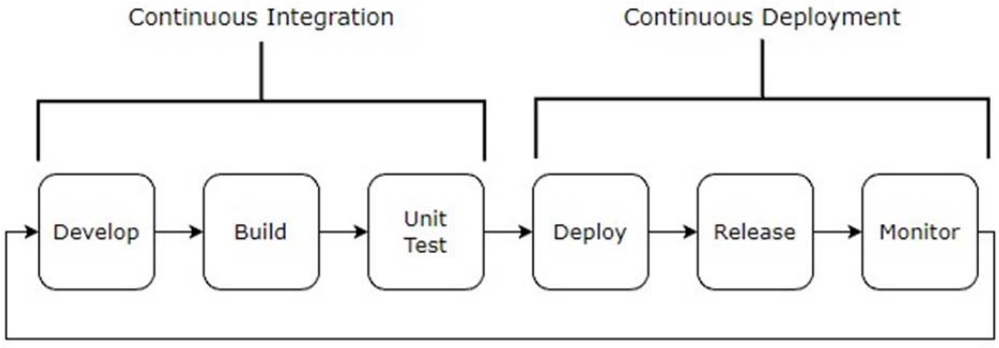

Рис. 4. Приклад автоматизації процесу збирання та розгортання коду

Через свої переваги, мікросервісна архітектура отримала визнання розробників та широке поширення. Першою великою компанією, що почала активно застосовувати та сприяти розвитку мікросервісної архітектури прийнято вважати Netflix. Netflix почали міграцію від монолітної архітектури у 2009 році, через швидке зростання кількості активних користувачів та інформації, що потрібно зберігати та оброблювати, і на кінець 2011 року перенесли весь свій функціонал на мікросервіси у хмарі. Безліч інших великих компаній,

таких як Amazon, Microsoft, Uber, Spotify, Twitter, також використовують мікросервіси у своїх додатках.

Сьогодні мікросервісну архітектуру можна використовувати при розробці широкого спектру застосунків, особливо якщо вони мають підтримувати високе навантаження або оброблювати велику кількість інформації у режимі реального часу. Інтернет магазини, соціальні мережі, фінансові додатки, IoT та багато іншого – все це може ефективно використовувати переваги мікросервісної архітектури. Проте, незважаючи на велику кількість переваг, мікросервіси не позбавлені недоліків.

Недоліки мікросервісної архітектури.

1. *Вартість інфраструктури*. Через те, що кожний сервіс хоститься окремо від інших, кількість необхідної інфраструктури, а отже її кінцева вартість зростає. Різні сервіси можуть потребувати різні операційні системи, різні бази даних, різні обчислювальні потужності тощо. Якщо додаток розрахований на велику кількість користувачів, окремої уваги потребує налаштування мережі та розподілення трафіку, що теж потребує додаткових ресурсів та витрат. Також, через те, що кожний сервіс користується власним набором технологій, кількість різноманітних ліцензій зростає.

2. Важкість тестування. З одної сторони, мікросервіси полегшують тестування, оскільки перевірці зазнається окремий сервіс за раз; тестування окремого, конкретного функціоналу стає легше, оскільки за нього відповідає один сервіс. З іншої сторони, у випадку коли необхідно протестувати велику частину функціоналу, що може потребувати взаємодії великої кількості сервісів, важкість тестування значно зростає. У випадку, коли такий сценарій не проходить тестування, може бути абсолютно неочевидно, який саме із сервісів викликав помилку, тому кожний з них зазнає повторного тестування. Тестування взаємодії сервісів один з одним також не є простою задачею, адже в залежності від виду комунікації між сервісами, команді тестувальників можуть знадобитися різні навички та інструменти.

3. Вибагливість до експертизи. Через велику кількість технологій, що можуть використовуватись під час розробки додатку, що використовує мікросервісну архітектуру, нерідко одному розробнику потрібно мати навички із декількох технологій або інструментів. DevOps інженери, що відповідають за розгортання інфраструктури, налаштування мережі, автоматизацію процесів, також мають володіти широким спектром навичок, щоб можна було виконати всі поставлені вимоги. Все це тільки підвищує складність пошуку необхідних спеціалістів та витрати на них.

У статті було розглянуто поняття архітектури програмного забезпечення, мікросервісної архітектури, умови її виникнення та порівняння із монолітною архітектурою, головні принципи, переваги, недоліки та область застосування мікросервісної архітектури.

Список використаних джерел

1. Fowler M. Microservices: a definition of this new architectural term [Електронний ресурс] / Martin Fowler // martinfowler.com. – 2014. – Режим доступу до ресурсу: https://martinfowler.com/articles/microservices.html.
2. Richards M. Fundamentals of Software Architecture / M. Richards, F. Neal., 2020. – 265 с. – (O'Reilly Media, Inc).
3. Newman S. Building Microservices / Sam Newman., 2015. – 265 с. – (O'Reilly Media, Inc.).
4. Evans E. Domain-Driven Design: Tackling Complexity in the Heart of Software / Eric Evans., 2003. – 560 с. – (Addison Wesley).

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

КОМУНІКАТИВНИЙ ОНЛАЙН-СЕРВІС СОЦІАЛЬНОЇ СПІЛЬНОТИ

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

У статті розглянуті питання створення комунікативного онлайн-сервісу соціальної спільноти з фокусом на мову програмування C#. Обґрунтовується важливість таких сервісів в сучасному інтернет-ландшафті та описуються наявні програмні платформи, які можуть бути використані для розробки таких сервісів. Також досліджується перевага використання архітектури ASP.NET для програмування на мові C# та те, як вона може бути використана для створення комунікативного онлайн-сервісу соціальної спільноти. Загалом, стаття відзначається важливість технічних вимог та умов, які необхідні для успішної розробки онлайн-сервісу соціальної спільноти та може служити корисним джерелом інформації для розробників, які планують зайнятися таким проектом.

This article provides an overview of the creation of a communicative online social community service, with a focus on programming language C#. The article examines the importance of such services in today's internet landscape and discusses the existing software platforms that can be used to develop such services. The article also explores the benefits of using the Model-View-Controller (MVC) architecture for C# programming and how it can be utilized in creating a communicative online social community service. Overall, the article highlights the technical requirements and considerations involved in developing a successful online social community service and can serve as a helpful resource for developers looking to embark on such a project.

Актуальність. Комунікативні онлайн-сервіси соціальної спільноти стають все більш популярними серед користувачів Інтернету. Завдяки таким сервісам, люди можуть швидко та зручно зв'язуватися один з одним, обмінюватися інформацією, ділитися своїми думками та враженнями. Проте, для ефективного використання комунікативних сервісів соціальної спільноти необхідні відповідні програмні рішення, які дозволяють забезпечити якість та безпеку обміну даними. У цій статті розглядаються різні програмні платформи, що використовуються для створення комунікативних онлайн-сервісів соціальної спільноти, а також описано процес їх створення з використанням мови програмування C#. Враховуючи широке використання таких сервісів в сучасному світі, стаття є актуальною для розробників, які прагнуть створити високоякісні та безпечні комунікативні онлайн-сервіси соціальної спільноти.

Метою даної статті є дослідження та аналіз програмних рішень, які можна використовувати при створенні комунікативного онлайн-сервісу соціальної спільноти з використанням мови програмування C#. В статті розглянуто архітектурний шаблон MVC, веб-фреймворк ASP.NET, бази даних та їх використання у проекті, а також інші програмні засоби, які дозволяють створити функціональний та ефективний онлайн-сервіс соціальної спільноти. Результатом цієї роботи буде огляд та порівняння програмних платформ з метою вибору оптимального рішення для розробки даного проекту.

Об'єктом дослідження є комунікативний онлайн-сервіс соціальної спільноти, який розробляється з використанням мови програмування C#.

Предметом дослідження є програмні рішення та технології, що використовуються для розробки комунікативного онлайн-сервісу соціальної спільноти з використанням мови програмування C#.

Аналіз попередніх досліджень. З огляду на актуальність теми комунікативних онлайн-сервісів соціальних спільнот, було проведено аналіз попередніх досліджень у цьому напрямку, зокрема статтю «Розробка соціальної мережі для бібліотек на основі.NET

технологій» автора Н.С. Гайдука, де він детально описує процес розробки, зокрема, серед переваг використання.NET технологій автор зазначає високу продуктивність, безпеку та простоту розробки завдяки вбудованим функціям мови програмування C#. Крім того, використання платформи ASP.NET дозволяє розробляти веб-додатки з високим рівнем масштабованості та забезпечувати швидкий доступ до баз даних. Однак, автор також зазначає недоліки використання.NET технологій, зокрема, високу вартість ліцензування та обмеження у підтримці інших мов програмування. Також можуть виникнути проблеми зі сумісністю між різними версіями платформи.NET.

З комунікативними онлайн-сервісами соціальної спільноти ми можемо легко знаходити старих друзів та знайомитися з новими, обмінюватися фотографіями, відеороликами та іншими медіа-контентами, створювати групи та спільноти за інтересами, та навіть здійснювати бізнес-взаємодію. Такі сервіси стали не тільки місцем для розваги та дозвілля, але й невід'ємною частиною нашого соціального життя, де ми ділимося важливими подіями, поглядами, та сприймаємо світ через призму інших користувачів.

Водночас у статті «Програмна реалізація агрегатора соціальних мереж» за авторством М.Яковенка, А.Охрименка, С.Кузніченко аналізується наступне: серед переваг автори зазначають використання платформи ASP.NET для розробки соціальних мереж, де є можливість швидкої розробки веб-додатків завдяки вбудованому фреймворку MVC та багатому інструментарію.NET. Крім того, з використанням Entity Framework, розробники можуть легко працювати з базою даних та забезпечити її ефективну роботу. Однак, на думку авторів статті, недоліком використання платформи ASP.NET є потреба у великій кількості коду для розробки веб-додатків, а також необхідність високої кваліфікації розробника для ефективної роботи з цією платформою. Крім того, у статті було зазначено, що платформа має високі вимоги до обладнання сервера, що може стати проблемою для невеликих компаній з обмеженим бюджетом.

Виклад основного матеріалу. Комунікативний онлайн-сервіс соціальної спільноти є інтернет-платформою, яка надає користувачам можливість спілкуватися між собою, обмінюватися інформацією, фотографіями та відео з іншими учасниками спільноти. Онлайн-сервіси соціальних мереж вже давно займають головне місце серед інтернет-платформ. Їх популярність зростає з кожним роком, і це створює значні можливості для бізнесу та комерційних проектів.

C# є об'єктно-орієнтованою мовою програмування, розробленою компанією Microsoft. Вона має багатий функціонал та підтримує сучасні технології програмування, такі як:

- Мультипоточність – можливість програми виконувати кілька потоків одночасно для збільшення швидкості та продуктивності виконання завдань. Це означає, що програма може виконувати декілька операцій одночасно, якщо є відповідні потоки. В C# мультипоточність можна реалізувати за допомогою потоків (Thread) або задач (Task), які дають можливість розподілити завдання між потоками та виконувати їх паралельно.
- Асинхронність – дозволяє програмі виконувати багато задач одночасно, зменшуючи час очікування на виконання окремих завдань та підвищуючи продуктивність програми. Зокрема, в C# для роботи з асинхронним кодом використовують ключові слова async та await, які дозволяють забезпечувати продовження виконання програми в той час, коли відбувається очікування відповіді від зовнішнього сервісу, бази даних чи іншої операції, що може зайняти значний час. Асинхронність є важливим аспектом розробки комунікативних онлайн-сервісів соціальної спільноти, оскільки такі сервіси повинні забезпечувати швидкий та ефективний доступ до великих обсягів даних та надавати користувачам зручний та комфортний досвід взаємодії.
- Паралельність – це здатність виконувати декілька завдань одночасно на різних процесорах або ядрах в рамках одного процесу. Він дозволяє розподіляти обчислювальні завдання на декілька потоків, що прискорює їх виконання та забезпечує більш ефективне використання ресурсів обчислювальної системи. У C# для досягнення паралельної роботи використовуються бібліотеки Parallel і PLINQ. Бібліотека Parallel містить класи, що

дозволяють виконувати паралельні операції з масивами даних, циклами, послідовностями та іншими операціями. PLINQ (Parallel LINQ) є розширенням LINQ і дозволяє розподіляти обчислення на кілька ядер процесора.

Також, C# має велику кількість вбудованих засобів та бібліотек, що дозволяє забезпечувати високу продуктивність та надійність програмних рішень, проте ця мова програмування є компільованою мовою програмування, що дозволяє виявляти помилки на етапі компіляції та зменшує ймовірність виникнення помилок в рантаймі. Присутність підтримки об'єктно-орієнтованої парадигми програмування, що дозволяє забезпечити високий рівень модульності та розширюваності проекту.

Оскільки комунікативний онлайн-сервіс соціальної спільноти часто має велику кількість користувачів та обробляє великі обсяги даних, важливо використовувати мову програмування, яка забезпечує ефективну роботу з великими обсягами даних та швидкий відгук на запити користувачів. C# має вбудовані засоби для роботи з базами даних та збереження даних у форматах XML та JSON. Крім того, C# має підтримку платформи.NET, що дозволяє розробникам використовувати багато функцій та бібліотек, що надаються цією платформою, а також, дана мова програмування має велику спільноту розробників, що дозволяє отримувати підтримку та поради від інших спеціалістів.

Однією з ключових складових будь-якого онлайн-сервісу соціальної спільноти є можливість взаємодії між користувачами. Спілкування може відбуватися в різних форматах, таких як приватні повідомлення, коментарі та відгуки на пости, фото або відео. Для створення такого сервісу важливо розробити ефективний механізм взаємодії між користувачами. Крім взаємодії, сервіс соціальної спільноти повинен мати такі складові, як профілі користувачів, створення та редагування постів, можливість підписуватися на сторінки інших користувачів, рейтинги та відгуки. Для реалізації цих функцій необхідно використовувати відповідні програмні рішення, що дозволяють забезпечувати комфортну та безпечну взаємодію між користувачами. Одним з таких рішень є мова програмування C#, яка дозволяє створювати потужні та ефективні онлайн-сервіси з використанням.NET-фреймворку.

Один з найважливіших аспектів при створенні онлайн-сервісу соціальної спільноти – це його безпека. Користувачі повинні бути захищені від шахрайства, крадіжки даних та інших загроз. Тому важливо використовувати захист даних, двофакторну автентифікацію та інші заходи безпеки. Для цього в C# є вбудовані засоби та бібліотеки, які дозволяють забезпечити надійний рівень захисту:

- Криптографічні бібліотеки – дозволяють шифрувати та розшифровувати дані, створювати та перевіряти цифрові підписи, а також генерувати випадкові числа, які можуть бути використані для створення паролів та ключів шифрування.
- Бібліотека безпеки – містить класи для роботи з безпекою, такі як безпека мережі, безпека додатку, керування даними, керування доступом, керування ідентифікацією та автентифікацією, а також класи для роботи з різними типами захисту, такими як кодування та шифрування.
- Механізми автентифікації та авторизації – дозволяють перевіряти, чи має користувач достатньо прав для виконання певної дії, та перевіряти його ідентифікацію, щоб забезпечити безпеку даних та системи в цілому.
- Засоби обробки винятків – дозволяють програмістам обробляти помилки та виключення, що виникають у процесі роботи програми, та запобігати їх негативному впливу на безпеку даних та системи.

Для розробки онлайн-сервісу соціальної спільноти на мові програмування C# можна використовувати такі платформи, як ASP.NET, MVC та інші. Ці платформи дозволяють створювати потужні та складні сервіси з використанням різних технологій та підходів:

ASP.NET – це фреймворк, який використовується для створення веб-додатків та сервісів. Дана платформа є високопродуктивною для розробки, вона дозволяє швидко створювати динамічні веб-сторінки та веб-додатки з використанням мов програмування C#, Visual Basic і інших мов, що підтримують.NET Framework. Фреймворк має безліч переваг

для розробки комунікативного онлайн-сервісу соціальної спільноти, починаючи з переваг забезпечення безпеки, також має багато функціональних можливостей, таких як вбудована підтримка для аутентифікації та авторизації, підтримку HTTPS, яка забезпечує шифрування даних між сервером та клієнтом. Щодо продуктивності, ASP.NET забезпечує велику швидкість роботи веб-додатків, завдяки розширеному кешуванню даних та оптимізації коду. Крім того, на цій платформі можна використовувати мультипоточність, асинхронність та паралельність для оптимізації продуктивності. Щодо масштабованості, ASP.NET має вбудовану підтримку для віддаленого керування, що дозволяє легко масштабувати веб-додатки до великої кількості користувачів та маштабувати їх згідно з потребами.

ASP.NET є однією з найбільш популярних платформ для розробки веб-додатків на мові C#. Розробниками цієї платформи є компанія Microsoft, яка постійно підтримує та оновлює цей інструмент. За даними сайту W3Techs, який вивчає статистику використання технологій у веб-розробці, на початку 2021 року платформа ASP.NET використовувалась більше ніж на 18% веб-сайтів у всьому світі. Також, згідно з даними порталу StackOverflow, ASP.NET є однією з найпопулярніших платформ для розробки веб-додатків.

Одним із переваг ASP.NET є можливість використання багатофункціональних бібліотек та фреймворків, що значно спрощує розробку веб-додатків. Наприклад, платформа містить вбудовану бібліотеку Entity Framework для роботи з базами даних, а також фреймворки для створення користувацьких інтерфейсів, такі як Angular та React.

Окрім того, платформа ASP.NET надійна та безпечна, оскільки містить вбудовані засоби для захисту від різних видів атак, таких як внедрення SQL-запитів, перетин сайтів та інші.

MVC – це архітектурний шаблон, який дозволяє розділити додаток на компоненти, що забезпечує більш просту та ефективну розробку. Даний шаблон можна використовувати в C# для створення веб-додатків та сервісів, що дозволяє розробникам більш ефективно керувати кодом та забезпечити його більшу повторюваність та легкість супроводу. MVC став популярним в програмному забезпеченні, особливо в розробці веб-додатків, завдяки своїй здатності до розширення, тестування та підтримки. Він дозволяє розробникам зосередитися на різних аспектах додатку та забезпечити кращу підтримку його функцій.

MVC затребуваний серед розробників та має велику кількість прикладів використання у веб-додатках, таких як ASP.NET, Ruby on Rails, Django та інших. За даними статистики веб-сайту BuiltWith.com, майже 8% веб-сайтів використовують фреймворки на основі MVC, з найбільш популярними з них є ASP.NET. Особливою перевагою використання MVC є його здатність до розширення та підтримки, що дозволяє забезпечити кращу підтримку функцій додатку та зменшити ризики при розробці нових функцій. Крім того, MVC забезпечує більш високу продуктивність, так як він дозволяє розробникам зосередитися на різних аспектах додатку та забезпечити їх оптимізацію.

Для розробки також можна використовувати інші програмні засоби, такі як:

- Apache Cassandra – розподілена база даних, яка дозволяє зберігати великі обсяги даних зі швидкістю та масштабованістю, що є важливим для сервісу соціальної мережі.
- Elasticsearch – пошукова система, яка дозволяє швидко і ефективно знаходити та індексувати великі обсяги даних, що допомагає поліпшити швидкість пошуку та аналізу даних у соціальній мережі.
- Redis – розподілена база даних, яка дозволяє зберігати дані в оперативній пам’яті, що забезпечує високу швидкість доступу до даних та можливість кешування даних для поліпшення продуктивності сервісу.
- RabbitMQ – програмний брокер повідомлень, який дозволяє передавати повідомлення між різними компонентами сервісу, що забезпечує більш ефективну та масштабовану комунікацію в сервісі соціальної мережі.
- Amazon Web Services або Google Cloud Platform – хмарні платформи, які дозволяють розгортати та масштабувати сервіс соціальної мережі, забезпечуючи високу доступність та швидкість роботи.

Ці програмні засоби можуть бути використані для покращення функціональності та продуктивності комунікативного онлайн-сервісу соціальної спільноти.

Користувацький інтерфейс є важливою частиною будь-якого програмного забезпечення, оскільки саме через нього користувачі взаємодіють з програмою. Розробка користувацького інтерфейсу може бути виконана з використанням різноманітних інструментів, таких як Windows Presentation Foundation (WPF), що є частиною платформи.NET.WPF надає розширені можливості для розробки графічного інтерфейсу та дозволяє використовувати різні елементи управління, такі як кнопки, тексти, зображення та інші. Також існують сторонні бібліотеки, наприклад, Xamarin.Forms, які дозволяють створювати мультиплатформові мобільні додатки з користувацьким інтерфейсом.

REST (Representational State Transfer) – архітектурний стиль для побудови додатків, що працюють у мережевому середовищі, в основі якого лежить принцип передачі даних за запитом-відповіддю. REST API – це інтерфейс, що забезпечує доступ до ресурсів в мережевому середовищі за допомогою HTTP-протоколу, а також простоту та ефективність комунікації між різними додатками в Інтернеті, зокрема, між клієнтськими та серверними додатками. Для передачі даних REST API використовує HTTP-методи, такі як GET, POST, PUT, DELETE, що дозволяє взаємодіяти з ресурсами, що зберігаються на сервері.

У своїй роботі програмісти використовують цей інтерфейс для створення додатків, що працюють в мережевому середовищі, забезпечуючи їх користувачам зручний та швидкий доступ до необхідної інформації, також він дозволяє використовувати різноманітні мови програмування та платформи, що робить його універсальним інструментом для створення додатків різного рівня складності.

База даних – це один з найважливіших компонентів будь-якого онлайн-сервісу соціальної спільноти, оскільки вона забезпечує зберігання та організацію великої кількості даних, що включають профілі користувачів, повідомлення, фотографії, відео, коментарі тощо.

Для розробки комунікативного онлайн-сервісу соціальної спільноти, можна використовувати різні типи баз даних:

- MySQL – система управління реляційними базами даних, яка дозволяє зберігати, організовувати та керувати великими обсягами даних.
- NoSQL – це підхід до управління даними, що відрізняється від традиційних реляційних баз даних. У системах NoSQL дані зберігаються у вигляді документів, графів, ключ-значення або колонок, залежно від обраної моделі даних.
- Microsoft SQL Server (MS SQL Server або просто SQL Server) – це система управління базами даних, розроблена компанією Microsoft. Вона використовує мову запитів Transact-SQL (T-SQL) для взаємодії з базою даних. MS SQL Server має багато функціональних можливостей, таких як підтримка транзакцій, реплікація даних, аналітика та багато іншого.
- MongoDB – це документо-орієнтована база даних, яка зберігає дані у вигляді документів у форматі BSON (Binary JSON). Вона розроблена з орієнтацією на обробку великих обсягів даних та високі швидкості операцій з ними. MongoDB підтримує гнучкий формат даних, дозволяючи зберігати дані без встановленої схеми та змінювати її в процесі роботи з базою даних.

При проектуванні бази даних для комунікативного онлайн-сервісу потрібно враховувати такі фактори, як швидкість доступу до даних, масштабованість та безпеку. Наприклад, для забезпечення швидкого доступу до даних, можна використовувати кешування даних на рівні додатку або бази даних. Для забезпечення безпеки даних, можна використовувати різні методи шифрування даних та захисту від несанкціонованого доступу.

Також варто враховувати те, що онлайн-сервіс соціальної спільноти має бути доступним для користувачів з різних країн та мов і має підтримувати міжнародну локалізацію. Це означає, що інтерфейс користувача та контент на сайті повинні бути перекладені на мови різних країн. Для забезпечення міжнародної локалізації слід використовувати

спеціальні засоби, такі як міжнародні фреймворки локалізації, які дозволяють перекладати контент на різні мови та налаштовувати вигляд інтерфейсу користувача в залежності від мови.

Крім того, з метою забезпечення міжнародної доступності та швидкості роботи сайту, можна використовувати розподілені системи зберігання даних та міжнародні CDN (Content Delivery Network), що дозволяють ефективно розподіляти контент по всьому світу та зменшувати час завантаження сторінок сайту для користувачів з різних країн.

Застосування бази даних дозволяє зберігати значну кількість даних про користувачів та їх взаємодії, що дозволяє аналізувати ці дані та отримувати корисну інформацію щодо популярності сервісу, поведінки користувачів та інших важливих аспектів. База даних є необхідним компонентом будь-якого сервісу соціальної спільноти та важливою складовою успішної розробки імітатора соціальної спільноти.

Портування (англ. porting) – це процес перенесення програмного забезпечення з одного середовища на інше. В залежності від того, на яких платформах планується акористовувати свій онлайн-сервіс соціальної спільноти, можна розглянути портування його на Android та iOS.

Для перенесення на мобільні платформи можна використовувати інструменти, такі як Xamarin або React Native:

Xamarin – це платформа для розробки мобільних додатків, яка дозволяє розробляти кросплатформні додатки для iOS, Android і Windows Phone за допомогою мови програмування C#. За даними різних досліджень, популярність Xamarin зростає з року в рік, оскільки вона дозволяє зменшити час розробки і підтримки додатків, забезпечуючи високу якість і функціональність. Згідно з даними Stack Overflow Developer Survey за 2021 рік, Xamarin займає друге місце серед платформ для розробки мобільних додатків після React Native. Також, за даними Microsoft, більше 2 мільйонів розробників використовують Xamarin для розробки мобільних додатків. Основні переваги використання Xamarin полягають у тому, що розробники можуть використовувати мову C# для створення кросплатформних додатків, що дозволяє зменшити час розробки і підтримки. Крім того, Xamarin надає можливість використовувати переваги нативного коду для кожної платформи, що забезпечує оптимальну продуктивність додатку. Також важливо зазначити, що Xamarin має велику спільноту розробників та підтримку від Microsoft, що забезпечує регулярне оновлення платформи та надання різноманітних інструментів для розробників.

React Native – це відкрите програмне забезпечення для розробки мобільних додатків, що базується на ReactJS – бібліотеці JavaScript для створення інтерфейсів користувача. За допомогою нього розробники можуть створювати мобільні додатки для iOS та Android з використанням одного коду на JavaScript. Дане програмне забезпечення набуло значної популярності серед розробників мобільних додатків. За даними State of JS 2020, React Native стала другою за популярністю бібліотекою для розробки мобільних додатків після Flutter. У 2020 році вона була використана понад 42% респондентів дослідження для створення мобільних додатків.

React Native є популярним вибором для розробки мобільних додатків у випадку, коли потрібна швидкість розробки та висока продуктивність додатків. Програма надає можливість швидко створювати прототипи мобільних додатків та дозволяє ефективно використовувати переносимий код між платформами. Більшість розробників знаходять в ній легким для вивчення та швидким у розробці. Однією з переваг React Native є підтримка гарячого перезавантаження, що дозволяє розробникам швидко бачити зміни, які вони роблять в коді, на мобільних пристроях без необхідності перезавантаження додатку.

Створення комунікативних онлайн-сервісів соціальної спільноти – це завдання, яке потребує високої кваліфікації розробників. Оскільки такі сервіси дозволяють взаємодіяти з користувачами в режимі реального часу та обмінюватися великим обсягом даних, тестування такого програмного забезпечення є невід’ємною складовою процесу його розробки.

Аналіз проекту є необхідним етапом розробки будь-якого програмного забезпечення, оскільки воно дозволяє виявити помилки та недоліки в роботі програми та виправити їх до випуску продукту в експлуатацію.

У разі комунікативних онлайн-сервісів соціальної спільноти, тестування включає проведення тестів на функціональність, відповідність стандартам безпеки, тестування навантаження та інших параметрів, що впливають на якість та ефективність роботи сервісу. Такі тести дозволяють виявити проблеми, що виникають під час використання сервісу реальними користувачами та виправити їх до випуску продукту в експлуатацію.

Кількість користувачів та обсяги даних, що обробляються комунікативними онлайн-сервісами соціальної спільноти, можуть бути величезними. Це ставить перед розробниками завдання забезпечити не тільки надійну роботу сервісу, але й забезпечити безпеку та захист приватності користувачів. На жаль, навіть найкращі комунікативні сервіси не є ідеальними, тому тестування стає невід'ємною складовою в процесі розробки таких сервісів.

Одним з основних видів тестування є функціональне тестування, яке включає у себе перевірку функцій та можливостей сервісу. Наприклад, тестування може включати перевірку можливості додавання друзів, обмін повідомленнями, відправку та отримання файлів тощо. Важливо перевірити, що всі ці функції працюють правильно та коректно взаємодіють з іншими функціями сервісу.

Окрім функціонального тестування, важливим є також тестування на масштаб. Це означає, що необхідно перевірити, як сервіс працює при великому навантаженні та великій кількості запитів одночасно. Тестування на масштаб може допомогти виявити проблеми з продуктивністю та оптимізувати роботу сервісу.

Також важливим є тестування безпеки. Комунікативні онлайн-сервіси соціальної спільноти містять велику кількість особистих даних користувачів, тому захист цих даних є надзвичайно важливим. Тестування безпеки може допомогти виявити проблеми з захистом даних, такі як уразливості в мережевих протоколах, управлінням ідентифікацією та авторизацією, та інші проблеми, пов'язані з безпекою. Важливо проводити тестування на різних етапах розробки сервісу, включаючи тестування на ранніх етапах, коли сервіс розробляється, а також після випуску на продакшн, коли користувачі починають активно використовувати сервіс.

Тестування програмного забезпечення також може допомогти виявити проблеми з функціональністю сервісу, такі як помилки в роботі функцій, неправильні дані, невірна поведінка та інші проблеми, які можуть призвести до негативного впливу на користувачів та їхній досвід використання сервісу.

Для забезпечення якості тестування ПЗ, необхідно використовувати різні види тестів, такі як модульні тести, інтеграційні тести, тести на прийняття та інші. Крім того, необхідно використовувати автоматизоване тестування, яке може забезпечити більшу швидкість та ефективність тестування, а також підвищити його точність та надійність.

У світі, де цифрові технології стали неодмінною складовою сучасного життя, комунікативні онлайн-сервіси соціальної спільноти відіграють ключову роль у спілкуванні, обміні інформацією та побудові зв'язків. Цей розділ підбиває короткі висновки стосовно комунікативних онлайн-сервісів соціальної спільноти.

Комунікативні онлайн-сервіси соціальної спільноти забезпечують учасникам можливість обміну ідеями, думками та враженнями без обмежень простору та часу. Це створює сприятливе середовище для віртуального спілкування, побудови особистих та професійних відносин, а також сприяє розширенню кругу спільноти.

Комунікативні онлайн-сервіси соціальної спільноти включають в себе багато функціональних можливостей, таких як чати, відеодзвінки, спільні новини, групові дискусії тощо. Це дозволяє користувачам обирати способи взаємодії, які найкраще відповідають їхнім потребам та вподобанням.

Незважаючи на всі переваги, комунікативні онлайн-сервіси соціальної спільноти також стикаються з викликами, пов'язаними зі збереженням приватності та безпекою даних

користувачів. Необхідно розробляти ефективні механізми захисту та забезпечення конфіденційності даних.

Висновки. У цій статті розглянута мова C#, яка є доцільною для розробки комунікативного онлайн-сервісу соціальної спільноти з великою кількістю користувачів та потребою у високій продуктивності, ефективності та модульності, крім того проаналізовані різні програмні платформи, що використовуються для створення комунікативних онлайн-сервісів. Також було вказано, що для ефективного використання необхідні відповідні програмні рішення, які дозволяють забезпечити якість та безпеку обміну даними. Важливо проводити тестування на різних етапах розробки сервісу, включаючи тестування безпеки, щоб запобігти можливим проблемам. Також були розглянуті різні типи баз даних, такі як реляційні та нереляційні, та їх використання для зберігання та обробки даних, що використовуються в комунікативних онлайн-сервісах.

Комунікативні онлайн-сервіси соціальної спільноти є потужним інструментом для побудови зв'язків, обміну інформацією та взаємодії у віртуальному просторі. Їхній успіх полягає у здатності надати різноманітні можливості взаємодії, зберігаючи при цьому захист і приватність користувачів. Незважаючи на виклики, з якими вони стикаються, ці сервіси впливають на спосіб, яким ми спілкуємося та співпрацюємо, розширюючи границі віртуальної соціальної спільноти.

В цілому, створення комунікативного онлайн-сервісу соціальної спільноти є складним процесом, який вимагає від розробників високої кваліфікації та уваги до деталей.

Список використаних джерел

1. Microsoft «Документація по ASP.NET» \\ Режим доступу: https://learn.microsoft.com/ru-ru/aspnet/core/?view=aspnetcore-7.0
2. Microsoft «Початок роботи з ASP.NET MVC 5 \\ Режим доступу: https://learn.microsoft.com/ru-ru/aspnet/mvc/overview/getting-started/introduction/getting-started
3. Ендрю Троелсен та Філіп Джепікс «Мова програмування C# 7 і платформи.NET і.NET Core»
4. Microsoft «Документація по C#» \\ Режим доступу: https://learn.microsoft.com/ru-ru/dotnet/csharp/
5. MySQL «MySQL Documentation» \\ Режим доступу: https://dev.mysql.com/doc/
6. Microsoft «Документація по Xamarin» \\ Режим доступу: https://learn.microsoft.com/ru-ru/xamarin/
7. Н.С. Гайдук «Розробка соціальної мережі для бібліотек на основі.NET технологій» \\ Режим доступу: https://elartu.tntu.edu.ua/handle/lib/30701
8. М.Яковенко, А.Охрименко, С.Кузніченко «Програмна реалізація агрегатора соціальних мереж» \\ Режим доступу: http://mdu.edu.ua/wp-content/uploads/gmit7-16.pdf
9. React Native «Introduction» \\ Режим доступу: https://reactnative.dev/docs/getting-started
10. «Керівництво по програмуванню для Xamarin Forms» \\ Режим доступу: https://metanit.com/sharp/xamarin/
11. «Welcome to Apache Cassandra's documentation!» \\ Режим доступу: https://cassandra.apache.org/doc/latest/
12. «Керівництво по Elasticsearch» \\ Режим доступу: https://coderlessons.com/tutorials/noveishie-tekhnologii/izuchite-uprugii-poisk/elasticsearch-kratkoe-rukovodstvo

Робота виконана під науковим керівництвом канд. техн. наук, доцента
РЗАЄВОЇ С. Л.

СПОСОБИ ПРОТИДІЇ ВПЛИВУ СПАМУ НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

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

У статті розглянуто поняття спаму та його види, оскільки різні види спаму вимагають різних підходів до їх боротьби. технічні, математичні та правові методи боротьби зі спамом. Описано принципи роботи кожного з цих методів, їх переваги та недоліки. Зазначено принципи та переваги застосування математичних методів боротьби зі спамом, зокрема, методів машинного навчання та статистичного аналізу. Висвітлено актуальність проблеми боротьби зі спамом, ризики, що він несе для інформаційно-комунікаційних систем, та постійно зростаюча складність боротьби з цією загрозою.

The article discusses the concept of spam and its types, as different types of spam require different approaches to combat them. It covers technical, mathematical, and legal methods for fighting spam. The principles of operation, advantages, and disadvantages of each of these methods are described. The article highlights the relevance of the problem of spam, the risks it poses to information and communication systems, and the constantly increasing complexity of combating this threat. The principles and advantages of using mathematical methods for combating spam, including machine learning and statistical analysis methods, are emphasized.

Актуальність. Всебічна інформатизація суспільства, збільшення обсягів створюваної, одержуваної і накопичуваної інформації ведуть до зростання актуальності питань, пов'язаних з поширенням спаму, його впливу на інформаційне середовище підприємств і фізичних осіб, ефективність їх діяльності; рівень інформаційної безпеки. Спам є серйозною загрозою для інформаційно-комунікаційних систем, оскільки він може призвести до перевантаження систем, зменшення продуктивності, витрат на зберігання даних та інших негативних наслідків. Крім того, спам може бути використаний зловмисниками для здійснення фішингових атак та інших видів кіберзлочинності.

У зв'язку з цим, розробка та вдосконалення методів боротьби зі спамом є одним з найважливіших завдань в галузі кібербезпеки. Компанії, що надають послуги електронної пошти та інші ІКС-провайдери, активно використовують спеціальні програми та алгоритми для виявлення та блокування спаму. Однак, зловмисники постійно розробляють нові способи обхіду захисту від спаму, що вимагає постійного вдосконалення методів боротьби з ним. Крім того, виникають нові види спаму, такі як соціальний спам, що використовується для поширення недостовірної інформації в соціальних мережах.

Актуальність способів протидії впливу спаму на інформаційно-комунікаційні системи полягає в тому, що спам є однією з найбільш поширених проблем в Інтернеті, яка може негативно вплинути на роботу інформаційно-комунікаційних систем, заважаючи користувачам отримувати та обробляти корисну інформацію. У зв'язку з цим, розробка та впровадження ефективних методів боротьби зі спамом є важливим завданням для підтримки безпеки та ефективності функціонування ІКС. Отже, актуальність способів протидії впливу спаму на ІКС буде залишатися високою в майбутньому, і провайдери інформаційно-комунікаційних систем та кібербезпеки мають постійно вдосконалювати свої методи боротьби зі спамом.

Метою статті є дослідження різних способів протидії впливу спаму на інформаційно-комунікаційні системи.

Об'єктом дослідження є процес боротьби зі спамом в інформаційно-комунікаційних системах, який включає в себе різноманітні технології та методи, спрямовані на захист

користувачів та інформаційно-комунікаційні системи від негативних наслідків, які можуть виникнути через спам.

Предмет дослідження − інформаційно-комунікаційні системи, які можуть бути піддані впливу спаму, а також технології та методи, які використовуються для захисту інформаційно-комунікаційних системах від спаму.

Аналіз попередніх досліджень. Тема протидії впливу спаму на інформаційно-комунікаційні системи є предметом досліджень багатьох українських та закордонних вчених. Зокрема, в Україні в цій галузі працюють науковці Національної академії наук України, Національного технічного університету України «Київський політехнічний інститут», Національного університету «Львівська політехніка» та інших вітчизняних університетів.

У світі науковими центрами, які досліджують протидію спаму на інформаційно-комунікаційні системи, є, зокрема, Інститут інформаційної безпеки в Університеті Флориди, Інститут комп'ютерних наук Массачусетського технологічного інституту, Лабораторія комп'ютерних наук корпорації Microsoft, Лабораторія з безпеки Інтернету у Вірджинському університеті та багато інших. Результати досліджень вказують на те, що застосування різноманітних технологій та методів захисту ІКС від спаму є ефективним. Наприклад, застосування фільтрів спаму здатне знизити кількість небажаних повідомлень до 99,9%. В той же час, існують нові технології штучного інтелекту, які забезпечують ще більш ефективний захист від спаму.

Отже, дослідження українських та закордонних вчених є важливим кроком у розробці нових технологій та методів протидії впливу спаму на ІКС, які забезпечують високу якість і безпеку роботи цих систем.

Виклад основного матеріалу. У сучасному світі, коли інформація стала найважливішим ресурсом, проблема спаму стала надзвичайно актуальною. Спам може мати шкідливий вплив на інформаційно-комунікаційні системи (ІКС) через займання мережевого простору, витрати ресурсів та загрозу для безпеки. Спам − це небажані повідомлення, які надсилаються без згоди отримувача, зазвичай з комерційною або шахрайською метою. Спам може завдати значних шкідливих наслідків для інформаційно-комунікаційних систем, включаючи перевантаження мережі, складність виявлення легітимних повідомлень та ризики відкриття вірусів або інших шкідливих програм [1]. Надходження спаму на поштові скриньки та інші комунікаційні канали може призвести до наступних наслідків:

1. Вірусні атаки: спамові повідомлення можуть містити віруси та інші шкідливі програми, що можуть пошкодити систему та зламати безпеку інформації. Віруси можуть поширюватися через електронні повідомлення та встановлюватися на комп'ютери користувачів, що відкриють спамове повідомлення.

2. Фішингові атаки: спамові повідомлення можуть містити фішингові ланки або приховані запити на введення особистих даних, таких як паролі або номери банківських карток. Фішингові атаки можуть використовуватися для викрадення особистої інформації користувачів та зламу їхніх акаунтів.

3. Соціальний інжиніринг: спамові повідомлення можуть містити запити на переказ грошей або інші шахрайські схеми, які можуть бути використані для шахрайства користувачів. Злочинці можуть використовувати соціальний інжиніринг, щоб переконати користувачів у необхідності здійснити переказ коштів або надати особисту інформацію.

4. Завантаження небезпечного контенту: спамові повідомлення можуть містити посилання на небезпечний контент, такий як порнографія або насильство. Клікнувши на посилання, користувач може завантажити шкідливий вміст на свій комп'ютер.

5. Перевантаження системи є ще однією серйозною загрозою, пов'язаною зі спамом. Частість спамових повідомлень може відправлятися великою кількістю користувачів одночасно, що може призвести до перевантаження інформаційної системи. Якщо спам-атака великої масштабності, то вона може спричинити перевантаження серверів, що може призвести до тимчасового або повного відключення веб-сайту або інших інформаційних систем.

Протидія впливу спаму на інформаційно-комунікаційні системи (ІКС) − це важлива задача, яка полягає в тому, щоб запобігти надходженню небажаних повідомлень на електронну пошту, соціальні мережі та інші інтернет-сервіси [1].

Основні методи протидії спаму на сьогоднішній день включають в себе:

- Встановлення антивірусного програмного забезпечення, яке може виявляти та блокувати спам-повідомлення, фішингові листи, віруси та інші загрози для безпеки користувачів. Також антивірусні програми можуть бути налаштовані на автоматичне видалення спаму зі скриньки електронної пошти.
- Встановлення спеціальних програм (антиспам-фільтри), які перевіряють вхідну пошту на наявність спаму та блокують його. Фільтри спаму − це програми, які автоматично відсікають небажані повідомлення на підставі певних критеріїв. Вони можуть бути настроєні на блокування спаму за ключовими словами, IP-адресами, доменними іменами та іншими параметрами. Фільтри спаму зазвичай використовуються в електронній пошті, але їх також можна застосувати до інших ІКС, таких як соціальні мережі та месенджери.
- Використання CAPTCHA. Це системи перевірки, що вимагають від користувача виконати певне завдання, щоб довести, що він є людиною, а не роботом. CAPTCHA може бути використана для захисту від автоматизованих спам-ботів, які розсилають великі обсяги спаму.
- Блокування IP-адрес використовуються для блокування повідомлень від спамерів з певних IP-адрес. Електронний поштовий сервер може перевіряти IP-адреси відправників та порівнювати їх з блеклістами, щоб блокувати повідомлення від відомих спамерів.
- Використання криптографічних методів для підтвердження відправника листа і перевірки на його автентичність.
- Системи автентифікації можуть бути використані для визначення того, що пошта, яка надходить до поштової скриньки користувача, є легітимною. Найпоширенішою системою автентифікації є SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting and Conformance). Ці системи дозволяють перевірити, що пошта була надіслана відправником, який має право відправляти листи від імені даного домену.
- Встановлення обмежень на кількість листів, які можна відправити з певної IP-адреси за певний час.
- Навчання користувачів правилам безпеки в Інтернеті. Користувачі повинні бути обізнані з тим, як розпізнавати спам, не відкривати невідомі повідомлення та не відповідати на них.
- Обмеження спаму: деякі веб-сайти та соціальні мережі використовують методи обмеження спаму, наприклад, обмеження частоти відправки повідомлень, обмеження кількості отримувачів тощо.
- Боротьба з ботнетами. Ботнети − мережа комп’ютерів, які контролюються зловмисниками, зазвичай з метою злочинної діяльності, такої як розсилання спаму, здійснення DDoS-атак, крадіжка конфіденційних даних та іншого шкідливого впливу на користувачів Інтернету. Один з найбільш ефективних методів − виявлення та відключення злочинних серверів, які контролюють ботнет. Це можна зробити шляхом спостереження за трафіком, що пересилається між злочинним сервером та інфікованими комп’ютерами, та ідентифікації вузлів мережі, які приймають та відправляють цей трафік. Після виявлення злочинного сервера, його можна відключити від Інтернету.

Протидія впливу спаму на інформаційно-комунікаційні системи включає в себе різні заходи, які повинні бути реалізовані на кількох рівнях: технічному, правовому та освітньому.

На технічному рівні протидія спаму може включати в себе такі заходи, як блокування IP-адрес, які відомі як джерело спаму, використання спеціальних програм для виявлення та блокування спаму, та обмеження обсягу відправлення листів на конкретний домен. Також можуть використовуватися методи евристичного аналізу, такі як аналіз заголовків та тексту повідомлення, для виявлення спаму та блокування його вхідного потоку (Рис. 1). Наприклад,

відповідні програми можуть розпізнавати та відфільтровувати спамові повідомлення, а також визначати IP-адреси, з яких вони надходять. Крім того, використання антивірусних програм та систем захисту може допомогти уникнути проблем з безпекою при отриманні спаму.

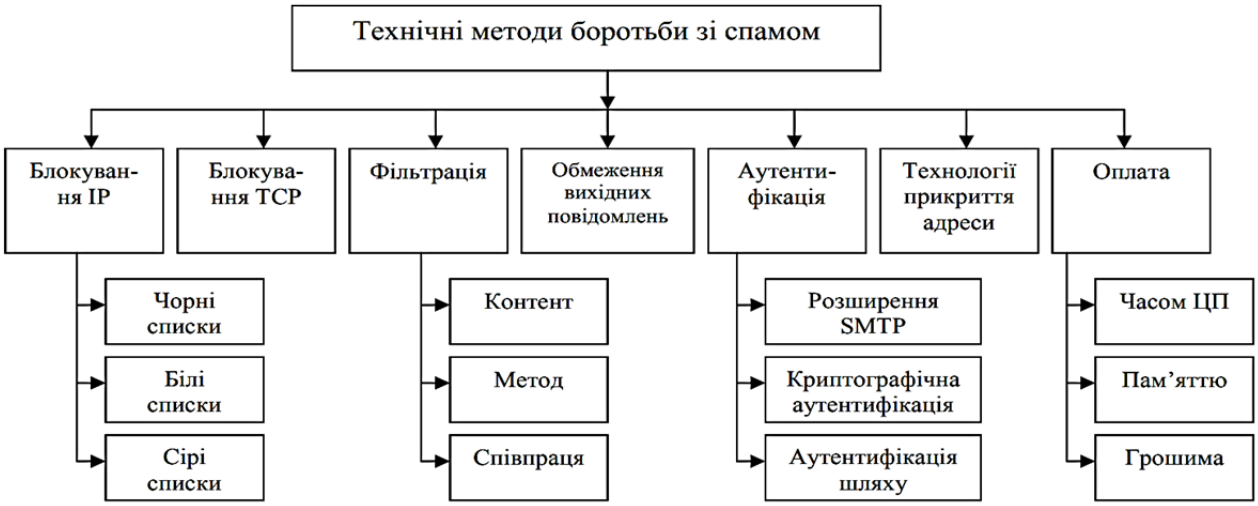

Рис. 1. Технічні методи боротьби із спамом

На правовому рівні протидія спаму може включати в себе прийняття законодавчих норм, що обмежують розсилку спаму. Наприклад, в Україні такі заходи регулюються Законом про електронні комунікації, який встановлює правила для відправників електронних повідомлень та визначає відповідальність за незаконну розсилку спаму.

Освітні заходи можуть допомогти в боротьбі зі спамом, допомагаючи користувачам розуміти, як розпізнавати спам та які дії потрібно вжити, щоб захистити себе від спаму. Освітні кампанії можуть проводитися на різних рівнях, включаючи школи, коледжі, університети та в мас-медіа.

Математичні технології боротьби зі спамом полягають у використанні різних математичних методів та алгоритмів для виявлення та фільтрації спамових повідомлень. Основні математичних технологій, які використовуються для боротьби зі спамом:

1. Байєсівський фільтр − математичний алгоритм, який використовується для визначення ймовірності того, що повідомлення є спамом або не спамом. Байєсівський фільтр працює на основі аналізу вмісту повідомлень та статистичних даних про спам та не спам. Алгоритм вивчає, які слова та фрази в спамових повідомленнях є найбільш ймовірними, а потім використовує цю інформацію для виявлення спаму. Байесівський фільтр спаму є досить ефективним методом, оскільки він може навчитися розпізнавати нові форми спаму [2, 3].

Байєсівський фільтр є одним з найпоширеніших методів боротьби зі спамом. Байєсівський фільтр − це математичний алгоритм, який може бути використаний для боротьби зі спамом. Він оснований на теорії ймовірності та використовується для класифікації повідомлень на спам і не-спам. Робота Байєсівського фільтра полягає у створенні моделі ймовірності, яка використовується для класифікації повідомлень. Напочатку роботи алгоритму необхідно побудувати базову модель, використовуючи набір тренувальних даних. Тренувальні дані містять набір повідомлень, які вже були класифіковані як спам або не-спам. Байєсівський фільтр аналізує ці повідомлення та знаходить зв'язок між словами, які з'являються в спамі та не-спамі. На основі цього алгоритм створює базову модель, яка допоможе в подальшій класифікації повідомлень. Кожне нове повідомлення відображується у вигляді набору слів та використовується для обчислення ймовірності, що це повідомлення є спамом. Для цього використовується формула Байєса, яка враховує ймовірності того, що слова з'являються в спамі та не-спамі.

Одним з головних переваг Байєсівського фільтра є те, що він вимагає досить мало обчислень, тому є досить швидким та ефективним. Крім того, Байєсівський фільтр може навчатися на нових данних та оновлювати свою статистику, що дозволяє йому бути ефективним і в актуальній ситуації.

2. Лінійний дискримінантний аналіз (ЛДА) – метод, який використовується для відокремлення спамових повідомлень від легітимних електронних листів на основі визначених характеристик. Алгоритм використовує статистичний аналіз для визначення, які змінні є найбільш корисними для відокремлення спаму від легітимних повідомлень [2, 4].

Лінійний дискримінантний аналіз (ЛДА) є методом машинного навчання, який може бути використаний для боротьби зі спамом. В контексті боротьби зі спамом, ЛДА може бути використаний для класифікації повідомлень на спам і не-спам на основі набору ознак, таких як слова, фрази, символи і т.д. ЛДА працює шляхом знаходження оптимальної границі розділення між спамом і не-спамом у просторі ознак. В результаті, ЛДА може дати високу точність при класифікації повідомлень на спам і не-спам, особливо якщо використовується комплексна система класифікації, що включає в себе багато ознак та алгоритмів. Одним з головних переваг ЛДА є те, що він працює швидко з великими наборами даних, а також він є легким у використанні та розумінні. Крім того, ЛДА може працювати з даними високої розмірності. Однак, ЛДА також має свої обмеження. Наприклад, він може бути менш ефективним у випадках, коли вхідні дані мають складну структуру або коли вони не можуть бути легко розділені границею. Загалом, ЛДА може бути ефективним методом для боротьби зі спамом, якщо він використовується в комплексі з іншими методами, такими як фільтри на основі правил, евристичні методи та інші.

3. Метод опорних векторів (SVM) − метод машинного навчання, який використовується для розпізнавання спамових повідомлень. Алгоритм використовується для виявлення лінійних та не лінійних залежностей між вхідними характеристиками повідомлень та їх класифікацією як спаму або легітимних повідомлень [2].

У контексті боротьби зі спамом, SVM може бути використаний для класифікації повідомлень на спам і не-спам на основі ряду ознак (features), таких як наявність певних слів, фраз, символів тощо. SVM навчається розпізнавати спамові повідомлення на основі прикладів, що містять як спам, так і не спам. В результаті навчання SVM будує математичну модель, яка може передбачити, чи є нове повідомлення спамом чи ні. SVM може вивчити границю прийняття рішень, яка дозволяє розділити вхідні дані на два класи: спам і не-спам. Ця границя може бути дуже ефективною, особливо якщо використовувати комплексну систему класифікації, яка включає в себе багато ознак та алгоритмів. Одним з найбільших переваг SVM є те, що він працює дуже швидко, навіть з великими наборами даних. Також, SVM є дуже ефективним для роботи з даними високої розмірності. Однак, SVM також має свої обмеження. Він може мати проблеми з використанням даних, які не можуть бути легко розділені границею, або які мають складну структуру. Крім того, SVM може потребувати попередньої підготовки даних, такої як видалення зайвої інформації або перетворення даних в інший формат.

Загалом, SVM може бути ефективним методом для боротьби зі спамом, якщо він використовується в комплексі з іншими методами, такими як фільтри на основі правил, евристичні методи та інші.

4. Співставлення хеш-сум − метод, який використовується для порівняння хеш-сум спамових повідомлень зі списком відомих спамових повідомлень. Хеш-сума − це математичне значення, яке використовується для ідентифікації повідомлення. Якщо хеш-сума спамового повідомлення співпадає з хеш-сумою зі списку відомих спамових повідомлень, то повідомлення відхиляється [2, 4].

Співставлення хеш-сум (або хешування) є одним з методів боротьби зі спамом. Цей метод полягає в тому, щоб створити унікальну цифрову підпис (хеш-суму) для кожного повідомлення і порівняти його з відомими хеш-сумами відомих спамових повідомлень. Хеш-сума − це невелика послідовність цифр, створена з текстового повідомлення за допомогою

функції хешування. Кожне повідомлення має свою власну унікальну хеш-суму, яка може бути використана для ідентифікації повідомлення. Якщо хеш-сума вхідного повідомлення співпадає з хеш-сумою, що відома як спам, то повідомлення вважається спамом і може бути відкинуте або помічене як спам. Цей метод може бути ефективним для боротьби з відомими типами спаму, але він може бути легко пропущений спамерами, які використовують нові методи або змінюють вміст повідомлень, щоб уникнути виявлення. Крім того, співставлення хеш-сум вимагає збереження бази даних відомих хеш-сум, що може бути дуже великим завданням при великій кількості спаму. Тому цей метод може бути дорогим у плані зберігання і обробки даних. У загальному, хеш-суми можуть бути використані як один з елементів комплексної системи боротьби зі спамом, яка включає в себе також інші методи, такі як фільтри на основі правил, машинне навчання, евристичні методи та інші [1].

5. Машинне навчання − метод, який використовується для розпізнавання спаму на основі аналізу великої кількості даних. За допомогою машинного навчання можна навчити комп'ютер розпізнавати спамові повідомлення на основі визначених характеристик, таких як адреса відправника, вміст повідомлення та інші параметри.

Інший підхід до машинного навчання для боротьби зі спамом – це використання навчальних алгоритмів класифікації, таких як метод опорних векторів (SVM) або дерева рішень. Ці алгоритми навчаються на великому наборі даних, які включають спамові та неспамові повідомлення, і використовують ці дані для класифікації нових повідомлень [1, 4].

У будь-якому випадку, машинне навчання є потужним інструментом для боротьби зі спамом. Однак, ефективність будь-якого методу машинного навчання залежить від якості вхідних даних та правильного налаштування алгоритмів.

6. Нейронні мережі є потужним інструментом для боротьби зі спамом, оскільки вони можуть навчатись на великій кількості даних і виявляти складні зв'язки між різними аспектами повідомлень [4].

Для цього використовуються різні типи нейронних мереж, такі як згорткові нейронні мережі, рекурентні нейронні мережі та мережі довготривалої пам'яті. Вони можуть використовуватись для розпізнавання спаму в текстових повідомленнях, зображеннях, аудіо та відео. Одним з найбільш ефективних методів використання нейронних мереж для боротьби зі спамом є глибоке навчання. Глибокі нейронні мережі, такі як рекурентні нейронні мережі (RNN) та згорткові нейронні мережі (CNN), можуть використовуватись для аналізу текстового повідомлення та визначення його категорії (спам або не спам). Наприклад, можна навчити рекурентну нейронну мережу на великому наборі даних, які містять текстові повідомлення, які вже були класифіковані як спам або не спам. Потім цю мережу можна застосувати до нових повідомлень, щоб визначити, чи вони є спамом чи ні. Іншим методом використання нейронних мереж для боротьби зі спамом є використання глибоких мереж для визначення аномалій в поведінці користувачів. Наприклад, можна використовувати глибокі нейронні мережі для аналізу великого обсягу даних, щоб виявити незвичайну активність на електронній пошті, таку як відправлення великої кількості повідомлень за короткий час. Згорткові нейронні мережі можуть бути використані для аналізу тексту повідомлень та виявлення ключових ознак, що вказують на його спамовий характер. Рекурентні нейронні мережі та мережі довготривалої пам'яті можуть використовуватись для аналізу поведінки користувачів та виявлення аномальної активності, що може вказувати на надсилання спаму [1, 3].

Однак, використання нейронних мереж для боротьби зі спамом також має свої виклики та обмеження. Наприклад, для успішного навчання нейронної мережі необхідно мати велику кількість даних, а також збалансований набір даних, що містить як спам, так і не-спам повідомлення. Також важливо враховувати, що спамери постійно розвивають свої методи, тому необхідно постійно оновлювати та покращувати систему захисту від спаму.

Більшість з існуючих програм для боротьби зі спамом фільтрують повідомлення, що приходять в поштову скриньку. Це зручно з двох причин. Поперше, за допомогою цих

програм можна не перекачувати з сервера непотрібні листи. По-друге, вони дозволяють організувати сортування решти кореспонденції.

Існує безліч програмних рішень для виявлення спаму, які використовують різні методи і технології [4]. Деякі з найпопулярніших програмних рішень для виявлення спаму включають:

1. SpamAssassin − це безкоштовний відкритий програмний продукт, який використовує різні методики, такі як Байєсівський фільтр, співставлення хеш-сум, евристики та інші, для виявлення спаму в електронних листах. SpamAssassin може бути інтегрований з поштовими серверами та клієнтами електронної пошти.

2. Barracuda Spam Firewall − це апаратний або програмний продукт, який використовує різні методики, включаючи Байєсівський фільтр, для виявлення спаму в пошті та інших мережевих протоколах. Він також використовує технології машинного навчання, такі як нейронні мережі, для покращення точності виявлення спаму.

3. Symantec Messaging Gateway − це програмне рішення, яке використовує різні методики, включаючи Байєсівський фільтр та метод опорних векторів, для виявлення спаму в електронній пошті та інших мережевих протоколах. Symantec Messaging Gateway також використовує технології машинного навчання для покращення точності виявлення спаму та зменшення кількості неправильно класифікованих повідомлень.

4. MailWasher − це програмний продукт для перегляду та управління електронною поштою, який використовує різні методики, такі як Байєсівський фільтр та евристики, для виявлення спаму. Він може бути інтегрований з більшістю поштових клієнтів та серверів.

Ці програмні рішення дозволяють знизити кількість спаму, який надходить на поштові

Висновки. Усі методи боротьби зі спамом, які були розглянуті, мають свої переваги та недоліки, тому їх застосування залежить від конкретних умов та потреб користувачів. Наприклад, технічні методи (фільтри) є досить ефективними, але можуть блокувати корисні повідомлення. Математичні методи дають можливість визначити ймовірність того, що повідомлення є спамом, але не дають абсолютної гарантії. Дослідження українських та закордонних вчених показують, що проблема спаму не є локальною, а має глобальний характер. Крім того, недостатня увага до проблеми може призвести до серйозних наслідків для користувачів ІКТ, таких як вірусні атаки, крадіжки особистих даних та інші. Отже, вирішення проблеми спаму потребує комплексного підходу, який включає в себе не тільки технічні та математичні методи, але й підвищення свідомості користувачів щодо безпеки в ІКТ, а також співпрацю провайдерів та державних органів у сфері боротьби зі спамом.

Список використаних джерел

1. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. An evaluation of naïve bayesian anti-spam filtering techniques // Utah State University [Електронний ресурс] // Режим доступу: http://digital.cs.usu.edu/~erbacher/publications/Bayes-Vikas2.pdf (останнє звернення 22.03.2023р.).
3. Bayesian poisoning // Wikipedia The Free Encyclopedia [Електронний ресурс] // Режим доступу: https://en.wikipedia.org/wiki/Bayesian_poisoning (останнє звернення 22.03.2023р.)
4. Єрьоменко М. О. Аналіз існуючих програмних рішень для виявлення спаму // Інформаційні технології: наука, техніка, технологія, освіта, здоров’я: тези доповідей XXVIII міжнародної науково-практичної конференції MicroCAD-2020. – Харків: НТУ «ХПІ» С. 118.

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

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 3

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
280-3Е-2023