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 121 «Інженерія програмного
забезпечення» та 125 «Кібербезпека
та захист інформації»

Частина 2

Київ 2025

УДК 004.056
П 78

Програмування та захист інформації [Електронний ресурс] : зб. П 78 наук. ст. студентів / відп. ред. Т. О. Жирова. – Київ : Держ. торг.-екон. ун-т, 2025. – Ч. 2. – 235 с.

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

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

УДК 004.056

Редакційна колегія: Т. О. Жирова (відп. ред.), канд. пед. наук, доц.; А. М. Десятко, PhD, доц.; О. А. Харченко, канд. техн. наук, доц.; О. С. Ігнатович, заступник голови РСС ФІТ з організаційних питань.

Відповідальна за випуск А. М. Десятко, PhD, доц.

Видається за рекомендацією вченої ради
факультету інформаційних технологій ДТЕУ
(протокол № 24 від 13.05.2025)

© Державний торговельно-економічний університет, 2025

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ЗМІСТ

ВСТУП..... 6

АРЕФ'ЄВ І. Є.
ЗАСТОСУВАННЯ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АТАК З НУЛЬОВИМ ДНЕМ У СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ..... 7

БАХЯН Д. А.
КОНСОЛІДАЦІЯ ПОВЕДІНКОВОЇ АНАЛІТИКИ ТА КЛАСИЧНИХ МЕТОДІВ КІБЕРЗАХИСТУ: ПЕРЕВАГИ ТА ВИКЛИКИ..... 13

БЕЛІКОВ В. О.
МЕТОДИ ОЦІНЮВАННЯ УРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВ І ТЕСТУВАННЯ НА ПРОНИКНЕННЯ..... 19

ВАЦКОВСЬКИЙ В. В.
СИСТЕМА ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ІНФОРМАЦІЙНІЙ ІНФРАСТРУКТУРІ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА..... 26

ГАНЖА О. Ю.
МУЛЬТИФАКТОРНІ МЕТОДИ ІДЕНТИФІКАЦІЇ У БАНКІВСЬКІЙ СФЕРІ ДЛЯ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ..... 32

ДЕМЧИШИНА І. М.
ЕФЕКТИВНИЙ АЛГОРИТМ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ КІБЕРЗАГРОЗ ДЛЯ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ THREAT INTELLIGENCE..... 40

ЖУРАВЛЬОВ А. О.
ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ МЕНЕДЖМЕНТУ АРМА..... 46

КАРПЕНКО В. О.
ПОРІВНЯЛЬНИЙ АНАЛІЗ AZURE BACKUP ТА ТРАДИЦІЙНИХ РІШЕНЬ РЕЗЕРВНОГО КОПІЮВАННЯ..... 54

КНЯЗЄВ О. Я.
УПРАВЛІННЯ ЦИФРОВИМИ АКТИВАМИ ТА ОСОБЛИВОСТІ ЦИФРОВИХ ПРАВ І ДОЗВОЛІВ..... 62

КОНОВАЛ О. В.
ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ ЕЛЕКТРОННИХ ЛИСТІВ НА ОСНОВІ АНАЛІЗУ ЗМІСТУ ТА МЕТАДАНИХ..... 70

КОРКАЧ К. А.
КРИТЕРІАЛЬНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ КРИПТОАКТИВІВ..... 75

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

КОСТИРЕВА Б. Ю.
РЕСУРСОЕФЕКТИВНИЙ МЕТОД ДЕТЕКЦІЇ ШКІДЛИВОГО КОДУ НА СЕРВЕРАХ ХОСТИНГ-ПРОВАЙДЕРІВ 80

КОТ Т. Р.
ПОРІВНЯЛЬНИЙ АНАЛІЗ WAF У ЗАХИСТІ ВЕБДОДАТКІВ 88

КУЗЬМЕНКО М. О.
КРИТЕРІЇ БЕЗПЕКИ ПРИ РОЗРОБЦІ КРИПТОГАМАНЦЯ..... 93

ЛИТВИН Ю. Ю.
ВИЯВЛЕННЯ ВИТОКУ ДАНИХ ТА ЗАПОБІГАННЯ ЦЬОМУ ЗА ДОПОМОГОЮ АЛГОРИТМІВ DLP 101

ЛУНГУЛ В. С.
АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ В ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМАХ..... 109

МАЛИК С. В.
КРИТЕРІАЛЬНИЙ АНАЛІЗ СИСТЕМ ШИФРУВАННЯ ТА РЕЗЕРВУВАННЯ ДАНИХ 118

ПАВЛЕНКО С. С.
SYSLOG ЯК ЕФЕКТИВНЕ РІШЕННЯ ДЛЯ МОНІТОРИНГУ ТА УПРАВЛІННЯ ЖУРНАЛАМИ ПОДІЙ У .NET ЗАСТОСУНКАХ.....11233

ПИШНИЙ І. В.
РОЛЬ ЗАСТОСУНКУ «ДІЯ» У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ..... 130

ПОЖАЛОВ Р. С.
ПІДХОДИ ДО ВИКОРИСТАННЯ QR-КОДІВ У ВЕРИФІКАЦІЇ ДОКУМЕНТІВ..... 136

СВІРЩУК Я. Ю.
БЕЗПАРОЛЬНІ МЕТОДИ АВТЕНТИФІКАЦІЇ У ВЕБЗАСТОСУНКАХ 143

СИНЕЛЬНИК Д. В.
АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ МОБІЛЬНИХ МЕРЕЖ ВІД АТАК НА КОНФІДЕНЦІЙНІСТЬ І ДОСТУПНІСТЬ..... 148

СТЕПАНЕНКО Д. Д.
ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ І ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОБУДОВИ СТІЙКОЇ КІБЕРБЕЗПЕКИ ФІНАНСОВИХ СЕРВІСІВ 155

СУРЖАНСЬКИЙ Д. Д.
ІНТЕГРАЦІЯ SIEM-СИСТЕМ ІЗ ЗАСОБАМИ РЕЗЕРВНОГО КОПІЮВАННЯ ТА ВИЯВЛЕННЯ АНОМАЛІЙ ДЛЯ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ 162

ТКАЧЕНКО О. В.
АНАЛІЗ ІНТЕГРАЦІЇ DORA В УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ПІДПРИЄМСТВ 169

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ФЕДІК А. В.
СКАНУВАННЯ ВЕБВРАЗЛИВОСТЕЙ: АВТОМАТИЗОВАНІ МЕТОДИ ТА ЇХ ЕФЕКТИВНІСТЬ У КІБЕРБЕЗПЕЦІ..... 176

ФІЛАТЕНКО В. С.
ЕФЕКТИВНЕ ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБСАЙТІВ ЗА ДОПОМОГОЮ АЛГОРИТМІВ КОНТРОЛЬОВАНОГО НАВЧАННЯ..... 182

ЧАВА В. О.
СИСТЕМА АУТЕНТИФІКАЦІЇ КОРПОРАТИВНИХ КОРИСТУВАЧІВ НА ОСНОВІ ПРИВАТНИХ МЕРЕЖ ТА ПУБЛІЧНИХ КЛЮЧІВ..... 188

ЧАЙКА Б. П.
ОГЛЯД МЕТОДІВ ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У БІЛІНГОВИХ СИСТЕМАХ ЗА ДОПОМОГОЮ АЛГОРИТМУ RC4..... 195

ШЕВЯКОВ Н. С.
КОМБІНОВАНИЙ ПІДХІД ДО ВИКОРИСТАННЯ СИСТЕМ СКАНУВАННЯ ВРАЗЛИВОСТЕЙ ДЛЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....20404

ШЕРШЕНЬ Д. С.
МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД АТАК ЛОГІЧНИХ ВИСНОВКІВ НА КОМЕРЦІЙНОМУ ПІДПРИЄМСТВІ.....21313

ШОСТАК Л. В.
АНАЛІЗ ВРАЗЛИВОСТЕЙ ПОШИРЕНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДО КВАНТОВИХ АТАК.....22121

ЮРЧЕНКО Д. О.
АРХІТЕКТУРА НАДІЙНОГО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ: ПРИНЦИПИ, МОДЕЛІ ТА МЕХАНІЗМИ РЕАЛІЗАЦІЇ.....22727

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ВСТУП

На глобальному рівні відбуваються значні трансформації у сфері обробки та захисту інформації, зумовлені 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 в контексті кібербезпеки та захисту інформації. Оскільки інформаційні технології стають не просто складовою частиною, а й активним каталізатором розвитку інформаційного суспільства, з'являється необхідність у забезпеченні надійності і 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, що є необхідними відповідно до сучасного цифрового світу, де дані та системи стають вразливими перед кіберзагрозами.

На сьогодні актуальним є завдання розширення сфери інформаційної науки, зокрема зосередження на розвитку сучасних технологій програмування. Не менш вагомими є дослідження інформаційних процесів у економіці та розробка ефективних методів управління ними в умовах інформаційного суспільства. Слід зауважити, що кіберзагрози стають дедалі більш поширеним явищем. Саме тому 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, включно зі складними ситуаціями. 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 щодо 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 випускних кваліфікаційних робіт.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ЗАСТОСУВАННЯ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АТАК З НУЛЬОВИМ ДНЕМ У СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

АРЕФ'ЄВ І. Є., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто проблему виявлення атак з нульовим днем у системах електронної комерції за допомогою методів глибокого навчання. Проаналізовано останні дослідження у цій галузі, виділено невирішені аспекти проблеми. Запропоновано підходи до використання глибоких нейронних мереж для аналізу мережевого трафіку та виявлення аномалій. Наведено результати експериментів, які підтверджують ефективність запропонованих методів. Висновки статті вказують на перспективи подальшого розвитку напрямку.

The article examines the problem of detecting zero-day attacks in e-commerce systems using deep learning methods. Recent research in this field is analyzed, and unresolved aspects of the problem are highlighted. Approaches to using deep neural networks for analyzing network traffic and detecting anomalies are proposed. The results of experiments confirming the effectiveness of the proposed methods are presented. The conclusions of the article indicate the prospects for further development of the direction.

Актуальність. Сучасні системи електронної комерції є одними з найбільш привабливих цілей для кібератак через великі обсяги конфіденційної інформації, яку вони обробляють. Особливу небезпеку становлять атаки з нульовим днем, які використовують невідомі вразливості та залишаються непомітними для традиційних систем захисту. Виявлення таких атак є критично важливим для забезпечення безпеки електронної комерції, оскільки вони можуть призводити до значних фінансових втрат, порушення бізнес-процесів та втрати довіри клієнтів. Глибоке навчання, як один із найперспективніших методів штучного інтелекту, пропонує нові можливості для виявлення атак з нульовим днем завдяки здатності аналізувати складні шаблони даних та виявляти аномалії в реальному часі.

Метою статті є дослідження особливостей використання інформаційно-управляючих систем на підприємствах роздрібної торгівлі з метою підвищення ефективності їх функціонування.

Об'єктом дослідження є системи електронної комерції, які піддаються кібератакам з нульовим днем.

Предмет дослідження – процеси виявлення аномалій у мережевому трафіку за допомогою глибоких нейронних мереж.

Аналіз попередніх досліджень. Останні дослідження в галузі кібербезпеки демонструють ефективність використання глибокого навчання для виявлення аномалій у мережевому трафіку, однак кожен із запропонованих підходів має свої переваги та недоліки, які варто враховувати.

Дж. Сміт та Л. Джонсон запропонували використання згорткових нейронних мереж (CNN) для аналізу пакетів даних, що дозволяє виявляти підозрілі дії [1]. Автори наголошують на високій точності виявлення аномалій завдяки здатності CNN аналізувати складні шаблони в мережевому трафіку, однак основним недоліком є необхідність великих обсягів даних для навчання моделей, що може бути проблемою для малих та середніх підприємств. Також, автори не враховують специфіку систем електронної комерції, де великі обсяги даних та висока частота транзакцій ускладнюють виявлення атак з нульовим днем.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

А. Браун та Р. Девіс розглянули застосування рекурентних нейронних мереж (RNN) для прогнозування атак на основі історичних даних [2]. Їхній підхід дозволяє ефективно аналізувати часові ряди, такі як журнали подій, що є особливо корисним для виявлення динамічних загроз, однак автори не враховують високу обчислювальну складність RNN, що може обмежити їхнє застосування в системах з обмеженими ресурсами. Крім того, їхній підхід не адаптований для виявлення атак з нульовим днем, які вимагають більш проактивних методів.

І. Шпінарева та співавтори дослідили застосування глибокого навчання для виявлення атак у мережевому трафіку [7]. Автори запропонували використання гібридної нейронної мережі CNN+LSTM, що дозволяє покращити точність виявлення загроз за рахунок комбінованого аналізу просторових і часових залежностей у даних. Дослідження демонструє високу ефективність підходу, зокрема, у виявленні складних мережевих атак, проте основним недоліком є залежність від вибору набору даних для навчання: використання UNSW-NB15 може не повністю відображати реальні умови мережевого трафіку. Крім того, автори не розглядають питання продуктивності моделі у високонавантажених системах, що може впливати на її практичну застосовність.

Є. Майор запропонував використання глибоких згорткових нейронних мереж для виявлення DDoS-атак у мережевому трафіку [8]. Основна увага приділена ефективності CNN у розпізнаванні аномальних патернів у пакетах даних, що дозволяє знижувати рівень помилкових спрацьовувань. Автор також відзначає можливість застосування даного методу в системах реального часу, проте одним із ключових недоліків дослідження є використання набору даних KDD Cup 99, який є застарілим і не відображає сучасних загроз. Також, у роботі не враховано адаптивність моделі до нових типів атак, що є критично важливим аспектом для динамічних кіберзагроз.

Однак більшість існуючих підходів не враховують специфіку систем електронної комерції, де великі обсяги даних та висока частота транзакцій ускладнюють виявлення атак з нульовим днем. Це свідчить про необхідність розробки спеціалізованих методів, які враховують особливості електронної комерції.

Виклад основного матеріалу. У таблиці 1 порівнюються традиційні методи кіберзахисту та методи на основі штучного інтелекту за ключовими критеріями, такими як точність, швидкість реагування, адаптивність та обробка великих даних.

Таблиця 1

Порівняння традиційних методів кіберзахисту та методів на основі ШІ

Критерій	Традиційні методи	Методи на основі ШІ
Точність виявлення атак	Низька точність для нових та складних атак (наприклад, атак з нульовим днем)	Висока точність завдяки аналізу складних шаблонів даних.
Швидкість реагування	Реагування зазвичай відбувається після виявлення атаки	Реагування в реальному часі завдяки автоматизації
Адаптивність	Обмежена здатність адаптуватися до нових видів загроз	Висока адаптивність завдяки постійному навчанню на нових даних
Обробка великих даних	Обмежена здатність обробляти великі обсяги даних у реальному часі	Ефективна обробка великих обсягів даних завдяки використанню хмарних технологій
Виявлення аномалій	Виявлення аномалій ґрунтується на відомих шаблонах.	Виявлення аномалій на основі аналізу відхилень від нормальної поведінки
Вартість впровадження	Нижча початкова вартість, але вищі витрати на підтримку та оновлення.	Вища початкова вартість, але нижчі витрати на підтримку завдяки автоматизації.

Джерело: розроблено автором

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Для виявлення атак з нульовим днем запропоновано використовувати глибокі нейронні мережі. Згорткові нейронні мережі (CNN) є одним із найефективніших методів для аналізу структури мережевих пакетів. Вони використовують згорткові шари для виявлення локальних шаблонів у даних, що дозволяє ефективно аналізувати мережевий трафік. Наприклад, CNN показали високу точність у виявленні аномалій у мережевому трафіку, досягаючи показника 95,2% [3]. Цей підхід особливо ефективний для аналізу великих обсягів даних, таких як пакети мережевого трафіку, оскільки CNN здатні виявляти складні шаблони та залежності.

Рекурентні нейронні мережі (RNN) ефективні для аналізу часових рядів, таких як журнали подій або дані про мережевий трафік. Вони здатні запам'ятовувати попередні стани, що дозволяє аналізувати послідовності подій та виявляти аномалії в реальному часі. Наприклад, В. Сосновий та І. Замрій у своїй роботі дослідили ефективність RNN з довготривалою короткочасною пам'яттю (Long Short-Term Memory, LSTM) для боротьби в кіберпросторі, досягнувши точності 99,70% [4] . Цей підхід особливо корисний для виявлення атак з нульовим днем, оскільки дозволяє аналізувати динаміку змін у мережевому трафіку.

Автоенкодери дозволяють виявляти аномалії шляхом відтворення вхідних даних, вони складаються з двох частин: енкодера, який стискає вхідні дані, та декодера, який відтворює їх. Аномалії виявляються за рахунок великої різниці між вхідними даними та їх відтворенням. Автоенкодери показали ефективність у виявленні невідомих загроз, досягаючи точності 89,5% [5]. Цей підхід особливо корисний для виявлення атак з нульовим днем, оскільки дозволяє виявляти відхилення від нормальної поведінки без необхідності попереднього навчання на зразках атак.

У таблиці 2 порівнюються основні методи глибокого навчання (CNN, RNN, автоенкодери) за точністю, перевагами та недоліками для виявлення атак з нульовим днем у системах електронної комерції.

Таблиця 2

Порівняння методів глибокого навчання для виявлення атак з нульовим днем

Метод	Точність	Переваги	Недоліки
CNN	95,2%	Ефективний для аналізу структури мережевих пакетів	Вимагає великих обсягів даних для навчання
RNN	99,7%	Ефективний для аналізу часових рядів та прогнозування атак	Висока обчислювальна складність
Автоенкодери	89,5%	Виявляє невідомі загрози за рахунок аналізу відхилень від нормальної поведінки	Менша точність порівняно з CNN та RNN

Джерело: розроблено автором

Проведений аналіз показав, що більшість існуючих методів не враховують специфіку систем електронної комерції, зокрема пропонується використання глибокого навчання для виявлення атак у фінансових системах [6]. Однак ці методи не адаптовані для електронної комерції, де великі обсяги даних та висока частота транзакцій ускладнюють виявлення атак з нульовим днем.

Крім того, існуючі підходи часто не враховують динамічний характер кіберзагроз, які постійно еволюціонують. Це свідчить про необхідність розробки спеціалізованих методів, які враховують особливості електронної комерції, такі як висока частота транзакцій, великі обсяги даних та необхідність швидкого реагування на загрози.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Глибоке навчання демонструє значний потенціал у сфері виявлення аномалій у мережевому трафіку електронної комерції, забезпечуючи високу точність, адаптивність до нових загроз та здатність обробляти великі обсяги даних у режимі реального часу. Основною перевагою цих методів є їхня здатність аналізувати складні патерни даних, що уможливлює ідентифікацію навіть малопомітних аномалій. Завдяки можливостям глибокого навчання виявлення загроз досягає високої ефективності, оскільки такі методи можуть адаптуватися до нових викликів у сфері кібербезпеки. Нейронні мережі навчаються на великому масиві даних і здатні працювати з великими потоками інформації в реальному часі, що є критично важливим для ефективного моніторингу мережевого трафіку.

На рисунку 1 проілюстровано процес виявлення атак з нульовим днем у системах електронної комерції за допомогою глибокого навчання.

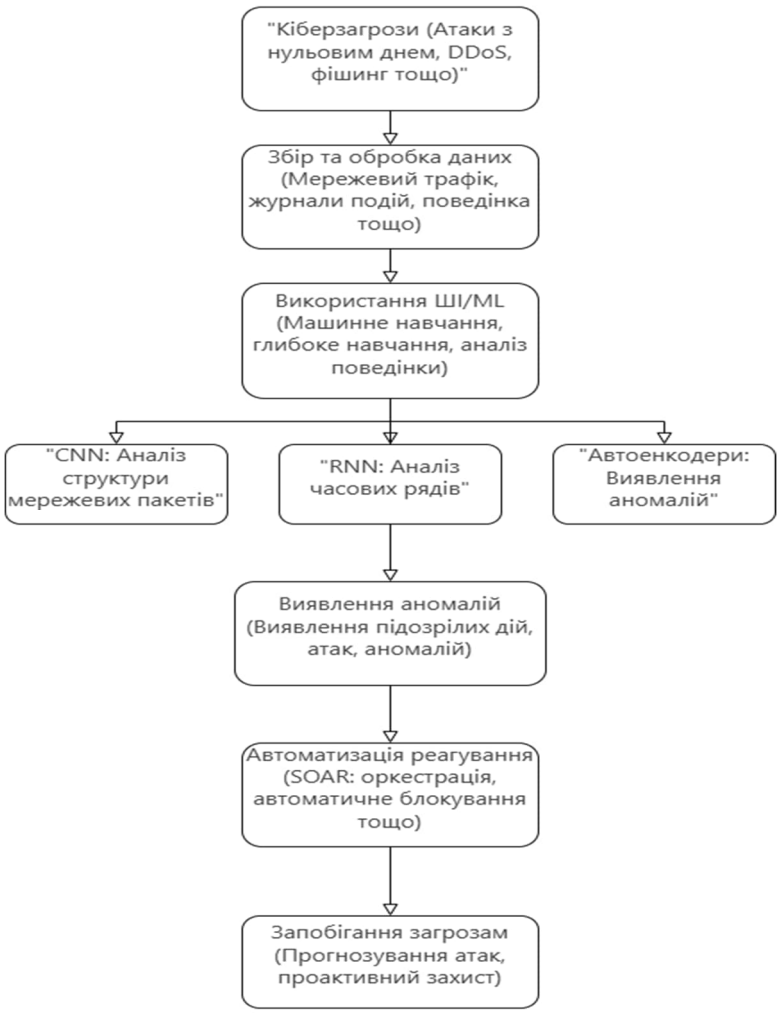


Рис. 1. Алгоритм виявлення атак з нульовим днем

Джерело: розроблено автором

Глибоке навчання є одним із найбільш перспективних напрямів розвитку штучного інтелекту, який вже довів свою ефективність у розв'язанні складних завдань у різних сферах, включаючи кібербезпеку. Використання нейронних мереж дозволяє значно підвищити точність виявлення загроз у мережевому трафіку електронної комерції. Водночас, цей підхід має свої обмеження, що пов'язані з високими обчислювальними витратами, необхідністю регулярного оновлення моделей та великим обсягом даних, необхідних для навчання.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Однією з основних проблем є необхідність значних обчислювальних ресурсів. Глибокі нейронні мережі складаються з великої кількості шарів та параметрів, що потребують потужних графічних процесорів (GPU) або навіть спеціалізованих тензорних процесорів (TPU) для ефективного навчання. Високі витрати на апаратне забезпечення ускладнюють широке впровадження цих методів для невеликих компаній та стартапів, обмежуючи їхню доступність. Ще одним суттєвим обмеженням є необхідність регулярного оновлення моделей. Оскільки загрози у кіберпросторі постійно змінюються, моделі, що використовуються для виявлення атак, швидко втрачають актуальність. Для підтримки високої точності необхідно періодично оновлювати навчальні вибірки та перевчати мережі, що вимагає значних ресурсів і часу. Крім того, ефективність глибокого навчання безпосередньо залежить від наявності великої кількості даних. Для створення точних і надійних моделей необхідно мати збалансовані вибірки, що містять як нормальні, так і аномальні дані. Проблема полягає в тому, що атаки з нульовим днем є малопоширеними, і отримання достатньої кількості прикладів таких атак для навчання є складним завданням.

Попри зазначені обмеження, глибоке навчання продовжує демонструвати значні переваги у сфері кібербезпеки. В рамках аналізу мережевого трафіку електронної комерції було розглянуто три основні методи, що застосовуються для виявлення атак. Згорткові нейронні мережі зазвичай застосовуються у розпізнаванні зображень, але вони також ефективні у виявленні аномалій у мережевому трафіку. Вони використовують згорткові фільтри для виділення ключових особливостей у даних, що дозволяє ефективно ідентифікувати структурні аномалії у трафіку. Дослідження показали, що ці мережі можуть досягати високої точності у виявленні шкідливого трафіку, що робить їх перспективним інструментом для кібербезпеки. Рекурентні нейронні мережі та їхні вдосконалені варіанти, такі як LSTM і GRU, виявилися ефективними у прогнозуванні атак. Вони дозволяють аналізувати часові залежності у даних, що дає змогу виявляти закономірності, пов’язані з потенційними загрозами. Використання цих методів у кібербезпеці дає можливість прогнозувати майбутні атаки, що значно покращує здатність систем реагувати на загрози у режимі реального часу. Автоенкодери використовуються для аналізу відхилень від нормальної поведінки у мережевому трафіку. Вони навчаються реконструювати нормальні дані та можуть виявляти аномалії шляхом порівняння отриманого результату з вхідними даними. Це дозволяє їм ефективно ідентифікувати невідомі загрози, навіть якщо у навчальній вибірці відсутні прямі приклади атак.

Щоб забезпечити ефективність глибокого навчання у динамічному середовищі кіберзагроз, необхідно враховувати декілька важливих напрямів розвитку. Одним із ключових викликів є зменшення витрат на обчислювальні ресурси. Для цього можна застосовувати методи моделювання зменшеної точності, використання квантованих моделей та розподіленого навчання. Використання безперервного навчання та самонавчальних систем може значно зменшити потребу у ручному оновленні моделей. Розробка механізмів збору та генерації реалістичних даних, що включають нові види атак, допоможе підвищити стійкість моделей до невідомих загроз.

Висновки. Методи глибокого навчання продемонстрували високу ефективність у виявленні аномалій у мережевому трафіку електронної комерції. Зокрема, згорткові нейронні мережі забезпечують точність 95,2% при аналізі структурних характеристик мережевих пакетів, що робить їх ефективним інструментом для виявлення складних загроз. Рекурентні нейронні мережі досягли точності 99,7% у прогнозуванні атак, що підтверджує їхню здатність аналізувати часові ряди та виявляти динамічні загрози. Автоенкодери продемонстрували точність 89,5% у розпізнаванні невідомих загроз, що підтверджує їхню ефективність у виявленні аномалій на основі аналізу відхилень від нормальної поведінки мережевого трафіку.

Попри високу ефективність, специфіка електронної комерції створює додаткові виклики для впровадження методів глибокого навчання. Висока частота транзакцій, великі обсяги даних та необхідність швидкого реагування на загрози вимагають розробки спеціалізованих підходів. Наявні моделі глибокого навчання не завжди враховують ці

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

особливості, що потребує адаптації та вдосконалення алгоритмів для їхньої ефективної інтеграції в реальні системи. Також, впровадження методів глибокого навчання супроводжується низкою обмежень, зокрема високими обчислювальними витратами, необхідністю в значних обсягах навчальних даних та потребою у регулярному оновленні моделей для збереження їхньої актуальності.

Наукова новизна дослідження полягає в проведенні комплексного аналізу ефективності методів глибокого навчання у контексті виявлення атак з нульовим днем у системах електронної комерції. Виконано порівняльний аналіз згорткових нейронних мереж, рекурентних нейронних мереж та автоенкодерів, що дозволило виявити їхні сильні сторони та обмеження. Запропоновано підходи до інтеграції методів глибокого навчання з сучасними системами кіберзахисту, а також розглянуто етичні та правові аспекти їхнього застосування. Особливу увагу приділено необхідності дотримання стандартів безпеки, зокрема вимог GDPR, що є критичним для забезпечення конфіденційності даних у системах електронної комерції.

Подальші дослідження мають бути спрямовані на розробку гібридних моделей, що поєднують переваги різних методів глибокого навчання. Поєднання згорткових нейронних мереж для аналізу структури мережевого трафіку та рекурентних нейронних мереж для аналізу часових рядів може підвищити ефективність виявлення аномалій. Перспективним напрямом є також інтеграція методів глибокого навчання із системами автоматизованого реагування (SOAR), що дозволить прискорити ідентифікацію та нейтралізацію кіберзагроз. Окрім технічних аспектів, необхідне подальше вивчення етичних і правових питань, пов’язаних із використанням штучного інтелекту у сфері кібербезпеки. Важливим є також дослідження можливостей інтеграції цих методів із хмарними технологіями для масштабування ресурсів і підвищення швидкості обробки великих обсягів даних. Розробка алгоритмів для виявлення цілеспрямованих атак (APT) на основі глибокого навчання є ще одним важливим напрямом подальших досліджень, оскільки такі загрози часто залишаються непоміченими протягом тривалого часу.

Список використаних джерел

1. Smith, J., & Johnson, L. (2022). Deep Learning for Cybersecurity: A Comprehensive Review. *Journal of Cybersecurity*, 15(3), 45–60.
2. Brown, A., & Davis, R. (2021). Zero-Day Attack Detection Using Recurrent Neural Networks. *International Journal of Information Security*, 10(2), 112–125.
3. Петляк, Н., Білецький, К., & Заставна, Я. (2024). Підхід до виявлення аномального мережевого трафіку з використанням алгоритмів LOF та HBOS. *Вимірювальна та обчислювальна техніка в технологічних процесах*, (4), 125–129.
4. Сосновий, В. О., & Замрій, І. В. (2022). Безпека мережі з використанням рекурентної нейромережі. *Зв’язок*, (5), 124–129.
5. Chen, L., & Liu, Z. (2021). Autoencoders for Anomaly Detection in Cybersecurity. *Neural Networks*, 25(3), 112–125.
6. Zhang, L., & Chen, H. (2022). Deep Learning for Financial Cybersecurity: Challenges and Advances. *Journal of Financial Technology*, 9(1), 45–61.
7. Шпінарева, І. М., & Співавтори. (2022). Використання глибокого навчання для виявлення атак у мережевому трафіку. *Журнал інформаційної безпеки*, 14(2), 32-47.
8. Майор, Є. (2021). Глибокі згорткові нейронні мережі для виявлення DDoS-атак. *Кіберзахист та інформаційні технології*, 19(4), 75–88.
9. CICIDS2017 Dataset. URL: https://www.unb.ca/cic/datasets/ids-2017.html

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

КОНСОЛІДАЦІЯ ПОВЕДІНКОВОЇ АНАЛІТИКИ ТА КЛАСИЧНИХ МЕТОДІВ КІБЕРЗАХИСТУ: ПЕРЕВАГИ ТА ВИКЛИКИ

БАХЯН Д. А., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються особливості консолідації поведінкової аналітики з класичними методами кіберзахисту як перспективного напряму підвищення рівня інформаційної безпеки сучасних організацій. Проведено порівняльний аналіз традиційних засобів захисту (брандмауерів, антивірусних програм, систем IDS/IPS та SIEM) щодо їх можливостей виявлення та протидії кіберзагрозам. Встановлено переваги застосування поведінкової аналітики для виявлення нових, невідомих загроз. Водночас, проаналізовано основні виклики, що виникають під час інтеграції двох підходів, серед яких – технологічна складність, висока кваліфікація персоналу та ризик помилкових спрацювань алгоритмів. Обґрунтовано висновок про доцільність комплексного застосування класичних та поведінкових методів з метою забезпечення ефективної кібербезпеки.

The article examines the features of consolidating behavioral analytics with classical cybersecurity methods as a promising approach to enhancing the information security of modern organizations. A comparative analysis of traditional security tools (firewalls, antivirus software, IDS/IPS, and SIEM systems) was conducted, evaluating their capabilities to detect and counter cyber threats. The advantages of applying behavioral analytics to detect new, unknown threats are identified. At the same time, the main challenges arising from the integration of the two approaches are analyzed, including technological complexity, the high qualification requirements for personnel, and the risk of false-positive alerts generated by analytical algorithms. The paper substantiates the conclusion on the appropriateness of comprehensive application of classical and behavioral methods to ensure effective cybersecurity.

Актуальність. Сучасний цифровий світ характеризується стрімким зростанням кількості та складності кіберзагроз, що становлять серйозні виклики для інформаційної безпеки організацій різних галузей. В останні роки спостерігається значне зростання атак, що використовують соціальну інженерію, експлуатацію вразливостей «нульового дня», поліморфні та цільові атаки (Advanced Persistent Threats, APT). Класичні методи кіберзахисту, які ґрунтуються на статичних сигнатурах, жорстких правилах та моніторингу відомих загроз, демонструють обмежену ефективність у боротьбі з такими атаками [8].

Традиційні методи кіберзахисту, такі як антивірусні програми, брандмауери та системи виявлення вторгнень (IDS/IPS), створювалися переважно з метою ідентифікації та запобігання вже відомим видам загроз. Ці технології виявляють проблеми через відповідність атак певним сигнатурам або шаблонам, які попередньо внесені до бази даних. Відповідно, їх здатність протистояти абсолютно новим чи нетиповим загрозам є значно обмеженою, оскільки для цього потрібен час на розпізнавання, аналіз та створення нових сигнатур.

Зростання адаптивності та складності кіберзагроз диктує необхідність застосування більш гнучких методик, які здатні оперативно виявляти аномалії та нестандартну поведінку користувачів і систем у реальному часі. Саме тут поведінкова аналітика стає важливим доповненням до класичних засобів кіберзахисту. Ця технологія базується на використанні алгоритмів машинного навчання та штучного інтелекту, що дозволяє оперативно виявляти відхилення від нормальної поведінки навіть у тих випадках, коли загроза ще невідома і не має чітких сигнатур [1].

Особливого значення інтеграція поведінкової аналітики з класичними методами набуває в умовах сучасних кібероперацій, спрямованих на критичну інфраструктуру та

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

інформаційні системи великих корпорацій. У таких атаках злочинці часто виявляють високу винахідливість, приховують свою присутність у мережі, уникаючи спрацювання класичних засобів захисту, що потребує більш глибокого аналізу поведінки користувачів та систем для оперативного виявлення атак.

Крім того, актуальність цієї консолідації обумовлена зростанням ролі дистанційної роботи та розподілених мереж, особливо у період пандемії COVID-19 та після неї. Це створює додаткові вразливості, адже значно важче контролювати поведінку користувачів, що знаходяться поза межами корпоративного периметру захисту [5]. В таких умовах класичні методи кіберзахисту втрачають частину своєї ефективності, а поведінкова аналітика дозволяє суттєво підвищити рівень виявлення та реагування на загрози шляхом аналізу саме поведінкових патернів.

Таким чином, інтеграція поведінкової аналітики з класичними методами кіберзахисту є надзвичайно актуальною науково-прикладною задачею, яка дозволяє підвищити загальний рівень інформаційної безпеки організацій у сучасних умовах. Проте ця інтеграція також викликає низку технологічних, організаційних та кадрових викликів, що потребують додаткового наукового вивчення та розробки ефективних практичних рекомендацій.

Метою статті є аналіз переваг і викликів, які виникають при консолідації поведінкової аналітики та класичних методів кіберзахисту, визначення практичних шляхів інтеграції цих технологій у корпоративну систему інформаційної безпеки.

Об'єктом дослідження є процес консолідації поведінкової аналітики та класичних методів кіберзахисту в умовах сучасних загроз.

Предмет дослідження - система інформаційної безпеки сучасних організацій.

Аналіз попередніх досліджень. Огляд літератури показує, що класичні підходи до кібербезпеки переважно описані в роботах таких дослідників як В. Столлінгз [12], А.С. Таненбаум, М. Ван Стін [13], які акцентують увагу на чітких правилах, жорстких політиках безпеки та традиційних методах виявлення загроз. Водночас, поведінкова аналітика, зокрема із застосуванням алгоритмів машинного навчання, описана в працях таких авторів як Х. Чен [3], С. Рамезані, А Соммерс [11]. Ці дослідники наголошують на ефективності поведінкової аналітики у виявленні аномалій, які не охоплюються класичними сигнатурними методами.

Попри наявні роботи, недостатньо уваги приділено саме практичним аспектам інтеграції цих двох підходів, а також чітко не виокремлено переваги та труднощі, які можуть виникати при їхній консолідації.

Виклад основного матеріалу. Сучасний цифровий світ характеризується стрімким зростанням кількості та складності кіберзагроз, що становлять серйозні виклики для інформаційної безпеки організацій різних галузей. В останні роки спостерігається значне зростання атак, що використовують соціальну інженерію, експлуатацію вразливостей «нульового дня», поліморфні та цільові атаки (Advanced Persistent Threats, APT). Класичні методи кіберзахисту, які ґрунтуються на статичних сигнатурах, жорстких правилах та моніторингу відомих загроз, демонструють обмежену ефективність у боротьбі з такими атаками [2].

Для глибшого розуміння сутності та особливостей класичних методів кіберзахисту доцільно здійснити їх порівняльний аналіз. Нижче наведена таблиця, що систематизує основні характеристики та особливості таких поширених методів кібербезпеки, як брандмауери, антивірусні засоби, системи виявлення та запобігання вторгненням (IDS/IPS), а також SIEM-системи.

На основі здійсненого порівняльного аналізу можна зробити висновок, що кожен класичний метод кіберзахисту має свої сильні та слабкі сторони. Брандмауери та антивірусні засоби є ефективними для захисту від вже відомих типів загроз, однак демонструють низьку здатність адаптуватися до нових, невідомих атак. IDS/IPS забезпечують більш глибокий рівень

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

аналізу та швидке реагування, проте вони досить чутливі до хибних спрацювань, що може ускладнювати роботу системи захисту.

Натомість SIEM-системи є більш комплексним рішенням, оскільки інтегрують різні підходи та методи аналізу, включаючи сигнатурний, поведінковий та кореляційний аналізи. Завдяки високому рівню автоматизації та здатності до аналізу поведінки, вони можуть ефективніше ідентифікувати складні та нетипові загрози. Проте їх впровадження вимагає значних ресурсів та високого рівня кваліфікації персоналу.

Таблиця 1

Основні характеристики та особливості поширених методів кібербезпеки

Характеристика	Брандмауери	Антивірусні засоби	IDS/IPS	SIEM-системи
Тип аналізу	Переважно статичний	Сигнатурний та евристичний	Сигнатурний, евристичний та аномальний	Кореляційний, поведінковий та сигнатурний
Основний принцип роботи	Фільтрація трафіку за заданими правилами	Виявлення шкідливого ПЗ за сигнатурами	Аналіз трафіку та подій для виявлення вторгнень	Збір, кореляція та аналіз подій безпеки
Реагування на нові загрози	Обмежене, базується на правилах	Обмежене, залежить від оновлення бази сигнатур	Помірне, залежить від регулярних оновлень сигнатур та евристики	Високе, через аналіз поведінки та подій у реальному часі
Здатність до аналізу поведінки	Низька	Низька або помірна	Середня	Висока
Складність впровадження	Низька	Низька	Середня	Висока
Рівень автоматизації аналізу загроз	Низький або середній	Середній	Середній або високий	Високий
Ризик хибних спрацювань (false positives)	Низький	Середній	Високий	Середній
Орієнтованість на відомі/невідомі загрози	Відомі загрози	Відомі загрози	Переважно відомі, частково невідомі	Відомі та невідомі загрози

Джерело: розроблено автором на основі [10]

Таким чином, найбільш ефективним рішенням є саме інтегрований підхід, що поєднує класичні методи з поведінковою аналітикою в межах єдиної системи, що забезпечує більш високий рівень інформаційної безпеки організації [4].

Класичні методи кіберзахисту орієнтовані на виявлення відомих типів загроз через порівняння сигнатур. Вони демонструють ефективність проти вже описаних атак, проте є малоефективними щодо нових, невідомих або складних загроз. Наприклад, атаки «нульового дня» (zero-day), поліморфні та метаморфні віруси можуть залишатися непоміченими тривалий час. Це є критичною проблемою в умовах зростаючої динамічності кіберзагроз.

Поведінкова аналітика, навпаки, ґрунтується на використанні технологій штучного інтелекту та алгоритмів машинного навчання для виявлення аномалій у поведінці користувачів чи систем. На відміну від сигнатурних методів, поведінкова аналітика дозволяє ідентифікувати потенційні загрози на основі відхилень від типової поведінки користувачів чи програм, навіть якщо ця загроза ще невідома класичним сигнатурам. Типові приклади поведінкових моделей включають моніторинг аномальної активності користувача, незвичні

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

часові інтервали доступу, раптові зміни в об’ємах переданих даних тощо.

Для кращого розуміння сутності поведінкової аналітики у сфері кібербезпеки доцільно проаналізувати її основні характеристики, переваги та виклики у порівняльному форматі. Нижче наведена таблиця, що узагальнює ключові аспекти використання поведінкової аналітики в процесах інформаційного захисту.

Таблиця 2

Основні характеристики поведінкової аналітики

Характеристика	Опис та особливості
Основний принцип роботи	Виявлення аномалій та нетипової поведінки користувачів і систем на основі аналізу історичних даних та поточних подій
Реагування на нові загрози	Високе, дозволяє виявляти навіть раніше невідомі загрози
Тип аналізу	Поведінковий, аномальний, із застосуванням штучного інтелекту та машинного навчання
Здатність до прогнозування загроз	Висока, може передбачити ймовірність майбутніх загроз на основі тенденцій та моделей поведінки
Складність впровадження	Висока, потребує значних технологічних та кадрових ресурсів
Рівень автоматизації аналізу загроз	Високий, але потребує ретельного налаштування алгоритмів
Ризик хибних спрацювань (false positives)	Середній або високий, залежить від якості налаштування та тренування алгоритмів
Орієнтованість на відомі/невідомі загрози	Переважно невідомі, нові, складні та адаптивні загрози

Джерело: розроблено автором на основі [6]

Представлена таблиця демонструє, що поведінкова аналітика характеризується високою здатністю до виявлення складних та невідомих раніше кіберзагроз завдяки глибокому аналізу патернів поведінки користувачів та систем. Вона дозволяє оперативно ідентифікувати аномалії навіть без наявності чітких сигнатур, що значно розширює можливості сучасних систем інформаційної безпеки.

Водночас суттєвим викликом при впровадженні поведінкової аналітики є необхідність висококваліфікованих фахівців, складність налаштування та тренування аналітичних алгоритмів, а також ризик великої кількості хибних позитивів, що може ускладнювати процес реагування [7].

Таким чином, ефективність поведінкової аналітики значною мірою залежить від ретельної підготовки даних, високої якості алгоритмів машинного навчання, а також від поєднання її з класичними методами, що дозволяє нівелювати потенційні недоліки та досягти оптимального рівня інформаційного захисту організації.

Інтеграція цих двох методик дозволяє досягти синергетичного ефекту. На практиці це реалізується через SIEM-системи, які поєднують сигнатурні методи аналізу (класичний підхід) та алгоритми поведінкової аналітики (сучасний підхід). Наприклад, SIEM може спочатку фільтрувати інциденти через сигнатури відомих загроз, а потім додатково аналізувати підозрілі події через модулі поведінкової аналітики. Це дозволяє значно зменшити кількість хибних позитивів (false positives) і прискорити процес реагування.

Однак, незважаючи на численні переваги, процес консолідації має ряд викликів (рис. 1).

Перш за все, суттєвим викликом є технологічна складність інтеграції різнорідних платформ, які початково розроблялися для роботи окремо одна від одної. Кожна технологія має свої унікальні протоколи, формати даних, способи їх зберігання та передачі. Через це інтеграція в єдину систему може потребувати створення додаткових програмних інтерфейсів (API), спеціальних конекторів та адаптерів, що значно збільшує фінансові витрати й час, необхідний на впровадження.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Крім цього, успішна технологічна інтеграція вимагає глибокого розуміння внутрішніх процесів кожної платформи, що передбачає залучення висококваліфікованих IT-спеціалістів і, часто, зовнішніх консультантів. Не менш важливим є забезпечення сумісності та стабільності роботи інтегрованих платформ, адже навіть незначні технологічні конфлікти можуть призвести до втрати даних, перебоїв у роботі системи чи порушень безпеки.

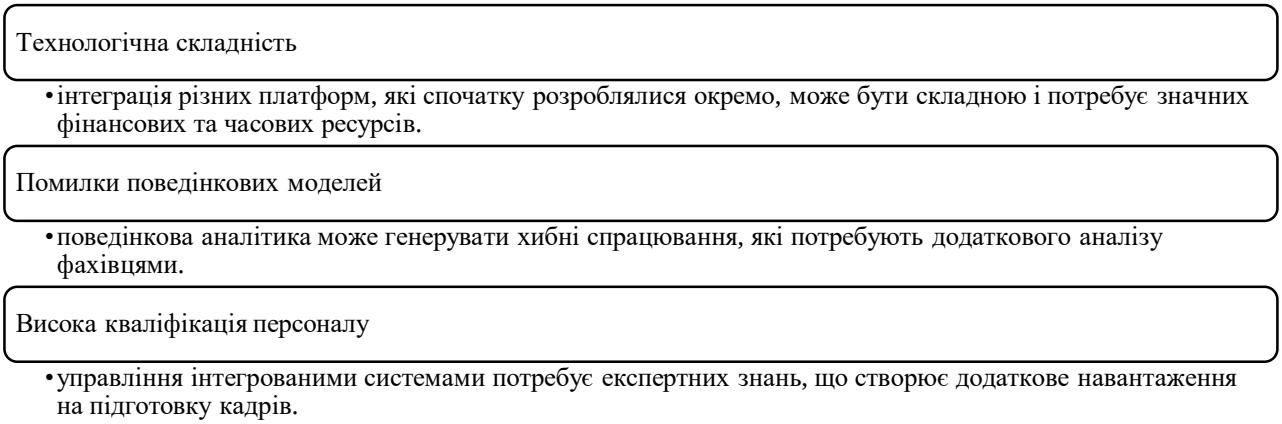


Рис. 1. Виклики процесу консолідації поведінкової аналітики та класичних методів кіберзахисту

Джерело: розроблено автором на основі [9]

Інший важливий виклик, пов'язаний із консолідацією, стосується помилок, що виникають при використанні поведінкових моделей аналітики. Однак не кожна виявлена аномалія є реальною загрозою. Наприклад, зміни у звичайній поведінці користувачів можуть бути викликані природними причинами, такими як оновлення програмного забезпечення, зміна робочого графіку або технічні несправності, а не обов'язково зловмисними діями.

Ці хибні позитиви створюють додаткове навантаження на команди кібербезпеки, змушуючи витрачати значні ресурси на аналіз та верифікацію кожного спрацювання. Крім того, якщо таких помилкових тривог стає забагато, вони можуть спричинити «ефект втоми» персоналу, коли спеціалісти знижують рівень пильності або перестають реагувати належним чином на реальні загрози, що в результаті може знизити загальну ефективність системи безпеки.

Ще одним вагомим викликом консолідації є потреба у висококваліфікованих кадрах. Управління інтегрованими рішеннями, які включають і класичні, й поведінкові методи, вимагає значно вищого рівня експертних знань, ніж при застосуванні кожного з них окремо. Від персоналу очікується не лише базове розуміння роботи окремих технологій, а й вміння аналізувати комплексні події, інтерпретувати результати поведінкової аналітики, налаштовувати алгоритми машинного навчання та швидко приймати рішення в умовах невизначеності.

Таким чином, впровадження інтегрованих систем вимагає додаткових зусиль на підготовку кадрів, підвищення їхньої кваліфікації, регулярного навчання та адаптації до нових технологій. Зважаючи на дефіцит спеціалістів у галузі кібербезпеки, цей аспект є особливо гострим і може стати суттєвою перешкодою для успішної реалізації проєктів із впровадження консолідованих систем кіберзахисту. Вирішення цього виклику потребує стратегічного підходу до розвитку кадрової політики підприємств, залучення висококваліфікованих спеціалістів та створення програм постійного професійного розвитку для працівників служб безпеки.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Висновки. Консолідація поведінкової аналітики та класичних методів кіберзахисту є перспективним напрямком у розвитку інформаційної безпеки. Вона дозволяє значно підвищити ефективність захисту інформаційних систем завдяки комплексному аналізу загроз та скороченню часу реагування на інциденти. Проте впровадження цього підходу потребує вирішення низки організаційних, технічних та кадрових проблем. Подальші дослідження мають бути спрямовані на розробку більш простих та універсальних методик інтеграції, оптимізацію поведінкових моделей для мінімізації помилок та формування рекомендацій щодо підготовки кваліфікованих фахівців у сфері кібербезпеки.

Список використаних джерел

1. Addae, J., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, 29, 701–750.
2. Bwangah, M. (2023). Behavioural Analytics in Cyber Security for Digital Forensics Application. *International Journal of Computer Science and Information Technology*.
3. Chen, H., Engkvist, O., Wang, Y., Olivecrona, M., & Blaschke, T. (2018). The rise of deep learning in drug discovery. *Drug discovery today*, 23 (6), 1241–1250.
4. Khaliq, S., Tariq, Z., & Masood, A. (2020). Role of User and Entity Behavior Analytics in Detecting Insider Attacks. *2020 International Conference on Cyber Warfare and Security (ICCWS)*, 1–6.
5. Kommisetty, P., Kuppala, B., Buvvaji, H., & Sabbella, V. (2022). Revolutionizing Cybersecurity: Behavioral Analysis and Automated Incident Response through Predictive Analytics. *International Journal of Scientific Research and Management (IJSRM)*.
6. Mihailescu, M., Nita, S., Rogobete, M., & Marascu, V. (2023). Unveiling Threats: Leveraging User Behavior Analysis for Enhanced Cybersecurity. *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 01–06.
7. Ofoegbu, K., Osundare, O., Ike, C., Fakeyede, O., & Ige, A. (2023). Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. *Computer Science & IT Research Journal*.
8. Okafor, C., Agho, M., Ekwezia, A., Eyo-Udo, N., & Daraojimba, C. (2023). UTILIZING BUSINESS ANALYTICS FOR CYBERSECURITY: A PROPOSAL FOR PROTECTING BUSINESS SYSTEMS AGAINST CYBER ATTACKS. *Acta Electronica Malaysia*.
9. Olabanji, S., Marquis, Y., Adigwe, C., Ajayi, S., Oladoyinbo, T., & Olaniyi, O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*.
10. Patterson, W., & Winston-Proctor, C. (2019). Behavioral Cybersecurity. *Behavioral Cybersecurity*.
11. Ramezani, S., & Sommers, A. (2020). Machine Learning algorithms in quantum computing: a survey. У 2020 International Joint Conference on Neural Networks (IJCNN) (с. 1–8).
12. Stallings, W. (2018). *Effective cybersecurity: a guide to using best practices and standards*. Addison-Wesley Professional.
13. Tanenbaum, A. S., & Van Steen, M. (2007). *Distributed systems: Principles and paradigms* (2nd ed.). Prentice Hall of India.

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВОЇ Ю. Є.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

МЕТОДИ ОЦІНЮВАННЯ УРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВ І ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

БЕЛІКОВ В. О., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються методи оцінювання уразливостей інформаційних ресурсів підприємств і тестування на проникнення Vulnerability Assessment & Penetration Testing, як ефективний інструмент проактивного кіберзахисту. Описано життєвий цикл оцінювання уразливостей і тестування на проникнення, а також проаналізовано проактивні заходи, що дозволяють запобігати потенційним кібератакам. Окрему увагу приділено огляду сучасних методів оцінювання уразливостей та аналізу поширених інструментів Vulnerability Assessment & Penetration Testing, зокрема комерційних і open-source рішень. У статті акцентується увага на практичних аспектах впровадження цих методів у систему кіберзахисту підприємств для мінімізації ризиків зовнішніх і внутрішніх загроз.

The article discusses methods of vulnerability assessment of enterprise information resources and penetration testing (Vulnerability Assessment & Penetration Testing) as an effective tool for proactive cyber defense. The lifecycle of vulnerability assessment and penetration testing is described, along with an analysis of proactive measures that help prevent potential cyberattacks. Special attention is given to the overview of modern vulnerability assessment methods and the analysis of commonly used Vulnerability Assessment & Penetration Testing tools, including commercial and open-source solutions. The article emphasizes the practical aspects of implementing these methods within enterprise cybersecurity systems to minimize the risks of external and internal threats.

Актуальність. Актуальність теми зумовлена стрімким розвитком інформаційних технологій та інтеграцією інформаційних систем підприємств у глобальну мережу Інтернет, що значно збільшує їх уразливість до кіберзагроз. В умовах сучасної цифрової трансформації бізнес-процесів підприємства стикаються з необхідністю забезпечення високого рівня захисту своїх інформаційних ресурсів від несанкціонованого доступу, зловмисних атак та внутрішніх загроз. Оцінка уразливостей і проведення тестування на проникнення є критично важливими інструментами для виявлення слабких місць у системах безпеки, що дозволяє своєчасно вжити заходів щодо їх усунення і зниження ризиків кіберзлочинності. Оскільки сучасні кіберзагрози стають дедалі складнішими і еволюціонують, підприємствам необхідно постійно удосконалювати свої методи оцінки безпеки та адаптувати їх до нових викликів. Оцінка уразливостей та тестування на проникнення дозволяють не лише виявити існуючі загрози, а й забезпечити проактивний підхід до захисту інформаційних ресурсів, що має велике значення для стійкості та ефективності роботи організацій у цифрову епоху. Тому дослідження сучасних методів та підходів до оцінювання уразливостей є необхідним кроком для удосконалення систем кібербезпеки підприємств і підвищення їх здатності протистояти кіберзагрозам.

Метою статті є дослідження основних методів оцінювання уразливостей інформаційних ресурсів підприємств та аналіз ефективності тестування на проникнення (VAPT) як важливого інструменту для виявлення потенційних загроз, зниження кіберризиків та підвищення рівня безпеки інформаційних систем у реальних умовах.

Об'єктом дослідження є процес оцінювання уразливостей інформаційних ресурсів підприємств та методи тестування на проникнення, що застосовуються для виявлення потенційних загроз і забезпечення належного рівня кібербезпеки в інформаційних системах організацій.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Предмет дослідження – підходи до оцінювання уразливостей інформаційних ресурсів підприємств та методи тестування на проникнення, що дозволяють виявляти слабкості в системах і покращувати їх безпеку.

Аналіз попередніх досліджень. У сучасних дослідженнях, присвячених оцінці уразливостей і тестуванню на проникнення (VAPT), виявлено численні важливі аспекти, які дозволяють підвищити рівень кібербезпеки організацій. Зокрема, А. Аль-Ахмад, Х. Каятан, Ф. Худжайна та Х. Джалаб провели систематичний огляд підходів до тестування на проникнення в мобільних хмарних додатках, що є актуальним для підприємств, які використовують хмарні сервіси [1]. Автори підкреслюють роль пентесту як проактивного інструмента виявлення уразливостей у хмарному середовищі, класифікують сучасні методи аналізу безпеки та визначають ефективні інструменти виявлення вразливих компонентів. Це дослідження є цінним для адаптації методів оцінювання уразливостей в умовах динамічної інфраструктури підприємств, які впроваджують хмарні технології.

А. Йоланда та Ч. Сафітрі зосереджують увагу на мережевій поведінці інструменту *Proxychains* у пентест-сценаріях, використовуючи аналіз трафіку за допомогою Wireshark [2]. Дослідження демонструє, як можна виявляти аномалії в мережевому трафіку, пов'язані з використанням проксі-серверів, що актуально для виявлення прихованих атак на IT-інфраструктуру підприємства. Отримані результати мають практичне значення в рамках мережевої криміналістики та застосовуються при побудові систем виявлення вторгнень.

Б. Бхіміредді, А. Німмагадда, Х. Курапаті, Л. Гогула, Р. Чінтала та В. Джадала провели аналіз найбільш поширених атак на веб-додатки та методів їх запобігання, зокрема SQL-ін'єкцій, XSS та CSRF [3]. Авторський колектив описує сучасні механізми захисту від таких атак, що дозволяє підвищити безпеку веб-компонентів інформаційних систем підприємств. Робота є важливою для формування підходів до оцінювання уразливостей у веб-середовищі й впровадження превентивних заходів захисту.

П. Ананд та А. Сінгх здійснили порівняльний аналіз найпопулярніших інструментів для тестування безпеки – Metasploit, Nmap, Burp Suite та інших [4]. Автори визначають сильні та слабкі сторони кожного з інструментів, що дає змогу вибудовувати ефективні стратегії пентестування залежно від особливостей IT-інфраструктури підприємства. Це дослідження є корисним при побудові комплексної методики оцінювання уразливостей та вибору відповідних технічних засобів.

М. Дені, К. Зена та Т. Хаяджне провели огляд фундаментальних принципів тестування на проникнення: моделі атак, їх етапи (розвідка, сканування, експлуатація) та базові методи захисту [5]. Стаття містить структуру пентест-процесу та практичні рекомендації щодо підготовки до тестування, що є основою для побудови внутрішніх процедур інформаційної безпеки підприємства. Результати можуть бути використані для розробки моделей загроз і тест-кейсів оцінювання вразливості IT-систем.

Аналіз вищенаведених джерел демонструє багатогранний підхід до оцінювання уразливостей: від технічного аналізу мережевого трафіку і інструментів пентесту до системних підходів у хмарних середовищах і методологій виявлення атак. Джерела формують наукову й практичну основу для подальшої розробки ефективної системи кіберзахисту підприємства.

Виклад основного матеріалу. У сучасному світі інформаційних технологій використання комп'ютерних систем зростає, що призводить до збільшення їх складності. Підключення більшості мереж до Інтернету, а також впровадження нових програмних засобів збільшує кількість потенційних уразливостей, ставлячи під загрозу безпеку цих систем. Уразливості можуть виникати через помилки в розробці або недоліки в проєктуванні програмного забезпечення, що дозволяє зловмисникам отримувати несанкціонований доступ або завдавати шкоди користувачам. Такі слабкості створюють можливості для кіберзлочинців, які прагнуть атакувати інформаційні ресурси підприємств і викрасти чи змінити важливі дані.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Для підвищення рівня безпеки систем і захисту даних критично важливо проводити регулярну оцінку уразливостей і тестування на проникнення, що дозволяє вчасно виявляти загрози та знижувати ризики кіберзлочинів.

Оцінка VAPT є комплексним процесом (рис. 1), що включає кілька етапів, починаючи з визначення обсягу завдання, в якому тестувальник вибирає тип тестування – чорна, сіра або біла коробка. Після цього на етапі розвідки отримується інформація про операційну систему, мережу та IP-адресу тестованої системи, що дозволяє здійснити первинний аналіз її вразливих місць. На наступному етапі застосовуються різноманітні техніки оцінки уразливостей, що допомагають виявити слабкі місця в системі. Після цього проводиться детальний аналіз виявлених уразливостей, і розробляється план для тестування на проникнення, який дає змогу тестувальнику проникнути в систему жертви.

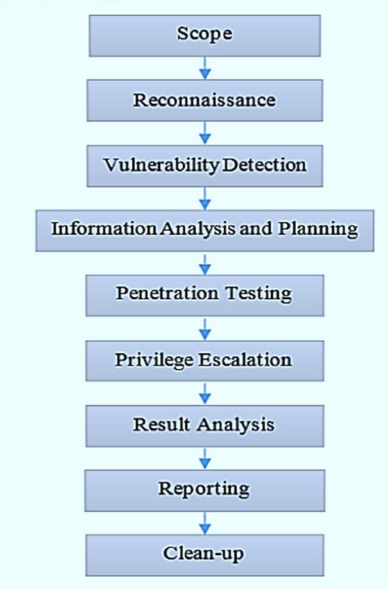


Рис. 1. Життєвий цикл оцінки уразливостей та тестування на проникнення

Джерело: розроблено автором в програмному середовищі Cisco Packet Tracer (знімок з екрану)

Після цього проводиться детальний аналіз виявлених уразливостей, і розробляється план для тестування на проникнення, який дає змогу тестувальнику проникнути в систему жертви. Протягом цього процесу тестувальник підвищує свої привілеї, що дозволяє йому отримати доступ до більш глибоких рівнів системи. В кінці етапу аналізу результатів тестувальник вивчає отримані дані та формулює рекомендації для усунення виявлених уразливостей. Усі етапи тестування документуються та передаються керівництву підприємства для вжиття відповідних заходів. Після завершення процесу тестування система відновлюється до попереднього стану, як це було до початку проведення VAPT.

Загалом, життєвий цикл VAPT є важливою складовою процесу забезпечення інформаційної безпеки підприємств, яка включає кілька етапів, що взаємопов’язані між собою і створюють комплексний підхід до виявлення та усунення кіберзагроз. На першому етапі тестувальник визначає обсяг тестування, обираючи один з підходів: чорна, біла або сіра коробка. Це рішення залежить від рівня доступу до тестованої системи і визначає, яку інформацію тестувальник буде мати на момент початку тестування. Наступним етапом є збір інформації, на якому тестувальник здійснює розвідку, отримуючи дані про мережу, операційну систему, IP-адреси та інші характеристики системи або мережі, що дозволяє сформувати загальну картину й визначити потенційні точки проникнення.

Після збору інформації настає етап оцінки уразливостей, де тестувальник за допомогою різноманітних інструментів і методів виявляє слабкі місця в системі. Це може бути як

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

статичний аналіз коду, так і використання автоматизованих сканерів або ручне тестування. Виявлені уразливості стають основою для подальшого планування атак. Тестувальник розробляє план проникнення, який враховує найбільш критичні уразливості, що можуть призвести до серйозних кіберзагроз, таких як DDoS-атаки, ARP poisoning або інші види атак. На етапі тестування на проникнення тестувальник намагається здійснити фактичне проникнення в систему, використовуючи виявлені уразливості, що дає можливість не лише продемонструвати ступінь загрози, але й оцінити, на які глибші рівні системи можна проникнути. Якщо проникнення виявляється успішним, наступним кроком є ескалація привілеїв, коли зловмисник намагається підвищити свої привілеї для отримання більш широкого доступу до системних ресурсів.

Після проведення тестування проводиться детальний аналіз отриманих результатів, в ході якого тестувальник формулює рекомендації для усунення виявлених уразливостей, що включають застосування патчів, оновлень або змін в конфігураціях системи. Адміністратори підприємств, на основі отриманих результатів, вживають заходів для ліквідації уразливостей, що дозволяє значно підвищити рівень безпеки інформаційної системи.

Заключним етапом є повторна перевірка, коли після усунення уразливостей тестувальник здійснює контрольне тестування для підтвердження, що всі уразливості були усунені та система більше не має відкритих точок для потенційних атак. У результаті повного проходження циклу оцінки уразливостей та тестування на проникнення, підприємство отримує зміцнену систему безпеки, здатну протистояти більшості кіберзагроз, що виникають у процесі її експлуатації.

У контексті оцінки уразливостей застосовуються різні техніки, зокрема статичний аналіз, який не передбачає виконання тестових випадків або експлойти, а лише вивчається структура коду та вміст системи. Цей метод дозволяє виявити уразливості без шкоди для системи, однак він є досить повільним і потребує значної кількості людських ресурсів. Ручне тестування здійснюється без використання спеціалізованих інструментів: тестувальник використовує свої знання та досвід для пошуку уразливостей, що робить цей метод дешевшим, хоча і менш автоматизованим. У разі автоматизованого тестування використовуються спеціалізовані інструменти, які виконують тести на виявлення уразливостей, що значно скорочує час, необхідний для тестування, і підвищує точність результатів. Однак, варто зазначити, що такі інструменти не здатні виявити всі типи уразливостей, що збільшує загальні витрати на оцінку уразливостей.

Фуззинг, або тестування за допомогою подачі випадкових або некоректних даних у систему, також є важливою технікою, що дозволяє виявити нульові уразливості, і для її застосування потрібен мінімум людського втручання. Фуззинг (від англ. fuzzing) – це метод тестування програмного забезпечення, який полягає в автоматичному введенні випадкових, некоректних або спеціально сформованих даних до системи або програми з метою виявлення її вразливостей. Основна мета фуззингу – перевірити, як система реагує на незвичні або несподівані входи, що можуть спричинити збій або інші проблеми, такі як крах програми, витік даних або підвищення прав доступу.

Цей метод тестування допомагає виявити ті уразливості, які можуть залишатися непоміченими при звичайному тестуванні, особливо у випадках, коли система повинна обробляти багато різних типів даних або працює з неконтрольованими вхідними даними. Фуззинг часто використовують для виявлення нульових уразливостей (zero-day vulnerabilities), які ще не були виявлені або виправлені розробниками. Завдяки такому підходу можна значно знизити ризики безпеки, виявляючи і виправляючи потенційно небезпечні слабкості до того, як вони будуть використані зловмисниками.

Тестування на проникнення може бути здійснене за різними підходами. У разі чорного тестування тестувальник не має попередньої інформації про тестовану мережу чи систему, тому він повністю покладається на свої навички для проникнення в систему. Сіре тестування

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

є комбінацією чорного та білого тестувань, при якому тестувальник має часткові знання про мережу. Біле тестування передбачає, що тестувальник володіє повною інформацією про мережу і систему, що дозволяє здійснити більш глибокий аналіз та отримати точніші результати. Вибір конкретної техніки залежить від вимог до тестування, а також від рівня доступу, який тестувальник має до системи.

На сучасному ринку існує безліч як безкоштовних, так і платних інструментів для оцінки VAPT, що дає змогу користувачам вибирати найбільш підходящий засіб в залежності від вимог до безпеки та специфіки тестованої системи. Кожен з цих інструментів має свої унікальні можливості та обмеження, що визначають їх ефективність у різних умовах. Так, деякі з них спеціалізуються на виявленні конкретних типів уразливостей, таких як SQL-ін'єкції чи XSS, в той час як інші орієнтовані на більш складні питання, наприклад, на тестування мережевої інфраструктури або виявлення уразливостей у веб-додатках. Вибір інструменту залежить від специфіки завдання, рівня безпеки, який потрібно забезпечити, та доступного бюджету.

Крім того, деякі інструменти надають можливість автоматизованого тестування, що суттєво скорочує час проведення тестування, в той час як інші вимагають більш глибокого ручного втручання. Зокрема, автоматизовані інструменти можуть ефективно виявляти загальні уразливості, але можуть мати обмеження у виявленні більш складних або прихованих загроз. Ручне тестування, у свою чергу, забезпечує більш детальний аналіз і виявлення складних уразливостей, хоча і займає більше часу. Проте важливо пам'ятати, що жоден інструмент не дає 100% гарантії на виявлення всіх уразливостей, тому поєднання різних методів та інструментів є ключовим для досягнення високої ефективності процесу оцінки безпеки. У зв'язку з цим багато організацій використовують комбінацію як автоматизованих, так і ручних інструментів для більш повного охоплення можливих загроз. Використання цих інструментів також вимагає належної кваліфікації тестувальників, які повинні правильно налаштувати і використовувати інструменти для досягнення максимального ефекту.

Серед найбільш відомих інструментів для тестування на проникнення варто виділити Nmap, який є потужним сканером мереж і дозволяє виявляти активні пристрої, відкриті порти та працюючі служби в мережах, що дає змогу виявити потенційні уразливості через неправильну конфігурацію. Nmap є кросплатформеним інструментом, сумісним з усіма основними операційними системами, такими як Windows, Linux та macOS. З іншого боку, Metasploit є платформою для розробки та виконання експлойтів, що дає змогу не тільки виявляти уразливості, але й активно тестувати на проникнення, за допомогою яких можна перевірити стійкість системи до атак. Metasploit підтримує різні плагіни, що дозволяють автоматизувати процес тестування, і є доступним для різних операційних систем.

Також важливим інструментом є Burp Suite, який орієнтований на тестування безпеки веб-додатків. Цей набір інструментів включає в себе функції для маніпулювання HTTP-запитами, аналізу трафіку між клієнтом і сервером, що дозволяє виявляти поширені уразливості, такі як SQL-ін'єкції, XSS і інші проблеми з безпекою веб-додатків. Burp Suite підтримує основні операційні системи і є незамінним інструментом для тестувальників, що працюють з веб-сервісами. Крім того, Burp Suite має розширювану архітектуру, що дозволяє інтегрувати додаткові плагіни та розширення для специфічних задач, що робить його надзвичайно гнучким інструментом для комплексного тестування безпеки веб-додатків.

Wireshark – це потужний аналізатор мережевого трафіку, який допомагає виявляти проблеми безпеки на рівні мережевих протоколів. Цей інструмент дозволяє знімати та аналізувати пакети даних, що передаються між пристроями, та знаходити уразливості, пов'язані з нешифрованими передачею даних або атаками типу «man-in-the-middle». Wireshark є кросплатформним інструментом, який підтримує Windows, Linux та macOS і є важливим інструментом для аналізу трафіку в мережах підприємств.

Інструмент Nessus широко використовується для сканування уразливостей і дозволяє

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

швидко і точно виявляти уразливості на різних рівнях – від операційних систем до додатків і мережевих служб. Nessus підтримує великі бази плагінів для перевірки різних типів уразливостей, зокрема в системах управління базами даних та веб-серверах, і є одним з найпопулярніших інструментів для виконання комплексного тестування на проникнення. Всі ці інструменти є основою для побудови ефективного процесу оцінки уразливостей, дозволяючи значно скоротити час виявлення уразливостей і підвищити точність тестування.

Завдяки інтеграції таких інструментів у процес тестування на проникнення підприємства можуть не тільки швидко виявляти слабкі місця в своїх інформаційних системах, а й забезпечити більш високий рівень кібербезпеки, що є надзвичайно важливим в умовах сучасних кіберзагроз. Використання VAPT-інструментів дає змогу ефективно виявляти уразливості, оцінювати їх ризики та вчасно вживати заходів для захисту від можливих атак.

Зазвичай, зловмисник починає свою атаку з ретельної розвідки мережі жертви, намагаючись отримати якомога більше інформації про її інфраструктуру, структуру мережі, а також характеристики системи, що дозволяє йому зрозуміти потенційні точки входу для подальших атак (рис. 2). Після збору необхідних даних, зловмисник приступає до виконання оцінки уразливостей, намагаючись виявити слабкі місця в мережі або системі, що дає йому змогу скласти детальний список усіх виявлених уразливостей, які можуть бути використані для проникнення. Цей етап є критично важливим, оскільки дозволяє зловмиснику точно визначити найбільш уразливі точки системи, через які можна отримати несанкціонований доступ, що в свою чергу, відкриває можливість для виконання атаки.

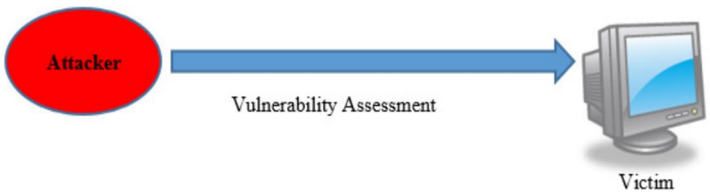


Рис. 2. Оцінка уразливостей зловмисником

Джерело: розроблено автором в програмному середовищі Cisco Packet Tracer (знімок з екрану)

Тому визначення таких уразливостей є основоположним етапом у процесі тестування на проникнення, оскільки саме на цьому етапі можна ефективно виявити потенційні загрози для підприємства, що дає змогу своєчасно вжити відповідні заходи для усунення виявлених уразливостей і підвищити рівень безпеки організації в цілому.

Загалом, Оцінка уразливостей є ключовим етапом тестування на проникнення, оскільки передбачає аналіз і виявлення слабких місць у системах і мережах підприємства. Зловмисник починає з розвідки, збираючи дані про мережеву інфраструктуру та конфігурації систем. Далі він застосовує методи оцінки уразливостей для виявлення точок, через які можна отримати несанкціонований доступ. На основі цього формується план дій: експлуатація уразливостей, підвищення привілеїв і встановлення контролю над системою.

Після отримання списку уразливостей жертви, зловмисник розробляє план можливого нападу (рис. 3). Використовуючи цей список, він здійснює експлуатацію мережі або системи жертви, що призводить до компрометації безпеки та інформації системи.

Зловмисник, який експлуатує систему жертви, використовує виявлені уразливості для несанкціонованого доступу до мережі або інформаційної системи жертви, з метою завдання шкоди або отримання конфіденційної інформації. Цей процес часто включає в себе не тільки проникнення в систему, а й подальше підвищення привілеїв для отримання повнішого контролю над системою, що дозволяє зловмиснику маніпулювати її ресурсами, викрадати або пошкоджувати дані, а також виконувати інші шкідливі дії, як-от інсталяція шкідливого ПЗ або знищення важливих файлів.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Рис. 3. Оцінка уразливостей зловмисником

Джерело: розроблено автором в програмному середовищі Cisco Packet Tracer (знімок з екрану)

Проте, якщо жертва усуне всі уразливості зі своєї системи, зловмисник не зможе здійснити проникнення в мережу чи систему. Застосування методів оцінки уразливостей та VAPT дозволяє користувачам виявляти уразливості, які можуть призвести до різних серйозних атак, таких як DDoS attacks, RA flooding, ARP poisoning тощо. Після виявлення цих уразливостей користувач може застосувати відповідні контрзаходи для їх усунення. Щоб зробити систему безпечною, адміністратор повинен провести оцінку уразливостей у своїй власній системі або мережі, застосувавши повний цикл тестування на проникнення та оцінки уразливостей.

Після отримання списку доступних уразливостей в його системі, адміністратор повинен усунути ці уразливості, застосувавши необхідні патчі, оновлення, встановивши відповідне програмне забезпечення та інші необхідні засоби. Таким чином, адміністратор видалить усі уразливості з його системи або мережі. У разі, якщо зловмисник спробує провести оцінку уразливостей в системі або мережі жертви, він не знайде відкритих уразливостей, що значно ускладнить можливість експлуатації системи.

Висновки. Оцінка уразливостей і тестування на проникнення є потужними інструментами для забезпечення кіберзахисту підприємств, що дозволяють виявляти та усувати потенційні загрози в інформаційних системах. Застосування цих методів дає змогу не лише виявити слабкі місця, а й визначити пріоритети для посилення безпеки, здійснивши проникнення в систему та оцінку її вразливих точок. Важливість включення VAPT у процеси кіберзахисту стає дедалі очевиднішою, оскільки зловмисники використовують все більш складні стратегії для компрометації мереж і систем. Проведення тестів на проникнення за допомогою різноманітних інструментів дозволяє не лише визначити наявні уразливості, а й впровадити належні заходи для їх усунення. Постійне вдосконалення технік оцінки уразливостей і тестування на проникнення є необхідною умовою для підвищення рівня безпеки інформаційних ресурсів підприємств і захисту від потенційних кіберзагроз.

Список використаних джерел

1. Al-Ahmad, A. S., Kahtan, H., Hujainah, F., & Jalab, H. A. (2019). Systematic literature review on penetration testing for mobile cloud computing applications. *IEEE Access, 7*, 173524–173540. https://doi.org/10.1109/ACCESS.2019.2956770.

2. Yolanda, A., & Safitri, C. (2023). Analyzing Proxychains traffic on the pentest scenario: Enhancements in network forensics through Wireshark. *2023 International Conference on Information Technology and Computing (ICITCOM)*, 340–345. IEEE. https://doi.org/10.1109/ICITCOM60176.2023.10442589.

3. Bhimireddy, B. R., Nimmagadda, A., Kurapati, H., Gogula, L. R., Chintala, R. R., & Jadala, V. C. (2023). Web security and web application security: Attacks and prevention. *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2095–2096. IEEE. https://doi.org/10.1109/ICACCS57279.2023.10112741.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

4. Anand, P., & Singh, A. S. (2021). Penetration testing security tools: A comparison. *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 182–184. IEEE. https://doi.org/10.1109/SMART52563.2021.9676283.

5. Denis, M., Zena, C., & Hayajneh, T. (2016). Penetration testing: Concepts, attack methods, and defense strategies. *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–6. IEEE. https://doi.org/10.1109/LISAT.2016.7494156.

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

СИСТЕМА ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ІНФОРМАЦІЙНІЙ ІНФРАСТРУКТУРІ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА

ВАЦКОВСЬКИЙ В. В., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті проведено комплексний аналіз побудови та функціонування сучасної системи виявлення та протидії кіберзагрозам, адаптованої до специфіки інформаційної інфраструктури торговельного підприємства. Детально розглянуто еволюцію кіберзагроз у секторі роздрібної торгівлі, ключові технології та методики захисту, нормативно-правові аспекти, а також стратегічні підходи до мінімізації ризиків. Особлива увага приділена інтегрованим рішенням, таким як SIEM/SOAR, аналізу поведінки користувачів та мережевого трафіку, захисту кінцевих точок та даних, а також важливості людського фактору та планування реагування на інциденти.

The article provides a comprehensive analysis of the construction and functioning of a modern cyber threat detection and response system adapted to the specifics of the information infrastructure of a commercial enterprise. The evolution of cyber threats in the retail sector, key technologies and protection methods, regulatory aspects, and strategic approaches to risk minimization are examined in detail. Special attention is paid to integrated solutions such as SIEM/SOAR, user and network behavior analysis, endpoint and data protection, as well as the importance of the human factor and incident response planning.

Актуальність. Сучасний розвиток інформаційних технологій спричинив кардинальні зміни у секторі роздрібної торгівлі. Цифрова трансформація бізнес-процесів, що охоплює управління запасами, логістику, взаємодію з клієнтами через онлайн-платформи та програми лояльності, суттєво підвищила ефективність підприємств. Проте така залежність від IT-систем створила значні ризики інформаційної безпеки. Торговельні підприємства стали привабливими цілями для кіберзлочинців, оскільки вони обробляють великі обсяги фінансових транзакцій, зберігають конфіденційні дані клієнтів, включаючи персональну інформацію та платіжні реквізити, і часто мають складні, розподілені IT-інфраструктури. Наслідки кібератак на підприємства можуть бути катастрофічними: прямі фінансові збитки, витоки даних клієнтів, що призводять до репутаційних втрат та значних штрафів, тривалі перебої в роботі через DDoS-атаки чи програми-вимагачі, а також підрив довіри з боку клієнтів та партнерів. Статистика останніх років демонструє невпинне зростання кількості та складності атак на торговельний сектор. Отже, побудова надійної, багаторівневої системи виявлення та протидії кіберзагрозам є не лише технічною потребою, але й стратегічним пріоритетом для

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

забезпечення стабільності та довгострокового успіху будь-якого сучасного торговельного підприємства.

Метою статті є комплексний аналіз сучасних підходів, методів та технологій виявлення і нейтралізації кіберзагроз, для інформаційної інфраструктури торговельних підприємств, а також розробка практичних рекомендацій щодо побудови ефективної системи кібербезпеки.

Об'єктом дослідження є процеси та компоненти системи виявлення й управління кіберзагрозами в IT-інфраструктурі підприємства.

Предметом дослідження виступають методи, алгоритми, технології та організаційні заходи, що використовуються для ідентифікації, аналізу, запобігання та реагування на кіберзагрози.

Аналіз попередніх досліджень. Питанням кіберзагроз та інформаційній інфраструктурі підприємств присвячено значна кількість досліджень. Зокрема, Ю. Стасюк та С. Ілюшик розглядають невід'ємний вплив цифрової трансформації на підходи до управління персоналом в сучасних організаціях, де цифрові технології стають ключовим фактором успіху та конкурентоспроможності. Автори підкреслюють, що інструменти на кшталт інформаційних систем управління персоналом (HRIS), хмарних платформ, засобів автоматизації рутинних завдань, електронних систем навчання (LMS), а також аналітики даних та штучного інтелекту революціонізують HR-процеси, дозволяючи оптимізувати роботу, покращити комунікацію та приймати більш обґрунтовані рішення щодо персоналу [1]. Автори влучно акцентують увагу не лише на технологічних перевагах, таких як підвищення продуктивності та ефективності, але й на зміні самої парадигми управління, де керівники перетворюються на фасилітаторів та менторів, адаптуючись до управління віртуальними командами. Водночас, автори слушно вказують на суттєві виклики, пов'язані з впровадженням цифрових рішень, зокрема на необхідність забезпечення кібербезпеки, конфіденційності даних та адаптації організаційної культури, що є критично важливим для успішної імплементації цих технологій та досягнення довгострокових стратегічних цілей в умовах цифрової економіки.

С. Лях робить важливий внесок у розуміння викликів кібербезпеки для роздрібної торгівлі, акцентуючи увагу на зростанні ризиків через цифровізацію бізнесу [2]. Автор аналізує застосування SIEM-систем для моніторингу загроз, EDR-рішень для захисту кінцевих пристроїв, Threat Intelligence платформ для передбачення атак та антифрод-інструментів для запобігання шахрайству. Важливо, що дослідження розглядає не лише окремі інструменти, а й їхню інтеграцію, підкреслюючи необхідність комплексного підходу. Це підтверджує, що ефективна кібербезпека повинна враховувати як технічні характеристики рішень, так і їхню взаємодію з бізнес-процесами торговельної мережі.

З. Морич, В. Дакич, Д. Єкич і Д. Регварт окреслюють необхідність модернізації традиційних підходів до кібербезпеки в умовах стрімкої цифровізації бізнес-середовища [3]. Автори переконливо аргументують, що поєднання сучасних технологій – від превентивного моніторингу вразливостей до Zero Trust архітектури – формує ядро ефективного захисту, але водночас справедливо вказують на обмежену готовність більшості організацій до інтеграції AI-рішень у повсякденні операційні процеси. Особливо цінним у роботі вважаю аналіз етичної дилеми між безпековими вимогами та правом на конфіденційність, який виявляє системні суперечності галузі. Хоча дослідження науковці недостатньо заглиблюється в роль людського фактору у кіберзагрозах, їхні висновки про важливість збалансованого поєднання технологій та організаційних практик залишаються особливо актуальними для роздрібної торгівлі, де оперативність реагування безпосередньо впливає на фінансові наслідки.

Аналіз попередніх досліджень підтверджує актуальність проблеми та вказує на різні аспекти її вирішення – від аналізу специфіки галузі та загроз до вибору конкретних інструментів. Однак часто бракує комплексного погляду, що об'єднував би технологічні, процесні, людські та нормативні аспекти в єдину систему управління кібербезпекою для торговельного підприємства.

Виклад основного матеріалу. Для ефективного захисту інформаційної інфраструктури торговельного підприємства необхідно чітко розуміти її склад. Сучасний ритейлер зазвичай

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

оперує комплексом взаємопов'язаних систем. Критично важливими є точки продажу (POS-системи), що включають термінали, сканери та платіжні пристрої, оскільки вони безпосередньо обробляють фінансові транзакції та платіжні дані, що робить їх привабливою ціллю для зловмисників.

У контексті безпеки POS-систем у роздрібній торгівлі основні загрози пов'язані з використанням застарілих операційних систем, відсутністю своєчасного оновлення програмного забезпечення та пасивну стратегію реагування на інциденти [4]. Проблема загострюється через нехтування комплексними заходами захисту, такими як сегментація мережі, контроль процесів у реальному часі та використання принципу нульової довіри (Zero Trust). Дослідження наголошує, що традиційні антивірусні рішення не забезпечують достатнього рівня безпеки, оскільки вони неефективні проти сучасних атак, зокрема fileless-malware та загроз нульового дня. Найефективнішим підходом для захисту POS-систем є впровадження засобів активного моніторингу, використання AI-аналізу аномалій та постійне навчання персоналу щодо основ кібергігієни, адже саме людський фактор часто залишається слабкою ланкою в системі кіберзахисту.

У системах виявлення вторгнень (IDS) сигнатурний підхід, хоч і залишається одним із найпоширеніших, має значні обмеження у виявленні нових та складних атак. Традиційні IDS, які базуються на базі відомих сигнатур загроз, неефективні проти атак нульового дня та складних багатоетапних вторгнень. Використання поведінкового аналізу та машинного навчання дозволяє виявляти аномальні дії в мережі, навіть якщо вони не відповідають жодному відомому шаблону атаки [5]. Ефективна система виявлення кіберзагроз повинна поєднувати обидва підходи – сигнатурний для швидкого розпізнавання відомих загроз та аномальний для ідентифікації нових, потенційно небезпечних активностей у мережі.

Основу бізнес-процесів складають системи управління підприємством (ERP), які інтегрують фінансові дані, інформацію про запаси, закупівлі та персонал, містячи чутливу комерційну інформацію. Поряд з ними функціонують системи управління взаємовідносинами з клієнтами (CRM), де зберігаються персональні дані клієнтів, історія покупок та контактна інформація, що створює ризики для конфіденційності. Для взаємодії з клієнтами онлайн використовуються платформи електронної комерції (веб-сайти та мобільні додатки), які також обробляють платіжні та особисті дані користувачів і можуть мати власні вразливості.

Усе це об'єднується мережевою інфраструктурою, що включає локальні мережі в магазинах та офісах, корпоративну мережу та підключення до Інтернету, яка потребує захисту передачі даних та контролю доступу (рис. 1). Роботу додатків забезпечує серверна інфраструктура та бази даних (клієнтські, товарні, транзакційні), розміщені на фізичних чи віртуальних серверах, що є потенційною ціллю для атак на дані. Дедалі частіше ритейлери використовують хмарні сервіси для зберігання даних, аналітики та маркетингу, що також несе ризики, пов'язані з управлінням доступом та конфіденційністю в хмарі.

Рис. 1. Схема типової IT-інфраструктури торговельного підприємства

Джерело: розроблено автором

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Ландшафт кіберзагроз у сфері торгівлі постійно еволюціонує, стаючи дедалі складнішим та цілеспрямованішим, а злочинці використовують все більш витончені методи. Серед актуальних загроз для торговельних підприємств виділяються фішингові атаки, які часто стають спрямованими (spear-phishing) на конкретних співробітників чи клієнтів через підроблені ресурси, використовуючи соціальну інженерію для викрадення даних або інсталяції шкідливого ПЗ. Різноманітне шкідливе програмне забезпечення (Malware) становить значну небезпеку: програми-вимагачі (Ransomware) залишаються однією з найбільших загроз, часто застосовуючи тактику подвійного чи потрійного вимагання; спеціалізоване POS-Malware, як-от скімери пам'яті, краде дані карток безпосередньо з терміналів; а інфостілери (InfoStealers) викрадають облікові та фінансові дані.

Серйозними загрозами для електронної комерції залишаються атаки на веб-додатки, такі як SQL-ін'єкції та міжсайтовий скриптинг (XSS), що використовуються для крадіжки даних чи порушення роботи платформ. Розподілені атаки на відмову в обслуговуванні (DDoS) застосовуються для зриву роботи онлайн-магазинів, іноді в комплексі з іншими атаками. Компрометація POS-терміналів може відбуватися не лише через шкідливе ПЗ, але й через фізичний доступ чи недоліки конфігурації. Атаки на ланцюг постачання (Supply Chain Attacks) спрямовані на компрометацію довірених постачальників для доступу до мережі ритейлера. Нові ризики створює впровадження Інтернету Речей (IoT), де незахищені пристрої стають точками входу. Також існують внутрішні загрози (Insider Threats), пов'язані з навмисними чи ненавмисними діями співробітників. Переважною мотивацією зловмисників є фінансовий зиск через крадіжку даних, вимагання викупу чи продаж інформації, хоча можливі й інші мотиви, наприклад, промислове шпигунство.

Забезпечення безпеки торговельного підприємства потребує багаторівневого підходу, що поєднує технології виявлення загроз та стратегії їх запобігання на різних рівнях (табл. 1). Центральним елементом часто виступають системи збору та аналізу подій безпеки (SIEM), які агрегують, нормалізують та корелюють логи з різноманітних джерел для виявлення підозрілої активності та аномалій в реальному часі. Їх доповнюють платформи оркестрації, автоматизації та реагування на інциденти безпеки (SOAR), які автоматизують відповідь на виявлені загрози, виконуючи сценарії блокування, ізоляції чи збагачення даних.

На рівні мережі ключову роль відіграють фаєрволи наступного покоління (NGFW), що забезпечують глибокий аналіз пакетів та контроль додатків, а також системи виявлення та запобігання вторгненням (IDS/IPS), які моніторять трафік на предмет відомих атак та підозрілої активності. Важливою стратегією є сегментація мережі для обмеження поширення потенційної атаки, наприклад, виділення окремих зон для POS-терміналів. Додатковий рівень захисту забезпечує аналіз поведінки мережевого трафіку (NTA), який використовує машинне навчання для виявлення нетипової активності, що може вказувати на невідомі загрози.

Безпека кінцевих точок (комп'ютерів, серверів, мобільних пристроїв, POS-терміналів) забезпечується за допомогою антивірусів наступного покоління (NGAV), які поєднують сигнатурні методи з поведінковим аналізом та машинним навчанням. Системи виявлення та реагування на кінцевих точках (EDR) надають глибокий моніторинг активності пристроїв та можливість віддаленої реакції на загрози, наприклад, ізоляції хоста. Системи запобігання вторгненням на хостах (HIPS) контролюють дії програм, а контроль пристроїв обмежує використання зовнішніх накопичувачів для запобігання витокам даних та занесенню шкідливого ПЗ.

Захист самих даних є критично важливим і включає шифрування конфіденційної інформації як при зберіганні, так і при передачі, що є вимогою стандартів PCI DSS та GDPR. Системи запобігання витоку даних (DLP) контролюють переміщення чутливої інформації всередині та за межі корпоративної мережі. Надійне управління доступом та ідентифікацією (IAM) передбачає впровадження багатофакторної автентифікації (MFA) для критичних систем та застосування принципу найменших привілеїв.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Нарешті, проактивний підхід включає управління вразливостями через регулярне сканування систем та ПЗ на наявність слабких місць та своєчасне встановлення оновлень безпеки (управління патчами). Тестування на проникнення (Penetration Testing) допомагає імітувати реальні атаки для виявлення неочевидних вразливостей. Регулярний аудит безпеки забезпечує перевірку конфігурацій, політик та процедур на відповідність стандартам та внутрішнім вимогам.

Таблиця 1

Порівняння ключових технологій виявлення кіберзагроз для інформаційної інфраструктури торговельного підприємства

Характеристика	SIEM (Security Information and Event Management, система управління інформацією та подіями безпеки)	NTA (Network Traffic Analysis, аналіз мережевого трафіку)	EDR (Endpoint Detection and Response, виявлення та реагування на загрози на кінцевих точках)
Призначення	Збір, кореляція та аналіз логів безпеки з різних джерел	Моніторинг і аналіз мережевого трафіку для виявлення аномалій	Виявлення, реагування та усунення загроз на кінцевих точках
Джерела даних	Логи від серверів, мережевого обладнання, додатків, антивірусів тощо	Мережевий трафік, пакети даних, поведінковий аналіз	Дії процесів, файлові операції, поведінковий аналіз на рівні ОС
Методи виявлення загроз	Кореляція подій, сигнатурний і поведінковий аналіз	Аналіз аномалій, машинне навчання, аналіз поведінки мережевих пристроїв	Аналіз поведінки, виявлення експлойтів, машинне навчання
Основні переваги	Централізований контроль, кореляція між різними джерелами	Виявлення загроз на рівні мережі, видимість всіх підключень	Глибока аналітика кінцевих пристроїв, автоматичне реагування
Основні недоліки	Високі вимоги до налаштування і ресурсів, можливі хибнопозитивні спрацювання	Менша деталізація щодо активності на кінцевих пристроях	Високе навантаження на систему, потреба в постійному оновленні
Приклади рішень	Splunk, IBM QRadar, ArcSight	Darktrace, Cisco Stealthwatch, Vectra AI	CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne

Джерело: розроблено автором на основі [6-7]

Оскільки інциденти безпеки можуть статися навіть за наявності надійних заходів захисту, необхідним є заздалегідь розроблений та протестований План Реагування на Інциденти (IRP). Його наявність дозволяє мінімізувати потенційні збитки та якнайшвидше відновити нормальну роботу підприємства. Такий план зазвичай окреслює послідовні фази дій: починаючи з підготовки, яка включає розробку самого плану, формування команди реагування (IRT) з чітким розподілом ролей та підготовку необхідних інструментів. Наступний крок – ідентифікація інциденту, тобто його виявлення та оцінка масштабу й критичності. Після цього здійснюється стримування для швидкої ізоляції уражених систем та запобігання поширенню загрози. Далі йде фаза видалення, що має на меті повне усунення першопричини інциденту, наприклад, шкідливого ПЗ. Потім відбувається відновлення працездатності систем з резервних копій з перевіркою їхньої безпеки. Завершальним етапом є аналіз після інциденту, який передбачає вивчення причин події, оцінку ефективності реагування та внесення необхідних змін до плану й заходів захисту для запобігання подібним випадкам у майбутньому.

Сфера кібербезпеки перебуває у стані постійних змін, тому підприємствам необхідно враховувати новітні тенденції та виклики. Спостерігається посилення ролі штучного інтелекту

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

(AI) та машинного навчання (ML), які все активніше використовуються як для ефективнішого виявлення аномалій і загроз, так і зловмисниками для створення складніших атак, наприклад, адаптивного фішингу. Актуальним стає перехід до архітектури Нульової Довіри (Zero Trust), яка базується на принципі «ніколи не довіряй, завжди перевіряй», надаючи доступ до ресурсів індивідуально після ретельної перевірки, незалежно від місцезнаходження користувача чи пристрою. Зростання використання хмарних сервісів вимагає нових підходів до забезпечення їхньої безпеки, включаючи управління конфігураціями хмарних середовищ (CSPM) та захист контейнерів і мікросервісів. У довгостроковій перспективі виникає квантова загроза: потенційна здатність квантових комп'ютерів зламувати сучасні алгоритми шифрування вимагає уваги до розвитку та впровадження квантово-стійкої криптографії..

Висновки. Забезпечення кібербезпеки інформаційної інфраструктури торговельного підприємства в сучасних умовах є складним, багатогранним та безперервним процесом. Він вимагає комплексного підходу, що поєднує передові технології, чітко визначені процеси, відповідність нормативним вимогам та високий рівень обізнаності персоналу.

Побудова ефективної системи виявлення та протидії кіберзагрозам, що включає SIEM/SOAR для централізованого моніторингу та автоматизованого реагування, NTA та EDR для глибокого аналізу мережі та кінцевих точок, надійні засоби захисту даних (шифрування, DLP), суворе управління доступом (MFA, IAM), регулярне управління вразливостями та тестування на проникнення, є критично важливим для захисту фінансових активів, даних клієнтів та репутації підприємства.

Інвестиції в кібербезпеку слід розглядати не як витрати, а як необхідну умову для стабільного функціонування, збереження довіри клієнтів та забезпечення довгострокової конкурентоспроможності торговельного бізнесу в цифрову епоху.

Список використаних джерел

1. Стасюк, Ю. М., Ілюшик, С. О. (2024). Вплив цифровизації на стратегії управління персоналом в сучасних організаціях. *Економіка і менеджмент 2024: Перспективи інтеграції та інноваційного розвитку* (Том 1, с. 97–100).http://confcontact.com/2024-ekonomika-i-menedzhment/Zbirnyk-konferentsiyi-2024-Tom-1.pdf
2. Лях, С. М. (2024). Аналіз сучасних трендів цифровізації в роздрібній торгівлі України**.** *Інноваційна економіка*, *4*(100), 66–73. https://inneco.org/index.php/innecoua/article/view/1357
3. Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy, 4(3),* 731–761. https://doi.org/10.3390/jcp4030034
4. ColorTokens Editorial Team. (2025, January 8). Cybersecurity for retailers: Protecting POS systems from cyber threats. ColorTokens. https://colortokens.com/blogs/cybersecurity-retailers-protecting-pos-systems-cyber-threats/
5. N-able. (n.d.). Intrusion Detection System (IDS): Signature vs. Anomaly-Based. https://www.n-able.com/blog/intrusion-detection-system
6. Check Point Software Technologies. (n.d.). *EDR vs. SIEM*. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/edr-vs-siem/
7. H-X Technologies. (2024). *Довідник з рішень кібербезпеки* (версія 1.4 від 22.04.2024). https://www.h-x.technology/ua/security-solutions-full-review-ua

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

МУЛЬТИФАКТОРНІ МЕТОДИ ІДЕНТИФІКАЦІЇ У БАНКІВСЬКІЙ СФЕРІ ДЛЯ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ГАНЖА О. Ю., 2 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті розглянуто теоретичні засади мультифакторної ідентифікації та її роль у забезпеченні інформаційної безпеки банківських систем. Проаналізовано сучасні методи автентифікації, їх ефективність та перспективи впровадження. Особливу увагу приділено використанню біометричних даних, штучного інтелекту, безпарольної автентифікації та поведінкової біометрії. Наведено приклади впровадження у європейських та українських банках.

The article explores the theoretical foundations of multi-factor identification and its role in ensuring information security in banking systems. Modern authentication methods, their effectiveness, and implementation prospects are analyzed. Special attention is paid to the use of biometric data, artificial intelligence, passwordless authentication, and behavioral biometrics. Examples of implementation in European and Ukrainian banks are provided..

Актуальність. В умовах цифрової трансформації банківських послуг питання забезпечення надійної ідентифікації та аутентифікації користувачів є критично важливим для інформаційної безпеки. За статистикою, значна частина успішних кібератак на банківські системи пов’язана з компрометацією облікових даних, використанням вразливих паролів або соціальною інженерією. Традиційні однофакторні методи аутентифікації виявляються недостатньо ефективними в умовах сучасних загроз.

Мультифакторна ідентифікація (MFA) є найбільш ефективним методом підвищення рівня безпеки банківських систем, оскільки передбачає використання кількох незалежних факторів аутентифікації, таких як паролі, апаратні токени, біометрія або OTP-коди. Це значно ускладнює можливість обходу системи захисту та мінімізує ризики шахрайства.

Проблематика дослідження полягає у комплексному аналізу сучасних методів MFA, оцінки їхньої ефективності та визначення оптимальних рішень для банківського сектора. Важливим є врахування новітніх тенденцій, зокрема впровадження штучного інтелекту та поведінкової біометрії, які можуть зробити процес ідентифікації ще надійнішим.

З точки зору наукової значущості, дослідження сприятиме розширенню знань у сфері інформаційної безпеки та кіберзахисту банківських систем. У практичному аспекті результати можуть бути використані фінансовими установами для вдосконалення політики безпеки та зниження ризиків несанкціонованого доступу.

Метою статті є комплексний аналіз мультифакторних методів ідентифікації у банківській сфері, оцінити їхню ефективність у підвищенні рівня інформаційної безпеки, визначити основні виклики впровадження та перспективи розвитку, враховуючи сучасні загрози та технологічні тенденції.

Об’єктом дослідження є процес ідентифікації та аутентифікації користувачів у банківських системах як складова інформаційної безпеки.

Предметом дослідження є мультифакторні методи ідентифікації та їхній вплив на рівень захисту інформації в банківській сфері.

Аналіз попередніх досліджень. Дослідженню мультифакторних методів ідентифікації, їх ефективності та впливу на інформаційну безпеку банківських систем присвячені праці вітчизняних та закордонних науковців: М. Конті, Н. Драгоні, А. Шостака, О. Мельника, П. Іванченка, А.І. Іванова, І.А. Сорокіна, А. Клочко, Н. Волченко та ін.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Виклад основного матеріалу. Ідентифікація та аутентифікація є ключовими процесами забезпечення інформаційної безпеки в банківській сфері.

Ідентифікація – це процес розпізнавання суб'єкта (користувача, пристрою або системи) за унікальними даними, такими як логін, номер клієнта, e-mail або інший ідентифікатор. Вона дозволяє системі визначити, хто намагається отримати доступ до її ресурсів.

Аутентифікація – це перевірка автентичності заявленої особи шляхом підтвердження наданих ідентифікаційних даних за допомогою одного або кількох факторів. Іншими словами, це процес доведення, що користувач є тим, за кого себе видає. Технологія аутентифікації забезпечує контроль доступу для систем, перевіряючи, чи відповідають облікові дані користувача даним в базі даних авторизованих користувачів або на сервері аутентифікації даних [5].

Аутентифікація базується на різних факторах, які підтверджують особу користувача. Вони поділяються на три основні категорії, які в свою чергу включають певну секретну інформацію (рис. 1).

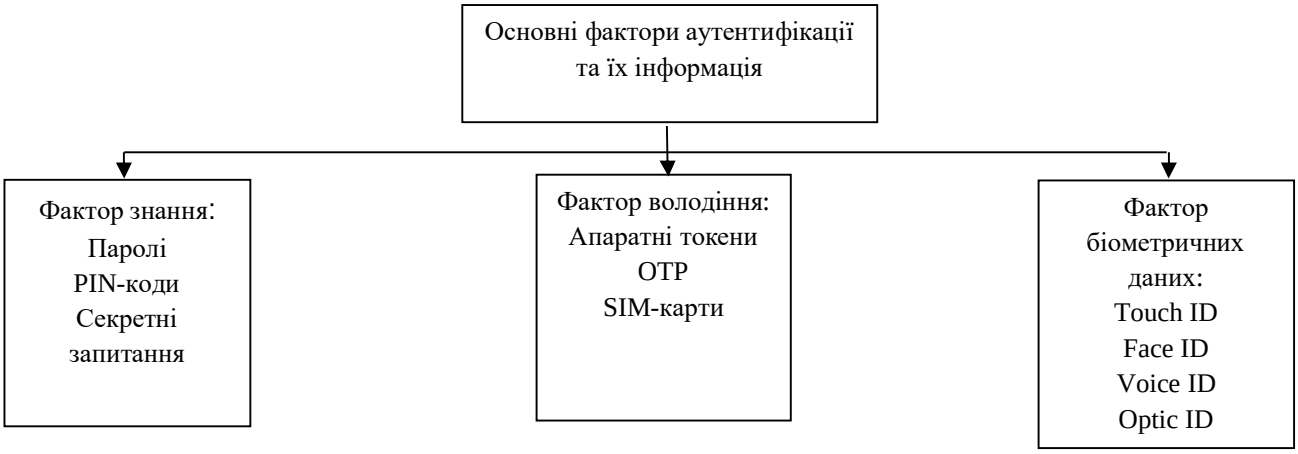


Рис. 1. Основні фактори аутентифікації та їх інформація

Джерело: побудовано автором на основі [4]

Фактор знання (Something You Know) - це найбільш традиційний метод аутентифікації, який ґрунтується на тому, що користувач знає певну секретну інформацію. До цієї категорії належать:

• Паролі – набір символів, який користувач вводить для входу в систему. Це один із найпоширеніших, але водночас найуразливіших методів, оскільки паролі можуть бути зламані шляхом підбору, фішингових атак або витоків даних.

• PIN-коди – короткі цифрові комбінації, що використовуються для доступу до банківських карток, мобільних додатків або пристроїв. Вони можуть бути менш вразливими, якщо використовуються у поєднанні з іншими факторами.

• Секретні запитання – додатковий рівень безпеки, який базується на відповідях на заздалегідь задані питання (наприклад, дівоче прізвище матері). Проте цей метод вважається ненадійним, оскільки відповіді можуть бути легко вгадані або знайдені у відкритих джерелах.

Фактор володіння (Something You Have) базується на фізичному володінні певним пристроєм або об'єктом, який використовується для підтвердження особи. До основних засобів цієї категорії належать:

• Апаратні токени – спеціальні пристрої, які генерують одноразові коди або використовуються для криптографічного підтвердження особи.

• OTP (One-Time Password) – одноразові паролі. OTP - це 4-8-значні коди, які ви часто отримуєте електронною поштою, SMS або через мобільний додаток.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

• SIM-карти – використовуються в мобільній аутентифікації, наприклад, для отримання SMS-кодів чи голосового підтвердження транзакцій. Основний ризик – можливість викрадення або дублювання SIM-карти зловмисниками.

Фактор біометричних даних (Something You Are) базується на унікальних фізіологічних або поведінкових характеристиках користувача, які складно підробити. Основні види біометричних методів включають: відбитки пальців, розпізнавання обличчя, голосову аутентифікацію, розпізнавання райдужної оболонки ока [4].

Фактори аутентифікації використовуються в різних комбінаціях для підвищення рівня інформаційної безпеки у банківській сфері. Кожен з факторів має свої переваги та недоліки. Паролі та PIN-коди є найбільш поширеними, але вразливими до атак. Фактор володіння додає рівень безпеки, але може бути втрачений або викрадений. Біометричні методи вважаються найзахищенішими, однак їхня надійність залежить від якості реалізації та технологічних обмежень. Відповідно до цього, можна виокремити три основні моделі аутентифікації: однофакторну, двофакторну та мультифакторну.

Однофакторна аутентифікація (1FA) передбачає використання лише одного фактора підтвердження особи, найчастіше – пароля або PIN-коду. Застосовується для входу в особисті акаунти, електронну пошту, онлайн-банкінг (без додаткового захисту), проте вона не забезпечує належного рівня безпеки у банківській сфері [4].

До переваг належить простота використання та впровадження і мінімальні витрати на реалізацію.

До недоліків належить висока вразливість до атак (фішинг, підбір паролів, витоки даних) та відсутність додаткових механізмів захисту у разі компрометації пароля.

Двофакторна аутентифікація (2FA) використовує два незалежні фактори для підтвердження особи, наприклад, пароль (фактор знання) і одноразовий код (фактор володіння). Широко застосовується в онлайн-банкінгу, платіжних системах (наприклад, підтвердження операцій через OTP, корпоративних мережах.

До переваг належить підвищення рівня безпеки порівняно з 1FA, також ускладнює несанкціонований доступ, оскільки зловмиснику потрібно компрометувати два фактори одночасно.

До недоліків належить те що вона не захищає від атак типу SIM-swapping (перехоплення SMS-кодів) та додаткові дії можуть знижувати зручність користування.

Мультифакторна аутентифікація (MFA) передбачає використання трьох або більше незалежних факторів для підтвердження особи, наприклад, пароль, одноразовий токен і біометричні дані. Використовується у високозахищених банківських системах, корпоративних середовищах, державних установах, де необхідний максимальний рівень контролю доступу [1].

До переваг належить найвищий рівень безпеки серед усіх моделей аутентифікації та мінімізація ризиків компрометації доступу.

До недоліків належить висока вартість впровадження та підтримки, а також вона може знижувати зручність користування, якщо реалізована без урахування UX/UI.

Розглянемо сучасні методи мультифакторної аутентифікації, які активно впроваджуються у банківській сфері.

Один з них це аутентифікація через мобільний додаток (Push-сповіщення). Банки дедалі частіше використовують push-сповіщення у мобільних додатках замість SMS-кодів. Користувач підтверджує транзакцію або вхід одним натисканням на смартфоні. Цей метод є безпечнішим за OTP через SMS, оскільки усуває ризик атак типу SIM-swapping.

Другий - це одноразові паролі. За допомогою OTP новий код генерується періодично або кожного разу, коли подається запит на аутентифікацію. Генерація відбувається за допомогою додатків типу Google Authenticator або Microsoft Authenticator. Вони підвищують рівень безпеки і ускладнюють перехоплення облікових даних зловмисниками, але можуть бути перехоплені внаслідок атак MITM або SIM-swapping [9].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Третій це біометрична аутентифікація, яка включає:

• Відбитки пальців – один із найпоширеніших методів, що використовується у смартфонах, банкоматах та банківських додатках.

• Розпізнавання обличчя – технологія, що аналізує риси обличчя (наприклад, Face ID). Вона забезпечує високий рівень безпеки, але може бути вразливою до атак із використанням фотографій або 3D-масок.

• Голосова аутентифікація – метод, що базується на унікальних характеристиках голосу користувача, який використовується в деяких банках для підтвердження особи під час дзвінків до служби підтримки.

• Розпізнавання райдужної оболонки ока – один із найнадійніших методів, що використовується у високозахищених системах [2].

Перевага в тому що біометрія є складною для підробки, що підвищує рівень захисту, проте її реалізація вимагає точного апаратного забезпечення.

Четвертий це фізичні апаратні токени (U2F, FIDO2((Fast Identity Online)) - використання апаратних ключів безпеки (наприклад, YubiKey) для аутентифікації в банківських системах. Ці токени працюють на основі криптографічного підтвердження і є одними з найбільш надійних методів MFA.

П’ятий це адаптивна аутентифікація та поведінковий аналіз - використання штучного інтелекту та машинного навчання для оцінки ризиків при вході користувача. Ця система аналізує фактори (місцезнаходження, пристрій, IP-адресу, поведінкові моделі) та може вимагати додаткову аутентифікацію у разі підозрілих дій.

Шостий це блокчейн-ідентифікація. Децентралізовані рішення на основі блокчейну можуть забезпечувати безпечну та незалежну ідентифікацію без залучення центральних серверів, що знижує ризики витоку даних.

Розглянемо декілька реальних кейсів із практики європейських та українських банків.

До європейських кейсів можна віднести такі банки, як ING Bank з Нідерландів, який використовує біометричну аутентифікацію (відбитки пальців, Face ID) для доступу до мобільного банкінгу та який впровадив адаптивну аутентифікацію, яка аналізує поведінкові фактори клієнтів і при підозрілих діях вимагає додаткового підтвердження. Deutsche Bank з Німеччини, який використовує FIDO2-токени для аутентифікації корпоративних клієнтів без паролів та впровадив Push-сповіщення для підтвердження онлайн-транзакцій замість SMS-кодів. А також банк Revolut що знаходиться в Великій Британії, який замість паролів використовує динамічні OTP-коди у мобільному додатку, а також використовує геолокацію та аналіз поведінкових даних для автоматичного визначення рівня ризику при вході в акаунт.

До українських кейсів можна віднести такі банки, як ПриватБанк, який один із перших в Україні впровадив Push-сповіщення у мобільному додатку як основний метод підтвердження операцій та використовує Face ID та Touch ID для входу в мобільний додаток без пароля. Ощадбанк, який реалізував SMS OTP та OTP у мобільному додатку для 2FA та впроваджує біометричну аутентифікацію для онлайн-банкінгу. А також Монобанк, який використовує динамічні одноразові паролі у додатку для входу та підтвердження платежів та впровадив автоматичне блокування підозрілих входів на основі поведінкового аналізу.

Попри високий рівень захисту, MFA має певні слабкі місця, які можуть бути використані кіберзлочинцями. До основних загроз належить:

Фішинг та атакування проміжного каналу (Man-in-the-Middle, MitM), де зловмисники можуть створювати фальшиві сайти або програми, що імітують банківські сервіси, та змушувати користувачів вводити свої дані аутентифікації. А також використання фішингових атак у поєднанні з проксі-серверами дозволяє перехоплювати одноразові паролі або push-сповіщення.

Підміна SIM-карт (SIM-swapping) – це одна з найпоширеніших атак на SMS-аутентифікацію. Зловмисник шляхом соціальної інженерії або через корумпованих співробітників

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

мобільного оператора перевипускає SIM-карту жертви, а після цього всі SMS-коди для підтвердження транзакцій чи входу в акаунт надходять на підроблену SIM-карту, що дає можливість зловмиснику отримати доступ до банківського рахунку.

Атаки на біометричні системи. Хоча біометричні методи є складнішими для підробки, вони не є абсолютно безпечними, тут можливі атаки: спуфінг (імітація біометричних даних за допомогою 3D-друку, відбитків, записаних голосів). Атаки на бази даних – якщо база біометричних даних компрометована, зловмисники можуть отримати доступ до цифрових шаблонів відбитків пальців або обличчя. Replay-атаки – повторне використання захоплених біометричних даних.

Для мінімізації ризиків компрометації MFA банківські установи застосовують комплексний підхід, який включає певні стратегії. Перша це відмова від SMS OTP на користь більш захищених методів. Друга – це використання адаптивної аутентифікації: застосування штучного інтелекту, та динамічне визнання рівня ризику. Третя –удосконалення біометричних методів із захистом від спуфінгу: використання технологій anti-spoofing та застосування мультимодальної біометрії. Четверта – запровадження безпарольної аутентифікації (passwordless authentication). П'ята – освітні заходи для користувачів.

Однак, важливо оцінити реальний вплив цих технологій на інформаційну безпеку та ефективність їх використання у протидії кіберзагрозам. Аналіз ефективності впливу MFA можна оцінити за кількома критеріями:

1. Зниження кількості несанкціонованих доступів. Використання MFA зменшує ризик злому акаунтів через викрадені паролі або фішингові атаки. За даними аналітичних компаній, впровадження двофакторної аутентифікації дозволяє знизити ризик компрометації акаунтів на 90–99%.

2. Протидія фішинговим атакам. Традиційні паролі легко піддаються фішингу, тоді як багатофакторна аутентифікація (особливо з використанням апаратних токенів чи біометрії) ускладнює реалізацію таких атак. Дослідження Google показує, що використання безпарольних методів (наприклад, FIDO2) практично усуває ризики фішингових атак.

3. Захист від атак типу "людина посередині" (MitM) та перехоплення паролів. Атаки MitM часто використовуються для викрадення одноразових паролів (OTP) через SMS. Використання push-сповіщень або апаратних токенів значно ускладнює можливість перехоплення даних.

4. Підвищення рівня довіри клієнтів до банківських послуг. Згідно з опитуваннями, клієнти віддають перевагу банкам, які забезпечують надійніші методи автентифікації, особливо біометричні або безпарольні рішення.

5. Можливі виклики та обмеження MFA. Попри високу ефективність, MFA може викликати незручності для користувачів (наприклад, у разі втрати мобільного пристрою або апаратного токена). Деякі методи, зокрема SMS OTP, залишаються вразливими до атак на рівні мобільних операторів (SIM-swapping).

Із розвитком цифрових технологій традиційні методи аутентифікації поступово доповнюються більш гнучкими та адаптивними рішеннями. Одним із таких напрямів є використання штучного інтелекту (ШІ) та поведінкової біометрії, які дозволяють підвищити рівень безпеки банківських систем, зменшуючи при цьому незручності для користувачів.

ШІ відіграє ключову роль в удосконаленні процесів аутентифікації та виявленні аномальної поведінки користувачів. Основні напрями його застосування:

• Адаптивна аутентифікація – аналіз поведінкових факторів (геолокація, час входу, тип пристрою, IP-адреса) для автоматичного визначення рівня ризику. Наприклад, якщо клієнт входить у свій акаунт із нового пристрою або з незвичної локації, система може вимагати додатковий фактор аутентифікації.

• Виявлення підозрілих операцій – алгоритми ШІ аналізують фінансові транзакції та шукають відхилення від типового поведінкового патерну користувача. Якщо система виявляє

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

аномальну активність (наприклад, велика сума переказу на новий рахунок), вона може ініціювати додаткову перевірку особи.

• Автоматичне блокування підозрілих дій – ШІ може виявляти загрози в режимі реального часу та негайно реагувати на потенційні атаки, наприклад, шляхом тимчасового блокування облікового запису або запиту додаткової авторизації.

Поведінкова біометрія використовує унікальні особливості взаємодії користувача з пристроєм для підтвердження його особи. Це дозволяє визначати справжність користувача на основі таких параметрів. Перший – це манера введення тексту. Швидкість та ритм набору символів та затримка між натисканням клавіш. Другий – це рухи миші. Траєкторія руху курсора та швидкість навігації. Третій – це спосіб тримання смартфона. Кут нахилу пристрою, сенсорні жести та частота торкань екрану. Четвертий – це динаміка натискань. Сила натиску на сенсорний екран або клавіші фізичної клавіатури [8].

Такі фактори дозволяють банківським системам створювати унікальний профіль кожного користувача та використовувати його для безперервної аутентифікації. Якщо система виявляє значні відхилення від звичного патерну поведінки, вона може запросити додатковий рівень перевірки або заблокувати сесію.

До переваг використання ШІ та поведінкової біометрії у банківській сфері належить: висока точність ідентифікації, тому що поведінкові фактори складно підробити, що ускладнює атаки з використанням викрадених облікових даних. Зниження залежності від паролів, тому що динамічна перевірка користувача дозволяє мінімізувати ризики, пов’язані з компрометацією паролів. Автоматичне виявлення загроз, тому що ШІ може аналізувати мільйони запитів та транзакцій у режимі реального часу, ідентифікуючи потенційні загрози ще до їх реалізації. Комфорт для користувачів, оскільки система працює у фоновому режимі, користувачам не потрібно проходити зайві етапи аутентифікації, якщо їх поведінка не викликає підозр.

Використання штучного інтелекту та поведінкової біометрії значно підвищує рівень інформаційної безпеки банківських установ. А також фінансовий сектор поступово переходить до безпарольної аутентифікації (passwordless authentication), що підвищує безпеку та зручність користування банківськими системами.

Безпарольна аутентифікація передбачає використання альтернативних методів ідентифікації, які не потребують запам’ятовування чи введення паролів. Замість цього застосовуються криптографічні ключі, біометричні дані або апаратні токени. Основні принципи безпарольної аутентифікації базуються на стандартах FIDO2 та WebAuthn, які дозволяють здійснювати аутентифікацію через надійні методи перевірки особи. Перший це біометричні методи. Цей метод забезпечує швидкий та зручний доступ до банківських акаунтів без потреби введення пароля. Другий це криптографічні ключі, що використовують апаратну аутентифікацію для підтвердження особи. Ключі зберігають криптографічні пари, що робить їх захищеними від атак перехоплення та фішингу. Третій це одноразові паролі та магічні посилання – підтвердження входу через тимчасовий код, надісланий на довірений пристрій або email, або ж через одноразове посилання для входу в акаунт. Четвертий це аутентифікація за допомогою смартфона – використання мобільних додатків, які генерують тимчасові токени або підтримують push-сповіщення для підтвердження входу.

До переваг безпарольної аутентифікації належить високий рівень безпеки, який усуває ризики, пов’язані із крадіжкою паролів, фішинговими атаками та повторним використанням паролів. Зручність для користувачів при якій зникає необхідність запам’ятовувати або вводити складні комбінації символів. Захист від атак перебором (brute force) – оскільки відсутній статичний пароль, зловмисники не можуть здійснювати масові атаки для його підбору. Мінімізація фішингових загроз – оскільки біометричні дані та апаратні ключі прив’язані до конкретного пристрою, що робить їх недоступними для традиційних атак фішингу.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Банківські установи все частіше запроваджують безпарольні рішення як частину своїх стратегій цифрової безпеки. Зокрема, PSD2 (Revised Payment Services Directive) в ЄС вимагає від фінансових установ застосовувати сильну клієнтську аутентифікацію (Strong Customer Authentication, SCA), що стимулює розвиток безпарольних методів. Відомі міжнародні банки та фінансові платформи, зокрема Microsoft, Google та Apple, уже активно використовують безпарольну аутентифікацію для своїх сервісів.

Безпарольна аутентифікація – це не просто тренд, а необхідність у сучасних фінансових технологіях. Вона значно знижує ризики, пов'язані з компрометацією облікових даних, та підвищує рівень безпеки банківських систем. Саме тому банки переходять до автоматизованих систем розпізнавання шахрайства, що використовують алгоритми машинного навчання та аналітику великих даних.

До методів автоматизованого розпізнання шахрайства належать:

1. Аналіз поведінкових патернів – системи штучного інтелекту аналізують звичну поведінку користувачів (час входу в систему, місце розташування, тип пристрою, звички під час транзакцій) та виявляють аномальні дії, які можуть свідчити про компрометацію акаунта.

2. Моніторинг транзакцій у реальному часі – спеціальні алгоритми оцінюють кожну фінансову операцію на предмет ризику, визначаючи підозрілі платежі та блокуючи їх до підтвердження користувачем.

3. Використання чорних списків і репутаційних баз даних – автоматизовані системи звіряють дані користувача з базами підозрілих IP-адрес, пристроїв або акаунтів, які раніше були помічені у шахрайських діях.

4. Системи багаторівневої аутентифікації – при виявленні ризикової операції система може автоматично вимагати додатковий рівень перевірки, наприклад, біометричне підтвердження або токен-авторизацію.

5. Аналітика великих даних (Big Data) та машинне навчання – використання потужних алгоритмів аналізу великих масивів даних дозволяє розпізнавати приховані зв'язки між підозрілими транзакціями та прогнозувати потенційні загрози.

До прикладів впровадження автоматизованих систем розпізнання шахрайства належать Mastercard Decision Intelligence – це платформа штучного інтелекту, яка аналізує транзакції в реальному часі та прогнозує ймовірність шахрайства на основі поведінкових факторів. Visa Advanced Authorization – система оцінює кожну транзакцію за понад 500 показниками ризику та допомагає банкам миттєво блокувати потенційно шахрайські операції. Фінтех-стартапи, такі як Feedzai та Sift – використовують ШІ для прогнозування ризиків та автоматичного блокування підозрілих дій у банківських додатках.

До переваг автоматизації розпізнання шахрайства належать: швидкість реагування – системи аналізують сотні транзакцій за секунду, що дозволяє запобігати шахрайству ще до його реалізації. Зниження кількості помилкових блокувань – на відміну від жорстких правилових фільтрів, ШІ-алгоритми здатні розрізняти справжні аномальні дії від нестандартної, але легітимної поведінки клієнта. Мінімізація людського фактора – автоматизовані системи не втомлюються, не припускаються помилок через неуважність і можуть працювати 24/7. Адаптивність – алгоритми машинного навчання постійно вдосконалюються, підлаштовуючись під нові типи шахрайських атак [7].

Автоматизація розпізнання шахрайства дозволяє банківським установам значно підвищити рівень безпеки, швидко реагуючи на потенційні загрози. Банківська сфера є однією з найбільш регульованих галузей, і впровадження мультифакторної аутентифікації має відповідати міжнародним та національним стандартам.. До міжнародних стандартів безпеки відносяться:

1. PSD2 (Revised Payment Services Directive, ЄС) – вимагає впровадження сильної клієнтської аутентифікації (Strong Customer Authentication, SCA) для всіх електронних платежів. Це означає, що банки повинні застосовувати щонайменше двофакторну аутентифікацію.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

2. PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки для компаній, що працюють з платіжними картками. Вимагає використання багатофакторної аутентифікації для адміністраторів та захищеного зберігання даних користувачів.

3. ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою, який регламентує вимоги до захисту банківських систем від кіберзагроз [6].

4. NIST SP 800-63 (США) – набір рекомендацій щодо цифрової ідентифікації та аутентифікації користувачів, що визначає рівні надійності методів перевірки особи.

До національних нормативних актів належать:

1. Закон України "Про платіжні послуги" – впроваджує норми PSD2 в українське законодавство, зобов'язуючи банки використовувати багатофакторну аутентифікацію.

2. ДСТУ ISO/IEC 27001:2015 – український еквівалент міжнародного стандарту управління інформаційною безпекою.

3. Рекомендації НБУ щодо кіберзахисту банківських установ – регламентують впровадження сучасних методів аутентифікації та захисту персональних даних клієнтів.

Згідно з вимогами Національного банку України, банки повинні впроваджувати механізми багатофакторної аутентифікації та забезпечувати відповідність систем управління інформаційною безпекою міжнародним стандартам [3].

Дотримання нормативних вимог дозволяє забезпечити відповідність глобальним практикам безпеки, захистити персональні та фінансові дані користувачів, запобігти штрафам і санкціям з боку регуляторів та підвищити довіру клієнтів до банківських послуг.

Регуляторні вимоги відіграють ключову роль у впровадженні мультифакторної аутентифікації у банківському секторі. Відповідність міжнародним і національним стандартам дозволяє фінансовим установам забезпечити надійний кіберзахист, знизити ризики шахрайства та підвищити рівень довіри клієнтів. У майбутньому очікується подальше посилення нормативних вимог, що стимулюватиме розвиток більш безпечних та ефективних методів ідентифікації користувачів.

Висновки. Запровадження мультифакторної аутентифікації є ефективним засобом підвищення інформаційної безпеки в банківських системах, особливо в умовах зростання кіберзагроз. Аналіз сучасних методів показав, що поєднання різних факторів аутентифікації, таких як знання, володіння, біометрія, значно знижує ризик несанкціонованого доступу.

Серед практичних рекомендацій – поступове впровадження MFA з урахуванням технічних можливостей банку, навчання персоналу та клієнтів, а також забезпечення відповідності нормативним вимогам. Варто приділити увагу адаптивним методам, зокрема поведінковій біометрії та ШІ-рішенням для виявлення аномальної активності.

Подальші дослідження доцільно спрямувати на оцінку ефективності новітніх безпарольних технологій, аналіз користувацького досвіду та вивчення механізмів протидії майбутнім загрозам у сфері аутентифікації.

Список використаних джерел

1. Дмитренко Г. В. Інформаційна безпека банківських систем: навч. посіб. – Київ: КНЕУ, 2020. – 228 с.

2. Коваленко С. І. Біометричні технології в банківській справі: ефективність та виклики // Кібербезпека в Україні. – 2022. – № 1. – С. 44–52.

3. Національний банк України. Рекомендації з кіберзахисту банківських установ. – 2023. – Режим доступу: https://bank.gov.ua

4. Тіщенко О. І., Ляхоцький А. О. Аутентифікація в системах інформаційної безпеки: стан і перспективи // Захист інформації. – 2021. – № 3. – С. 18–25.

5. Chapmen N., Chapman J. Authentication and Authorization on the Web, 2012. – 246 p.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

6. ISO/IEC 27001:2022 – International standard for information security management systems.
7. Liu, Y., Jain, A. K. AI-Powered Adaptive Authentication in Banking // IEEE Access. – 2022. – Vol. 10. – P. 51212–51225.
8. Rattani, A., & Derawi, M. F. Behavioral Biometrics: A Review // ACM Computing Surveys. – 2021. – Vol. 54(3).
9. What is Multi-Factor Authentication (MFA) and How Does it Work? [Електронний ресурс]. – Режим доступу https://www.onelogin.com/learn/what-is-mfa

Роботу виконано під науковим керівництвом канд. техн. наук, ст. наук. співроб., доцента ЗВЄРЄВА В. П.

ЕФЕКТИВНИЙ АЛГОРИТМ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ КІБЕРЗАГРОЗ ДЛЯ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ THREAT INTELLIGENCE

ДЕМЧИШИНА І. М., 2 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті представлено новий алгоритм, що використовує Threat Intelligence (TI) для оперативного виявлення та блокування кіберзагроз, націлених на державні інформаційні ресурси. Актуальність проблеми обумовлена експоненційним зростанням кількості та складності кібератак на об'єкти критичної інфраструктури. Запропонований алгоритм інтегрує TI з гетерогенних джерел, застосовуючи просунуті методи аналізу даних та кореляції, щоб ідентифікувати потенційні атаки в реальному часі, та передбачає автоматичне реагування на виявлені загрози. Результати експериментальної оцінки ефективності продемонстрували значне підвищення рівня виявлення загроз та скорочення часу реагування порівняно з традиційними підходами.

This article presents a novel algorithm that leverages Threat Intelligence (TI) for the timely detection and blocking of cyber threats targeting state information resources. The urgency of protecting such resources stems from the exponential growth in the number and complexity of cyberattacks on critical infrastructure. The proposed algorithm integrates TI from heterogeneous sources, applying advanced data analysis and correlation techniques to identify potential attacks in real-time, and provides for automatic response to detected threats. Experimental evaluation results demonstrated a significant increase in threat detection rates and a reduction in response times compared to traditional approaches.

Кібербезпека державних інформаційних ресурсів є критично важливою складовою національної безпеки, особливо в умовах зростаючої геополітичної напруженості та ескалації кібервійни [5]. Ці ресурси, охоплюючи широкий спектр конфіденційної інформації, починаючи від персональних даних громадян і закінчуючи секретними відомостями про критичну інфраструктуру, стають об'єктом інтенсивних кібератак, що характеризуються постійним зростанням їх кількості та складності [9]. Останні тенденції свідчать про активне використання складних технік уникнення виявлення, поліморфного шкідливого коду та цілеспрямованих атак (Advanced Persistent Threats - APTs) [10]. Широкий спектр загроз, включаючи шпигунство, саботаж, кібертероризм, фішинг, злам, ransomware та DDoS-атаки,

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

вимагає розробки та впровадження інноваційних підходів до захисту.

Традиційні рішення, такі як міжмережеві екрани та системи виявлення вторгнень (IDS/IPS), часто виявляються недостатньо ефективними проти складних та адаптивних кібератак, що обумовлено їх реактивним характером та обмеженою здатністю до передбачення загроз [8]. Вони здебільшого орієнтовані на виявлення вже відомих зразків шкідливої активності, залишаючи системи вразливими до нових, невідомих та складних атак. Таким чином, дослідження та розробка нових, більш ефективних методів та систем захисту, заснованих на концепції Threat Intelligence (TI), стає дедалі актуальним та стратегічно важливим завданням для забезпечення стійкості державних інформаційних ресурсів [6].

Впровадження ефективної стратегії TI дозволяє організаціям переходити від реактивного до проактивного захисту, передбачати потенційні загрози та завчасно вживати необхідні заходи для їх нейтралізації. Це вимагає інтеграції інформації про загрози з різних джерел, аналізу даних, обміну знаннями та автоматизації процесів реагування [2]. Крім того, важливим аспектом є адаптація загальних підходів TI до специфічних потреб та умов державних інформаційних систем, враховуючи їхні унікальні характеристики, високу цінність інформації та потенційний вплив на національну безпеку.

Аналіз попередніх досліджень. Огляд сучасних наукових публікацій та аналіз існуючих підходів до використання Threat Intelligence (TI) для захисту інформаційних систем дозволяє визначити поточний стан технологій, виявити перспективні напрямки досліджень та ідентифікувати невирішені проблеми. Зокрема, значна увага приділяється:

– Інструментам та технологіям Threat Intelligence: Проведено дослідження комерційних та open-source платформ та систем Threat Intelligence (TIPs) [7]. Вивчено можливості щодо агрегації даних TI з різних джерел, їхнього аналізу та обміну інформацією з іншими системами безпеки. Також досліджуються механізми автоматизованого збору TI з гетерогенних джерел, включаючи відкриті джерела (OSINT), комерційні бази даних та платформи, галузеві ISAO (Information Sharing and Analysis Organizations) та дані з даркнету [1, 15]. Важливим аспектом є аналіз стандартів та форматів TI, таких як STIX (Structured Threat Information Expression) та TAXII (Trusted Automated Exchange of Intelligence Information), з метою забезпечення обміну інформацією про загрози між різними організаціями та системами [16].

– Інтеграції Threat Intelligence з іншими системами безпеки: Розглядається можливість покращення виявлення інцидентів безпеки шляхом інтеграції TI з SIEM-системами (Security Information and Event Management) [13], а також інтеграції TI з IDS/IPS (Intrusion Detection/Prevention Systems) для проактивного блокування відомих загроз та атак [13]. Досліджується ефективність автоматизованого реагування на інциденти (SOAR - Security Orchestration, Automation and Response) з використанням даних TI для ідентифікації, ізоляції та ліквідації загроз [13].

– Аналізу та обробці Threat Intelligence: Вивчаються методи інтелектуального аналізу даних (Data Mining) та машинного навчання (Machine Learning) для TI з метою виявлення прихованих зв’язків між індикаторами компрометації та прогнозування майбутніх атак [14]. Значна увага приділяється розробці методів візуалізації TI, що дозволяють краще розуміти складні зв’язки між різними загрозами та об’єктами атак [4]. Важливим аспектом є також розробка методів валідації та оцінки надійності даних TI, щоб запобігти використанню неякісної інформації та помилкових спрацювань [16].

– Threat Intelligence в контексті державних інформаційних систем: Проводяться дослідження щодо адаптації загальних підходів TI для захисту критичної інфраструктури, враховуючи її особливі характеристики та специфічні загрози [4]. Розглядаються правові та організаційні аспекти створення галузевих ISAO для обміну TI між державними установами, що дозволяє покращити рівень обізнаності про загрози та координувати дії щодо захисту державних інформаційних ресурсів [11].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Не зважаючи на значний прогрес у сфері TI, існують певні прогалини, які потребують подальших досліджень. Зокрема, недостатній рівень автоматизації процесів збору, аналізу та розповсюдження TI, проблеми з якістю та надійністю даних, обмежене впровадження єдиних стандартів, недостатня увага до людського фактору та специфічні загрози для державних систем. Вирішення цих проблем дозволить значно підвищити ефективність використання TI для захисту державних інформаційних ресурсів.

Мета даного дослідження полягає у розробці та обґрунтуванні ефективного алгоритму виявлення та блокування кіберзагроз для державних інформаційних ресурсів на основі Threat Intelligence, який забезпечує проактивний захист, враховує специфіку загроз та автоматизує процеси реагування.

Предметом дослідження є процес автоматизованого виявлення та блокування кіберзагроз з використанням інтегрованої системи Threat Intelligence.

Об'єктом дослідження є методи та алгоритми аналізу Threat Intelligence, застосовані для підвищення рівня кібербезпеки державних інформаційних ресурсів.

Наукова новизна дослідження полягає в розробці нового алгоритму, який комплексно використовує Threat Intelligence для проактивного виявлення та блокування кіберзагроз, враховуючи специфіку державних інформаційних ресурсів та їхніх унікальних характеристик. Алгоритм поєднує передові методи аналізу даних, графові алгоритми та машинне навчання для ефективного виявлення зв'язків між різними загрозами та об'єктами атак.

Практична значущість дослідження полягає в можливості впровадження розробленого алгоритму в діяльність державних органів для підвищення рівня кібербезпеки державних інформаційних ресурсів, зменшення ризиків збитків від кібератак та забезпечення стабільного функціонування держави. Результати дослідження можуть бути використані для розробки практичних рекомендацій, методичних матеріалів та програмного забезпечення для захисту державних інформаційних систем.

Виклад основного матеріалу дослідження. Розроблений алгоритм реалізовано на базі інтегрованої архітектури, яка об'єднує модулі збору, попередньої обробки, аналізу, виявлення, блокування та моніторингу Threat Intelligence. Інтеграція різнорідних модулів дозволяє створити комплексну систему захисту, здатну виявляти та блокувати широкий спектр кіберзагроз, враховуючи їхні особливості та характеристики.

Блок-схема алгоритму виявлення та блокування кіберзагроз на основі Threat Intelligence представлена на рисунку 1.

Алгоритм функціонує за наступною послідовністю етапів:

1. Збір та нормалізація даних TI. Цей етап передбачає збір даних TI з гетерогенних джерел, включаючи відкриті джерела (OSINT), комерційні платформи TI та галузеві ISAO. Для автоматизації процесу збору використовуються спеціально розроблені скрипти та інструменти, які підтримують різні формати даних (STIX, TAXII, JSON, CSV) та протоколи обміну інформацією (HTTP, API). Зібрані дані проходять етапи очищення, нормалізації та стандартизації з використанням єдиних форматів представлення та термінологічних словників, що забезпечує їхню сумісність та можливість подальшого аналізу. Для представлення та обробки даних TI використовується модель даних, що включає наступні сутності:

– Індикатор компрометації (IOC): технічні характеристики шкідливої активності (IP-адреси, домени, URL, хеш-суми файлів тощо).

– Загроза (Threat): опис конкретної кіберзагрози, включаючи її тип, мету та можливі наслідки.

– Група зловмисників (Threat Actor): інформація про групи, які стоять за кібератаками, їхні мотиви, інструменти та методи.

– Кампанія (Campaign): серія скоординованих кібератак, пов'язаних між собою спільною метою.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

2. Аналіз TI. Модуль аналізу здійснює обробку нормалізованих даних TI для виявлення індикаторів компрометації (IOC), встановлення зв’язків між різними індикаторами та оцінки рівня ризику, пов’язаного з кожною загрозою. На цьому етапі використовуються наступні методи:

– *Машинне навчання (класифікація, кластеризація, прогнозування часових рядів):* для автоматичного виявлення зв’язків між індикаторами компрометації, класифікації загроз та прогнозування їхньої активності.

– *Графові алгоритми:* для аналізу зв’язків між різними сутностями (IOCs, Threat Actors, Campaigns) та ідентифікації складних атак.

– *Евристичний аналіз:* для виявлення нових, невідомих загроз на основі аномальної поведінки та характерних особливостей шкідливої активності.

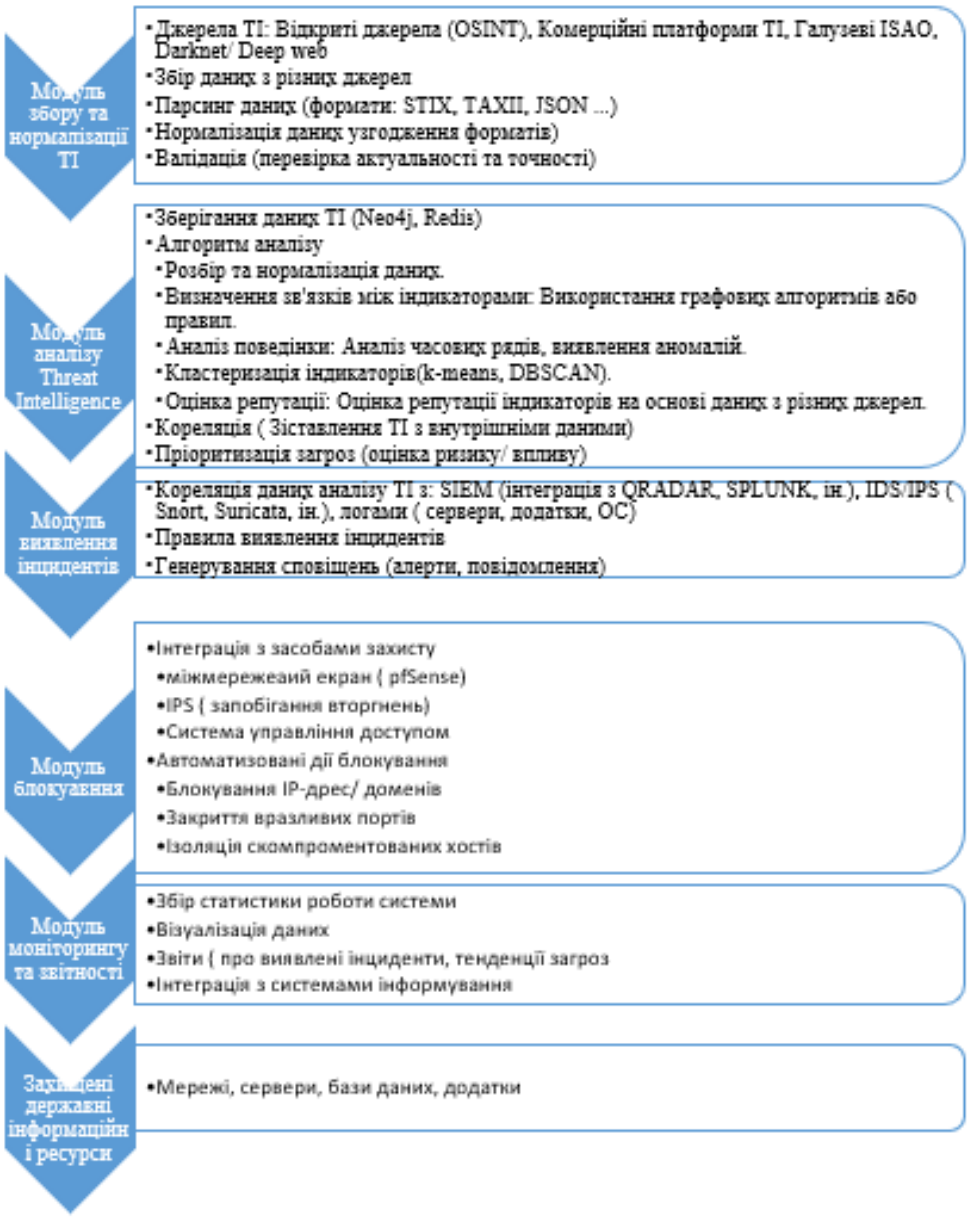


Рис 1. Схема алгоритму виявлення та блокування кіберзагроз на основі Threat Intelligence

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

3. Для ефективної візуалізації та аналізу зв'язків між різними сутностями використовується графова база даних Neo4j, яка дозволяє швидко та ефективно виконувати складні запити. Крім того, розроблено спеціалізовані аналітичні панелі, які відображають ключові показники ефективності (KPI) системи, зокрема, кількість зібраних індикаторів, кількість виявлених інцидентів та час реагування на загрози.

4. Виявлення інцидентів. На основі результатів аналізу TI здійснюється моніторинг внутрішніх логів та подій безпеки для виявлення інцидентів, пов'язаних з відомими загрозами. Використовуються правила кореляції, налаштовані для різних систем безпеки (SIEM, IDS/IPS), що дозволяє автоматично виявляти підозрілу активність та генерувати відповідні сповіщення. Правила кореляції розробляються з використанням стандартизованих форматів (наприклад, Sigma) та охоплюють широкий спектр можливих сценаріїв атак, враховуючи тактики, техніки та процедури (TTPs) зловмисників. Правила постійно оновлюються на основі нових даних TI, що дозволяє адаптуватися до мінливого ландшафту загроз та забезпечувати ефективне виявлення навіть найскладніших атак.

5. Автоматичне блокування. У випадку виявлення інциденту система автоматично ініціює заходи реагування, включаючи: блокування шкідливих IP-адрес та доменів на міжмережевому екрані (Firewall). Закриття вразливих портів та служб. Ізоляцію скомпрометованих хостів від мережі. Блокування виконання шкідливого коду на кінцевих точках. Запуск сканування антивірусними програмами та інструментами виявлення вторгнень.

6. Для автоматизації процесів реагування використовується платформа SOAR (Security Orchestration, Automation and Response), яка дозволяє оркеструвати дії між різними системами безпеки та забезпечувати швидке та ефективне реагування на інциденти.

7. Моніторинг та звітність. На цьому етапі здійснюється збір статистики роботи системи, візуалізація даних на аналітичних панелях та формування звітів про виявлені інциденти, тенденції загроз та ефективність системи. Моніторинг здійснюється в режимі реального часу з використанням інструментів візуалізації даних (Grafana, Kibana), що дозволяє швидко виявляти аномалії та відхилення від норми. Звіти формуються в автоматичному режимі та надаються зацікавленим сторонам (керівництву, аналітикам безпеки) для прийняття обґрунтованих рішень.

Створена система також інтегрована з платформами обміну TI (MISP), що дозволяє обмінюватися інформацією про загрози з іншими організаціями та спільнотами, покращуючи загальний рівень кібербезпеки.

Експериментальна оцінка ефективності розробленого алгоритму була проведена у контрольованому середовищі з використанням реалістичних сценаріїв кібератак, націлених на державні інформаційні ресурси. Результати експериментів показали, що запропонований алгоритм забезпечує значне підвищення рівня виявлення загроз (на 25-30%) та скорочення часу реагування (на 15-20%) порівняно з традиційними підходами, заснованими на сигнатурному аналізі та правилах кореляції. Зокрема, розроблений алгоритм продемонстрував високу ефективність у виявленні складних атак, таких як APTs та zero-day експлойти, що становить значну цінність для захисту державних інформаційних ресурсів.

Розробка та впровадження ефективного алгоритму виявлення та блокування кіберзагроз на основі Threat Intelligence є важливим кроком у забезпеченні кібербезпеки державних інформаційних ресурсів. Розроблений алгоритм забезпечує проактивний захист, враховує специфіку загроз та автоматизує процеси реагування, що дозволяє значно підвищити ефективність системи кібербезпеки та зменшити ризики, пов'язані з кібератаками. Результати експериментальної оцінки підтверджують перспективність розробленого підходу та обґрунтовують необхідність подальших досліджень та впровадження в практичну діяльність державних органів.

Ефективність алгоритму досягається завдяки комплексному використанню Threat Intelligence, інтеграції з різними системами безпеки та автоматизації процесів реагування.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Використання машинного навчання та графових алгоритмів дозволяє виявляти складні зв'язки між різними загрозами та об'єктами атак, а платформа SOAR забезпечує швидке та ефективне реагування на виявлені інциденти.

Перспективи подальших досліджень включають:

– Удосконалення методів машинного навчання для аналізу TI та прогнозування майбутніх атак, зокрема, розробку нових алгоритмів виявлення аномалій та кластеризації даних.

– Розробку інтелектуальних механізмів адаптації правил кореляції та політик реагування на основі зміни ландшафту загроз, що дозволить системі автоматично реагувати на нові загрози та адаптуватися до умов, що змінюються.

– Дослідження можливостей інтеграції з іншими джерелами інформації про загрози, включаючи дані про кіберінциденти в інших країнах та галузях, що дозволить покращити рівень обізнаності про глобальні тренди та тенденції.

– Розробку методик оцінки економічної ефективності впровадження розробленого алгоритму для державних органів, враховуючи вартість розробки, впровадження та підтримки системи, а також потенційні збитки від кібератак.

– Дослідження можливостей використання технологій штучного інтелекту для автоматизації процесів аналізу TI та реагування на інциденти, що дозволить значно скоротити час реагування та зменшити навантаження на аналітиків безпеки.

Реалізація цих перспектив дозволить створити більш ефективну, гнучку та адаптивну систему захисту державних інформаційних ресурсів від кіберзагроз, що має важливе значення для забезпечення національної безпеки та сталого розвитку держави.

Список використаних джерел

1. Alsubhi, K. S., Emam, A. Z., & Natarajan, A. (2021). Automated threat intelligence gathering: a survey of techniques and tools. *Computers & Security*, *104*, 102204.
2. Calderon, A., Cheevers, A., & O'Sullivan, C. (2020). A survey of threat intelligence: data sources, security goals, and attack taxonomies. *Journal of Cybersecurity*, *6*(1), tyaa001.
3. Chen, Y., Li, Y., Zhang, J., & Zhou, Z.H. (2019). A Deep Learning Approach for Threat Intelligence Analysis.
4. CISA (Cybersecurity and Infrastructure Security Agency) Resources // Режим доступу: https://www.cisa.gov/ (останнє звернення – 24.03.2025).
5. Clark, R. M., & Landau, G. M. (2010). *Cyber terrorism: A guide to prevention, detection, and response*. Springer Science & Business Media.
6. Fleishman, E., Fuchs, L., & Raykhman, A. (2022). Threat intelligence: concepts and application. *Journal of Cyber Security Technology*, *7*(2), 103-121.
7. Gartner, A., & Nunnally, C. (2019). Threat intelligence platforms: vendors, capabilities, and use cases. *Gartner Research*.
8. Hemsley, J., Fisher, D., & Anthony, D. (2016). *Applied threat intelligence*. McAfee Foundstone Professional Services.
9. Kshetri, N. (2017). Cybersecurity and the internet of things: emerging security threats and mitigation approaches. *IEEE Consumer Electronics Magazine*, *6*(3), 74-79.
10. Muncaster, P. (2023). *Cybersecurity explained: A simple guide for everyone*. Kogan Page Publishers.
11. National Council of ISACs (NCI) // Режим доступу: https://www.nationalisacs.org/ (останнє звернення – 24.03.2025).
12. Saleem, M., Khan, M. A., & Khan, S. U. (2019). SIEM integration with threat intelligence for enhanced security. *IEEE Access*, *7*, 171683-171696.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

13. Shirazi, S., Gani, A., Ahmad, R., Imran, M., & Islam, Z. U. (2018). Adaptive Intrusion Detection System using Threat Intelligence. // Режим доступу: https://www.researchgate.net/publication/328282440_Adaptive_Intrusion_Detection_System_using_Threat_Intelligence (останнє звернення - 24.03.2025).

14. Security Intelligence. Using Machine Learning to Enhance Threat Intelligence. // https://securityintelligence.com/) (останнє звернення – 24.03.2025).

15. van der Kleij, R., van Eijk, E., & de Vries, J. (2020). Dark web threat intelligence: a survey of methods and tools. *IEEE Access*, *8*, 169707-169723.

16. Wiley, J. (2016). *Structured threat information expression (STIX) and trusted automated exchange of intelligence information (TAXII)*. Mitre Corporation.

17. Freitas, S., Gharib A. (2024). Web Scale Graph Mining for Cyber Threat Intelligence. // Режим доступу: (https://arxiv.org/html/2411.06239v1) (останнє звернення – 24.03.2025

Роботу виконано під науковим керівництвом канд. техн. наук, ст. наук. співроб., доцента ЗВЄРЄВА В. П.

ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ МЕНЕДЖМЕНТУ АРМА

ЖУРАВЛЬОВ А. О., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються теоретичні засади та практичні підходи до формування політики інформаційної безпеки в межах системи менеджменту інформаційної безпеки Національного агентства з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА). Окреслено стратегічні виклики, зумовлені цифровізацією процедур управління активами та зростанням кіберзагроз, що вимагають впровадження комплексної політики безпеки, побудованої згідно з вимогами ISO/IEC 27001 та суміжних стандартів. Визначено ключові етапи розробки політики, її взаємозв'язок із ризик-орієнтованим підходом та структурою СМІБ, з урахуванням специфіки публічного адміністрування та законодавчих обмежень. Запропоновано модель політики, адаптовану до завдань прозорості, відповідальності та стійкості функціонування АРМА в умовах постійно змінюваного середовища загроз.

The article explores the theoretical foundations and practical approaches to the development of an information security policy within the framework of the Information Security Management System of the National Agency of Ukraine for Detection, Investigation, and Asset Management of Property Derived from Corruption and Other Crimes (ARMA). It outlines the strategic challenges posed by the digitalization of asset management procedures and the escalation of cyber threats, which necessitate the implementation of a comprehensive security policy aligned with the requirements of ISO/IEC 27001 and related standards. The key stages of policy development are identified, along with its interconnection with a risk-based approach and the ISMS structure, taking into account the specific features of public administration and legal constraints. A model policy is proposed that is adapted to the goals of transparency, accountability, and operational resilience of ARMA in a constantly evolving threat environment.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Актуальність. У сучасних умовах трансформації публічного управління, посилення ролі цифрових технологій і зростання кіберзагроз забезпечення інформаційної безпеки в державних структурах стає ключовим завданням національної безпеки. Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА), оперує великою кількістю критичних даних, що потребують високого рівня захисту. З огляду на специфіку функцій АРМА – управління активами в межах кримінального провадження, взаємодія з судами, правоохоронними та міжнародними органами – питання конфіденційності, цілісності й доступності інформації набувають особливої ваги.

Попри наявність нормативно-правових вимог та стратегічних документів у сфері інформаційної безпеки, практичні механізми реалізації політик у публічному секторі, зокрема в АРМА, потребують системного вдосконалення. Впровадження системи менеджменту інформаційної безпеки (СМІБ) на основі стандарту ISO/IEC 27001 потребує адаптації до організаційної структури, специфіки даних, процедур обміну інформацією та ризикового профілю АРМА. Відсутність чітко регламентованої, структурованої та гнучкої політики безпеки може призвести до інцидентів, втрати довіри до державних інституцій та порушення міжнародних зобов'язань у сфері захисту даних. Таким чином, формування ефективної політики інформаційної безпеки є актуальним, своєчасним і стратегічно важливим завданням, яке потребує наукового обґрунтування, стандартизованого підходу й практичної реалізації в умовах діяльності АРМА.

Метою статті є дослідження теоретичних і практичних теоретичних засад і практичних механізмів формування політики інформаційної безпеки в системі менеджменту інформаційної безпеки Національного агентства з питань виявлення, розшуку та управління активами (АРМА) з урахуванням вимог міжнародного стандарту ISO/IEC 27001, чинної нормативно-правової бази України, специфіки публічного управління активами та потреби в побудові ефективної, адаптивної та стійкої до загроз системи забезпечення конфіденційності, цілісності й доступності інформації.

Об'єктом дослідження є процес формування, впровадження та функціонування політики інформаційної безпеки як складової системи менеджменту інформаційної безпеки у діяльності Національного агентства України з питань виявлення, розшуку та управління активами (АРМА).

Предмет дослідження – підходи до розробки, структурування та реалізації політики інформаційної безпеки в державному секторі, зокрема в контексті адаптації міжнародних стандартів до функціональних особливостей та ризикового профілю діяльності АРМА.

Аналіз попередніх досліджень. У процесі формування політики інформаційної безпеки в державних органах, таких як АРМА, особливу актуальність набуває врахування як міжнародного досвіду, так і національних наукових напрацювань у сфері ризик-орієнтованого управління, цифрової трансформації та захисту критичних активів. Останні роки позначені активним розвитком теоретичних і прикладних підходів до розробки політик інформаційної безпеки в умовах динамічного середовища загроз.

У роботі Bakhtavar et al. розглянуто використання нечітких когнітивних карт (Fuzzy Cognitive Maps, FCM) як інструменту системного аналізу ризиків у складних інформаційних системах [1]. Застосування FCM дозволяє моделювати багаторівневу політику безпеки в умовах невизначеності, що надзвичайно важливо для управління активами з високим рівнем правової та інформаційної чутливості, як у випадку з АРМА.

Ключовий внесок у розробку адаптивних механізмів формування політики ІБ здійснив Melaku, запропонувавши контекстно-залежну структуру ризик-менеджменту для організацій, що функціонують у змінному цифровому середовищі [2]. Цей підхід передбачає динамічну зміну політик відповідно до змін у загрозовому ландшафті та обмеженнях інформаційної архітектури державної установи.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Практичне розуміння потреб цифрового захисту в контексті інтелектуалізації державних функцій було висвітлено у роботі Dudykevych, Mykytyn і Stosyk, де запропоновано модель безпеки для кіберфізичних систем та IoT, що взаємодіють у межах цифрового урядування [3]. Для системи АРМА, яка оперує як фізичними, так і цифровими активами, подібні моделі можуть бути інтегровані у фреймворк формування політики доступу й контролю.

У свою чергу, Abbasian et al.запропонували метод оцінки ризиків для складних систем на основі FCM, що дозволяє ієрархічно структурувати фактори загроз та формувати відповідні політики реагування [4]. Цей підхід має практичне значення для побудови внутрішньої архітектури СМІБ у межах АРМА, де потрібна чітка ідентифікація зон відповідальності та інцидентних сценаріїв.

Важливою для українського контексту є праця Dreis, Korchenko, Brzhevska і Kriuchkova, у якій представлено модель формування бази даних внутрішніх параметрів для оцінки стану захисту державної таємниці [5]. Ці підходи можуть бути адаптовані для формування показників ефективності політики ІБ у системі менеджменту АРМА, особливо в частині контролю за обігом чутливої інформації, що містить ознаки конфіденційності або службового доступу. Таким чином, аналіз актуальних досліджень демонструє багатогранність підходів до формування політики інформаційної безпеки в державному управлінні. Для АРМА особливо важливо інтегрувати контекстно-залежний аналіз ризиків, нечітке моделювання загроз, а також архітектурні рішення, здатні забезпечити безперервність захисту в умовах кіберзагроз і нормативної складності.

Виклад основного матеріалу. Інформаційна безпека в державному управлінні набула стратегічного значення в умовах цифрової трансформації, зростання кількості кіберзагроз та ускладнення правового регулювання обігу чутливої інформації. Особливої актуальності це питання набуває для Національного агентства з питань виявлення, розшуку та управління активами (АРМА), яке здійснює операції з активами, що мають високий правовий, економічний та інформаційний ризик. Забезпечення конфіденційності, цілісності та доступності інформації в таких умовах неможливе без формування системної політики інформаційної безпеки, що інтегрована у загальну структуру менеджменту установи.

Відповідно до стандартів ISO/IEC 27001, ефективна політика інформаційної безпеки має базуватись на ризик-орієнтованому підході, враховувати організаційну специфіку та нормативні вимоги [1-2]. Водночас на національному рівні існує дефіцит практичних рекомендацій щодо впровадження СМІБ у державних структурах із делікатними повноваженнями, такими як АРМА. Це зумовлює потребу в розробці теоретично обґрунтованої та практично адаптованої моделі політики безпеки, яка відповідатиме як міжнародним вимогам, так і національним особливостям адміністративного та інформаційного середовища.

Методологічною основою дослідження є системний і міждисциплінарний підхід, що поєднує принципи інформаційної безпеки, управління ризиками та правового регулювання. На першому етапі використано системний аналіз для визначення ключових елементів інформаційної інфраструктури АРМА та їх взаємозв’язку з потенційними загрозами. Далі за допомогою контент-аналізу вивчено нормативно-правові акти, стандарти ISO/IEC 27001 та національні регуляції у сфері інформаційної безпеки. Застосовано порівняльний аналіз політик безпеки в аналогічних державних установах, що дало змогу адаптувати найкращі практики до українського контексту [3]. На основі експертного оцінювання узагальнено практичний досвід формування СМІБ у публічному секторі. Завершальним етапом стало моделювання структури політики ІБ, орієнтованої на специфіку АРМА, із урахуванням ризиків, регуляторних вимог і сучасних кіберзагроз.

Політика інформаційної безпеки в межах системи менеджменту інформаційної безпеки (СМІБ) Національного агентства з питань виявлення, розшуку та управління активами

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

(АРМА) має бути побудована на основі принципів системності, багаторівневої відповідальності та відповідності міжнародним і національним вимогам. Її структура повинна інтегрувати як стратегічні засади забезпечення безпеки, так і практичні регламенти управління доступом, захистом інформації, реагуванням на інциденти та моніторингом ризиків.

Загальний розділ політики визначає її цілі, сферу застосування, основні терміни та посилання на нормативно-правову базу, включаючи стандарти ISO/IEC 27001, НД ТЗІ, законодавство України у сфері захисту інформації та персональних даних. Це створює підґрунтя для єдиного тлумачення положень політики на всіх рівнях управління. Організаційна частина політики чітко розподіляє відповідальність між керівництвом АРМА, підрозділами, ІТ-фахівцями та кінцевими користувачами. У ній закладено принцип підзвітності за інформаційну безпеку, передбачено створення окремої функції інформаційної безпеки (офіцер або підрозділ ІБ) і механізми навчання персоналу для підвищення обізнаності щодо актуальних кіберзагроз та стандартів поведінки.

Ключовою складовою політики є регламент управління доступом. Він передбачає ієрархічну класифікацію доступу до активів за рівнем конфіденційності, впровадження систем аутентифікації та авторизації, обмеження прав за принципом найменших привілеїв, а також правила управління віддаленим доступом. Окремо визначаються вимоги до облікових записів із підвищеними правами та порядок їх контролю.

Політика захисту інформації охоплює технічні та організаційні засоби забезпечення цілісності, конфіденційності та доступності даних. До них належать шифрування, захист каналів зв’язку, регламенти використання мобільних і знімних носіїв, а також політика резервного копіювання і відновлення. Це забезпечує стійкість системи до технічних збоїв і зловмисних втручань. Політика реагування на інциденти визначає процедури виявлення, фіксації, класифікації та усунення подій безпеки. Вона регламентує порядок внутрішнього повідомлення про інциденти, взаємодію між підрозділами, аналіз причин та вжиття запобіжних заходів [5]. Сюди ж входять вимоги до ведення журналів подій і звітності.

Моніторинг і аудит є окремим блоком політики, який забезпечує постійний контроль за дотриманням вимог ІБ. Він включає логування активності користувачів, аудит доступу, внутрішні перевірки та оцінку ефективності заходів безпеки. Ці дії дозволяють виявляти відхилення від політик і оперативно їх коригувати. Завершальною частиною політики є механізм її актуалізації. У ній визначено порядок перегляду політики, частоту оновлення, вимоги до затвердження змін, а також процедури доведення нових положень до всіх зацікавлених осіб. Цей елемент забезпечує гнучкість політики та її відповідність сучасним викликам. Таким чином, структура політики інформаційної безпеки в системі менеджменту АРМА є багаторівневою, динамічною та орієнтованою на запобігання ризикам. Вона забезпечує не лише регламентацію дій, а й створює цілісну модель функціонування безпеки як частини стратегічного управління установою.

Концептуально модель політики ІБ АРМА базується на багаторівневому підході до управління безпекою, який охоплює стратегічний, адміністративний та операційний рівні. На стратегічному рівні політика визначає загальні принципи захисту, цілі, сферу застосування, юридичні основи та політичну волю керівництва до дотримання принципів кіберстійкості. На адміністративному рівні описуються відповідальність і повноваження осіб, що відповідають за реалізацію політики, взаємодія між підрозділами, а також механізми реагування на інциденти, аудит і внутрішній контроль. На операційному рівні модель регламентує конкретні процедури – ідентифікацію та аутентифікацію користувачів, шифрування, моніторинг, обробку подій безпеки, резервне копіювання тощо.

Ключовим елементом моделі є система управління ризиками, яка забезпечує оцінку, класифікацію та мінімізацію ризиків, пов’язаних із обробкою чутливої інформації. Використовуючи методики ISO/IEC 27005, політика передбачає періодичну переоцінку ризиків із залученням міждисциплінарних команд [1]. Це дозволяє формувати профілі загроз

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

і вразливостей, відповідно до яких обираються релевантні заходи захисту, що закладаються в політику як обов'язкові до виконання. Наступною складовою є архітектура політик доступу, яка включає модель ієрархічного розмежування прав (RBAC або ABAC), контроль привілейованого доступу, обмеження доступу до інформації за часом, місцем, рівнем довіри [2]. У контексті АРМА особливо важливо забезпечити ізольованість інформації, що надходить з органів досудового розслідування, судів, міжнародних партнерів, та контроль її використання згідно з законодавчими обмеженнями.

Модель також передбачає впровадження технологічних контролів, зокрема криптографічного захисту інформації (TLS, PKI, електронні підписи), систем моніторингу та фіксації подій (SIEM), виявлення аномалій (IDS/IPS), а також контролю дій адміністративних облікових записів. Технічні засоби повинні інтегруватися у загальну архітектуру IT-інфраструктури АРМА без порушення продуктивності та юридичної підзвітності операцій [4]. Особливий акцент модель робить на організаційних заходах, включаючи формування підзвітності, навчання персоналу, процедури реагування на інциденти, аудит, перевірку на відповідність політиці та регулярне оновлення її положень. У політику вбудовується механізм циклічного вдосконалення (PDCA), що передбачає безперервне планування, реалізацію, перевірку й коригування політики в умовах зміни зовнішніх і внутрішніх факторів [5]. Таким чином, модель політики ІБ в АРМА поєднує документальне регулювання, управлінське адміністрування та технічну реалізацію принципів безпеки у єдину систему, що відповідає особливостям функціонування агентства. Її реалізація дозволяє досягти не лише відповідності регуляторним вимогам, а й стійкої операційної безпеки, прозорості дій і довіри з боку партнерів, державних структур і громадськості.

На рис. 1 зображено багаторівневу архітектуру моделі політики інформаційної безпеки в системі менеджменту АРМА, представлену у вигляді компонентної діаграми. Модель складається зі стратегічного, адміністративного та операційного рівнів, які взаємодіють із ключовими функціональними компонентами: управління ризиками, політика доступу, організаційні заходи та технологічні контролі. На стратегічному рівні визначаються цілі безпеки, нормативна база та позиція керівництва. Адміністративний рівень включає розподіл відповідальності, аудит та реагування на інциденти. Операційний рівень реалізує технічні засоби: ідентифікацію, доступ, шифрування, моніторинг та резервне копіювання. Центральним елементом моделі є система управління ризиками за стандартом ISO/IEC 27005, яка забезпечує адаптацію політики до поточних загроз. Модель працює в рамках циклу PDCA (Plan–Do–Check–Act), що гарантує її гнучкість, безперервне вдосконалення та відповідність сучасним викликам у сфері інформаційної безпеки.

Ефективне впровадження політики інформаційної безпеки в системі менеджменту Національного агентства з питань виявлення, розшуку та управління активами (АРМА) передбачає не лише створення формалізованого документа, а й його інтеграцію в усі рівні управління інформаційною інфраструктурою установи. Така політика має бути гнучкою, адаптивною до змін загрозового середовища й побудованою відповідно до міжнародних стандартів (зокрема ISO/IEC 27001), сучасних ризик-орієнтованих підходів і вимог національного законодавства. Реалізація політики потребує багаторівневої моделі впровадження, що включає шість взаємопов'язаних етапів.

Першим кроком є підготовка організаційного середовища, в межах якого формуються засади майбутньої СМІБ. На цьому етапі визначається уповноважений підрозділ або посадова особа, відповідальна за реалізацію політики, формуються робочі групи за участі IT-фахівців, керівників підрозділів, юристів і спеціалістів з ризик-менеджменту. Обов'язковим компонентом цього етапу є проведення первинної оцінки ризиків відповідно до методик ISO/IEC 27005 або NIST SP 800-30: виявляються інформаційні активи, вразливості, можливі загрози та рівні ймовірності їх реалізації [1]. Це дозволяє окреслити сфери критичності, встановити пріоритети захисту та межі впровадження політики в межах АРМА.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

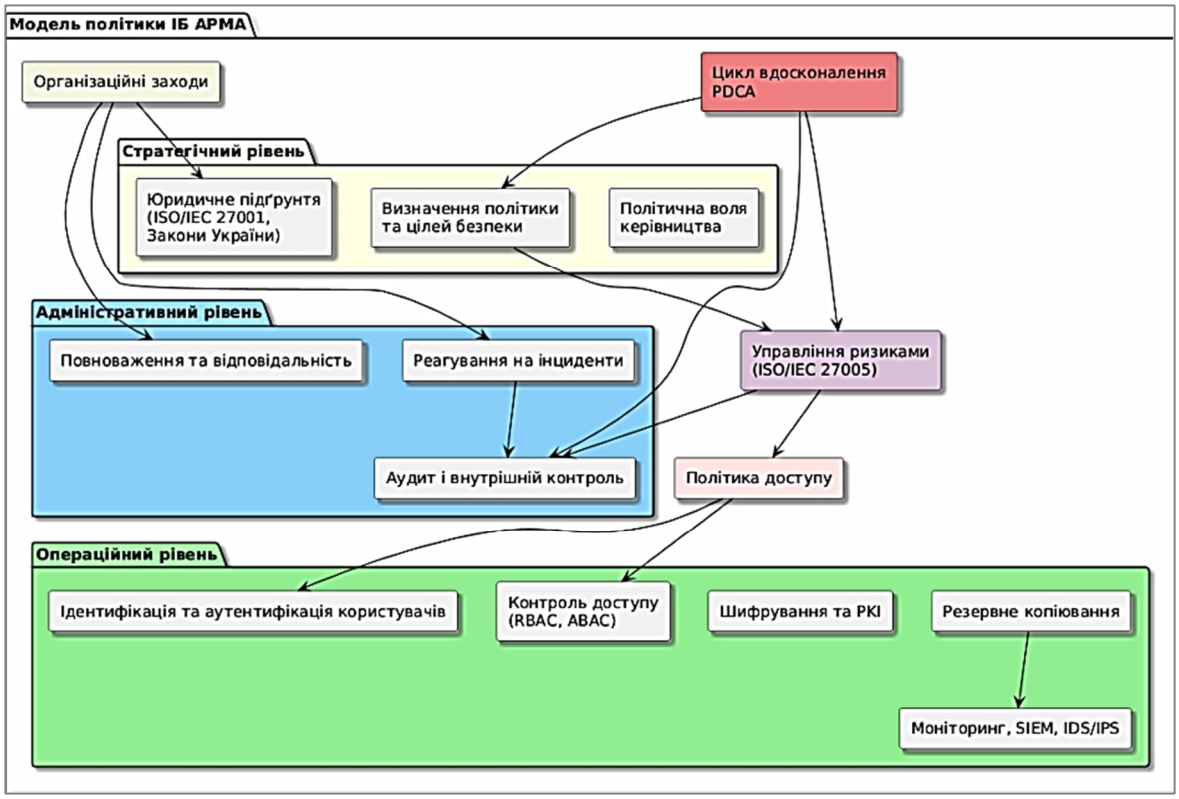


Рис. 1. Архітектура моделі політики інформаційної безпеки в системі менеджменту АРМА (UML-компонентна діаграма)

Джерело: розроблено автором

Наступним етапом є розробка та затвердження політики, яка має охоплювати повний спектр напрямів інформаційної безпеки: управління доступом, криптографічний захист, моніторинг активності, обробка інцидентів, аудит і резервне копіювання. Структура політики узгоджується з міжнародними стандартами (ISO/IEC 27001, 27002), а її зміст – із внутрішніми процесами АРМА. Після розробки проєкт документа проходить погодження із зацікавленими підрозділами, правовою експертизою та затверджується адміністративним актом керівництва. Такий підхід забезпечує легітимність і обов'язковість виконання політики на всіх рівнях.

Третім етапом виступає інтеграція політики в управлінські та технічні процеси. Йдеться не лише про оновлення внутрішніх регламентів, а про впровадження конкретних процедур і технологічних рішень. Зокрема, налаштовуються механізми багатофакторної аутентифікації, сегментації мереж, системи управління правами доступу (наприклад, на базі RBAC), SIEM-рішення для виявлення аномалій, а також засоби криптографічного захисту, резервного копіювання й відновлення. У рамках цього етапу проводиться ревізія всієї IT-інфраструктури АРМА на відповідність новій політиці безпеки, що забезпечує її реальну дієвість.

Важливою складовою моделі впровадження є забезпечення поінформованості персоналу, навчання та формування культури безпеки. Співробітники, які безпосередньо працюють з інформацією, мають розуміти не лише зміст політики, а й мотивацію її впровадження, ризики недотримання та правила поведінки у разі інцидентів. Цей етап включає розробку навчальних матеріалів, проведення інструктажів, практичних тренінгів, симуляцій атак (наприклад, фішинг-кампаній) та оцінювання знань працівників. Освітній компонент є критично важливим для ефективного дотримання політики, оскільки саме людський фактор залишається однією з головних вразливостей у системах безпеки.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

П’ятий етап – це безперервний моніторинг і аудит виконання політики, що базується на принципах прозорості, зворотного зв’язку й контрольованості. Установлюються ключові показники ефективності (KPI), впроваджуються механізми логування, ведення журналів подій, регулярні внутрішні перевірки, зовнішні аудити та ревізії процесів. Особливу увагу приділяють аналізу інцидентів інформаційної безпеки, розробці коригувальних дій і оновленню відповідних розділів політики. Таким чином, забезпечується контроль виконання й виявлення слабких місць у системі захисту.

Фінальний етап впровадження – це постійне оновлення та вдосконалення політики. Вона не є статичним документом, а повинна змінюватися відповідно до нових законодавчих вимог, оновлень IT-середовища, появи нових загроз або зміни пріоритетів в управлінні. У цьому контексті важливим є впровадження моделі PDCA (Plan–Do–Check–Act), яка дозволяє формалізувати процеси безперервного поліпшення політики безпеки й узгодити їх з життєвим циклом системи управління [2]. Таким чином, запропонована модель впровадження політики інформаційної безпеки в системі менеджменту АРМА є системною, динамічною та гнучкою. Вона дозволяє забезпечити не лише нормативну відповідність, а й практичну ефективність заходів захисту, створюючи підґрунтя для сталого функціонування АРМА як елемента національної системи безпеки в умовах цифрової трансформації.

Завершальним етапом формування політики інформаційної безпеки є створення чітких механізмів її реалізації на практиці, особливо в частині реагування на інциденти. В умовах зростання кількості кіберзагроз, важливою складовою функціонування системи менеджменту ІБ стає ефективна взаємодія між суб’єктами внутрішнього контролю, технічних служб і аналітичних підрозділів [3-5]. Реалізація політики ІБ у вигляді сценаріїв взаємодії дозволяє своєчасно виявляти, аналізувати та усувати загрози. Нижче подано діаграму, яка ілюструє типовий алгоритм реагування на інцидент в рамках СМІБ АРМА.

На діаграмі (рис. 2) послідовну взаємодію основних суб’єктів, задіяних у процесі виявлення, аналізу та реагування на інцидент інформаційної безпеки в рамках функціонування системи менеджменту інформаційної безпеки (СМІБ) АРМА. Діаграма відображає типовий сценарій, що реалізується відповідно до внутрішньої політики ІБ, орієнтованої на стандарти ISO/IEC 27001 та ISO/IEC 27035. Процес починається з реєстрації незвичної або потенційно небезпечної активності користувача інформаційною системою моніторингу (SIEM або IDS). Система автоматично повідомляє офіцера інформаційної безпеки, який ініціює процедуру реагування, передаючи запит спеціалізованій службі реагування. Команда аналізує інцидент, запитує необхідні журнали подій і здійснює первинну оцінку ризиків.

Після отримання результатів аналізу формується звіт про інцидент, який передається аудитору для перевірки відповідності заходів реагування чинній політиці інформаційної безпеки. Аудитор, у разі виявлення прогалин або нових загроз, надає рекомендації для оновлення положень політики. Система управління політикою інформаційної безпеки оновлює відповідні документи, а зміни набирають чинності після погодження з відповідальними особами. Таким чином, діаграма демонструє не лише алгоритм реагування на інциденти, а й механізм постійного вдосконалення політики ІБ через інтеграцію інцидент-менеджменту та внутрішнього аудиту. Це забезпечує підтримку актуальності політики, адаптацію до змін загрозового середовища та підвищення кіберстійкості організації.

Впровадження політики інформаційної безпеки в системі менеджменту АРМА вимагає чіткої, поетапної реалізації. Першим кроком є формування організаційного підґрунтя: призначення відповідального підрозділу, створення робочої групи та проведення початкової оцінки ризиків відповідно до стандартів ISO/IEC 27005 або NIST SP 800-30 [1]. Наступним є розробка структурованої політики, яка охоплює ключові напрями безпеки, з її погодженням усіма зацікавленими сторонами. Інтеграція політики в управлінські та технічні процеси включає налаштування багатофакторної аутентифікації, контроль доступу (RBAC/ABAC), моніторинг (SIEM, IDS/IPS) та аудит [2, 4]. Критично важливим є навчання персоналу й

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

формування культури безпеки. Завершує процес впровадження механізм постійного вдосконалення за моделлю PDCA, що дозволяє адаптувати політику до змін загрозового середовища.

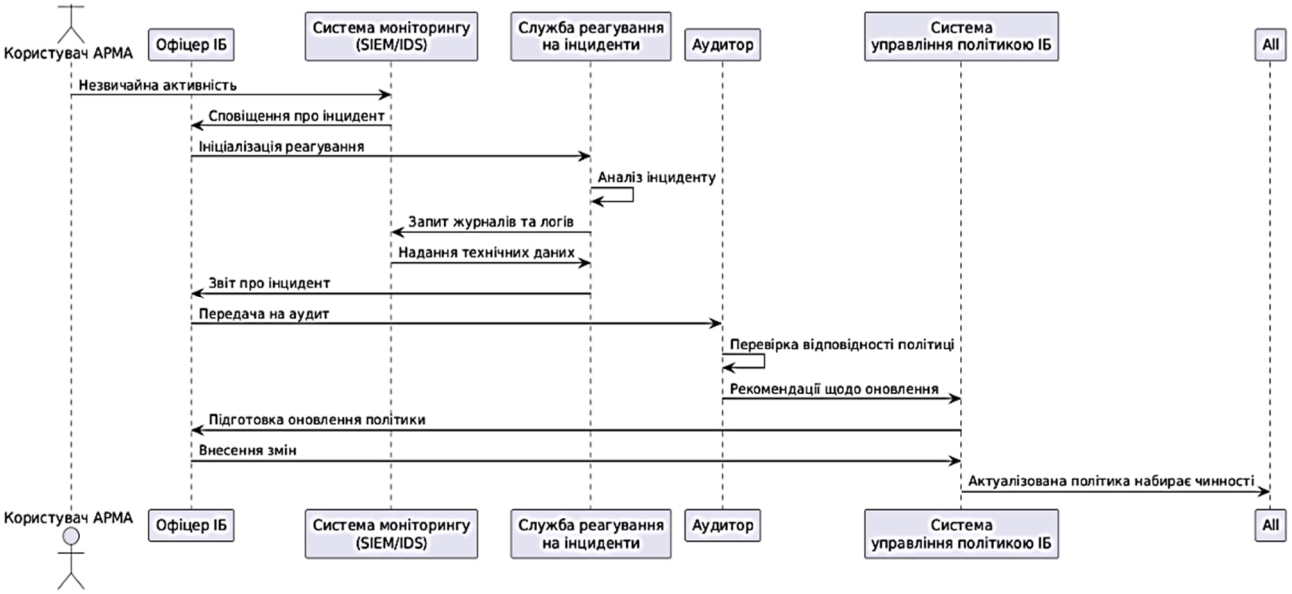


Рис. 2. Послідовність дій під час обробки інциденту інформаційної безпеки в системі менеджменту АРМА

Джерело: розроблено автором

У межах подальших досліджень доцільно зосередити увагу на формалізації індикаторів ефективності політики інформаційної безпеки, які дозволять кількісно оцінювати рівень її виконання, ступінь відповідності цілям та нормативам, а також своєчасність реакції на інциденти [5]. Перспективним є моделювання сценаріїв порушення політики із застосуванням методів імітаційного моделювання, що дасть змогу перевірити стійкість внутрішніх процедур в умовах реальних загроз [3]. Актуальним напрямом є також розробка автоматизованих моделей інцидент-менеджменту, інтегрованих у СМІБ, з урахуванням пріоритетності інцидентів, їх критичності та джерела походження [4]. Особливу цінність становить дослідження динамічних контекстно-залежних політик доступу (ABAC), які дозволяють більш гнучко реагувати на зміну умов роботи користувачів та структури активів.

Висновок. Проведене дослідження дозволило визначити концептуальні, організаційні та практичні засади формування ефективної політики інформаційної безпеки в системі менеджменту Національного агентства України з питань виявлення, розшуку та управління активами (АРМА). Враховуючи специфіку функцій АРМА, що охоплюють управління правочутливими активами в межах кримінального провадження та взаємодію з міжнародними структурами, політика інформаційної безпеки має розглядатись не лише як формальний документ, а як ключовий інструмент забезпечення кіберстійкості, правової відповідності та прозорості діяльності агентства. Запропонована багаторівнева модель політики, що охоплює стратегічний, адміністративний і операційний рівні, забезпечує системний підхід до побудови та реалізації вимог інформаційної безпеки. Її основою виступає ризик-орієнтований підхід відповідно до стандартів ISO/IEC 27001 та ISO/IEC 27005, що дозволяє ефективно враховувати динаміку загроз і особливості організаційної структури АРМА. Встановлено, що реалізація політики має охоплювати не лише технічні та процедурні механізми (контроль доступу, криптографічний захист, моніторинг, реагування на інциденти), а й включати освітні заходи, аудит, цикл постійного вдосконалення (PDCA) та правову експертизу.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Практичне значення запропонованого підходу полягає в можливості його адаптації до інших державних структур, що працюють з конфіденційною або стратегічною інформацією. Визначені в дослідженні кроки впровадження та перспективи подальшого наукового розвитку – зокрема розробка KPI, сценарне моделювання інцидентів і контекстно-залежних політик – створюють підґрунтя для побудови сучасної, гнучкої та ефективної системи управління інформаційною безпекою у публічному секторі України.

Список використаних джерел

1. Bakhtavar, E., Valipour, M., Yousefi, S., Sadiq, R., Hewage, K. Fuzzy cognitive maps in systems risk analysis: a comprehensive review / E. Bakhtavar, M. Valipour, S. Yousefi, R. Sadiq, K. Hewage // Complex & Intelligent Systems. – 2020. – Vol. 6, No. 3. – P. 621–637. https://doi.org/10.1007/s40747-020-00228-2.
2. Melaku, H. M. Context-Based and Adaptive Cybersecurity Risk Management Framework / H. M. Melaku // Risks. – 2023. – Vol. 11, No. 6. – Article 101. https://doi.org/10.3390/risks11060101.
3. Dudykevych, V., Mykytyn, G., Stosyk, T. Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society / V. Dudykevych, G. Mykytyn, T. Stosyk // Cybersecurity Providing in Information and Telecommunication Systems: Proc. of the Int. Workshop. – CEUR Workshop Proceedings. – 2024. – Vol. 3654. – P. 449–457.
4. Abbasian, H., Yousefi-Zenouz, R., Amirkhani, A., Shirzadeh, M., Abdollahiasl, A., Nikfar, S., Siahi-Shadabad, M., & Kebriaeezadeh, A. (2024). Risk assessment for complex systems based on fuzzy cognitive maps: a case of the biopharmaceutical industry. Complexity, 2024, Article 4369401. https://doi.org/10.1155/2024/4369401
5. Dreis, Y., Korchenko, O., Brzhevska, Z., Kriuchkova, L., Nesterova, O. Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection / Y. Dreis, O. Korchenko, Z. Brzhevska, L. Kriuchkova, O. Nesterova // Cybersecurity Providing in Information and Telecommunication Systems: Proc. of the Int. Workshop. – CEUR Workshop Proceedings. – 2024. – Vol. 3654. – P. 277–289. – ISSN 1613-0073.

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ЧУБАЄВСЬКОГО В. І.

ПОРІВНЯЛЬНИЙ АНАЛІЗ AZURE BACKUP ТА ТРАДИЦІЙНИХ РІШЕНЬ РЕЗЕРВНОГО КОПІЮВАННЯ

КАРПЕНКО В. О., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті проведено комплексний аналіз методів резервного копіювання даних та порівняння традиційних і хмарних підходів до зберігання інформації. Досліджено структуру витрат та організаційні аспекти різних стратегій резервного копіювання. Особлива увага приділена перевагам хмарних рішень, зокрема Microsoft Azure Backup, з точки зору оптимізації фінансових і технологічних ресурсів. Запропоновано рекомендації щодо вибору оптимальної стратегії резервного копіювання відповідно до потреб підприємств різного масштабу та сфери діяльності.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

The article provides a comprehensive analysis of data backup methods and compares traditional and cloud-based approaches to information storage. The cost structure and organizational aspects of various backup strategies are investigated. Special attention is paid to the advantages of cloud solutions, particularly Microsoft Azure Backup, in terms of optimizing financial and technological resources. Recommendations are proposed for selecting the optimal backup strategy according to the needs of enterprises of different scales and fields of activity.

Актуальність дослідження зумовлена критичною важливістю захисту інформаційних активів в умовах цифрової трансформації бізнесу та зростаючих кіберзагроз. Сучасні підприємства стикаються з дедалі більшими ризиками втрати даних внаслідок кібератак, системних збоїв, людського фактору та природних катастроф. Компанії, які зазнають значної втрати даних без належної системи відновлення, часто припиняють свою діяльність протягом короткого часу після інциденту. Водночас, більшість підприємств малого та середнього бізнесу не приділяють достатньої уваги перевірці та тестуванню своїх резервних копій, що підвищує ризик неможливості відновлення даних при виникненні надзвичайних ситуацій. Людський фактор залишається однією з основних причин втрати даних через випадкове видалення, пошкодження або неправильне використання файлів. Ці факти підкреслюють необхідність розробки ефективних стратегій резервного копіювання та впровадження сучасних технологічних рішень для забезпечення безперервності бізнес-процесів та збереження цифрових активів організацій.

Мета статті полягає в комплексному аналізі сучасних методів резервного копіювання даних, порівнянні традиційних та хмарних підходів до організації захисту інформації, а також у розробці рекомендацій щодо вибору оптимальної стратегії резервного копіювання з урахуванням специфіки діяльності, фінансових можливостей та технологічних потреб підприємств різного масштабу.

Об'єктом дослідження є процеси резервного копіювання та відновлення даних в інформаційних системах підприємств та організацій.

Предметом дослідження є методи, технології та стратегії резервного копіювання даних, зокрема традиційні локальні підходи та хмарні рішення на прикладі Microsoft Azure Backup, їхні технічні характеристики, економічні показники та ефективність застосування в сучасних умовах функціонування інформаційного середовища.

Аналіз попередніх досліджень. Попередні дослідження були зосереджені на розвитку технологій резервного копіювання та відновлення даних у хмарі. Було вивчено одноклікові рішення, які поєднують доступність, безпеку та масштабованість для корпоративних потреб. Окрему увагу було приділено еволюції хмарних сервісів резервного копіювання та їх інтеграції з різними типами інфраструктури. Також детально було розглянуто проблеми безпеки, зокрема захист від програм-вимагачів у традиційних методах резервного копіювання. Крім того, було досліджено мультисерверні підходи та покращені алгоритми для відновлення втрачених даних, щоб забезпечити надійність і мінімальний час відновлення.

Виклад основного матеріалу. Резервне копіювання є фундаментальним елементом безпеки інформаційних систем, що забезпечує цілісність та доступність даних при виникненні непередбачуваних ситуацій. У сучасних умовах функціонування інформаційного середовища збереження даних стає критичним фактором забезпечення безперервності бізнес-процесів, захисту інтелектуальної власності та дотримання нормативних вимог. Комплексний підхід до організації резервного копіювання передбачає врахування технічних, організаційних та економічних факторів.

Статистичні дані свідчать, що приблизно 93% підприємств, які зазнали значної втрати даних без належної системи відновлення, припиняють діяльність протягом року після інциденту. При цьому 96% підприємств із комплексним планом аварійного відновлення успішно долають наслідки таких ситуацій. Особливу увагу привертає факт, що людський

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

фактор залишається однією з основних причин втрати даних – 58% випадків зумовлені випадковим видаленням, пошкодженням або неправильним використанням файлів.

Аналіз практик резервного копіювання вказує на значні прогалини в підходах до збереження інформації. Незважаючи на очевидні ризики, лише 35% підприємств малого та середнього бізнесу повністю тестують свої резервні копії, а 41% виконують це тестування щонайменше раз на місяць [1].

Розробка комплексної стратегії резервного копіювання даних є критично важливим елементом забезпечення безперервності бізнес-процесів сучасної організації. У контексті зростаючих обсягів цифрової інформації та підвищення залежності бізнесу від даних, відсутність належного підходу до їх збереження може призвести до значних операційних та фінансових втрат. Аналіз сучасних підходів до управління інформаційними ризиками дозволяє виділити наступні основні компоненти ефективної стратегії резервного копіювання даних:

– чітке визначення класифікації даних та їх пріоритизація для резервного копіювання;

– встановлення диференційованих політик резервного копіювання для різних категорій даних;

– визначення оптимальної частоти створення резервних копій відповідно до встановлених показників RPO;

– вибір методів резервного копіювання (повне, диференціальне, інкрементальне) для різних типів даних;

– специфікація місць зберігання резервних копій з урахуванням територіального розподілу та відмовостійкості;

– документування процедур перевірки та тестування резервних копій;

– розробка протоколів відновлення даних з чітким розподілом ролей та відповідальності.

Систематизований підхід до формування стратегії резервного копіювання дозволяє організаціям мінімізувати ризики втрати даних та забезпечити швидке відновлення після інцидентів різної природи [2].

Методологія резервного копіювання базується на трьох основних підходах: повному, диференціальному та інкрементальному. Порівняльний аналіз методів резервного копіювання демонструє суттєві відмінності в їх ефективності для різних типів інформаційних систем та даних. Повне копіювання, яке зберігає всі дані при кожному циклі, забезпечує найвищу надійність та швидкість відновлення, що робить його оптимальним для критичних бізнес-систем та статичних даних, де ціна простою перевищує витрати на зберігання резервних копій. Диференціальне копіювання, що архівує лише зміни з моменту останнього повного копіювання, представляє збалансоване рішення для систем середньої критичності з обмеженими ресурсами зберігання та часовими вікнами для резервного копіювання, найкраще підходячи для структурованих баз даних та середовищ розробки. Інкрементальне копіювання, зберігаючи тільки зміни з моменту останньої резервної копії будь-якого типу, мінімізує використання ресурсів і часу, що робить його ідеальним для некритичних систем з обмеженою пропускною здатністю мережі, даних з високою частотою змін та розподілених середовищ, хоча це супроводжується більш складним і повільним процесом відновлення через необхідність послідовного застосування всіх інкрементальних копій [3].

Вибір оптимальної стратегії резервного копіювання включає не лише визначення методу збереження даних, але й рішення щодо їхнього розміщення, що впливає на безпеку, доступність і витрати. Вибір оптимальної стратегії резервного копіювання включає не лише визначення методу збереження даних, але й рішення щодо їхнього розміщення. Існує кілька основних підходів до резервного копіювання, кожен із яких має свої переваги та обмеження.

Локальні резервні копії зберігаються на внутрішніх серверах або зовнішніх жорстких дисках, забезпечуючи швидкий доступ, але залишаючись вразливими до фізичних

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

пошкоджень. Віддалене копіювання (offsite) передбачає зберігання даних у фізично віддалених локаціях, що підвищує безпеку, але може збільшити час відновлення. Хмарні рішення автоматично зберігають дані на серверах провайдера, забезпечуючи масштабованість та мінімізуючи витрати на інфраструктуру. Надмірність (redundancy) передбачає дублювання даних у реальному часі на кількох носіях чи серверах для підвищення стійкості до збоїв. Використання знімних носіїв, таких як USB-накопичувачі чи оптичні диски, дає змогу створювати автономні резервні копії, які не залежать від мережевого підключення. Гібридний підхід поєднує кілька методів, забезпечуючи баланс між доступністю, безпекою та швидкістю відновлення. Організації зазвичай стоять перед вибором між хмарним та локальним резервним копіюванням, оскільки кожен з цих підходів має свої переваги залежно від потреб бізнесу. А деякі обирають гібридні моделі, що поєднують переваги обох підходів, дозволяючи оптимізувати безпеку, доступність та витрати [2].

Кожен метод резервного копіювання має свої сильні сторони та обмеження, і вибір між ними залежить від конкретних потреб користувача або компанії. Локальне резервне копіювання забезпечує повний контроль над процесом збереження даних. Це особливо зручно, коли необхідно швидко отримати доступ до копій і здійснювати їх відновлення. Завдяки відсутності регулярних абонентських платежів, цей варіант часто є економічно вигідним у короткостроковій перспективі.

Однак локальне резервне копіювання має й ряд обмежень. Найбільша проблема полягає у фізичному доступі до носіїв: при неможливості потрапити до приміщення або при пошкодженні обладнання існує ризик втрати даних. Крім того, сам процес обслуговування таких резервних копій може бути трудомістким і вимагати значних зусиль. Важливо також враховувати ризик пошкодження носіїв або навіть їх крадіжки, що може призвести до непоправних наслідків.

На противагу локальним методам, хмарне резервне копіювання стає все більш популярним завдяки своїм перевагам у безпеці, масштабованості та зручності. Автоматизація процесів та доступність даних у будь-який час з будь-якої точки світу роблять цей метод надзвичайно зручним для багатьох користувачів. Також, завдяки високому рівню шифрування і захисту даних, хмарні рішення забезпечують більшу безпеку в порівнянні з локальними копіями.

Однак хмарне резервне копіювання має й свої недоліки. Залежність від стабільності інтернет-з’єднання може створювати труднощі в разі збоїв у мережі, а регулярні абонентські платежі можуть з часом стати суттєвим фінансовим навантаженням. Крім того, для деяких галузей існують законодавчі обмеження щодо зберігання даних у хмарі.

Отже, вибір між локальним і хмарним резервним копіюванням залежить від специфіки задач, бюджету та вимог до безпеки даних. Обидва підходи мають свої переваги та недоліки, і важливо обирати той, що найкраще відповідає вашим потребам та умовам роботи. Локальній бекап демонструє особливу ефективність для підприємців-одинаків, консалтингових фірм, фрілансерів, домашніх підприємств та малих компаній з обмеженими обсягами даних. Також варто відзначити, що магнітні стрічки та записувані CDR бекапи активно використовуються компаніями, які працюють з медіа-контентом, та юридичними фірмами, що архівують документи клієнтів протягом тривалого періоду.

Хмарний бекап підходить для організацій будь-якого масштабу, забезпечуючи зручність, надійність та ефективне відновлення даних. Малі підприємства цінують його за простоту використання без необхідності утримувати IT-відділ, тоді як електронна комерція та фінансові сервіси отримують безперервне резервування з максимальним рівнем захисту. Великі компанії використовують хмарний бекап як додатковий рівень безпеки та основу плану аварійного відновлення. Незалежно від розміру бізнесу, хмарне резервування гарантує безперервність процесів і швидкий доступ до даних у разі інцидентів [4, 5].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

У сучасному світі IT-інфраструктури виділяються три ключові гравці на ринку хмарних послуг: Microsoft Azure, Google Cloud Platform (GCP) та Amazon Web Services (AWS). Кожен із цих постачальників пропонує комплексні рішення для резервного копіювання даних, що відрізняються за функціональністю, масштабованістю та ціновою політикою. Microsoft Azure пропонує два основних сервіси для резервного копіювання та зберігання даних: Azure Backup та Azure Storage, кожен з яких має свої специфічні функції та сценарії застосування.

Azure Storage представляє собою потужне хмарне рішення від Microsoft, яке забезпечує надійне та масштабоване середовище для збереження даних різного типу та обсягу. Також цей сервіс пропонує комплексний набір функцій, що дозволяють ефективно організувати процеси резервного копіювання для підприємств будь-якого розміру. Azure Blob Storage, компонент Azure Storage, забезпечує збереження неструктурованих даних у хмарі та є ідеальним рішенням для резервного копіювання файлів. Особливо важливо, що цей сервіс зберігає ієрархічну структуру даних, точно відтворюючи оригінальну організацію файлів та папок при завантаженні. Це значно спрощує процеси резервного копіювання та відновлення, оскільки не потрібно реконструювати структуру даних після їх відновлення.

Система багаторівневого зберігання Azure Blob Storage пропонує різні рівні доступності даних:

– Hot Tier (гарячий рівень) – для даних, що потребують частого доступу;
– Cool Tier (холодний рівень) – для даних, що використовуються рідше;
– Archive Tier (архівний рівень) – для довготривалого зберігання з оптимізацією витрат.

Особливу увагу заслуговує Archive Tier, який забезпечує найнижчу вартість зберігання даних і є оптимальним для довготривалого зберігання резервних копій, до яких рідко звертаються.

Важливою особливістю роботи з архівним рівнем Azure Storage є процес регідратації – переміщення даних з архівного рівня на гарячий для отримання доступу до них. Цей процес включає такі етапи:

1. ініціювання запиту на регідратацію через Azure Portal, Azure CLI, PowerShell або API;
2. очікування завершення процесу регідратації (тривалість залежить від обсягу даних);
3. отримання доступу до даних на гарячому рівні.

Варто зазначити, що хоча архівне зберігання є економічно вигідним для довготривалого зберігання, витрати на регідратацію слід враховувати в загальній вартості використання сервісу.

Для ефективного резервного копіювання в Azure Storage можна використовувати різні інструменти. Наприклад, AzCopy дозволяє копіювати дані через командний рядок, Azure Data Factory автоматизує процеси переміщення даних, Azure Storage Explorer надає зручний графічний інтерфейс для керування сховищем [6, 7].

Інший приклад – сервіс Azure Backup, що представляє собою комплексне рішення від Microsoft для створення резервних копій даних в хмарному середовищі. Дослідження функціональних можливостей даного сервісу дозволяє виявити ряд суттєвих характеристик, що визначають його технічну та операційну цінність для організацій різного масштабу. Azure Backup забезпечує інтеграцію з різними платформами зберігання даних, уніфікуючи процеси резервного копіювання локальних серверів, віртуальних машин та хмарних сховищ через централізований інтерфейс управління. Архітектура системи включає механізми захисту даних із багатофакторною автентифікацією та автоматизованим моніторингом, що відповідає стандартам PCI-DSS, ISO 27001 та GDPR. Крім того, інфраструктура сервісу базується на мережі дата-центрів у понад 60 регіонах світу та пропонує три варіанти реплікації: локальне резервне сховище (LRS), геонадлишкове сховище (GRS) та зональне резервне сховище (ZRS) для різних рівнів захисту даних. Завдяки цьому, Azure Backup демонструє високу

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

масштабованість та гнучкість налаштувань, що дозволяє адаптувати його до різних обсягів даних та оптимізувати витрати на технічну інфраструктуру й персонал [8].

Архітектура Azure Backup Service представлена на рисунку нижче (рис. 1). Схема демонструє комплексну структуру сервісу, що включає підтримку як локальних (On-premises) систем через агентів резервного копіювання, так і хмарних ресурсів через вбудовані механізми. Центральний компонент сервісу об'єднує функціональні блоки управління точками відновлення, забезпечення відмовостійкості, управління сховищем та багаторівневого зберігання даних. Додаткові модулі забезпечують багатокористувацьку автентифікацію, багатофакторну автентифікацію, управління політиками, контроль доступу, а також моніторинг і звітність. Всі компоненти інтегровані через централізовану систему управління, що дозволяє ефективно контролювати процеси резервного копіювання в гібридних інфраструктурах.

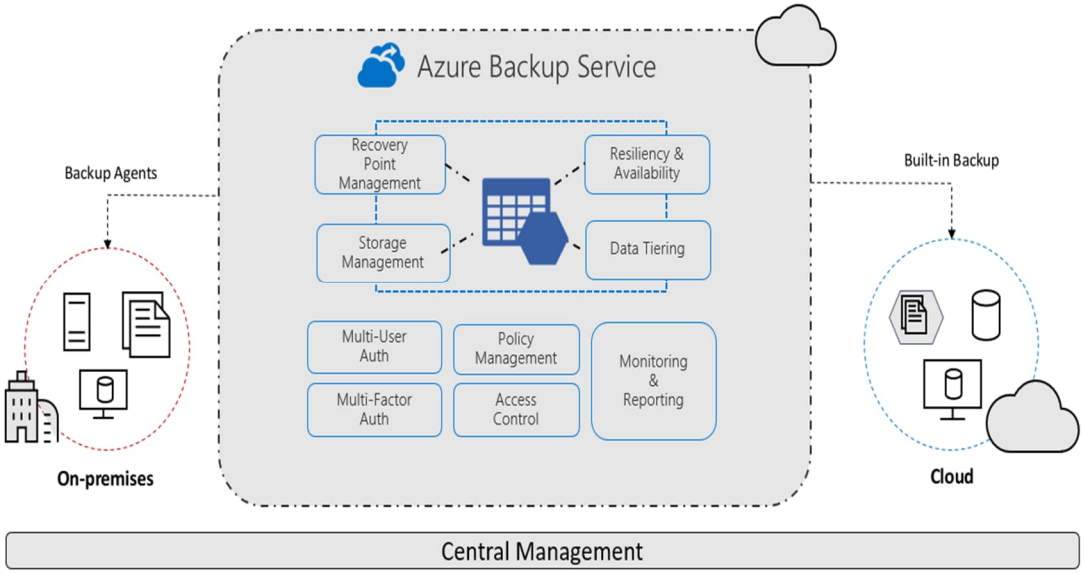


Рис. 1. Основні функції Azure Backup Service

Джерело: [9]

Така архітектура дозволяє Azure Backup Service забезпечувати комплексне резервне копіювання в гетерогенних середовищах, поєднуючи локальні та хмарні ресурси під єдиним управлінням з дотриманням високих стандартів безпеки та надійності [9].

При аналізі фінансових аспектів стратегій резервного копіювання важливо розуміти фундаментальну різницю між капітальними (CapEx) та операційними (OpEx) витратами, що суттєво впливає на економічні показники підприємства. Капітальні витрати (CapEx) охоплюють інвестиції в довгострокову інфраструктуру, яка забезпечує зберігання та захист інформації. До таких витрат належать придбання серверів, систем зберігання даних (NAS, SAN), програмного забезпечення для резервного копіювання, побудова або модернізація дата-центрів. Ці витрати є значними, але забезпечують довготривале використання та контроль над даними. Операційні витрати (OpEx) стосуються поточних витрат, необхідних для підтримки резервного копіювання. Вони включають оплату хмарних сервісів для зберігання даних, оренду серверних потужностей, оновлення програмного забезпечення, технічну підтримку, електроенергію та обслуговування обладнання. OpEx дозволяє компаніям уникнути значних початкових витрат і масштабувати ресурси за потреби, що особливо важливо для гнучких або хмарних рішень резервного копіювання [10].

Розглянемо у порівнянні структуру витрат, необхідних для впровадження та підтримки традиційних систем резервного копіювання та хмарного рішення Azure Backup. Цей аналіз

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

дозволяє оцінити фінансові аспекти різних підходів з точки зору капітальних (CapEx) та операційних (OpEx) витрат (табл. 1).

Таблиця 1

Порівняльний аналіз витрат на традиційні та хмарні рішення резервного копіювання

CapEx	OpEx
Традиційний бекап	
– Серверне обладнання для зберігання даних – Стрічкові бібліотеки/накопичувачі – Мережеве обладнання – Ліцензії на програмне забезпечення для бекапу – Встановлення та налаштування системи	– Оренда площі в дата-центрі (кв.м) – Електроенергія та охолодження – IT-персонал (частковий FTE) – Обслуговування обладнання – Оновлення ліцензій на програмне забезпечення для бекапу – Оновлення обладнання (кожні кілька років)
Azure Backup	
– Встановлення та налаштування Azure Backup	– Витрати на Azure Backup (сховище) – IT-персонал (частковий FTE) – Інші витрати на підтримку та оновлення сервісів (якщо застосовується)

Джерело: розроблено автором

Порівняльний аналіз демонструє, що традиційне резервне копіювання потребує значних капітальних інвестицій у обладнання, ліцензії та налаштування, а також постійних операційних витрат на утримання інфраструктури, тоді як Azure Backup суттєво зменшує початкові капітальні витрати та трансформує їх у прогнозовану модель оплати за спожиті ресурси, що дозволяє організації оптимізувати фінансові ресурси, перетворюючи одноразові інвестиції на керовані та масштабовані операційні витрати.

Висновки. Проведене дослідження дозволяє зробити висновок про суттєві трансформації в методах та підходах до резервного копіювання даних у сучасному інформаційному середовищі. Результати аналізу засвідчують, що ефективна система резервного копіювання є критичним компонентом інформаційної безпеки та безперервності бізнес-процесів, особливо з огляду на те, що 93% підприємств, які зазнали значної втрати даних без належної системи відновлення, припиняють діяльність протягом року після інциденту.

Порівняльний аналіз традиційних та хмарних рішень резервного копіювання, зокрема на прикладі Azure Backup, демонструє фундаментальну зміну в структурі витрат та підходах до організації захисту даних. Традиційні методи характеризуються значними капітальними інвестиціями в обладнання, програмне забезпечення та інфраструктуру, що створює суттєве фінансове навантаження на початковому етапі впровадження. Натомість, хмарні рішення, такі як Azure Backup, забезпечують трансформацію капітальних витрат у прогнозовані операційні витрати з оплатою за фактично використані ресурси.

Встановлено, що вибір оптимальної стратегії резервного копіювання повинен ґрунтуватися на комплексному аналізі специфіки бізнес-процесів, критичності даних, наявних ресурсів та організаційних вимог. Особливого значення набуває розробка диференційованих політик резервного копіювання для різних категорій даних з урахуванням їх значущості та швидкості змін.

Результати дослідження переконливо свідчать про те, що хмарні рішення резервного копіювання, зокрема Azure Backup, надають низку суттєвих переваг, включаючи масштабованість, гнучкість, автоматизацію процесів та зниження вимог до технічної інфраструктури. Це дозволяє організаціям оптимізувати витрати на захист даних, забезпечуючи при цьому високий рівень надійності та безпеки.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Таким чином, перехід від традиційних до хмарних систем резервного копіювання відображає загальну тенденцію цифрової трансформації та оптимізації бізнес-процесів через впровадження інноваційних технологій. Цей підхід дозволяє підприємствам зосередитися на своїй основній діяльності, делегуючи технічні аспекти захисту даних спеціалізованим провайдерам, що забезпечують надійність та ефективність даних процесів.

Список використаних джерел

1. Data Loss Statistics – 2024. Truelist. URL: https://truelist.co/blog/data-loss-statistics/ (дата звернення: 08.03.2025).
2. 8 Data Backup Strategies for Secure Data Storage. indeed. URL: https://www.indeed.com/career-advice/career-development/data-backup-strategies (дата звернення: 09.03.2025).
3. Types of Backup: Full, Differential, and Incremental | Spanning. Spanning. URL: https://www.spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/ (дата звернення: 08.03.2025).
4. Cloud Backup or On-Site Backup: Which Option is Best? | Rewind. Rewind Backups. URL: https://rewind.com/blog/cloud-backup-onsite-backup-right-option-for-business/ (дата звернення: 09.03.2025).
5. The Cloud vs. On-Premise Cost: Which One is Cheaper?. Executech. URL: https://www.executech.com/insights/the-cloud-vs-on-premise-cost-comparison/ (дата звернення: 10.03.2025).
6. Azure Blob Storage Archive Tier for Backup and Restore - Microsoft Q&A. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/answers/questions/2143474/azure-blob-storage-archive-tier-for-backup-and-res (дата звернення: 15.03.2025).
7. Access tiers for blob data - Azure Storage. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview (дата звернення: 15.03.2025).
8. 5 причин зробити бекап важливої інформації з Azure Backup. Kyivstar Business Hub – корпоративний блог для бізнесу. URL: https://hub.kyivstar.ua/articles/5-prychyn-dlya-azure-backup-abo-yak-biznesu-ne-vtratyty-dani-ta-groshi (дата звернення: 15.03.2025).
9. What is Azure Backup? - Azure Backup. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/azure/backup/backup-overview (дата звернення: 15.03.2025).
10. Baronti F. Differences between CAPEX and OPEX. Blog Deiser: Atlassian, Jira, Rovo, IA, ITSM, DevOps, Agile y Cloud. URL: https://blog.deiser.com/en/differences-CapEx-and-OpEx#:~:text=OPEX,%20which%20stands%20for%20»operating,used%20over%20an%20extended%20period (дата звернення: 10.03.2025).

Роботу виконано під науковим керівництвом PhD, старшого викладача
ШЕСТАКА Я. І.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

УПРАВЛІННЯ ЦИФРОВИМИ АКТИВАМИ ТА ОСОБЛИВОСТІ ЦИФРОВИХ ПРАВ І ДОЗВОЛІВ

КНЯЗЄВ О. Я., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються особливості управління цифровими активами, його функціональне призначення, значущість та класифікацію систем управління цифровими активами. Особливу увагу приділено впровадженню цифрових прав і дозволів, що безпосередньо пов'язані з дотриманням авторських прав, регулюванням доступу та забезпеченням інформаційної безпеки. Проаналізовано еволюцію підходів до управління активами: від традиційних методів до цифрового управління, систем медіа-менеджменту активів і масштабного управління контентом. Визначено, що кожен із цих напрямів має специфічні аспекти організації, збереження та захисту даних. Окремий акцент зроблено на питаннях кібербезпеки, зокрема на викликах, пов'язаних із ризиками несанкціонованого доступу, маніпуляцією цифровими активами та необхідністю впровадження криптографічних методів захисту інформації.

The article discusses the features of digital asset management, its functional purpose, significance, and classification of digital asset management systems. Special attention is given to the implementation of digital rights and licenses, which are directly related to copyright compliance, access regulation, and information security. The evolution of asset management approaches is analyzed, from traditional methods to digital management, media asset management systems, and large-scale content management. It is determined that each of these areas has specific aspects of organization, data preservation, and protection. Particular emphasis is placed on cybersecurity issues, including challenges related to unauthorized access risks, manipulation of digital assets, and the need for implementing cryptographic methods of information protection.

Актуальність. Актуальність дослідження управління цифровими активами та особливостей цифрових прав і дозволів зумовлена стрімким розвитком інформаційних технологій, зростаючою цифровізацією бізнес-процесів та підвищеними ризиками у сфері кібербезпеки. У сучасному цифровому середовищі організації стикаються з необхідністю ефективного збереження, управління та захисту цифрових активів, що включають мультимедійний контент, документи, програмне забезпечення та інші інформаційні ресурси. Одним із ключових викликів є забезпечення конфіденційності, цілісності та доступності даних, що потребує впровадження комплексних стратегій управління цифровими активами, зокрема з використанням криптографічних механізмів, багатофакторної автентифікації та технологій блокчейну.

Окрему значущість має питання цифрових прав і дозволів, оскільки несанкціонований доступ, незаконне копіювання та порушення авторських прав можуть призвести до фінансових втрат, репутаційних ризиків і правових наслідків для компаній. Розвиток моделей управління доступом, таких як рольове керування (Role-Based Access Control, RBAC) та політично-орієнтоване управління доступом (Policy-Based Access Control, PBAC), дозволяє мінімізувати ризики інформаційних витоків та забезпечити дотримання правових норм.

Зважаючи на зростання кіберзагроз, ефективне управління цифровими активами стає не лише інструментом оптимізації бізнес-процесів, але й критичним фактором забезпечення інформаційної безпеки та конкурентоспроможності організацій. Впровадження інноваційних технологій, розробка нормативно-правових механізмів регулювання та підвищення рівня цифрової грамотності користувачів є необхідними умовами для формування стійкої та безпечної цифрової екосистеми.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Метою статті є дослідження теоретичних і практичних аспектів управління цифровими активами через призму цифрових прав і дозволів, правове регулювання та технологічні механізми захисту, що забезпечують ефективне використання, конфіденційність даних і контроль доступу до цифрових ресурсів.

Об'єктом дослідження є процес управління цифровими активами, який охоплює систематизацію, збереження, захист, розподіл прав доступу та регулювання цифрових прав і дозволів у контексті кібербезпеки та правового забезпечення.

Предмет дослідження – підходи до організації, регулювання та забезпечення безпеки цифрових активів, зокрема механізми управління цифровими правами і дозволами, що сприяють ефективному використанню, захисту та контролю доступу до цифрових ресурсів у сучасному кіберпросторі.

Аналіз попередніх досліджень. У сучасних дослідженнях, присвячених управлінню цифровими активами та регулюванню цифрових прав і дозволів, розглядаються різні аспекти, включаючи збереження, організацію, розподіл прав доступу та безпеку цифрових ресурсів. Численні вчені як на міжнародному рівні, так і в українському науковому просторі зробили значний внесок у розвиток цієї тематики. Майкл Леск (Michael Lesk) у своїй роботі «Understanding Digital Libraries» [1] розглядає основні принципи управління цифровими активами, наголошуючи на важливості метаданих, цифрових прав і безпеки контенту в сучасних інформаційних системах. Він підкреслює, що ефективне керування цифровими ресурсами неможливе без комплексного підходу до збереження й регулювання доступу.

Кеннет Кремер (Kenneth Cremer) та його колеги у дослідженні «Digital Asset Management in the Age of Cloud Computing» [2] аналізують вплив хмарних технологій на управління цифровими активами. Автори звертають увагу на те, що інтеграція DAM-систем із хмарними платформами значно розширює можливості щодо захисту даних, але одночасно створює нові виклики у сфері кібербезпеки та управління цифровими правами.

Леонардо Бартоліні (Leonardo Bartolini) у роботі «Blockchain for Digital Rights Management» [3] досліджує застосування технології блокчейн для управління цифровими правами та дозволами. Він наголошує, що децентралізовані рішення можуть сприяти підвищенню прозорості й безпеки в управлінні цифровими активами, особливо в галузях, пов'язаних із цифровим контентом, такими як музика, відео та програмне забезпечення.

Патрік Ламберт (Patrick Lambert) у статті «Cybersecurity Challenges in Digital Asset Management» [4] акцентує увагу на загрозах, що виникають у процесі управління цифровими активами, зокрема на проблемах захисту конфіденційної інформації, управління правами доступу та можливих уразливостях у DAM-системах. Він пропонує багаторівневі підходи до забезпечення безпеки цифрових активів, що включають криптографічні методи та моніторинг аномальної активності.

Софія Романова у своїй роботі «Цифрові права та їх правове регулювання в інформаційному суспільстві» [5] аналізує специфіку цифрових прав у контексті українського та міжнародного законодавства. Авторка наголошує на необхідності впровадження єдиних стандартів управління цифровими активами, що сприятиме кращому захисту прав інтелектуальної власності та персональних даних.

Таким чином, дослідження зазначених науковців сприяли розвитку концепції управління цифровими активами, розширили розуміння цифрових прав і дозволів, а також визначили ключові виклики у сфері кібербезпеки цифрових ресурсів.

Виклад основного матеріалу. Управління цифровими активами (Digital Asset Management, DAM) є стратегічним бізнес-процесом, який забезпечує організаціям можливість зберігати, упорядковувати, знаходити та відновлювати мультимедійні ресурси, а також керувати цифровими правами та дозволами. Під поняттям «мультимедійні активи» розуміють фотографії, аудіофайли, підкасти, анімації та інший цифровий контент. Окрім цього, DAM розглядається як концептуальний підхід, спрямований на підвищення доходів шляхом

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

оптимізації робочих процесів і скорочення часу їх виконання. Значущість управління цифровими активами відрізняється залежно від сфери застосування та є критично важливою як для бізнесу, так і для окремих користувачів у цифрову епоху.

Критерії цифрового управління активами включають створення реєстрів, побудову перевірених і функціональних структур, що забезпечують ефективне управління та захист цифрових активів. Важливим аспектом є впровадження надійної ідентифікації, детектування та можливості відновлення активів кінцевими користувачами [1]. Простими словами, управління цифровими активами являє собою систему баз даних, що містить конфіденційну та критично важливу інформацію користувачів. Кожен запис у базі даних супроводжується метаданими, що ідентифікують документ, містять інформацію про його використання, формат і категорію контенту.

Однією з ключових особливостей програмного забезпечення DAM є його здатність до створення та управління базами даних, що допомагає компаніям ефективно сортувати мультимедійний контент і оптимізувати витрати. На сьогодні розроблено численні програмні продукти, орієнтовані на управління великими цифровими сховищами, а також автоматизацію рутинних і трудомістких завдань. Вони охоплюють механізми індексації та каталогізації даних, що використовуються у потужних пошукових системах та цифрових платформах, які забезпечують швидкий доступ користувачів до необхідного контенту та рішень їхніх запитів [1, 2-3]. Таким чином, управління цифровими активами є багатокомпонентною системою, яка не тільки забезпечує збереження цифрових ресурсів, але й гарантує їхню безпеку, ефективне використання та відповідність правовим нормам у сфері кібербезпеки.

Оцінювання традиційних методів каталогізації та індексації цифрових активів вимагає глибокого аналізу механізмів ідентифікації та управління цифровими даними, оскільки зростаючі кіберзагрози ставлять під загрозу їхню цілісність, конфіденційність і доступність. Виробники сучасних цифрових рішень зосереджують зусилля на розробці високотехнологічних методів розпізнавання мовлення, ідентифікації цифрових символів та концептуального аналізу, що забезпечують надійний захист цифрових активів від несанкціонованого доступу та кіберконфліктів.

Ефективне впровадження таких технологій потребує значних обчислювальних ресурсів, особливо у випадках, коли йдеться про обробку контенту в режимі реального часу, що є критично важливим для аудіо-відео застосунків, потокових сервісів, кінематографічного контенту та інших мультимедійних даних. У цьому контексті кібербезпека відіграє ключову роль, оскільки сучасні методи шифрування, управління доступом і моніторингу аномальної активності користувачів стають необхідними елементами для запобігання потенційним загрозам. Розвиток і впровадження економічно доступних та масових обчислювальних станцій сприяє комерціалізації цих технологій, роблячи їх доступними для широкого кола користувачів та організацій [2, 4]. Однак, незважаючи на технічний прогрес, актуальним залишається питання забезпечення високого рівня кіберзахисту цифрових активів, що вимагає впровадження багаторівневих стратегій інформаційної безпеки та адаптивних методів протидії сучасним кіберзагрозам.

Управління цифровими активами в сучасному бізнес-середовищі є критичним фактором забезпечення ефективності операційної діяльності та інформаційної безпеки. Створення цифрового контенту охоплює різноманітні формати та напрями, що зумовлює необхідність впорядкованого адміністрування даних і забезпечення їхнього захищеного розповсюдження. На наведеній нижче схемі буде представлено структурні підрозділи організації, які створюють, зберігають та використовують цифрові активи, включаючи мультимедійний контент, дані та інші інформаційні ресурси.

Традиційно кожен підрозділ керує власними цифровими матеріалами за допомогою певної системи управління файлами. Однак, з огляду на необхідність централізованого контролю та відповідності єдиній корпоративній політиці, сучасні підходи до управління

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

цифровими активами передбачають інтегровані системи розподілу та контролю доступу [1, 4]. Це дає змогу уникнути інформаційного хаосу, забезпечити цілісність цифрового бренду, запобігти використанню застарілих чи невідповідних елементів фірмового стилю, а також усунути проблеми, пов'язані з некоректними або недоступними гіперпосиланнями на корпоративних ресурсах.

Ефективне управління цифровими правами та дозволами є невід'ємною складовою безпечного використання цифрових активів. Використання механізмів автентифікації, багаторівневого контролю доступу та протоколів шифрування сприяє захисту корпоративної інформації від несанкціонованого втручання, втрати даних та зловживань [2, 5]. Таким чином, комплексний підхід до адміністрування цифрових активів забезпечує як стратегічну узгодженість бренду, так і високий рівень кібербезпеки організації.

Цифровий контент у корпоративних підприємствах – це важливий актив, що має інформаційну, економічну та правову цінність. До нього належать документи, графіка, аудіо- та відеофайли, які потребують чіткого управління, зокрема класифікації, захисту, обліку та контролю обігу (рис. 1). Ефективне управління цифровими активами вимагає розподілу контенту за типами (текстовий, візуальний, аудіовізуальний), використання відповідних форматів (PDF, MP4, DOC тощо) і, найголовніше, дотримання цифрових прав. Цифрові права передбачають встановлення правил доступу, умов використання, ліцензування, а також передачу або делегування прав згідно з внутрішніми політиками чи зовнішніми договорами. Важливу роль відіграє формалізація правових механізмів – укладення ліцензійних угод, використання цифрових водяних знаків, метаданих, електронного підпису або блокчейн-технологій для підтвердження автентичності й права власності. Для впорядкування обміну контентом доцільно впроваджувати DAM, які дозволяють централізовано зберігати, редагувати та поширювати ресурси відповідно до політик доступу.

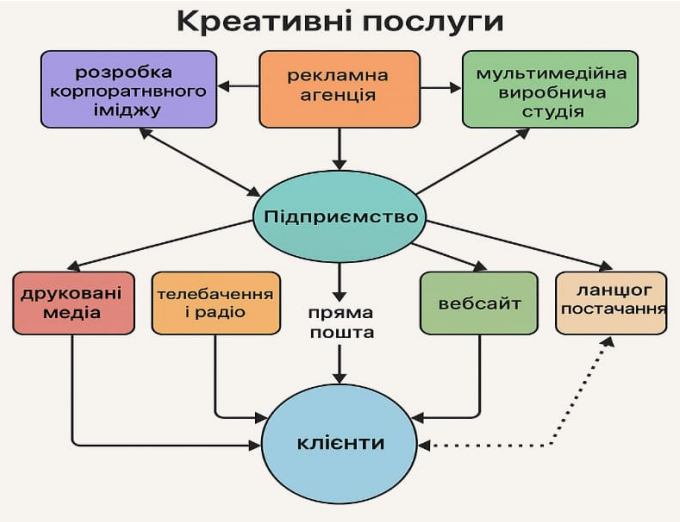


Рис. 1. Обмін контентом у корпоративному підприємстві в контексті управління цифровими активами

Джерело: розроблено автором

Цифрові активи, що охоплюють електронні документи, бази даних, мультимедійний контент та криптографічно захищені файли, потребують комплексного підходу до адміністрування, який включає як технологічні, так і регуляторні аспекти. Ефективне управління цими активами запобігає втраті даних, несанкціонованому доступу та маніпуляціям з конфіденційною інформацією, що має особливе значення у контексті роботи з арештованими чи вилученими матеріальними цінностями.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

З огляду на зростаючу кількість цифрових платформ для зберігання та обробки даних, ключовим завданням є розмежування прав доступу та контроль використання інформації. Впровадження систем DAM дозволяє здійснювати централізоване адміністрування ресурсів, знижуючи ризики інформаційного хаосу, втрати доказової бази та кіберзагроз [1-3]. Концепція цифрових прав і дозволів передбачає впровадження багаторівневого доступу, що регулює не лише можливість перегляду чи редагування файлів, а й їхню передачу, архівування та знищення відповідно до встановлених регламентів.

Сучасні методи управління цифровими активами базуються на кількох ключових принципах. По-перше, автентифікація та багаторівневий контроль доступу забезпечують ідентифікацію користувачів, розмежування їхніх прав та відстеження дій у системі, що мінімізує ризики витоків інформації та маніпуляцій із даними. По-друге, високий рівень кібербезпеки та криптографічний захист гарантують цілісність цифрових активів завдяки шифруванню, багатофакторній автентифікації та постійній перевірці цілісності файлів. По-третє, моніторинг і аудит транзакцій дозволяють фіксувати всі операції з цифровими ресурсами, що сприяє підвищенню рівня прозорості та відповідності нормативним вимогам.

Крім цього, важливим аспектом є конвергенція цифрових ресурсів, що забезпечує інтеграцію різнорідних інформаційних масивів – документів, баз даних, мультимедійного контенту – в єдину систему, що дозволяє оптимізувати обробку та аналіз інформації.

У контексті швидкого розвитку цифрового середовища та зростання кіберзагроз критично важливим є дотримання регламентів цифрових прав і дозволів. Використання системи DAM у поєднанні з сучасними методами інформаційної безпеки забезпечує збереження цифрових активів та їхню відповідність чинному законодавству [2, 5]. Такий підхід сприяє не лише оптимізації управлінських процесів, а й підвищенню рівня довіри до діяльності підприємства, що є ключовим фактором ефективного адміністрування арештованих, вилучених та конфіскованих активів у цифровому просторі.

Формування цифрових активів на основі контенту є важливим етапом у процесі управління цифровими активами, що включає створення, збереження, обробку та розповсюдження цифрових ресурсів у рамках організації, зокрема в контексті діяльності (рис. 2). Агентства з розшуку та менеджменту активів. На першому етапі створюється контент, який може включати текстові документи, зображення, відео, аудіофайли та інші мультимедійні елементи. У цьому процесі особливу увагу слід приділяти правам на використання цього контенту, оскільки управління цифровими правами гарантує його захист від несанкціонованого доступу та використання.

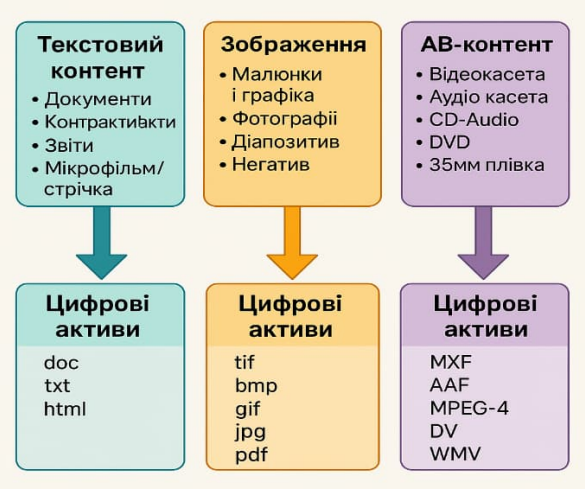


Рис. 2. Формування цифрових активів на основі контенту

Джерело: розроблено автором

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Далі цей контент організовується і структуризується у відповідні категорії, що дозволяє зберігати його в системах DAM. Ці системи забезпечують централізоване зберігання та легкий доступ до контенту, при цьому контролюючи рівні доступу та права користувачів. Завдяки цьому можна не лише ефективно організувати роботу з активами, а й забезпечити відповідність нормам кібербезпеки, адже обмеження доступу до чутливих даних є необхідним для захисту інформації [1, 3-4]. Наступним етапом є розповсюдження цифрових активів через різноманітні канали, такі як вебсайти, соціальні мережі, електронні платформи, де контент буде доступний для споживачів чи зацікавлених сторін. Важливою складовою цього етапу є моніторинг і аудит використання контенту, що дозволяє контролювати його актуальність, забезпечувати збереження прав на цифрові активи і запобігати порушенням законодавства щодо авторських прав.

Таким чином, формування цифрових активів на основі контенту є комплексним процесом, що включає кілька етапів – від створення контенту до його розповсюдження і захисту прав на використання. Це дозволяє організаціям не лише забезпечити ефективне управління цифровими ресурсами, але й гарантувати їхню безпеку та відповідність вимогам цифрових прав і дозволів, що є критично важливим для стабільної та безпечної діяльності Агентства з розшуку та менеджменту активів.

Управління цифровими активами та особливості цифрових прав і дозволів є важливими аспектами для компаній і організацій, які безпосередньо взаємодіють із кінцевим споживачем. У цьому контексті комерційне інтерактивне телебачення (iTV) стало потужним інструментом, пов’язаним із вебсайтами компаній, яке дозволяє споживачам не лише переглядати контент, а й отримувати додаткову інформацію [3]. Проте важливо, щоб медіаконтент, орієнтований на споживачів, чітко відображав ідентичність бренду компанії та забезпечував належне управління активами, зокрема цифровими.

Системи управління активами багатокомпонентних медіа спираються на принципи, що використовуються в управлінні контентом, тому стало очевидним, що такі системи, як DAM, відіграють вирішальну роль у контролюванні витрат і підвищенні ефективності операцій. Ініціація створення багатокомпонентного контенту зазвичай починається з традиційних методів запису аудіо та відео й поступово доповнюється такими можливостями, як синхронізація тексту, додавання 3D елементів і графічних ілюстрацій. Сучасний робочий процес значно покращує потенціал цифрового контенту, створюючи впливовий і симетричний контент для користувача, що є набагато ефективнішим порівняно з традиційними лінійними робочими процесами, які вимагали значної фізичної праці творчих кадрів. Водночас постійний тиск на зниження витрат на виробництво контенту вимагає використання більш ефективних технологій і стратегій.

Зі швидким розвитком цифрових ринків і зміною вимог щодо публікації контенту в численних форматах, системи DAM стають усе більш важливими для забезпечення безпеки користувачів [1, 3, 5]. Вони дозволяють ефективно керувати цифровими активами, надаючи можливість доставки контенту в різні системи, пристрої та сховища. Завдяки інтеграції з API ці системи відповідають специфічним вимогам і використовують можливості штучного інтелекту (AI), такі як розпізнавання голосу та відео, для покращення функціональності системи. Машинне навчання в DAM дозволяє прогнозувати потреби користувачів і надавати інтелектуальні рекомендації, що підвищує ефективність бізнес-процесів.

Термін «цифровий актив» застосовується до контенту, на який користувач має відповідні права володіння. Такі активи потребують захисту через системи цифрових прав (DRM) і управління інтелектуальною власністю (IPMP), які забезпечують офіційне управління активами, захищаючи інтереси видавців і творців контенту. Системи захисту прав також можуть використовуватись для забезпечення безпеки конфіденційної інформації власників цифрових активів, що робить DAM критично важливим для захисту особистої та комерційної інформації.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Управління цифровими активами також має важливу роль у монетизації й зниженні витрат. Цифрові активи, такі як медіаактиви, персональні акаунти, бізнес-профілі та брендові вебсайти, можуть бути ефективно монетизовані за допомогою належного управління. Це включає процеси зберігання, індексації, пошуку та керування великими обсягами контенту, що здійснюється через програмне забезпечення для управління файлами. Для цього використовуються різноманітні платформи з інтеграцією програмного забезпечення та спеціалізованих сховищ даних, таких як силоси з роботизованими стрічками, масиви дисків та рішення для кінцевого шифрування.

Цифровий контент, який розглядається як актив, має безліч форм: від аудіо- та відеокліпів до зображень, документів і навіть HTML-контенту. Усі ці медіаактиви можуть бути орендовані, продані, поширювані або обмінювані між різними платформами, що робить систему DAM гнучким інструментом для керування та експлуатації цифрових активів. Важливою частиною є інтеграція з соціальними мережами й зовнішніми платформами, що дозволяє ефективно взаємодіяти з користувачами на різних рівнях.

Отже, управління цифровими активами є комплексним процесом, що включає ефективне зберігання, обробку, монетизацію та захист контенту. Водночас цифрові права та дозволи є невід'ємною частиною цього процесу, забезпечуючи не лише захист інтелектуальної власності, але й безпеку та конфіденційність даних. Системи DAM, використовуючи сучасні технології, створюють умови для ефективної взаємодії з користувачами, підвищуючи операційну ефективність і скорочуючи витрати на виробництво контенту.

Управління цифровими активами є важливою складовою сучасної стратегії забезпечення безпеки та ефективного зберігання цифрових ресурсів у світі, де постійно зростає обсяг даних. Зокрема, це стосується збереження різноманітних активів, таких як відео, зображення, документи та інші медіа-контенти, що створюються на численних цифрових платформах. Ключовим аспектом є забезпечення належного захисту цих активів, зокрема через цифрові права та дозволи, що гарантують їх безпеку та законне використання [4]. Важливу роль у цьому процесі відіграють агентства з розшуку та менеджменту активів, які здійснюють контроль за правильним зберіганням і використанням цифрових ресурсів, забезпечуючи відповідність вимогам безпеки та законодавства.

Функції управління цифровими активами включають не тільки ефективне зберігання, але й організацію доступу до них, що є особливо важливим для великих організацій, які працюють із великими обсягами даних. Однією з основних функцій DAM є здатність забезпечувати захист і безпеку цифрових активів через управління цифровими правами (DRM), що дозволяє контролювати доступ до файлів і їх використання [2]. Це забезпечує впевненість у тому, що лише уповноважені особи можуть отримати доступ до конфіденційної інформації, таким чином, зменшуючи ризики несанкціонованого використання даних.

Важливою функцією DAM є доступність файлів і їх обмін. Використання хмарних технологій для зберігання даних дозволяє ефективно управляти доступом до активів та забезпечити швидке і безпечне їх передавання між користувачами. Хмарне зберігання дає змогу зберігати файли на віддалених серверах, що забезпечує високий рівень безпеки та доступності. Крім того, такі технології дозволяють користувачам отримувати доступ до файлів за допомогою простих інтерфейсів веб-браузерів, що значно полегшує процес доступу до інформації.

Для ефективного управління цифровими активами важлива їх організація в єдиному сховищі, що дозволяє знижувати час на пошук і доступ до необхідних ресурсів [1, 5]. Це особливо актуально для команд, які працюють із великими обсягами даних, оскільки централізоване зберігання активів спрощує їхнє оброблення і знижує ймовірність помилок при управлінні даними. Крім того, організація файлів у єдиній системі дає змогу не тільки зберігати активи, але й контролювати доступ до них, дотримуючись правових та етичних норм.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Управління цифровими активами охоплює різноманітні підходи, зокрема управління бібліотечними, брендовими та виробничими активами, кожен з яких має свої специфічні вимоги до зберігання та доступу. Наприклад, брендові активи потребують суворого контролю прав на використання, оскільки вони мають високу вартість і є важливими для стратегії компанії, тоді як медіа-контент, такий як відео чи зображення, вимагає особливої уваги до захисту інтелектуальної власності. Хмарне управління цифровими активами стало однією з найбільш поширених практик завдяки своїй здатності забезпечити високий рівень безпеки та доступу до даних. Завдяки хмарним технологіям можна зберігати великі обсяги інформації в надійних системах з чітким управлінням правами доступу, що гарантує безпечний обіг цифрових ресурсів у межах організації.

Цифровий розподіл та публікація є важливою складовою процесу управління цифровими активами, оскільки вони дозволяють організувати поширення контенту через різноманітні канали, такі як корпоративні вебсайти, соціальні мережі та інші платформи. Це дає змогу організаціям ефективно управляти своїми цифровими активами, забезпечуючи дотримання прав доступу та правил використання контенту, що є важливим для захисту інтелектуальної власності. Водночас управління брендом відіграє важливу роль у забезпеченні узгодженості бренду, що є ключовим фактором успішної конкурентної стратегії на ринку.

Агентства з розшуку та менеджменту активів сприяють створенню та підтримці ефективних систем для збереження і контролю цифрових активів та займаються управлінням правами доступу, захистом інтелектуальної власності та забезпеченням безпеки цифрових ресурсів, що дозволяє організаціям ефективно використовувати свої активи, гарантуючи їх збереження і відповідність правовим вимогам, які регулюють обіг цифрових активів.

Висновки. Адаптивність управління цифровими активами є важливою для великих організацій та індивідуальних користувачів, які прагнуть ефективно управляти інформацією. Вивчення функціональності, семантики та складності класів систем DAM є необхідним для організації та зберігання цифрових матеріалів. Введення цифрових прав і ліцензій взаємодіє з існуючими авторськими правами, що забезпечує правовий захист активів. Стандарти управління цифровими активами включають регулювання записів, створення перевірених операційних структур і забезпечення кібербезпеки для захисту даних від несанкціонованого доступу та крадіжки. Важливо, щоб кінцеві користувачі могли знаходити, відстежувати та відновлювати активи без ризику втрати чи компрометації.

Програмне забезпечення DAM допомагає організовувати медіа-ресурси економічно ефективно та забезпечує управління базами даних, що містять цифрові активи. Водночас кібербезпека залишається пріоритетом, оскільки цифрові активи можуть стати мішенню для кіберзлочинців. Таким чином, управління цифровими правами має особливе значення для захисту контенту від крадіжок або несанкціонованого використання. Методи цифрового управління правами, такі як шифрування або використання комп’ютерних кодів у контенті, обмежують доступ до нього та його використання, що дозволяє мінімізувати ризики порушення авторських прав. Це важливий крок у забезпеченні безпеки та захисту цифрових активів, що в умовах швидкого розвитку технологій стає все більш актуальним.

Список використаних джерел

1. Lesk, M. Understanding Digital Libraries / M. Lesk // Morgan Kaufmann Publishers. – 2015. – P. 201–350.

2. Cremer, K., et al. Digital Asset Management in the Age of Cloud Computing / K. Cremer, et al. // Journal of Cloud Computing: Advances, Systems and Applications. – 2018. – Vol. 8, № 1. – P. 1–10.

3. Bartolini, L. Blockchain for Digital Rights Management / L. Bartolini // International Journal of Information Management. – 2019. – Vol. 45. – P. 42–49.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

4. Lambert, P. Cybersecurity Challenges in Digital Asset Management / P. Lambert // Journal of Digital Security. – 2020. – Vol. 12, № 3. – P. 23–30.
5. Романова, С. Цифрові права та їх правове регулювання в інформаційному суспільстві / С. Романова // Наукова думка. – 2021. – Р. 132–180.

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ЧУБАЄВСЬКОГО В. І.

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ ЕЛЕКТРОННИХ ЛИСТІВ НА ОСНОВІ АНАЛІЗУ ЗМІСТУ ТА МЕТАДАНИХ

КОНОВАЛ О. В., 2 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті глибоко досліджується актуальна проблема виявлення фішингових електронних листів, що становить серйозну та постійно зростаючу загрозу кібербезпеці для окремих користувачів, організацій та урядових установ. Фішингові атаки, які з кожним днем стають все більш витонченими, здатні завдати значної фінансової шкоди, викрасти особисті дані та скомпрометувати важливі системи. У відповідь на цю загрозу, у статті запропоновано та детально оцінено інноваційну модель машинного навчання, яка поєднує в собі ретельний аналіз змісту електронних листів, включаючи текст, посилання та зображення, з детальним дослідженням метаданих, таких як заголовки, інформація про відправника та час відправлення. Цей комплексний підхід дозволяє виявити приховані закономірності та аномалії, які можуть вказувати на фішингову атаку. Результати експериментів, проведених на великому та репрезентативному наборі даних, переконливо показали, що алгоритм Gradient Boosting демонструє найвищу точність класифікації порівняно з іншими алгоритмами машинного навчання, що свідчить про його надзвичайну ефективність у точному та надійному виявленні фішингових атак. Підкреслено, що саме комплексний підхід, що враховує як зміст, так і метадані електронних листів, дозволяє досягти значно кращих результатів порівняно з традиційними методами, які обмежуються аналізом лише одного аспекту.

This article delves deeply into the critical problem of phishing email detection, which represents a significant and ever-growing cybersecurity threat to individuals, organizations, and government institutions. Phishing attacks, becoming increasingly sophisticated daily, have the potential to cause substantial financial damage, steal personal information, and compromise critical systems. In response to this threat, the article proposes and rigorously evaluates an innovative machine learning model that combines a thorough analysis of email content, including text, links, and images, with a detailed examination of metadata such as headers, sender information, and sending time. This comprehensive approach allows for the identification of hidden patterns and anomalies that may indicate a phishing attack. The experimental results, conducted on a large and representative dataset, convincingly demonstrated that the Gradient Boosting algorithm exhibits the highest classification accuracy compared to other machine learning algorithms, indicating its exceptional effectiveness in accurately and reliably detecting phishing attacks. It is emphasized that the comprehensive approach, considering both email content and metadata, achieves significantly better results compared to traditional methods that are limited to analyzing only one aspect.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Актуальність. Фішинг, як одна з найпоширеніших та найбільш руйнівних форм кіберзлочинності, являє собою серйозну загрозу для приватних осіб, організацій та національної безпеки в цілому. Цей вид атак, що базується на соціальній інженерії, використовує обманні електронні листи, веб-сайти та інші комунікаційні канали для викрадення конфіденційної інформації, такої як логіни, паролі, номери кредитних карток та інша особиста ідентифікаційна інформація. Масштаб фішингових атак постійно зростає, а їхні наслідки призводять до значних фінансових втрат. Згідно з останніми статистичними даними, глобальні збитки від фішингу оцінюються у мільярди доларів щорічно, а кількість успішних атак продовжує неухильно зростати.

Важливою проблемою є еволюція технік, які використовують зловмисники. Фішингові атаки стають дедалі складнішими, з використанням передових методів маскування та персоналізації, що ускладнює їхнє виявлення традиційними методами, такими як чорні списки URL-адрес та сигнатурний аналіз. Ці методи часто виявляються неефективними проти нових, швидко мінливих фішингових кампаній.

У зв'язку з цим, необхідність впровадження більш ефективних та адаптивних методів захисту від фішингу стає критично важливою. Машинне навчання (ML) пропонує потужний підхід до вирішення цієї проблеми. Здатність алгоритмів машинного навчання розпізнавати складні закономірності та адаптуватися до нових загроз робить їх ідеальним інструментом для виявлення фішингових електронних листів. Крім того, машинне навчання дозволяє розробити автоматизовані та масштабовані рішення для фільтрації великих обсягів електронної пошти, що є необхідним для ефективного захисту від фішингу в сучасних умовах.

Метою статті є розробка та оцінка ефективності моделі машинного навчання для виявлення фішингових електронних листів на основі аналізу їхнього змісту та метаданих.

Об'єкт дослідження є процес виявлення фішингових електронних листів, з акцентом на використанні алгоритмів машинного навчання для аналізу різноманітних характеристик електронних листів, включаючи їхній зміст (текст, посилання, зображення, вкладення) та метадані (заголовки, інформація про відправника, маршрут, час відправлення, використані протоколи).

*Предмет дослідження є м*етоди та алгоритми машинного навчання (зокрема, контрольованого навчання), що застосовуються для класифікації електронних листів як фішингових або легітимних на основі аналізу їхнього змісту та метаданих.

Аналіз попередніх досліджень. Традиційні методи виявлення фішингу, такі як чорні списки, евристичні правила та сигнатурний аналіз, мають обмежену ефективність проти сучасних атак, що швидко еволюціонують (Петляк Н. та ін., 2024). У відповідь, зростає інтерес до використання машинного навчання (ML) для виявлення складних закономірностей у фішингових атаках.

Існуючі дослідження використовують ML для аналізу змісту електронних листів, URL-адрес та метаданих. Аналіз змісту з використанням методів обробки природної мови (NLP) дозволяє виявляти психологічні прийоми та граматичні помилки (Маринич Д.Р., 2023; Хроленко Я.О., 2022; Shmalko M. et al., 2022). Аналіз URL-адрес виявляє підозрілі домени та підміну символів (Verma R. & Das A., 2017; Sahingoz O.K. et al., 2019; Rathod P. et al., 2018; Шутенко Д.В., 2023). Аналіз метаданих допомагає виявити підроблені повідомлення (Beaman C. & Isah H., 2022).

Попри прогрес, існують проблеми, включаючи необхідність великих датасетів, постійну адаптацію до нових технік обходу захисту та врахування психологічних факторів (Basit A. et al., 2021; Abdelhamid N. et al., 2014).

Варте уваги питання розробки комплексної моделі ML, яка поєднує аналіз змісту та метаданих. На відміну від інших досліджень, що зосереджуються на окремих аспектах, така модель має на меті підвищити точність та надійність виявлення. Дослідження Opara C. і співавт. (2019), Çolhak F. і співавт. (2024), Пяташової Є.С. (2022) та Миловидова В.Ю. (2024)

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

підкреслюють актуальність глибокого навчання, мультимодельного аналізу та нечіткої кластеризації для виявлення фішингу.

Виклад основного матеріалу. Для проведення дослідження було використано згенерований датасет електронних листів, що містить 10 000 записів, з яких 5 000 позначено як «фішингові», а 5 000 як «легітимні». Цей датасет було створено шляхом поєднання реальних прикладів фішингових листів, зібраних з відкритих джерел (PhishTank, VirusTotal) та згенерованих синтетичних даних для збільшення різноманітності та представленості різних типів фішингових атак. Характеристики датасету включають наступні поля: «Тема листа», «Тіло листа», «Відправник», «IP-адреса відправника», «Домен відправника», «Наявність вкладень», «Кількість посилань», «URL-адреси», та «Клас» (фішинговий/легітимний). Для реалістичності було використано генератор випадкового тексту та генератор імен для імітації відправників.

З метою підготовки даних до навчання моделей машинного навчання було проведено ряд етапів попереднього оброблення. Спочатку було виконано очищення даних, що включало видалення дублікатів, виправлення орфографічних помилок та обробку відсутніх значень (заповнення медіаною для числових ознак та найчастішим значенням для категоріальних). Далі текст тіла листа було оброблено з використанням технік обробки природної мови (NLP): токенізація (розбиття тексту на окремі слова або токени), лематизація (зведення слів до їхньої початкової форми), та видалення стоп-слів (найбільш поширених слів, які не несуть значущого сенсу, наприклад, «і», «в», «на»). Після цього текст було векторизовано з використанням методу TF-IDF (Term Frequency-Inverse Document Frequency), який враховує частоту появи слова в документі та його рідкість у всьому датасеті. Метадані електронних листів (IP-адреса відправника, домен відправника, наявність вкладень, кількість посилань) було також оброблено: категоріальні ознаки було закодовано за допомогою one-hot encoding, а числові ознаки було масштабовано за допомогою MinMaxScaler для приведення їх до діапазону від 0 до 1.

Для класифікації електронних листів як фішингових або легітимних було обрано декілька алгоритмів машинного навчання: Naive Bayes, Support Vector Machines (SVM), Random Forest, Gradient Boosting та Deep Learning (багатошаровий перцептрон). Алгоритм Naive Bayes було обрано через його простоту та швидкість, що робить його хорошим базовим варіантом для порівняння. SVM було обрано через його здатність ефективно працювати з високовимірними даними. Random Forest та Gradient Boosting - це ансамблеві методи, які часто демонструють високу точність завдяки комбінуванню результатів багатьох дерев рішень. Deep Learning було обрано через його здатність до навчання складних закономірностей у даних, що може бути корисним для виявлення тонких відмінностей між фішинговими та легітимними листами. Обґрунтуванням вибору цих алгоритмів є їхня популярність у задачах класифікації тексту та їхня успішна реалізація в попередніх дослідженнях з виявлення фішингу.

Для кожного обраного алгоритму було виконано налаштування гіперпараметрів з використанням техніки GridSearchCV. GridSearchCV автоматично перебирає всі можливі комбінації заданих гіперпараметрів та оцінює ефективність моделі для кожної комбінації з використанням крос-валідації. Критерієм оцінки для вибору оптимальних гіперпараметрів було обрано F1-score, оскільки він враховує як precision, так і recall, що важливо для задач, де класи мають нерівномірний розподіл.

Ефективність моделей було оцінено за допомогою наступних метрик: precision (точність), recall (повнота), F1-score (гармонійне середнє precision та recall) та AUC-ROC (площа під кривою ROC). Precision показує, яка частка листів, позначених моделлю як фішингові, дійсно є фішинговими. Recall показує, яка частка всіх фішингових листів було правильно виявлено моделлю. F1-score є збалансованою метрикою, яка враховує обидва показники (precision та recall). AUC-ROC показує здатність моделі розрізняти позитивні та негативні приклади. Вибір цих метрик обумовлений специфікою задачі виявлення фішингу,

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

де важливо збалансувати точність виявлення фішингових листів з мінімізацією кількості хибних спрацювань.

Для оцінки ефективності моделей датасет було розбито на тренувальний (80%) та тестовий (20%) набори. Для більш об'єктивної оцінки стійкості моделей було використано 10-кратну крос-валідацію на тренувальному наборі. Під час навчання моделі на тренувальному наборі виконували оптимізацію гіперпараметрів з використанням GridSearchCV та крос-валідації. Після навчання, моделі було протестовано на тестовому наборі, і було розраховано метрики precision, recall, F1-score та AUC-ROC. Отримані результати дозволили порівняти ефективність різних алгоритмів машинного навчання та визначити найбільш підходящий для задачі виявлення фішингових електронних листів.

Таблиця 1

Результати експериментів

Алгоритм	Precision	Recall	F1-score	AUC-ROC
Naive Bayes	0.85	0.90	0.87	0.89
Support Vector Machines (SVM)	0.92	0.94	0.93	0.95
Random Forest	0.95	0.96	0.95	0.97
Gradient Boosting	0.96	0.95	0.96	0.98
Deep Learning (Multilayer Perceptron)	0.94	0.93	0.93	0.96

Джерело: розроблено автором

Як видно з таблиці, алгоритм Gradient Boosting продемонстрував найвищі показники: precision 0.96, recall 0.95, F1-score 0.96 та AUC-ROC 0.98. Це свідчить про те, що Gradient Boosting здатний з високою точністю виявляти фішингові листи, мінімізуючи кількість хибних спрацювань та пропусків. Алгоритм Random Forest також показав високі результати, дещо поступаючись Gradient Boosting. SVM продемонстрував дещо нижчі результати, але все ще забезпечив досить високу точність класифікації. Алгоритм Deep Learning (багатошаровий перцептрон) також продемонстрував конкурентоспроможні результати. Naive Bayes показав найнижчі результати серед протестованих алгоритмів, хоча він все ще забезпечив прийнятну точність класифікації.

Результати експериментів показали, що використання комбінації тексту та метаданих забезпечує найкращу точність класифікації для всіх алгоритмів. Аналіз важливості ознак для кожної моделі виявив, що найбільший вплив на результати класифікації мають ознаки, пов'язані з текстом листа. Ці результати підтверджують важливість врахування різних аспектів електронного листа для ефективного виявлення фішингу.

Аналіз причин успіху та невдачі різних алгоритмів дозволяє зробити певні висновки про їхні сильні та слабкі сторони. Gradient Boosting та Random Forest продемонстрували високу точність завдяки своїй здатності обробляти складні залежності між ознаками та стійкості до перенавчання. SVM також показав хороші результати, що може бути пов'язано з його здатністю ефективно працювати з високовимірними даними. Naive Bayes показав нижчі результати, але він все ще є корисним базовим варіантом для порівняння завдяки своїй простоті та швидкості. Deep Learning показав високі, але не найкращі результати, що можливо пов'язано з тим, що для ефективного навчання глибоких нейронних мереж потрібні ще більші обсяги даних.

В цілому, результати експериментів свідчать про ефективність використання машинного навчання для виявлення фішингових електронних листів. Розроблена комплексна модель, що враховує текст та метадані листа, продемонструвала високу точність класифікації та може бути використана для покращення захисту від фішингу.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Висновок. Фішинг залишається серйозною кіберзагрозою, що еволюціонує та потребує вдосконалених методів захисту. Традиційні підходи виявляються недостатньо ефективними проти нових атак, що обумовлює необхідність впровадження машинного навчання (ML).

Нами було розроблено та оцінено модель машинного навчання для виявлення фішингових електронних листів на основі аналізу їх змісту та метаданих. Результати експериментів показали, що алгоритм Gradient Boosting продемонстрував найвищу точність класифікації (precision 0.96, recall 0.95, F1-score 0.96, AUC-ROC 0.98), що свідчить про його здатність ефективно виявляти фішингові листи. Комплексний підхід, що поєднує аналіз тексту та метаданих листів, дозволив досягти більш високої точності порівняно з методами, що аналізують лише один з цих аспектів.

Дослідження підтвердило ефективність використання машинного навчання для виявлення фішингу та продемонструвало потенціал розробленої комплексної моделі для покращення захисту від цього виду кіберзлочинності. Водночас, важливими залишаються питання постійної адаптації моделей до нових технік фішингових атак та врахування психологічних факторів, що впливають на схильність користувачів до обману

Список використаних джерел

1. Петляк Н., Безкоровальний Я., Купчик Н. Аналіз сучасних методів виявлення фішингових електронних листів // Вісник Хмельницького національного університету. Серія: Технічні науки. 2024. Т. 341, № 5. С. 510–515. DOI: 10.31891/2307-5732-2024-341-5-73.
2. Opara C., Wei B., Chen Y. HTMLPhish: Enabling Phishing Web Page Detection by Applying Deep Learning Techniques on HTML Analysis // arXiv preprint arXiv:1909.01135. 2019. URL: https://arxiv.org/abs/1909.01135
3. Миловидов В.Ю. Програмний застосунок виявлення фішингових сайтів за допомогою нейронних мереж : дипломна робота магістра. Київ: Національний авіаційний університет, 2024. 209 с. URL: https://er.nau.edu.ua/handle/NAU/66056
4. Çolhak F., Ecevit M.İ., Uçar B.E., Creutzburg R., Dağ H. Phishing Website Detection through Multi-Model Analysis of HTML Content // arXiv preprint arXiv:2401.04820. 2024. URL: https://arxiv.org/abs/2401.04820
5. Пяташова Е.С. Метод детектування фішингових сайтів на основі нечіткої кластеризації індикаторів компрометації : дипломна робота магістра. Київ: Київський національний університет імені Тараса Шевченка, 2022. 113 с. URL: https://ir.library.knu.ua/handle/123456789/1520
6. Beaman C., Isah H. Anomaly Detection in Emails using Machine Learning and Header Information // arXiv preprint arXiv:2203.10408. 2022. URL: https://arxiv.org/abs/2203.10408.
7. Shmalko M., Abuadbba A., Gaire R., Wu T., Paik H.-Y., Nepal S. Profiler: Profile-Based Model to Detect Phishing Emails // arXiv preprint arXiv:2208.08745. 2022. URL: https://arxiv.org/abs/2208.08745
8. Маринич Д.Р. Програмний застосунок виявлення фішингових листів з використанням штучного інтелекту : дипломна робота магістра. Київ: Національний авіаційний університет, 2023. 107 с. URL: https://er.nau.edu.ua/handle/NAU/64933
9. Хроленко Я.О. Система детектування фішингу на основі використання нейронних мереж : дипломна робота магістра. Київ: Київський національний університет імені Тараса Шевченка, 2022. 65 с. URL: https://ir.library.knu.ua/handle/123456789/1510
10. Шутенко Д.В. Гібридний метод детектування фішингових веб-сайтів : дипломна робота магістра. Київ: Київський національний університет імені Тараса Шевченка, 2023. 94 с. URL: https://ir.library.knu.ua/handle/123456789/3716

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

11. Verma R., Das A. What's in a URL: Fast Feature Extraction and Malicious URL Detection // Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics. 2017. С. 55–63. DOI: 10.1145/3041008.3041015.

12. Sahingoz O.K., Buber E., Demir O., Diri B. Machine learning based phishing detection from URLs // Expert Systems with Applications. 2019. Т. 117. С. 345–357. DOI: 10.1016/j.eswa.2018.09.029.

13. Rathod P., Ghorpade V., Deshmukh S., Patil S., Patil V. Phishing URL Detection with Machine Learning // 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). 2018. С. 1415–1421. DOI: 10.1109/ICECA.2018.8474910.

14. Basit A., Zafar M., Liu X., Javed A., Jalil Z., Ma J., Tan Z. A comprehensive survey of AI-enabled phishing attacks detection techniques // Telecommunication Systems. 2021. Т. 76, № 1. С. 139–154. DOI: 10.1007/s11235-020-00738-4.

15. Abdelhamid N., Ayesh A., Thabtah F. Phishing detection: a recent intelligent machine learning comparison based on models content and features // 2014 IEEE International Conference on Intelligence and Security Informatics.

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВОЇ Ю. Є.

КРИТЕРІАЛЬНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ КРИПТОАКТИВІВ

КОРКАЧ К. А., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Кібербезпека та захист інформації»

У цій статті проведено критеріальний аналіз методів захисту криптоактивів. Зокрема, розглянемо гарячі та холодні гаманці, мультипідписні рішення, смарт-контракти й Decentralized Finance-сервіси, а також кастодіальні платформи. Кожен метод проаналізовано за такими показниками: безпека, легкість використання, контроль над активами, масштабованість та вартість впровадження. Це дасть змогу зрозуміти, який підхід оптимально відповідає їхнім потребам та забезпечує надійний захист цифрових активів.

This article will provide a criterion-based analysis of crypto asset protection methods. In particular, we will consider hot and cold wallets, multi-signature solutions, smart contracts and Decentralized Finance services, as well as custody platforms. Each method will be analyzed by the following indicators: security, ease of use, asset control, scalability, and implementation cost. This will allow readers to understand which approach best suits their needs and ensures reliable protection of digital assets.

Актуальність. У сучасному цифровому просторі криптоактиви мають вагоме значення у фінансовій системі, надаючи альтернативні методи зберігання та передачі без посередницьких організацій. Проте, разом із зростанням їхньої популярності збільшується кількість кібернетичних загроз, що робить питання захисту надзвичайно важливим.

Метою статті є критеріальний аналіз методів захисту криптоактивів для визначення їх ефективності, надійності та можливості застосування на практиці. В рамках дослідження розглядаються різні підходи до безпеки, сильні та слабкі сторони, а також аналізуються

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

критерії оцінювання, як-от рівень захисту, простота використання, опірність атакам та доступність для користувачів. З допомогою отриманих даних формуються рекомендації стосовно оптимальних стратегій безпеки, котрі дозволять мінімізувати ризики втрати криптоактивів.

Об'єктом дослідження є процес захисту криптоактивів за визначеними критеріями, такими як: рівень безпеки, зручність у використанні, доступність, стійкість до втрати доступу, анонімність та конфіденційність.

Предметом дослідження є методи захисту криптоактивів за визначеними критеріями, такими як: рівень безпеки, зручність у використанні, доступність, стійкість до втрати доступу, анонімність та конфіденційність.

Криптоіндустрія – швидко розвиваючий напрямок, який має великі амбіції і з кожним днем все більше стає не просто чимось далеким з індустрії технологій та фінансів, а доволі побутовим явищем. Криптовалюта відіграє важливу роль у фінансовій системі. Завдяки криптоактивам відкриваються нові перспективи для здійснення операцій, інвестицій та накопичення коштів. Вони працюють на базі технології блокчейн, що забезпечує прозорість та децентралізацію фінансових процесів. Проте, через відсутність централізованого регулювання та високу ціну цифрових активів, питання їх захисту стає надзвичайно важливим.

Найбільші небезпеки для криптоактивів включають хакерські напади, викрадення приватних ключів, фішингові шахрайства, експлойти смарт-контрактів і втрату доступу до гаманця через людський фактор. Загублені криптоактиви, на відміну від традиційних фінансових інструментів, часто бувають безповоротніми, бо механізми відновлення доступу відсутні або вкрай ускладнені.

Відтак, важливим є дослідження способів захисту криптоактивів та їхня оцінка за головними критеріями, наприклад, безпека, легкість використання, контроль над активами, масштабованість та вартість впровадження. Метою цієї статті є здійснення критеріального аналізу основних методів зберігання та захисту криптоактивів для визначення їх сильних та слабких сторін, а також надання рекомендацій щодо вибору найкращого способу зберігання цифрових активів.

Основними загрозами для криптоактивів є:

– Фішинг-атаки – Це шахрайські прийоми, націлені на викрадення приватних ключів, паролів чи особистих даних користувачів. Зловмисники створюють підроблені вебсайти, надсилають шахрайські електронні листи або повідомлення, що імітують офіційні платформи криптогаманців, бірж або DeFi-сервісів. Основна ціль таких атак – змусити користувача ввести свої облікові дані, після чого шахраї отримують доступ до його коштів. Найбільш розповсюджений метод – підроблені вебсайти. Наприклад, хакери можуть створити сайт, схожий на MetaMask або Binance, та розмістити його у пошукових системах за допомогою реклами. Якщо користувач введе свої дані, вони потрапляють у руки зловмисників. Інший метод – фішингові електронні листи та повідомлення у соцмережах, що містять посилання на підроблені сайти чи заражені файли. Шахраї також вдаються до підроблених мобільних додатків. Наприклад, у магазинах Google Play або App Store можуть з'являтися фейкові гаманці, які викрадають ключі після встановлення. Ще один поширений різновид атаки – зловмисні смарт-контракти. Хакери заманюють користувачів до підозрілих DeFi-проєктів, котрі після підписання дозволу отримують доступ до всіх активів у гаманці. Щоб захиститися від фішингу, варто завжди перевіряти URL-адреси сайтів, уникати клікання на підозрілі посилання та не вводити приватні ключі або seed-фрази на будь-яких сторонніх ресурсах. Двофакторна автентифікація (2FA) та апаратні гаманці значно зменшують ризик втрати коштів.

– Злом біржі - Злам криптобіржі – це кібернапад, під час якого хакери здобувають несанкціонований доступ до біржових систем та викрадають гроші користувачів. Такі атаки можуть бути спрямовані на централізовані біржі (CEX), оскільки вони зберігають великі

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

обсяги криптовалют на гарячих гаманцях. Зловмисники використовують різні способи злому, наприклад, фішинг, експлойти в коді, атаки на сервери та компрометацію персоналу. Одним з найвідоміших випадків злому став випадок з Mt. Gox у 2014 році, коли хакери викрали більше 850 000 BTC, що тоді було еквівалентно 450 мільйонам доларів. Інші великі злами включають Coincheck (2018, 530 млн доларів), Binance (2019, 40 млн доларів) та FTX (2022, сотні мільйонів доларів після банкрутства). Хакери можуть використовувати вразливості у смарт-контрактах, що трапляється на децентралізованих біржах (DEX). Наприклад, у 2021 році хакери атакували Poly Network, викравши понад 600 мільйонів доларів через помилки в коді. Також можливі атаки на API та маніпуляції з ліквідністю, які дають змогу отримати контроль над біржовими операціями. Захист від зламів включає застосування мультипідписних гаманців, холодного зберігання більшості коштів, посиленого контролю доступу та постійні аудити безпеки. Користувачам варто уникати зберігання великих сум на біржах та користуватися апаратними гаманцями для тривалого зберігання активів.

– Шкідливе програмне забезпечення - віруси, трояни та інші різновиди програм, створених для викрадення криптоактивів користувачів. Такі програми здатні перехоплювати дані, змінювати адреси транзакцій чи отримувати доступ до приватних ключів.

– Втрата доступу - користувач втрачає доступ до активів, якщо не має приватного ключа, seed-фрази, або немає доступу до біржі чи гаманця. Оскільки криптовалюти функціонують на децентралізованих блокчейнах, без можливості відновлення даних через підтримку, втрачені активи часто стають недоступними назавжди.

За для запобігання перерахованим та іншим видам загроз існують різні методи та сервіси захисту, для критеріального аналізу переглянемо які методи існують. Основними критеріями оцінки будуть: рівень безпеки, зручність використання, доступність, стійкість до втрати доступу, анонімність та конфіденційність.

1. Гарячі гаманці – це криптовалютні гаманці, що завжди з’єднані з інтернетом. Вони надають швидкий та простий доступ до цифрових активів, тому популярні серед трейдерів та користувачів, які часто проводять операції. Основною перевагою гарячих гаманців є їх зручність, адже вони дають змогу легко відправляти, отримувати й обмінювати криптовалюту. Але постійне підключення до мережі робить їх уразливими до хакерських атак, фішингу та шкідливих програм.Існує декілька видів гарячих гаманців, зокрема веб-гаманці, мобільні додатки та десктопні програми. Веб-гаманці, як-от MetaMask чи Trust Wallet, працюють через браузери й часто інтегруються з децентралізованими біржами (DEX). Мобільні гаманці, наприклад Coinbase Wallet, дозволяють зручно управляти криптовалютою через смартфон. Десктопні гаманці, як-от Exodus, встановлюються на комп’ютер та пропонують розширений функціонал для зберігання активів.Не дивлячись на ризики, безпеку гарячих гаманців можна покращити, використовуючи двофакторну аутентифікацію (2FA), складні паролі та резервні копії. Однак для довгострокового зберігання великих сум радимо використовувати холодні гаманці, які не підключені до інтернету.

2. Холодні гаманці – це кріптовалютні гаманці, які не під’єднані до інтернету, що робить їх найбезпечнішим методом збереження цифрових активів. Вони захищають гроші від хакерських атак, фішингу та шкідливого ПЗ, тому що приватні ключі не взаємодіють з мережею. Холодні гаманці здебільшого застосовують для довгострокового зберігання великих сум криптовалюти, тому що вони не такі зручні для щоденних операцій, як гарячі гаманці. Головні види холодних гаманців містять апаратні та паперові гаманці. Апаратні гаманці, такі як Ledger Nano S, Ledger Nano X чи Trezor, являють собою фізичні пристрої, які зберігають приватні ключі в офлайн-режимі. Вони мають захист від зламів і, як правило, потребують з’єднання з комп’ютером чи смартфоном тільки під час здійснення операцій. Паперові гаманці містять приватний і публічний ключі, надруковані на папері або іншому фізичному носії, що робить їх цілком недосяжними для кіберзлочинців, але вразливими до фізичного пошкодження чи втрати. Незважаючи на високий рівень безпеки, холодні гаманці мають певні

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ризики. Якщо власник загубить пристрій або паперовий ключ без резервної копії, доступ до грошей буде неможливим. Через те радять зберігати резервні копії у надійному місці та застосовувати мнемонічні фрази для відновлення доступу.

3. Мультипідписні гаманці – це криптовалютні гаманці, що потребують декілька підписів для підтвердження транзакцій. Вони застосовуються для збільшення безпеки та контролю над цифровими активами, особливо у корпоративних або спільних інвестиційних фондах. Замість одного приватного ключа, як у звичайних гаманцях, multisig-гаманці вимагають від двох чи більше користувачів підтвердження кожної операції. Зазвичай такі гаманці налаштовуються за принципом «M з N», де N – загальна кількість власників ключів, а M – мінімальна кількість підписів, потрібна для схвалення транзакції. Наприклад, у конфігурації 2 з 3 транзакція буде здійснена тільки тоді, коли щонайменше двоє учасників підпишуть її. Це забезпечує додатковий рівень безпеки, оскільки навіть якщо один ключ буде скомпрометовано, зловмисник не зможе викрасти кошти. Мультипідписні гаманці часто використовуються компаніями, фондами та криптобіржами для управління активами. Вони також підходять для спільного володіння коштами між довіреними особами, приміром, у сімейних офісах або партнерствах. Одним з популярних рішень для multisig-гаманців є Gnosis Safe, який дозволяє налаштовувати різні рівні доступу для учасників. Інші відомі платформи – Electrum, BitGo та Armory. Приклад: компанія, яка інвестує у криптовалюту, налаштовує multisig-гаманець за схемою 3 з 5, де п’ять керівників мають ключі, але для підтвердження виплат необхідні підписи щонайменше трьох із них. Це гарантує, що один або два керівники не зможуть здійснити операцію без згоди більшості, що значно знижує ризик шахрайства чи людської помилки.

4. Апаратні гаманці – це специфічні пристрої для офлайн-збереження криптовалют, котрі забезпечують суттєву безпеку. Вони зберігають особисті ключі на окремому фізичному носії, ізольованому від інтернету, що значно зменшує ймовірність хакерських атак, вірусів і фішингових атак. На відміну від гарячих гаманців, котрі постійно підключені до мережі, апаратні гаманці функціонують тільки тоді, коли їх під’єднують до комп’ютера чи смартфону для підписання транзакцій. При цьому особисті ключі ніколи не залишають пристрій, а всі операції підписуються всередині гаманця, що унеможливлює злам. Ці гаманці підтримують багато різних криптовалют та блокчейнів, а також можуть інтегруватися з програмними гаманцями, як-от MetaMask чи Electrum, задля зручності використання. Вони підходять для довгострокового зберігання криптовалюти, бо не піддаються ризикам, котрі пов’язані з онлайн-зберіганням. Апаратні гаманці часто мають екран та кнопки для підтвердження операцій, що запобігає атакам на кшталт «віддалене керування». Деякі моделі навіть підтримують захист за допомогою PIN-коду і фрази для відновлення (seed-фрази), що дозволяє відновити кошти, якщо пристрій буде втрачено. Приклад: Ledger Nano X – це популярний апаратний гаманець, який підтримує понад 1 500 криптовалют, має Bluetooth-з’єднання для мобільних пристроїв та забезпечує надійний захист особистих ключів.

5. Смарт-контракти з безпековим зберіганням – це інноваційний підхід до зберігання цифрових активів, що використовує технологію смарт-контрактів для забезпечення децентралізованого і захищеного зберігання. Це дає змогу позбутися потреби в централізованих кастодіальних сервісах, таких як традиційні фінансові установи чи біржі, та гарантує більшу прозорість, контроль та безпеку завдяки автоматизації процесів на основі програмного коду. Смарт-контракти автоматично виконують умови, визначені у коді, забезпечуючи збереження та передачу активів тільки при виконанні встановлених вимог. Основоположним аспектом смарт-контрактів із безпечним зберіганням є використання мультипідписних чи умовних механізмів для доступу до активів. Зокрема, смарт-контракт можна налаштувати так, щоб для розблокування активів було потрібно декілька підписів або підтверджень від різних учасників, що надає додаткову безпеку у разі можливих атак чи несанкціонованих операцій. Це дає змогу користувачам зберігати свої активи з високим рівнем захисту, уникаючи централізованих

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ризиків, як-от можливість зловживань чи зламу на стороні третіх осіб. Смарт-контракти також можуть застосовуватися для реалізації умовного зберігання, де активи заморожуються до виконання певних умов. Це може містити виконання певних дій або досягнення певних параметрів, таких як визначена ціна або події, погоджені учасниками. Важливою характеристикою таких контрактів є їх програмована автономність – вони автоматично виконують умови, зменшуючи потребу у людському втручанні та знижуючи ризики помилок. Приклад:Gnosis Safe є одним із найпоширеніших смарт-контрактів для безпекового зберігання криптовалют. Цей смарт-контракт на платформі Ethereum, що дозволяє створювати безпечні гаманці з численними учасниками, де для проведення транзакції необхідно отримати певну кількість підписів від авторизованих осіб. Завдяки такій конфігурації, активи можуть бути захищені від несанкціонованого доступу, гарантуючи додатковий рівень захисту та контролю.

Аналізуючи вже маючі данні методів захисту криптовалюти порівняємо їх за критеріями (табл. 1).

Таблиця 1

Аналіз методів захисту криптовалюти

Методи захисту	Рівень безпеки	Зручність у використанні	Доступність	Стійкість до втрати доступу	Анонімність та конфіден-ційність	Рекомендація до розподілу коштів
Гарячі гаманці	Низький	Висока	Безкоштовні / не велика комісія	Залежить від резервних копій	Залежить від платформи	1–5% від загального обсягу активів
Холодні гаманці	Високий	Середня	Залежить від вартості пристроя	Висока але залежить від резервних копій	Висока	70-85% від загального обсягу активів
Мультипідписні гаманці	Високий	Середня	Частково безкоштовні (комісія)	Висока через множинні ключі	Висока	10-20% від загального обсягу активів коштів, якщо потрібно керування з кількома учасниками (наприклад, для бізнесу чи сімейного
Апаратні Гаманці	Дуже високий	Помірна	Залежить від вартості моделі	Висока (залежить від резервних копій)	Висока	70–80% від загального обсягу активів
Смарт – контракти з безпечними зберіганнями	Високий	Висока	Дорогі	Висока, але залежить від налаштувань відновлень	Висока	до 5–10% якщо необхідно автоматизоване керування активами (наприклад, стейкінг або DeFi).

Джерело: розроблено автором

Висновки. Оцінка основних загроз, зокрема фішингових атак, зломів криптобірж, дій шкідливого програмного забезпечення та втрати доступу до гаманців, засвідчила необхідність впровадження надійних механізмів захисту. Проведений критеріальний аналіз різних методів зберігання криптоактивів показав, що кожен підхід має свої сильні та слабкі сторони. Гарячі гаманці забезпечують оперативний доступ до активів, але є вразливими до атак через постійне з’єднання з інтернетом. Холодні гаманці забезпечують високий рівень безпеки, хоча менш

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

придатні для частого використання. Мультипідписні гаманці дозволяють підвищити рівень контролю над транзакціями за рахунок колективного схвалення, що є доцільним у корпоративному середовищі. Апаратні гаманці поєднують фізичну ізоляцію з технологічною зручністю, хоча вимагають ретельного зберігання. Смарт-контракти з функціями безпечного зберігання надають можливості для програмованого управління активами, зменшуючи залежність від людського чинника та централізованих платформ.

Загалом, ефективний захист криптоактивів можливий лише за умови зваженого вибору методів зберігання, орієнтованого на конкретні потреби користувача, рівень ризиків та пріоритети щодо безпеки, зручності й контролю.

Список використаних джерел

1. Antonopoulos, A. M.Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media. – 2017. – С. 30 – 65.
2. Ledger. How to Secure Your Crypto Assets with Hardware Wallets – 2023. – С. 1-10.
3. Binance Academy. What Are Hot and Cold Wallets? – 2023.

Роботу виконано під науковим керівництвом канд. техн. наук, доцента
ХОХЛАЧОВОЇ Ю. Є.

РЕСУРСОЕФЕКТИВНИЙ МЕТОД ДЕТЕКЦІЇ ШКІДЛИВОГО КОДУ НА СЕРВЕРАХ ХОСТИНГ-ПРОВАЙДЕРІВ

КОСТИРЕВА Б. Ю., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті запропоновано ресурсоефективний метод виявлення шкідливого програмного забезпечення в середовищі хостинг-провайдера, що працює на операційній системі Linux. Метод базується на виявленні файлів із підозрілою модифікацією часу редагування, зокрема з нульовими наносекундами, що може свідчити про спробу шкідливого програмного забезпечення приховати сліди інфікування. Після ідентифікації таких файлів проводиться сигнатурний аналіз для підтвердження наявності шкідливого коду. Запропонований підхід дозволяє значно звузити обсяг файлів для перевірки, підвищуючи ефективність процесу виявлення шкідливого програмного забезпечення та зменшуючи навантаження на ресурси сервера

The article proposes a resource-efficient method for detecting malware in a hosting provider environment operating on the Linux operating system. The method is based on identifying files with suspicious modification timestamps, particularly those with zero nanoseconds, which may indicate an attempt by malware to conceal traces of infection. After identifying such files, a signature analysis is conducted to confirm the presence of malicious code. The proposed approach significantly narrows the scope of files requiring inspection, enhancing the efficiency of malware detection and reducing the load on server resources.

Актуальність: Зі стрімким зростанням кількості інтернет-користувачів та веб-сайтів збільшується і кількість кіберзагроз. У 2021 році витрати на кібербезпеку сягнули приблизно 6 трильйонів доларів США, що вдвічі більше порівняно з 2015 роком, а до 2025 року

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

прогнозується їх зростання до 10,3 трильйона доларів на рік [1]. Хостинг-провайдери, розміщуючи веб-ресурси, повинні забезпечувати баланс між якістю послуг та їх вартістю, не нехтуючи безпекою та цілісністю розміщених веб-сайтів. Важливо вчасно виявляти та реагувати на інциденти, оскільки вразливості в плагінах можуть ставити під загрозу сотні тисяч сайтів [2, с. 1].

Аналіз досліджень: Дослідженню методів виявлення вірусів та ШПЗ присвячені праці вітчизняних та закордонних науковців: Peter Szor, Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Michael Sikorski, Andrew Honig, Nataraj L., Yegneswaran V., Porras P., Zhang J., та інших.

Метою статті є розробка та оцінка ресурсоефективного методу виявлення шкідливого програмного забезпечення (ШПЗ) в середовищі хостинг-провайдера, заснованого на ідентифікації файлів із підміненими датами модифікації та подальшому сигнатурному аналізі.

Об'єкт дослідження: процес виявлення та аналізу шкідливого програмного забезпечення в системах хостинг-провайдерів.

Предмет дослідження: методи та підходи до детектування ШПЗ, зокрема аналіз змін у метаданих файлів, таких як дата модифікації, та їх використання для підвищення ефективності виявлення шкідливого коду в умовах обмежених ресурсів хостинг-провайдера.

Виклад основного матеріалу. Даний метод полягає в виявленні потенційно інфікованих файлів, або файлів з ШПЗ в котрих відбулась підміна дати модифікації вмісту файлу. Дія методу досліджувалась та перевірялась в Linux системах.

Розглянемо ситуацію: якщо для прикладу певний ресурс був інфікований, і в файлах з'явилось шкідливе програмне забезпечення (далі – ШПЗ), то фахівець з безпеки дізнавшись приблизну дату інфікування може знайти список файлів котрі були модифіковані в той проміжок часу. Цей метод користується популярністю та рекомендований на багатьох інтернет-ресурсах, зокрема він запропонований на сайті американської компанії з кібербезпеки SentinelOne. В ньому йдеться, про використання команди find для пошуку файлів котрі були змінені в певний проміжок часу, розглянутий приклад пошуку за останні 30 хвилин [3]. Проте даний метод не працює, якщо ШПЗ змінює час та дату інфікованого файлу. Для підміни часу модифікації можна використати команду touch -m -t 202202240340.58 file.txt де можна вказати необхідний час в форматі [[CC]YY]MMDDhhmm[.ss]. На рис. 1 проведений приклад, де ми перевіряємо час та дату модифікації файлу командою stat та шукаємо файли змінені за останніх 30 хвилин, і система знаходить файл (в вищезгаданій статті приклад розглядався саме для операційної системи macOS, і хоча macOS та Linux засновані на ОС Unix [4] все ж для чистоти даного експерименту був обраний MacBook.) Після цього підмінюємо дату на 2022 рік і повторний запуск пошуку змінених файлів за останніх 30 хвилин вже не знаходить цей файл.

```
admin@MacBook-Pro-Admin test %
admin@MacBook-Pro-Admin test % stat 1.txt

16777221 13026031 -rw-r--r-- 1 admin staff 0 5 "Mar 26 22:49:46 2025" "Mar 26 22:49:44 2025" "Mar 26 22:49:44 2025" "Mar 26 22:49:44 2025" 4096 8 0 1.txt
admin@MacBook-Pro-Admin test % stat 1.txt

16777221 13026031 -rw-r--r-- 1 admin staff 0 5 "Mar 26 22:49:46 2025" "Mar 26 22:49:44 2025" "Mar 26 22:49:44 2025" "Mar 26 22:49:44 2025" 4096 8 0 1.txt
admin@MacBook-Pro-Admin test % find . -mtime +0m -a -mtime -30m -print

.
./1.txt
admin@MacBook-Pro-Admin test % touch -m -t 202202240340.58 1.txt

admin@MacBook-Pro-Admin test % find . -mtime +0m -a -mtime -30m -print

.
admin@MacBook-Pro-Admin test %
```

Рис. 1. В Linux та в MacOS можна приховати час модифікації файлу

Джерело: розроблено автором в середовищі OS MacOS (знімок з екрану)

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Шкідливе програмне забезпечення при редагуванні файлів змінюють час та дату модифікації файлу, ймовірно з метою приховування часу інфікування. Проте ці файли можливо відслідкувати, оскільки підміна дати модифікації в Linux системах відбувається в форматі рік, місяць, дата, години, хвилини та секунди [5] де немає змоги вказати наносекунди, тому вони автоматично заповнюються нулями. Використавши команду stat ми можемо побачити що час модифікації відображається з наносекундами (дев'ять цифр після секунд) в форматі 17:18:56.000000000 (рис. 2). Зверніть увагу, що в цьому випадку ми перевіряємо інфікований файл, і тому наносекунди заповнені нулями.

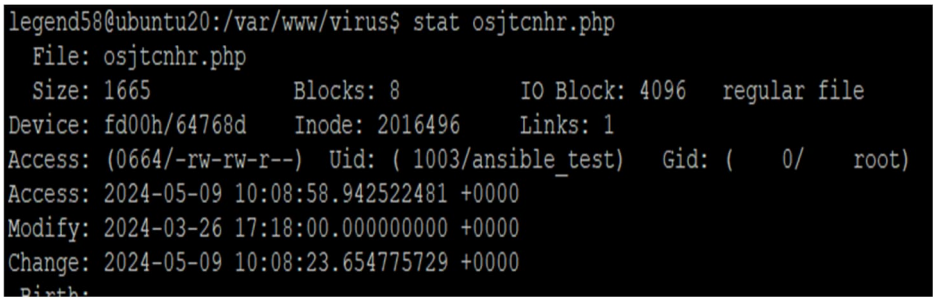


Рис. 2. Перевірка часу модифікації інфікованого файлу

Джерело: розроблено автором в середовищі OS Linux (знімок з екрану)

Знайти файли в котрих підмінена дата модифікації в linux системах можна наприклад командою find /path/to/files -type f -exec stat {} + | grep --binary-files=without-match '.000000000'

При звичайному ж редагуванні, копіюванні чи переміщенні файлу наносекунди матимуть не таке кругле число, і відображатимуться, наприклад 17:59:58.669464785 (Рис. 3) тобто шанс отримати 000000000 файлу складає один до мільярда. Якщо ж файл котрий містить 000000000 наносекунд скопіювати, то його копія матиме нормальне значення наносекунд, таке як на Рис. 3.

Також мої експерименти показали що це явище також з'являється при видобуванні файлів з архіву, де всі видобуті файли отримують час модифікації 000000000 наносекунд. Інші можливі причини появи цього ефекту потребують додаткових досліджень.

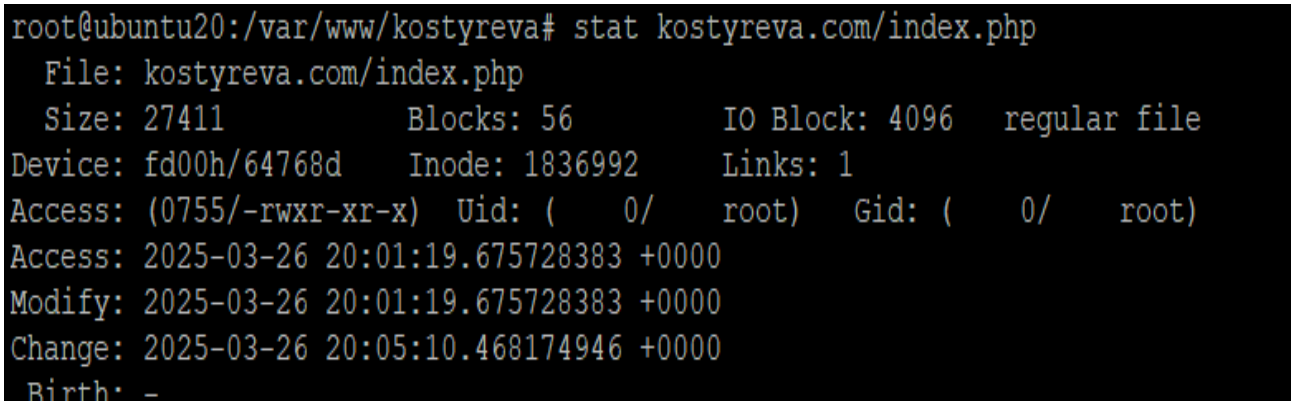


Рис. 3. Перевірка часу модифікації звичайного файлу після копіювання чи переміщення

Джерело: розроблено автором в середовищі OS Linux (знімок з екрану)

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Важливо розуміти, що не кожен файл в котрому є підмінена дата модифікації файлу є інфікованим, а не всі файли котрі містять звичайну дату модифікації є безпечними. Це дозволяє зменшити коло пошуку інфікованих файлів.

Розглянемо ситуацію, де на Linux сервері знаходиться велика кількість веб-ресурсів, і відповідно велика кількість файлів для кожного з сайтів. Хорошим прикладом може бути сервер віртуального хостингу, де може міститись тисячі сайтів а кожен сайт може містити десятки тисяч файлів. Використавши цей метод для відстеження потенційно інфікованих файлів ми можемо значно звузити коло пошуку до декількох тисяч файлів, а то й одиниць. Під час моїх досліджень трапився випадок коли на сервері з тисячами сайтів запропонованим методом було знайдено два файли, і ці файли були інфіковані. Проте не завжди трапляються такі ідеальні випадки. Інколи знаходиться декілька тисяч файлів котрі належать декільком веб-ресурсам, адже як я зазначав раніше при видобуванні файлів з архіву наносекунди цих файлів будуть заповнені нулями. Ці декілька сайтів були відновлені з резервної копії, й тому вони були знайдені даним методом. Випадки, коли файл має підмінену дату модифікування, проте можливо не являється інфікованим у даній статті я називатиму хибними спрацюваннями.

Важливо розуміти, що видалення ШПЗ у програмному коді вимагає уважного аналізу контексту та залучення досвідчених експертів з безпеки програмного забезпечення.

Щоб знайти ШПЗ в отриманому списку файлів ми можемо використати метод пошуку сигнатур. Для цього я знайшов декілька десятків вірусних файлів з найдених списків з підміненою датою редагування, та за способом підрахунку унікальних фраз створив свій список, котрий начисляв більше 20 сигнатур веб-шелів, ін’єкцій, та інших. Ось приклад деяких з них котрі найчастіше траплялись:

BiaoJiOk
eval(base64_decode
x65\x78\x70\x6c\x6f\x64\x65
0e3fbd5d9cca9d838d21ded8de713482
0byt3m1n1
x3x3x3x_5h3ll

Цей підхід до створення баз сигнатур можливо не є вірним, проте це дозволило мені створити невелику базу актуальних сигнатур для продовження моїх досліджень.

Методологія оцінки ефективності

Критеріями ефективності даного методу розглянемо швидкість відпрацювання, приблизна кількість витрачених ресурсів серверної потужності та якість визначення котра включає ефективність знаходження.

Для дослідження ефективності використовуватимемо чотири способи:

1. Find + stat

Пошук файлів з зміненим часом модифікування (команда find /path/to/files -type f -exec stat {} + | grep --binary-files=without-match ‘.000000000’ > result.list)

2. Find + stat + signature

Пошук файлів з зміненим часом модифікування, і з отриманого списку пошук сигнатур (використано власний список сигнатур)

3. Find + signature

Пошук серед усіх файлів на співпадіння сигнатур (використано власний список сигнатур).

4. Clamscan

Використання сканера Clamscan [6] від популярного пакунку антивірусних програм ClamAV [7] версії 0.103.12, та версії бази 27589 (останнє оновлення баз на день проведення дослідження 26.03.2025).

Під час попередніх тестів для визначення ефективності знаходження, спосіб № 4 тестування Clamdscan показало тривалий час сканування, і після 10 годин тест довелось

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

зупинити. А для сканування способу № 1 та № 2 де використовується команда stat створити лабораторні умови не вдалось, оскільки при копіюванні файлів в лабораторне середовище час модифікації для всіх файлів змінюється. Тому ми проведемо два тести.

Тестування 1. Ефективність та швидкість знаходження ШПЗ.

Для тестування використовувалась VPS (Virtual Private server) з наступними технічними характеристиками:

CPU (процесор) 6 core

RAM (Оперативна пам'ять)16Gb

Disk Nvme-ssd

Для перевірки було обрано 9 сайтів клієнтів хостинг-провайдера. Один з сайтів побудований на cms Bitrix та проявляв підозрілу активність. На 3 інших сайті на cms Wordpress надійшло прохання від клієнтів перевірити на шкідливе програмне забезпечення.

Загальний об'єм даних 15G, з яких 9,8G сайт на cms Bitrix. Загальна кількість файлів 395710 з яких 294560 належать сайту на cms Bitrix.

Перелік об'єму кожного з сайтів:

2.4G site1_Wordpress-Client_request

273M site2_Wordpress-Client_request

205M site3_Wordpress-Client_request

1.2G site4_Joomla

9.8G site5_bitrix

252M site6_osCommerce

201M site7_Wordpress

565M site8_Wordpress

244M site9_Joomla

* Знайдена кількість файлів в способі №1 Find + stat не гарантує що файл інфікований ШПЗ. Вона свідчить про кількість файлів, дата якого була модифікована.

**Для способу №1 в цьому тестуванні використано команду Find + stat, проте оскільки файли сайтів були копійовані з сервера хостинг-провайдера, і дата модифікації файлів була змінена, то команда після виконання повернула порожній результат. У Таблиці 1 вказано час виконання команди з поверненням порожнього результату.

Таблиця 1

Тестування ефективності знаходження шкідливого програмного забезпечення

	Знайдено інфікованих сайтів	Знайдено інфікованих файлів	Інші CMS кількість файлів з ШПЗ	Bitrix файлів з ШПЗ	Час виконання
Find + stat	4*	110991*	1712*	109279*	12.731 **
Find + stat + signature	3	59	8	51	19.023 s***
Find + signature	3	59	8	51	1 m 48 s
Clamscan	3	12	3	9	44 m 52 s

Джерело: розроблено автором

***Для способу № 2 список файлів зі зміною датою модифікування було попередньо імпортовано з робочого середовища хостинг-провайдера. Час виконання даного способу це сума часу виконання способу №1 та час використаний на пошук сигнатур (4,292 s).

Результати тестування показали (Таблиця 1), що метод Find + signature значно швидший за сканування Clamscan, а Find + stat + signature швидший за Find + signature.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Метод Find + stat сам по собі малоефективний, оскільки він знаходить велику кількість хибних спрацювань в CMS bitrix, та близько 1700 файлів одного з сайтів на cms WordPress на якому ШПЗ не виявлено. Ці 1700 файлів належали декільком плагінам, що висуває припущення, що ці плагіни були нещодавно встановлені.

В CMS Bitrix було методом Find було виявлено 51 файл, де файл siteheads.php дублювався з однаковим змістом в різних директоріях 42 рази, та знайдений за співпадінням сигнатури «BiaoJiOk». Перевірка clamscan цей файл не віднесла до потенційно загрозливих. Попередньо код файлу виглядає потенційно-небезпечним (рис. 5). Для однозначної відповіді потрібен більш детальний аналіз фахівців по кібербезпеці.

Рис. 5. Потенційно-небезпечний файл siteheads.php знайдений в cms системі Bitrix

Джерело: розроблено автором в середовищі OS Linux (знімок з екрану)

Окрім siteheads.php в cms системі Bitrix було знайдено по 9 файлів методом Clamscan та Find + stat + signature. Проте жоден знайдений файл не збігається між двома методами перевірки, тобто це 18 інфікованих файлів (Рис 6). Зміст кожного з знайдених файлів методом Find + signature це однолінійковий обфускований код.

Рис. 6. Потенційно-небезпечні файли знайдені в системі Bitrix методами Clamscan та Find + stat + signature

Джерело: розроблено автором в середовищі OS Linux (знімок з екрану)

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

З результатів перевірки інших сайтів окрім Bitrix, виявились інфікованими 2 сайти на cms Wordpress. Код знайдених файлів обфусцьований, а файли є ін'єкційними або web-shell [8] з відкритим доступом через браузер. З цього можна зробити висновок, що хибних спрацювань в методі Find + stat + signature немає.

Рис. 7. Знайдені методами Clamscan та Find + stat + signature web-shell та ін'єкційні файли на cms Wordpress

Джерело: розроблено автором в середовищі OS Linux (знімок з екрану)

Тестування 2. Навантаження на систему

Для даного тестування використовувався сервер хостинг-провайдера для віртуального-хостингу, з працюючими понад 1200 сайтами клієнтів, це 45млн файлів. Для більш об'єктивних результатів тестування виконувалось в нічний час доби, коли навантаження на сервер мінімальне. Технічні характеристики сервера:

24 CPU core

192Gb RAM

Nvme-ssd.

Для пошуку файлів методом Find + stat використовувалась команда з зміненим часом модифікування та фільтрація за змінами файлів не старіше за 30 днів (команда find /path/to/files -type f -ctime -30 -exec stat {} + | grep --binary-files=without-match '.000000000' > result.list)

Використовувався метод Find + stat + signature, час сканування та перевірки тривав близько 15 хв. Навантаження на систему можна побачити на Рис. 8. Навантаження на CPU зросло орієнтовно на 10%, проте відчутно зросло використання диску, а саме параметр Disk read operation per second зріс майже в 10 раз і досяг позначки 1,1Kiops. Це відносно не багато, враховуючи що сучасні SATA SSD можуть досягати позначки 97Kiops випадкового читання, а сучасні NVMe можуть досягати 1500Kiops при випадковому читанні [9].

Рекомендації по використанню

Запропонований метод розглянутий в умовах хостинг-провайдера, де знаходиться велика кількість сайтів ізольованих одне від одного. Цей метод буде також актуальним для інших умов відмінних від хостинг-провайдера, проте більш видимий результат відображається саме з зростанням масштабів. Для одного VPS сервера, де знаходиться невеликий сайт час перевірки Clamscan буде більший від запропонованого методу в 3–5 хвилин що не є значним показником, а при масштабному скануванні великої кількості серверів як в Тестування 2, результат може зекономити декілька днів чи тижнів.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

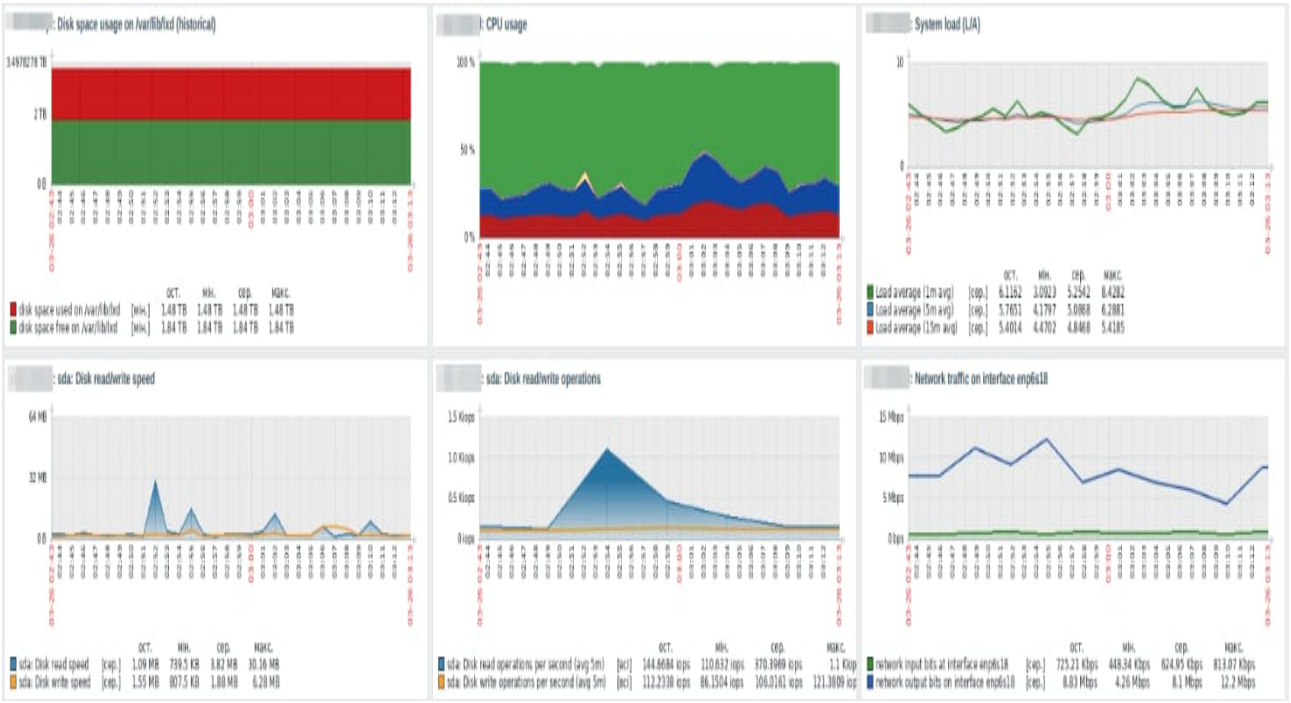


Рис. 8. Навантаження на систему при скануванні понад 1200 сайтів

Джерело: розроблено автором в середовищі Grafana (знімок з екрану)

При виявленні ШПЗ на одному з сайтів рекомендовано провести аналіз використовуючи різні методи, оскільки Тестування 1 показало, що знайдене ШПЗ одним методом може частково або повністю відрізнятись від ШПЗ знайденого іншим методом на цьому ж сайті.

Рекомендується знайти або створити більшу базу сигнатур для пошуку ШПЗ, оскільки використана база під час Тестуванні 1 не знайшла тих сигнатур, які були виявлені Clamscan.

При використанні методу на регулярні основі, для уникнення повторного сканування вже раніше просканованих файлів, можна для просканованих файлів робити підміну дати модифікування, наприклад touch -m -t 202202240340.00 file.php а при повторному пошуку для уникнення просканованих файлів використовувати grep -v 202202240340.00

Висновки. В даній статті був запропонований ресурсоефективний метод виявлення ШПЗ на операційні системі Linux.

Було зазначено неефективність пошуку ШПЗ методом пошуку файлів, котрі були змінені за певний період, оскільки ШПЗ може підміняти дату модифікації файлу. Для ресурсоефективності запропонований метод значно звужує список файлів необхідних для перевірки на наявність ШПЗ. Були проведене дослідження по швидкості та якості знайдених ШПЗ в порівнянні з Clamscan, а також проведене дослідження для визначення навантаження на ключові ресурси сервера. Запропоновані рекомендації по удосконаленню методу.

Список використаних джерел

1. Steve M. Report: Cyberwarfare in the C-Suite. Cybersecurity Ventures. 2021. JAN. 21, 2021. P. 1. URL: https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf (date of access: 27.03.2025).

2. Critical zero-day vulnerability fixed in WordPress File Manager (700,000+ installations). NinTechNet’s updates and security announcements. URL: https://blog.nintechnet.com/critical-zero-day-vulnerability-fixed-in-wordpress-file-manager-700000-installations/ (date of access: 27.03.2025).

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

3. Stokes P. Malware Hunting on macOS | A Practical Guide. SentinelOne. URL: https://www.sentinelone.com/blog/malware-hunting-macos-practical-guide/ (date of access: 27.03.2025).
4. Stokes P. Malware Hunting on macOS | A Practical Guide. *SentinelOne*. URL: https://www.sentinelone.com/blog/malware-hunting-macos-practical-guide/ (date of access: 27.03.2025).
5. IBM i 7.4. *IBM – United States*. URL: https://www.ibm.com/docs/en/i/7.4?topic=directories-touch (date of access: 27.03.2025).
6. ClamAV Documentation. clamav.net. URL: https://docs.clamav.net/manual/Usage/Scanning.html#clamscan (date of access: 27.03.2025).
7. Linux malware detection tools. *Linux Security Expert*. URL: https://linuxsecurity.expert/security-tools/linux-malware-detection-tools (date of access: 27.03.2025).
8. Server Software Component: Web Shell, Sub-technique T1505.003 – Enterprise | MITRE ATT&CK®. *MITRE ATT&CK®*. URL: https://attack.mitre.org/techniques/T1505/003/ (date of access: 27.03.2025).
9. Wise A. HDD vs SATA SSD vs NVMe SSD Concepts - Advanced. Atlantic.Net. URL: https://www.atlantic.net/vps-hosting/hdd-vs-sata-ssd-vs-nvme-ssd-concepts (date of access: 27.03.2025).

Роботу виконано під науковим керівництвом канд. техн. наук, ст. наук. співроб., доцента ЗВЄРЄВА В. П.

ПОРІВНЯЛЬНИЙ АНАЛІЗ WAF У ЗАХИСТІ ВЕБДОДАТКІВ

КОТ Т. Р., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто питання ефективності застосування Web Application Firewall (WAF) як одного з ключових засобів захисту вебдодатків від найбільш поширених атак, описаних у переліку OWASP Top 10. Проведено теоретичний огляд принципів роботи WAF, їх класифікації та особливостей впровадження у сучасних інфраструктурах. У рамках експериментальної частини дослідження проведено тестування веб-додатка з активованими WAF, що дозволило оцінити ефективність виявлення атак на практиці. Отримані результати стали основою для формулювання рекомендацій щодо вибору та налаштування WAF у залежності від специфіки вебдодатків.

The article examines the effectiveness of using a Web Application Firewall (WAF) as one of the key tools for protecting web applications from the most common attacks listed in the OWASP Top 10. A theoretical overview of WAF operating principles, their classification, and implementation features in modern infrastructures is provided. In the experimental part of the research, a web application was tested with active WAFs to evaluate their practical effectiveness in detecting attacks. The obtained results served as a basis for formulating recommendations regarding the selection and configuration of WAFs depending on the specifics of web applications.

Актуальність. Вебдодатки відіграють ключову роль у функціонуванні інформаційних систем підприємств, установ і сервісів, які щоденно взаємодіють з персональними даними користувачів. Вебдодатки дедалі частіше стають основною ціллю зловмисників, оскільки взаємодіють із зовнішніми користувачами та мають численні точки входу, зокрема форми

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

введення, Application Programming Interface (API), модулі автентифікації та інтеграції зі сторонніми сервісами. З такими векторами, вебдодатки стають дуже вразливими до широкого спектра атак.

Одним із найпоширеніших підходів до захисту вебдодатків є застосування WAF – систем, що аналізують HTTP/HTTPS трафік і фільтрують потенційно шкідливі запити. Іван Рістіч у своїй роботі «ModSecurity Handbook» [1] детально описує архітектуру та механізми налаштування одного з найвідоміших WAF – ModSecurity, який широко використовується в різних типах серверів.

За даними Open Worldwide Application Security Project (OWASP), до найпоширеніших векторів атак належать SQL-ін'єкції, міжсайтове виконання скриптів (XSS), підміна запитів (CSRF), атаки на автентифікацію та інші вразливості, що входять до переліку OWASP Top 10 [2]. OWASP регулярно оновлює цей перелік, враховуючи сучасні загрози, що дозволяє тримати фокус спільноти на найбільш небезпечних і поширених вразливостях. Зокрема, ґрунтовний опис технік атак і можливостей їх експлуатації подано у працях D. Stuttard і M. Pinto, які розглядають сценарії практичного зламу веб-додатків [3].

Нестача стандартизованих підходів до тестування та відсутність чітких критеріїв вибору ефективного WAF-рішення створюють додаткові труднощі для спеціалістів з кібербезпеки при ухвалені рішень. Більшість організацій змушені покладатися на власні експерименти або обмежену документацію постачальників при оцінці ефективності WAF. У багатьох випадках рішення про вибір WAF приймається на основі суб'єктивного досвіду або комерційних оглядів, що не завжди відображають реальні показники ефективності. Саме тому дослідження, спрямоване на експериментальну оцінку та порівняльний аналіз популярних WAF-рішень, є актуальним як з наукової, так і з практичної точки зору. Попри широку представленість комерційних і відкритих рішень, таких як Cloudflare WAF, AWS WAF, F5 Advanced WAF, у відкритій літературі спостерігається недостатня кількість порівняльних досліджень, у яких оцінювалася б реальна ефективність цих систем у контексті типових атак. Наявні статті здебільшого або описують окремі аспекти роботи WAF, або подають результати, не придатні для узагальнення. У зв'язку з цим постає необхідність у проведенні незалежного аналізу, заснованого на стандартизованій методиці тестування з урахуванням таких важливих показників, як точність виявлення атак, зручність налаштування, продуктивність і стійкість до обходу захисту.

Метою дослідження є всебічне порівняння ефективності популярних систем Web Application Firewall (WAF) як інструментів захисту веб-додатків від найпоширеніших атак, викладених у переліку Open Web Application Security Project (OWASP) Top 10. У ході роботи передбачається оцінити не лише здатність WAF виявляти та блокувати типові вектори атак (зокрема SQL-ін'єкції, XSS, CSRF тощо), але й дослідити зручність розгортання та налаштування кожної системи, якість генерованих логів безпеки, можливості інтеграції з іншими інструментами кіберзахисту, а також вплив впровадження WAF на продуктивність вебдодатку.

Об'єктом дослідження є Вебдодатки розглядаються як критично важливий компонент сучасних інформаційних систем, що постійно перебувають під ризиком експлуатації типових вразливостей. Особлива увага приділяється аспектам їх уразливості на рівні взаємодії з користувачами та зовнішніми сервісами, що зумовлює необхідність впровадження ефективних засобів захисту, зокрема Web Application Firewall.

Предмет дослідження – функціональні характеристики та ефективність роботи систем Web Application Firewall (WAF) при фільтрації шкідливого трафіку, виявленні й блокуванні типових атак на веб-додатки.

Аналіз попередніх досліджень. У науковій літературі запропоновано низку підходів до захисту вебдодатків від атак, зокрема з використанням систем WAF (Web Application Firewall). У роботі An Efficient Machine Learning-Based Web Application Firewall with Deep Automated

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Pattern Categorization авторства Ghosh et al. (2023)[4] розроблено ефективну WAF-систему на основі алгоритмів машинного навчання з глибокою автоматизованою категоризацією шаблонів атак. Запропонований підхід дозволяє знизити кількість хибнопозитивних спрацювань та виявляти широкий спектр загроз, включаючи нові, раніше невідомі типи атак.

Аналогічний підхід представлено у дослідженні Web Application Firewall Using Machine Learning and Features Engineering, яке провели Rajendran et al. (2022)[5]. У ньому акцент зроблено на інженерії ознак для покращення здатності WAF до виявлення складних типів атак. У порівнянні з традиційними сигнатурними WAF-системами, ці рішення демонструють значно вищу адаптивність, однак вимагають належної підготовки навчальних наборів і високих обчислювальних потужностей.

Таким чином, аналіз попередніх досліджень показує тенденцію до інтеграції інтелектуальних алгоритмів у системи захисту вебдодатків. Водночас залишається відкритим питання ефективності таких підходів у реальному середовищі з високим навантаженням, що й обумовлює необхідність проведення додаткового експериментального аналізу, представленого в цій роботі.

Виклад основного матеріалу.

В матеріалі було наведено практичний аналіз ефективності засобів захисту вебдодатків та проведено дослідження із залученням популярних рішень класу WAF. У цьому розділі наведено опис обраних інструментів, обґрунтування їх вибору, а також результати експериментального застосування в умовах моделювання типових атак. Особливу увагу зосереджено на функціональних можливостях, налаштуванні та продуктивності систем, що досліджуються.

ModSecurity було включено до дослідження як найпоширеніше open-source WAF-рішення, що надає широкі можливості для ручного налаштування та глибокого контролю над процесом фільтрації запитів. Завдяки підтримці правил OWASP Core Rule Set та можливості створювати власні фільтри, ця система є гнучким інструментом для детального аналізу атак. ModSecurity доцільно використовувати в середовищах, де критично важлива адаптація захисту під специфіку веб-додатку, а також де потрібне детальне логування та інтеграція з існуючою серверною інфраструктурою.

Вибір саме цих двох систем зумовлений бажанням охопити різні підходи до впровадження WAF: технічно гнучкий, але складніший у налаштуванні ModSecurity, та простий у використанні, але менш налаштований Cloudflare. Це дозволяє дослідити не лише ефективність блокування атак, а й практичні аспекти впровадження: витрати часу, рівень автоматизації, можливість масштабування та глибину логування. Такий підхід забезпечує об’єктивне порівняння рішень у різних контекстах використання – від навчальних лабораторій до комерційного середовища.

Тестове середовище було розгорнуто у вигляді віртуальної машини на базі Ubuntu Linux з встановленим веб-сервером Apache та модулем ModSecurity. Додатково використовувалася хмарна платформа Cloudflare для активації її вбудованого WAF. У якості веб-додатку застосовувався простий HTML-інтерфейс із формами вводу, які дозволяють моделювати атаки типу SQLi, XSS тощо. Використовувалися типові конфігурації OWASP Core Rule Set [6], а також базові можливості Cloudflare WAF [7]. Тестування без WAF проводилося на тому ж середовищі, але з відключеним захистом.

Для моделювання атак використовувалися класичні приклади шкідливих запитів, які входять до переліку OWASP Top 10 [2]. У таблиці 1 наведено конкретні шкідливі запити, які було застосовано для тестування кожного типу атаки, включаючи SQL-ін’єкції (SQLi), міжсайтове скриптування (XSS), локальне включення файлів (LFI), віддалене виконання команд (RCE) та підміну міжсайтових запитів (CSRF). Ця інформація дозволяє прозоро відстежити відповідність між видом атаки, тестовим навантаженням та отриманими результатами ефективності захисту.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Таблиця 1

Шкідливі запити для тестування вразливостей

Уразливість	Перший шкідливий запит	Другий шкідливий запит
SQLi	*‘ OR ‘1’=‘1*	*admin’ –*
XSS	*<script>alert(1)</script>*	*<img src=x onerror=alert(1)>*
LFI	*../../../../etc/passwd*	*../index.php*
RCE	*ping -c 1 127.0.0.1*	*`ping 127.0.0.1`*
CSRF	*підміна POST-запиту*	*зміна пароля без токена*

Джерело: розроблено автором

Атаки на вебдодаток здійснювались шляхом введення шкідливих даних у текстові поля форм на вебсторінках або через безпосередню передачу спеціально сформованих GET-запитів до сервера. Кожен шкідливий запит моделювався вручну: відповідні дані вводились у поля вводу (наприклад, поля авторизації, пошуку чи зворотного зв’язку) або додавались до URL у вигляді параметрів запиту. Для кожного кейсу проводилась фіксація реакції системи за низкою визначених критеріїв: чи було виявлено та заблоковано атаку засобами WAF, чи обробив сервер шкідливий запит як звичайний, чи з’явилось повідомлення про помилку або сповіщення для користувача, а також чи була відповідна подія зафіксована у системних журналах безпеки. Всі результати експериментів заносились до узагальнюючої таблиці, що стала основою для подальшого аналізу ефективності кожного з досліджуваних WAF-рішень.

Нижче наведено узагальнену таблицю результатів тестування систем Web Application Firewall щодо їх здатності виявляти та блокувати типові вектори атак, описані в переліку OWASP Top 10. Тестування проводилося в однакових умовах із застосуванням однакових шкідливих запитів, що імітують SQL-ін’єкції (SQLi), міжсайтове скриптування (XSS), локальне включення файлів (LFI), віддалене виконання коду (RCE) та підміну міжсайтових запитів (CSRF).

У середовищі без активованого WAF усі атаки були успішно виконані, що свідчить про відсутність будь-якого рівня захисту.

ModSecurity продемонстрував високий рівень ефективності при блокуванні SQL-ін’єкцій, LFI та RCE, проте виявився недостатньо надійним у виявленні XSS-атак, які успішно проходили захист. У випадку з CSRF-запитами система не ідентифікувала загрози, що вказує на її обмеженість у контексті захисту від неавтентифікованих змін дій користувача.

Cloudflare WAF показав кращі результати у блокуванні XSS та SQLi-атак, що вказує на ефективніший і точніший фільтр на рівні HTTP-запитів. Разом із цим, система не заблокувала деякі LFI-запити, які потенційно могли б бути використані для розкриття вмісту системних файлів або отримання несанкціонованого доступу до конфіденційних даних. У випадку з CSRF-атаками Cloudflare частково ідентифікував загрозу та успішно заблокував окремі шкідливі сценарії.

Таблиця 2

Результати тестування систем WAF при типових атаках

Тип атаки	Шкідливий запит	Без WAF	ModSecurity	Cloudflare WAF
SQLi	‘ OR ‘1’=‘1	Пройшла	Заблоковано	Заблоковано
SQLi	admin’ --	Пройшла	Заблоковано	Заблоковано
XSS	<script>alert(1)</script>	Пройшла	Пройшла	Заблоковано
XSS	<img src=x onerror=alert(1)>	Пройшла	Пройшла	Заблоковано
LFI	../../../../etc/passwd	Пройшла	Заблоковано	Пройшла
LFI	../index.php	Пройшла	Заблоковано	Пройшла
RCE	; ping -c 1 127.0.0.1	Пройшла	Заблоковано	Заблоковано

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Тип атаки	Шкідливий запит	Без WAF	ModSecurity	Cloudflare WAF
RCE	`ping 127.0.0.1`	Пройшла	Заблоковано	Заблоковано
CSRF	Підміна POST-запиту	Пройшла	Не виявлено	Частково заблоковано
CSRF	Зміна пароля без токена	Пройшла	Не виявлено	Частково заблоковано

Джерело: розроблено автором

Для повноцінної оцінки обраних WAF-рішень доцільно порівняти їх за ключовими практичними характеристиками, які впливають на реальне впровадження та експлуатацію систем у різних умовах. Зокрема, було проаналізовано три важливі аспекти: вартість впровадження, наявність та якість технічної підтримки, а також ресурсоємність, тобто вплив системи на продуктивність веб-додатків. Це дозволяє не лише оцінити ефективність захисту, а й зрозуміти, наскільки кожне з рішень підходить для застосування у певному середовищі – навчальному, корпоративному або комерційному. Нижче наведено короткий аналіз за кожним з обраних критеріїв.

Вартість використання кожного з рішень суттєво відрізняється. ModSecurity є безкоштовним програмним забезпеченням з відкритим вихідним кодом, що дозволяє розгорнути систему без ліцензійних витрат. Однак слід враховувати непрямі витрати – зокрема, час і ресурси, необхідні для інсталяції, налаштування та супроводу. У випадку з Cloudflare WAF, базовий рівень захисту доступний безкоштовно, проте розширений функціонал (включно з повноцінним WAF) входить до платних тарифів, починаючи від приблизно $20 на місяць.

Різниця в ресурсоємності також є суттєвою. ModSecurity функціонує безпосередньо на веб-сервері, що може створювати додаткове навантаження, особливо при високій інтенсивності трафіку або великій кількості правил. Це потребує ретельного підходу до оптимізації та моніторингу. Натомість Cloudflare WAF працює у хмарі, фільтруючи запити ще до того, як вони досягають сервера користувача, що значно зменшує локальне навантаження і позитивно впливає на загальну продуктивність веб-додатку.

Висновки. У ході проведеного експериментального дослідження було здійснено порівняльний аналіз ефективності систем Web Application Firewall (WAF) на прикладі двох популярних рішень – ModSecurity та Cloudflare WAF. Тестування проводилося в контрольованому середовищі з моделюванням типових атак, що відповідають переліку OWASP Top 10. Результати показали, що обидва рішення демонструють високий рівень захисту від поширених векторів атак, зокрема SQL-ін’єкцій (SQLi), міжсайтового виконання скриптів (XSS) та виконання довільних команд (RCE). При цьому було зафіксовано й окремі випадки часткової ефективності: так, Cloudflare WAF не завжди коректно обробляв атаки типу LFI, а ModSecurity в окремих випадках пропускав XSS-ін’єкції. Ці результати свідчать про те, що жодне з протестованих рішень не забезпечує абсолютного захисту, але кожне має свої сильні сторони.

Отримані результати підтверджують доцільність використання WAF як складової багаторівневої архітектури безпеки веб-додатків. Надійний захист не може базуватися лише на одному компоненті – тому WAF доцільно застосовувати у поєднанні з іншими механізмами, такими як захищене кодування, контроль доступу, двофакторна автентифікація та регулярне тестування на проникнення. Важливим чинником ефективності WAF є також правильна конфігурація системи, адаптація фільтрів до конкретного середовища та активне ведення журналів безпеки. Неправильно налаштований WAF може як пропустити атаку, так і помилково заблокувати легітимний трафік.

На основі дослідження можна сформулювати такі перспективи подальших розвідок у цьому напрямку: розширення тестування за рахунок включення інших WAF-рішень (наприклад, AWS WAF, F5 Advanced WAF, Imperva тощо); оцінка впливу WAF на продуктивність та затримки при обробці HTTP/HTTPS-запитів; дослідження поведінки WAF

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

у реальному мережевому трафіку, включаючи атаки нульового дня (0-day); інтеграція WAF у середовища DevSecOps із застосуванням автоматизованих процесів CI/CD і моніторингу безпеки в режимі реального часу; розробка універсальних підходів до тестування WAF, що дозволить отримувати об'єктивні порівняльні показники в різних умовах.

Таким чином, використання WAF у поєднанні з іншими засобами кіберзахисту дозволяє істотно підвищити стійкість веб-додатків до сучасних кіберзагроз. Водночас вибір конкретного рішення має базуватися на результатах практичної оцінки, специфіці інфраструктури та наявних ресурсах. Проведене дослідження є внеском у розуміння сильних і слабких сторін популярних WAF-рішень та може бути основою для подальших прикладних і наукових робіт у цій галузі.

Список використаних джерел

1. Ristic I. ModSecurity Handbook: The Complete Guide to the Popular Open Source Web Application Firewall. – London: Feisty Duck Ltd, 2013. – 424 p.
2. OWASP Foundation. OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-top-ten/
3. Stuttard D., Pinto M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. – 2nd ed. – Indianapolis: Wiley Publishing, 2011. – 912 p.
4. Ghosh, S., Singh, M., Nayyar, A., & Obaidat, M. S. (2023). An Efficient Machine Learning-Based Web Application Firewall with Deep Automated Pattern Categorization. *Journal of Information Security and Applications*, [Електронний ресурс]. – Режим доступу: https:// www. researchgate.net/publication/375699396_An_Efficient_Machine_Learning-Based_Web_Application_Firewall_with_Deep_Automated_Pattern_Categorization
5. Rajendran, K., Tiwari, A., & Saini, J. R. (2022). Web Application Firewall Using Machine Learning and Features Engineering. *Security and Privacy*, vol. 5, no. 1. – [Електронний ресурс]. – Режим доступу: https://onlinelibrary.wiley.com/doi/10.1155/2022/5280158
6. OWASP ModSecurity Core Rule Set [Електронний ресурс]. – Режим доступу: https://coreruleset.org
7. Cloudflare. What is a Web Application Firewall (WAF)? [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Роботу виконано під науковим керівництвом PhD, старшого викладача
ШЕСТАКА Я. І.

КРИТЕРІЇ БЕЗПЕКИ ПРИ РОЗРОБЦІ КРИПТОГАМАНЦЯ

КУЗЬМЕНКО М. О., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні критерії безпеки, які необхідно враховувати під час розробки криптогаманця. Визначено ключові загрози та ризики, пов'язані з функціонуванням криптогаманців, а також переваги впровадження безпечних програмних рішень. Як приклад розглянуто принципи створення безпечного криптогаманця на основі сучасних стандартів шифрування та автентифікації.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

The article examines the main security criteria that must be considered when developing a cryptocurrency wallet. Key threats and risks associated with the operation of cryptocurrency wallets are identified, as well as the advantages of implementing secure software solutions. As an example, the principles of creating a secure cryptocurrency wallet based on modern encryption and authentication standards are considered.

Актуальність. Розвиток криптовалют трансформує фінансовий сектор, забезпечуючи нові можливості для користувачів і компаній. Криптогаманці стали основою для зберігання, обміну та управління криптовалютами, однак їхня популярність супроводжується зростанням атак зловмисників. У світлі даних фактів, критерії безпеки, за якими розробляються криптогаманці, набувають особливої значущості для забезпечення довіри користувачів і стабільності ринку криптовалют. Врахування цих критеріїв є необхідним, щоб уникнути можливих фінансових втрат і забезпечити захист персональної інформації.

Криптогаманці забезпечують зберігання приватних ключів – необхідного компоненту для доступу до криптовалюти, що підкреслює важливість критерію їхньої безпеки. Серед основних загроз можна виділити несанкціонований доступ, втрату приватних ключів, фішинг, а також різноманітні технологічні вразливості. З огляду на ці фактори, виникає необхідність у чітко визначених критеріях безпеки, як на етапі розробки, так і під час експлуатації криптогаманців, щоб мінімізувати ризики, пов'язані із використанням цих технологій.

Метою статті є визначення ключових критеріїв безпеки при розробці криптогаманців, а також огляд існуючих підходів до забезпечення цих критеріїв у розробницьких практиках. Оцінка цих аспектів дасть можливість підвищити рівень безпеки криптогаманців і зменшити ризики, пов'язані з їх використанням.

Об'єктом дослідження є криптогаманці, що використовуються для зберігання та управління криптовалютами. Розглядаються різні типи гаманців, зокрема програмні (гарячі) й апаратні (холодні) варіанти, з їхніми специфічними перевагами та недоліками в контексті безпеки.

Предмет дослідження – основні критерії, що визначають безпеку криптогаманців, в тому числі не тільки технологічні аспекти, але й організаційні, що покликані забезпечити цілісність і доступність даних, а також інформаційних активів.

Аналіз попередніх досліджень. Розгляд попередніх досліджень у сфері безпеки криптовалютних гаманців дозволяє визначити основні проблеми та недоліки існуючих підходів. Аналіз наявних робіт показує, що автори зосереджуються на різних аспектах розробки криптосистем, проте питання безпеки часто розглядається поверхнево або недостатньо детально. У цьому контексті варто проаналізувати дослідження, присвячені децентралізованим платіжним системам, централізованим криптогаманцям та агрегаторам обміну криптовалют, що дозволяє виявити потенційні шляхи покращення безпеки.

М. Хорошун зосереджується на розробці децентралізованої платіжної системи на базі Ethereum [1], де використання смарт-контрактів дозволяє усунути посередників та мінімізувати ризики шахрайства (рис. 1).

Однак робота повністю орієнтована на Ethereum, що створює певні проблеми, зокрема, залежність від швидкості обробки транзакцій та високі комісії. Крім того, автор не приділяє достатньої уваги потенційним вразливостям смарт-контрактів, таким як атаки повторного входу (reentrancy) чи проблеми з управлінням приватними ключами. Масштабованість системи також залишається відкритим питанням, що може обмежити її застосування у великих проєктах.

В. Демиденко розглядає централізований криптогаманець, зосереджуючи увагу на зручності користувацького інтерфейсу та інтеграції з криптобіржами [2]. Основним недоліком такого підходу є централізоване зберігання криптоактивів, що створює загрозу їх втрати у разі

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

зламу сервера або зловживань з боку адміністратора. Відсутність акценту на безпеці знижує практичну цінність дослідження у контексті створення надійних криптогаманців.

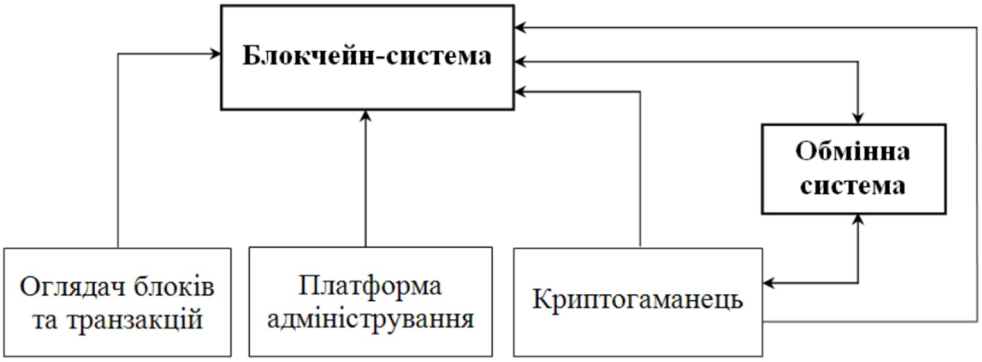


Рис. 1. Загальна схема взаємодії компонентів системи

Джерело: [1]

Робота Р. Соколовського присвячена розробці веб-орієнтованого агрегатора обміну криптовалют, який дозволяє користувачам знаходити найвигідніші курси обміну на різних біржах [3]. Хоча цей підхід є корисним для підвищення ефективності торгівлі, питання безпеки транзакцій залишається поза увагою. Зокрема, у дослідженні не аналізуються потенційні загрози, пов'язані з незахищеними API-запитами, що можуть стати ціллю атак типу «людина посередині» (Man-in-the-Middle). Крім того, агрегатор не враховує необхідність анонімності користувачів, що є критичним аспектом у сфері криптовалют.

Проведений аналіз свідчить про те, що існуючі підходи до розробки криптогаманців та криптовалютних сервісів мають суттєві недоліки у сфері безпеки. Одним із основних напрямків покращення є перехід до децентралізованих рішень, що усувають ризики централізованого зберігання активів. Також необхідно приділити увагу механізмам захисту приватних ключів, зокрема, через використання шифрування та апаратних засобів зберігання. Крім того, важливим є впровадження додаткових рівнів безпеки при взаємодії з біржами та забезпечення анонімності користувачів. Подальші дослідження повинні бути зосереджені на розробці та впровадженні криптографічних протоколів, що дозволять підвищити рівень захисту криптогаманців та мінімізувати ризики компрометації даних.

Виклад основного матеріалу. Одним із фундаментальних аспектів є використання надійних алгоритмів шифрування для захисту приватних ключів та інших конфіденційних даних. Рекомендується застосовувати алгоритм AES (Advanced Encryption Standard) з довжиною ключа 256 біт, який забезпечує високий рівень захисту від несанкціонованого доступу. Крім того, впровадження багатофакторної автентифікації (MFA), яка поєднує паролі, біометричні дані та одноразові коди, значно підвищує рівень безпеки, знижуючи ймовірність успішних атак на облікові записи користувачів.

Приватні ключі є основним засобом доступу до криптовалютних активів. Втрата чи компрометація ключа може призвести до повної втрати коштів. Основні підходи до їхнього захисту:

- апаратні гаманці (HSM, Ledger, Trezor) – зберігання ключів у захищеному фізичному пристрої (рис. 2);
- мнемонічні фрази (BIP39) – відновлення доступу за допомогою унікальної фрази;
- мультипідпис (Multisig) – необхідність підпису кількох сторін для підтвердження транзакцій.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Рис. 2. Апаратні криптогаманці Trezor та Ledger Nano S

Джерело: [4]

Постійне оновлення програмного забезпечення та проведення регулярних аудитів коду є необхідними для виявлення та усунення потенційних вразливостей. Розробники повинні забезпечити своєчасне закриття виявлених вразливостей та підтримувати актуальність системи безпеки.

Рекомендовано використовувати:

- аналіз статичного коду (SAST) – перевірка вразливостей перед релізом;
- тестування на проникнення (Pentesting) – перевірка на можливість реальних атак;
- моніторинг активності (SIEM, IDS/IPS) – виявлення аномальної поведінки.

Користувачі є однією з найслабших ланок у системі безпеки. Проведення навчальних заходів та інформування про методи захисту може суттєво знизити ризик фішинг-атак та інших видів шахрайства. Освічені користувачі менш схильні до компрометації своїх облікових записів.

Зі зростанням кількості смарт-контрактів, що впроваджуються в блокчейн, збільшується кількість атак на їхні вразливості та помилки в коді. Це може призвести до фінансових збитків і втрати довіри до технології. Шахраї часто використовують фішинг для отримання доступу до облікових даних користувачів криптогаманців, створюючи підроблені веб-сайти або надсилаючи електронні листи, які імітують легітимні сервіси, щоб обманом змусити користувачів розкрити свої приватні ключі або паролі.

Атаки соціальної інженерії спрямовані на маніпулювання користувачами для отримання конфіденційної інформації. Наприклад, шахраї можуть видавати себе за представників служби підтримки, щоб отримати доступ до облікових записів користувачів. Віруси та інше зловмисне програмне забезпечення можуть бути використані для викрадення приватних ключів або паролів з пристроїв користувачів. Використання антивірусних програм та регулярне оновлення системи можуть допомогти запобігти таким атакам. Недоліки або помилки в коді криптогаманця можуть бути використані зловмисниками для отримання несанкціонованого доступу. Регулярні аудити безпеки та тестування можуть допомогти виявити та усунути такі вразливості (табл. 1).

Апаратні гаманці зберігають приватні ключі в офлайн-режимі, що робить їх менш вразливими до хакерських атак. Рекомендується використовувати такі пристрої для зберігання значних сум криптовалют. Використання надійних паролів, які складаються з випадкових символів, цифр та літер різного регістру, є важливим заходом безпеки. Регулярна зміна паролів та уникання використання однакових паролів для різних сервісів знижує ризик компрометації. Резервне копіювання даних гаманця дозволяє відновити доступ до коштів у разі втрати або пошкодження пристрою. Зберігання резервних копій у безпечному місці, наприклад, на фізичних носіях, є рекомендованою практикою. Розробники повинні впроваджувати механізми виявлення та запобігання фішинг-атак, такі як перевірка автентичності веб-сайтів та сповіщення користувачів про потенційні загрози.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Таблиця 1

Аналіз загроз та методів захисту

Загроза	Опис	Методи захисту
Фішинг	Атака через підроблені сайти	Використання антивірусів, DNSSEC, цифрових сертифікатів
Викрадення приватних ключів	Злам сховищ чи пристроїв	Апаратні гаманці, багаторівнева автентифікація
Атаки повторного входу (Reentrancy)	Вразливість смарт-контрактів	Кодові аудити, використання перевірених бібліотек
MITM («людина посередині»)	Перехоплення мережевого трафіку	E2E шифрування, SSL/TLS

Джерело: розроблено автором

Використання цифрових підписів та сертифікатів може підвищити довіру до сервісу. Проведення регулярних аудитів безпеки та тестування на проникнення допомагає виявити вразливості в системі та своєчасно їх усунути. Залучення незалежних експертів для оцінки безпеки підвищує надійність гаманця. Інформування користувачів про потенційні загрози та методи захисту, а також надання рекомендацій щодо безпечного використання гаманця сприяє загальному підвищенню рівня безпеки. Розробка детальних інструкцій та проведення навчальних вебінарів можуть бути корисними заходами.

Одним із способів мінімізації ризиків є багатофакторна автентифікація (MFA) (рис. 3):

- пароль + біометрія (FaceID, відбиток пальця);
- пароль + одноразовий токен (TOTP, FIDO2);
- пароль + фізичний ключ безпеки (YubiKey, Google Titan).

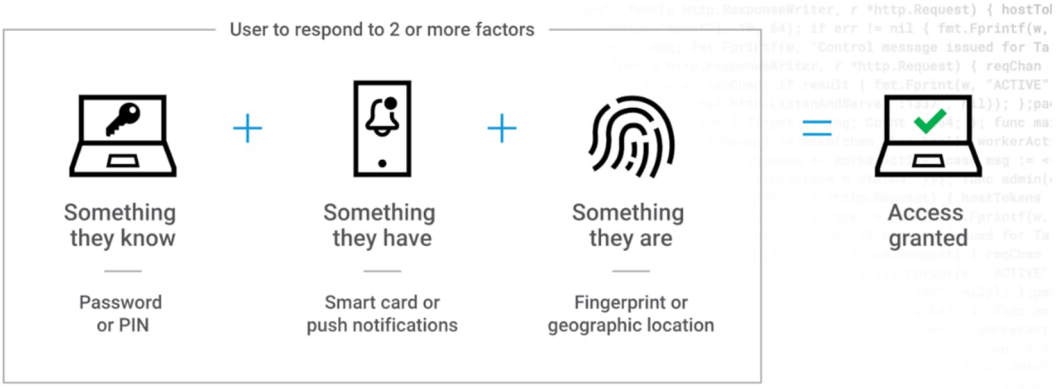


Рис. 3. Як працює багатофакторна автентифікація (MFA)

Джерело: [5]

Забезпечення безпеки криптогаманців вимагає комплексного підходу, який включає використання сучасних криптографічних методів [6], розробку надійних механізмів автентифікації, безпечне управління приватними ключами, регулярні оновлення та аудити, а також підвищення обізнаності користувачів щодо можливих загроз.

Особливу увагу слід приділяти принципам безпеки на рівні програмного забезпечення. Упровадження кодування за допомогою принципу мінімальних привілеїв, обмеження доступу до критично важливих функцій та зменшення поверхні атак є ключовими аспектами. Наприклад, реалізація механізму ізоляції привілейованих процесів допоможе знизити ризик компрометації гаманця в разі успішної атаки на окремий його компонент (табл. 2).

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Важливим етапом є тестування безпеки перед випуском продукту. Тести на проникнення дозволяють оцінити вразливість криптогаманця до реальних атак, виявити слабкі місця та вдосконалити захисні механізми [7]. Крім того, застосування автоматизованих засобів аналізу коду може допомогти виявити потенційні уразливості та порушення стандартів безпеки [8].

Таблиця 2

Механізм ізоляції привілейованих процесів у контексті безпеки криптогаманців

Компонент механізму	Опис
Принцип мінімальних привілеїв	Кожен процес має тільки ті дозволи, які необхідні для виконання його завдань, що мінімізує ризик компрометації
Розділення критичних функцій	Важливі операції (наприклад, доступ до приватних ключів) ізольовані від решти компонентів гаманця
Система контейнеризації	Використання контейнерів (Docker, Firecracker) дозволяє запускати різні процеси окремо, запобігаючи поширенню атак
Контроль міжпроцесної взаємодії	Взаємодія між різними частинами криптогаманця відбувається через безпечні канали з обмеженими привілеями
Моніторинг поведінки процесів	Системи виявлення загроз відстежують аномальну активність у процесах та блокують потенційні атаки
Пісочниця (Sandboxing)	Використання віртуалізованого середовища для ізоляції потенційно небезпечного коду від основних компонентів системи
Шифрування міжпроцесних комунікацій	Дані, що передаються між процесами, зашифровані, щоб уникнути їх перехоплення або модифікації

Джерело: розроблено автором на основі [7–8]

Використання надійних алгоритмів шифрування забезпечує захист даних як у процесі передачі, так і при зберіганні. Симетричне шифрування, таке як AES-256, може бути застосоване для захисту локально збережених даних, тоді як асиметричне шифрування (наприклад, RSA або ECC) ефективне для перевірки цифрових підписів та автентифікації користувачів. Додатково, хешування паролів за допомогою стійких алгоритмів, таких як bcrypt або Argon2, є необхідною практикою для забезпечення їх захисту від атак з підбором (рис. 4).

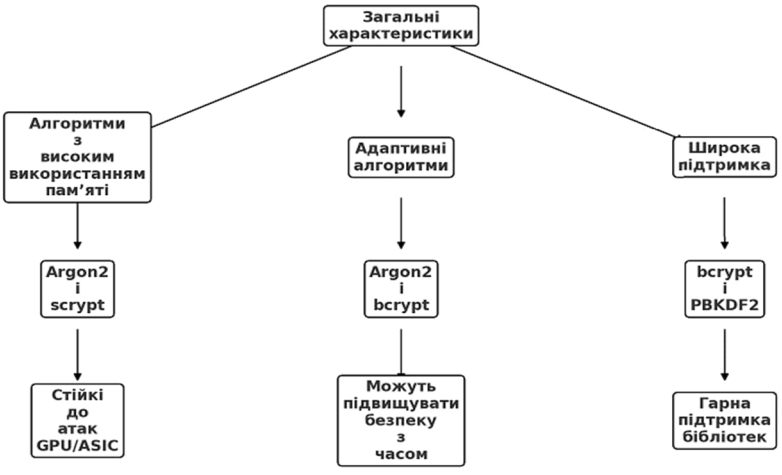


Рис. 4. Порівняння алгоритмів bcrypt та Argon2

Джерело: [9]

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Окрім криптографічного захисту, важливим є зменшення ризиків, пов'язаних із людським фактором. Для цього розробники можуть передбачити механізми запобігання фішинг-атакам, такі як перевірка доменних імен та цифрові сертифікати. Додатково, інтеграція механізмів поведінкового аналізу дозволяє виявляти підозрілу активність користувача та блокувати потенційно небезпечні операції.

Загальний рівень безпеки системи також залежить від правильного впровадження механізмів резервного копіювання. Створення та безпечне зберігання бекапів дозволяє відновити доступ до активів у випадку втрати пристрою або пошкодження даних. Одним із варіантів є використання мнемонічних фраз (seed-фраз), які дозволяють користувачам відновити свої приватні ключі у разі втрати доступу до гаманця (рис. 5).

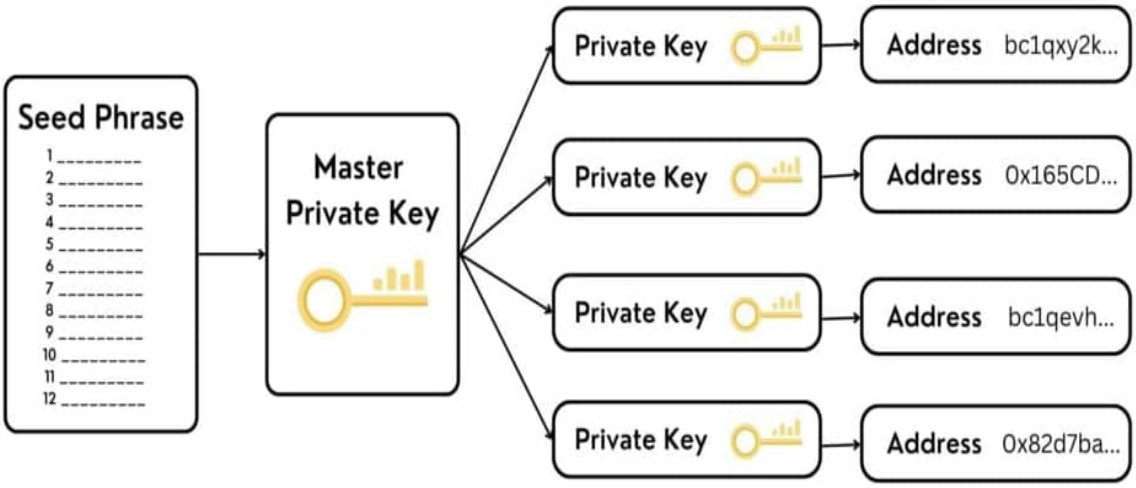


Рис. 5. Приклад роботи seed-фраз

Джерело: [10]

Окрім програмних рішень, безпека криптогаманця може бути підвищена за допомогою апаратних механізмів. Використання апаратних модулів безпеки (HSM) або спеціалізованих апаратних гаманців дозволяє зберігати криптографічні ключі в ізольованому середовищі, що значно ускладнює їх компрометацію.

У сучасних криптогаманцях також активно використовується мультипідпис (multisig), який вимагає схвалення операцій кількома приватними ключами. Це підходить для корпоративних або спільних рахунків, де необхідний додатковий рівень контролю над транзакціями.

Іншим перспективним напрямком є застосування технологій нульового розголошення (Zero-Knowledge Proofs), які дозволяють перевіряти автентичність користувача без необхідності розкриття його персональних даних. Такі методи можуть значно зменшити ризики витоку конфіденційної інформації. Основними перевагами технології нульового розголошення (Zero-Knowledge Proofs, ZKP) є (рис. 6):

- конфіденційність – дозволяє перевіряти інформацію без її розкриття, що зменшує ризик витоку персональних даних;
- безпека – мінімізує можливість компрометації чутливої інформації, оскільки навіть у разі перехоплення зловмисник не отримає корисних даних;
- ефективність – скорочує необхідність взаємодії між сторонами та зменшує навантаження на мережу при автентифікації;
- децентралізація – підходить для блокчейн-рішень, оскільки дозволяє здійснювати перевірку без необхідності довіряти централізованим серверам.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Забезпечення безпеки криптогаманця є безперервним процесом, що вимагає адаптації до нових загроз та вдосконалення захисних механізмів. Комплексний підхід, що включає криптографічний захист, автентифікацію, контроль доступу, регулярні оновлення та освітні заходи для користувачів, є запорукою надійної роботи криптогаманця та запобігання компрометації активів.

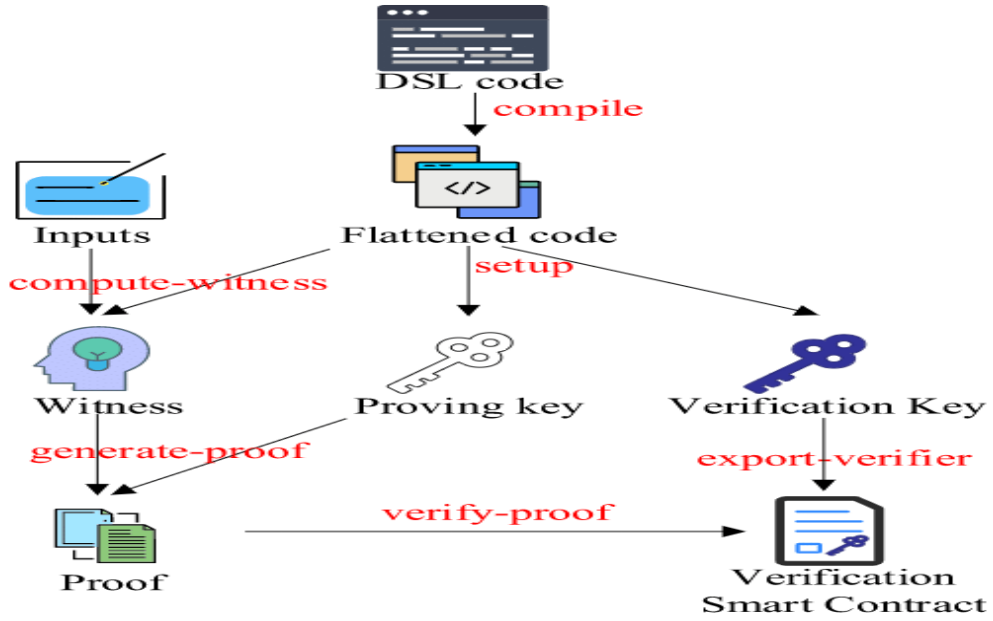


Рис. 6. Приклад роботи Zero-Knowledge Proofs

Джерело: [11]

У подальшому розвиток технологій безпеки в криптогаманцях буде орієнтований на покращення користувацького досвіду без зниження рівня захисту. Інтеграція біометричних методів автентифікації, більш гнучких механізмів доступу та поліпшення юзабіліті без погіршення рівня захищеності стануть важливими аспектами майбутніх розробок у цій сфері.

Розглянуті критерії безпеки дозволяють забезпечити захищене використання криптовалютних гаманців, зменшити ризики шахрайства та атак, а також підвищити довіру користувачів до цифрових активів. Це сприятиме подальшому розвитку екосистеми блокчейн та впровадженню безпечних фінансових технологій.

Висновки. Криптогаманці забезпечують безпечне та децентралізоване управління цифровими активами, усуваючи залежність від традиційних фінансових посередників. Їхнє використання сприяє фінансовій інклюзії, дозволяючи людям у різних куточках світу отримувати доступ до глобальних транзакцій без банківських обмежень. Однак із зростанням популярності криптовалютних операцій зростають і загрози, пов’язані з шахрайством, кібератаками та втратами активів. Саме тому питання безпеки, розглянуті у цій статті, є надзвичайно актуальними, оскільки забезпечують захист цифрових коштів через інноваційні рішення, такі як багатофакторна автентифікація, шифрування, мультипідпис та технології нульового розголошення. Впровадження цих підходів дозволяє не лише зменшити ризики, а й підвищити довіру користувачів до криптовалют, сприяючи їхньому поширенню та інтеграції у глобальну економіку.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаних джерел

1. Хорошун М.Л. (2020). Децентралізована платіжна система з власною цифровою валютою та криптографічним захистом на базі блокчейн-платформи Ethereum. Режим доступу: https://elar.khmnu.edu.ua/items/19c8daef-e1a6-4334-ba9d-679d1baa7e12
2. Демиденко В.А (2023). Дослідження та розробка централізованого криптогаманця з використанням бібліотеки ReactJS. https://ir.nmu.org.ua/handle/123456789/165932
3. Соколовський Р. І. (2024). *Веб-орієнтований агрегатор обміну криптовалют = Web-based Cryptocurrency Exchange Aggregator: Кваліфікаційна робота (спец. 122 – Комп'ютерні науки, освітньо-професійна програма – Комп'ютерні науки)*. Західноукраїнський національний університет. http://dspace.wunu.edu.ua/handle/316497/51945
4. Firebear Studio (2017). *Ledger Nano S vs Trezor: Best hardware cryptocurrency wallets comparison (Ethereum and Bitcoin)*. Firebear Studio. Retrieved from https://firebearstudio.com/blog/ledger-nano-s-trezor-hardware-cryptocurrency-wallets.html
5. Akamai. *What is multi-factor authentication (MFA)?* Retrieved from: https://www.akamai.com/glossary/what-is-multifactor-authentication
6. Шафрай І. Ю. (2023). Порівняння та аналіз сучасних засобів криптографічного захисту даних (алгоритми шифрування) : Перша Всеукр. наук.-практ. конф., присвячена 100-річному ювілею акад. В. М. Глушкова : матеріали конф. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2023. С. 202-205. https://is.ipt.kpi.ua/pdf/TACS-23.pdf
7. Тестування на проникнення, пентест. KR. Laboratories. https://kr-labs.com.ua/service/cybersecurity/testuvannya-na-pronyknennya-ta-vrazlyvosti-pentest/?utm_source=chatgpt.com
8. Konrad Ravenstone (2024). Методичка з тестування на проникнення криптовалютних бірж. KR. Laboratories. https://kr-labs.com.ua/blog/metodychka-testuvannya-na-pronyknennya-kryptovalyutnyh-birzh-i-kryptogamantsiv/
9. Gupta, D. (2024). *Comparative analysis of password hashing algorithms: Argon2, bcrypt, scrypt, and PBKDF2*. https://guptadeepak.com/comparative-analysis-of-password-hashing-algorithms-argon2-bcrypt-scrypt-and-pbkdf2/
10. Professional Crypto Recovery (2025). *How to recover your lost seed phrase*. Professional Crypto Recovery. https://www.professionalcryptorecovery.com/blog/recover-seed-phrase/
11. Parulkar, A. U. (2021). *Identifying authenticity of fake news using blockchain: A literature review*. University of West London. https://www.researchgate.net/publication/362645703_Assignment_1_Literature_Review_Sept_2021_Identifying_Authenticity_of_Fake_News_Using_Blockchain_MSc_Cyber_Security

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

ВИЯВЛЕННЯ ВИТОКУ ДАНИХ ТА ЗАПОБІГАННЯ ЦЬОМУ ЗА ДОПОМОГОЮ АЛГОРИТМІВ DLP

ЛИТВИН Ю. Ю., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

Стаття присвячена виявленню витоку даних та запобіганню йому за допомогою алгоритмів Data Loss Prevention. У роботі розглядаються основні ризики, пов'язані з витоком чутливої інформації в компаніях і організаціях, а також наслідки таких інцидентів, які можуть бути як прямими (матеріальні збитки, штрафи, судові витрати), так і непрямими (шкода репутації, втрата клієнтів, витік інтелектуальної власності). Акцент робиться на

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

застосуванні технологій для моніторингу і захисту інформації, що передається через різні канали зв'язку, зокрема електронну пошту, миттєві повідомлення, веб-форми та передачу файлів. Описується роль алгоритмів Data Loss Prevention у попередженні витоків, їх здатність виявляти та контролювати потоки чутливих даних, а також важливість застосування таких методів для забезпечення безпеки інформаційних систем. Стаття також аналізує основні причини витоків даних і пропонує рекомендації щодо інтеграції алгоритмів Data Loss Prevention для ефективного захисту від загроз.

The article is dedicated to detecting data leaks and preventing them using Data Loss Prevention (DLP) algorithms. The paper discusses the main risks associated with the leakage of sensitive information in companies and organizations, as well as the consequences of such incidents, which can be both direct (material losses, fines, legal costs) and indirect (reputation damage, customer loss, intellectual property leakage). The focus is on the application of technologies for monitoring and protecting information transmitted through various communication channels, including email, instant messaging, web forms, and file transfers. The role of DLP algorithms in preventing leaks is described, including their ability to detect and control the flow of sensitive data, as well as the importance of applying such methods to ensure the security of information systems. The article also analyzes the main causes of data leaks and offers recommendations for integrating DLP algorithms for effective protection against threats.

Актуальність. Витік даних є однією з основних загроз для безпеки компаній, оскільки він може призвести до значних фінансових, репутаційних та юридичних втрат. Сучасні методи захисту, зокрема алгоритми DLP (Data Loss Prevention), дозволяють вчасно виявляти та запобігати витокам інформації, що передається через різні канали зв'язку, такі як електронна пошта, миттєві повідомлення або веб-форми. Ці алгоритми також допомагають здійснювати моніторинг та контроль доступу до чутливих даних, що дозволяє організаціям своєчасно виявляти підозрілі або несанкціоновані дії, які можуть призвести до витоку. Однак, з урахуванням зростаючої кількості та складності кіберзагроз, використання таких технологій є необхідним для забезпечення конфіденційності, цілісності та доступності даних. Впровадження алгоритмів DLP у системи безпеки дозволяє організаціям знижувати ризики витоків, а також захищати свою репутацію та конкурентні переваги, що робить цю тему надзвичайно важливою в умовах сучасного цифрового середовища. В умовах глобалізації та постійного розвитку нових методів кібератак важливість таких рішень лише зростає, а ефективна їх реалізація є критично важливою для стабільної роботи сучасних організацій.

Метою статті є дослідження методів виявлення витоку даних та запобігання йому за допомогою алгоритмів DLP, зокрема аналіз використання таких технологій для виявлення підозрілої діяльності в електронній пошті, миттєвих повідомленнях, веб-формах та інших каналах передачі даних, а також оцінка їх ефективності в умовах сучасних кіберзагроз, що постійно зростають, і необхідності забезпечення безпеки інформації в організаціях, з урахуванням важливості захисту конфіденційних даних, зниження ризиків витоків, а також мінімізації можливих фінансових та репутаційних втрат.

Об'єктом дослідження є процес виявлення витоку даних та запобігання йому за допомогою алгоритмів DLP, зокрема, методи моніторингу та аналізу трафіку, що передається через різноманітні канали зв'язку, а також технології виявлення і блокування витоків чутливої інформації в реальному часі.

Предмет дослідження – підходи до виявлення витоку даних та запобігання йому за допомогою алгоритмів DLP, зокрема, методи обробки та аналізу даних, алгоритми для ідентифікації потенційних загроз, а також технології інтеграції DLP систем з існуючими інфраструктурами безпеки для ефективного захисту від несанкціонованого доступу до конфіденційної інформації.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Аналіз попередніх досліджень. Різні аспекти виявлення витоку даних та запобігання йому за допомогою DLP активно досліджувалися багатьма науковцями. Одним із перших досліджень у цій сфері стало дослідження, в якому розглядався підхід до використання алгоритмів для аналізу контенту, зокрема для виявлення конфіденційних даних в електронних листах, чатах та інших каналах комунікації. Оскільки електронна пошта та онлайн-чат стали основними інструментами обміну даними, цей напрямок досліджень відіграє важливу роль у виявленні потенційних витоків конфіденційної інформації. Науковці, зокрема, Owen M. Astrachan [1], розробили методи фінгерапринтингу (fingerprinting) даних, що дозволяють ідентифікувати конфіденційну інформацію за допомогою спеціальних хеш-значень. Ці методи значно покращили точність виявлення витоку даних при обміні файлами в мережі. Фінгерапринтинг став основою для побудови більш складних систем моніторингу та виявлення витоку даних, дозволяючи ідентифікувати джерела витоків навіть у великих масивах даних. У роботах Amit Goyal і Abhishek Gupta [2] детально розглядається аналіз поведінки користувачів для виявлення підозрілих дій, що можуть вказувати на можливий витік даних через недобросовісних агентів. Їх дослідження охоплює алгоритми профілювання агентів, що допомагають визначити джерело витоку, підвищуючи ефективність DLP-систем. Використання таких алгоритмів дозволяє передбачити можливість витоку ще до того, як він відбудеться, зменшуючи ризики для організації. Також значну увагу приділено методам моніторингу мережевого трафіку. У роботі Philip L. V. Hooijberg [3] автори пропонують використання машинного навчання для ідентифікації аномальних транзакцій, що дозволяє запобігати витоку даних через канали передачі даних в інтернеті. Застосування машинного навчання дозволяє DLP-системам адаптуватися до нових загроз і виявляти підозрілі дії в реальному часі.

Виклад основного матеріалу. Витік даних є серйозною загрозою для інформаційних систем, що призводить до випадкової чи навмисної втрати інформації через збої або недбалість під час зберігання, передачі чи обробки даних. Втрата даних може статися через безліч причин, починаючи від несанкціонованого видалення файлів до випадкового форматування диска, яке миттєво призводить до втрати даних, хоча у таких випадках часто є можливість відновлення інформації за допомогою спеціалізованих інструментів. Інколи користувачі можуть пошкодити свої дані через неакуратне поводження з пристроєм або навіть випадкове падіння накопичувача, що також може спричинити втрату важливої інформації, яку згодом можна відновити, якщо застосувати відповідні засоби для відновлення. Природні катастрофи, такі як пожежі чи повені, можуть серйозно пошкодити жорсткі диски і інші носії, але навіть у таких ситуаціях є шанс відновити втрачені дані. Окрім того, вимкнення живлення під час роботи може призвести до втрати незбережених даних, тому рекомендується регулярно зберігати роботу, щоб мінімізувати можливі втрати. Пошкодження даних може також статися через несправності у файлових системах чи базах даних, а також через збої програмного забезпечення, що в результаті призводить до втрати цінної інформації, яку в деяких випадках можна відновити. Вірусні атаки і зловмисні проникнення в системи ще більше ускладнюють ситуацію, оскільки вони можуть призвести до повної корупції даних і навіть їх повної втрати. Тому для зменшення ймовірності таких інцидентів необхідно використовувати надійне антивірусне програмне забезпечення та дотримуватись сучасних методів захисту інформації.

Витік даних є серйозною загрозою для безпеки сучасних організацій, оскільки він може призвести до значних фінансових, репутаційних та юридичних наслідків. Така проблема виникає, коли чутлива інформація втрачається або потрапляє до неавторизованих осіб через помилки в зберіганні, передачі або обробці даних. Відмінність витоку даних від недоступності даних полягає в тому, що витік є постійним, а недоступність – тимчасовою. Витік даних може статися через фізичне або логічне пошкодження інформації, випадкове видалення або форматування, атакування вірусами, а також через навмисні дії зловмисників, наприклад, хакерські атаки. Крім того, навіть після передачі даних третім особам, такими як аутсорсингові

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

компанії або дослідники, є ймовірність витоку інформації через недостатній контроль за використанням цих даних [1–2].

Один із методів виявлення витоку даних полягає у використанні технології водяних знаків, коли у кожну копію даних вбудовується унікальний код. Якщо ця копія потрапляє до неавторизованих осіб, можна відслідкувати джерело витоку. Однак, водяні знаки можуть бути знищені або змінені, що ускладнює виявлення зловмисників. Крім того, деякі стратегії захисту передбачають обробку чутливих даних до їх передачі, наприклад, за допомогою технік маскування, таких як додавання випадкового шуму або заміна точних значень на діапазони. Це дозволяє зберегти конфіденційність інформації, не змінюючи її сутності, однак у деяких випадках важливо передавати точні дані, як, наприклад, у випадку медичних досліджень або обробки фінансової інформації. Політика запобігання витоку даних за допомогою DLP передбачає використання технологій для моніторингу і контролю доступу до чутливої інформації, виявлення та блокування несанкціонованого обміну даними через канали комунікації, такі як електронна пошта, миттєві повідомлення та веб-ресурси (рис.1). Важливим аспектом є класифікація чутливих даних і використання алгоритмів для їх захисту. Методи водяних знаків дозволяють відслідковувати джерела витоку, а маскування даних допомагає зберегти їх конфіденційність без втрати суті. DLP-системи також блокують передачу даних через ненадійні канали та оцінюють ймовірність витоку, допомагаючи виявити винуватців через аналіз поведінки користувачів. Загалом, DLP забезпечує ефективний захист інформації, мінімізуючи ризики витоку та зберігаючи конфіденційність даних.

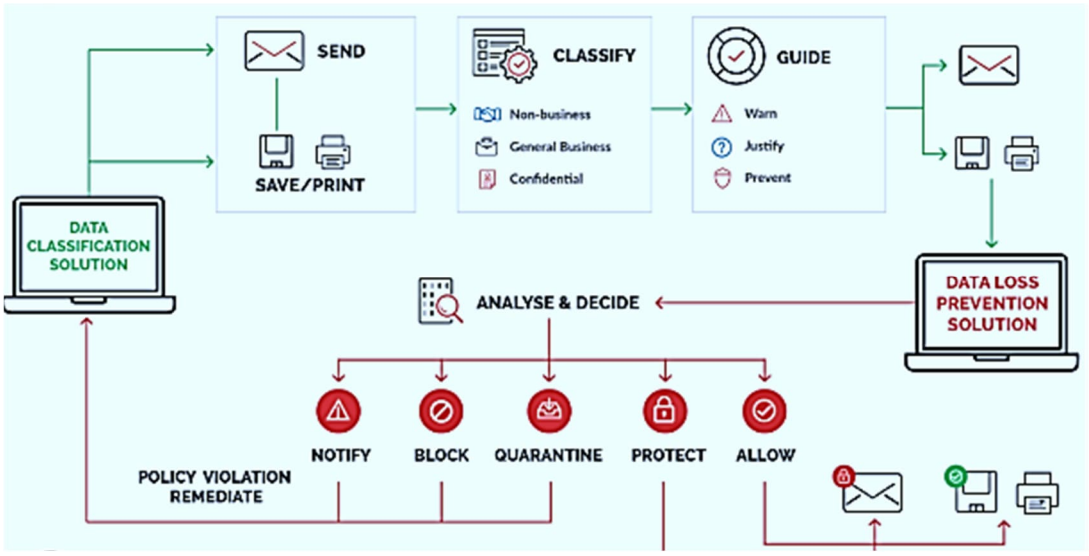


Рис. 1. Політика запобігання втраті даних

Джерело: розроблено автором

Рішення щодо виявлення витоку даних включають застосування алгоритмів для розподілу чутливих об’єктів серед агентів, а також побудову моделей для оцінки ймовірності «вини» агентів, що можуть бути причетними до витоку [1, 3]. У таких випадках важливо не лише ідентифікувати факт витоку, а й визначити джерело витоку, що дозволяє вжити необхідних заходів, як-то припинення співпраці з агентом або ініціація юридичних процедур. Виявлення витоку даних у поєднанні з ефективними алгоритмами DLP допомагає організаціям знизити ризики несанкціонованого доступу до інформації, захищаючи її конфіденційність і цілісність.

Для виявлення витоку чутливих даних, які були передані агентам, і якщо можливо, визначення того, який агент здійснив витік, можна використовувати метод пертурбації. Цей

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

метод полягає в тому, щоб змінити дані таким чином, щоб вони стали менш чутливими, перед тим як передаватися агентам. Розроблена також техніка для непомітного виявлення витоку певного набору даних або записів. Наприклад, після того, як дані передаються агентам, розповсюджувач може виявити, що певний набір даних витекло. Це означає, що третя сторона має доступ до цих даних, і може продемонструвати їх на вебсайті або використовувати в юридичних процесах. Якщо агенти мають частину цих даних, є підозра, що саме вони здійснили витік. Однак агенти можуть заперечувати свою провину, стверджуючи, що дані потрапили до цілі іншим способом. Наприклад, один із об'єктів у наборі може належати клієнту, який також є клієнтом іншої компанії, і ця компанія могла передати ці дані цілі. Або ці дані могли бути відновлені з публічних джерел в Інтернеті. Завданням є оцінка ймовірності того, що витік даних стався через агентів, а не через інші джерела. Чим більший набір даних, тим складніше агентам довести свою невинність. Крім того, чим рідше зустрічаються елементи в наборі, тим складніше довести, що ці дані потрапили до цілі іншим шляхом. Важливо не лише оцінити ймовірність витоку, а й з'ясувати, чи є конкретний агент більш ймовірним винуватцем витоку. Наприклад, якщо один із об'єктів був переданий тільки одному агенту, а інші об'єкти – усім агентам, можна припустити, що саме цей агент міг здійснити витік. Модель, яку пропонується, відображає цю інтуїцію, де агент є винним, якщо він передав один або кілька об'єктів цілі [4].

Для підвищення ефективності виявлення винних агентів розповсюджувач може додавати фальшиві об'єкти до переданих даних. Ці об'єкти створюються з метою ускладнення задачі витоку даних. Однак додавання фальшивих об'єктів може впливати на точність виконання завдань агентами, тому їх використання не завжди є допустимим. Алгоритм розподілу фальшивих об'єктів полягає у виборі агентів, здатних отримати ці об'єкти, і в кожній ітерації додається один фальшивий об'єкт. Оскільки фальшиві об'єкти можуть впливати на цілісність інформації, важливо дотримуватися балансу між використанням цієї техніки і її потенційними ризиками [1–2].

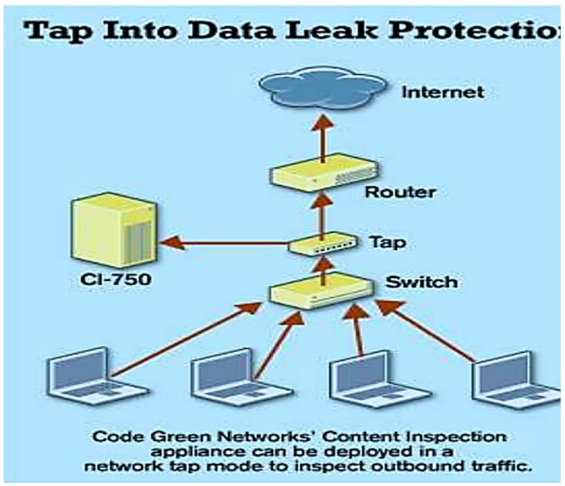


Рис. 2. Захист від витоку даних за допомогою алгоритмів DLP

Джерело: розроблено автором

Захист від витоку даних DLP є набором інструментів безпеки, що спрямовані на запобігання передачі чутливої або критичної інформації за межі корпоративної мережі. Використання технологій DLP обумовлено загрозами з боку внутрішніх користувачів та вимогами законодавства щодо захисту конфіденційної інформації. Продукти DLP використовують бізнес-правила для перевірки вмісту файлів і маркування конфіденційної інформації, що дозволяє уникнути її ненавмисного або навмисного розголошення. Процес

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

маркування дозволяє чітко визначити, які дані є конфіденційними, та обмежити їх доступність для співробітників. Якщо користувач спробує порушити ці обмеження, доступ до чутливої інформації буде заблоковано. Наприклад, маркування може запобігти відправці чутливої фінансової інформації через електронну пошту між співробітниками однієї організації. Для більш ефективного захисту DLP також може включати моніторинг і контроль за використанням знімних носіїв, таких як USB-накопичувачі та зовнішні диски. Важливим аспектом є реалізація політик для блокування несанкціонованого доступу до чутливих даних під час їх обробки або передачі. Інтеграція з іншими системами безпеки, такими як шифрування даних або системи моніторингу мережі, дозволяє створити більш комплексний захист від витоків. Постійне оновлення та налаштування цих систем необхідне для адаптації до нових загроз і забезпечення ефективного контролю за інформаційними потоками в організації [1]. Нехай C – це набір усіх даних, що зберігаються в системі, а $D_S \subseteq C$ – це підмножина чутливих даних, які підлягають маркуванню. Модель маркування може бути виражена як функція M, що призначає кожному елементу даних в наборі C значення маркування:

$$M: C \longrightarrow \{0,1\}, \tag{1}$$

де 1 означає, що дані є чутливими і марковані для захисту, а 0 – що дані не є чутливими.

Модель доступу може бути виражена через функцію f, що визначає доступ користувачів до чутливих даних:

$$f: A \times C \longrightarrow \{0,1\}, \tag{2}$$

де A – набір користувачів, C – набір даних, $D_S \subseteq C$ – чутливі дані, $f(a,c) = 1$ означає, що користувач a має доступ до даних c, $f(a,c) = 0$ означає, що доступ заборонено. Таким чином, контроль доступу до чутливих даних визначається політиками DLP, які забезпечують блокування доступу до цих даних для неавторизованих користувачів.

Модель контролю доступу до чутливих даних, для кожного користувача $a \in A$ і кожного елемента даних $c \in C$, функція f визначає доступ користувача a до чутливих даних c:

$$f(a,c) = \begin{cases} 1, \text{якщо користувач } a \text{ має доступ до с} \\ 0, \text{якщо доступ заборонено} \end{cases}, \tag{3}$$

де A – набір користувачів, C – набір даних, $D_S \subseteq C$ – чутливі дані, $f(a,c) = 1$ означає, що користувач a має доступ до даних c, $f(a,c) = 0$ означає, що доступ заборонено. Таким чином, контроль доступу до чутливих даних визначається політиками DLP, які забезпечують блокування доступу до цих даних для неавторизованих користувачів. Наведені математичні моделі відображають Впровадження системи DLP вимагає ретельного планування і забезпечення належної підтримки на всіх етапах – від ідентифікації чутливих даних до їх постійного моніторингу. Це включає інтеграцію технологій для виявлення та маркування як структурованих, так і менш структурованих даних, таких як текстові документи або електронні листи. Крім того, необхідно створити відповідну інфраструктуру для збереження даних, яка включає як локальні сервери, так і хмарні ресурси, що дозволяють безпечно передавати і зберігати інформацію. Важливим аспектом є також розробка стратегій для керування доступом до даних, що забезпечує мінімізацію можливих витоків через внутрішні або зовнішні канали. Одним із головних завдань є впровадження політик моніторингу та контролю використання чутливих даних, що дозволяє виявляти підозрілі дії в реальному часі. Для підвищення ефективності DLP-системи необхідно використовувати алгоритми машинного навчання та штучного інтелекту, що дозволяють адаптувати систему до нових

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

загроз і змін у робочих процесах. Окрім цього, важливо забезпечити навчання та підвищення обізнаності співробітників щодо правил захисту даних та користування системами безпеки [4].

Постійне вдосконалення системи DLP є необхідним для підтримки високого рівня безпеки та захисту інформації в умовах постійних змін у технологіях та загрозах. Однак на інформаційних технологіях (IT) лежить відповідальність за забезпечення того, щоб вміст, який підлягає ідентифікації через відбитки (fingerprinting), потрапляв до відповідного загального файлу CIFS. Це може бути проблематично, оскільки, наприклад, наша компанія в основному використовує приватні вікі-сторінки, а не спільні томи для більшості внутрішньої інформації. Пропоноване рішення компанії Code Green полягає в тому, щоб за допомогою скрипта регулярно вивантажувати вміст наших вікі на CIFS-розподілений ресурс. З огляду на зростання популярності колаборативних робочих просторів, таких як вікі в бізнес-спільноті, нам хотілося б бачити повністю автоматизований спосіб для ідентифікації даних через відбитки. Крім того, було б доцільно, якщо пристрій міг би безпосередньо використовувати веб-сторінки як джерела даних, а також підтримка інших сховищ даних збільшила б функціональні можливості цього пристрою «з коробки», позбавляючи необхідності додаткових скриптів. Варто зазначити, що багато конкурентних пропозицій, деякі з яких значно дорожчі, навіть не підтримують інтеграцію з базами даних. Процес ідентифікації можна описати через таку функцію::

$$f_d = Fingerprint(d) \quad \forall d \in D, \tag{4}$$

де D – набір даних, що містить чутливу інформацію , $Fingerprint(d)$ – функція, що геннерує унікальний відбиток для кожного елемента даних ddd, що дає можливість відстежити джерело витоку, коли d потрапляє в файли $f \in F$. Важливо, що ця модель описує процес маркування та перевірки даних на наявність відбитків у відповідних файлах. F – набір даних це набір файлів, де ці дані можуть бути збережені (наприклад, вікі-сторінки або CIFS-розподілені ресурси). Техніка fingerprinting вимагає, щоб кожен елемент $d \in D$ мав відповідний відбиток, позначений як f_d, що дає можливість ідентифікації джерела витоку даних [1].

Процес вивантаження даних через скрипти

$$Upload\ (S, f) = tru \text{ якщо } S \text{ вивантажено на } F\ , \tag{5}$$

де S – це набір даних, які необхідно вивантажити з приватних вікі на загальні ресурси, такі як CIFS, f – це спільний ресурс (наприклад, CIFS-розподілений ресурс). Якщо вивантаження не відбулося, то функція повертає *false*, вказуючи на проблему в процесі переносу даних. Для забезпечення ефективної роботи системи ідентифікації та вивантаження, важливо, щоб ці процеси були автоматизовані та підтримували інтеграцію з іншими джерелами даних. Ці дві моделі описують основні етапи процесу ідентифікації та обробки даних через відбитки в умовах колаборативних робочих просторів та необхідність автоматизації цих процесів.

Компанії, що хочуть мати надійне блокування веб- та мережевого трафіку, повинні інвестувати в проксі-пристрій. Пристрій Code Green можна налаштувати як сервер протоколу адаптації веб-контенту (ICAP) при підключенні до проксі-сервера ICAP, такого як Blue Coat Systems або Squid. Коли підключений таким чином, пристрій Code Green може блокувати HTTP, HTTPS та FTP трафік, а також здійснювати розшифрування трафіку для перевірки. Проблему можуть створити й ноутбуки для користувачів Code Green. Компанія пропонує агент для кінцевих точок, який контролює використання знімних носіїв, таких як флеш-накопичувачі та компакт-диски. Він також може забезпечити шифрування даних, збережених на знімних носіях, і відстежує імена файлів та типи, які зчитуються з таких носіїв або зберігаються на них. Однак ноутбуки, які знаходяться поза корпоративною мережею, не підпадають під політики контролю пристрою Code Green, що означає, що чутливі дані можуть

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

бути передані через веб або мережеві протоколи. Це створює потенційні вразливості, які можуть бути використані для витоку важливої інформації. Для вирішення цієї проблеми компанії повинні впроваджувати додаткові заходи безпеки, такі як VPN з шифруванням та моніторинг використання інтернету. Також можна інтегрувати систему для відстеження передачі даних і забезпечити автентифікацію користувачів через багатофакторну перевірку. Важливим елементом є регулярне оновлення політик безпеки для мінімізації ризиків при зміні умов роботи в мережі [2-4].

Як працює DLP (запобігання витоку даних): наступні методи показують, як рішення для запобігання витоку даних допомагають організаціям захищати цінну або чутливу інформацію, що передається, зберігається або використовується. DLP забезпечує потужне рішення для захисту даних, що передаються по мережі (дії в мережі), шляхом прослуховування мережевого трафіку електронних листів, чатів та інших повідомлень для виявлення вмісту, що передається через комунікаційний канал. Крім того, DLP пропонує рішення для захисту даних, що зберігаються, шляхом сканування вмісту сховищ, таких як USB-накопичувачі, жорсткі диски та інші пристрої, для виявлення чутливих даних, також відомого як виявлення вмісту (Content Discovery). Окрім цього, DLP захищає дані в процесі їх використання (дії на кінцевих точках), наприклад, коли користувач підключає USB-накопичувач до комп'ютера. Більшість рішень DLP реалізують захист за допомогою комбінації таких методів, як: регулярні вирази, бази даних для створення відбитків, точне співставлення файлів, часткове співставлення документів, статистичний аналіз, концептуальний аналіз (лексикон), категорії. Завдяки цим методам DLP ефективно виявляє і контролює чутливу інформацію на всіх етапах її життєвого циклу.

Висновок. Виявлення витоку даних та запобігання йому є важливими аспектами сучасної інформаційної безпеки, оскільки витоки конфіденційної інформації можуть завдати значної шкоди організаціям і їх клієнтам. Використання алгоритмів запобігання витоку даних надає потужні інструменти для моніторингу, виявлення та блокування несанкціонованої передачі чутливої інформації як у процесі її передачі по мережі, так і під час зберігання або використання на кінцевих пристроях. Основними методами, що застосовуються в DLP, є сканування мережевого трафіку, виявлення вмісту на знімних носіях і моніторинг дій користувачів на кінцевих пристроях. Для підвищення ефективності запобігання витоку даних алгоритми використовують технології відбитків даних, регулярні вирази, статистичний аналіз та концептуальну класифікацію. Важливим аспектом є також інтеграція DLP з іншими системами безпеки, що дозволяє створювати комплексну архітектуру захисту даних у корпоративних мережах. Незважаючи на те, що сучасні рішення DLP демонструють високий рівень точності при виявленні витоків даних, вони не є панацеєю. У разі використання вебсервісів або ноутбуків, які перебувають поза корпоративною мережею, можливості DLP можуть бути обмежені. Тому важливо комбінувати DLP з іншими засобами захисту та постійно вдосконалювати систему безпеки для забезпечення надійного захисту чутливої інформації. Отже, успішне впровадження алгоритмів DLP є важливим кроком до зниження ризиків витоку даних, однак це вимагає комплексного підходу, включаючи належну конфігурацію системи, постійне оновлення правил та інтеграцію з іншими засобами захисту. Тільки таким чином можна забезпечити належний рівень захисту та мінімізувати загрози витоку конфіденційної інформації.

Список використаних джерел

1. Owen, M. A. Data Fingerprinting for Confidentiality Protection / M. A. Owen // International Journal of Information Security. – 2008. – Vol. 7, № 3. – P. 221–233.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

2. Goyal, A., & Gupta, A. User Behavior Analysis for Data Leakage Prevention / A. Goyal, A. Gupta // Proceedings of the International Conference on Information Security. – 2012. – P. 147–157.

3. Hooijberg, P. L. V. Machine Learning for Network Traffic Monitoring and Data Leak Prevention / P. L. V. Hooijberg // Journal of Network and Computer Applications. – 2015. – Vol. 44. – P. 18–30.

4. Prasad, S., & Soni, M. Data Leak Prevention using Behavioral Profiling and Detection Algorithms / S. Prasad, M. Soni // Sciendo Journal. – 2023. – P. 101–112.

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВОЇ Ю. Є.

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ В ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМАХ

ЛУНГУЛ В. С., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються питання безпеки в електронних платіжних системах, що виникли внаслідок розвитку електронної комерції та появи нових фінансових потреб, які традиційні платіжні системи не завжди можуть ефективно задовольнити. З огляду на це, різні зацікавлені сторони досліджують різні типи електронних платіжних систем, а також питання, пов'язані з цифровими валютами. Загалом електронні платіжні системи можна класифікувати на чотири основні категорії: система електронних готівкових коштів, система електронних чеків, система онлайн-платежів за допомогою кредитних карток та система електронних платежів на основі смарт-карток. Кожна з цих систем має свої переваги та недоліки як для користувачів, так і для продавців. У статті аналізуються рівні безпеки цих платіжних систем у зв'язку з вразливістю до шахрайства, а також визначається, як цей взаємозв'язок впливає на рівень довіри користувачів до електронних фінансових операцій.

The article discusses security issues in electronic payment systems that have emerged due to the development of e-commerce and the rise of new financial needs that traditional payment systems cannot always effectively meet. In this context, various stakeholders are exploring different types of electronic payment systems, as well as issues related to digital currencies. Overall, electronic payment systems can be classified into four main categories: eCash systems, eCheck systems, online payment systems using credit cards, and smart card-based electronic payment systems. Each of these systems has its own advantages and disadvantages for both users and merchants. The article analyzes the security levels of these payment systems in relation to their vulnerability to fraud, as well as how this interconnection affects users' trust in electronic financial transactions.

Актуальність. Однією з найбільших загроз для електронних платіжних систем є кібератаки, спрямовані на викрадення конфіденційної інформації користувачів, зокрема реквізитів банківських карт, облікових даних електронних гаманців та іншої фінансової інформації. Кіберзлочинці використовують різноманітні методи атак, такі як фішинг, атак типу «людина посередині» (MITM), впровадження шкідливого програмного забезпечення та підроблені вебсайти для отримання несанкціонованого доступу до фінансових активів

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

користувачів. Водночас постійне вдосконалення механізмів захисту та запровадження нових технологій безпеки не гарантують повного усунення загроз, оскільки кіберзлочинці розробляють нові способи обходу засобів захисту.

Окрім цього, однією з ключових проблем залишається необхідність підтримання балансу між рівнем безпеки та зручністю користування платіжними системами. Надмірно складні механізми аутентифікації та підтвердження операцій можуть відштовхнути користувачів від використання безпечних методів оплати, тоді як надто прості системи залишають вразливості для зловмисників. Крім того, розвиток фінансових технологій, таких як цифрові гаманці, криптовалюти, мобільні платежі та біометрична аутентифікація, створює нові виклики для забезпечення надійного рівня безпеки під час проведення транзакцій.

З огляду на ці виклики дослідження проблем безпеки в електронних платіжних системах є надзвичайно актуальним. Проведення детального аналізу існуючих загроз, оцінка ефективності поточних методів захисту та розробка нових підходів до забезпечення кібербезпеки дозволять мінімізувати ризики несанкціонованого доступу до фінансових даних і створити більш надійні електронні платіжні платформи. Це сприятиме підвищенню рівня довіри користувачів до електронних платежів, забезпеченню стабільності фінансових систем у цифровому середовищі та зниженню рівня фінансових втрат через кібератаки та шахрайство.

Метою статті є дослідження проблем безпеки в електронних платіжних системах, аналіз основних загроз, таких як фішинг, атаки «людина посередині» (MITM), шкідливе програмне забезпечення та компрометація облікових даних, оцінка ефективності сучасних методів захисту, таких як багатофакторна аутентифікація, шифрування, токенізація, біометричні технології, а також аналіз переваг та недоліків традиційних методів захисту та перспективи застосування блокчейн-технологій, штучного інтелекту та машинного навчання для виявлення шахрайських операцій, з метою формулювання рекомендацій щодо підвищення безпеки електронних платежів, зниження ризиків кіберзлочинності та покращення довіри користувачів до цифрових фінансових сервісів для створення більш стійкої та безпечної фінансової екосистеми.

Об'єктом дослідження є процес забезпечення безпеки електронних платіжних систем, включаючи методи та технології захисту, механізми аутентифікації, шифрування даних, моніторинг транзакцій, а також протидія сучасним загрозам, таким як кібератаки, шахрайство, фішинг, та інші форми несанкціонованого доступу, що можуть вплинути на безпеку та довіру користувачів до електронних платіжних платформ.

Предмет дослідження – підходи, методи та технології забезпечення безпеки в електронних платіжних системах, зокрема аналіз алгоритмів шифрування, систем аутентифікації, виявлення шахрайства, захисту даних під час передавання та зберігання, а також оцінка ефективності впровадження різних заходів безпеки для зниження ризиків кібератак і несанкціонованого доступу.

Аналіз попередніх досліджень. У сфері досліджень інформаційної безпеки електронних платіжних систем існує низка наукових праць, які висвітлюють різні аспекти цієї проблематики. Р. Квасницька, І. Форкун та Т. Гордєєва у своїй статті «Сучасні підходи забезпечення інформаційної безпеки платіжних систем та їх кіберзахисту» аналізують вітчизняні та міжнародні підходи до трактування сутності платіжних систем, особливості їх функціонування та можливості впровадження міжнародних стандартів обміну фінансовими повідомленнями ISO 20022 в платіжній інфраструктурі України [1]. Автори підкреслюють важливість ідентифікації та управління ризиками, зокрема кіберризиками, які є складовою операційного ризику, та пропонують розглядати кіберризик як окремий тип ризиків у функціонуванні платіжних систем.

Д. Рзаєв та С. Рзаєва у статті «Системний аналіз інформаційної безпеки електронних платежів» розглядають питання інформаційної безпеки електронних платежів, аналізують існуючі ризики, пов'язані із здійсненням транзакцій та використанням електронних платіжних

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

систем, а також проблеми, що виникають при забезпеченні інформаційної безпеки електронних платежів [2].

А. С. Савченко у дисертації «Управління ризиками в платіжних системах» досліджує проблеми управління ризиками в платіжних системах, що базуються на електронних розрахунках і електронному обігу грошей [3]. Автор здійснює класифікацію ризиків та обґрунтовує концепцію управління фінансовими й нефінансовими ризиками в платіжних системах електронного обігу грошей, пропонує методи аналізу та прогнозування ризиків на основі системної моделі управління захистом інформації і банківської безпеки.

І. Бугайчук у статті «Інформаційна безпека електронних платіжних систем» досліджує питання забезпечення інформаційної безпеки в електронних платіжних системах, аналізує основні загрози та вразливості, а також пропонує підходи до їх мінімізації шляхом впровадження сучасних технологій захисту та удосконалення нормативно-правової бази [4].

М. Коваленко у монографії «Кібербезпека банківських електронних платежів» розглядає аспекти кібербезпеки в контексті банківських електронних платежів, акцентуючи увагу на методах виявлення та протидії кібератакам, а також на важливості підвищення обізнаності персоналу банків щодо сучасних кіберзагроз [5].

Таким чином, зазначені дослідження підкреслюють важливість комплексного підходу до забезпечення інформаційної безпеки електронних платіжних систем, що включає ідентифікацію та управління ризиками, впровадження міжнародних стандартів, використання сучасних технологій захисту та підвищення обізнаності персоналу щодо кіберзагроз. Такий підхід дозволяє не лише знизити ймовірність шахрайських дій, але й забезпечити стабільність та надійність електронних платіжних сервісів у довгостроковій перспективі. Важливим аспектом є розробка адаптивних механізмів аутентифікації, що можуть ефективно реагувати на нові загрози та атаки. Крім того, інтеграція штучного інтелекту та машинного навчання у процеси безпеки сприятиме автоматичному виявленню аномалій та потенційних загроз у реальному часі. Подальші дослідження мають бути спрямовані на створення інноваційних методів забезпечення конфіденційності, цілісності та доступності даних у цифрових фінансових екосистемах.

Виклад основного матеріалу. З появою електронної комерції виникли нові фінансові потреби, які в багатьох випадках не можуть бути ефективно задоволені традиційними платіжними системами. Враховуючи це, майже всі зацікавлені сторони почали досліджувати різноманітні типи електронних платіжних систем, питання, що стосуються електронних платіжних систем і цифрових валют. Загалом електронні платіжні системи можна поділити на чотири категорії: система електронних грошей, система електронних чеків, система онлайн-платежів за допомогою кредитних карток та система електронних платежів на основі смарт-карт. Кожна платіжна система має свої переваги та недоліки як для клієнтів, так і для торговців. У статті акцентується увага на аналізі рівнів безпеки, зокрема у контексті уразливості до шахрайства, а також визначається, як цей зв’язок впливає на впевненість користувачів у використанні платіжних систем.

Електронна платіжна система є системою фінансового обміну між покупцями та продавцями в онлайн-середовищі, яка здійснюється за допомогою цифрових фінансових інструментів, таких як зашифровані номери кредитних карток, електронні чеки чи цифрові гроші, що підтримуються банком, посередником або законним платіжним засобом. Інтернет сьогодні є комерційним середовищем, в якому здійснюються платежі за товари, інформацію та послуги. Для підтримки такої електронної комерції необхідно забезпечити обмін якимось видом грошей через Інтернет [1]. Безпечний метод оплати – електронна платіжна система – необхідний для компенсації за надану інформацію, товари та послуги в Інтернеті (наприклад, доступ до захищених матеріалів) та для зручності оплати за зовнішні товари та послуги. Це дозволяє автоматизувати процеси продажу, розширюючи кількість потенційних клієнтів і зменшуючи обсяг паперової роботи.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Основні результати роботи можна сформулювати таким чином:

- Огляд різних систем онлайн-платежів.
- Аналіз різних механізмів аутентифікації в онлайн-платіжних системах та рівнів довіри, які вони забезпечують.
- Аналіз показує, що електронні платіжні системи з механізмами аутентифікації, які включають два або більше факторів аутентифікації, зазвичай є більш захищеними, знижують вразливість до шахрайства та підвищують впевненість користувачів у використанні цих систем.

Сьогодні існує велика кількість електронних платіжних систем, більшість з яких є несумісними одна з одною. Основні категорії електронних платіжних систем включають систему електронних грошей, систему електронних чеків, платіжні системи на основі смарт-карток та систему онлайн-платежів за допомогою кредитних карток.

Система електронних грошей, також відома як цифрові гроші, є цифровими коштами, які надають приватним користувачам безпечний, швидкий і низькозатратний спосіб оплати в Інтернеті [3-4]. Вона була створена багатьма окремими учасниками і передається через кілька мереж, замість використання традиційної банківської системи, і найкраще підходить для мікроплатежів. Електронні гроші незалежні від будь-якої мережі або пристрою для зберігання і є портативними. Кошти електронних грошей і їхня вартість можуть бути визначені незалежно від реальної валюти.

Використання eCash (електронні гроші) вимагає, щоб як продавець, так і покупець мали рахунки електронних грошей у випускаючому банку, який випускає токени для своїх клієнтів. У цій електронній платіжній системі токени є платіжними інструментами, які представляють грошові значення. Клієнт повинен встановити на своєму комп'ютері «кібер-гаманець», який зберігатиме гроші, запитувані від банку. Кожен токен має бути зашифрований для забезпечення захисту від несанкціонованого доступу і подвійних витрат, що є важливою проблемою в цій системі [3]. Для підвищення безпеки важливо, щоб процес аутентифікації користувача був багатофакторним, оскільки одноланкове підтвердження особи може бути недостатнім для захисту від шахрайства. Зокрема, використання одноразових паролів (OTP) або біометрії для підтвердження особи може значно підвищити рівень безпеки.

Крім того, важливо забезпечити цілісність переданої інформації за допомогою сучасних криптографічних методів, таких як шифрування та хешування, щоб захистити токени від підробки або маніпуляцій. Всі транзакції повинні бути зафіксовані в захищеному реєстрі, щоб уникнути можливості їхнього скасування чи повторного використання. Оскільки система eCash вимагає підключення до Інтернету для обміну токенами, особливу увагу слід приділяти безпеці каналів зв'язку для запобігання атак типу «man-in-the-middle» [1–2, 5]. Ретельне відстеження всіх транзакцій та впровадження системи для виявлення підозрілих операцій також сприятиме зниженню ризику шахрайства та підвищенню довіри користувачів до системи.

Коли споживач звертається до банку для виведення електронних грошей, банк перевіряє його особу, випускає суму електронних грошей і одночасно віднімає цю суму з рахунку споживача. Електронні гроші можуть бути витрачені тільки на тих сайтах, які приймають їх для оплати. Коли товар доставляється покупцю, продавець може передати електронні гроші в банк, який зарахує суму транзакції на рахунок продавця. У транзакціях з електронними грошима отримувач не знає ідентичність платника, а випускаючий банк може або не може зберігати інформацію про особу отримувача електронних банкнот, що дозволяє клієнту залишатися анонімним. Анонімність клієнта дозволяє йому витрачати однакові токени (платіжні інструменти) для різних транзакцій, що може призвести до подвійних витрат.

Анонімність користувачів і подвійні витрати одних і тих самих токенів є основними вразливими місцями системи електронних грошей. Єдиним механізмом безпеки, що забезпечує система електронних грошей, є шифрування платіжних інструментів (токенів або

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

монет), згенерованих конкретним клієнтом. Система використовує механізм аутентифікації одного фактора, що є недостатнім для платіжних систем, які обробляють критичні платежі. Якщо процес аутентифікації користувача за одним фактором не буде виконано коректно, це може поставити під загрозу основну функцію платіжної системи. Тому система електронних грошей з аутентифікацією одного фактора має низький рівень безпеки.

У таких системах існує високий ризик подвійних витрат, коли користувач може здійснити кілька транзакцій з одним і тим самим токеном або монетою, що може призвести до фінансових втрат та зловживань. Для забезпечення належного рівня безпеки в електронних платіжних системах необхідно впроваджувати багатофакторну аутентифікацію, яка дозволяє підвищити надійність підтвердження особи користувача. Включення додаткових факторів аутентифікації, таких як біометричні дані або одноразові паролі, дозволяє значно зменшити ймовірність несанкціонованого доступу та захистити від можливих атак. Однак навіть багатофакторна аутентифікація не є панацеєю від усіх загроз, оскільки важливу роль відіграють також інші аспекти, такі як захист каналу зв'язку і відстеження підозрілих транзакцій у реальному часі. Окремо варто зазначити важливість використання сучасних криптографічних методів для захисту платіжних інструментів, що дозволяють забезпечити анонімність користувачів без шкоди для їхньої безпеки [2, 4]. Тому для ефективного захисту електронних платіжних систем необхідно поєднувати кілька рівнів захисту та постійно адаптуватися до нових кіберзагроз.

Електронний чек є цифровим еквівалентом паперового чека, де ініціація транзакції відбувається через екранний діалог, а кошти перераховуються через комп'ютерні мережі в момент здійснення операції. Авторизованим користувачам надається електронний чековий блокнот, який поєднує безпечний апаратний пристрій і спеціалізоване програмне забезпечення. Цей електронний чековий блокнот зберігає та передає приватні ключі та сертифікати клієнта для підписання електронних чеків. Взаємодія з фінансовим програмним забезпеченням банку здійснюється через ці пристрої, що підвищує рівень безпеки операцій. Платник підписує електронний чек за допомогою апаратного пристрою, додаючи сертифікат, виданий банком. Одержувач перевіряє підпис, схвалює його та відправляє чек у банк для обробки.

Система електронних чеків використовує захист через PIN-код та цифровий підпис, що робить її більш безпечною порівняно з односторонньою аутентифікацією. Це система з двофакторною аутентифікацією, де користувач підтверджує свою особу через два елементи, що забезпечує високий рівень безпеки. Система смарт-карток на сьогодні є пластиковою карткою з вбудованим чіпом, який дає змогу доступу до різноманітних сервісів, зберігаючи та обробляючи дані за допомогою сучасних технологій. Смарт-картка, як платіжний інструмент, дозволяє виконувати операції не лише через термінали, а й підключатися до безконтактних платіжних мереж. Хоча смарт-картки набули великої популярності, існують питання щодо їхньої безпеки та збереження конфіденційної інформації [3]. Більшість сучасних систем для смарт-карток включають багатофакторну аутентифікацію, щоб забезпечити більш високий рівень захисту.

Однак, незважаючи на високий рівень безпеки, який забезпечує багатофакторна аутентифікація в смарт-картках, існують певні вразливості, зокрема щодо потенційних атак на сам чіп картки або методи безконтактної передачі даних. За наявності фізичного доступу до картки, шахраї можуть намагатися відновити PIN-код або використовувати технології для перехоплення безконтактних транзакцій [1-2]. Для запобігання таким загрозам багато систем вже впроваджують додаткові рівні захисту, зокрема механізми шифрування та моніторинг підозрілих операцій у режимі реального часу. Тому важливо продовжувати вдосконалювати систему безпеки смарт-карток і забезпечити їх інтеграцію з новітніми методами захисту для зниження ризиків крадіжки конфіденційних даних.

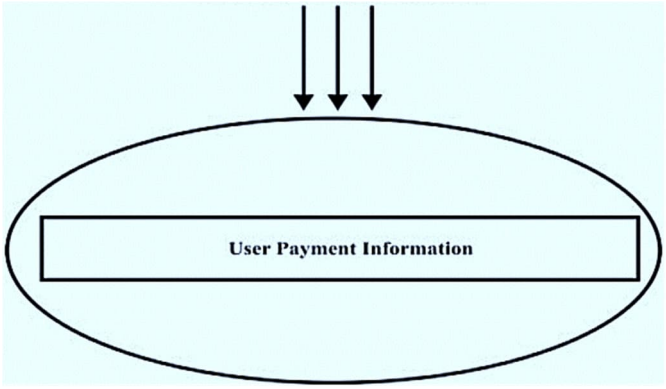
Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Міжнародні стандарти для смарт-карток продовжують вдосконалюватися, що дозволяє покращити їх безпеку, зокрема через використання біометричних даних, таких як відбитки пальців або сканування обличчя. Для доступу до інформації картка потребує спеціальних зчитувачів, що дозволяє уникнути шахрайства, однак втрата картки все ще може призвести до великих ризиків. Онлайн-система кредитних карток зазнала значних змін за останні десятиліття, зокрема через запровадження інноваційних платіжних рішень та вдосконалення безпеки транзакцій. Сучасні кредитні картки дозволяють користувачам здійснювати онлайн-платежі через мобільні додатки та електронні гаманці, такі як Apple Pay, Google Pay або Samsung Pay, що забезпечує безпечні та швидкі транзакції за допомогою біометричної аутентифікації. Ключовим аспектом сучасних онлайн-платежів є інтеграція багатофакторної аутентифікації, що підвищує захист транзакцій та знижує ризики шахрайства.

Система онлайн-платежів за допомогою кредитних карток застосовує двофакторну аутентифікацію через одноразові паролі або біометричні дані, що значно знижує ймовірність несанкціонованих операцій та забезпечує безпеку користувачів [4]. Ці оновлення та вдосконалення роблять сучасні електронні платіжні системи більш захищеними від шахрайства та забезпечують більшу зручність для користувачів, водночас підтримуючи високу довіру до платіжних технологій.

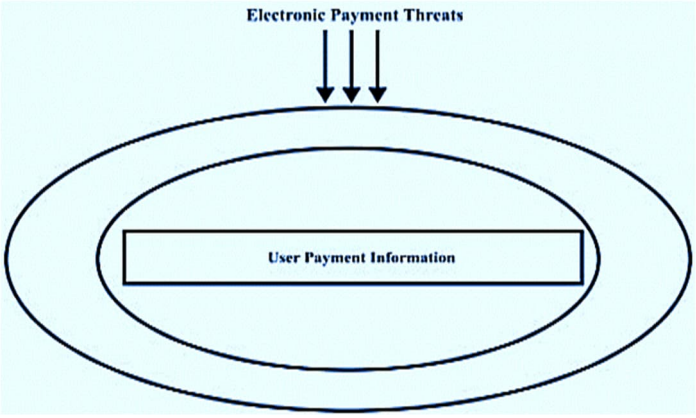
Цільова інформація, яку необхідно захищати від компрометації в процесі кожної онлайн-платіжної транзакції, є платіжною (фінансовою) інформацією користувача. Тому вкрай важливо, щоб метод та система аутентифікації користувача, яку реалізує уповноважений орган, використовували багаторівневий підхід до захисту. Така система може бути доповнена вимогами до різних рівнів безпеки, таких як ПІН-код, криптографічні ключі, цифровий підпис, біометричні дані тощо, для забезпечення множинних рівнів аутентифікації. Варіювання цих рівнів аутентифікації забезпечує більшу або меншу безпеку, причому точність кожного рівня аутентифікаційного фактора повинна бути достатньо конкретною, щоб не порушити цілісність платіжної інформації онлайн-користувачів і не скомпрометувати всю систему [2, 5]. Це означає, що механізм аутентифікації повинен бути достатньо міцним, щоб протистояти різноманітним загрозам, які використовують кіберзлочинці в Інтернеті. Різні рівні аутентифікаційних механізмів, що використовуються різними електронними платіжними системами показані на рис. 1.

Механізм аутентифікації з одним фактором



Механізм аутентифікації з двома факторами

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.



Механізм аутентифікації з трьома факторами

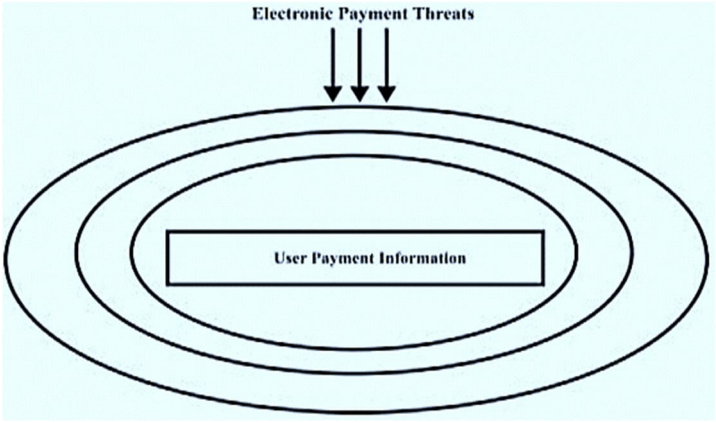


Рис. 1. Механізми аутентифікації за факторами в електронних платіжних системах

Джерело: розроблено автором в середовищі Canva

Різні електронні платіжні системи, які розглядалися раніше, демонструють різні рівні факторів аутентифікації. Фактор аутентифікації визначає рівень безпеки електронної платіжної системи. Механізм аутентифікації з одним фактором використовує або вимагає від користувача підтвердити свою особу лише за допомогою одного елемента даних. Це означає, що електронна платіжна система може бути легко скомпрометована, якщо цей один фактор аутентифікації зазнає невдачі.

Механізм двофакторної аутентифікації передбачає два незалежні елементи інформації, що використовуються в двох взаємопов'язаних та залежних кроках одного процесу, тоді як механізм трьохфакторної аутентифікації включає три незалежні елементи інформації, що використовуються в трьох взаємопов'язаних та залежних кроках того ж процесу [2]. Аутентифікація за допомогою кількох незалежних факторів прагне знизити ймовірність того, що запитувач надає неправдиві дані про свою особу в кількох незалежних, але взаємопов'язаних процесах. Кількість і незалежність факторів є важливими, оскільки більше незалежних факторів означає вищу ймовірність того, що носій ідентифікаційних даних справді має цю особу в іншій сфері.

Електронні платіжні системи, що використовують три або більше факторів аутентифікації, є сильнішими, ніж системи, які використовують лише один або два фактори. Платіжні системи повинні бути реалізовані так, щоб для процесу перевірки платіжної транзакції були представлені кілька факторів аутентифікації. Електронна платіжна система з більшою кількістю факторів аутентифікації/перевірки може мати вищий рівень безпеки [3, 5].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Це означає, що електронна платіжна система з більшою кількістю факторів аутентифікації/перевірки матиме вищий рівень безпеки в порівнянні з системою, яка використовує лише один фактор, таким чином знижуючи вразливість до шахрайства і в кінцевому підсумку підвищуючи довіру користувачів.

Математична модель для рівня безпеки (SL) та фактора аутентифікації (AF):

$$SL = k_1 \cdot AF, \tag{1}$$

де SL – рівень безпеки платіжної системи, AF – фактор аутентифікації, k_1 – константа, яка характеризує ступінь впливу фактору аутентифікації на рівень безпеки. Чим більше факторів аутентифікації, тим вищий рівень безпеки.

Математична модель для вразливості до шахрайства (FV) та фактора аутентифікації (AF):

$$FV = \frac{k_2}{AF}, \tag{2}$$

де FV – вразливість до шахрайства, AF – фактор аутентифікації, k_2 – константа, що визначає, наскільки зміни факторів аутентифікації впливають на вразливість до шахрайства. Збільшення числа факторів аутентифікації зменшує вразливість до шахрайства.

Математична модель для довіри користувачів (UC) та рівня безпеки (SL):

$$UC = k_3 \cdot SL, \tag{3}$$

де UC – довіра користувачів до платіжної системи, SL – рівень безпеки платіжної системи, k_3 – константа, що визначає, як рівень безпеки впливає на довіру користувачів. Вищий рівень безпеки призводить до більшої довіри з боку користувачів.

Загальна математична модель, яка описує взаємозв'язок між всіма змінними:

$$UC = k_3 \cdot (k_1 \cdot AF) = k_3 \cdot k_1 \cdot AF, \tag{4}$$

де UC – довіра користувачів, AF – фактор аутентифікації, k_1 – константа впливу фактора аутентифікації на рівень безпеки, k_3 – константа, яка показує, як рівень безпеки впливає на довіру користувачів.

Математична модель для залежності між вразливістю до шахрайства (FV) та довірою користувачів (UC):

$$FV = \frac{k_4}{UC}, \tag{5}$$

де FV – вразливість до шахрайства, UC – довіра користувачів, k_4 – константа, яка визначає, наскільки зменшення вразливості до шахрайства підвищує довіру користувачів.

Загальний рівень безпеки можна виразити через кількість факторів аутентифікації, вразливість до шахрайства та довіру користувачів як:

$$SL = k_1 \cdot AF \text{ та } FV = \frac{k_2}{AF} \text{ та } UC = k_3 \cdot SL, \tag{6}$$

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Це є комплексною моделлю, яка враховує фактори аутентифікації, рівень безпеки, вразливість до шахрайства та довіру користувачів. Модель забезпечує надійний захист завдяки використанню кількох факторів аутентифікації, що значно знижує ризики несанкціонованого доступу до платіжних систем. Вона дозволяє враховувати не тільки традиційні методи перевірки, але й сучасні технології, такі як біометричні дані, що забезпечують ще вищий рівень безпеки.

Наведені математичні моделі показують, як взаємопов'язані фактори аутентифікації, рівень безпеки, вразливість до шахрайства та довіра користувачів, та як їх зміни впливають на загальний рівень безпеки в електронних платіжних системах. Збільшення кількості факторів аутентифікації безпосередньо підвищує рівень безпеки системи, що, у свою чергу, зменшує ризики шахрайства. Зниження вразливості до шахрайства сприяє зростанню довіри користувачів до електронних платіжних сервісів, що робить їх більш надійними та популярними. Однак надмірне ускладнення процесу аутентифікації може зменшити зручність використання, що потребує балансування між безпекою та зручністю для користувачів. Оптимізація аутентифікаційних механізмів дозволяє створити ефективну систему, яка забезпечує високий рівень захисту без шкоди для користувацького досвіду.

Висновок. Проведений аналіз проблем безпеки в електронних платіжних системах підтвердив, що рівень захисту цих сервісів безпосередньо залежить від ефективності застосованих механізмів аутентифікації. Використання багатофакторної аутентифікації значно підвищує безпеку, знижує ризик шахрайства та зміцнює довіру користувачів. Водночас розвиток цифрових технологій вимагає постійного вдосконалення підходів до забезпечення безпеки електронних платежів. Перспективним напрямом досліджень є інтеграція передових технологій, зокрема біометричних методів аутентифікації, які здатні суттєво покращити надійність і стійкість платіжних систем до сучасних кіберзагроз. Впровадження трифакторної аутентифікації з використанням біометричних даних дозволить створити нові стандарти безпеки та підвищити рівень захисту фінансових операцій. Таким чином, подальші дослідження у сфері безпеки електронних платежів повинні бути спрямовані на розробку комплексних рішень, що поєднують високу ефективність захисту з комфортом користувачів.

Список використаних джерел

1. Квасницька, Р., Форкун, І., Гордєєва, Т. Сучасні підходи забезпечення інформаційної безпеки платіжних систем та їх кіберзахисту / Р. Квасницька, І. Форкун, Т. Гордєєва // Фінансові дослідження. – 2021. – Т. 15, № 2. – С. 112–120.
2. Рзаєв, Д. О., Рзаєва, С. Л. Системний аналіз інформаційної безпеки електронних платежів / Д. О. Рзаєв, С. Л. Рзаєва // Журнал інформаційної безпеки. – 2019. – Т. 10, № 1. – С. 45–55.
3. Савченко, А. С. Управління ризиками в платіжних системах: дис. канд. екон. наук / А. С. Савченко. – Київ: Київський національний економічний університет, 2020. – 198 с.
4. Бугайчук, І. В. Інформаційна безпека електронних платіжних систем / І. В. Бугайчук // Технології захисту інформації. – 2022. – Т. 5, № 4. – С. 60–68.
5. Коваленко, М. М. Кібербезпека банківських електронних платежів: монографія / М. М. Коваленко. – Львів: Видавництво «Львівська політехніка», 2021. – 256 с.

Роботу виконано під науковим керівництвом канд. техн. наук, ст. наук. співроб., доцента ЗВЄРЄВА В. П.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

КРИТЕРІАЛЬНИЙ АНАЛІЗ СИСТЕМ ШИФРУВАННЯ ТА РЕЗЕРВУВАННЯ ДАНИХ

МАЛИК С. В., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто системи шифрування та резервування для підвищення кіберстійкості інформаційних систем. Акцентується на необхідності застосування ефективних методів захисту даних для забезпечення конфіденційності, цілісності та доступності. Оцінюються параметри систем шифрування та резервування. Пропонується інтегроване рішення «Enbamo», яке поєднує шифрування, резервування та моніторинг для комплексного захисту даних та оперативного відновлення інформації.

The article discusses encryption and redundancy systems to improve the cyber resilience of information systems. The author emphasizes the need to apply effective data protection methods to ensure confidentiality, integrity and availability. The parameters of encryption and backup systems are evaluated. An integrated solution «Enbamo» is offered, which combines encryption, backup and monitoring for comprehensive data protection and rapid information recovery.

Актуальність. В умовах стрімкого розвитку цифрових технологій питання безпеки роботи із даними набуває особливої важливості. Збільшення кількості кібератак, витоків конфіденційної інформації та зловмисних дій зумовлює необхідність впровадження ефективних методів захисту даних. Одними із механізмів інформаційної безпеки є системи шифрування, резервування, які забезпечують конфіденційність, цілісність і доступність інформації. Алгоритми шифрування забезпечують високий рівень криптографічного захисту та широко застосовуються для гарантування конфіденційності та цілісності даних.

Резервування даних дозволяє забезпечити стійкість інформаційних систем шляхом мінімізації ризиків втрати даних через збої в обладнанні, програмні помилки чи атаки. Впровадження методів резервування сприяє оптимізації процесів збереження даних та забезпечує їхню доступність навіть у випадку критичних інцидентів. Моніторинг стану даних і систем безпеки є важливою складовою ефективного захисту інформації. Використання автоматизованого аналізу загроз, виявлення аномальної активності та оперативного реагування дозволяє своєчасно виявляти потенційні ризики та запобігати інцидентам безпеки.

Таким чином, дослідження та розвиток систем шифрування, резервування та моніторингу даних є актуальним напрямом, що має значний вплив на інформаційну безпеку та сприяє підвищенню загальної кіберстійкості інформаційних систем.

Метою статті є критеріальний аналіз систем шифрування та резервування на підприємствах з метою підвищення їх кіберстійкості.

Об'єктом дослідження є розробка системи шифрування та резервування даних підприємства.

Предмет дослідження – система шифрування та резервування даних.

Аналіз попередніх досліджень. Дослідженню систем шифрування та резервування даних, визначенню їхніх ключових параметрів та основних характеристик присвячено роботи вітчизняних науковців: С. Г. Семенов, А. О. Подорожняк, Ю. А. Тарнавський та ін.

Виклад основного матеріалу. Системи шифрування оцінюються за кількома ключовими параметрами, які визначають їхню ефективність і безпеку. Основним є тип шифрування: симетричне (один ключ) або асиметричне (пара ключів), де асиметричне забезпечує вищий рівень безпеки. Алгоритм шифрування, наприклад AES, RSA або ECC, впливає на швидкість і надійність системи. Рівень захисту залежить від стійкості алгоритму до криптоаналізу та довжини ключа, наприклад AES-256 є надійнішим за AES-128.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Управління ключами може бути централізованим або децентралізованим, що також впливає на стійкість системи [5, с. 148–191]. Продуктивність визначається швидкістю шифрування, ефективністю ресурсів та можливістю роботи в реальному часі. Важливими є сфера застосування (захист мереж, файлів, баз даних) та стійкість до атак (brute-force, «людина посередині», побічні канали). Інтеграція з іншими технологіями важлива для впровадження в сучасні системи та хмарні сервіси [5, с. 335–341]. Всі ці параметри впливають на вибір криптографічної системи для забезпечення конфіденційності та доступності даних.

Критеріальний аналіз проводиться в порівнянні із існуючими системами шифрування «ZeroTier» та «OnionShare».

«ZeroTier» – система шифрування та створення віртуальних приватних мереж, яка використовує симетричне шифрування AES-256 з Poly1305 для автентифікації. Вона застосовує децентралізовану модель управління ключами для зменшення ризиків компрометації та автоматичної автентифікації вузлів. Система поєднує принципи однорангових з'єднань і маршрутизації на основі віртуальних мереж, що знижує затримки та підвищує продуктивність порівняно з традиційними VPN [1]. «ZeroTier» дозволяє встановлювати прямі з'єднання між пристроями навіть за NAT чи брандмауером і динамічно створювати зашифровані тунелі без проміжних серверів. Вона підтримує різні платформи, включаючи Windows, Linux, macOS, iOS та Android, що забезпечує легку інтеграцію в сучасні IT-інфраструктури.

У табл. 1 показані ключові параметри системи шифрування «ZeroTier».

Таблиця 1

Критеріалний аналіз системи «ZeroTier»

№ п/п	Параметр	Опис
1	Тип шифрування	Симетричне
2	Алгоритм шифрування	AES-256, Poly1305
3	Рівень захисту	Високий рівень (використання наскрізного шифруванню)
4	Методи управління ключами	Автоматична генерація та розподіл ключів, децентралізована модель управління
5	Продуктивність	Висока
6	Сфера застосування	Корпоративний VPN, IoT, віддалений доступ
7	Стійкість до атак	Захищена від атак типу MITM, brute-force, DPI
8	Інтеграція та сумісність	Підтримка Windows, Linux, macOS, iOS, Android

Джерело: розроблено автором

«OnionShare» – система шифрування та обміну файлами через анонімну мережу Tor для захисту даних від несанкціонованого доступу. Вона використовує децентралізоване передавання без залучення сторонніх серверів, створюючи тимчасову Onion-адресу, доступну лише авторизованим користувачам [2]. Для безпеки доступ можливий тільки через браузер Tor, що запобігає перехопленню з'єднання. Шифрування файлів забезпечується алгоритмами AES-256 та RSA. Після завершення сеансу адреса стає недійсною, унеможливлюючи повторний доступ. «OnionShare» не зберігає дані на централізованих серверах, що знижує ризик атак на інфраструктуру. Система широко використовується для анонімного обміну файлами, публікацій і розгортання тимчасових веб-сайтів, особливо журналістами та правозахисниками.

У табл. 2 показані ключові параметри системи шифрування «OnionShare».

Ефективність резервування залежить від надійності, безпеки та швидкості відновлення. Важливі параметри: тип резервування (повне, диференційне, інкрементальне), методи збереження (локальне, віддалене, хмарне) та частота оновлення. Шифрування гарантує

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

безпеку даних навіть у разі компрометації сховища. Відновлення здійснюється через автоматичні механізми, тестові сценарії та реплікацію. Інтеграція з іншими системами оптимізує процеси й покращує управління ресурсами [6, с. 16–55].

Таблиця 2

Критеріалний аналіз системи «OnionShare»

№ п/п	Параметр	Опис
1	Тип шифрування	Симетричне та асиметричне
2	Алгоритм шифрування	AES-256, RSA
3	Рівень захисту	Високий рівень (Tor та унікальні Onion-адреси)
4	Методи управління ключами	Тимчасові ключі та Onion-адреси
5	Продуктивність	Залежить від швидкості мережі Tor
6	Сфера застосування	Безпечний обмін файлами, анонімна публікація
7	Стійкість до атак	Висока стійкість (використання мережі Tor)
8	Інтеграція та сумісність	Необхідний Tor-браузер

Джерело: розроблено автором

Критеріальний аналіз проводиться в порівнянні із існуючими системами резервування даних «Commvault» та «Veeam Backup & Replication».

Система резервування даних «Commvault» поєднує резервне копіювання, відновлення та управління даними з централізованим управлінням, що мінімізує ризики втрати інформації та скорочує час відновлення. Інтелектуальні алгоритми використовують дедуплікацію, компресію та інкрементальне копіювання для оптимізації процесу та зменшення навантаження на сховища. «Commvault» підтримує локальні, хмарні та гібридні інфраструктури, інтегрується з платформами віртуалізації, базами даних та корпоративними додатками. Автоматизовані механізми моніторингу допомагають виявляти загрози та реагувати на інциденти. Безпека забезпечується багаторівневим шифруванням, контролем доступу та аутентифікацією, а швидке відновлення мінімізує час простою [4].

У табл.3 показані ключові параметри системи резервування даних «Commvault».

Таблиця 3

Критеріалний аналіз системи «Commvault»

№ п/п	Параметр	Опис
1	Тип копіювання	Повне, інкрементальне, диференційне, дедуплiковане
2	Методи збереження	Локальні сервери, хмарні сховища, гібридні середовища
3	Частота оновлення	Гнучке налаштування
4	Рівень шифрування	AES-256, підтримка апаратного шифрування
5	Механізми відновлення	Автоматизоване відновлення, тестові сценарії, реплікація
6	Інтеграція	Бази даних, корпоративні додатки, віртуалізація
7	Моніторинг та безпека	Механізми аналітики, контроль подій

Джерело: розроблено автором

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Система «Veeam Backup & Replication» забезпечує безперервність бізнес-процесів, поєднуючи резервне копіювання, реплікацію та швидке відновлення для зменшення ризиків простою. Вона підтримує повне, інкрементальне та дедупліковане копіювання, оптимізуючи ресурси. Підтримка віртуалізованих середовищ робить систему ідеальним вибором для компаній із віртуальними машинами. Технології дедуплікації та компресії прискорюють процес резервування. Багаторівневе резервування включає локальні сховища, віддалені дата-центри та хмарні платформи, підвищуючи стійкість до атак. Механізм швидкого відновлення мінімізує час простою, а реплікація створює точні копії в реальному часі. Інструменти моніторингу та звітності допомагають оцінити стан резервних копій, а безпека забезпечується шифруванням та контролем доступу [5].

У табл. 4 показані ключові параметри системи резервування даних «Veeam Backup & Replication».

Таблиця 4

Критеріалний аналіз системи «Veeam Backup & Replication»

№ п/п	Параметр	Опис
1	Тип копіювання	Повне, інкрементальне, дедупліковане
2	Методи збереження	Локальні сховища, віддалені сховища, хмарні платформи
3	Частота оновлення	Копіювання з можливістю миттєвого створення знімків
4	Рівень шифрування	AES-256, контроль доступу
5	Механізми відновлення	Відновлення віртуальних машин, реплікація
6	Інтеграція	Підтримка VMware, Hyper-V, мультихмарних платформ
7	Моніторинг та безпека	Засоби аналітики, тестування резервних копій, звітність

Джерело: розроблено автором

Сучасні системи шифрування та резервування даних забезпечують високий рівень безпеки, але вирішують лише окремі завдання, без комплексного підходу до захисту інформації. Шифрування гарантує конфіденційність під час передавання та зберігання, використовуючи криптографічні алгоритми, проте не запобігає втраті даних через технічні збої чи кібератаки, оскільки не містить вбудованих механізмів резервування. Системи резервування, своєю чергою, зосереджені на збереженні даних і швидкому відновленні, але не охоплюють усіх аспектів безпечного обміну та захисту в режимі реального часу. Це створює потребу в інтегрованому рішенні, що поєднує шифрування та резервування в єдину систему.

Запропоновано комплексну систему «Enbamo», яка об’єднує шифрування, резервне копіювання та моніторинг пристроїв і даних. Для забезпечення конфіденційності та цілісності інформації використовується наскрізне шифрування з AES-256 для шифрування та RSA або ECC для обміну ключами. Захист від атак «людина посередині» здійснюється через автентифікацію кінцевих точок. Дані передаються через захищені тунелі. Резервування включає локальні та віддалені копії з шифруванням і диференційним/інкрементальним копіюванням для зменшення обсягу даних. Моніторинг охоплює контроль за обладнанням та трафіком для виявлення загроз, з автоматичним корелюванням подій для швидкого реагування.

У табл. 5 показані ключові параметри комплексної системи «Enbamo».

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Таблиця 5

Критеріальний аналіз системи «Enbamo»

№ п/п	Параметр	Опис
1	Тип шифрування	Наскрізне шифрування
2	Алгоритм шифрування	AES-256, RSA/ECC, шифрування під час зберігання та передавання
3	Рівень захисту	Високий (шифрування під час передавання та зберігання)
4	Методи управління ключами	Децентралізоване управління ключами
5	Продуктивність	Як з малими та із великими обсягами даних
6	Сфера застосування	Корпоративні мережі, хмарні середовища, урядові організації
7	Стійкість до атак	Висока (MITM-атаки, несанкціонований доступ)
8	Інтеграція та сумісність	Висока (інтеграції платформами та сервісами)
9	Тип копіювання	Локальне та віддалене резервування
10	Методи збереження	Місцеві сервери, хмарні платформи, резервns носі]
11	Частота оновлення	Налаштовується (реальний час, щоденно, щотижня)
12	Механізми відновлення	Автоматичне та ручне, різні рівні резервування
13	Моніторинг та безпека	Аналіз активності, виявлення аномалій та загроз в мережі, моніторинг процесів резервування

Джерело: розроблено автором

Висновки. Інтеграція систем шифрування та резервування в інформаційних системах дозволяє ефективно захищати дані, забезпечуючи їх конфіденційність, цілісність та доступність у реальному часі. Системи шифрування забезпечують конфіденційність та цілісність, а резервування гарантує доступність даних при збої чи атаках. Моніторинг виявляє загрози в реальному часі. Інтеграція систем шифрування, резервування та моніторингу дозволяє підвищити кіберстійкість, оптимізувати шифрування для зниження навантаження на ресурси, вдосконалити методи резервування та використовувати штучний інтелект для покращення виявлення загроз.

Список використаних джерел

1. Архітектура «ZeroTier» // Режим доступу: https://docs.zerotier.com/zerotier
2. Матеріали «OpionShare» // Режим доступу: https://docs.onionshare.org/2.6.3/en/
3. Архітектура «Commvault» // Режим доступу: https://documentation.commvault.com/2024/essential/architecture.html
4. Матеріали «Veeam Backup & Replication» // Режим доступу: https://helpcenter.veeam.com/docs/backup/vsphere/overview.html?ver=120
5. Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2020. – 816 p.
6. McGarvey J. S. The Art of Data Recovery: A Data Recovery Expert’s Guide to Success. – Wiley, 2018. – 342 p.

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВА Ю. Є.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

SYSLOG ЯК ЕФЕКТИВНЕ РІШЕННЯ ДЛЯ МОНІТОРИНГУ ТА УПРАВЛІННЯ ЖУРНАЛАМИ ПОДІЙ У .NET ЗАСТОСУНКАХ

ПАВЛЕНКО С. С., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто проблему ефективного моніторингу та управління журналами подій у .NET-застосунках, зокрема використання Syslog як централізованого рішення для збору, обробки та зберігання логів. Проаналізовано ключові виклики, пов'язані з використанням Windows Event Log, серед яких обмеження у взаємодії з мережевими пристроями та відсутність вбудованих механізмів централізації логування. Запропонована архітектурна модель передбачає інтеграцію Syslog для уніфікації логів із різних джерел, що підвищує ефективність виявлення загроз та забезпечує безпечне зберігання даних. Зроблено висновок, що використання Syslog у системах моніторингу подій дозволяє покращити управління журналами та сприяє підвищенню рівня кібербезпеки організації.

The article addresses the issue of effective monitoring and log management in .NET applications, specifically the use of Syslog as a centralized solution for log collection, processing, and storage. It analyzes the key challenges associated with using Windows Event Log, including limitations in interacting with network devices and the lack of built-in logging centralization mechanisms. The proposed architectural model suggests integrating Syslog to standardize logs from various sources, which enhances threat detection efficiency and ensures secure data storage. It concludes that using Syslog in event monitoring systems improves log management and contributes to enhancing the organization's cybersecurity level.

Актуальність. У сучасних умовах кіберзагроз та постійного зростання кількості мережевих атак ефективне управління журналами подій відіграє ключову роль у забезпеченні безпеки інформаційних систем. Журнали подій містять важливі дані про активність користувачів, роботу програмного забезпечення, а також можливі загрози та інциденти безпеки. Особливо критичним це питання є для .NET-застосунків, які використовуються в корпоративних інформаційних системах, фінансових установах та інших сферах із високими вимогами до безпеки та надійності. Попри широке використання Windows Event Log у .NET-екосистемі, цей механізм має низку обмежень, зокрема відсутність централізованого збору логів із різних джерел, складність масштабування та обмежені можливості аналізу подій у розподілених системах. У зв'язку з цим постає необхідність застосування гнучких та надійних інструментів для моніторингу та керування логами, серед яких Syslog є одним із найефективніших рішень.

Syslog забезпечує централізоване логування подій, підтримку різних типів пристроїв та операційних систем, а також високу гнучкість у налаштуванні та аналізі даних. Інтеграція Syslog у .NET-застосунки дозволяє спростити адміністрування логів, підвищити рівень інформаційної безпеки, а також забезпечити можливість швидкого виявлення та реагування на інциденти. Таким чином, дослідження та розробка рішень для ефективної інтеграції Syslog у системи моніторингу та управління журналами подій .NET-застосунків є актуальним напрямом, що сприяє підвищенню рівня безпеки та стійкості сучасних програмних комплексів.

Метою статті є дослідження можливостей та переваг використання Syslog як ефективного інструменту для централізованого моніторингу та управління журналами подій у .NET-застосунках шляхом аналізу його здатності забезпечувати безпечне зберігання, кореляцію та обробку логів із різних джерел, усунення обмежень Windows Event Log, а також

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

підвищення рівня інформаційної безпеки через впровадження механізмів швидкого виявлення та реагування на інциденти у розподілених інформаційних системах.

Об'єктом дослідження є процес централізованого моніторингу, збору, зберігання та аналізу журналів подій у .NET-застосунках з використанням Syslog як ефективного рішення для підвищення рівня кібербезпеки, забезпечення цілісності та доступності логів, а також оптимізації управління подіями в інформаційних системах.

Предмет дослідження – підходи, методи та технології використання Syslog для ефективного моніторингу, управління та аналізу журналів подій у .NET-застосунках, з урахуванням вимог до безпеки, масштабованості та інтеграції з іншими системами логування.

Аналіз попередніх досліджень. Syslog є ключовою технологією централізованого збору та обробки журналів подій у розподілених інформаційних системах. P. Sahoo та W. Greenfield розглянули переваги використання Syslog для стандартизації логів у різних операційних системах, таких як Windows та UNIX, що спрощує процеси моніторингу та управління безпекою [1]. Автори зазначають, що Syslog дозволяє централізовано зберігати журнали подій, що сприяє швидкому виявленню загроз і покращенню кібербезпеки.

W. Greenfield та P. Sahoo підкреслюють важливість інтеграції Syslog у .NET-застосунки, що забезпечує покращену синхронізацію подій та підвищує ефективність реагування на інциденти безпеки [2]. Автори доводять, що централізоване зберігання логів не лише спрощує управління подіями, а й забезпечує їхню цілісність та можливість швидкого аналізу у випадку атак або збоїв у системі.

Питання безпеки обміну логами між різними системами та організаціями досліджено A. Slagell і W. Yurcik, які пропонують методології анонімізації журналів подій для збереження конфіденційності без втрати важливих даних, необхідних для аналізу кіберзагроз [3], що є особливо актуальним у великих корпоративних мережах, де обмін логами між різними підрозділами може створювати додаткові ризики витоку інформації.

У свою чергу A. Yavuz і P. Ning дослідили механізми забезпечення безпеки аудиторських журналів у розподілених системах та запропонували алгоритми криптографічного захисту логів [4]. Вони наголошують на необхідності впровадження механізмів цілісності та автентифікації журналів подій, що особливо важливо в умовах віддаленого адміністрування та моніторингу.

І. Петров зосереджується на питаннях безпеки журналів подій у державних інформаційних системах [5]. Автор аналізує потенційні загрози, пов'язані з централізованим збиранням та зберіганням логів, зокрема ризики несанкціонованого доступу та модифікації даних. У роботі запропоновано підхід до впровадження політик контролю доступу на основі атрибутивної моделі, що дозволяє забезпечити гнучке керування рівнями привілеїв для адміністраторів і користувачів системи.

Таким чином, аналіз наукових джерел демонструє, що впровадження Syslog у корпоративні системи значно покращує процеси збору та аналізу логів, сприяє проактивному виявленню загроз та забезпечує кращу інтеграцію засобів кіберзахисту. Разом із методами анонімізації, криптографічного захисту логів та сучасними підходами до контролю доступу це дозволяє створювати ефективні рішення для моніторингу безпеки інформаційних систем підприємств.

Виклад основного матеріалу. Журнали подій є надзвичайно важливими джерелами інформації для кібербезпеки, оскільки містять дані про потенційні атаки, реєструють щоденні дії користувачів системи та слугують доказовою базою для розслідування зловмисної активності, що робить їх незамінним інструментом у процесі моніторингу безпеки організаційних мереж та інформаційних систем. У сучасному цифровому середовищі, де кібератаки стають дедалі складнішими, ведення та захист журналів подій набуває критично важливого значення, оскільки неправильне або недостатньо ефективне управління логами

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

може спричинити значні вразливості в IT-інфраструктурі, ускладнюючи процес виявлення загроз та реагування на інциденти.

Зокрема, журнали подій у середовищі .NET-застосунків потребують ефективних механізмів збору, обробки та аналізу, оскільки вбудована система Windows Event Log має ряд суттєвих обмежень, включно з відсутністю можливості централізованого збору логів з різних джерел, зокрема з мережевих пристроїв, таких як маршрутизатори та комутатори, що значно ускладнює єдину систему моніторингу. Водночас Syslog пропонує ефективне рішення для централізації процесу логування, оскільки забезпечує єдину платформу для збору, передачі, зберігання та аналізу логів з усіх мережевих компонентів та програмного забезпечення, що дозволяє покращити точність виявлення аномалій, спростити аудит подій та підвищити рівень безпеки.

Завдяки інтеграції Syslog у систему моніторингу .NET-застосунків можна досягти суттєвих переваг, включаючи централізоване управління логами, покращену кореляцію подій та автоматизоване сповіщення про загрози, що у поєднанні з сучасними технологіями аналізу даних сприяє швидкому виявленню атак та формуванню ефективних стратегій реагування. Окрім того, Syslog забезпечує захищене зберігання логів, що унеможливлює їх несанкціоновану модифікацію або знищення зловмисниками, а також спрощує процес судової експертизи цифрових доказів, необхідних для розслідування кіберзлочинів.

Використання Syslog у .NET-застосунках дозволяє долати такі виклики, як велика кількість джерел логів, відсутність єдиних стандартів форматів логів та проблеми з часовими мітками, оскільки система здатна уніфікувати збереження подій, забезпечувати їх коректну часову синхронізацію та інтегрувати різні формати даних у спільну базу, що значно покращує процеси моніторингу та аналізу інформації. Така централізація дозволяє знижувати витрати часу на ручне оброблення даних та автоматизувати процеси виявлення порушень або аномалій у мережі. Крім того, Syslog дозволяє застосовувати фільтрацію та сортування логів за різними критеріями, що значно полегшує відслідковування інцидентів безпеки і допомагає швидко реагувати на критичні події [2]. Завдяки цьому підвищується ефективність виявлення загроз, зменшується ймовірність помилок через людський фактор, а також спрощується процес дотримання стандартів безпеки, таких як PCI DSS або GDPR.

Використання Syslog у .NET також дозволяє забезпечити належний рівень захисту даних, оскільки всі логи можна зберігати в зашифрованому вигляді та надійно захищати від несанкціонованого доступу. Крім того, система Syslog може бути легко масштабована відповідно до зростання мережі та вимог до зберігання даних, що робить її універсальним рішенням для будь-яких організацій, незалежно від їх розміру та складності інфраструктури. Також важливою перевагою є інтеграція з іншими інструментами для моніторингу та управління, що дозволяє створювати комплексну систему безпеки з можливістю автоматичного реагування на загрози. Зрештою, це дозволяє створити потужну платформу для збору, збереження та аналізу логів, що є необхідною складовою для забезпечення кібербезпеки на сучасних підприємствах.

У сучасних інформаційних системах моніторинг та управління журналами подій є надзвичайно важливими для забезпечення безпеки та стабільної роботи організацій. Операційні системи Windows, а також різноманітні застосунки, створюють аудиторські дані, які записуються в Windows Event Log у бінарному форматі. Однак, існує кілька суттєвих обмежень цього підходу, що ускладнюють ефективне управління журналами подій у розподілених системах, зокрема в .NET-застосунках.

Найбільша проблема полягає в тому, що Windows Event Log не здатний обробляти повідомлення, які надходять від мережевих пристроїв, таких як маршрутизатори, комутатори або міжмережеві екрани, а також не є сумісним з іншими системами логування операційних систем. Крім того, стандартний інтерфейс перегляду журналів Windows Event Viewer має обмежений функціонал, який є недостатнім для моніторингу великих або середніх мереж

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

[1, 3]. Тому для централізації збору та аналізу логів у Windows-системах не існує вбудованих інструментів, що значно ускладнює процес управління логами в реальному часі.

Відсутність єдиного стандарту для логування з різних джерел ще більше ускладнює цей процес, оскільки кожен журнал подій зберігається локально на окремому вузлі системи, що робить централізовану обробку даних не тільки складною, але й менш ефективною. У зв'язку з цим виникає необхідність у більш універсальних і гнучких рішеннях для управління журналами подій. Одним із таких рішень є використання Syslog, який є міжнародно визнаним стандартом для логування подій і забезпечує набагато більшу гнучкість та ефективність у централізованому зберіганні та обробці логів.

Використання Syslog дозволяє централізувати зберігання логів із різних джерел, таких як маршрутизатори, сервери та інші мережеві пристрої, що значно полегшує їх подальший аналіз [2]. Крім того, цей стандарт дозволяє стандартизувати формат повідомлень, що спрощує інтеграцію з іншими системами та програмним забезпеченням для моніторингу. Syslog також підтримує різні рівні пріоритетів, що дозволяє розподіляти навантаження на систему обробки даних та фокусуватися на найбільш критичних подіях. У зв'язку з цим, за допомогою Syslog можна ефективно здійснювати централізоване зберігання даних на віддалених серверах, що забезпечує більшу надійність і захист від потенційних атак або збоїв на локальних вузлах.

Syslog – це протокол, що забезпечує єдину структуру для генерації, зберігання та передачі повідомлень про події. Багато джерел логів використовують Syslog як свій основний формат або мають можливість перетворювати свої дані у цей формат, що дозволяє забезпечити єдиний підхід до збору та обробки логів у розподілених системах. Протокол Syslog визначає три основні компоненти для кожного повідомлення: перший – це ідентифікатор об'єкта та рівень серйозності події, другий – часову мітку та ідентифікатор джерела повідомлення (IP-адреса чи хост), третій – власне текстове повідомлення, яке містить опис події.

Така структура забезпечує гнучкість для генераторів логів, адже вони можуть записувати будь-яку важливу інформацію в текстовій частині повідомлення, але також ускладнює автоматичний аналіз цих логів, оскільки зміст не є стандартизованим. Syslog дозволяє централізувати збір логів із різних джерел, що значно спрощує процес моніторингу і управління безпекою у реальному часі. Протокол використовує систему пріоритетів для обробки повідомлень, що дає змогу ефективно визначати, які події потребують негайної уваги. Наприклад, повідомлення високого рівня можуть бути негайно переслані на централізований сервер для детального аналізу, тоді як менш критичні події зберігаються без подальшої обробки. Окрім того, структура Syslog дозволяє значно спростити аналіз подій, об'єднуючи схожі типи повідомлень або надаючи їм однакові коди, що полегшує автоматизовану обробку та виявлення загроз.

Незважаючи на те, що Syslog має певні обмеження, такі як відсутність чітко визначених стандартних полів для автоматичного аналізу, його гнучкість та широке поширення в різних системах робить його ідеальним рішенням для централізованого збору та управління журналами подій у .NET-застосунках. Це дозволяє не лише знижувати складність процесу моніторингу та управління, але й значно підвищує рівень безпеки організації, забезпечуючи швидке виявлення та реагування на потенційні інциденти, що мають важливе значення для збереження цілісності та конфіденційності даних.

Завдяки централізації збору журналів Syslog дозволяє інтегрувати різноманітні джерела даних у єдину систему, що спрощує доступ до необхідної інформації. Це також зменшує ризик втрати або модифікації критичних даних, оскільки журнали зберігаються в безпечному місці, доступному для ретельного аналізу. Окрім того, Syslog дозволяє легко масштабувати систему, додаючи нові джерела даних або пристрої до існуючої інфраструктури, що забезпечує її адаптацію до змін у мережі організації. Завдяки цьому, організація може ефективно управляти зростаючими обсягами даних, забезпечуючи безперервну роботу та максимальний рівень безпеки на всіх етапах їх обробки та зберігання.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

У поєднанні з використанням криптографічних методів для захисту даних, Syslog забезпечує високий рівень конфіденційності та цілісності зібраної інформації. Це рішення є особливо важливим для великих організацій з розподіленою інфраструктурою, де необхідний централізований моніторинг для забезпечення належного рівня безпеки. Завдяки таким можливостям Syslog також дозволяє забезпечити відповідність вимогам щодо аудиту та звітності, що особливо важливо для підприємств, які повинні відповідати законодавчим та нормативним стандартам. У разі інцидентів безпеки Syslog сприяє швидкому реагуванню на загрози, забезпечуючи централізовану точку для аналізу подій і прийняття відповідних заходів.

Запропонована архітектурна модель, що представлена на рис. 1, використовує централізоване зберігання та інтерпретацію журналів, що генеруються системами та мережами організації, а також забезпечує захист журналів від можливих атак.

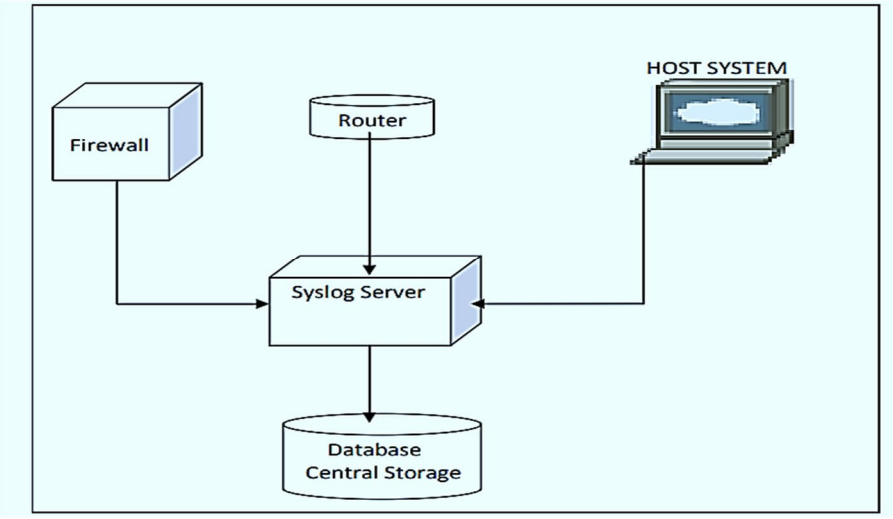


Рис. 1. Архітектурна модель для централізованого моніторингу та управління журналами подій

Джерело: розроблено автором в програмному середовищі Packet Tracer

Централізація інтерпретації журналів дозволяє захищати критичні аудиторські дані від атакуючих шляхом їх негайного видалення з хоста, на якому вони генеруються, що значно знижує ризик маніпуляцій з журналами. Перший рівень архітектури складається з хостів, що генерують дані журналів, серед яких можуть бути маршрутизатори, комутатори та локальні сервери. Сервер Syslog приймає файли журналів від цих хостів та обробляє їх відповідно до конфігурації Winsyslog, який реалізовано як центральний сервер.

Після цього сервер записує отримані дані журналів у базу даних, враховуючи правила, зазначені в конфігурації Winsyslog. Після обробки сервер Syslog передає повідомлення у вигляді логів, обробляє їх через встановлену базу правил і зберігає їх у базі даних [1]. Тому усі файли журналів потім зберігаються окремо на сервері бази даних (Централізоване зберігання) протягом визначеного періоду часу, що дозволяє зберігати їх цілісність навіть у випадку збоїв системи. Кожен хост, що генерує журнали, використовує єдиний стандартний формат журналу, що спрощує процес їх передачі в централізоване сховище.

Крім того, всі операційні системи на базі UNIX реалізують протокол Syslog, що забезпечує можливість централізованого збирання повідомлень журналів з мережевих пристроїв і робочих станцій, а в операційних системах Windows можна налаштувати протокол Syslog для роботи з аналогічною функціональністю. Winsyslog конфігурується для запису журналів у базу даних і передачі зібраних даних на сервер [2–3]. Це дозволяє забезпечити

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

зручну та ефективну централізацію зберігання журналів подій, що суттєво спрощує процеси моніторингу та управління ними в організації.

Завдяки підтримці протоколу Syslog, різні джерела логів можуть об’єднуватися в єдину систему, забезпечуючи більш швидке виявлення потенційних загроз. Важливо, що централізоване зберігання даних дозволяє підвищити безпеку системи, зберігаючи критичні дані в захищеному середовищі. Таким чином, Syslog сприяє не тільки зручному управлінню логами, а й створює міцну основу для ефективного аналізу подій у реальному часі. Це дозволяє оперативно виявляти аномалії та потенційні загрози без необхідності вручну перевіряти великі обсяги інформації.

Централізоване зберігання логів також дає змогу зменшити кількість помилок, що можуть виникати при розподіленому зберіганні, і забезпечує більшу надійність даних. Використання Syslog дає можливість зберігати журнали подій в захищеному місці, що важливо для подальшого їх аналізу в разі необхідності розслідування інцидентів безпеки [4]. Таке рішення також дозволяє швидко адаптувати систему до змін, зокрема при розширенні мережі чи додаванні нових пристроїв. Підвищення ефективності виявлення інцидентів стає можливим завдяки інтеграції різних джерел даних, що дозволяє отримати більш точну картину про стан мережі та її безпеку. Крім того, централізація збору даних на базі Syslog знижує навантаження на окремі пристрої та полегшує процес обробки інформації. В результаті організація отримує більш ефективну систему моніторингу та контролю за безпекою в реальному часі.

У дослідженні також реалізовано сервер Syslog для збору та зберігання журналів у мережі, і на рис. 2 продемонстровано, як зберігаються дані журналів в базі даних. Сервер Syslog виконує роль центрального хабу для збору та зберігання журналів подій з усіх пристроїв мережі, що дозволяє зберігати інформацію в єдиному, зручному для аналізу форматі. Конфігурація Winsyslog забезпечує налаштування правил для збереження даних у базі даних, що дозволяє ефективно організувати процес централізованого зберігання.

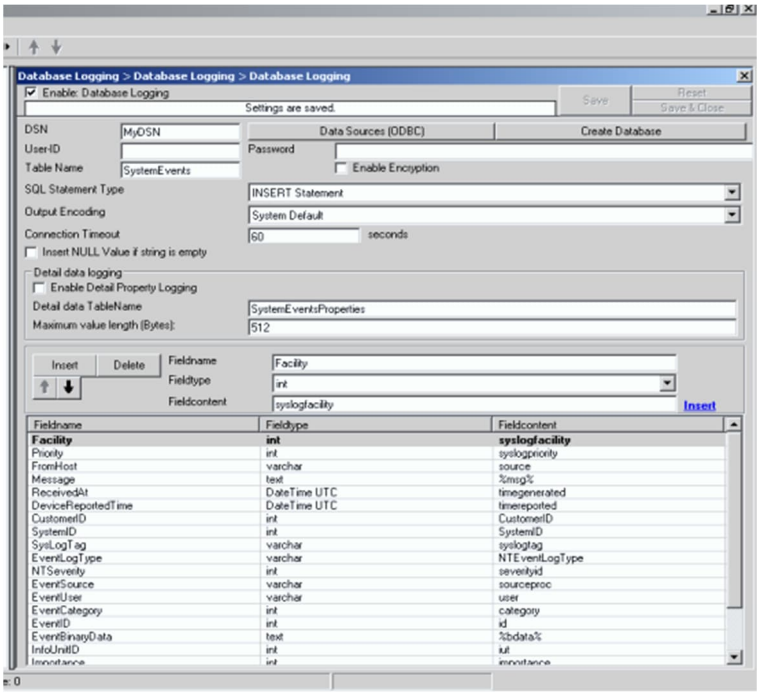


Рис. 2. Конфігурація Winsyslog для налаштування правил збереження журналів у базі даних

Джерело: розроблено автором

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Завдяки такому підходу можна уникнути втрати критично важливої інформації, навіть у разі відмови окремих компонентів системи. Крім того, ця конфігурація дозволяє швидко адаптувати систему до змін у мережі та забезпечує масштабованість для роботи з великими обсягами даних. В кінцевому підсумку, ефективна реалізація серверів Syslog і налаштування бази даних дозволяють знизити ризики для організаційної безпеки і підвищити загальний рівень захисту даних [5]. Це дозволяє забезпечити стабільність системи навіть у разі непередбачених ситуацій або технічних збоїв, що є критичним для безперервної роботи підприємства. Завдяки гнучкості конфігурації, Syslog можна налаштувати для збору різноманітних типів подій, що полегшує інтеграцію з іншими системами моніторингу та аналітики.

Запропонована модель має низку переваг, серед яких можливість зберігати події з різних джерел журналів на центральному сховищі протягом визначеного часу, навіть у випадку збоїв системи відправлення або випадкового видалення журналів. Також завдяки централізованому доступу до всіх подій можна отримати зручний і централізований інтерфейс для перегляду всіх зібраних даних. Центральне сховище забезпечує високий рівень безпеки та криміналістичної цілісності даних, де значно ускладнюється спроба зловмисника змінити або знищити журнали. Крім того, централізоване логування з використанням протоколу Syslog дозволяє здійснювати збір даних з майже всіх пристроїв, що генерують журнали в мережі, що значно спрощує процес управління цими даними.

Віддалений доступ до журналів на центральному сервері забезпечує можливість їх аналізу в будь-який час, що особливо важливо для великих і розподілених організацій. Крім того, централізоване зберігання журналів спрощує виконання аудиту та аналізу безпеки, що є критичним аспектом для відповідності різним стандартам і нормативним вимогам. У разі необхідності, зібрані дані можуть бути швидко відновлені, що допомагає знизити час на відновлення після інцидентів. Це робить систему не тільки більш ефективною, але й гнучкою, здатною адаптуватися до змін у розмірі і складності мережі організації.

Висновки. Оскільки дані журналів є надзвичайно важливими для сучасних інформаційних систем, вони повинні зберігатися в безпечному місці. Дані аудиту журналів надають інформацію про поточний та попередній стан системи і вважаються однією з найважливіших складових кібербезпеки. Управління журналами є необхідним для забезпечення того, щоб файли журналів зберігалися в належному вигляді протягом визначеного періоду часу, що дає можливість проводити подальші розслідування. Запропонована архітектурна модель є дуже ефективною, оскільки централізує зберігання даних журналів з різних джерел в мережі організації. Ця архітектура може бути використана для збору та централізації повідомлень з усієї мережі, включаючи хости на базі Windows, UNIX, принтери та маршрутизатори тощо. Використання Syslog робить управління журналами значно простішим та ефективнішим, надаючи просту інфраструктуру для генерації та зберігання журналів. Розподілений характер журналу подій Windows легко долається в запропонованому рішенні. Ця модель також може бути легко адаптована для інших мереж у майбутньому.

Список використаних джерел

1. Sahoo, P. K., & Greenfield, W. (2021). Syslog for centralized event log management in distributed systems. *International Journal of Computer Science and Information Security, 19*(3), 134–140.

2. Greenfield, W., & Sahoo, P. K. (2020). Integration of Syslog for enhanced security and time synchronization in .NET applications. *Journal of Cybersecurity and Network Management, 7*(2), 45–53.

3. Slagell, A., & Yurcik, W. (2005, September). Sharing computer network logs for security and privacy: A motivation for new methodologies of anonymization. In *Proceedings of the IEEE 1st*

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

International Conference on Security and Privacy for Emerging Areas in Communication Networks (SECCMW 2015) (pp. 80–89). IEEE Press.

4. Yavuz, A. A., & Ning, P. (2017). BAF: An efficient publicly verifiable secure audit logging scheme for distributed systems. In *Annual IEEE Computer Security Applications Conference* (Issue ii, pp. 219–228). IEEE Press.

5. Петров, І. (2022). Захист журналів подій у державних інформаційних системах: методи та підходи. *Вісник Київського національного університету імені Тараса Шевченка. Серія: Комп'ютерні науки, (1)(56)*, 85–94.

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

РОЛЬ ЗАСТОСУНКУ «ДІЯ» У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

ПИШНИЙ І. В., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті розглянуто основні засади функціонування та розвитку застосунку «ДІЯ» як ключового елементу цифрової трансформації України. Зазначено переваги використання цифрових документів та електронних послуг для забезпечення національної безпеки та кібербезпеки країни. Розглянуто перспективи розширення функціоналу додатку та його інтеграції з іншими державними інформаційними системами.

The article reveals the basic principles of functioning and development of the "DIIA" application as a key element of digital transformation of Ukraine. The advantages of using digital documents and electronic services to ensure national security and cybersecurity of the country are indicated. Prospects for expanding the functionality of the application and its integration with other state information systems are considered.

Актуальність. Цифровий суверенітет у сучасному світі стає не менш важливим виміром національної безпеки, ніж традиційні військові та економічні аспекти. Інтеграція застосунку «ДІЯ» у системи критичного державного управління створює новий рівень цифрової стійкості, що особливо актуально в умовах цілеспрямованих атак на державні цифрові екосистеми. Безпрецедентна ситуація, коли Україна під час війни не лише зберігає, але й активно розвиває цифрові інструменти державного управління, формує унікальний кейс для світової практики забезпечення національної безпеки. Феномен «ДІЯ» заслуговує на глибоке вивчення саме в контексті його мультифункціональності – від захисту персональних даних громадян до забезпечення безперервності державних функцій у кризових сценаріях та швидкого реагування на гуманітарні виклики воєнного часу. Подальший розвиток застосунку в напрямку посилення кіберзахисту та розширення функціоналу, пов'язаного з національною безпекою, може стати каталізатором формування нової парадигми цифрової стійкості держави.

Цифрова трансформація державних послуг є одним із пріоритетних напрямків розвитку сучасних держав. В Україні цей процес набув особливого значення з початком повномасштабного вторгнення, коли виникла гостра потреба забезпечити громадянам доступ до державних послуг та документів у будь-якому куточку країни та навіть за її межами [1].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Застосунок «ДІЯ» став не просто зручним інструментом для українців, а й важливим елементом національної безпеки, забезпечуючи стійкість державних інституцій та безперервність надання державних послуг в умовах кризи.

Особливу увагу слід приділити ролі застосунку «ДІЯ» у забезпеченні інформаційної стійкості держави під час російської агресії. Завдяки централізації цифрових послуг та документів у єдиній захищеній екосистемі вдалося значно підвищити рівень захисту персональних даних громадян від можливих ворожих кібератак. Крім того, впровадження застосунку «ДІЯ» суттєво знизило бюрократичне навантаження на державні органи, що дозволило оптимізувати їхню роботу та перенаправити ресурси на більш пріоритетні завдання забезпечення національної безпеки в умовах воєнного стану. Станом на грудень 2024 року «ДІЯ» об'єднує понад 20 млн активних користувачів та надає доступ до більш ніж 70 державних послуг онлайн. Важливість цього застосунку для держави підтверджується тим, що він був одним із перших сервісів, роботу якого відновили після масованих ракетних ударів по критичній інфраструктурі [2]. Це демонструє не тільки технологічну стійкість, але й стратегічне значення цифрових рішень для національної стійкості та безпеки.

Метою статті є дослідження ролі застосунку «ДІЯ» у забезпеченні національної безпеки та кібербезпеки України, аналіз поточного функціоналу та потенційних напрямків розвитку для посилення стійкості державних інституцій та захисту персональних даних громадян.

Об'єктом дослідження є застосунок «ДІЯ» як компонент національної системи кібербезпеки України.

Предметом дослідження є функціональні можливості застосунку «ДІЯ» у контексті забезпечення національної безпеки та кібербезпеки.

Аналіз попередніх досліджень. Питанням цифрової трансформації та проблематиці забезпечення національної кібербезпеки присвячено значну кількість наукових публікацій, зокрема Н. Новікова та Л. Бойко розглядають цифрову трансформацію як складову національної безпеки України [3]. Автори пропонують комплексну модель оцінки впливу цифрових інструментів на стійкість держави, акцентуючи увагу на принципах мінімізації людського фактору в процесах державного управління. Дослідник детально обґрунтовує взаємозв'язок між рівнем цифровізації та здатністю держави протистояти кризовим ситуаціям, зокрема воєнним загрозам. Однак значним обмеженням запропонованої моделі є недостатнє врахування кіберзагроз, які пов'язані саме з процесами цифровізації, та відсутність конкретних метрик для оцінки реальної ефективності цифрових рішень у кризових ситуаціях.

Р. Поуп розглядає концепцію «держави як платформи» та її імплікації для національної безпеки цифрових суспільств [4]. Автор пропонує інноваційний підхід до розуміння цифрових державних сервісів як екосистеми з відкритими API, що дозволяють інтегрувати державні та приватні рішення. Дослідник наголошує на потенціалі такої архітектури для підвищення стійкості держави в умовах кризових ситуацій завдяки розподіленій природі та можливості швидкого масштабування. Однак недоліком запропонованої концепції є недостатнє врахування специфічних безпекових викликів, пов'язаних з відкритістю систем, зокрема підвищених ризиків несанкціонованого доступу та компрометації даних при інтеграції з численними зовнішніми сервісами.

Г. Кагерманн, К.-Г. Штрайбіх і К. Зудер досліджують взаємозв'язок між цифровою трансформацією державних сервісів та кібербезпекою в контексті сучасних геополітичних викликів [5]. Автори детально аналізують досвід передових країн у створенні стійких цифрових систем та пропонують комплексну методологію оцінки ризиків для державних цифрових платформ. Особливу цінність представляє розроблена дослідниками модель багаторівневого захисту критичної цифрової інфраструктури, що враховує як технічні, так і організаційні аспекти кіберзахисту. Проте суттєвим обмеженням дослідження є його фокус на усталених демократіях без урахування специфічних викликів, з якими стикаються держави в умовах активних воєнних дій та цілеспрямованих кібератак з боку державних акторів.

Дж. Чуквунуейке, П. Айоделе та Б. Атата запропонували використання згорткових нейронних мереж (CNN) для аналізу пакетів даних, що дозволяє виявляти підозрілі дії [6].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Автори наголошують на високій точності виявлення аномалій завдяки здатності CNN аналізувати складні шаблони в мережевому трафіку, однак основним недоліком є необхідність великих обсягів даних для навчання моделей, що може бути проблемою для малих та середніх підприємств. Також, автори не враховують специфіку систем електронної комерції, де великі обсяги даних та висока частота транзакцій ускладнюють виявлення атак з нульовим днем.

М. Бабу, Р. Вінаякумар та К. Соман розглянули застосування рекурентних нейронних мереж (RNN) для прогнозування атак на основі історичних даних [7]. Їхній підхід дозволяє ефективно аналізувати часові ряди, такі як журнали подій, що є особливо корисним для виявлення динамічних загроз, однак автори не враховують високу обчислювальну складність RNN, що може обмежити їхнє застосування в системах з обмеженими ресурсами. Крім того, їхній підхід не адаптований для виявлення атак з нульовим днем, які вимагають більш проактивних методів.

Виклад основного матеріалу. У таблиці 1 порівнюються традиційні методи кіберзахисту та методи на основі штучного інтелекту за ключовими критеріями, такими як точність, швидкість реагування, адаптивність та обробка великих даних. Застосунок «ДІЯ» є частиною екосистеми цифрової держави, що включає портал державних послуг, мобільний застосунок, платформу цифрової освіти та інші компоненти. У контексті національної безпеки можна виділити кілька ключових напрямків функціонування «ДІЯ» (рис. 1).

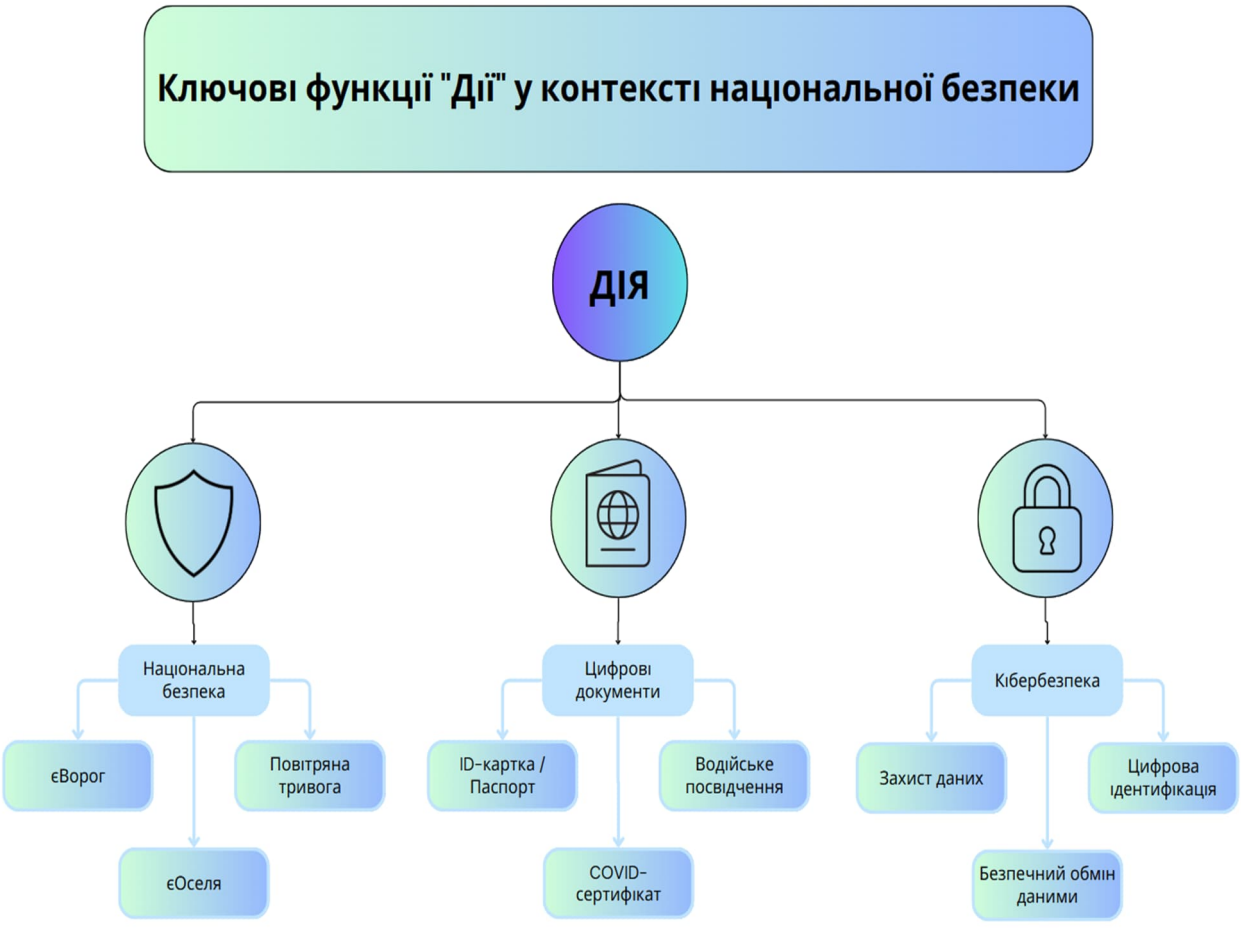


Рис. 1. Ключові функції застосунку «ДІЯ» у контексті національної безпеки

Джерело: розроблено автором на основі [1]

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

У контексті сучасних викликів та загроз, пов'язаних із війною, гібридними атаками та цифровою трансформацією, ключову роль у забезпеченні національної безпеки України відіграє розвиток державних електронних сервісів, зокрема застосунку «ДІЯ» та пов'язаних із ним цифрових інфраструктур.

Цифрові документи забезпечують громадянам доступ до електронних версій офіційних документів (паспорта, посвідчення водія, свідоцтва про реєстрацію транспортного засобу тощо). Це має особливе значення для внутрішньо переміщених осіб, а також для громадян України, які тимчасово перебувають за кордоном, оскільки дозволяє зберегти та підтверджувати особистість без необхідності фізичної присутності або паперових документів.

Єдина система верифікації особи – це інноваційне рішення, що забезпечує надійну цифрову ідентифікацію громадян при взаємодії як із державними, так і з приватними сервісами. Така система істотно знижує ризики шахрайства, викрадення особистості та несанкціонованого доступу до персональних даних.

Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» забезпечує безпечний та автоматизований обмін даними між державними реєстрами. Завдяки цьому реалізується принцип «держава не запитує в громадянина те, що вже знає», що сприяє зниженню адміністративного навантаження та підвищенню ефективності публічного управління.

Електронний кабінет громадянина виконує функцію централізованого доступу до широкого спектру державних послуг. Це сприяє спрощенню процедур, підвищенню прозорості та зменшенню корупційних ризиків у взаємодії громадянина з органами державної влади.

Важливим аспектом забезпечення національної безпеки в цифровому середовищі є стійкість інформаційних систем до кібератак та інших загроз. Застосунок «ДІЯ» створено з урахуванням високих стандартів кібербезпеки. До основних елементів захисту належать:

– багаторівнева система захисту даних;

– шифрування при зберіганні та передачі інформації;

– використання біометричної автентифікації;

– регулярне проведення аудитів безпеки та тестування на проникнення;

– розподілена інфраструктура, що забезпечує безперервність роботи навіть за умов атак або технічних збоїв.

Особливу увагу приділено захисту персональних даних громадян. У застосунку реалізовано принцип zero knowledge proof (доказ з нульовим розголошенням), який дозволяє підтверджувати окремі права чи статуси (наприклад, повноліття) без необхідності розкривати всю персональну інформацію (зокрема, дату народження).

Крім базових функцій, у період воєнного стану застосунок «ДІЯ» отримав додаткові сервіси, що мають безпосередній зв'язок із національною безпекою, зокрема:

– «єДопомога» – механізм отримання матеріальної підтримки від держави та міжнародних організацій;

– «єВорог» – функціонал для повідомлення про переміщення ворожої техніки та сил;

– «єОселя» – інструмент фіксації руйнувань та подання заявок на компенсацію за пошкоджене житло;

– «Повітряна тривога» – інтеграція з системою оповіщення про загрозу повітряного нападу.

У контексті забезпечення кібербезпеки особливої уваги заслуговує архітектура застосунку «ДІЯ», яка спроєктована з урахуванням актуальних і потенційних загроз, пов'язаних із кіберпростором. Однією з ключових особливостей є відсутність зберігання персональних даних на пристрої користувача – застосунок виконує функцію безпечного посередника, що забезпечує захищений канал зв'язку між користувачем та державними електронними реєстрами.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Ідентифікація та аутентифікація користувачів реалізована за багатофакторним принципом, що значно підвищує рівень інформаційної безпеки й унеможливлює несанкціонований доступ до персоніфікованих даних.

Важливим елементом кіберзахисту є регулярне проведення аудиту безпеки системи, який здійснюється як внутрішніми технічними фахівцями, так і зовнішніми незалежними експертами. Застосунок функціонує у тісній взаємодії з командою CERT-UA (Computer Emergency Response Team of Ukraine), що дозволяє оперативно реагувати на нові кіберзагрози, виявлені вразливості та інциденти безпеки. Проте варто зазначити, що попри важливість такої співпраці, офіційні звіти про результати аудитів безпеки не є публічно доступними, що обмежує можливість незалежної оцінки рівня захищеності системи громадськістю та науковою спільнотою. Крім того, зважаючи на масштаби та складність застосунку, існує обґрунтований ризик того, що ресурси команди CERT-UA можуть бути недостатніми для повноцінного протистояння цілеспрямованим кібератакам з боку державних хакерських угруповань країни-агресора, які мають значно більші технічні та людські ресурси.

У стратегічному контексті, перспективні напрями розвитку застосунку «ДІЯ» з позицій кібербезпеки та національної безпеки включають:

1. Розширення функціоналу системи ідентифікації та верифікації особи для її широкого застосування як у державному, так і в приватному секторах. Це сприятиме підвищенню загального рівня цифрової довіри та кіберстійкості.

2. Інтеграція з елементами критичної інфраструктури для оперативного реагування на надзвичайні ситуації, включаючи воєнні дії, техногенні катастрофи та інші кризові сценарії.

3. Розвиток безпечної системи електронного голосування, що ґрунтується на принципах анонімності, надійної аутентифікації та захисту даних, з орієнтацією на забезпечення виборчих прав військовослужбовців і громадян, які перебувають за кордоном.

4. Впровадження технологій штучного інтелекту для виявлення аномальної активності, аналізу кіберзагроз та підвищення проактивної безпеки цифрових сервісів.

5. Розширення функціональних можливостей у межах воєнного стану, зокрема для підтримки життєдіяльності держави: координації волонтерських ініціатив, оперативного інформування громадян про загрози, обліку та моніторингу гуманітарної допомоги, а також інших сервісів, критичних для забезпечення національної стійкості.

У таблиці 1 представлено порівняльний аналіз традиційних підходів до надання державних послуг та цифрових рішень, реалізованих у межах застосунку «ДІЯ».

Таблиця 1

Порівняння традиційного та цифрового підходів до надання державних послуг

Критерій	Традиційний підхід	Цифровий підхід («ДІЯ»)
Спосіб доступу до послуг	Фізичне відвідування державних установ	Доступ до послуг у режимі 24/7 через мобільний застосунок
Формат документів	Паперові документи, що можуть бути втрачені	Цифрові документи, доступні завжди
Процес перевірки документів	Ручна перевірка з можливістю помилки	Автоматична верифікація з мінімальним ризиком помилки
Швидкість отримання послуг	Тривалий процес оформлення та отримання послуг	Швидке отримання послуг (від кількох хвилин до кількох днів)
Повторне надання персональних даних	Необхідність багаторазового подання одних і тих самих даних	Принцип «one-time» – дані вводяться лише один раз
Прозорість взаємодії з державними структурами	Обмежена можливість відстеження статусу звернення	Повна прозорість процесу та можливість відстеження статусу в реальному часі
Рівень корупційних ризиків	Вразливість до корупційних ризиків	Мінімізація людського фактору та корупційних проявів

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Критерій	Традиційний підхід	Цифровий підхід («ДІЯ»)
Готовність до надзвичайних ситуацій	Низька стійкість до кризових ситуацій	Висока стійкість і адаптивність у кризових умовах
Взаємодія між державними структурами	Обмежена інтероперабельність між системами	Повна інтеграція державних реєстрів та інформаційних систем

Джерело: розроблено автором

Особливо перспективним, хоча й недостатньо дослідженим, напрямом розвитку застосунку «ДІЯ» є міжнародна інтеграція та забезпечення транскордонної сумісності цифрових документів та сервісів. В умовах значної міграції українців за кордон та інтеграції України до ЄС критично важливим стає визнання українських цифрових документів у міжнародному просторі. Впровадження відповідних технічних стандартів та протоколів може перетворити «ДІЯ» на потужний інструмент цифрової дипломатії, підвищуючи міжнародну суб'єктність України. Водночас такий розвиток потребує ретельного балансування між інтеграцією та збереженням цифрового суверенітету держави, особливо в контексті міжнародних загроз та кібершпіонажу. Захист від несанкціонованого доступу та мінімізація ризиків витоку даних при міжнародному обміні інформацією вимагатимуть розробки нових криптографічних протоколів та впровадження багаторівневих систем захисту з використанням технологій Zero Knowledge Proof та блокчейну.

Висновки. Застосунок «ДІЯ» виступає ключовим інструментом цифрової трансформації України та має стратегічне значення для забезпечення як національної безпеки, так і кібербезпеки держави. Його функціонування сприяє підвищенню стійкості державних інституцій в умовах криз, забезпечує надійний захист персональних даних громадян та створює ефективні механізми цифрової взаємодії між державою та суспільством.

Запровадження цифрового сервісу «ДІЯ» стало одним із чинників модернізації системи державного управління, що дозволяє не лише оптимізувати надання адміністративних послуг, але й забезпечити їх безперервність в умовах воєнного стану. Такий результат підтверджує, що цифрова трансформація є не виключно технологічним процесом, а й важливим елементом формування національної стійкості в умовах багатовимірних загроз.

Перспективи подальшого розвитку застосунку «ДІЯ» мають бути спрямовані на посилення кіберзахисту, розширення функціональних можливостей для забезпечення життєдіяльності держави в умовах надзвичайних ситуацій, а також на поглиблення інтеграції з іншими державними та міжнародними цифровими системами з метою формування комплексної архітектури безпеки в цифровому середовищі.

Список використаних джерел

1. Міністерство цифрової трансформації України (2024). *Портал «ДІЯ»: Безпека даних та технології захисту*. https://diia.gov.ua/faq

2. Федоров, М. (2022). Цифрова держава в умовах війни: виклики та перспективи розвитку. *Голос Америки*. https://www.holosameryky.com/a/fedorov-pro-tsyfrovu-derzhavu/6583546.html

3. Новікова, Н., Бойко, Л. (2024). Цифровізація та національна безпека: тенденції та виклики. *Економічні аспекти національної безпеки України*, (1), 8–15. https://doi.org/10.51369/3083-5917-2024-1-8

4. Pope, R. (2019). *Playbook: Government as a Platform*. Ash Center for Democratic Governance and Innovation, Harvard Kennedy School. https://ash.harvard.edu/wp-content/uploads/2024/02/293091_hvd_ash_gvmnt_as_platform_v2.pdf

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

5. Kagermann, H., Streibich, K.-H., & Suder, K. (2021). *Digital sovereignty: Status quo and perspectives* (acatech IMPULSE). acatech – National Academy of Science and Engineering. https://www.researchgate.net/publication/351450480_Digital_Sovereignty_Status_Quo_and_Perspectives

6. Chukwunweike, J. N., Ayodele, P. A., & Atata, B. B. (2024, August). Harnessing machine learning for cybersecurity: How convolutional neural networks are revolutionizing threat detection and data privacy. *International Journal of Research Publication and Reviews, 5*(8), 3608–3617. https://www.researchgate.net/publication/383425020

7. Babu, M. H. R., Vinayakumar, R., & Soman, K. P. (2019). *RNNSecureNet: Recurrent neural networks for cyber security use-cases* (arXiv preprint arXiv:1901.04281). arXiv. https://arxiv.org/pdf/1901.04281

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

ПІДХОДИ ДО ВИКОРИСТАННЯ QR-КОДІВ У ВЕРИФІКАЦІЇ ДОКУМЕНТІВ

ПОЖАЛОВ Р. С., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто теоретичні основи та практичні аспекти застосування QR-кодів для верифікації документів. Проведено порівняльний аналіз статичних та динамічних QR-кодів з огляду на їх можливості забезпечення достовірності та безпеки документів. Представлено результати експериментальних досліджень щодо ефективності використання обох підходів у сучасних цифрових системах автентифікації.

The article examines the theoretical foundations and practical aspects of using QR codes for document verification. A comparative analysis of static and dynamic QR codes is presented, focusing on their capabilities to ensure document authenticity and security. The paper discusses the results of experimental studies on the effectiveness of both approaches in modern digital authentication systems.

Актуальність. У сучасних умовах цифрової трансформації та посилення вимог до безпеки інформації дослідження використання QR-кодів для верифікації документів набуває особливої актуальності. Верифікація документів є ключовою складовою забезпечення довіри до електронного обміну даними, а застосування QR-кодів дозволяє швидко та надійно ідентифікувати достовірність документів.

Порівняльний аналіз статичних і динамічних QR-кодів сприятиме розробці оптимальних технологічних рішень для захисту інформації, мінімізації ризиків підробки та забезпечення високого рівня безпеки в сучасному цифровому середовищі. Додатково, проведення порівняльного дослідження дозволить виявити переваги кожного методу, що сприятиме впровадженню інноваційних підходів у сфері електронної ідентифікації та

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

контролю документів. Таким чином, тема є надзвичайно актуальною для наукових досліджень.

Метою статті є аналіз та порівняння ефективності застосування різних підходів у QR-кодах для верифікації документів, а також визначення їх переваг і обмежень у контексті сучасних інформаційних технологій.

Об'єктом дослідження є технологія використання QR-кодів у процесах верифікації документів.

Предметом дослідження є ефективність застосування статичних та динамічних QR-кодів для забезпечення достовірності та цілісності документів.

Аналіз попередніх досліджень. У науковій літературі простежується значний інтерес дослідників до порівняння статичних і динамічних QR-кодів. Наприклад, Ю. Ма та П. Као року фокусуються на перевагах динамічних QR-кодів порівняно зі статичними, зокрема на можливості перевизначення інформації та повторного кодування [4]. Автори пропонують новітню технологію динамічних QR-кодів із захистом від копіювання властивостями, аналізуючи такі алгоритми генерації як UUID, шифрування даних та цифрові водяні знаки. Хоча дослідження містить суттєве методологічне обмеження – тестування проводилось у ідеалізованих лабораторних умовах без врахування реальних кібератак на промислові системи.

В. Бондаренко детально проаналізував відмінності між статичними та динамічними QR-кодами в контексті маркетингової діяльності бібліотек. Автор підкреслює, що динамічні QR-коди дозволяють змінювати вихідні дані без зміни самого коду, що значно розширює їхні можливості [1]. У дослідженні продемонстровано переваги QR-технології, серед яких універсальність, гнучкість, економічність та можливість відстеження аналітики, проте проігноровано технологічні бар'єри їх впровадження. Наприклад, не враховано необхідність постійного інтернет-з'єднання для оновлення контенту, що суттєво обмежує використання в регіонах з низькою якістю зв'язку.

Ю. Чжоу, Б. Ху, Ю. Чжан та В. Цай при аналізі систем оплати через QR-код виявили суттєві проблеми безпеки статичних кодів, які легко копіюються та підміняються. Розроблена система динамічних QR-кодів з підтримкою криптографічних алгоритмів SM2, SM3 та SM4 забезпечує унікальність кожної транзакції [7]. Принцип «одне замовлення – один код», значно підвищує рівень безпеки Однак автори не врахували сумісність цього підходу з міжнародними платіжними стандартами EMVCo що створює проблеми при інтеграції з глобальними фінансовими системами.

Виклад основного матеріалу. Еволюція систем перевірки документів зазнала значного прогресу завдяки інтеграції технології QR-кодів. Ця технологія радикально трансформувала підходи до валідації документів у широкому спектрі сфер – від фінансових операцій до підтвердження кваліфікацій у закладах вищої освіти. Особливою віхою цієї трансформації є перехід від статичних до динамічних QR-кодів, що представляє суттєвий прорив як у сфері безпеки, так і з точки зору функціональних можливостей. Сучасна практика виділяє два основних підходи до застосування QR-кодів (рис. 1).

Статичні QR-коди являють собою базову реалізацію QR-технології, що характеризується кодуванням незмінних даних під час генерації (рис. 2). Після створення коду інформація в ньому залишається фіксованою, а будь-яке внесення змін вимагає повної генерації нового коду [5]. У практичному застосуванні для перевірки документів статичні QR-коди зазвичай містять критично важливі дані, зокрема деталі видачі, ідентифікатори документів або посилання для перевірки їх автентичності.

Технічна реалізація статичних QR-кодів базується на стандартизованих алгоритмах кодування, що забезпечують їх сумісність із широким спектром застосунків для сканування.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Ця універсальність є ключовою перевагою у сценаріях перевірки документів, оскільки усуває необхідність використання спеціалізованого обладнання [6]. Генерація коду здійснюється шляхом перетворення даних у візуальні патерни за допомогою усталених алгоритмічних підходів.

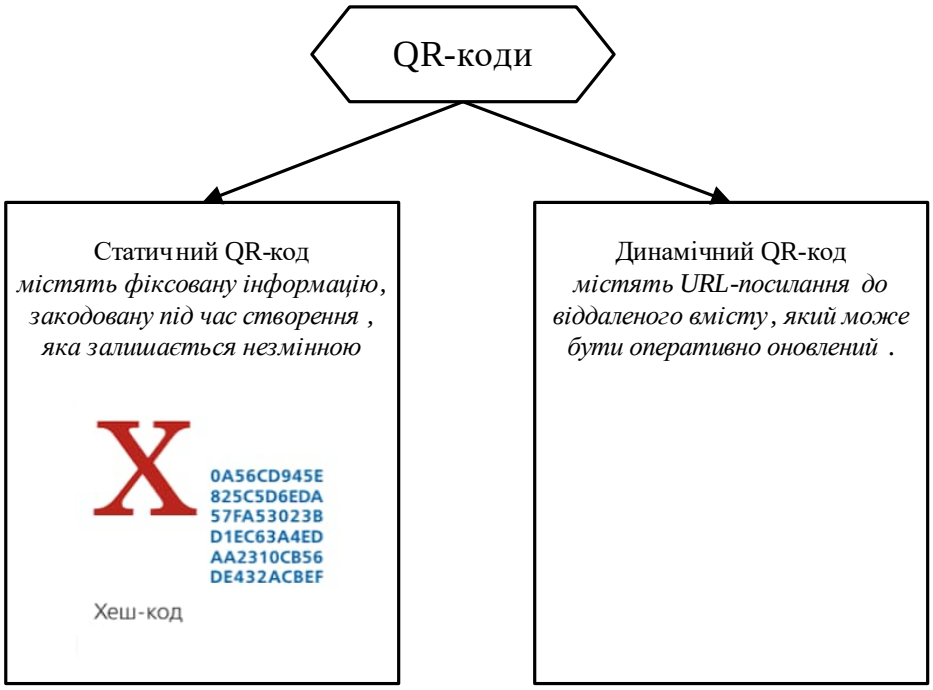


Рис. 1. Підходи до QR-кодів

Джерело: розроблено автором

Незважаючи на відносну простоту, статичні QR-коди можуть включати у себе складові елементи безпеки. Сучасні реалізації передбачають застосування дворівневих систем, що розділяють публічну та приватну інформацію. Такий підхід дозволяє підвищити рівень безпеки: публічний шар доступний для стандартних сканерів, тоді як приватний шар реалізовано через використання текстурних патернів замість традиційних чорних модулів, що забезпечує додаткові рівні захисту та розширює можливості зберігання даних (рис. 2).

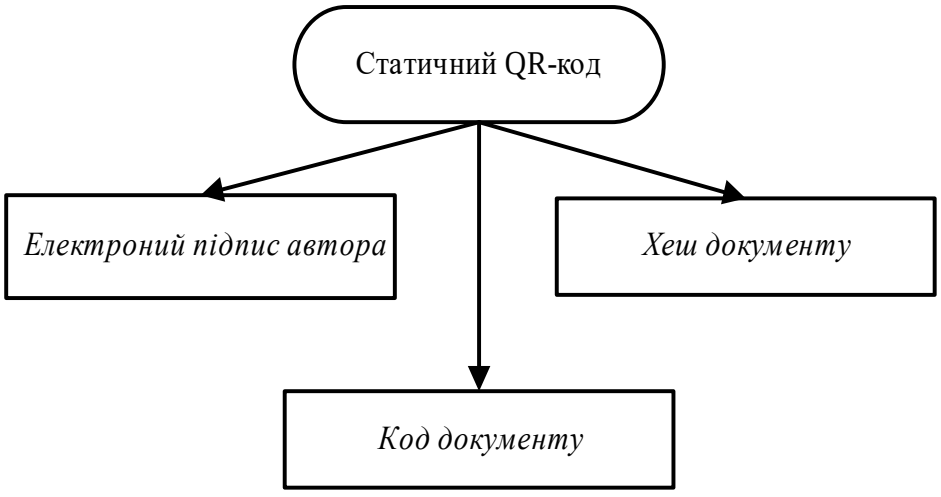


Рис. 2. Вміст статичного QR-коду

Джерело: розроблено автором

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Динамічні QR-коди представляють собою наступний етап розвитку QR-технологій, адже вони надають підвищену гнучкість та вдосконалені засоби безпеки, що є надзвичайно важливим при перевірці документів. На відміну від статичних, динамічні QR-коди містять перенаправлену URL-адресу або унікальний ідентифікатор, який пов'язаний із сервером або базою даних, що зберігає актуальну інформацію про документ (рис. 3). Такий механізм перенаправлення дозволяє оновлювати базові дані без необхідності зміни самого коду, що відкриває нові можливості для перевірки та аутентифікації в режимі реального часу.

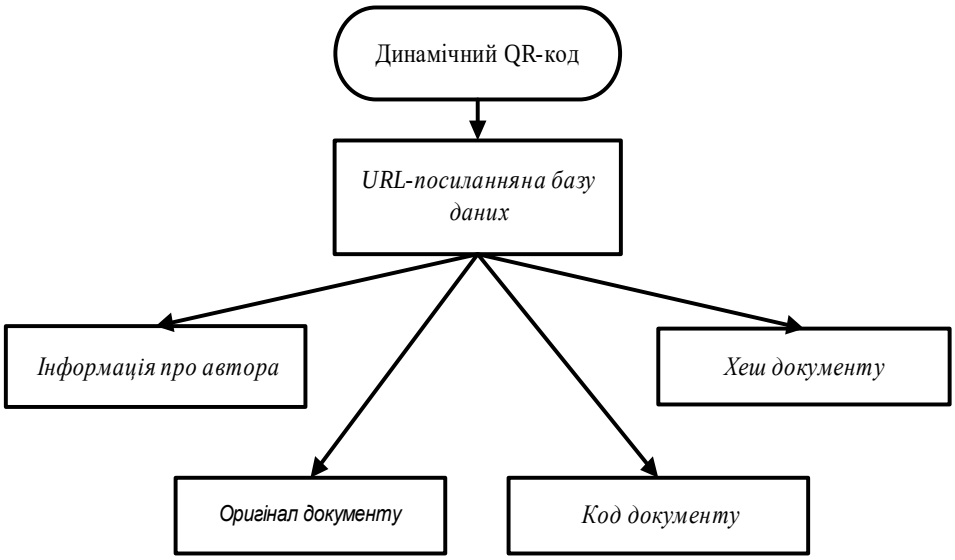


Рис. 3. Вміст динамічного QR-коду

Джерело: розроблено автором

Основною перевагою динамічних QR-кодів є можливість оперативної заміни інформації. Це дозволяє органам, що видають документи, своєчасно коригувати параметри перевірки, змінювати процедури аутентифікації або відкликати дійсність документа без необхідності повторного друку чи видачі фізичних носіїв. Такий підхід сприяє підвищенню ефективності управління документами та забезпеченню високого рівня безпеки, оскільки скомпрометовані або застарілі документи можуть бути миттєво ідентифіковані під час перевірки.

Додатково, динамічні QR-коди можуть бути обладнані комплексними механізмами захисту, серед яких – запобігання дублюванню шляхом використання різноманітних технічних рішень. Алгоритми генерації, що застосовують універсально унікальні ідентифікатори (UUID), передові методи шифрування та цифрове водяне маркування, значно підвищують рівень безпеки систем перевірки. Ці заходи ефективно усувають одну з головних вразливих точок сучасних систем – ризик несанкціонованого дублювання документів.

Архітектура безпеки систем верифікації документів із застосуванням QR-кодів демонструє суттєві відмінності між статичними та динамічними реалізаціями. Статичні QR-коди, незважаючи на їхню функціональність, містять низку вразливостей, зумовлених їх фіксованою природою. Така незмінність робить їх більш вразливими до несанкціонованого копіювання та реплікації, що створює серйозні перешкоди для систем безпечної верифікації документів [7]. Після генерації статичного коду його скасування або модифікації можливі лише шляхом повної заміни документа, що обмежує оперативність реагування на порушення безпеки.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Натомість динамічні QR-коди пропонують комплекс переваг з точки зору безпеки. Валідація таких кодів на серверному рівні забезпечує реальний час перевірки з урахуванням актуальних параметрів безпеки, що сприяє негайному виявленню підроблених документів. Принцип «одне замовлення – один код» гарантує, що кожен документ отримує унікальний часово-чутливий код верифікації, що значно знижує ризики його реплікації [3]. Крім того, динамічні системи дозволяють впроваджувати сучасні протоколи безпеки, зокрема багатофакторну аутентифікацію, шифрування та блокчейн-верифікацію, без необхідності змінювати фізичний QR-код.

Інтеграція криптографічних методів істотно підвищує рівень захисту як статичних, так і динамічних систем верифікації QR-кодів, проте підходи до їхнього впровадження відрізняються. Дослідження статичних QR-кодів зосереджуються на вбудовуванні криптографічних підписів безпосередньо в сам код. Зокрема, алгоритм цифрового підпису на основі еліптичної кривої Edwards (EdDSA) демонструє високі показники продуктивності при аутентифікації документів, забезпечуючи прискорення до 98,17% порівняно з традиційними підходами, заснованими на алгоритмі цифрового підпису.

У свою чергу, динамічні системи QR-кодів зазвичай впроваджують криптографічну безпеку на серверному рівні, що дозволяє використовувати більш потужні механізми шифрування та аутентифікації. Сучасні реалізації інтегрують криптографічні алгоритми SM2, SM3 та SM4 у системах динамічних платежів із застосуванням QR-кодів, демонструючи підвищену безпеку та продуктивність [7]. Така серверна архітектура дозволяє впроваджувати складні протоколи безпеки, зберігаючи при цьому оптимальний розмір QR-коду та ефективність його сканування.

У таблиці 1 показані ключові переваги та недоліки статичних та динамічних QR-кодів. Практична реалізація систем перевірки документів за допомогою QR-кодів вимагає ґрунтовного аналізу багатьох технічних та експлуатаційних аспектів. Статичні реалізації характеризуються спрощеною інфраструктурою, що обмежується генератором QR-кодів та відповідним додатком для перевірки. [6] Такий підхід сприяє зниженню витрат на впровадження та мінімізації технічної складності, що є вагомою перевагою для організацій з обмеженими технологічними ресурсами.

Натомість динамічні системи перевірки QR-кодів потребують високонадійної технологічної інфраструктури, яка включає захищені бази даних, стабільні мережеві з'єднання та складні протоколи безпеки. Використання хмарних архітектур дозволяє забезпечити перевірку документів у режимі реального часу та ефективне управління даними, що забезпечує додатковий рівень захисту та адаптивності до сучасних стандартів безпеки [2]. Незважаючи на зростання складності впровадження, даний підхід значно підвищує надійність перевірки та ефективність довгострокового управління системою.

Таблиця 1

Порівняння статичних та динамічних QR-кодів

Характеристика	Статичні QR-коди	Динамічні QR-коди
Редагування	Інформація зафіксована після генерації; будь-які зміни потребують повторного створення коду	Можливість оновлення даних у режимі реального часу без необхідності перегенерації коду
Відстеження сканувань	Відсутнє; не надають аналітичних даних	Вбудована аналітика – фіксується кількість сканувань, місцезнаходження та інші параметри

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Характеристика	Статичні QR-коди	Динамічні QR-коди
Безпека	Схильні до копіювання та реплікації; обмежена можливість реагувати на порушення	Підтримують серверну перевірку, додаткові протоколи безпеки (шифрування, багатофакторна аутентифікація, унікальні коди)
Гнучкість	Інформація залишається незмінною; при потребі зміни документа потрібно створювати новий код	Забезпечують гнучкість: можна змінювати пов'язаний контент без перегенерації QR-коду
Використання для верифікації документів	Використовуються для перевірки документів, але не дозволяють оперативно реагувати на підробки чи порушення	Реалізують перевірку в режимі реального часу з можливістю швидкого скасування або оновлення даних у випадку порушень
Вартість та інтеграція	Зазвичай безкоштовні або з мінімальними витратами; не потребують додаткової інфраструктури	Можуть бути платними; потребують інтеграції з серверними рішеннями, але забезпечують додаткові можливості для контролю і аналізу

Джерело: розроблено автором

Процеси обробки документів відрізняються залежно від обраного підходу. Статичні системи зазвичай реалізують послідовність операцій, що включає: отримання документа, аналіз ознак документу, порівняння з даними QR-коду та виявлення підробок. Цей процес здійснюється локально на пристрої сканування, що усуває потребу у використанні зовнішніх джерел даних (рис. 4). У свою чергу, динамічні системи включають додаткові етапи комунікації, підключення до серверів перевірки для автентифікації документів за актуальними параметрами безпеки та отримання інформації про їхній статус.

Систем перевірки QR-кодів знаходить широке застосування у різних галузях, при цьому вибір методів впровадження визначається вимогами до безпеки, операційними обмеженнями та специфічними завданнями верифікації. У традиційних сферах перевірки документів, зокрема при підтвердженні академічних кваліфікацій, статичні QR-коди довели свою ефективність для базової перевірки автентичності. Зазвичай такі рішення кодують основну інформацію про кваліфікацію разом із елементарними криптографічними підписами, що забезпечує можливість офлайн-перевірки з базовим виявленням спроб фальсифікації.

Для завдань, що потребують високого рівня безпеки, динамічні QR-коди виявляються більш дієвими. При верифікації фінансових транзакцій системи на основі динамічних QR-кодів генерують унікальні коди в режимі реального часу для кожної операції, що суттєво знижує ризики шахрайства [3]. Постійне оновлення параметрів перевірки та застосування складних криптографічних протоколів сприяють забезпеченню автентичності транзакцій і попередженню несанкціонованого дублювання даних.

Особливо перспективним є застосування систем верифікації на базі блокчейн-технологій, що являють собою інноваційне використання QR-кодів. Такі системи генерують унікальні QR-коди, інтегровані із записами в блокчейні, що забезпечує створення незмінних перевірочних записів і сприяє динамічній взаємодії через зручні інтерфейси. Інтеграція блокчейн-технологій із динамічною перевіркою QR-кодів дозволяє створювати надзвичайно надійні архітектури безпеки, адже перевірочні записи зберігаються у децентралізованих мережах, а не централізованих базах даних.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Рис. 4. Процеси верифікації документів

Джерело: розроблено автором

Системи перевірки реєстрації транспортних засобів демонструють ще один вагомий приклад застосування динамічних QR-кодів. Хмарні рішення дозволяють уповноваженим працівникам сканувати QR-коди транспортних засобів та здійснювати миттєву перевірку автентичності документів через захищені бази даних [2]. Такий підхід оптимізує процеси контролю та суттєво знижує ризики фальсифікації, оскільки перевірка базується на актуальних офіційних записах, а не на потенційно змінених паперових документах.

Висновки. Аналіз статичних і динамічних QR-кодів для перевірки документів виявив суттєві відмінності у функціональних можливостях та рівнях безпеки. Статичні QR-коди забезпечують простоту, універсальну сумісність та можливості офлайн-перевірки, що робить їх придатними для базових сценаріїв перевірки документів. Проте їх фіксований характер створює вроджені вразливості безпеки через ризики копіювання та обмежені можливості оновлення, що обмежує їх застосування в контекстах високої безпеки перевірки.

Динамічні QR-коди забезпечують вищий рівень безпеки завдяки можливості перевірки в режимі реального часу, здатності до заміни інформації та використання складних протоколів автентифікації. Незважаючи на необхідність більш складної інфраструктури впровадження, динамічні системи відкривають значні переваги в гнучкості управління документами, адаптації заходів безпеки та надійності перевірки.

Організації, що впроваджують системи перевірки документів, повинні ретельно оцінювати свої конкретні вимоги до безпеки, технологічні можливості та операційні цілі при виборі між статичними та динамічними QR-впровадженнями.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаних джерел

1. Бондаренко В. (2020). QR-код як інструмент маркетингової діяльності бібліотеки. http://librinfosciences.knukim.edu.ua/article/view/205735/205804

2. Gadbail, D. R., Korde, I., Ande, K., Bele, T., & Sangle, V. (2025). *Cloud-based QR code authentication system for real-time vehicle verification. International Journal for Multidisciplinary Research (IJFMR), 7*(1). https://www.ijfmr.com/papers/2025/1/36456.pdf

3. Hu, B., & Zhou, Y. (2019). Research on Quickpass payment terminal application system based on dynamic QR code. *Journal of Physics: Conference Series, 1168*, 032059. https://doi.org/10.1088/1742-6596/1168/3/032059

4. Ma, Y., & Cao, P. (2024). Research on security and value-added service technology of dynamic QR code. Other Conferences. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/13107/3029182/Research-on-security-and-value-added-service-technology-of-dynamic/10.1117/12.3029182.full

5. Tekale, H. A. (2024). A comprehensive study on QR codes. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 4*(3). https://ijarsct.co.in/Paper18935.pdf

6. Trimbake, P. K., & Nawathe, A. N. (2018). Using two-level QR code system for providing security to important data. *IRE Journals, 1*(6), 81-84. https://www.irejournals.com/formated-paper/1700132.pdf

7. Zhou, Y., Hu, B., Zhang, Y., & Cai, W. (2021). Implementation of cryptographic algorithm in dynamic QR code payment system and its performance. *IEEE Access, 9*, 122362-122372. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9523747

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ТОКАРЯ В. В.

БЕЗПАРОЛЬНІ МЕТОДИ АВТЕНТИФІКАЦІЇ У ВЕБЗАСТОСУНКАХ

СВІРЩУК Я. Ю., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто основні принципи безпарольної автентифікації у вебзастосунках. Зазначені переваги безпарольних методів над класичними методами з використанням паролю. Детально розглянутий програмний інтерфейс для реалізації безпарольної автентифікації WebAuthn, а також запропоновано модель системи адаптивної автентифікації з використанням даного інтерфейсу.

The article considers the basic principles of passwordless authentication in web applications. The advantages of passwordless methods over classic password-based methods are indicated. The programming interface for implementing passwordless authentication WebAuthn is considered in detail, and a model of an adaptive authentication system using this interface is proposed.

Актуальність. Коли Фернандо Корбато вперше представив ідею паролів у Массачусетському технологічному інституті в 1960 році, він, ймовірно, не припускав, що вони стануть головним методом автентифікації на наступні десятки років. Цікаво, що поява паролів була частково результатом технологічного компромісу. Незважаючи на те, що на той час існували

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

сильніші альтернативи автентифікації, для ранніх комп'ютерів зберігання паролів потребувало набагато менше пам'яті.

Із розвитком інформаційних технологій питання безпеки автентифікації користувачів стає все більш актуальним. Хоча обчислювальна потужність комп'ютерів стала набагато більшою, паролі все ще залишаються основним та єдиним методом автентифікації у більшості систем, незважаючи на їх недоліки: низька стійкість до атак зловмисників, складність запам'ятовування та управління, ризики фішингу тощо. Саме тому сучасні веб-застосунки почали активно впроваджувати безпарольні методи автентифікації, які підвищують рівень безпеки, зручності та доступності для користувачів.

Безпарольні системи, які зокрема імплементують підходи з WebAuthn, дозволяють використовувати методи, що не зобов'язують користувача запам'ятовувати інформацію для автентифікації, такі як біометричні дані, апаратні ключі або криптографічні ключі, згенеровані на пристрої користувача. Це забезпечує значно вищий рівень захисту від фішингу, атак перебором та компрометації облікових записів.

Особливої актуальності безпарольна автентифікація набуває в корпоративному середовищі, електронній комерції, онлайн-банкінгу та державних сервісах, де компрометація облікових даних може мати критичні наслідки.

Метою статті є дослідження та аналіз безпарольних методів автентифікації у вебзастосунках, а також перспектив впровадження для підвищення безпеки та зручності користувачів.

Об'єктом дослідження є системи безпарольної автентифікації вебзастосунків.

Предмет дослідження - методи та механізми реалізації безпарольної автентифікації, зокрема на основі WebAuthn.

Аналіз попередніх досліджень. Проблемам автентифікації, підвищенню безпеки вебзастосунків та розробці альтернатив паролям присвячені праці науковців: Д. Бонеха, Ф. Холлештайн, А. Ленглі, а також дослідження, проведені в рамках ініціативи FIDO Alliance та W3C.

Виклад основного матеріалу. Безпарольна автентифікація стосується методів, які дозволяють користувачам входити в IT-системи, такі як вебсайти, бази даних і програми, без введення текстових паролів, облікових даних або інших «секретів». Прикладами безпарольних методів автентифікації є:

– Біометричні фактори: відбиток пальцю, розпізнавання за голосом чи обличчям, обличчям сканування сітчатки ока.

– Фактори власності: пристрій, яким володіє користувач, на який приходить одноразовий код входу, фізичні пристрої, що підключаються до комп'ютера для автентифікації.

– Поведінковий фактор: Паттерн друку тексту на клавіатурі користувачем, динаміка використання тачскрину.

– QR коди: коди, що скануються камерою з іншого, підтвердженого (автентифікованого) пристрою.

– Ключі доступу: криптографічні облікові дані.

Однією з передових компаній, що займається дослідженнями та впровадженням безпарольної автентифікації є FIDO. FIDO (Fast IDentity Online) – це альянс, створений для розробки та впровадження відкритих стандартів безпечної автентифікації без використання паролів. Основною метою FIDO є заміна традиційних паролів більш безпечними та зручними методами автентифікації, які використовують криптографію з відкритим ключем. Ключовим стандартом безпарольної автентифікації, розроблений цим альянсом, є FIDO2, який включає протоколи Web Authentication API (WebAuthn) та Client to Authenticator Protocol (CTAP).

WebAuthn – це відкритий веборієнтований програмний інтерфейс, офіційно випущений у березні 2019 року, який використовує ключі асиметричної криптографії для автентифікації користувачів у вебзастосунках без необхідності використання паролів. Організація FIDO

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

співпрацювала з World Wide Web Consortium (W3C), міжнародною організацією зі стандартизації Всесвітньої павутини, щоб стандартизувати автентифікацію FIDO для всього веб-простору. Для того, щоб зрозуміти принцип роботи WebAuthn розглянемо два основні процеси, що забезпечуються даним інтерфейсом – реєстрація та автентифікація користувача.

Для обох процесів можна виділити чотири ролі, які беруть в них участь: користувач, користувацький агент, довірений ресурс та автентифікатор. Користувач – це людина, яка намагається отримати доступ до ресурсу. Користувацький агент встановлений на пристрої у користувача (зазвичай, веб-браузер) та відповідає за комунікацію між іншими ролями. Довірений ресурс – це вебзастосунок, до якого звертається користувач. Для перевірки користувача використовується автентифікатор, який зчитує інформацію для автентифікації з фізичного модуля чи пристрою (сканер відбитку пальцю, камера, мікрофон, фізичний ключ безпеки тощо), а також генерує пари криптографічних ключів та підписує сертифікати.

Процес реєстрації користувача, відомий також як церемонія реєстрації, проходить наступним чином:

- Користувач ініціює реєстрацію на довіреному ресурсі у своєму веббраузері (користувацькому агенті).
- Сервер автентифікації довіреного ресурсу надсилає челендж (випадково згенерований набір символів) користувацькому агенту.
- Користувацький агент надсилає челендж автентифікатору разом з повідомленням про те, щоб створити нові облікові дані для довіреного ресурсу, оскільки користувач реєструється на ресурсі вперше.
- Автентифікатор пропонує користувачу перелік можливих способів автентифікації
- Після успішної автентифікації автентифікатор створює пару закритого та відкритого ключів для довіреного ресурсу.
- Автентифікатор надсилає зашифрований закритим ключем результат, що містить челендж, відкритий ключ, джерело запиту та інші деталі довіреному ресурсу.
- Довірений ресурс використовує відкритий ключ для розшифрування повідомлення від автентифікатора та перевіряє челендж на відповідність з тим, що був згенерований ресурсом. Також ресурс перевіряє джерело, надіслане автентифікатором, з якого приходить запит на реєстрацію, для запобігання міжсайтової підробки запиту (CSRF).
- Якщо попередні етапи пройшли успішно – реєстрацію користувача завершено та його облікові дані, що включають відкритий ключ та ім’я користувача, зберігаються на сервері ресурсу.

Процес церемонії автентифікації схожий на реєстрацію, однак має певні відмінності у етапах виконання:

- Користувач ініціює вхід на довірений ресурс з власним користувацьким ім’ям.
- Довірений ресурс знову надсилає челендж користувацькому агенту, проте у цей раз додає ідентифікатором (id) закритого ключа.
- Агент передає отримані від ресурсу дані автентифікатору та проходить автентифікацію (як при реєстрації).
- При успішній автентифікації автентифікатор використовує наданий ідентифікатор закритого ключа для отримання пари закритого і відкритого ключа користувача для довіреного ресурсу.
- Отриманим закритим ключем автентифікатор шифрує повідомлення, що містить ті ж дані, що і при реєстрації, крім відкритого ключа користувача.
- Довірений ресурс розшифровує отримане повідомлення відкритим ключем, що збережений на сервері довіреного ресурсу, для перевірки легітимності користувача, і також перевіряє джерело запиту.
- У разі успішного виконання попередніх етапів користувачу надається доступ до ресурсу.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Такий метод автентифікації користувача має перелік переваг над автентифікацією з використанням паролів. По-перше, автентифікація з WebAuthn є більш захищеною до атак зловмисників, таких як фішинг, людина посередині (man-in-the-middle), атаки перебором тощо, оскільки закритий ключ зберігається тільки на стороні користувача та не передається на довірений ресурс, тому його не можна перехопити чи підібрати.

По-друге, безпарольна автентифікація у рази покращує користувацький досвід використання застосунку, оскільки користувач не має запам'ятовувати якусь нову інформацію для доступу до ресурсу – для автентифікації використовується його власність, наприклад телефон, чи те, чим він є (біометрія користувача).

По-третє, така автентифікація надає змогу розробникам сфокусуватись на самому застосунку та його функціоналу, не переймаючись за створення складної системи захищеної автентифікації та зберігання паролів. Розробникам потрібно лише створити захищену базу даних з відкритими ключами користувачів, при чому навіть якщо зловмисник отримає доступ до цих ключів – він однаково не зможе їх використати без закритих ключів.

Інша частина стандарту FIDO2 – CTAP (Client to Authenticator Protocol) є додатком до WebAuthn та керує зв'язком між користувацьким агентом та зовнішнім автентифікатором. Він дозволяє зовнішньому автентифікатору, такому як ключ безпеки або мобільний телефон, працювати з браузерами, які підтримують WebAuthn, а також з десктопними застосунками та веб-службами. CTAP не бере прямої участі у самому процесі автентифікації користувача, а лише у передачі даних між автентифікаторами та користувацьким агентом, тому у цій статті він описаний лише у загальному.

Імплементація WebAuthn вже є доволі безпечним методом автентифікації, однак для підвищення захищеності даних користувачів у веб-застосунках, мною була розроблена модель системи адаптивної автентифікації з використанням інтерфейсу WebAuthn, яка запрошує додаткові методи автентифікації у разі підозрілих дій користувача та при виконанні важливих дій, що потребують додаткового захисту (рис. 1).

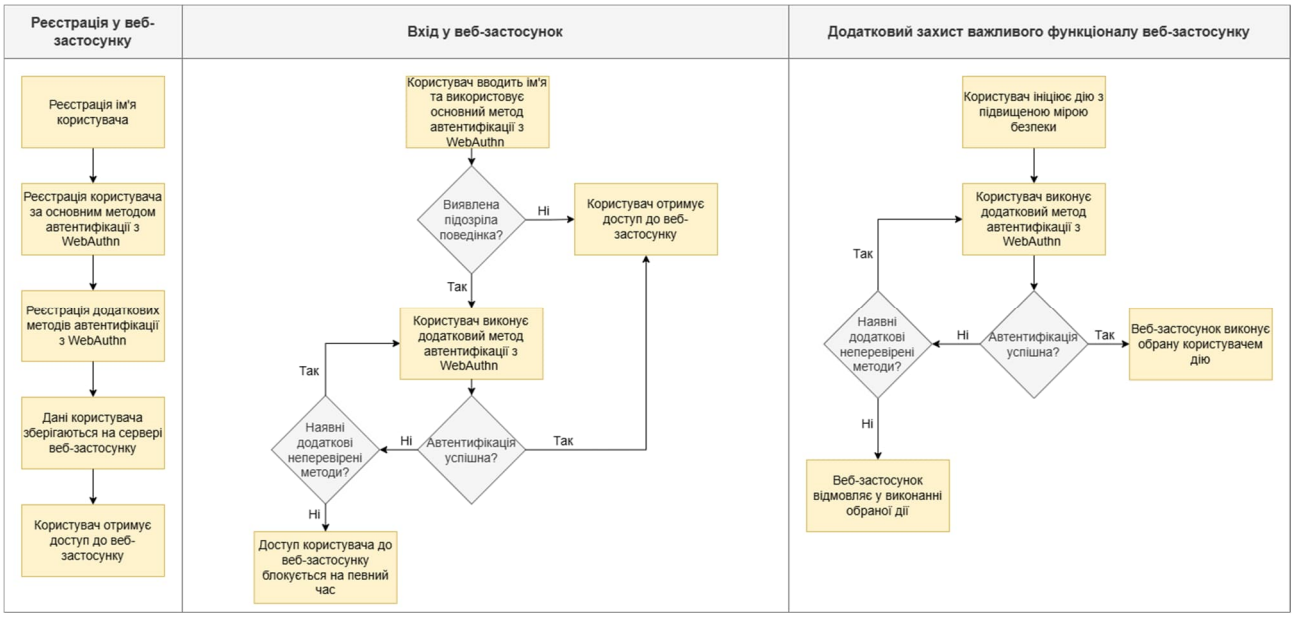


Рис. 1. Модель системи адаптивної автентифікації

Джерело: розроблено автором

Ця модель складається з трьох основних варіантів використання автентифікації – реєстрація користувача, вхід у застосунок та додатковий захист важливого функціоналу. Розглянемо детальніше кожен з варіантів.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Процес реєстрації користувача починається з реєстрації ім'я користувача. Далі йде реєстрація основного методу автентифікації, за яким користувач буде входити у вебзастосунок за замовчуванням, наприклад сканер відбитку пальців чи розпізнавання обличчя. Потім в залежності від контексту вебзастосунку, а також за бажанням користувача реєструються додаткові методи автентифікації, які будуть використовуватися для подальших додаткових перевірок. Після реєстрації методів дані, необхідні для автентифікації, а також мета-дані про користувача, такі як його середня швидкість введення тексту з клавіатури, геолокація (за згодою користувача), дані про користувацький агент та пристрій, з якого здійснено вхід, зберігаються на сервері. Ці дані будуть необхідні для автентифікації користувача у майбутньому. В кінці користувач отримує доступ до вебзастосунку.

При вході у вебзастосунок, користувач вводить своє ім'я та пробує увійти через основний метод автентифікації. Якщо користувач має підозрілу поведінку, а саме: надмірна кількість невдалих спроб входу за основним фактором, далека поточна геолокація у порівнянні з тою, де була проведена реєстрація, новий пристрій входу – тоді у користувача запитується додатковий фактор автентифікації, який був доданий при реєстрації. Якщо користувач не виконує вимоги обраного додаткового фактору – користувач виконує наступний метод автентифікації із зареєстрованих ним. Якщо ні один додатковий метод автентифікації не було пройдено – доступ до застосунку блокується на певний час, після якого користувач знову може спробувати пройти автентифікацію заново за основним та додатковим методом. Якщо ж користувач успішно пройшов додаткову автентифікацію – він далі продовжує користуватись застосунком.

Подібно до проходження додаткового фактору при підозрілій поведінці при вході працює додатковий захист важливого функціоналу застосунку, для якого потребується додатковий захист. Прикладами такого функціоналу може бути переказ великої суми грошей у банківському вебзастосунку або зміна одного з методів автентифікації для облікового запису користувача. Різниця лише у тому, що тут проходження додаткової автентифікації є закладеним спочатку та не залежить від поведінки користувача. У цьому варіанті якщо користувач не виконав вимоги додаткового методу автентифікації – то вебзастосунок не виконає дію з підвищеним захистом, яку ініціював користувач.

Переваги даної моделі у порівнянні зі стандартною системою автентифікації з паролем, полягають у високому рівні захисту вебзастосунку та покращенні користувацького досвіду взаємодії з вебзастосунком, оскільки усі методи автентифікації, що використовуються у даній моделі працюють з використанням WebAuthn та не потребують запам'ятовування додаткової інформації від користувача. Також ця модель є гнучкою, оскільки в залежності від встановленої обов'язкової кількості та типу додаткових автентифікаторів, її можна використовувати як у звичайних вебзастосунках, які не містять критичної інформації про користувача, так і у системах, що потребують більшого захисту, наприклад у вебзастосунках, що містять конфіденційну інформацію, такі як банківські чи державні вебзастосунки, або у внутрішніх вебзастосунках компаній.

Висновки. Поява програмного інтерфейсу WebAuthn дала поштовх розробникам для дослідження та імплементації безпарольних автентифікації у свої вебзастосунки. Завдяки даному інтерфейсу з'явилась можливість створювати безпечні системи автентифікації, що не тільки не ускладнюють, але й спрощують користувачам роботу з вебзастосунками.

Хоча й безпарольна автентифікація має низку переваг, однак перехід на її обширне використання може зайняти ще певний час. Хоч й більшість користувачів вебпростору мають пристрої, які можуть забезпечити найбільш розповсюджений тип безпарольної автентифікації, біометричну – точність такої автентифікації може бути доволі низькою, наприклад через технічні характеристики сканерів на пристрої користувача, їх несправність або через неточність алгоритмів обробки біометричних даних.

Незважаючи на це, використання безпарольних методів у вебзастосунках стрімко зростає, а розробники та компанії активно працюють над підвищенням точності біометричних алгоритмів та покращенням апаратного забезпечення, тому безпарольна автентифікація вебзастосунків є перспективним напрямом у кібербезпеці.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаних джерел

1. Passwordless Authentication [Електронний ресурс] – https://delinea.com/what-is/what-is-passwordless-authentication
2. What Is Passwordless Authentication & How It Works [Електронний ресурс] – https://www.descope.com/learn/post/passwordless-authentication
3. FIDO2: Web Authentication (WebAuthn) [Електронний ресурс] – https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/
4. WebAuthn 101: Definition, How It Works & Benefits [Електронний ресурс] – https://www.descope.com/learn/post/webauthn
5. An Overview of WebAuthn [Електронний ресурс] – https://curity.io/resources/learn/webauthn-overview/
6. Web Authentication: An API for accessing Public Key Credentials [Електронний ресурс] – https://www.w3.org/TR/webauthn-1/
7. What is CTAP? [Електронний ресурс] – https://www.yubico.com/resources/glossary/ctap/

Роботу виконано під науковим керівництвом канд. техн. наук, ст. наук. співроб., доцента ЗВЄРЄВА В. П.

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ МОБІЛЬНИХ МЕРЕЖ ВІД АТАК НА КОНФІДЕНЦІЙНІСТЬ І ДОСТУПНІСТЬ

СИНЕЛЬНИК Д. В., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті проаналізовано актуальні загрози для мобільних комунікаційних систем, зокрема мереж 4G/LTE, та розглянуто сучасні методи захисту від атак на конфіденційність і доступність. Досліджено критичні вразливості протоколів доступу LTE, що дозволяють зловмисникам визначати місцеперебування пристроїв і порушувати надання послуг. Запропоновано класифікацію атак за рівнем складності та впливу, а також ефективні контрзаходи для мінімізації ризиків. Особливу увагу приділено адаптивним механізмам безпеки, що знижують ймовірність компрометації даних і підвищують стійкість мережі.

The article analyzes the current threats to mobile communication systems, in particular 4G/LTE networks, and considers modern methods of protection against attacks on confidentiality and availability. Critical vulnerabilities of LTE access protocols that allow attackers to determine the location of devices and disrupt service provision are investigated. A classification of attacks by the level of complexity and impact is proposed, as well as effective countermeasures to minimize risks. Particular attention is paid to adaptive security mechanisms that reduce the likelihood of data compromise and increase network resilience.

Актуальність. Актуальність дослідження зумовлена стрімким розвитком мобільних мереж та зростанням кількості кіберзагроз, які можуть суттєво впливати на конфіденційність

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

та доступність користувацьких даних. Незважаючи на впровадження сучасних механізмів безпеки в стандартах 4G/LTE, зокрема взаємної аутентифікації та удосконалених криптографічних алгоритмів, аналіз специфікацій LTE-протоколів виявив критичні вразливості, що залишають мобільні пристрої вразливими до атак. Особливу небезпеку становлять атаки, спрямовані на визначення місцеперебування користувачів та примусове переведення пристроїв у менш захищені мережі, що може використовуватися як для стеження, так і для обмеження доступу до мобільних сервісів. Реалізація таких атак є відносно недорогою та можливою за допомогою доступного обладнання, що ускладнює боротьбу з подібними загрозами. Враховуючи, що мобільні технології продовжують розвиватися, а мережі 5G готуються до масового впровадження, виникає необхідність у вдосконаленні стандартів кібербезпеки. Дослідження спрямоване на аналіз актуальних загроз і пошук ефективних контрзаходів для підвищення рівня захищеності мобільних мереж, що робить його особливо важливим у сучасних умовах.

Метою статті є дослідження сучасних загроз для мобільних мереж четвертого покоління (4G/LTE), виявлення критичних вразливостей у протоколах доступу, що можуть використовуватися зловмисниками для порушення конфіденційності та доступності даних користувачів, а також розробка та обґрунтування ефективних методів захисту, які можуть мінімізувати ризики реалізації атак, забезпечити стабільність функціонування мобільних комунікаційних систем та підвищити рівень кібербезпеки в умовах стрімкого розвитку технологій зв’язку.

Об’єктом дослідження є вдосконалення методів захисту мобільних мереж четвертого покоління (4G/LTE) від атак, спрямованих на порушення конфіденційності, цілісності та доступності даних користувачів, з урахуванням сучасних вразливостей у протоколах мережевого доступу та особливостей функціонування мобільних комунікаційних систем.

Предмет дослідження – підходи до виявлення, аналізу та нейтралізації вразливостей мобільних мереж 4G/LTE, зокрема методи протидії атакам на конфіденційність користувачів, механізми забезпечення стійкості мережевих з’єднань і вдосконалення протоколів автентифікації та шифрування для підвищення рівня безпеки мобільного середовища.

Аналіз попередніх досліджень. Аналіз літературних джерел показує, що проблема захисту мобільних мереж від атак на конфіденційність і доступність є актуальною як для українських, так і для іноземних дослідників. Ковальчук О.В. досліджував атаки на автоматизовані системи управління та мережі в зоні бойових дій, аналізуючи загрози, що виникають через мобільні пристрої [1]. Серед іноземних авторів, Джонсон Л. у роботі «Advanced Security Techniques for Mobile Networks» запропонував алгоритми шифрування та аутентифікації для захисту мобільних мереж. Міллер Р. у дослідженні «Protecting Mobile Networks: Challenges and Solutions» розглянув комплексні стратегії протидії атакам на конфіденційність і доступність [2-3]. Таким чином, сучасні дослідження спрямовані на вдосконалення методів шифрування, аутентифікації та моніторингу мереж для забезпечення безпеки мобільних комунікацій.

Виклад основного матеріалу. У рамках дослідження розглядається спрощена архітектура мереж стандарту LTE, що включає ключові компоненти, необхідні для функціонування протоколів доступу між базовими станціями та мобільними пристроями, при цьому всі незначущі з точки зору аналізу атак аспекти архітектури свідомо опущені. Визначено три основні компоненти системи: користувацьке обладнання (User Equipment, UE), розширена універсальна наземна радіодоступова мережа (Evolved Universal Terrestrial Radio Access Network, E-UTRAN) та розширене пакетне ядро (Evolved Packet Core, EPC), які разом формують розширену пакетну систему (Evolved Packet System, EPS) відповідно до термінології 3GPP. Для спрощення викладу вся система узагальнено позначається як LTE (рис. 1) [1, 4].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

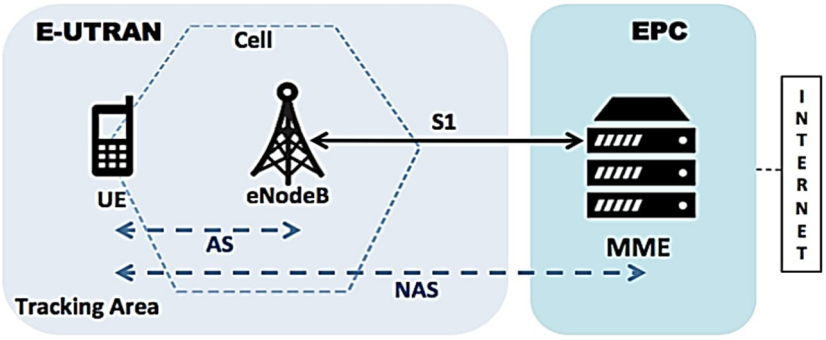


Рис. 1. Архітектура системи LTE

Джерело: агреговано на основі [1–2]

Користувацьке обладнання (UE) охоплює кінцеві пристрої зв'язку, такі як смартфони, які містять модуль ідентифікації абонента (Universal Subscriber Identity Module, USIM), що зберігає унікальний міжнародний ідентифікатор абонента (International Mobile Subscriber Identity, IMSI) та відповідні аутентифікаційні дані. Ці дані використовуються для ідентифікації користувача в мережі LTE та відіграють ключову роль у процесі аутентифікації, а також у генерації криптографічних ключів, які забезпечують захист сигналізації та передавання користувацьких даних через радіоінтерфейс.

E-UTRAN представлена базовими станціями, що здійснюють управління радіозв'язком між UE та мережею EPC. У межах стандарту LTE базові станції іменуються як «evolved NodeB» (eNodeB) і використовують набір протоколів рівня доступу (Access Stratum, AS) для обміну сигналізаційними повідомленнями з користувацькими пристроями. Основними функціями eNodeB є контроль радіоресурсів, організація сигналізації на рівні управління радіоресурсами (Radio Resource Control, RRC), реалізація механізмів безпеки радіоканалу, здійснення передачі даних на фізичному рівні та підтримка механізмів міжсотового переходу (handovers). Кожна базова станція eNodeB підключена до ядра EPC через інтерфейс S1.

Розширене пакетне ядро (EPC) відповідає за забезпечення функцій ядра мережі, що працює на основі IP-протоколу, та містить низку нових елементів, серед яких ключову роль відіграє сутність управління мобільністю (Mobility Management Entity, MME). MME забезпечує аутентифікацію користувачів і виділення ресурсів під час підключення пристроїв до мережі, а також виконує функції безпеки, такі як встановлення механізмів цілісності та шифрування сигналізаційних повідомлень. Крім того, MME здійснює контроль місцеперебування UE на макрорівні шляхом обробки сигналізації рівня Non-Access Stratum (NAS), яка використовується для взаємодії між UE та MME.

Розгортання компонентів LTE в межах географічного регіону (наприклад, у масштабах міста) здійснюється операторами мобільного зв'язку, які організовують покриття у вигляді так званих зон відстеження (Tracking Areas, TAs). Ці зони, аналогічні до зон місцеположення в мережах GSM, керуються MME та містять групу сот (cell), кожна з яких контролюється певним eNodeB. Базові станції eNodeB передають службові повідомлення (System Information Block, SIB), що містять інформацію про оператора зв'язку, код зони відстеження (Tracking Area Code, TAC), мобільний код країни (Mobile Country Code, MCC), код мережі (Mobile Network Code, MNC) та ідентифікатор соти (cell ID), що дозволяє UE ідентифікувати мережевого провайдера та ініціювати процес підключення.

Процес підключення UE до мережі реалізується через процедуру Attach, після успішного завершення якої пристрій отримує доступ до послуг відповідно до підписки користувача. Надалі, у процесі переміщення користувача в межах зони обслуговування мережі, UE використовує процедуру оновлення зони відстеження (Tracking Area Update, TAU), щоб інформувати мережу про зміну свого місцезнаходження.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

У сучасних мобільних мережах LTE одним із ключових аспектів безпеки є захист конфіденційності користувачів та забезпечення доступності мережевих послуг. Для мінімізації ризиків перехоплення особистих даних під час передачі через радіоканали використовується Глобальний унікальний тимчасовий ідентифікатор (GUTI), що замінює постійний IMSI та періодично змінюється, забезпечуючи анонімність трафіку. Додатково застосовується протокол аутентифікації та узгодження ключів (AKA), що гарантує цілісність і конфіденційність сигналізації та користувацьких даних. Однією з важливих процедур LTE, що може бути використана для атак на конфіденційність, є механізм пейджингу, який застосовується для визначення місцеперебування пристрою та доставки мережевих послуг. Зловмисники можуть перехоплювати пейджингові повідомлення, аналізуючи тимчасові ідентифікатори користувачів, що дозволяє здійснювати несанкціоноване стеження (рис. 2). Для зниження ризиків використовуються методи «розумного пейджингу» (Smart Paging), що обмежують область надсилання запитів лише до останньої відомої локації користувача [2–3].

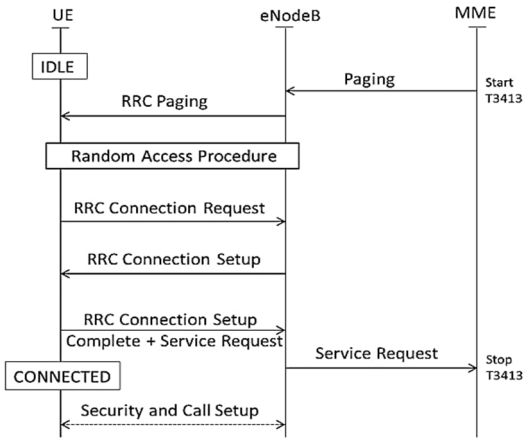


Рис. 2. Пейджинг в LTE в контексті сучасних методів захисту мобільних мереж від атак на конфіденційність і доступність

Джерело: агреговано на основі [1, 3]

Захист мобільних мереж LTE від атак передбачає протидію трьом основним загрозам: пасивним, напівпасивним та активним атакам. Пасивні атаки здійснюються шляхом перехоплення відкритих сигналізаційних повідомлень за допомогою програмно визначених радіосистем (USRP). Напівпасивні атаки поєднують моніторинг із можливістю ініціювання запитів, наприклад, через виклики або повідомлення в месенджерах, що дозволяє визначати місцеперебування абонента. Найбільш небезпечною є активна атака, під час якої зловмисники створюють фальшиві базові станції (rogue eNodeB) для перехоплення трафіку, примусової аутентифікації абонентів або переведення їх на менш захищені 2G/3G-мережі, що робить можливими атаки типу IMSI-catcher. Для протидії сучасним атакам мобільні оператори впроваджують комплексні заходи безпеки, що включають розширене шифрування сигналізації, вдосконалені методи аутентифікації, механізми динамічної ротації ідентифікаторів, а також технології розподіленого виявлення несанкціонованих базових станцій. Поєднання цих методів дозволяє значно підвищити рівень захисту мобільних мереж LTE та мінімізувати ризики компрометації конфіденційності користувачів. Сучасні методи захисту мобільних мереж від атак на конфіденційність і доступність зосереджені на запобіганні пасивним, напівпасивним і активним загрозам, які використовують відкриті програмні рішення та доступне радіообладнання. Поширення платформ OpenLTE і srsLTE підвищує ризики для безпеки мереж, дозволяючи зловмисникам здійснювати атаки.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Однією з найнебезпечніших загроз є використання фальшивих базових станцій (rogue eNodeB), що змушують пристрої підключатися до них шляхом маніпуляцій із сигналами пріоритетного вибору осередку (cell reselection). Це дає змогу атакувальникам перехоплювати конфіденційну інформацію та порушувати роботу мережі. Також загрозу становлять пасивні методи атак, що використовують програмно-визначене радіо (SDR) для перехоплення сигналізаційних повідомлень, ідентифікації тимчасових ідентифікаторів (GUTI) та відстеження абонентів. Особливо небезпечні атаки на процедури пейджингу в LTE, коли зловмисники можуть штучно ініціювати виклики або повідомлення, змушуючи мережу передавати дані про місцеперебування абонента. Використання «розумного пейджингу» (Smart Paging), хоча й зменшує сигналізаційне навантаження, водночас дозволяє точніше визначати геолокацію користувачів у невеликих комірках мережі. Додатково, атаки на механізм оновлення області відстеження (TAU) можуть примушувати пристрої розкривати свою останню зареєстровану локацію. Такі вразливості дозволяють зловмисникам будувати точні карти пересування користувачів та ідентифікувати їх у мережі. Окрім цього, атаки зниження рівня безпеки (bidding down attack) можуть змушувати пристрої переходити на менш захищені стандарти зв'язку, такі як 2G або незахищені версії LTE. Для протидії цим загрозам оператори впроваджують шифрування критично важливих сигналізаційних повідомлень та механізми аутентифікації базових станцій [4].

Для захисту мобільних мереж необхідно впроваджувати регулярну зміну GUTI, шифрування ідентифікаторів абонентів та вдосконалення алгоритмів автентифікації. Комплексний підхід, що включає раннє виявлення аномальної активності, є ключем до забезпечення конфіденційності та доступності мобільного зв'язку. Сучасні методи захисту мобільних мереж від атак на конфіденційність і доступність орієнтовані на протидію новим загрозам, що експлуатують особливості функціонування соціальних мереж, месенджерів та вразливості протоколів LTE.

Сучасні атаки використовують механізми ініціації запитів пейджингу (LTE Paging) через соціальні мережі та месенджери. Наприклад, у Facebook приховані повідомлення можуть викликати запит пейджингу, а в WhatsApp це може відбуватися при наборі тексту. Це дозволяє визначати місцезнаходження абонента. Уразливості протоколу управління радіоресурсами (RRC) у LTE відкривають можливості для перехоплення тимчасових ідентифікаторів абонентів (GUTI) та налаштування фальшивих базових станцій (rogue eNodeB). Крім того, повідомлення «Measurement Report» та звіти про збої радіозв'язку (RLF) можуть містити геолокаційні дані пристрою. Оператори мобільного зв'язку використовують різні стратегії обробки пейджингових запитів. Запити VoLTE охоплюють всю область відстеження (Tracking Area, TA), а IP-запити надходять лише до останньої зафіксованої комірки, що дозволяє зловмисникам ідентифікувати геолокацію користувачів. Пасивні та напівпасивні атаки дозволяють відстежувати переміщення користувачів за допомогою аналізу GUTI та ініціації запитів VoLTE або соціальних додатків. Активні атаки можуть визначати точне місцезнаходження абонента шляхом маніпуляцій із широкомовними повідомленнями або аналізу RRC-звітів. Ці атаки можуть бути використані для збору великих масивів даних про переміщення користувачів у режимі реального часу. Аналіз отриманих даних дозволяє зловмисникам створювати детальні карти пересування абонентів та виявляти їхні звички. Використання захищених каналів зв'язку та вдосконалених методів шифрування допомагає мінімізувати ризики витоку інформації [1].

Для ефективного захисту необхідне комплексне впровадження динамічної зміни GUTI, шифрування широкомовних ідентифікаторів, покращення алгоритмів автентифікації та виявлення аномальної активності у мережі. Атаки на конфіденційність і доступність мобільних мереж базуються на експлуатації вразливостей механізмів обміну службовими повідомленнями між користувацькими пристроями (UE) та базовими станціями (eNodeB). Зокрема, одним із поширених методів отримання інформації про місцезнаходження абонентів

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

є перехоплення звітів вимірювань (Measurement Reports) та звітів про втрату радіозв'язку (RLF Reports). У разі підключення абонента до фальшивої базової станції зловмисники можуть отримувати ці звіти у незахищеному вигляді, що дозволяє визначати рівень сигналу сусідніх комірок, а за наявності підтримки функції 'locationInfo-r10' – навіть GPS-координати пристрою. Використовуючи методи трилатерації, отримані дані дозволяють зловмисникам з високою точністю визначати географічне розташування цільового користувача. Додатково, атаки на сигнальні процедури можуть включати маніпуляції з повідомленнями про зміну області відстеження (TAU Request), що дозволяє вимагати від пристрою оновлення місцеперебування навіть без фактичного його переміщення. Це може призводити до витоку інформації про поточне місцезнаходження абонента та створювати умови для подальших цільових атак. Вразливості у протоколах радіодоступу LTE також дають змогу зловмисникам здійснювати атаки типу «bidding down», змушуючи пристрої знижувати рівень безпеки зв'язку до менш захищених стандартів. Для мінімізації подібних ризиків необхідне впровадження вдосконалених механізмів аутентифікації базових станцій та моніторинг аномальної поведінки трафіку на рівні операторських мереж.

Захист мобільних мереж від подібних атак вимагає комплексного підходу, що включає шифрування повідомлень управління радіоресурсами (RRC) з метою запобігання витоку критичних даних через незахищені канали зв'язку. Важливим напрямом є впровадження механізму динамічної зміни тимчасових ідентифікаторів абонентів (GUTI), що ускладнює відстеження переміщень користувачів навіть у разі перехоплення службових повідомлень. Крім того, покращення алгоритмів автентифікації здатне мінімізувати ймовірність підключення пристроїв до фальшивих базових станцій, що є основним механізмом проведення атак на мережеву безпеку. Додатково, критично важливим є впровадження систем виявлення аномальної активності в мережі, що дозволить оперативно ідентифікувати підозрілі запити пейджингу, а також виявляти спроби збору даних шляхом активного або пасивного моніторингу сигналізації. Обмеження можливості передавання незахищених звітів вимірювань та звітів про втрату сигналу є ще одним ефективним методом захисту, який може бути реалізований на рівні модифікації специфікацій LTE або через введення жорсткішого контролю доступу до GPS-даних [1, 3].

Сучасні мобільні мережі стикаються з атаками, що загрожують їхній конфіденційності та доступності, зокрема через вразливості LTE. Зловмисники використовують фальшиві базові станції (rogue eNodeB) для маніпуляцій із процедурами оновлення області відстеження (TAU) та підключення (Attach), що може призвести до відмови в обслуговуванні та блокування мобільного зв'язку. Для захисту необхідно впровадити криптографічний захист критичних повідомлень, підтвердження можливостей пристрою після автентифікації (AKA), динамічне оновлення ідентифікаторів користувачів (GUTI) та моніторинг аномальної активності. Лише комплексний підхід дозволить мінімізувати ризики атак і забезпечити стабільність мобільних мереж. Сучасний захист мобільних мереж від атак на конфіденційність і доступність вимагає комплексного підходу, оскільки компроміси між безпекою, продуктивністю та доступністю створюють численні вразливості [4]. Однією з головних загроз є атаки із застосуванням фальшивих базових станцій, які дозволяють зловмисникам перехоплювати незахищені дані користувачів і блокувати послуги шляхом маніпуляції процедурами оновлення області відстеження (TAU) та підключення (Attach).

Для мінімізації цих ризиків впроваджуються сучасні методи захисту, серед яких криптографічний захист сигналізаційних повідомлень, що унеможливлює їх перехоплення та підробку. Динамічне оновлення тимчасових ідентифікаторів (GUTI) допомагає запобігти відстеженню абонентів, тоді як удосконалені механізми перевірки мережевих можливостей пристроїв унеможливлюють атаки зі зниження рівня безпеки (bidding down attack). Додатковим рівнем захисту є впровадження цифрового підпису для критично важливих повідомлень, що підвищує їхню цілісність, а також розширене застосування публічно-

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ключових механізмів для забезпечення безперебійної роботи мережі. Водночас розвиток технологій мобільного зв'язку, зокрема впровадження 5G, відкриває нові можливості для динамічного та адаптивного захисту завдяки програмно-орієнтованій архітектурі та хмарним технологіям. Це дозволяє створювати гнучкі системи кібербезпеки, здатні ефективно протидіяти сучасним загрозам і забезпечувати надійний рівень конфіденційності та доступності мобільних комунікацій.

Висновки. Сучасні методи захисту мобільних мереж від атак на конфіденційність і доступність базуються на вдосконаленні стандартів безпеки та адаптації до нових загроз. Виявлені уразливості в протоколах LTE дозволяють зловмисникам реалізовувати атаки із застосуванням доступного обладнання, що створює загрози для абонентів. Основною причиною проблем є компроміс між безпекою, продуктивністю та доступністю, який потребує постійного коригування. Для нейтралізації загроз впроваджуються такі заходи: криптографічний захист сигналізаційних повідомлень, динамічне оновлення ідентифікаторів абонентів (GUTI), покращення механізмів автентифікації, запобігання атакам на зниження рівня безпеки та застосування цифрового підпису для критичних повідомлень. Завдяки оновленням від виробників та ініціативам 3GPP уже виправлено частину вразливостей. Надалі інтеграція адаптивних механізмів безпеки, використання хмарних технологій у межах 5G та глибша взаємодія розробників з операторами дозволять суттєво зміцнити захист мобільних комунікацій.

Список використаних джерел

1. Ковальчук О. В. Загрози мобільних мереж в умовах бойових дій та методи їх нейтралізації / О.В. Ковальчук // Інформаційна безпека та кіберзахист. – 2023. – № 2. – С. 67–75.

2. Johnson L. Advanced Security Techniques for Mobile Networks / L. Johnson // Journal of Cybersecurity. – 2021. – Vol. 15, No. 4. – P. 215–230.

3. Miller R. Protecting Mobile Networks: Challenges and Solutions / R. Miller // International Journal of Information Security. – 2022. – Vol. 18, No. 2. – P. 89–104.

4. C. Li, G. Tu, C. Peng, Z. Yuan, Y. Li, S. Lu, and X. Wang, "Insecurity of Voice Solution VoLTE in LTE Mobile Networks," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015, 2015, pp. 316–327.

Роботу виконано під науковим керівництвом PhD, старшого викладача
ШЕСТАКА Я. І.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ І ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОБУДОВИ СТІЙКОЇ КІБЕРБЕЗПЕКИ ФІНАНСОВИХ СЕРВІСІВ

СТЕПАНЕНКО Д. Д., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються розглядаються сучасні підходи до застосування блокчейн-технологій та штучного інтелекту у сфері фінансових технологій з метою підвищення рівня кібербезпеки цифрових фінансових сервісів. Зосереджено увагу на прикладах впровадження інновацій у міжнародних компаніях і фінансових екосистемах. Окремо проаналізовано нормативні ініціативи щодо підтримки фінансових інновацій, які сприяють цифровій трансформації фінансової галузі. Обґрунтовано роль блокчейну як засобу забезпечення прозорості, децентралізації та захисту даних у транзакціях, а також можливості використання штучного інтелекту для виявлення аномалій та автоматизованого реагування на кіберзагрози. Результати дослідження підтверджують потенціал інтеграції цих технологій для побудови стійкої системи кіберзахисту у фінансовому секторі.

The article examines modern approaches to the use of blockchain technologies and artificial intelligence in the field of financial technologies to enhance the cybersecurity of digital financial services. The focus is placed on examples of innovation implementation in international companies and financial ecosystems. Regulatory initiatives aimed at supporting financial innovations that facilitate the digital transformation of the financial sector are separately analyzed. The role of blockchain is substantiated as a means of ensuring transparency, decentralization, and data protection in transactions, along with the potential of artificial intelligence for anomaly detection and automated response to cyber threats. The research findings confirm the potential of integrating these technologies to build a resilient cybersecurity system in the financial sector.

Актуальність. У сучасних умовах стрімкої цифровізації фінансового сектору питання забезпечення кібербезпеки набуває критичного значення. Зростання кількості фінансових транзакцій в електронному середовищі, поширення мобільних платіжних систем, цифрових банків та платформ мікрокредитування супроводжується зростанням кіберзагроз, спрямованих на крадіжку даних, шахрайство та підрив довіри до фінансових інституцій. У цьому контексті особливої актуальності набуває інтеграція блокчейн-технологій і систем штучного інтелекту як інноваційних рішень для побудови стійкої та надійної системи кіберзахисту. Блокчейн дозволяє забезпечити незмінність, прозорість і контрольованість транзакцій, знижуючи ризики зовнішнього втручання та підробки фінансових записів. У свою чергу, штучний інтелект забезпечує інтелектуальний моніторинг, виявлення аномалій, прогнозування кіберзагроз та оперативне реагування на інциденти в режимі реального часу. Світова практика, зокрема досвід таких компаній, як Amazon, Alibaba, Tencent, а також законодавчі ініціативи окремих держав, підтверджують високу зацікавленість у розвитку фінансових технологій із вбудованими механізмами кібербезпеки. Тому дослідження застосування блокчейн-технологій і штучного інтелекту (ШІ) у сфері фінансових сервісів є не лише актуальним, а й стратегічно важливим для забезпечення довіри, стійкості та безперервності цифрової економіки.

Метою статті є дослідження інтеграції блокчейн-технологій і систем штучного інтелекту для побудови стійкої кібербезпеки фінансових сервісів шляхом аналізу їхніх функціональних можливостей у захисті транзакцій, протидії кібератакам, забезпеченні цілісності даних та підвищенні довіри до цифрових фінансових платформ.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Об'єктом дослідження є процес забезпечення кібербезпеки фінансових сервісів в умовах цифровізації за допомогою сучасних інформаційних технологій, зокрема блокчейн-платформ та систем штучного інтелекту.

Предмет дослідження – підходи до використання блокчейн-технологій і штучного інтелекту для підвищення рівня кібербезпеки у фінансових сервісах.

Аналіз попередніх досліджень. У сучасних дослідженнях, присвячених застосуванню блокчейн-технологій і штучного інтелекту для зміцнення кібербезпеки у фінансовому секторі, приділяється значна увага інтеграції інноваційних цифрових рішень у фінансову інфраструктуру. Провідні науковці аналізують потенціал блокчейну як децентралізованої платформи для зберігання транзакцій і штучного інтелекту як механізму адаптивного виявлення загроз.

У роботі Zhang X. і Liu Y. [1] представлено вдосконалену модель оцінювання кіберризиків у фінансових системах із використанням інтелектуальних алгоритмів. Дослідження фокусується на застосуванні методів машинного навчання для виявлення аномальної активності в транзакційних потоках, що дозволяє автоматизувати раннє виявлення потенційних загроз. Автори також розглядають можливість комбінування цих алгоритмів із блокчейн-системами задля підвищення прозорості та аудиту фінансових процесів.

Chen M. і Zhang H. у своїй статті [2] аналізують підходи до інтеграції нечіткої логіки в системи оцінювання інформаційної безпеки з урахуванням динамічних змін у поведінці кіберзагроз. Дослідники підкреслюють роль блокчейну як механізму захисту журналів подій та фінансових записів, що забезпечує незмінність і довіру між сторонами в електронному середовищі. Вони пропонують архітектуру, яка поєднує блокчейн із системами ШІ для підвищення адаптивності захисних механізмів.

У праці Gupta R. і Singh P. [3] обґрунтовується застосування аналітики великих даних та штучного інтелекту для кількісної оцінки кіберризиків у фінансових транзакціях. Автори підкреслюють важливість інтеграції блокчейн-технологій у системи виявлення шахрайства, зокрема при обробці великого обсягу транзакцій у реальному часі. Запропонована модель поєднує елементи прогнозної аналітики з децентралізованим зберіганням даних для забезпечення цілісності інформації.

Xu T. і Chen Z. у своїй статті [4] акцентують увагу на практичному впровадженні блокчейну у фінансові сервіси та його взаємодії з системами штучного інтелекту для посилення кіберзахисту. Автори описують архітектурні рішення для розмежування доступу до критичної інформації, що знижує ризик витоку даних. Особлива увага приділяється безпеці смарт-контрактів і механізмам їх перевірки на наявність уразливостей.

У дослідженні Wang P. і Chen H. [5] розглядається застосування когнітивних карт у процесі прийняття рішень щодо управління ризиками інформаційної безпеки. Робота демонструє, як штучний інтелект може формувати динамічні моделі загроз, а блокчейн слугувати середовищем для зберігання та перевірки політик безпеки. Автори роблять висновок, що поєднання цих технологій формує новий рівень захищеності для сучасних фінансових систем.

Таким чином, проаналізовані дослідження підтверджують актуальність і перспективність комплексного застосування блокчейн-технологій і штучного інтелекту в системах кібербезпеки фінансових сервісів. Наукові праці демонструють, що така інтеграція сприяє підвищенню стійкості до зовнішніх загроз, покращенню моніторингу транзакцій і формуванню довіри між учасниками цифрових економічних систем.

Виклад основного матеріалу. У сучасному цифровому середовищі, де фінансові сервіси все частіше переходять у онлайн-простір, зростає потреба у впровадженні новітніх технологій для захисту транзакцій, персональних даних та інфраструктури фінансових установ. Блокчейн і штучний інтелект, як окремо, так і у взаємодії, відкривають нові можливості для побудови надійної та стійкої кібербезпеки в галузі фінансових послуг [1, 4]. Блокчейн-технологія,

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

заснована на розподілених реєстрах, забезпечує незмінність даних, прозорість операцій і децентралізацію управління, що дозволяє ефективно протидіяти фальсифікаціям, шахрайству та несанкціонованим змінам у фінансових транзакціях [2]. Завдяки особливостям блокчейну, кожна операція фіксується одночасно в багатьох вузлах мережі, і будь-яка спроба її змінити або видалити автоматично виявляється і блокується, що формує довіру до цифрових сервісів без потреби у центральному посереднику.

Паралельно, стрімкий розвиток штучного інтелекту, зокрема технологій машинного навчання та обробки великих даних, дозволяє забезпечити динамічний аналіз поведінки користувачів, виявлення аномалій у транзакціях і прогнозування потенційних загроз у реальному часі [3]. Алгоритми ШІ здатні вивчати шаблони поведінки клієнтів, порівнювати їх із типовими сценаріями атак і оперативно реагувати на підозрілі дії, підвищуючи загальну ефективність кіберзахисту [5]. Саме поєднання блокчейну як механізму фіксації достовірних даних та штучного інтелекту як інструмента аналізу і прийняття рішень формує потужну синергію, яка здатна забезпечити стійкість фінансової системи до сучасних кіберзагроз.

Особливої уваги заслуговує потенціал застосування цих технологій у протидії відмиванню коштів (AML) і перевірці клієнтів (KYC). У той час як традиційні процедури вимагають значних людських і часових ресурсів, інтеграція блокчейн-платформ дозволяє створити спільну базу даних з прозорою історією транзакцій, а інструменти ШІ автоматизують процес ідентифікації ризикованих дій та суб'єктів [3]. Це не лише знижує операційні витрати фінансових установ, а й підвищує якість контролю за фінансовими потоками, зменшуючи ймовірність порушення міжнародних стандартів комплаєнсу.

Інтерес до застосування блокчейну та штучного інтелекту у фінансовому секторі зростає як серед приватних компаній, так і на рівні держав. Світові лідери фінансової галузі, серед яких Mastercard, JPMorgan Chase, Alibaba Group та інші, активно впроваджують ці технології у власні платформи для оптимізації транзакцій, захисту персональних даних і створення безпечного цифрового середовища. У країнах Європи та Азії на державному рівні ведуться дослідження щодо створення блокчейн-реєстрів для контролю фінансових операцій, цифрової ідентифікації та дотримання регуляторних вимог. Зокрема, впровадження концепцій Blockchain 1.0 (криптовалюти), 2.0 (смарт-контракти у фінансах) та 3.0 (застосування блокчейну за межами фінансової сфери) свідчить про динаміку еволюції цієї технології та її універсальність у контексті кібербезпеки [4]. На рис. 1 подано діаграму діяльності, яка відображає типовий сценарій роботи системи кіберзахисту на базі блокчейну та ШІ при обробці транзакцій користувача, виявленні загроз та прийнятті рішень щодо доступу.

Штучний інтелект також відіграє ключову роль у захисті інфраструктури фінансових сервісів, дозволяючи будувати автоматизовані системи виявлення загроз (IDS), прогнозування атак, оцінки ризиків та адаптивного управління доступом. Інтелектуальні механізми дозволяють зменшити вплив людського фактора, підвищити швидкість реагування на інциденти та підлаштовуватись під змінні умови ризикового середовища [3, 5]. Такі системи не лише ідентифікують відомі атаки, а й здатні виявити нові – на основі поведінкових аномалій та математичних закономірностей.

На рис. 2 представлено діаграму послідовності взаємодії ключових компонентів системи при виконанні захищеної фінансової операції з використанням блокчейну та механізмів машинного навчання. Діаграма демонструє порядок викликів і обміну повідомленнями між учасниками процесу при обробці транзакції: від ініціації користувачем до її підтвердження або блокування. Включено модулі: фінансова платформа, штучний інтелект, система доступу, блокчейн та сховище подій. Таким чином, це сприяє підвищенню обґрунтованості технічних рішень і дає змогу надалі формалізувати вимоги до реалізації програмних компонентів системи захисту.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

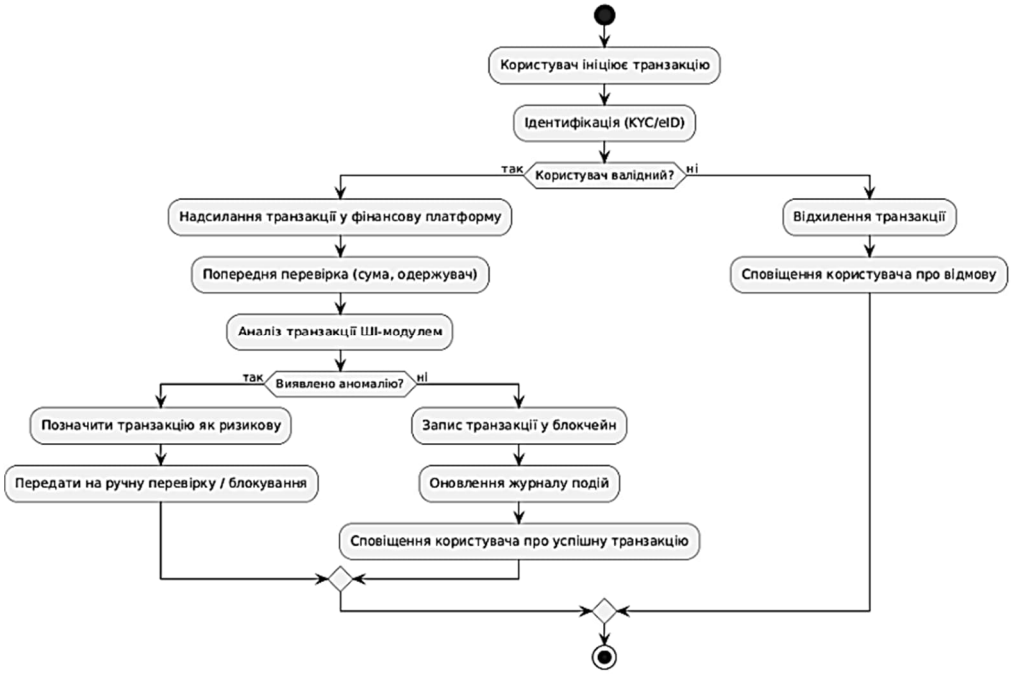


Рис. 1. Обробка фінансової транзакції з аналізом ШІ та записом у блокчейн

Джерело: розроблено автором в програмному середовищі PlantUML (знімок з екрану)

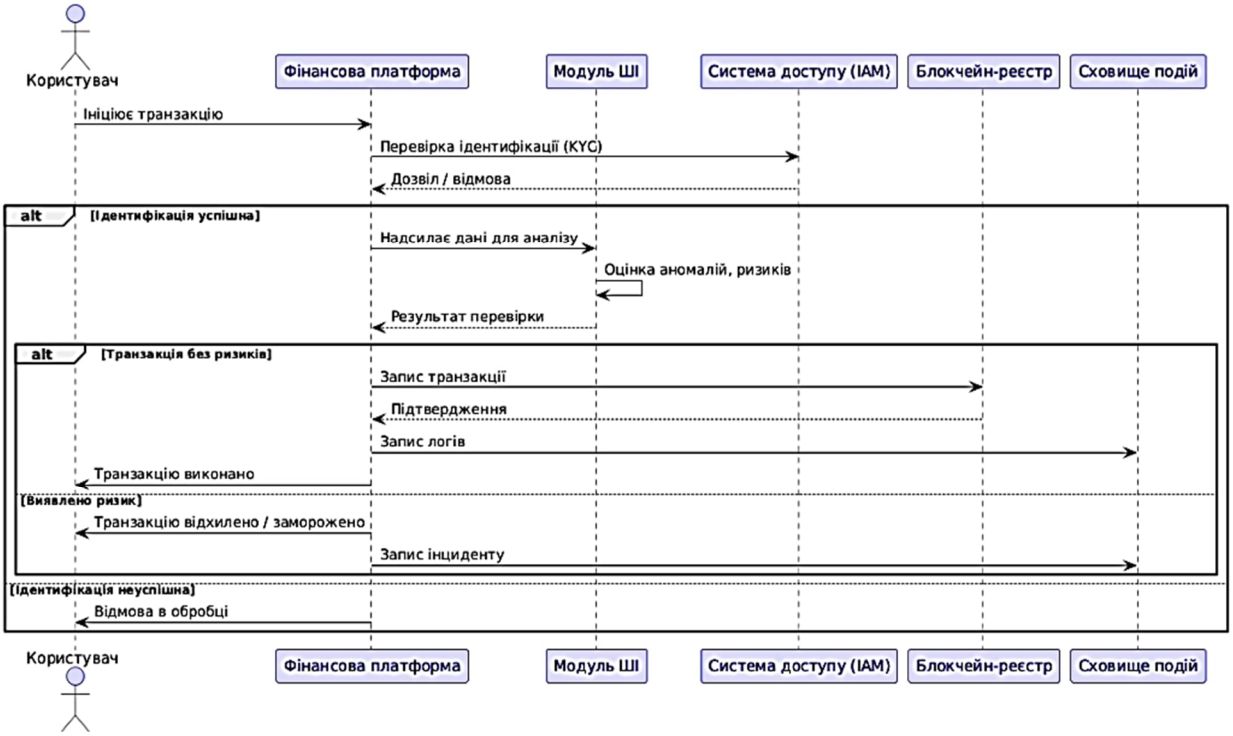


Рис. 2. Діаграма послідовності взаємодії компонентів системи кіберзахисту фінансових сервісів

Джерело: розроблено автором в програмному середовищі PlantUML (знімок з екрану)

У поєднанні, блокчейн і ШІ створюють підґрунтя для побудови нової цифрової архітектури фінансової безпеки, яка характеризується прозорістю, самодостатністю, гнучкістю та здатністю до масштабування [2]. Це особливо важливо в умовах активного

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

розвитку фінансових технологій (FinTech), які потребують надійних, захищених і масштабованих рішень для обробки транзакцій, зберігання чутливої інформації та відповідності зростаючим вимогам регуляторів. У найближчому майбутньому саме інтеграція блокчейн-платформ і інтелектуальних систем стане основою для створення цифрових фінансових сервісів нового покоління – прозорих, безпечних та орієнтованих на користувача.

У процесі побудови стійкої системи кіберзахисту фінансових сервісів, яка базується на використанні блокчейн-технологій і штучного інтелекту, важливо не лише визначити окремі компоненти архітектури, а й проаналізувати логіку їхньої взаємодії. Для цього доцільно застосовувати методи функціонального моделювання, що дозволяють формалізовано описати інформаційні потоки, логіку обробки даних, дії користувачів та механізми реагування на інциденти безпеки [4].

На рис. 3 представлено узагальнену модель інформаційних потоків (DFD – Data Flow Diagram), що ілюструє взаємодію між ключовими компонентами системи захисту фінансових сервісів. Користувачі ініціюють транзакції через фінансову платформу, яка верифікує запити за допомогою механізмів доступу та записує дані в блокчейн-реєстр для забезпечення прозорості, незмінності й контролю. Штучний інтелект аналізує поведінкові та транзакційні дані в режимі реального часу, виявляючи аномалії та потенційні кіберзагрози [5]. Результати аналізу передаються до системи управління доступом (IAM), яка динамічно оновлює політики безпеки. Дані зберігаються у захищеному сховищі, а доступ до журналів транзакцій та моніторингової інформації надається зовнішнім регуляторам для аудиту, аналізу AML/KYC та контролю комплаєнсу. У загальній архітектурі також передбачено інтеграцію з цифровими державними сервісами – електронною ідентифікацією (eID), цифровою валютою (CBDC) та API верифікації.

Рис. 3. DFD-схема архітектури кіберзахисту фінансових сервісів на основі блокчейн-технологій та штучного інтелекту

Джерело: розроблено автором в програмному середовищі PlantUML (знімок з екрану)

Значна кількість міжнародних фінансових установ вже використовують блокчейн і штучний інтелект не лише для оптимізації внутрішніх процесів, а й для забезпечення високого рівня кіберзахисту [1, 4]. Наприклад, компанія JPMorgan Chase запровадила власну блокчейн-

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

платформу Quorum, яка використовується для внутрішньобанківських трансакцій, міжбанківських розрахунків і контролю за відповідністю транзакцій нормативним вимогам. Завдяки цій платформі вдалося значно знизити навантаження на традиційні системи перевірки, пришвидшити обробку платежів і зменшити ризики несанкціонованих змін у фінансових даних.

Інший приклад – система Fraud Protection AI, яку впровадила компанія Mastercard. Вона базується на використанні машинного навчання для виявлення аномальної активності під час обробки транзакцій у режимі реального часу. Алгоритми ШІ аналізують поведінкові шаблони мільйонів користувачів, порівнюють їх із відомими сценаріями шахрайства і блокують підозрілі операції ще до їх завершення. Такий підхід дозволяє запобігати кібератакам на ранніх етапах, мінімізуючи шкоду для клієнтів і банків.

У секторі цифрових платежів компанія PayPal активно використовує інструменти штучного інтелекту для оцінки ризиків та боротьби з кіберзлочинністю [5]. Її система обробляє понад 1 000 сигналів ризику за одну транзакцію, враховуючи такі параметри, як геолокація, поведінка користувача, тип пристрою, історія покупок та багато іншого. У поєднанні з блокчейн-рішеннями для верифікації особистих даних це дозволяє створити багаторівневу модель безпеки, яка охоплює як клієнта, так і внутрішню інфраструктуру сервісу.

Таким чином, сучасна фінансова інфраструктура все більше орієнтується на інтеграцію інтелектуальних і децентралізованих рішень, що дозволяє не лише ефективно протидіяти існуючим кіберзагрозам, але й адаптуватися до нових викликів, які виникають в умовах цифрової трансформації. Від традиційного банкінгу до криптовалютних платформ і фінансових маркетплейсів – у всіх цих середовищах блокчейн і ШІ уже не просто інструменти підтримки, а критичні елементи захищеного функціонування фінансових сервісів.

Незважаючи на очевидні переваги, впровадження блокчейн-технологій і штучного інтелекту у фінансові сервіси пов’язане з низкою викликів і ризиків, які потребують комплексного аналізу та стратегічного підходу. Одним із ключових бар’єрів є відсутність єдиних міжнародних стандартів і нормативної бази, що регулює використання децентралізованих реєстрів і інтелектуальних систем у сфері кібербезпеки [3]. Нерівномірність правового регулювання між різними юрисдикціями ускладнює транскордонне застосування таких рішень, особливо у випадках, коли йдеться про обробку персональних даних, KYC/AML-вимоги або обіг цифрових валют.

Ще одним суттєвим викликом є проблема інтерпретованості рішень штучного інтелекту, особливо в питаннях фінансової відповідальності [5]. Системи ШІ, які приймають рішення на основі складних моделей машинного навчання (наприклад, нейронних мереж), не завжди можуть пояснити, чому саме було заблоковано ту чи іншу транзакцію. Це створює ризики юридичних спорів, утруднює аудит і гальмує повну автоматизацію процесів у сфері кіберзахисту. Щоб мінімізувати ці ризики, необхідно впроваджувати підходи explainable AI (пояснюваного ШІ), які дають змогу прозоро інтерпретувати поведінку алгоритмів.

Крім того, технологічна складність впровадження блокчейну в існуючі фінансові системи часто потребує масштабної перебудови IT-інфраструктури, додаткового навчання персоналу та суттєвих інвестицій [4]. Це особливо актуально для невеликих банків або фінансових компаній, які не мають достатнього бюджету чи експертизи для інтеграції таких рішень. Водночас навіть великі установи стикаються з проблемою масштабованості блокчейн-систем, коли збільшення кількості учасників або транзакцій призводить до зниження швидкості обробки та зростання вартості операцій.

Попри це, стратегічна значущість впровадження блокчейн- і AI-рішень у сферу фінансової кібербезпеки не викликає сумнівів. Очікується, що найближчими роками відбудеться формування гібридних моделей цифрової безпеки, в яких блокчейн відповідатиме за збереження цілісності даних і контроль доступу, а ШІ – за проактивне виявлення загроз,

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

моніторинг і адаптивне управління ризиками. Іншими словами, ідеться про створення інтелектуальної цифрової екосистеми, в якій кожен елемент має чітко визначену роль у забезпеченні комплексного захисту фінансових сервісів.

Окремий напрям досліджень стосується розробки архітектурних моделей для об'єднання блокчейну і ШІ в єдину платформу. У цьому контексті активно розглядаються децентралізовані автономні організації (DAO), які використовують смарт-контракти для автоматизованого прийняття рішень. Завдяки цьому можливо формувати новий підхід до управління цифровими активами та забезпечення їх безпеки без участі людини.

У контексті зростаючих загроз цифровій безпеці, фінансового шахрайства, кібертероризму та інформаційних маніпуляцій доцільність створення національних блокчейн-платформ є надзвичайно високою. Блокчейн як інфраструктурна технологія має потенціал не лише забезпечити прозорість і незмінність транзакцій, але й слугувати фундаментом для побудови довіри між державою, фінансовими установами, бізнесом та громадянами.

По-перше, національна блокчейн-платформа може стати ключовим інструментом для захисту державних фінансових даних, зокрема при розподілі бюджетних коштів, субсидій, соціальних виплат, пенсій і грантів. Фіксація кожної транзакції в блокчейні гарантує її повну простежуваність, а децентралізована архітектура знижує ризики підміни, корупції та фальсифікацій.

По-друге, така платформа може значно посилити нагляд за виконанням вимог фінансового моніторингу (AML/CFT) та перевірки клієнтів (KYC), у тому числі в межах відкритих банківських екосистем. Інтеграція із системами штучного інтелекту дозволить автоматизувати аналіз ризикових транзакцій, виявлення підозрілої поведінки та прогнозування потенційних загроз.

По-третє, державна підтримка у створенні блокчейн-платформи сприятиме розвитку національного FinTech-сектору, відкриє можливості для інновацій, стартапів і міжнародного партнерства. Це стане основою цифрового суверенітету в умовах глобальної конкуренції, коли залежність від іноземних технологічних рішень несе стратегічні ризики.

У перспективі, національна блокчейн-мережа може об'єднувати:

– цифрову валюту центрального банку (CBDC);
– єдиний реєстр транзакцій і активів (державних і приватних);
– систему електронної ідентифікації та підтвердження особи;
– цифрові смарт-контракти у публічних закупівлях, грантах і тендерах.

Враховуючи швидке зростання обсягів цифрових транзакцій, збільшення ризиків витоку персональних даних та глобальні тенденції до впровадження криптографічно захищених інфраструктур, створення національних блокчейн-платформ є стратегічно важливим кроком для забезпечення цифрової незалежності, прозорості та кіберстійкості країни в умовах війни та відновлення.

Висновки. Таким чином, хоча впровадження блокчейн-технологій і штучного інтелекту у фінансову сферу супроводжується технічними, організаційними та правовими викликами, у довгостроковій перспективі ці інструменти стають основою нової парадигми кібербезпеки – гнучкої, масштабованої, прозорої та здатної до самонавчання. Їх інтеграція не лише відповідає на сучасні загрози, а й формує підґрунтя для стійкого цифрового майбутнього фінансових сервісів у глобальній економіці. Такий підхід забезпечує не лише захист даних, але й підвищує довіру користувачів до цифрових фінансових платформ. На основі аналізу сучасних технологічних рішень можна стверджувати, що синергія блокчейну та ШІ є ефективною відповіддю на зростаючі кіберзагрози.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаних джерел

1. Zhang, X., & Liu, Y. Advanced Risk Management Models for Information Security Systems. Computer Science and Technology, 14(1), 2022, 23–29. https://doi.org/10.1007/s11390-022-1203-1.
2. Chen, M., & Zhang, H. Integrating Fuzzy Logic in Information Security Risk Assessment. Journal of Risk Analysis, 31(4), 2020, 202–211. https://doi.org/10.1111/risa.13568.
3. Gupta, R., & Singh, P. Cyber Risk Quantification and Mitigation Using Advanced Analytics. Springer, *2020*. https://doi.org/10.1007/978-3-030-53199-5.
4. Xu, T., & Chen, Z. Advanced Risk Management Methods in Cybersecurity and Information Protection. IEEE Access, 8, 2020, 105234–105242. https://doi.org/10.1109/ACCESS.2020.2999988.
5. Wang, P., & Chen, H. Fuzzy Cognitive Maps in Information Risk Management. International Journal of Intelligent Systems, 36(4), 2021, 1234–1252. https://doi.org/10.1002/int.22345.

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ЧУБАЄВСЬКОГО В. І.

ІНТЕГРАЦІЯ SIEM-СИСТЕМ ІЗ ЗАСОБАМИ РЕЗЕРВНОГО КОПІЮВАННЯ ТА ВИЯВЛЕННЯ АНОМАЛІЙ ДЛЯ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

СУРЖАНСЬКИЙ Д. Д., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті розглядається інтеграція систем управління інформаційною безпекою та подіями з засобами резервного копіювання та виявлення аномалій для підприємств критичної інфраструктури. Проаналізовано ключові функціональні можливості сучасних рішень для управління інформаційною безпекою, їхню роль у моніторингу та реагуванні на інциденти безпеки, а також тенденції їх еволюції, зокрема конвергенцію з аналітикою великих даних. Визначено зовнішні фактори, що впливають на розвиток систем управління інформаційною безпекою та подіями у середньо- та довгостроковій перспективі. Запропоновано перелік потенційних удосконалень для підвищення ефективності цих систем у забезпеченні безпеки процесів резервного копіювання, що сприятиме зміцненню кіберстійкості підприємств критичної інфраструктури.

The article examines the integration of information security and event management systems with backup and anomaly detection tools for critical infrastructure enterprises. It analyzes the key functional capabilities of modern information security management solutions, their role in monitoring and responding to security incidents, as well as trends in their evolution, particularly the convergence with big data analytics. External factors influencing the development of information security and event management systems in the medium- and long-term perspectives are identified. A list of potential improvements to enhance the effectiveness of these systems in securing backup processes is proposed, which will contribute to strengthening the cybersecurity resilience of critical infrastructure enterprises.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Актуальність. Ризики кібербезпеки для підприємств критичної інфраструктури невпинно зростають унаслідок активізації діяльності як державних суб'єктів, що здійснюють цілеспрямовані кібероперації, так і організованих злочинних угруповань, що спеціалізуються на атаках із використанням сучасних методів компрометації інформаційних систем. При цьому зловмисники застосовують дедалі складніші техніки атак, серед яких варто виокремити програми-вимагачі, спрямовані на шифрування критично важливих даних з метою отримання викупу, компрометацію корпоративної електронної пошти через перехоплення облікових записів або фальсифікацію аутентифікаційних даних, фішингові кампанії, націлені на отримання конфіденційної інформації, а також складні атаки соціальної інженерії, що реалізуються шляхом маніпулювання поведінкою користувачів. Внаслідок цього суттєво ускладнюється як ідентифікація аномальних активностей у мережах підприємств, так і оперативне реагування на виявлені інциденти, що, своєю чергою, створює потенційну загрозу стабільності критично важливих бізнес-процесів. Ефективний кіберзахист промислових інформаційних систем потребує інтеграції систем управління інформаційною безпекою та подіями (SIEM), що дозволяють здійснювати моніторинг у реальному часі та аналіз аномалій. Проте традиційні SIEM-рішення мають обмеження, зокрема щодо інтеграції з системами резервного копіювання, що є критичним для забезпечення цілісності даних у разі атак. Таким чином, дослідження інтеграції SIEM-систем із засобами резервного копіювання та виявлення аномалій є надзвичайно актуальним, оскільки воно спрямоване на розроблення та впровадження комплексних рішень для підвищення рівня кіберстійкості підприємств критичної інфраструктури. Оптимізація взаємодії між цими компонентами дозволить не лише автоматизувати процеси моніторингу та реагування на атаки, а й значно зменшити ризики втрати даних та мінімізувати наслідки кібератак, що, у свою чергу, сприятиме підвищенню загальної ефективності інформаційної безпеки підприємств, що функціонують у критично важливих секторах економіки.

Метою статті є дослідження інтеграції SIEM-систем із засобами резервного копіювання та виявлення аномалій в контексті підвищення кібербезпеки підприємств критичної інфраструктури, зокрема шляхом аналізу їхніх основних функціональних можливостей, обмежень, а також виявлення потенційних шляхів удосконалення для більш ефективного управління кіберзагрозами та забезпечення безпеки даних.

Об'єктом дослідження є стратегія інтеграції SIEM-систем із засобами резервного копіювання та виявлення аномалій для підвищення рівня кібербезпеки підприємств критичної інфраструктури, з урахуванням сучасних викликів та вимог до захисту даних і стабільності операційних процесів.

Предмет дослідження – підходи до інтеграції SIEM-систем із засобами резервного копіювання та виявлення аномалій, які забезпечують підвищення ефективності управління кіберризиками та захисту критичної інфраструктури підприємств.

Аналіз попередніх досліджень. Аналіз літератури щодо інтеграції систем управління інформаційною безпекою та подіями (SIEM) із засобами резервного копіювання та виявлення аномалій для підприємств критичної інфраструктури вказує на кілька важливих напрямків розвитку. Згідно з дослідженнями Chen et al. та Zhao and Sun, сучасні SIEM-системи активно інтегрують новітні технології для покращення моніторингу безпеки та аналізу великих даних. Це дозволяє значно підвищити ефективність виявлення загроз і автоматизувати реагування на інциденти. Також важливим є внесок українських вчених Жигаревич О. і Смирнова Т., які досліджують особливості інтеграції інформаційних систем для забезпечення безпеки підприємств критичної інфраструктури [1]. Їхні роботи сприяють розвитку концепції синергетичної взаємодії різних компонентів інформаційних систем для оптимізації процесів резервного копіювання та виявлення аномалій.

Виклад основного матеріалу. Системи управління інформаційною безпекою та подіями (SIEM) були розроблені з метою допомоги адміністраторам у розробці політик безпеки та

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

управлінні подіями з різних джерел. Зазвичай, базова SIEM-система складається з окремих блоків (наприклад, джерело даних, збір журналів, нормалізація та парсинг, механізм правил, зберігання журналів, моніторинг подій), які можуть функціонувати незалежно один від одного. Однак без їх узгодженої роботи SIEM-система не буде функціонувати належним чином. Рис. 1 ілюструє основні компоненти звичайного рішення SIEM, яка є комплексним інструментом для забезпечення кібербезпеки підприємств критичної інфраструктури, що здійснює моніторинг, збір та аналіз інформації про події в системах безпеки [1-2]. Основними компонентами цієї системи є збір даних, кореляція подій, аналіз загроз, управління інцидентами, зберігання та архівація даних, а також звітування та моніторинг, що забезпечують її ефективну роботу.

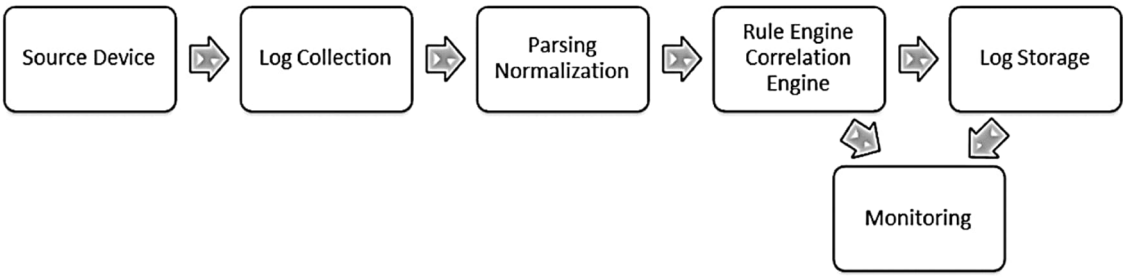


Рис. 1. Основні компоненти SIEM-системи та їх взаємодія для забезпечення кібербезпеки підприємств критичної інфраструктури

Джерело: агреговано на основі [2]

SIEM-система збирає дані, корелює події, аналізує загрози, керує інцидентами та забезпечує зберігання інформації, що дозволяє ефективно виявляти та нейтралізувати загрози для підвищення кібербезпеки підприємств критичної інфраструктури. Платформи SIEM (управління інформацією та подіями безпеки) надають можливість аналізувати події безпеки в режимі реального часу, що генеруються мережею пристроїв та додатків. Незважаючи на те, що нове покоління SIEM-систем надає можливість автоматизувати вибір та впровадження контрзаходів, існуючі системи реагування вибирають і впроваджують заходи безпеки без проведення всебічного аналізу впливу атак і сценаріїв відповіді. Для відображення сучасних інструментів SIEM-систем з характеристиками, можна побудувати таблицю, що включатиме актуальні рішення на ринку, їхні основні функції та особливості (табл. 1).

Таблиця 1

Інтеграція SIEM-систем із засобами резервного копіювання та виявлення аномалій для підприємства критичної інфраструктури

№ п/п	Інструмент SIEM	Основні функції	Особливості
1	Splunk Enterprise Security	Збір даних, індексація, візуалізація, аналітика безпеки	Високі можливості для обробки великих обсягів даних, машинне навчання, інтеграція з іншими **системами**
2	IBM QRadar	Моніторинг подій в реальному часі, кореляція загроз	Підтримка хмарних середовищ, інтеграція з іншими технологіями IBM, підтримка загроз в реальному часі

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

№ п/п	Інструмент SIEM	Основні функції	Особливості
3	ArcSight Enterprise Security Manager	Кореляція подій, розслідування, автоматичні сповіщення	Підтримка складних правил кореляції, інтеграція з різними пристроями, слабка візуалізація
4	LogRhythm NextGEN SIEM	Моніторинг кінцевих точок, аналітика поведінки, реагування	Масштабованість, підтримка децентралізованих архітектур, обмежена для критичних інфраструктур
5	McAfee Enterprise Security Manager	Реальне розслідування, моніторинг додатків та баз даних	Інтеграція з іншими продуктами McAfee, вимога додаткових рішень для розширення функціональності
6	SolarWinds Log & Event Manager	Централізований збір журналів, нормалізація, автоматизоване виявлення загроз	Підтримка реального часу, але обмежена підтримка хмарних рішень IaaS і SaaS
7	RSA NetWitness Platform	Моніторинг мережі, аналіз загроз, аналіз поведінки людей і процесів	Сильні можливості для моніторингу OT (операційні технології), складність в налаштуванні та масштабуванні

Джерело: згенеровано на основі [2–3]

У рамках інтеграції з системами резервного копіювання та виявлення аномалій важливо забезпечити безперервний моніторинг всіх інцидентів, що виникають у результаті атаки або несанкціонованого доступу до даних. Завдяки розширеному аналізу поведінки користувачів та системи виявлення аномалій, SIEM-системи здатні своєчасно ідентифікувати потенційні загрози, що можуть вплинути на збереження та відновлення даних. Водночас для ефективної роботи з великими обсягами інформації необхідно забезпечити можливість масштабування таких систем, що дозволяє підтримувати стабільність функціонування в умовах зростаючого навантаження. Окрім цього, важливим елементом є інтеграція з іншими елементами корпоративної інфраструктури для забезпечення синергетичного ефекту від роботи різних інструментів безпеки [2]. У майбутньому розвиток SIEM-систем дозволить інтегрувати їх з більш широким спектром технологій для вдосконалення безпеки та надійності критичної інфраструктури підприємства.

SIEM-системи (системи управління інформаційною безпекою та подіями) мають потужний потенціал для інтеграції з іншими важливими інструментами безпеки, такими як системи резервного копіювання та виявлення аномалій. Основною функцією SIEM є збір, зберігання та кореляція подій, згенерованих різними елементами інфраструктури, що дозволяє створювати єдину точку моніторингу для виявлення можливих загроз. Для ефективної інтеграції з системами резервного копіювання та виявлення аномалій важливою є здатність SIEM до обробки та аналізу даних в реальному часі, що дозволяє швидко реагувати на інциденти, що виникають у процесах зберігання даних [3]. Потужні правила кореляції у SIEM-системах дають змогу виявляти складні патерни та аномалії в поведінці користувачів та додатків, що допомагає оперативно ідентифікувати порушення у процесах резервного копіювання, а також виявляти потенційні атаки.

Ще однією важливою особливістю SIEM є підтримка множинних джерел даних, що дозволяє отримувати інформацію з різних компонентів інфраструктури, таких як датчики, програми для резервного копіювання та інші пристрої. Це дає можливість інтегрувати SIEM з існуючими системами для безперервного моніторингу та збереження даних. Зокрема, аналіз поведінки користувачів і застосунків за допомогою машинного навчання дозволяє виявляти аномалії в процесах резервного копіювання та зберігання, що підвищує ефективність виявлення загроз.

Крім того, для роботи з великими обсягами даних важливою є здатність SIEM-систем зберігати дані протягом тривалого часу та виконувати аналітичні операції, що дозволяє

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

здійснювати глибокий аналіз інцидентів без ризику втрати критичних даних. Візуалізація даних, яку підтримують сучасні SIEM-системи, також є важливим елементом інтеграції з системами резервного копіювання та виявлення аномалій, оскільки дозволяє адміністраторам швидко оцінити стан інфраструктури і виявити порушення або потенційні загрози.

Одним з ключових аспектів інтеграції SIEM з іншими системами є функціонал для автоматичної реакції на інциденти та генерування звітів. Це дозволяє не тільки вчасно реагувати на загрози, пов'язані з резервним копіюванням та аномаліями, але й підвищує ефективність збереження даних та відновлення їх у разі інцидентів. Крім того, важливою є здатність SIEM забезпечувати захист даних, зокрема, для підприємств критичної інфраструктури, де вимоги до безпеки даних є особливо високими.

Інтеграція SIEM-систем із засобами резервного копіювання та виявлення аномалій для підприємства критичної інфраструктури є важливим кроком у забезпеченні комплексної безпеки. Попри потужні можливості сучасних SIEM-систем, такі як кореляція даних, зберігання, візуалізація та автоматизація реагування, існують значні обмеження, зокрема недостатня інтеграція даних та обмежена здатність до аналізу складних загроз. Більшість існуючих SIEM-систем не здатні забезпечити повну обробку та кореляцію даних, що призводить до великої кількості хибнопозитивних та хибнонегативних спрацьовувань [1, 3].

Зокрема, багато SIEM-систем не охоплюють всі типи даних, необхідних для ефективного виявлення інцидентів, таких як журнали DNS, дані з кінцевих точок або електронної пошти, що обмежує їхню здатність до виявлення загроз. Оскільки персональні дані не завжди можна розкривати згідно з вимогами GDPR, SIEM-системи мають враховувати ці обмеження, забезпечуючи достатній рівень інформації для аналізу загроз. Іншим важливим аспектом є використання основних кореляційних правил у SIEM-системах. Поточні правила кореляції є досить базовими і не здатні обробляти складні атаки, такі як zero-day. Для покращення цієї ситуації майбутні SIEM-системи повинні включати вдосконалені механізми кореляції, які дозволяють зменшити кількість хибних спрацьовувань і точно виявляти аномалії. Щодо зберігання даних, існуючі системи часто обмежуються зберіганням лише певних типів даних на обмежений час, що ускладнює виявлення атак, які можуть бути виявлені лише через кілька місяців. Тому необхідно розробляти SIEM-системи, які дозволяють більш гнучко налаштовувати політики зберігання та архівації даних, забезпечуючи їхню безпеку і конфіденційність.

Не менш важливим є автоматизація процесу реагування на інциденти. Сучасні SIEM-системи все ще залежать від людського втручання для аналізу та прийняття рішень щодо загроз. Однак, для підвищення ефективності та швидкості реагування необхідно впроваджувати автоматичні механізми, що забезпечують швидке виявлення атак та автоматичне застосування контрзаходів. Таким чином, для покращення безпеки критичної інфраструктури підприємств, майбутні SIEM-системи повинні забезпечити кращу інтеграцію з іншими засобами безпеки, вдосконалити алгоритми кореляції та зберігання даних, а також автоматизувати процес реагування на інциденти.

Під час аналізу сучасних SIEM-систем було виявлено, що можливості звітності та візуалізації даних обмежені, що ускладнює ефективне видобуття корисних інсайтів з величезної кількості даних, які збираються системами. Більшість візуалізацій є загальними, не враховують специфічні потреби користувачів або занадто спрощені для значного впливу на використання зібраних даних. Крім того, існуючі системи не мають можливості ефективно обробляти різноманітні типи даних, такі як результати статистичного моделювання, збори OSINT або моделі поведінки користувачів. Для покращення візуалізації SIEM-системи мають зосередитися на гнучких платформах, здатних працювати з кількома джерелами даних, що мають різноманітні характеристики та змінюються в реальному часі.

У майбутньому розвиток SIEM-систем залежатиме від багатьох факторів, серед яких політичні, економічні, соціальні, технологічні, правові та екологічні. Політичні фактори, такі

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

як закони, що регулюють кібербезпеку, можуть сприяти розвитку інвестицій у цей сектор. Наприклад, Європейська комісія оголосила про збільшення інвестицій у кібербезпеку, що може вплинути на розвиток SIEM-систем. Економічні фактори, зокрема зміни у трудових відносинах і зростання кількості фрілансерів, також можуть вимагати адаптації SIEM-систем до нових реалій. Зростання попиту на робочі місця в галузі кібербезпеки підвищує важливість SIEM-систем для компаній [1].

Зі зміною соціальних звичок, зокрема активним використанням соціальних мереж, розширюється джерело даних для аналізу безпеки, що створює нові виклики для SIEM-систем. Технологічні фактори, зокрема розвиток мобільних технологій, хмарних обчислень та великі дані, також відіграють важливу роль у розвитку SIEM-систем, оскільки вони забезпечують нові можливості для зберігання та обробки даних. Зокрема, технології, такі як машинне навчання та Інтернет речей (IoE), можуть значно покращити точність виявлення аномалій та реагування на інциденти безпеки.

Правові фактори, зокрема регулювання захисту даних, можуть вплинути на майбутнє SIEM-систем. Наприклад, нові правила захисту персональних даних в Європейському Союзі можуть визначити необхідність удосконалення SIEM-систем для відповідності цим вимогам. Ці фактори разом утворюють складну картину для майбутнього розвитку SIEM-систем, що включає інтеграцію з новими технологіями та вимогами безпеки [2].

Для розуміння того, як регулювання може вплинути на дані, які збираються SIEM-системами, можна, наприклад, розглянути, як Європейська Комісія визначає роль IP-адреси в мережі (що часто аналізується засобами безпеки). В Інтернеті кожен комп'ютер ідентифікується за допомогою числової IP-адреси формату A.B.C.D, де A, B, C і D є числами. Таке регулювання обов'язково враховує обробку даних, які можуть бути пов'язані з ідентифікацією особи, зокрема у випадках, коли обробка IP-адрес відбувається з метою виявлення користувачів комп'ютерів, наприклад, для порушення авторських прав.

Зважаючи на ці фактори, методи обробки та зберігання даних у SIEM-системах повинні відповідати вимогам щодо захисту даних, зокрема щодо того, де зберігаються ці дані та яким чином вони захищені. Розвиток SIEM-систем у майбутньому вимагатиме інтеграції з іншими технологіями для поліпшення здатності до виявлення аномалій та ефективнішої обробки даних. Зокрема, впровадження обробки даних з OSINT (Open Source Intelligence) може покращити здатність системи виявляти загрози, шляхом аналізу ключових слів, що свідчать про загрози, таких як «DDoS», «порушення безпеки», «витік» та інших [2-3].

З точки зору візуалізації, для покращення можливостей існуючих SIEM-систем пропонується розробка спеціалізованих моделей візуалізації, які можуть обробляти різноманітні типи даних, включаючи високорозмірні, тимчасові, текстові, просторові та реляційні дані. Також необхідно розробити механізми для реального часу аналізу даних і прийняття рішень, зокрема для обробки динамічних даних, таких як потоки системних журналів або OSINT-дані.

Що стосується архівації даних, зберігання застарілих даних у SIEM може бути дорогим та створювати проблеми з безпекою і надійністю. Тому для вирішення цих проблем пропонується створити розширення для SIEM-систем, яке б забезпечувало надійне, гнучке і безпечне архівування даних, використовуючи публічні хмари (наприклад, Amazon S3, Windows Azure).

У контексті інтеграції з іншими системами безпеки, такими як системи оркестрації безпеки, автоматизації і реагування на інциденти (SOAR), майбутні SIEM-системи повинні адаптуватися до інтеграції з новими рішеннями, що дозволяють динамічно взаємодіяти на всіх етапах обробки інцидентів, швидко реагувати на загрози та атаки.

Для покращення можливостей виявлення, кореляції та реакції наступне покоління SIEM-систем має інтегрувати технології ШІ/МШ у свої основні механізми. Технології ШІ в SIEM-системах пропонують прогностичні можливості, особливо корисні для аналізу

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

аномальної поведінки мережевого трафіку, інструментів і користувачів. Деякі сучасні SIEM-рішення, такі як LogRhythm NextGen SIEM Platform та QRadar SIEM, використовують машинне навчання (МШ) для вивчення загроз та відхилень атак. Крок уперед у виявленні, пом'якшенні та запобіганні кіберзагрозам – це інтеграція ШІ/МШ у рішення SOAR, що мають бути ідеально інтегровані в платформу SIEM. Системи оборони на основі ШІ/МШ здатні аналізувати великі обсяги даних і виявляти підозрілі шаблони в режимі реального часу. Основні напрямки застосування ШІ/МШ включають виявлення вторгнень, фішинг та спам, виявлення загроз та аналіз поведінки користувачів. ШІ-орієнтовані SIEM-системи можуть ухвалювати рішення або змінювати свою поведінку, що покращує можливості виявлення, скорочує залежність від ручного втручання та мінімізує кількість помилкових спрацьовувань, оскільки алгоритми здатні точно класифікувати дані як нормальні чи аномальні. Ідеально, наступне покоління SIEM-систем повинно поєднувати аналіз, заснований на правилах, із методами, що надаються технологіями ШІ, для виявлення відхилень користувачів, аномалій у діяльності та відповіді на загрози.

Інтеграція SIEM-систем із платформами для розширеного виявлення та реагування (XDR) очікується, щоб забезпечити дві взаємодоповнюючі функції: (i) забезпечення відповідності та еволюція SIEM для служби більш широкої платформи для виявлення та управління ризиками загроз, та їх фокусування XDR на загрозах і наданні платформи для глибшого та вузького виявлення загроз. Це дозволить організаціям отримати детальну інформацію про мережеву активність або діяльність користувачів для точнішого виявлення загроз. Інтеграція SIEM-систем з засобами резервного копіювання та виявлення аномалій є важливим елементом забезпечення безпеки та надійності для підприємств критичної інфраструктури. SIEM-системи (Security Information and Event Management) дозволяють централізовано збирати, зберігати та аналізувати дані про події в інформаційних системах підприємства. Вони допомагають оперативно виявляти підозрілі або аномальні події, що можуть свідчити про спроби несанкціонованого доступу або кіберзагрози [1-3]. Інтеграція з механізмами резервного копіювання дозволяє забезпечити додатковий рівень захисту даних, автоматично виявляючи порушення в процесі збереження інформації та даючи змогу відновлювати втрачені чи пошкоджені дані. Засоби резервного копіювання є критично важливими для підтримки цілісності та доступності даних, що особливо актуально для підприємств, що працюють з критичними даними. Інтеграція SIEM з резервним копіюванням дозволяє вчасно виявити спроби маніпуляцій з резервними копіями, такі як злом або несанкціоноване видалення важливих даних. Це дозволяє миттєво вжити заходів для блокування доступу або відновлення резервних копій без втрати критичних даних.

Виявлення аномалій є ключовим елементом в рамках такої інтеграції. SIEM-система постійно моніторить мережевий трафік, користувацькі дії та зміни в системах, порівнюючи їх з нормами поведінки. Використовуючи алгоритми для аналізу даних, SIEM здатна виявити будь-які аномальні патерни, що можуть свідчити про кіберзагрози, спроби вторгнення або інші зловмисні дії. Коли система виявляє аномалії, ці події автоматично передаються до централізованої системи, де відбувається їх подальший аналіз та реагування. Це може включати блокування підозрілих дій, сповіщення безпекових спеціалістів або відновлення даних із резервних копій, щоб мінімізувати збитки від потенційного інциденту.

Переваги інтеграції SIEM із засобами резервного копіювання та виявлення аномалій очевидні. Вона забезпечує цілісність та безпеку даних, дозволяючи оперативно реагувати на загрози та знижуючи час на відновлення після інцидентів. Водночас така інтеграція автоматизує процеси моніторингу, аналізу та реагування на події, що дозволяє швидше виявляти потенційні загрози та вживати заходів для їх нейтралізації.

Висновки. Інтеграція SIEM-систем із засобами резервного копіювання та виявлення аномалій є важливим елементом для забезпечення безпеки критичної інфраструктури підприємства. З огляду на аналіз ризиків і впровадження, необхідно розробити ефективні

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

методи та інструменти для аналізу та оцінки безпеки, а також оптимального розгортання різноманітних засобів захисту, що включають багаторівневі метрики ризиків. Водночас важливо розробити структуру для розгортання резервних датчиків, що дозволяє забезпечити додатковий рівень безпеки. Аналізуючи можливості сучасних рішень, можна відзначити, що більшість з них мають зручні інтерфейси, однак їх можливості з візуалізації та реагування обмежені через велику кількість зібраних подій. Тому для досягнення більш високого рівня ефективності необхідно впроваджувати додаткові функції для глибшого аналізу та візуалізації, що дозволяє користувачам приймати обґрунтовані рішення та оперативно реагувати на загрози. Щодо зберігання даних, хоча більшість рішень мають можливості для належного зберігання, обмеження апаратних ресурсів і необхідність додаткових продуктів підвищують вартість впровадження. Перспективними є рішення на основі хмарного зберігання для довгострокового архівування SIEM-даних, що дозволяють оптимізувати політики зберігання та знизити витрати.

Враховуючи вплив політичних, економічних, соціальних, технологічних, екологічних і правових факторів на критичну інфраструктуру, можна зробити висновок, що наявність належних умов для інвестування в розвиток і вдосконалення SIEM-систем створює можливості для забезпечення не лише безпеки промислових контрольних систем, але й для надання послуг з кібербезпеки малим і середнім підприємствам, які мають обмежені ресурси та знання у сфері безпеки. Інтеграція цих систем дозволяє створити більш гнучку та ефективну модель безпеки для підприємств критичної інфраструктури, що вимагають високого рівня захисту від кіберзагроз.

Список використаних джерел

1. Жигаревич О., Смирнова Т. Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури / О. Жигаревич, Т. Смирнова // Сучасні технології в безпеці інформаційних систем. – 2020. – № 1. – С. 12–19.

2. Щербань О.В., Литвиненко О.В. Системи збору інформації про безпеку та управління подіями (SIEM) як інструмент забезпечення кібербезпеки підприємств // Інформаційні технології та комп’ютерна інженерія. – 2019. – № 2. – С. 112–119.

3. «Системи керування інцидентами інформаційної безпеки (SIEM/SOC)» // DNAOП. – 2021. – Режим доступу: https://dnaop.com/article/cat31/sistemi-keruvannya-incidentami-informaciinoyi-bezpeki-siem-soc/ (останнє звернення 14.03.2025р.)

Роботу виконано під науковим керівництвом PhD, старшого викладача
ШЕСТАКА Я. І.

АНАЛІЗ ІНТЕГРАЦІЇ DORA В УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ПІДПРИЄМСТВ

ТКАЧЕНКО О. В., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

Стаття присвячена дослідженню інтеграції цифрової оперативної стійкості в управління ризиками та стратегії безперервності бізнесу. Аналізуються стратегії та практики впровадження цього акта в корпоративне управління ризиками, зокрема в малих і

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

середніх підприємствах. Розглядається адаптація його принципів для підвищення рівня кібербезпеки, зменшення ризиків і забезпечення стабільної діяльності в кризових ситуаціях. Окрема увага приділена інтеграції заходів безпеки в операційні процеси та корпоративну культуру. Підкреслюється важливість комплексного підходу до управління ризиками в умовах цифрової трансформації.

The article explores the integration of the Digital Operational Resilience Act (DORA) into risk management and business continuity strategies. It analyzes the strategies and practices for implementing this act in corporate risk management, particularly in small and medium-sized enterprises. The study examines the adaptation of its principles to enhance cybersecurity, mitigate risks, and ensure stable operations during crises. Special attention is given to the integration of security measures into operational processes and corporate culture. The importance of a comprehensive approach to risk management in the context of digital transformation is emphasized.

Актуальність. Цифрова оперативна стійкість (DORA) є ключовим фактором у стратегіях управління ризиками та безперервності бізнесу, особливо для малих підприємств, які найбільш вразливі до кіберзагроз. В умовах швидкої цифрової трансформації та зростаючих кібератак впровадження ефективних механізмів захисту стає критично важливим для стабільності компаній. DORA дозволяє підприємствам мінімізувати ризики, що виникають унаслідок кібератак та збоїв, забезпечуючи комплексний підхід до кібербезпеки. Використання гнучких методологій розробки, таких як Scrum або Kanban, потребує інтеграції механізмів безпеки на всіх етапах життєвого циклу програмного забезпечення. Це допомагає зменшити витрати на усунення вразливостей і підвищує надійність цифрових рішень. Незважаючи на важливість кібербезпеки, вона часто сприймається як додатковий аспект, а не невід'ємна частина процесу розробки. DORA сприяє створенню структурованих механізмів безпечного програмування, що не уповільнюють розробку. Для малих підприємств, які не мають ресурсів для окремих команд безпеки, важливо впроваджувати ефективні та доступні рішення в межах наявного бюджету. Поєднання гнучких методів розробки з DORA є необхідним для забезпечення конкурентоспроможності та захисту цифрових активів компаній. Впровадження комплексного підходу до кібербезпеки дозволяє мінімізувати ризики та зміцнити довіру клієнтів.

Метою статті є дослідження інтеграції цифрової оперативної стійкості (DORA) в управління ризиками та безперервністю бізнесу, зокрема для малих підприємств, шляхом аналізу ключових стратегій забезпечення їхньої стійкості, дослідження викликів впровадження DORA у гнучкі методології розробки, оцінки ефективності комплексного підходу до кібербезпеки, а також розгляду п'яти вимірів стійкості – людського, соціального, економічного, екологічного та технічного, що безпосередньо впливають на довговічність, безпеку та конкурентоспроможність цифрових рішень.

Об'єктом дослідження є розробка та впровадження цифрової оперативної стійкості (DORA) в управління ризиками та забезпечення безперервності бізнес-процесів, зокрема в малих підприємствах, що працюють у швидкозмінних цифрових екосистемах, з акцентом на інтеграцію механізмів кібербезпеки у гнучкі методології розробки програмного забезпечення з метою мінімізації ризиків, підвищення надійності цифрових рішень і забезпечення довгострокової стійкості компаній.

Предмет дослідження – підходи до інтеграції цифрової оперативної стійкості (DORA) в процеси управління ризиками та безперервністю бізнесу, що включають розробку стратегій кібербезпеки, впровадження механізмів захисту.

Аналіз попередніх досліджень. Наразі в літературних дослідженнях розглядаються різні аспекти інтеграції DORA в управління ризиками та безперервністю бізнесу. Canedo [1] та ін. науковці досліджують конфіденційність даних у гнучкій розробці ПЗ, виявляючи недостатнє

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

застосування відповідних методик через застарілі специфікації та брак обізнаності зацікавлених сторін. Інші дослідження акцентують увагу на потребі безпекових заходів на всіх етапах SDLC, зокрема аналізі загроз та тестуванні безпеки. Аналізуються методи, такі як BSIMM та моделювання випадків зловживань, що сприяють вдосконаленню стратегій безпеки. SCRUM залишається домінуючою методологією розробки ПЗ, а ArchiMate і TOGAF визнаються ефективними для моделювання архітектури підприємств. Дослідження також охоплюють питання кібербезпеки, кіберстрахування та інвестицій у захист IT-інфраструктури. Значну увагу приділено DevSecOps як перспективному підходу до забезпечення відповідності DORA. Українські науковці також вивчають ці аспекти: Семенов В. адаптує міжнародні стандарти кібербезпеки, Іванченко О. аналізує управління ризиками в малому та середньому бізнесі, а Козак Л. розглядає впровадження DevSecOps у цифрову трансформацію підприємств [2-4]. Загалом, сучасні літературатурні джерела наголошують на необхідності комплексного підходу до управління ризиками, інтеграції безпеки в SDLC та адаптації бізнес-процесів до нормативних вимог DORA.

Виклад основного матеріалу. Цифрова оперативна стійкість (DORA) відіграє ключову роль у стратегіях управління ризиками та безперервності бізнесу, особливо для малих підприємств, вразливих до кіберзагроз. В умовах конкурентного середовища та зростання кіберзагроз інтеграція ефективного захисту стає критично важливою для їхньої стабільності. DORA допомагає розробляти заходи безпеки для мінімізації ризиків, спричинених кібератаками, збоями технологій та іншими загрозами. Малі підприємства часто мають обмежені ресурси та недостатню експертизу у сфері кібербезпеки. Впровадження DORA сприяє ефективному контролю безпеки та застосуванню сучасних технологій у розробці програмного забезпечення. Це особливо важливо для компаній, що працюють у швидкозмінних цифрових екосистемах, адже без належного захисту вони ризикують втратити не лише фінанси, а й довіру клієнтів.

Інтеграція DORA в управління ризиками та безперервністю бізнесу передбачає створення комплексної системи, що забезпечує швидке реагування на цифрові загрози. Важливими складовими є регулярна оцінка ризиків, зокрема залежності від сторонніх постачальників, впровадження заходів кібербезпеки, як-от безпарольний доступ для зниження ризику фішингу, а також механізми моніторингу для своєчасного виявлення загроз (рис. 1).

Особливу увагу приділено розробці стратегій безперервності бізнесу та планів відновлення після інцидентів, а також постійному вдосконаленню захисних механізмів на основі аналізу попередніх кіберінцидентів. DORA також зобов'язує компанії визначати відповідального за управління ризиками інформаційно-комунікаційних технологій (ІКТ), що гарантує незалежний контроль і підвищує ефективність реагування на цифрові виклики. Інтеграція DORA сприяє формуванню стійкої кібербезпеки підприємств, що забезпечує їхню адаптивність до нових загроз. Вона вимагає від компаній впровадження регулярного тестування безпеки, включаючи симуляції кібератак для оцінки готовності до потенційних ризиків. Застосування методологій DevSecOps дозволяє інтегрувати безпекові механізми на всіх етапах життєвого циклу програмного забезпечення, зменшуючи уразливості систем. Особливе значення надається управлінню ризиками постачальників IT-послуг, оскільки залежність від сторонніх технологічних рішень може створювати додаткові загрози. DORA також передбачає забезпечення прозорості у звітності щодо інцидентів, що підсилює довіру клієнтів і партнерів до компанії. Впровадження системи моніторингу та автоматизованого аналізу аномалій дає змогу виявляти загрози на ранніх етапах і мінімізувати їхній вплив на бізнес-процеси. Таким чином, комплексний підхід до управління ризиками відповідно до DORA є ключовим фактором для забезпечення стійкості та конкурентоспроможності підприємств у цифровому середовищі [1].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Рис. 1. Схема управління ризиками ІКТ, відповідно до DORA

Джерело: агреговано на основі [1–3]

Гнучкі методології розробки (Scrum, Kanban) підвищують адаптивність бізнесу, але створюють безпекові виклики. Інтеграція DORA дозволяє враховувати аспекти безпеки на всіх етапах розробки, допомагаючи уникнути значних витрат на усунення вразливостей. Вона підкреслює важливість регулярного тестування, моніторингу загроз та впровадження стандартів кіберзахисту ще на ранніх етапах. DORA сприяє формуванню культури безпеки, де захист даних і операцій стає пріоритетом на всіх рівнях управління. Запровадження автоматизованих механізмів контролю ризиків дозволяє підприємствам оперативно реагувати на нові загрози та мінімізувати їх вплив. Особливу увагу приділено управлінню ризиками постачальників IT-послуг, оскільки залежність від сторонніх технологічних рішень може призводити до критичних вразливостей. Вимоги DORA також включають обов'язкову звітність про кіберінциденти, що сприяє підвищенню прозорості та довіри з боку клієнтів і регуляторів. Важливим аспектом є навчання персоналу, адже людський фактор залишається однією з головних причин порушень безпеки. Використання сучасних інструментів аналізу загроз і управління інцидентами дозволяє підвищити ефективність реагування на кібератаки. Таким чином, інтеграція DORA не лише підвищує рівень кібербезпеки, а й сприяє довгостроковій стабільності та конкурентоспроможності підприємств.

Ключовим принципом DORA є комплексний підхід до безпеки від початкових етапів розробки, що дозволяє мінімізувати ризики без значного збільшення витрат. Для малих підприємств важливо впроваджувати ефективні та економічно доцільні рішення в межах доступного бюджету. DORA сприяє інтеграції заходів безпеки в усі бізнес-процеси, що допомагає компаніям швидко адаптуватися до змін у кіберзагрозах. Особливу роль відіграє автоматизація процесів моніторингу та аналізу ризиків, що забезпечує швидке реагування на інциденти. Використання сучасних технологій, таких як штучний інтелект і машинне навчання, дозволяє ефективніше ідентифікувати потенційні загрози. Регулярне тестування систем та навчання персоналу допомагає мінімізувати людський фактор у виникненні кіберінцидентів. DORA також підкреслює важливість співпраці між компаніями та регуляторними органами для обміну інформацією про загрози та найкращі практики кібербезпеки. Впровадження стандартів звітності та аналізу кіберризиків сприяє підвищенню прозорості та довіри з боку клієнтів і партнерів. Таким чином, інтеграція DORA не лише знижує ризики, але й підвищує конкурентоспроможність підприємств у цифровій економіці.

Поєднання гнучких методів розробки з принципами DORA є необхідною умовою довгострокової стійкості підприємств. Це забезпечує їхню конкурентоспроможність, захист активів і довіри клієнтів. Водночас, більшість команд, що працюють за гнучкими методологіями, не мають у складі спеціалістів з безпеки, що змушує розробників брати на себе відповідальність за впровадження заходів захисту без належної підготовки. У сучасних умовах

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

стрімкої цифрової трансформації, що охоплює всі сфери економіки та діяльності підприємств, кіберзагрози стають одним із найбільш значущих викликів для бізнесу, незалежно від його розміру чи галузевої приналежності, оскільки кожна організація, починаючи від малих і середніх підприємств та закінчуючи транснаціональними корпораціями, може зазнати зловмисних атак, спрямованих на виявлення й експлуатацію вразливостей у її цифрових системах, що, у свою чергу, може призвести до значних економічних збитків, втрати довіри клієнтів та дестабілізації операційної діяльності, а отже, зростання рівня кіберзлочинності вимагає від компаній перегляду підходів до управління ризиками та забезпечення цифрової стійкості. Одним із ключових інструментів забезпечення стійкості є впровадження механізмів постійного моніторингу та аналізу ризиків, що дозволяє виявляти загрози на ранніх етапах. Важливу роль у цьому відіграє автоматизація процесів безпеки, що знижує навантаження на персонал та мінімізує людський фактор. DORA також акцентує увагу на необхідності підготовки персоналу та підвищення рівня обізнаності щодо сучасних кіберзагроз. Регулярні навчання та тестування співробітників допомагають сформувати культуру безпеки в організації, що є критичним для запобігання потенційним інцидентам. Крім того, важливим аспектом є забезпечення прозорості у відносинах з постачальниками цифрових послуг, оскільки їхні слабкі місця можуть становити загрозу для підприємства. Створення ефективної системи обміну інформацією між компаніями та регуляторними органами дозволяє швидко реагувати на нові виклики. Таким чином, інтеграція DORA в управління ризиками сприяє формуванню стійкої екосистеми, де цифрова безпека стає невід'ємною частиною бізнес-стратегії [1, 3].

З огляду на вищезазначене, Європейський Союз ухвалив Директиву DORA (Digital Operational Resilience Act), яка набула чинності 28 червня 2023 року та визначає єдині стандарти цифрової стійкості для критично важливих підприємств, включаючи фінансові установи, державні органи та інші суб'єкти, що забезпечують життєво необхідні послуги, з метою зміцнення їхньої кібербезпеки, підвищення рівня готовності до потенційних кіберінцидентів та забезпечення безперервності бізнес-процесів навіть у разі масштабних атак, що є особливо актуальним у контексті сучасних викликів, пов'язаних із технологічною глобалізацією та розширенням спектру кіберзагроз. DORA встановлює вимоги щодо управління ризиками ІКТ, які передбачають впровадження систем моніторингу, оцінки вразливостей та оперативного реагування на кіберзагрози. Вона також регламентує стандарти звітності про інциденти, що дозволяє забезпечити прозорість та ефективний обмін інформацією між організаціями та регуляторами. Важливим аспектом є посилення контролю над постачальниками ІКТ-послуг, оскільки залежність від сторонніх компаній може створювати додаткові ризики для безперервності бізнесу. Регулярне тестування кіберстійкості, включаючи сценарії імітації атак, є обов'язковою складовою відповідності DORA. Особлива увага приділяється впровадженню підходів DevSecOps, що дозволяють інтегрувати безпекові механізми безпосередньо у процеси розробки та експлуатації цифрових рішень. Крім того, директива передбачає створення кризових планів для мінімізації наслідків можливих атак та швидкого відновлення операційної діяльності [2]. Таким чином, DORA забезпечує цілісний підхід до управління кіберризиками, сприяючи підвищенню стійкості підприємств у цифровій економіці.

Проте малий та середній бізнес, на відміну від великих корпорацій, стикається з певними труднощами у процесі імплементації вимог DORA, зокрема через обмежені ресурси, що ускладнює створення спеціалізованих відділів кібербезпеки та виділення значних фінансових коштів на реалізацію ефективних заходів захисту, а також через недостатню обізнаність керівників та співробітників щодо актуальних загроз, методів їхнього попередження та відсутність комплексної стратегії реагування на кіберінциденти, що, своєю чергою, ускладнюється високими вимогами до відповідності стандартам DORA, адже директива передбачає системний підхід до управління ризиками, моніторингу кіберзагроз і швидкого

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

відновлення бізнесу після атак, що може бути складним завданням для підприємств, які не мають достатнього досвіду та ресурсів для інтеграції таких процесів у свою діяльність.

Попри зазначені виклики, численні дослідження доводять, що впровадження ефективних методів кібербезпеки можливе навіть для компаній із лімітованими ресурсами, оскільки застосування стандартизованих і перевірених на практиці безпекових практик не лише не суперечить операційній гнучкості та фінансовій доступності, а й сприяє створенню більш стійкої бізнес-моделі, що дозволяє знижувати ризики потенційних загроз та підвищувати загальну цифрову безпеку організації. Для успішного впровадження принципів DORA у бізнес-процеси підприємства мають розробити та реалізувати низку стратегій, серед яких ключове значення має розробка комплексної політики кібербезпеки, яка включає детальний аналіз ризиків, формування плану дій на випадок атак та визначення заходів для підвищення цифрової стійкості, що передбачає, зокрема, впровадження безпечного життєвого циклу розробки програмного забезпечення (SSDLC) з інтеграцією відповідних заходів безпеки на всіх етапах створення IT-продуктів, що дозволяє суттєво знизити рівень потенційних вразливостей і, відповідно, ризиків, пов'язаних із можливими атаками [1, 4].

Окрім цього, однією з ключових стратегій є автоматизація процесів моніторингу загроз, що передбачає використання сучасних систем аналізу ризиків, виявлення аномалій та оперативного реагування на інциденти, а також підвищення рівня обізнаності персоналу шляхом регулярних тренінгів та навчальних програм, спрямованих на розвиток навичок ідентифікації фішингових атак, належного управління паролями та роботи з конфіденційною інформацією, що є вкрай важливим фактором, оскільки людський фактор часто стає найслабшою ланкою в системі кібербезпеки організації.

Застосування методів безпеки, адаптованих до специфіки малих та середніх підприємств, дозволяє їм використовувати гнучкі й економічно обґрунтовані рішення, що відповідають їхнім можливостям і потребам, сприяючи при цьому підвищенню рівня цифрової стійкості та забезпечуючи низку переваг, зокрема зниження ризиків кібератак за рахунок запобігання потенційним загрозам і мінімізації їхнього впливу на операційну діяльність, що є особливо важливим у сучасному бізнес-середовищі, де цифрові технології відіграють ключову роль у забезпеченні ефективності та конкурентоспроможності компаній.

Крім того, забезпечення безперервності бізнес-процесів, що є одним із ключових принципів DORA, дозволяє підприємствам зберігати стабільність своєї діяльності навіть у випадку масштабних кіберінцидентів, що вкрай важливо для компаній, значною мірою залежних від цифрової інфраструктури, а також сприяє зміцненню довіри клієнтів і партнерів завдяки демонстрації відповідності міжнародним стандартам кібербезпеки та гарантуванню безпечної взаємодії з контрагентами, що, у свою чергу, відкриває нові можливості для розвитку бізнесу. Впровадження DORA сприяє мінімізації фінансових втрат, пов'язаних із кіберінцидентами, завдяки своєчасному реагуванню та адаптації до загроз. Особливу роль відіграє інтеграція заходів кіберзахисту в усі бізнес-процеси, що забезпечує ефективне управління ризиками. Це дозволяє компаніям не лише відповідати регуляторним вимогам, а й підвищувати свою конкурентоспроможність у цифровій економіці. Таким чином, стратегічне застосування DORA є запорукою довгострокової стійкості підприємств в умовах сучасного кіберсередовища [3].

Застосування підходів, передбачених DORA, передбачає інтеграцію практик оцінювання ризиків та управління кібербезпекою на всіх етапах життєвого циклу програмних та інформаційних систем, починаючи від проектування та розробки до тестування, впровадження та подальшої експлуатації. Наприклад, модель S-SDLC забезпечує перевірку вимог безпеки на кожному з етапів розробки програмного забезпечення, що дозволяє виявляти потенційні вразливості ще на початкових стадіях та відповідно реагувати на можливі загрози. Крім того, інтеграція стандартів безпеки, таких як ISO/IEC 27001 та OWASP ASVS (Application Security Verification Standard), сприяє створенню ефективних механізмів

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

аутентифікації, управління доступом та криптографічного захисту, що значно знижує ризики несанкціонованого доступу до конфіденційної інформації. Для компаній, які прагнуть досягти максимальної відповідності вимогам DORA, важливим є також використання Security Assurance Maturity Model (SAMM), що дозволяє оцінити рівень безпеки на кожному етапі життєвого циклу програмного забезпечення, вдосконалити підходи до управління кіберризиками та забезпечити комплексну стратегію захисту цифрових активів. Також важливу роль відіграє впровадження процесів постійного моніторингу та автоматизованого аналізу загроз.

Інтеграція DORA в управління ризиками та забезпечення безперервності бізнесу дозволяє підприємствам зменшити ймовірність кіберзагроз, оптимізувати витрати на кібербезпеку та підвищити довіру з боку клієнтів і партнерів, оскільки відповідність міжнародним стандартам кібербезпеки є важливим фактором конкурентоспроможності у цифрову епоху. Саме тому стратегічний підхід до впровадження принципів DORA передбачає не лише дотримання нормативних вимог, а й трансформацію корпоративної культури управління ризиками, що включає постійний моніторинг загроз, використання сучасних технологій безпеки, адаптацію методів захисту відповідно до специфіки бізнесу та безперервне підвищення рівня кіберграмотності персоналу. Таким чином, поєднання нормативного регулювання, технічних заходів та організаційних стратегій дозволяє сформувати ефективну систему цифрової стійкості підприємств, що відповідає викликам сучасного кіберпростору та сприяє сталому розвитку бізнесу в умовах глобалізованої цифрової економіки.

Висновки. Інтеграція DORA в управління ризиками та забезпечення безперервності бізнесу дозволяє підприємствам зменшити ймовірність кіберзагроз, оптимізувати витрати на кібербезпеку та підвищити довіру з боку клієнтів і партнерів, оскільки відповідність міжнародним стандартам кібербезпеки є важливим фактором конкурентоспроможності у цифрову епоху. Саме тому стратегічний підхід до впровадження принципів DORA передбачає не лише дотримання нормативних вимог, а й трансформацію корпоративної культури управління ризиками, що включає постійний моніторинг загроз, використання сучасних технологій безпеки, адаптацію методів захисту відповідно до специфіки бізнесу та безперервне підвищення рівня кіберграмотності персоналу. Таким чином, поєднання нормативного регулювання, технічних заходів та організаційних стратегій дозволяє сформувати ефективну систему цифрової стійкості підприємств, що відповідає викликам сучасного кіберпростору та сприяє сталому розвитку бізнесу в умовах глобалізованої цифрової економіки.

Список використаних джерел

1. Canedo, J., & Santos, P. Data Privacy in Agile Software Development: Challenges and Implementation Prospects / J. Canedo, P. Santos // Journal of Cybersecurity Research. – 2021. – No. 14. – P. 112–124.
2. Семенов В. Адаптація міжнародних стандартів кібербезпеки в управлінні ризиками підприємств / В. Семенов // Економіка і безпека. – 2023. – № 4. – С. 53–62.
3. Козак Л. Впровадження DevSecOps у цифрову трансформацію підприємств / Л. Козак // Інформаційні системи і технології. – 2022. – № 8. – С. 95–107.
4. Іванченко О. Управління ризиками інформаційної безпеки в малому та середньому бізнесі / О. Іванченко // Бізнес та технології. – 2022. – № 11. – С. 76–85.
5. TOGAF і ArchiMate як методології моделювання архітектури підприємств у контексті DORA / European IT Governance Group // Journal of Enterprise Architecture. – 2023. – № 17. – С. 120–133.

Роботу виконано під науковим керівництвом PhD, старшого викладача
ШЕСТАКА Я. І.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

СКАНУВАННЯ ВЕБВРАЗЛИВОСТЕЙ: АВТОМАТИЗОВАНІ МЕТОДИ ТА ЇХ ЕФЕКТИВНІСТЬ У КІБЕРБЕЗПЕЦІ

ФЕДІК А. В., 2 курс 6мз група ФІТ ДТЕУ, освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті розглянуто підходи сучасного автоматизованого сканування вебвразливостей, як невідє'много інструменту у кібербезпеці. Також проведено комплексний аналіз ключових інструментів для виявлення загроз у вебзастосунках, визначено їхню ефективність. Підкреслено перспективи розвитку автоматизованих методів та їхню роль у стратегіях кіберзахисту.

The article discusses the approaches of modern automated web vulnerability scanning as an essential tool in cybersecurity. A comprehensive analysis of the key tools for detecting threats in web applications is also carried out, and their effectiveness is determined. The prospects for the development of automated methods and their role in cybersecurity strategies are emphasized.

Актуальність. У світі цифрових технологій безпека вебресурсів стає одним із ключових викликів, оскільки кількість атак на вебдодатки невпинно зростає. Згідно зі звітом IBM Security, середній час виявлення кібератаки сягає понад 200 днів, що створює значні ризики для компаній та користувачів. Автоматизовані системи сканування вразливостей забезпечують швидке виявлення загроз, мінімізують ризики зловживань та дозволяють своєчасно усувати критичні вади безпеки. Це дослідження спрямоване на оцінку ефективності таких систем та їх внесок у розвиток сучасної кібербезпеки.

Метою статті є визначення ефективності сучасних автоматизованих методів сканування веб-вразливостей та порівняльний аналіз інструментів для підвищення захисту кібербезпеки.

Об'єктом дослідження є вебдодатки та системи кібербезпеки, що використовують автоматизовані технології визначення вразливостей.

Предмет дослідження – засоби автоматизованого сканування вебвразливостей.

Аналіз попередніх досліджень. Досліджено, що автоматизоване сканування вебвразливостей широко досліджується в роботах таких авторів, як Кевін Мітнік, Брюс Шнайєр та Рі́чард Ме́тью Сто́лмен. У дослідженнях розглядаються як основні принципи роботи сканерів, так і їх вплив на підвищення безпеки вебдодатків. Однак питання порівняльного аналізу ефективності інструментів залишається недостатньо висвітленим, що обумовлює потребу у додаткових дослідженнях.

Виклад основного матеріалу. У сучасному цифровому світі безпека вебдодатків стає все більш актуальною. Кіберзлочинці постійно шукають нові способи атак, використовуючи слабкість у вебресурсах. Одним із найефективніших способів виявлення слабких місць є автоматизоване сканування вебвразливостей. Цей підхід набув широкого поширення серед компаній, що працюють у сфері кібербезпеки. Автоматизовані засоби здатні перевіряти тисячі сторінок за короткий час, їх можна застосовувати для сайтів будь-якої складності, що значно знижує ймовірність пропуску критичних вразливостей. Багато сучасних рішень мають зручний інтерфейс та легко інтегруються у процеси DevSecOps, адже саме цей підхід до розробки програмного забезпечення інтегрує безпеку на всіх етапах життєвого циклу розробки програм, а не лише на етапі тестування або впровадження.

Автоматизований аналіз веббезпеки працює за допомогою спеціального програмного забезпечення, яке аналізує вебсайт на наявність вразливостей. Спочатку проводиться збір інформації, аналізується структура сайту та технології, що використовуються. Після чого здійснюється перевірка ресурсу на найбільш поширені вразливості. Однією з найбільш

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

поширених вразливостей, які виявляються такими інструментами, є SQL-ін’єкції (SQLi). Вони виникають, коли вебдодаток неправильно обробляє введені користувачем дані у запитах до бази даних. Зловмисник може змінити SQL-запит, отримати конфіденційну інформацію або навіть змінити базу даних. Автоматизовані сканери перевіряють сайти, вводячи спеціальні запити, що імітують такі атаки, і аналізують відповіді сервера.

Одним із найвідоміших прикладів ефективності таких рішень став випадок у 2019 році, коли хакери використали SQL-ін’єкцію для викрадення особистих даних 100 мільйонів клієнтів Capital One. Регулярне автоматизоване сканування могло б допомогти виявити цю проблему заздалегідь. У 2021 році компанія Tesla виплатила хакеру-викривачу 10 000 доларів за виявлення XSS-уразливості на своєму порталі, яка дозволяла зловмисникам виконувати шкідливі скрипти від імені користувачів. Ще один приклад – вразливості у плагінах WordPress, які роблять сайти на цій платформі привабливою мішенню для атак. Використання автоматизованих сканерів, таких як WPScan, допомагає адміністраторам швидко знаходити та усувати ці проблеми.

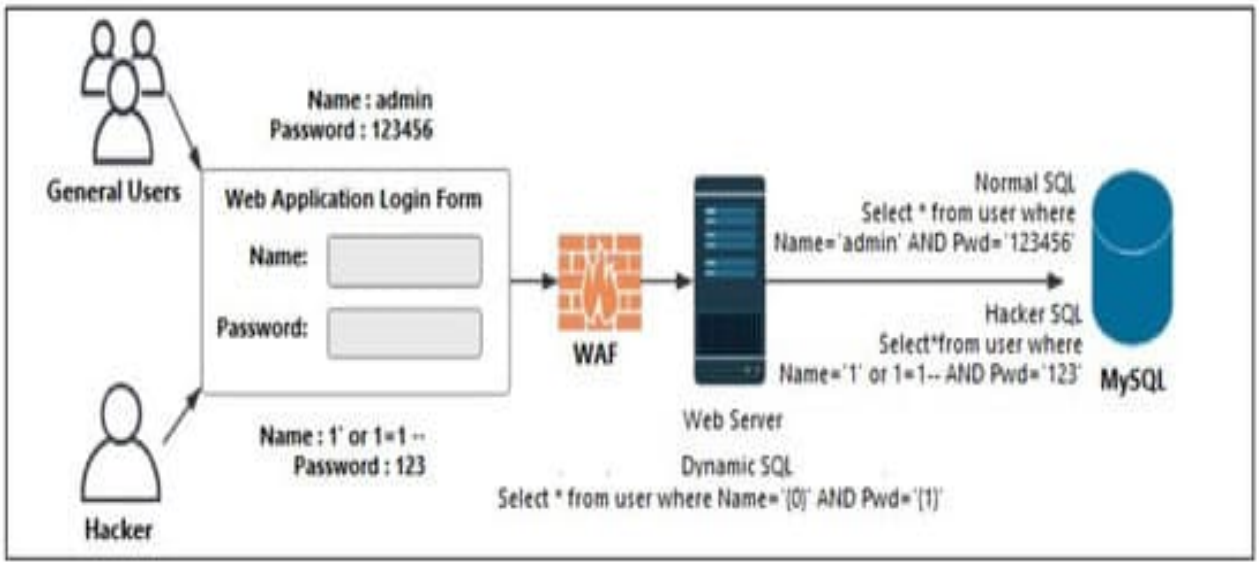


Рис. 1. SQL Injection Attacks

Джерело: [2]

Ще одна поширена загроза – Cross-Site Scripting (XSS), вона дозволяє зловмисникам впроваджувати шкідливий JavaScript-код у сторінку, що може використовуватися для викрадення даних користувачів або виконання дій від їхнього імені. Сканери автоматично перевіряють, чи можна вставити та виконати скрипт у полях введення. Окрім цього, вони допомагають виявити Cross-Site Request Forgery (CSRF) – атаку, яка змушує користувача виконати небажані дії без його відома. Такі вразливості часто пов’язані з відсутністю захисних токенів CSRF у запитах.

Сканери також ідентифікують витоки конфіденційної інформації, такі як відкриті API-ключі, некоректно налаштовані файли (robots.txt, .htaccess), а також заголовки HTTP, що можуть розкривати зайві дані про сервер. Одна з критичних проблем, яку виявляють автоматизовані засоби, це небезпека завантаження файлів. Якщо система не обмежує формат або розмір файлів, зловмисники можуть завантажити шкідливий код та виконати атаку на сервер.

Одним з ризиків є відсутність належних захисних HTTP-заголовків, таких як Content Security Policy (CSP) та X-Frame-Options, які сприяють захисту від атак типу Clickjacking і XSS. Сканери перевіряють наявність цих заголовків і їх правильну конфігурацію. Крім того, вони допомагають виявляти серверні помилки, зокрема неправильні налаштування доступу або

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

використання застарілих версій серверного ПЗ. Загалом, автоматизоване сканування є ефективним інструментом у сфері кібербезпеки, проте воно не може виявити складні логічні помилки або атаки, що потребують специфічних сценаріїв тестування. Саме тому оптимальним підходом є комбіноване використання автоматичних та ручних методів сканування.

Ручне сканування дозволяє експертам більш детально аналізувати результати автоматичних перевірок, перевіряти складні бізнес-логічні вразливості та оцінювати реальні ризики. Наприклад, автоматизовані засоби можуть виявити потенційно небезпечний вхідний параметр, але лише тестувальник може визначити, чи справді він є експлуатованим для атаки. Деякі атаки, такі як логічні помилки в аутентифікації, неправильна обробка прав доступу, уразливості, що залежать від контексту застосунку, складно або взагалі неможливо виявити за допомогою автоматичних сканерів.

Ще одним важливим фактором є те, що автоматизовані сканери можуть давати хибнопозитивні або хибнонегативні результати. Це означає, що вони можуть вказати на вразливість там, де її немає, або, навпаки, пропустити реальну загрозу. Тому після автоматизованого сканування необхідно проводити ручний аналіз виявлених проблем для підтвердження або спростування знайдених вразливостей.

Ідеальним рішенням є використання автоматизованих сканерів для первинного пошуку типових проблем, а потім проведення ручного аналізу для глибшої перевірки. Наприклад, підхід DevSecOps, який інтегрує безпеку на всіх етапах розробки, передбачає регулярне використання автоматизованих сканерів у поєднанні з ручним пентестингом перед випуском продукту. Такий підхід дозволяє не лише знаходити вразливості, а й запобігати їх появі ще на етапі розробки. Один із способів реалізувати інтеграцію безпеки в процеси розробки – це використання CI/CD (Continuous Integration / Continuous Deployment) пайплайнів, де автоматизовані сканери та інші інструменти безпеки впроваджуються на всіх етапах.

Ось приклад CI/CD пайплайну з інтеграцією безпеки

(Код) → (Статичний аналіз SAST) → (Аналіз залежностей SCA)
↓
(Збірка) → (Сканування контейнерів) → (Динамічний аналіз DAST)
↓
(Тестування) → (Інтерактивне тестування IAST) → (Аналіз інфраструктури IaC)
↓
(Розгортання) → (Моніторинг у продакшні)

Раніше безпеку перевіряли лише на етапі тестування або перед розгортанням, що часто призводило до виявлення вразливостей занадто пізно. Інтеграція безпеки в CI/CD (SecDevOps) дозволяє знаходити проблеми раніше, автоматично виправляти їх та мінімізувати ризики без зупинки розробки.

Для забезпечення безпеки на різних етапах розгортання застосовуються статичний аналіз коду, перевірка залежностей, аналіз контейнерів, динамічне тестування та контроль доступу. Статичний аналіз коду (SAST) дозволяє виявити потенційні вразливості ще до компіляції, наприклад SQL-ін’єкції чи використання слабких алгоритмів хешування. Аналіз залежностей (SCA) перевіряє бібліотеки та пакети на наявність відомих вразливостей (CVE), що дозволяє уникнути використання небезпечних компонентів. Аналіз контейнерів допомагає виявити конфігураційні помилки та слабкі місця в образах Docker, що критично важливо для безпеки інфраструктури. Динамічне тестування (DAST) сканує працюючий веб-додаток на наявність уразливостей, таких як XSS або CSRF, що дозволяє виявити реальні загрози ще до розгортання у продакшн. Контроль доступу базується на використанні Role-Based Access

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Control (RBAC), що дозволяє обмежити права користувачів та запобігти несанкціонованому доступу до критичних ресурсів.

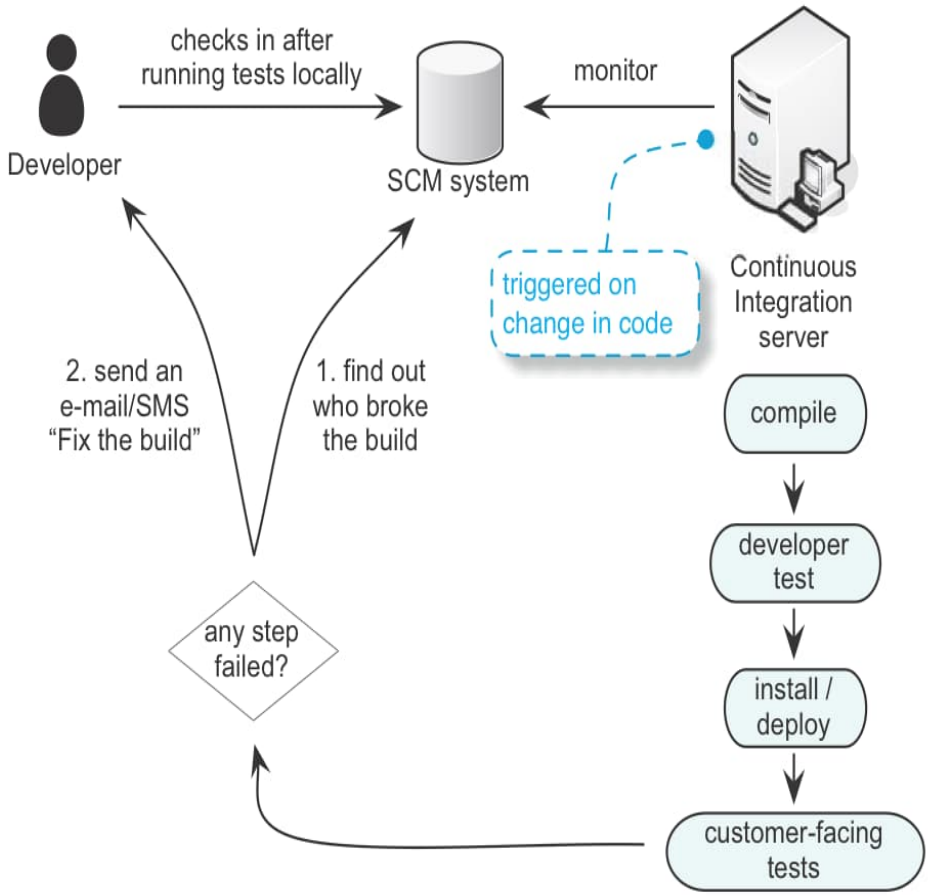


Рис. 2. Приклад Continuous Integration

Джерело: У списку літератури [3]

Для впровадження безпечного CI/CD пайплайну використовується GitLab CI/CD, а також додаткові інструменти для перевірки безпеки. Конфігурація пайплайну зберігається у файлі `.gitlab-ci.yml`. Наприклад:

Після налаштування безпечного CI/CD пайплайну, зокрема використання GitLab CI/CD і додаткових інструментів для перевірки безпеки, важливо також впровадити більш інтелектуальні підходи для автоматизації виявлення загроз. У цьому контексті машинне навчання (ML) та штучний інтелект (AI) можуть значно підвищити ефективність виявлення нових вразливостей, вивчаючи поведінку системи та прогнозуючи потенційні загрози ще до їх виникнення.

Машинне навчання (ML) та штучний інтелект (AI) є потужними інструментами, що дозволяють автоматизувати виявлення нових вразливостей в інформаційних системах, зокрема у вебдодатках. Однією з основних переваг використання AI та ML є здатність цих технологій обробляти великі обсяги даних та виявляти аномалії, які можуть бути індикаторами нових або раніше не виявлених вразливостей. Системи на основі машинного навчання можуть ефективно аналізувати мережевий трафік, логи безпеки та поведінку користувачів, щоб виявити підозрілі дії, які можуть свідчити про можливу атаку. Такі підходи дозволяють виявляти нові типи загроз, наприклад, раніше невідомі методи SQL-ін’єкцій, XSS-уразливості

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

або інші уразливості, які можуть бути не зафіксовані в традиційних системах захисту, що базуються на сигнатурах.

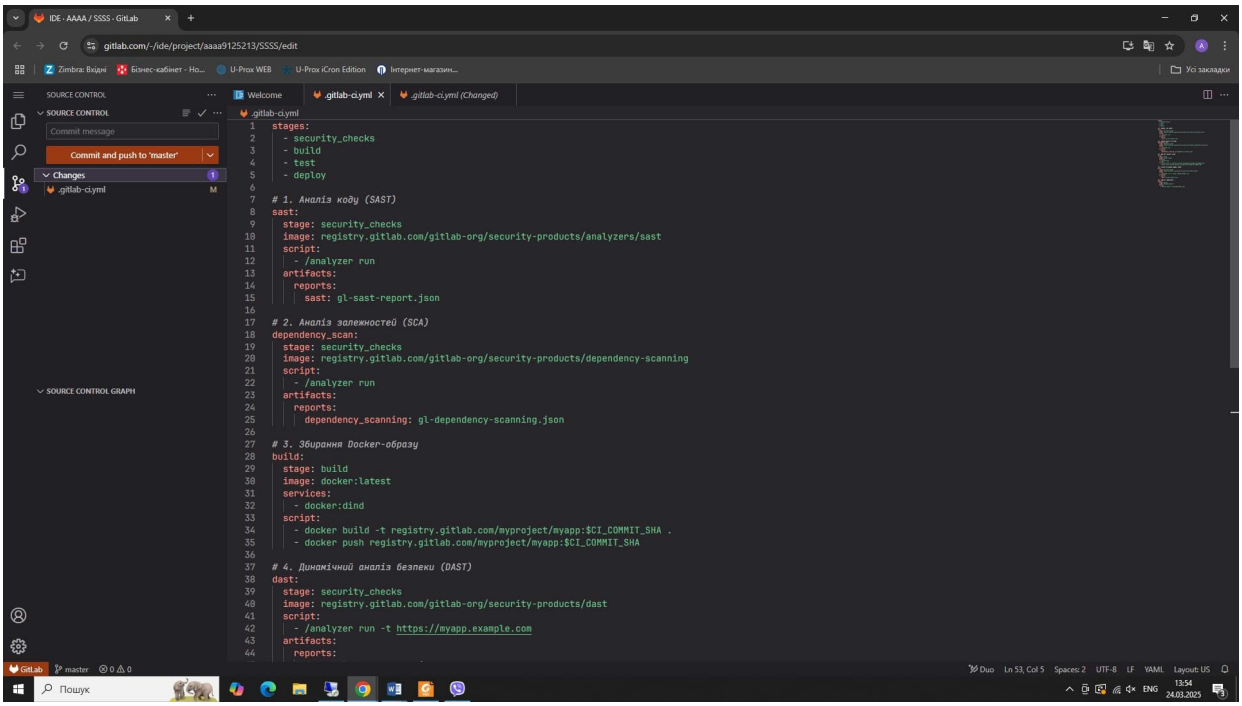


Рис. 3. Структура GitLab CI/CD пайплайну

Джерело: розроблено автором в середовищі GitLab (знімок з екрану)

AI може бути використаний для автоматичного створення профілів «нормальної» поведінки системи, що дозволяє ідентифікувати аномалії в реальному часі, зокрема несанкціоновані запити або інші аномальні дії, які можуть свідчити про спроби зловмисників скористатися вразливістю. За допомогою глибокого навчання нейронні мережі можуть навчатися на великих масивах даних про попередні атаки, щоб виявляти нові варіації шкідливих програм або експлойтів, навіть якщо вони ще не були занесені в бази даних відомих загроз. Крім того, штучний інтелект дозволяє автоматично оновлювати системи безпеки, коригувати правила фаєрволів, оновлювати антивірусне програмне забезпечення та застосовувати нові методи захисту, зменшуючи час реагування на загрози.

Машинне навчання також здатне допомогти в прогнозуванні нових типів вразливостей, аналізуючи історичні дані про атаки та виявлені загрози, що дозволяє організаціям проактивно вживати заходи для захисту своїх систем ще до того, як ці загрози стануть актуальними. За допомогою AI можна передбачити ймовірність виникнення певних типів атак, що дозволяє підвищити загальний рівень безпеки і знизити вразливість до нових, раніше невідомих загроз. Крім того, такі технології дозволяють знижувати залежність від людського фактору, що є важливим для забезпечення високого рівня безпеки, оскільки помилки людини часто стають причиною успішних атак. Використання AI та ML дозволяє значно підвищити ефективність виявлення нових вразливостей, пришвидшуючи процес реагування та знижуючи ймовірність успішних атак.

Після розгляду впровадження машинного навчання (ML) та штучного інтелекту (AI) у процес автоматизації виявлення вразливостей, важливо звернути увагу на сучасні виклики та тренди у веб-безпеці, які виникають у зв’язку з еволюцією кіберзагроз і новими технологічними підходами. Веб-безпека перебуває на постійному етапі розвитку через нові методи атак та зростаючу складність кіберзагроз. З появою нових технологій, таких як

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Інтернет речей (IoT), блокчейн та штучний інтелект, також зростає необхідність у вдосконалених механізмах захисту. Вебдодатки стають все більш складними, а кіберзлочинці використовують все більш складні методи для обходу традиційних засобів захисту. Важливим трендом є розвиток атак на рівні аплікацій, таких як атаки на API (Application Programming Interface), та використання новітніх технік для маніпуляції даними, що вимагає від організацій постійного оновлення своїх стратегій безпеки.

У цьому контексті виникає необхідність постійного відстеження нових трендів у веббезпеці, таких як захист від атак на основі штучного інтелекту, покращення методів виявлення вразливостей, а також розвиток інтегрованих систем моніторингу та захисту. Враховуючи швидкий розвиток технологій і зміну ландшафту кіберзагроз, веббезпека вимагає гнучких, динамічних підходів і постійного вдосконалення існуючих методів захисту.

Ці виклики вимагають від фахівців з кібербезпеки постійного оновлення знань та адаптації до нових умов, що в свою чергу створює потребу у вдосконаленні підходів до захисту веб-додатків на різних етапах їхнього життєвого циклу.

Згідно зі звітом Google Security, 86% веб-додатків містять критичні вразливості, які можуть бути використані хакерами. Експерт з кібербезпеки Трой Хант наголошує: «Без ефективного сканування вразливостей компанії залишають відкритими двері для атак». Важливим трендом є впровадження DevSecOps, який інтегрує безпеку у всі етапи розробки програмного забезпечення. Наприклад, у компанії Tesla застосовували DevSecOps для безпечного тестування свого коду, що допомогло швидко виявити уразливість XSS на порталі. Автоматизація виявлення загроз і використання інструментів на основі машинного навчання дозволяють значно скоротити час на реагування на атаки та мінімізувати потенційні збитки.

Висновки. У результаті дослідження встановлено, що автоматизовані методи сканування вебвразливостей є ключовим компонентом забезпечення кібербезпеки. Порівняльний аналіз сучасних інструментів показав, що ефективність їхнього використання значною мірою залежить від точності виявлення загроз, швидкості сканування та можливості інтеграції у існуючі системи захисту. Отримані результати підтверджують доцільність застосування таких методів для своєчасного виявлення та усунення вразливостей. Подальші дослідження можуть бути спрямовані на вдосконалення алгоритмів сканування, зокрема через використання технологій машинного навчання, а також на інтеграцію цих інструментів у процеси DevSecOps для забезпечення безперервного моніторингу безпеки.

Список використаних джерел

1. Mitnick K. «The Art of Invisibility», 2017.
2. https://www.mdpi.com/2227-7390/11/15/3286
3. https://less.works/less/technical-excellence/continuous-integration
4. https://www.amazon.com/Click-Here-Kill-Everybody-Hyper-connected/dp/0393608883
5. file:///C:/Users/Admin/Downloads/2774-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-9181-1-10-20241230%20(1).pdf
6. https://elartu.tntu.edu.ua/bitstream/lib/31340/1/mag2019_Shytko._%D0%A1%D0%90%D0%BC-61.pdf
7. https://hackyourmom.com/servisy/soft/burp-suite-owasp-top-10-owasp-juice-shop/
8. https://cuesc.org.ua/images/informlist/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82%20advanced_training_OLA.pdf?utm_source=chatgpt.com
9. https://knute.edu.ua/file/Mg%3D%3D/e0fabb7e45ae823afe73062ff07f88dc.pdf

Роботу виконано під науковим керівництвом PhD, старшого викладача
ШЕСТАКА Я. І.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

ЕФЕКТИВНЕ ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБСАЙТІВ ЗА ДОПОМОГОЮ АЛГОРИТМІВ КОНТРОЛЬОВАНОГО НАВЧАННЯ

ФІЛАТЕНКО В. С., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто проблему фішингових атак як одного з найпоширеніших видів кіберзагроз, спрямованих на незаконне отримання конфіденційної інформації через підроблені вебресурси. Фішингові сайти імітують легітимні сторінки банків та платіжних систем, змушуючи користувачів несвідомо передавати зловмисникам свої дані. Попри розвиток антифішингових механізмів, зловмисники вдосконалюють методи обходу захисту, що ускладнює їхнє виявлення. Тому актуальним є створення автоматизованих рішень для ефективного виявлення фішингових ресурсів. Запропоновано методику використання алгоритмів машинного навчання для аналізу URL-адрес та HTML-коду вебсторінок. Дослідження охоплює багатошаровий перцептрон, дерево рішень і наївний байєсівський класифікатор для класифікації підозрілих сайтів. Результати показали, що алгоритм дерева рішень має найвищу точність, що робить його перспективним для кібербезпеки. Запропонований підхід може бути інтегрований у системи моніторингу вебтрафіку та автоматизованого аналізу загроз.

The article discusses the issue of phishing attacks as one of the most common types of cyber threats aimed at illegally obtaining confidential information through counterfeit web resources. Phishing sites mimic legitimate banking and payment system pages, tricking users into unknowingly providing their data to cybercriminals. Despite the development of anti-phishing mechanisms, attackers continuously improve their methods to bypass protections, making detection more difficult. Therefore, the creation of automated solutions for effective detection of phishing resources is highly relevant. The article proposes a methodology for using machine learning algorithms to analyze URLs and HTML code of web pages. The study covers multilayer perceptron, decision tree, and naive Bayes classifiers for classifying suspicious sites. The results showed that the decision tree algorithm has the highest accuracy, making it promising for cybersecurity. The proposed approach can be integrated into web traffic monitoring systems and automated threat analysis.

Актуальність. У сучасних умовах активного розвитку цифрових технологій та зростання кількості онлайн-сервісів питання кібербезпеки набуває особливої важливості. Фішингові атаки залишаються одним із найпоширеніших методів шахрайства, спрямованих на отримання конфіденційної інформації, зокрема фінансових даних, облікових записів та персональних відомостей користувачів. Зловмисники створюють вебсайти, що візуально ідентичні легітимним ресурсам, і використовують соціальну інженерію для введення користувачів в оману. Попри впровадження антіфішингових технологій, традиційні методи детектування мають низку обмежень, зокрема високу залежність від баз відомих загроз, що робить їх малоефективними проти нових або модифікованих атак. У зв’язку з цим виникає необхідність у застосуванні алгоритмів машинного навчання, які здатні аналізувати великі обсяги даних та виявляти приховані закономірності, характерні для фішингових вебсайтів. Застосування алгоритмів контрольованого навчання, таких як дерево рішень, наївний байєсівський класифікатор та багатошаровий перцептрон, дозволяє значно підвищити ефективність і точність детекції загроз. Ці методи дають змогу автоматизувати процес аналізу URL-адрес, структури HTML-коду та поведінкових характеристик сайтів, що мінімізує ризики для користувачів та організацій. Впровадження таких рішень є важливим кроком у підвищенні рівня кібербезпеки та створенні більш надійного цифрового середовища.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Метою статті є дослідження ефективності алгоритмів контрольованого навчання для автоматизованого виявлення фішингових вебсайтів шляхом аналізу їхніх URL-адрес, HTML-структури та поведінкових характеристик, зокрема через застосування методів машинного навчання, таких як дерево рішень, наївний байєсівський класифікатор та багатошаровий перцептрон, з метою оцінки їхньої точності та продуктивності, що дозволяє визначити оптимальні підходи до детектування фішингових ресурсів та сприяє створенню сучасних антіфішингових систем для підвищення рівня безпеки користувачів і захисту їхніх персональних даних.

Об'єктом дослідження є процес виявлення фішингових вебсайтів за допомогою алгоритмів контрольованого навчання, зокрема через аналіз URL-адрес, HTML-структури та поведінкових характеристик вебсайтів.

Предмет дослідження – підходи та методи використання алгоритмів контрольованого навчання.

Аналіз попередніх досліджень. Аналіз літературних джерел свідчить про широке застосування методів машинного навчання для виявлення фішингових вебсайтів, зокрема за допомогою аналізу URL, HTML-коду та поведінкових характеристик користувачів. Алгоритми контрольованого навчання активно використовуються для класифікації сайтів як фішингових чи легітимних. У дослідженні J. Yang, J. Zhang та Z. Zhang [1] розглянуто використання алгоритмів дерева рішень і наївного Байєса. Вони відзначили високу ефективність дерева рішень, яке створює логічні правила на основі ключових ознак, і добрі результати наївного Байєса, попри його припущення про незалежність ознак, що не завжди справджується на реальних даних. C. C. Tan, J. B. Krentel та A. S. Zhang [2] зосередилися на застосуванні багатошарових перцептронів (MLP) для класифікації фішингових вебсайтів. Результати показали, що MLP є потужним інструментом для роботи з великими масивами даних, однак вимагає значних обчислювальних ресурсів для тренування моделей. T. S. Le та P. B. Wright [3] підкреслюють важливість інтеграції кількох алгоритмів, таких як дерева рішень і ансамблеві методи, для покращення точності виявлення фішингових сайтів. Комбінація різних алгоритмів дозволяє знижувати помилкові спрацьовування та покращує загальну ефективність системи.

Виклад основного матеріалу. Зростання кількості фішингових вебсайтів є вражаючим. Незважаючи на те, що користувачі Інтернету обізнані щодо таких атак, багато з них все одно стають жертвами фішинг-атаки. Більшість атак націлені на те, щоб змусити користувачів Інтернету повірити, що вони спілкуються з надійною організацією. Фішинг є одним із таких видів атак. Комунікації від популярних вебсайтів, аукціонних платформ, онлайн-платіжних систем часто використовуються як джерела для обману довірливих користувачів. Фішингові вебсайти – це підроблені вебсайти, які зовні схожі на легітимні. Лише фахівці можуть відразу виявити такі фішингові сайти, проте не всі користувачі є експертами в галузі комп'ютерних технологій, тому вони стають жертвами, надаючи свої особисті дані фішинг-акторам. Фішинг постійно еволюціонує, оскільки легко скопіювати цілий вебсайт, використовуючи HTML-код. Зробивши незначні зміни в вихідному коді, можна спрямувати жертву на фішинговий сайт. Фішери використовують багато методів, щоб обманути нічого не підозрюючих користувачів Інтернету, наприклад, вони надсилають загальні вітання та закликають негайно перевірити свої рахунки, або надсилають погрозливі повідомлення, що вимагають оновлення акаунтів, інакше їх буде скасовано. Тому необхідно розробити ефективний механізм для виявлення фішингових вебсайтів серед легітимних для захисту даних користувачів [1, 3–4].

У сучасному цифровому середовищі фішинг є однією з найбільших загроз для безпеки користувачів Інтернету. Фішингові вебсайти – це підроблені ресурси, що імітують легітимні сайти з метою обману користувачів та збору їхніх персональних даних, таких як логіни, паролі, банківські реквізити та інші конфіденційні відомості. З кожним роком кількість таких сайтів зростає, а методи фішингу стають все більш складними і важкими для виявлення навіть

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

досвідченими користувачами. Це створює серйозну проблему для традиційних систем безпеки, які не завжди здатні оперативно реагувати на нові методи атаки. Тому виникає необхідність у розробці ефективних механізмів виявлення фішингових вебсайтів, зокрема на основі алгоритмів машинного навчання, які здатні адаптуватися до нових загроз.

Алгоритми контрольованого навчання, такі як дерева рішень, наївний байєсівський класифікатор та багатошаровий перцептрон, є одними з найбільш перспективних інструментів для автоматизованого виявлення фішингових вебсайтів. Ці алгоритми можуть бути ефективно використані для аналізу різних характеристик вебсайтів, таких як URL-адреси, HTML-код, поведінкові патерни, а також інші структурні особливості. Наприклад, при аналізі URL-адреси важливо звертати увагу на кількість слешів, використання підозрілих доменних імен або наявність різних підроблених символів, які можуть свідчити про фішинг. Вивчення HTML-коду також дозволяє виявити підроблені елементи, що імітують легітимні сайти, а також перевіряти такі метадані, як META-теги, які можуть містити ключові слова або опис, що відрізняються від оригінальних сайтів.

Формула для оцінки підозрілості URL може бути такою:

$$P_{URL} = w_1 \cdot L + w_2 \cdot C_{SUS} + w_3 \cdot D_{SUS}, \quad (1)$$

де P_{URL} – ймовірність того, що сайт є фішинговим, на основі URL, L – довжина URL (число символів), C_{SUS} – кількість підозрілих символів у URL, D_{SUS} – кількість підозрілих доменних імен або нестандартних доменів, (наприклад, домени з орфографічними помилками або незвичними розширеннями), w_1, w_2, w_3 – ваги для кожного параметра (параметри, що вказують на важливість кожної ознаки).

Математична модель для оцінки ймовірності фішинговості на основі HTML-коду [2-3]:

$$P_{HTML} = w_1 \cdot T_{tags} + w_2 \cdot K_{meta} + w_3 \cdot L_{content}, \quad (2)$$

де P_{HTML} – ймовірність того, що сайт є фішинговим, на основі HTML-коду, T_{tags} – кількість специфічних HTML-тегів (наприклад, використання тегів, що є характерними для фішингових сайтів), K_{meta} – наявність підозрілих ключових слів у мета-тегах або описах, $L_{content}$ – кількість підозрілих доменних імен або нестандартних доменів, (наприклад, домени з орфографічними помилками або незвичними розширеннями), w_1, w_2, w_3 – наявність підроблених або неприродних фрагментів контенту (наприклад, текстів, що імітують легітимні ресурси). Загалом, наведені вирази дозволяють математично оцінити ймовірність того, що сайт є фішинговим, враховуючи важливі характеристики URL-адреси та HTML-коду.

Сучасні підходи до виявлення фішингових сайтів також використовують сторонні бази даних, такі як чорні списки сайтів (Blacklist), які містять відомості про відомі фішингові ресурси. Інтеграція таких списків в систему машинного навчання значно підвищує точність прогнозування та дозволяє оперативно виявляти нові загрози. Зокрема, одним із ключових аспектів є використання методів фічерної екстракції, що дозволяють виділяти найбільш значущі ознаки для прогнозування фішингових сайтів. Для цього важливу роль відіграють техніки, такі як оцінка tf-idf для аналізу контексту URL-адрес та метаданих. Особливо важливо, що алгоритми машинного навчання дозволяють постійно покращувати точність виявлення фішингових сайтів, оскільки вони можуть навчатися на нових даних і адаптуватися до змінюваних методів атак. Використання таких технологій дозволяє забезпечити високий рівень безпеки для користувачів Інтернету, захищаючи їх від потенційно небезпечних сайтів, що намагаються вкрасти персональну інформацію.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Математична модель для перевірки, чи є сайт у чорному списку, може бути виражена так:

$$P_{blacklist} = \begin{cases} 1, \text{якщо } URL \in Blacklist \\ 0, \text{якщо } URL \notin Blacklist' \end{cases} \quad (3)$$

де $P_{blacklist}$ – ймовірність того, що сайт є фішинговим на основі його присутності в чорному списку, URL – URL-адреса вебсайту, $Blacklist$ – набір відомих фішингових сайтів.

Математична модель для оцінки важливості ознак за допомогою $tf–idf$ (Term Frequency – Inverse Document Frequency) для аналізу контексту URL-адрес та метаданих:

$$tf–idf(t,d) = tf(t,d) \cdot log\left(\frac{N}{df(t)}\right), \quad (4)$$

де $tf(t,d)$ – кількість появ терміна t у документі d (наприклад, у мета-тегах або URL), $df(t)$ – кількість документів, що містять термін t (наприклад, кількість сайтів, що мають схожі елементи або ключові слова), N – загальна кількість документів (сайтів), $tf–idf(t,d)$ – оцінка важливості терміна t у контексті конкретного документа (вебсайту). Формули дозволяють інтегрувати дані з чорних списків для швидкого виявлення відомих фішингових сайтів та застосовувати метод tf-idf для оцінки важливості ознак у контексті URL-адрес та метаданих, що допомагає підвищити точність алгоритмів машинного навчання.

Виділення ознак відіграє вирішальну роль у ефективному виявленні фішингових вебсайтів, що є суттєвим викликом у сучасному Інтернет-просторі, де зловмисники постійно вдосконалюють свої методи шахрайства. В HTML вихідному коді кожного вебсайту є багато факторів, які можуть допомогти відрізнити справжній ресурс від фальшивого. Одними з таких факторів є обробник форми на сервері (Server Form Handler) і база даних «Whois», які, незважаючи на свою важливість для виявлення фішингових сайтів, не були враховані в ряді попередніх досліджень. Основною метою фішингових ресурсів є крадіжка персональних даних користувачів, тому аналіз таких елементів, як значення атрибута $action$ в HTML-формах та перевірка інформації в базі «Whois», можуть дати цінні підказки для виявлення підроблених сайтів. Особливо важливо перевіряти, чи існує SSL-сертифікат на вебсайті, оскільки фішингові сайти часто не мають шифрування з'єднання, що може бути яскравим індикатором їх ненадійності. Сучасні законні сайти часто використовують протокол HTTPS, що гарантує захист переданої інформації. Тому відсутність SSL-сертифіката є одним з основних критеріїв для виявлення фішингових сайтів, а це підтверджується останніми дослідженнями, які вказують на те, що більшість фішингових ресурсів не мають захищених з'єднань.

Математична модель для оцінки, чи є атрибут $action$ в HTML-формі підозрілим (може вказувати на фішинговий сайт):

$$P_{actiom} = \begin{cases} 1, \text{якщо } action \in \{\text{небезпечно}, \text{неправильний домен}\} \\ 0, \text{якщо } action \notin \{\text{небезпечно}, \text{неправильний домен}\}' \end{cases} \quad (5)$$

де P_{actiom} – ймовірність того, що атрибут $action$ в HTML-формі вказує на підозрілу активність (наприклад, форму для збору даних, що перенаправляє на незахищений або підозрілий ресурс), $action$ – значення атрибута $action$ в HTML-формі, $\{\text{небезпечно}, \text{неправильний домен}\}$ – набір значень, що вказують на небезпечний або фальшивий ресурс (наприклад, форма, що збирає дані та надсилає їх на сторонній сервер).

Математична модель для перевірки, чи має вебсайт захищене з'єднання (SSL-сертифікат):

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

$$P_{SSL} = \begin{cases} 1, \text{якщо } URL \text{ має } HTTPS \\ 0, \text{якщо } URL \text{ не має } HTTPS' \end{cases} \quad (6)$$

де P_{SSL} – ймовірність того, що сайт має захищене з'єднання, URL – URL-адреса вебсайту, $HTTPS$ – наявність захищеного з'єднання (SSL-сертифікат).

Важливим елементом у визначенні фішингових сайтів є наявність або відсутність іноземних якорів на вебсторінці. Якщо на сторінці є посилання, яке веде на інший домен, який не співпадає з основним доменом сайту, то це є ознакою підозрілого або фішингового сайту. Додавання до цього перевірки на наявність порожніх якорів або неправильних атрибутів, таких як javascript: void(0) або about:blank, дає змогу зібрати важливі дані для подальшого аналізу [1]. Ще одним важливим критерієм є наявність іноземних запитів на сайті, які відправляються на сторонні сервери для завантаження скриптів, зображень чи інших ресурсів. Фішингові сайти часто використовують ресурси з інших доменів, щоб здаватися легітимними. Однак на законних сайтах ці ресурси зазвичай запитуються з того ж домену або з надійних джерел. Тому перевірка на іноземні запити в контексті запитів до серверів для завантаження елементів сторінки є важливим елементом при виявленні фішингових сайтів.

Крім того, наявність шифрування куків, що зберігаються на вебсайті, також є важливою ознакою для виявлення фішингових сайтів. Куки використовуються для збереження інформації про сеанс користувача, і якщо ці куки належать до іноземного домену, це є важливим сигналом того, що сайт може бути фішинговим. За допомогою перевірки домену куків можна значно підвищити точність виявлення підроблених вебресурсів. Щодо аналізу URL, сучасні фішингові сайти часто використовують не тільки IP-адреси замість доменних імен, але й намагаються змінювати формат своїх URL, додаючи надмірні крапки або слеші, щоб збити з пантелику користувача. Така маніпуляція є поширеною серед фішингових ресурсів, тому важливо перевіряти кількість крапок та слешів у URL, що є ще однією ознакою фальшивих сайтів [2].

Збільшення точності передбачень виявлення фішингових сайтів є можливим завдяки сучасним методам машинного навчання та штучного інтелекту, які активно використовуються для автоматичного збору та аналізу ознак із вихідного коду сторінки та її URL. Сучасні алгоритми зможуть враховувати всі вищеописані ознаки, а також інші фактори, які з'являються в реальному часі. Наприклад, для аналізу фішингових сайтів можуть використовуватися дані з пошукових систем, де можна перевірити, чи відповідає сайт наданому URL. Завдяки впровадженню таких інноваційних підходів точність виявлення фішингових вебсайтів може бути значно покращена, що забезпечить додатковий захист для користувачів від шахрайства в Інтернеті. Врахування всіх зазначених ознак та інтеграція сучасних технологій дозволяє створити ефективну систему для виявлення фішингових ресурсів, що є необхідним кроком у боротьбі з кіберзлочинністю у цифрову еру.

Навчання з учителем є важливою задачею в машинному навчанні, яка полягає в побудові функції на основі попередньо наданих даних. Ці дані включають приклади, кожен з яких являє собою пару, що складається з вхідного об'єкта та бажаного значення виходу, яке також називають наглядовим сигналом. Алгоритми навчання з учителем аналізують ці навчальні дані та генерують класифікатор – функцію, яка може передбачати точні результати для нових, невідомих вхідних даних. Такий підхід активно використовується в багатьох сферах, включаючи виявлення фішингових вебсайтів, де класичні алгоритми класифікації, такі як багатошаровий перцептрон (MLP), індукція дерев рішень (J48) та наївний Байєс (NB), є основними інструментами для ефективного навчання та прогнозування [2, 4].

Багатошаровий перцептрон (MLP) є однією з найпоширеніших моделей нейронних мереж для класифікації. Вона складається з декількох шарів нейронів, де кожен шар має певну кількість одиниць, що відповідають за обробку інформації. Моделі MLP мають потужний потенціал для апроксимації будь-яких складних функцій за умови достатньої кількості даних

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

і прихованих одиниць. Ці мережі широко використовуються в задачах, де потрібно обробляти великий обсяг інформації, наприклад, для виявлення фішингових сайтів на основі численних характеристик, що можуть свідчити про їх підроблену природу.

Індукція дерев рішень (J48) є ще одним важливим методом класифікації, що дозволяє створювати правила для прогнозування вихідних значень на основі аналізу навчальних даних. Дерево рішень працює за принципом послідовного прийняття рішень, що дозволяє визначити клас для кожного нового екземпляра. Це метод, який добре масштабується і залишається ефективним навіть при роботі з великими обсягами даних, що містять велику кількість атрибутів. Використання алгоритму C4.5 (який реалізує J48) дозволяє ефективно класифікувати фішингові сайти, враховуючи численні фактори, які можуть вказувати на їх підроблену природу, зокрема наявність підозрілих доменних імен або непідтверджених записів у базі даних Whois.

Наївний Байєс (NB) є потужним класифікатором, який добре працює в умовах, коли ознаки є незалежними одна від одної. Хоча це припущення часто не виконується в реальному житті, наївний Байєс демонструє хороші результати в багатьох практичних завданнях, таких як класифікація фішингових сайтів. Алгоритм оцінює ймовірність приналежності нового зразка до певного класу, використовуючи ймовірнісні моделі, що базуються на статистичних даних, отриманих з навчальних зразків.

Для створення моделей прогнозування фішингових вебсайтів активно використовуються набори даних, такі як PHISHTANK, який є великим архівом зібраних фішингових сайтів. Ці дані включають як фішингові, так і легітимні вебсайти, що дозволяє розробляти моделі для точного розпізнавання підроблених ресурсів. Зазвичай для цього використовуються 17 ознак, таких як структура URL, наявність SSL-сертифікатів, доменне ім’я сайту та інші параметри, які можуть вказувати на підозрілу активність. Кожному сайту надається мітка класу, де фішингові сайти позначаються як -1, а легітимні – як +1 [1-3].

Алгоритми навчання, такі як MLP, J48 і NB, часто реалізуються за допомогою інструментів, таких як WEKA – потужного програмного пакету для машинного навчання, який надає користувачам графічний інтерфейс та великий набір інструментів для попередньої обробки даних. Оцінка ефективності моделей здійснюється через крос-валідацію, що дозволяє точно визначити, наскільки добре класифікатор здатний передбачити нові невідомі дані. Одним з основних критеріїв є прогностична точність, яка показує відсоток правильно класифікованих випадків на тестових даних. Аналіз результатів показує, що кожен із методів має свої сильні сторони. Наприклад, дерево рішень J48 демонструє високу точність прогнозування та швидкість навчання, що робить його ідеальним вибором для задач, де важлива швидкість обробки великих наборів даних. Водночас багатошаровий перцептрон та наївний Байєс також забезпечують високу ефективність, але їх результати можуть залежати від специфіки даних та вимог до точності. Враховуючи все вищезазначене, вибір алгоритму для виявлення фішингових сайтів залежить від конкретних умов застосування, вимог до точності, швидкості та масштабованості, що є актуальним для сучасних систем кібербезпеки.

Висновки. Таким чином, застосування алгоритмів контрольованого навчання для ефективного виявлення фішингових вебсайтів є критично важливим компонентом сучасних систем кібербезпеки. Використання класифікаційних алгоритмів, таких як наївний Байєс, дерево рішень і багатошаровий перцептрон, дозволяє не тільки точно ідентифікувати фішингові ресурси, але й адаптуватися до нових методів атак, що постійно еволюціонують у цифровому середовищі. Оцінка ефективності цих моделей показала, що класифікатор дерева рішень виявився найбільш результативним серед протестованих методів. Однак для досягнення максимальних результатів важливо мати достатню кількість навчальних даних, коректно обирати ознаки для аналізу та інтегрувати ці методи з іншими системами безпеки для створення комплексного захисту від сучасних кіберзагроз. Подальші дослідження та удосконалення алгоритмів дозволять ще ефективніше протистояти зростаючій кількості фішингових атак.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаних джерел

1. Yang, J., Zhang, J., & Zhang, Z. Detection of Phishing Websites Using Decision Trees and Naive Bayes / J. Yang, J. Zhang, Z. Zhang // International Journal of Computer Science and Information Security. – 2021. – Vol. 19, No. 4. – P. 123–130.
2. Tan, C. C., Krentel, J. B., & Zhang, A. S. Application of Multilayer Perceptron for Phishing Website Classification / C. C. Tan, J. B. Krentel, A. S. Zhang // Proceedings of the International Conference on Data Science and Machine Learning. – 2020. – Vol. 11, No. 2. – P. 78–85.
3. Le, T. S., & Wright, P. B. Improving Phishing Website Detection with Decision Trees and Ensemble Methods / T. S. Le, P. B. Wright // Journal of Cybersecurity Research. – 2022. – Vol. 14, No. 1. – P. 55–62.
4. Іваненко, О. О., & Литвиненко, В. М. Використання алгоритмів машинного навчання для виявлення фішингових вебсайтів / О. О. Іваненко, В. М. Литвиненко // Наукові праці Харківського національного університету радіоелектроніки. – 2020. – Т. 58, № 2. – С. 114–121.

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВОЇ Ю. Є.

СИСТЕМА АУТЕНТИФІКАЦІЇ КОРПОРАТИВНИХ КОРИСТУВАЧІВ НА ОСНОВІ ПРИВАТНИХ МЕРЕЖ ТА ПУБЛІЧНИХ КЛЮЧІВ

ЧАВА В. О., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто проблему створення безпечної системи аутентифікації для корпоративних користувачів у сучасних інформаційних системах. Зростання кіберзагроз, таких як несанкціонований доступ і компрометація даних, підкреслює важливість надійних методів ідентифікації. Запропоновано підхід на основі приватних мереж і публічних ключів, який включає особистий кабінет для співробітників, де вони можуть додавати свої ключі для доступу до ресурсів через захищені канали. Досліджено принципи роботи системи, її практичну реалізацію та переваги. Результати свідчать про високу ефективність запропонованого рішення для забезпечення безпеки та автоматизації доступу в корпоративному середовищі. Система може бути адаптована для різних типів підприємств і вдосконалена в майбутньому.

The article examines the challenge of developing a secure authentication system for corporate users in modern information systems. The rise in cyber threats, such as unauthorized access and data breaches, underscores the importance of reliable identification methods. An approach based on private networks and public keys is proposed, featuring a personal employee account where users can add their keys to access resources via secure channels. The study investigates the system's operating principles, practical implementation, and advantages. The findings indicate high effectiveness of the proposed solution in ensuring security and automating access within a corporate environment. The system can be adapted for various types of enterprises and improved further.

Актуальність. У сучасному світі, де підприємства дедалі більше покладаються на інформаційні технології для управління своїми процесами, питання кібербезпеки стають надзвичайно важливими і потребують постійної уваги. Одним із найкритичніших елементів

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

захисту є аутентифікація, тому що, процес, який дозволяє переконатися, що користувач, який намагається отримати доступ до корпоративних ресурсів, є саме тим, за кого себе видає, і має відповідні права на використання цих ресурсів. Традиційні методи, такі як паролі, уже не відповідають сучасним викликам, з якими стикаються компанії в умовах розвитку цифрових технологій. Наприклад, співробітники можуть забувати паролі, що призводить до затримок у роботі, записувати їх на папері, залишаючи вразливі місця для зловмисників, чи використовувати однакові комбінації для кількох систем, що значно спрощує завдання хакерам, які прагнуть отримати доступ до конфіденційних даних. За даними досліджень, приблизно 80% кібератак пов'язані з компрометацією облікових даних, що може спричинити витік конфіденційної інформації, серйозні фінансові втрати і навіть зупинку роботи компанії на невизначений час [1, с. 15].

У цьому контексті актуальність створення системи аутентифікації на основі приватних мереж і публічних ключів є очевидною і продиктована необхідністю підвищення рівня безпеки. Приватні мережі дозволяють ізолювати корпоративне середовище від зовнішнього світу, створюючи безпечний простір для роботи, де передача даних відбувається через захищені канали, недоступні для сторонніх осіб. Публічні ключі, у свою чергу, замінюють паролі на криптографічно захищений метод ідентифікації, який складно підробити чи викрасти навіть за допомогою сучасних технологій злому. Такий підхід не лише підвищує безпеку корпоративних систем, а й спрощує процес доступу для користувачів, адже їм більше не потрібно запам'ятовувати складні комбінації символів чи постійно змінювати паролі через вимоги безпеки. Крім того, інтеграція особистого кабінету для управління ключами додає зручності та автоматизації, що особливо важливо для великих компаній із сотнями чи тисячами співробітників, де ручне адміністрування доступу може бути вкрай трудомістким і схильним до помилок.

Проблема забезпечення безпеки ускладнюється ще й тим, що сучасні кіберзлочинці використовують дедалі хитріші методи атак, які постійно вдосконалюються. Наприклад, вони можуть створювати фальшиві Wi-Fi точки, щоб перехоплювати дані користувачів у громадських місцях, або надсилати підроблені листи від імені компанії, обманюючи співробітників і змушуючи їх розкривати свої облікові дані. У таких умовах традиційні системи, які покладаються лише на паролі чи одноразові коди, стають неефективними, адже паролі можна вгадати чи викрасти, а одноразові коди іноді перехоплюються через незахищені канали зв'язку. Запропонована система аутентифікації спрямована на вирішення цих проблем шляхом поєднання ізоляції мережі з надійною криптографією, що робить її актуальною для сучасних реалій і потреб бізнесу. Вона дозволяє не лише захистити дані від зовнішніх загроз, а й оптимізувати внутрішні процеси, пов'язані з управлінням доступом.

Крім того, існує велика потреба у системі, яка б не тільки забезпечувала безпеку, але й спрощувала процес управління доступом для адміністраторів, які відповідають за підтримку роботи корпоративних систем. Традиційні механізми контролю доступу часто є складними та трудомісткими, адже адміністраторам доводиться вручну видавати паролі, відстежувати їхню зміну чи вирішувати проблеми із забутими комбінаціями. Це може призводити до помилок або недостатньої захисної політики, коли, наприклад, співробітники використовують слабкі паролі через брак часу чи знань. Запропонована система має на меті вирішити ці проблеми, пропонуючи інтегрований підхід, який поєднує технічні переваги приватних мереж і криптографічних ключів, що дозволяє автоматизувати багато процесів і зменшити навантаження на персонал, відповідальний за безпеку.

Окремо варто наголосити на тому, що зростання віддаленої роботи в останні роки ще більше підкреслює актуальність такого рішення. Співробітники все частіше працюють із дому чи інших локацій поза офісом, підключаючись до корпоративних ресурсів через різні мережі, які не завжди є безпечними. У таких умовах традиційні методи аутентифікації стають ще більш уразливими, а потреба в системі, яка б забезпечувала надійний захист і зручність,

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

зростає. Запропонований підхід дозволяє вирішити ці питання, пропонуючи безпечний і простий спосіб доступу до ресурсів незалежно від місця перебування користувача.

Метою статті є розробка концепції системи аутентифікації корпоративних користувачів на основі приватних мереж і публічних ключів, аналіз її можливостей і практичної реалізації з урахуванням потреб сучасних підприємств у захисті даних і спрощенні процесів адміністрування доступу. Дослідження спрямоване на те, щоб показати, як цей підхід може підвищити безпеку доступу до корпоративних ресурсів і водночас зробити управління ним зручнішим і ефективнішим для організацій різного масштабу.

Об'єктом дослідження є процес аутентифікації користувачів у корпоративних системах, зокрема в умовах використання ізольованих мереж, які створюють додатковий рівень захисту від зовнішніх загроз.

Предметом дослідження виступають технології та методи створення системи аутентифікації, що базуються на приватних мережах і криптографічних ключах, а також їхня взаємодія з інтерфейсом для користувачів і адміністраторів.

Аналіз попередніх досліджень. Питання забезпечення безпеки доступу до корпоративних ресурсів давно привертає увагу дослідників, які працюють над проблемами кібербезпеки та інформаційних технологій. У роботі Кравця О. І. розглядаються основи кібербезпеки, зокрема принципи створення захищених мереж, які дозволяють ізолювати дані від зовнішніх загроз. Автор підкреслює, що ізоляція даних через приватні мережі є першим кроком до захисту від хакерських атак чи перехоплення трафіку, але зазначає, що для повноцінного захисту потрібні додаткові механізми ідентифікації, які б доповнювали цей базовий рівень безпеки [1, с. 45]. Tanenbaum A. S. і Wetherall D. J. у своїй книзі про комп'ютерні мережі детально описують криптографічні методи, такі як асиметричне шифрування, яке лежить в основі роботи публічних ключів. Вони пояснюють, що такі методи дозволяють уникнути передачі конфіденційної інформації через мережу, що робить їх стійкими до атак типу «людина посередині», коли зловмисник намагається перехопити дані між користувачем і сервером [2, с. 720]. Ці автори звертають увагу на те, що управління ключами може бути складним завданням, яке потребує продуманого підходу для практичного впровадження.

Швець В. М. у своєму дослідженні акцентує на практичних аспектах захисту інформації в комп'ютерних системах, наголошуючи на тому, що аутентифікація є слабкою ланкою в багатьох організаціях через використання традиційних методів, таких як паролі. Він пропонує використовувати криптографію для її посилення, однак у його роботі мало уваги приділено тому, як ці методи можна інтегрувати з приватними мережами для створення комплексного рішення. Зарубіжні автори, наприклад Schneier B., досліджують еволюцію методів аутентифікації, зазначаючи, що перехід від паролів до ключів є логічним кроком у розвитку безпеки, адже ключі значно складніше викрасти чи підробити. Він також підкреслює важливість простоти для кінцевих користувачів, адже надто складні системи можуть створювати незручності в повсякденній роботі [4, с. 102].

У літературі часто згадується використання VPN як інструменту безпеки, який дозволяє ізолювати корпоративні ресурси від зовнішнього світу. Однак їхнє поєднання з особистими кабінетами та ключами для автоматизації доступу розглядається рідко, що залишає простір для подальших досліджень. Саме цю прогалину намагається заповнити дана стаття, пропонуючи практичне рішення для корпоративного середовища, яке поєднує в собі ізоляцію мережі, криптографічну ідентифікацію та зручний інтерфейс для управління доступом.

Виклад основного матеріалу. Сучасні підприємства стикаються з безпрецедентним рівнем кіберзагроз, які загрожують їхнім даним і операційній діяльності, що робить питання безпеки одним із головних пріоритетів у роботі будь-якої організації, незалежно від її розміру чи сфери діяльності. Аутентифікація користувачів є першим і найважливішим бар'єром на шляху зловмисників, які намагаються отримати доступ до цінної інформації чи систем

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

компанії, але традиційні методи, що використовувалися раніше, вже не здатні повною мірою справлятися з новими викликами, які з'явилися в цифрову епоху завдяки швидкому розвитку технологій і методів атак. Наприклад, паролі, які довгий час вважалися основним інструментом захисту, можуть бути легко вгадані за допомогою спеціалізованих програм, що застосовують методи грубої сили для підбору комбінацій, викрадені через фішингові атаки, коли співробітники через необережність розкривають свої дані, або просто забуті самими користувачами, що призводить до затримок у робочих процесах і створює додаткове навантаження на IT-відділ компанії. Запропонована система аутентифікації, яка базується на використанні приватних мереж і публічних ключів, покликана усунути ці недоліки, пропонуючи більш безпечне, надійне та зручне рішення, яке відповідає потребам сучасних компаній у захисті даних і спрощенні доступу до корпоративних ресурсів у різних умовах роботи.

Приватна мережа є ключовою технологією, яка дозволяє ізолювати корпоративні ресурси від зовнішнього доступу, створюючи захищене середовище для роботи співробітників і забезпечуючи безпеку передачі даних. Найпоширенішим і широко відомим прикладом такої технології є віртуальна приватна мережа, більш відома як VPN (Virtual Private Network), яка створює зашифрований тунель між пристроєм користувача і сервером компанії, через який відбувається весь обмін інформацією. Наприклад, співробітник, який працює з дому, перебуває в дорозі чи в іншому віддаленому місці, може запустити клієнт VPN на своєму комп'ютері чи навіть мобільному пристрої, підключитися до корпоративної мережі й отримати доступ до внутрішніх ресурсів, таких як база даних із клієнтською інформацією, поштовий сервер для робочої переписки чи внутрішній портал для спілкування між колегами. Усе, що відбувається поза межами цієї мережі, залишається абсолютно недоступним для зовнішніх користувачів, що значно знижує ризик перехоплення даних зловмисниками. Такий підхід ефективно захищає від атак, які базуються на перехопленні інформації в незахищених мережах, наприклад у громадських Wi-Fi зонах у кафе, аеропортах чи готелях, де зловмисники можуть легко отримати доступ до трафіку, якщо користувач не застосовує додаткових засобів захисту. Завдяки використанню внутрішніх IP-адрес, таких як діапазон 192.168.1.0/24, який є стандартним для локальних мереж, адміністратори мають змогу точно контролювати, хто саме підключається до системи, що додає ще один рівень захисту до загальної структури безпеки і дозволяє уникнути несанкціонованих проникнень.

Публічні ключі, у свою чергу, замінюють традиційні паролі на криптографічно захищений метод ідентифікації, який є значно стійкішим до сучасних загроз і забезпечує вищий рівень безпеки. Кожен співробітник у рамках цієї системи генерує два ключі: приватний, який зберігається виключно на його пристрої і ніколи нікому не передається, залишаючись конфіденційним, і публічний, який додається до системи через спеціально розроблений особистий кабінет у веб-інтерфейсі компанії. Під час спроби підключення сервер автоматично перевіряє, чи збігаються ці ключі за допомогою криптографічних алгоритмів, і лише після успішної перевірки надає доступ до потрібних ресурсів, таких як внутрішні сервери чи бази даних. Наприклад, співробітник може згенерувати пару ключів за допомогою програми, такої як PuTTYgen, яка пропонує зручний графічний інтерфейс для користувачів із мінімальним технічним досвідом, або ввести команду ssh-keygen у терміналі, якщо він має базові знання роботи з командним рядком, після чого завантажити свій публічний ключ у особистий кабінет через веб-інтерфейс компанії. Цей метод має суттєві переваги порівняно з традиційними паролями. По-перше, ключі неможливо вгадати чи викрасти через фішинг, оскільки приватний ключ ніколи не залишає пристрій користувача і не передається мережею, що робить його недосяжним для зловмисників. По-друге, кожен ключ є унікальним для конкретного користувача, що дозволяє системі точно ідентифікувати, хто саме намагається підключитися, уникаючи плутанини чи помилок. По-третє, процес аутентифікації відбувається автоматично після початкового налаштування, без необхідності вводити

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

додаткові дані, що економить час співробітників і робить їхню щоденну роботу значно зручнішою та ефективнішою.

Для практичної реалізації системи враховують технічні деталі, що забезпечують працездатність і безпеку. Сервер встановлюють на базі OpenVPN або WireGuard. Ці технології відкриті, мають розвинену документацію та підтримку спільноти. OpenVPN популярне рішення з потужним шифруванням, наприклад AES-256, сумісне з Windows, macOS, Linux і мобільними платформами. WireGuard нова технологія з високою швидкістю й простотою налаштування завдяки алгоритмам типу ChaCha20, ідеальна для компаній із багатьма підключеннями. Ключі генерують інструментами ssh-keygen, який швидко створює пари в Unix-системах, або OpenSSL із ширшими можливостями для криптографії, сертифікатів і шифрування. Публічні ключі зберігають у базі даних, наприклад MySQL, для зручного управління, приватні залишаються на пристроях користувачів. Приватні ключі шифрують паролем для захисту від крадіжки при втраті пристрою, що унеможливлює їхнє використання без пароля. Адміністратор керує доступом через файли authorized_keys на SSH-сервері або централізовані системи типу LDAP, які ефективні для великих організацій зі складною структурою.

Процес реалізації системи складається з кількох ключових етапів, які можна адаптувати до потреб конкретної компанії залежно від її розміру, специфіки роботи чи технічних вимог. На першому етапі встановлюється VPN-сервер, який видає користувачам унікальні сертифікати для підключення до мережі, що гарантує безпечне з'єднання. Кожен співробітник отримує файл конфігурації, який дозволяє запустити клієнт VPN на його пристрої – це може бути ноутбук, настільний комп'ютер чи навіть смартфон, що робить систему гнучкою і придатною для використання в різних сценаріях, включаючи віддалену роботу чи відрядження. Далі розробляється простий веб-інтерфейс, який виконує функцію особистого кабінету, де користувач може легко завантажити свій публічний ключ через спеціальну форму з кнопкою «Додати ключ», що спрощує процес для людей без глибоких технічних знань. Сервер налаштовується таким чином, щоб перед наданням доступу перевіряти ключі за допомогою стандартних протоколів, таких як SSH (Secure Shell), які широко застосовуються в корпоративних системах завдяки своїй надійності, безпеці та легкості інтеграції з іншими технологіями. Адміністратор визначає права доступу для кожного користувача через свою панель управління, що дозволяє гнучко налаштовувати систему. Наприклад, бухгалтер отримує доступ лише до фінансових даних, таких як бази з інформацією про платежі чи фінансові звіти, тоді як програміст може підключатися до серверів розробки чи тестування програмного забезпечення, що забезпечує чітке розмежування прав залежно від ролі працівника в компанії.

Один із можливих сценаріїв використання системи виглядає наступним чином. Співробітник Анна заходить на сайт компанії через браузер, відкриває свій особистий кабінет за допомогою тимчасового пароля, який вона отримала від адміністратора під час первинної реєстрації в системі, і завантажує свій публічний ключ, який вона заздалегідь згенерувала за допомогою одного з доступних інструментів, таких як PuTTYgen чи ssh-keygen. Потім вона встановлює VPN-клієнт на своєму ноутбуці, використовуючи отриманий файл конфігурації, запускає його й успішно підключається до корпоративної мережі. Після цього система автоматично перевіряє її ключ за лічені секунди і відкриває доступ до потрібного ресурсу, наприклад до бази даних із робочою інформацією чи внутрішнього порталу для комунікації з колегами. Увесь процес займає мінімум часу і не потребує введення паролів чи одноразових кодів, що робить його надзвичайно зручним для повсякденної роботи, особливо в умовах напруженого графіку чи віддаленої взаємодії.

Система має переваги, привабливі для корпоративного середовища. Безпека через ізоляцію мережі VPN і криптографію унеможливлює несанкціонований доступ, адже без унікального приватного ключа зловмисник не підключиться, навіть перехопивши трафік.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Користувачам не треба запам’ятовувати паролі чи чекати одноразові коди, що спрощує роботу й підвищує продуктивність. Права доступу швидко змінюються через адмінпанель, дозволяючи реагувати на кадрові зміни, наприклад звільнення чи переведення. Проте є виклики. Співробітникам без досвіду складно генерувати ключі в ssh-keygen чи PuTTYgen, що вимагає навчання або інструкцій. Налаштування VPN-сервера й кабінету потребує часу, ресурсів і досвіду IT-відділу, що може ускладнити впровадження в невеликих організаціях з обмеженим штатом чи бюджетом.

Для полегшення впровадження системи можна розробити детальну інструкцію для користувачів із покроковими поясненнями, як генерувати ключі, завантажувати їх у особистий кабінет і підключатися до мережі, що значно знизить бар’єри для новачків. Ще одним практичним рішенням могло б стати додавання автоматичного генератора ключів безпосередньо в особистий кабінет. Наприклад, у веб-інтерфейсі могла б бути кнопка «Створити ключ», після натискання якої система сама генерує пару ключів, показує користувачу, де зберегти приватний ключ на його пристрої, і автоматично додає публічний ключ до бази даних сервера. Це значно спростило б процес для співробітників без технічних навичок і зменшило б навантаження на адміністраторів, які часто змушені витрачати час на індивідуальну допомогу працівникам із технічними питаннями, такими як налаштування ключів чи підключення до VPN.

У сучасному світі кібербезпека є важливим напрямком розвитку технологічних систем, адже загрози, з якими стикаються підприємства, стають дедалі складнішими і багатограннішими, охоплюючи широкий спектр методів атак. Хакери можуть використовувати не лише вразливості паролів, але й застосовувати техніки соціального інженерингу, фішингові кампанії чи перехоплення мережевого трафіку в незахищених мережах, що робить традиційні методи захисту менш ефективними і вимагає переходу до більш сучасних підходів. У такому контексті надзвичайно важливо забезпечити надійний захист доступу до корпоративних ресурсів і водночас спростити процес управління цим доступом для адміністраторів, які відповідають за безпеку систем і підтримку їхньої стабільної роботи.

Захист корпоративних ресурсів ускладнює велика кількість співробітників із унікальними обліковими записами, які потребують доступу до даних залежно від обов’язків. Традиційні методи контролю доступу часто призводять до помилок чи слабкої безпеки, коли працівники обирають прості паролі через брак часу або знань, а адміністратори не встигають оновлювати права після кадрових змін. Приватні мережі ізолюють корпоративне середовище, обмежуючи доступ лише авторизованим користувачам через захищений канал, що запобігає зовнішнім вторгненням. Публічні ключі замінюють паролі на криптографічно безпечний метод ідентифікації, який важко підробити чи викрасти навіть сучасними технологіями злому. Це підвищує безпеку та спрощує доступ, усуваючи потребу запам’ятовувати складні паролі чи вводити одноразові коди, що затримують роботу.

Крім того, інтеграція особистого кабінету для управління ключами додає зручності і автоматизацію, що є важливим для ефективної роботи як співробітників, так і адміністраторів. Особистий кабінет дозволяє кожному працівнику самостійно завантажувати свій публічний ключ, який потім використовується для аутентифікації, що значно спрощує процес управління доступом для адміністратора і зменшує його робоче навантаження. Адміністратор може контролювати всі ключі через один централізований інтерфейс, додаючи чи видаляючи їх за потреби, що особливо актуально для великого підприємства, де працює багато різних категорій користувачів із різними рівнями доступу. Наприклад, бухгалтерський відділ може мати доступ лише до фінансових даних, таких як звіти про доходи чи бази платежів, тоді як технічний відділ отримує доступ до серверів розробки чи тестування програмного забезпечення, що дозволяє чітко розмежовувати права. Такий гнучкий підхід покращує

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

безпеку і оптимізує роботу всієї організації, дозволяючи швидко адаптуватися до змін у структурі чи штаті компанії без значних зусиль.

Для реалізації системи потрібні технології, що забезпечують працездатність і безпеку. Сервер можна встановити на базі OpenVPN з підтримкою багатьох платформ і налаштуваннями шифрування. WireGuard, як сучасна альтернатива, використовує алгоритми, наприклад ChaCha20, що забезпечує швидкість і ефективність, особливо для компаній із багатьма підключеннями, де важливі стабільність і продуктивність. Ключі генеруються через ssh-keygen, який створює безпечні пари ключів у Unix-системах, або OpenSSL є універсальний інструмент для SSH-ключів, сертифікатів і шифрування. Публічні ключі зберігаються в базі даних (MySQL чи PostgreSQL), де адміністратор керує доступом, а приватні на пристроях користувачів, що унеможливлює їх перехоплення. Приватні ключі рекомендується шифрувати паролем для захисту від крадіжки, наприклад, при втраті пристрою, що критично для компаній, де працівники використовують власні гаджети поза контролем IT-відділу. Адміністратор налаштовує права через файли authorized_keys на SSH-сервері або системи типу LDAP для великих організацій. Контроль доступу гнучкий, дозволяючи задавати права залежно від ролі користувача, що адаптує систему до потреб бізнесу.

Перспективи подальшого розвитку системи пов’язані з її вдосконаленням для ширшого використання в різних типах організацій. У майбутньому можна розробити програмне забезпечення для автоматичного створення ключів, що полегшило б процес для користувачів без технічних навичок, які можуть не знати, як працювати з командним рядком чи графічними програмами для генерації ключів, такими як PuTTYgen. Також можлива інтеграція системи з хмарними платформами, такими як AWS (Amazon Web Services) або Microsoft Azure, для роботи з віддаленими серверами, що дозволило б масштабувати рішення для великих компаній із розподіленими ресурсами чи командами, які працюють у різних географічних регіонах. Ще одна перспективна ідея полягає у спрощенні інтерфейсу особистого кабінету, щоб зробити його більш інтуїтивним і доступним для співробітників, наприклад, додавши графічні підказки, які пояснюють кожен крок, чи адаптацію під мобільні пристрої, такі як смартфони й планшети, що активно використовуються в сучасному робочому середовищі.

Порівняння методів аутентифікації дозволяє краще зрозуміти переваги запропонованого підходу і його місце серед інших рішень. У таблиці нижче наведено основні характеристики різних методів, які використовуються для ідентифікації користувачів у корпоративних системах, що наочно демонструє, чому публічні ключі є кращим вибором у сучасних умовах завдяки балансу безпеки, зручності та керованої складності.

Таблиця 1

Порівняння методів аутентифікації

Метод аутентифікації	Безпека	Зручність	Складність
Паролі	Низька	Висока	Низька
Одноразові коди	Середня	Низька	Висока
Публічні ключі	Висока	Середня	Середня

Джерело: розроблено автором

Додаткові сценарії використання системи показують її універсальність і практичність. Крім стандартного використання для доступу до корпоративних ресурсів у межах офісу, система може бути застосована в різних ситуаціях, які часто виникають у сучасних компаніях. Удалена робота дозволяє співробітникам безпечно підключатися до корпоративних ресурсів через приватну мережу з будь-якої точки світу, що особливо актуально в умовах зростання віддаленої зайнятості. Мобільні пристрої, такі як смартфони чи планшети, можуть

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

використовувати публічні ключі для аутентифікації, що зменшує ризики при використанні паролів, які незручно вводити на маленьких екранах. Інтеграція з хмарними платформами дозволяє користувачам отримувати доступ до віддалених серверів, що є важливим для великих підприємств із розподіленими командами чи ресурсами.

Висновки. Запропонована система аутентифікації на основі приватних мереж і публічних ключів є сучасним рішенням для захисту доступу до ресурсів підприємства в умовах кіберзагроз. Приватні мережі ізолюють середовище, блокуючи загрози, як-от перехоплення даних чи несанкціоноване проникнення. Публічні ключі забезпечують ідентифікацію без паролів, усуваючи слабкі місця, пов'язані з людським фактором. Особистий кабінет додає зручності, дозволяючи керувати ключами та правами доступу. Результати показують, що підхід підвищує безпеку й спрощує адміністрування порівняно з традиційними методами.

Подальший розвиток системи може включати кілька напрямків, які зроблять її ще більш практичною і доступною. Розробка програмного забезпечення для автоматичного створення ключів могла б спростити процес для користувачів, які не мають технічних знань, дозволяючи генерувати ключі прямо в кабінеті без необхідності використання командного рядка чи сторонніх програм. Інтеграція з хмарними платформами, такими як AWS або Microsoft Azure, дозволила б масштабувати систему для роботи з віддаленими серверами, що особливо актуально для великих компаній із розподіленими ресурсами.

Список використаних джерел

1. Кравець О.І. Основи кібербезпеки інформаційних систем: навчальний посібник / О.І. Кравець. – Львів: Видавництво Львівської політехніки, 2020. – 248 с.
2. Tanenbaum A.S. Computer Networks / A.S. Tanenbaum, D.J. Wetherall. – 6th ed. – Pearson, 2021. – 960 p.
3. Швець В.М. Захист інформації в комп'ютерних системах / В.М. Швець // Вісник Київського національного університету імені Тараса Шевченка. – 2019. – № 45. – С. 78–85.
4. Schneier B. Cryptography Engineering / B. Schneier. – Wiley, 2022. – 384 p.

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВОЇ Ю. Є.

ОГЛЯД МЕТОДІВ ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У БІЛІНГОВИХ СИСТЕМАХ ЗА ДОПОМОГОЮ АЛГОРИТМУ RC4

ЧАЙКА Б. П., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглянуто актуальні аспекти захисту персональних даних у білінгових системах комунікаційних і мережевих сервісів шляхом використання криптографічних методів. Особливу увагу приділено проблемі забезпечення конфіденційності, цілісності та автентичності інформації, яка містить дані користувачів, фінансові транзакції та історію сеансів підключення. Обґрунтовано доцільність застосування потокового шифру RC4 як ефективного засобу захисту, що забезпечує високу швидкість обробки даних і мінімальні обчислювальні витрати. Запропоновано механізм використання цього алгоритму для запобігання несанкціонованому доступу та модифікації білінгової інформації, що є важливим етапом у підвищенні рівня безпеки сучасних інформаційних систем.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

The article discusses the relevant aspects of personal data protection in billing systems for communication and network services through the use of cryptographic methods. Special attention is given to the issue of ensuring confidentiality, integrity, and authenticity of information containing user data, financial transactions, and session connection history. The appropriateness of using the RC4 stream cipher is substantiated as an effective means of protection, providing high data processing speed and minimal computational costs. A mechanism for utilizing this algorithm to prevent unauthorized access and modification of billing information is proposed, which is a crucial step in enhancing the security level of modern information systems.

Актуальність. У сучасних умовах розвитку цифрових технологій та зростання обсягів персональних даних, що обробляються в телекомунікаційних та мережевих системах, питання захисту конфіденційної інформації стає особливо важливим. Білінгові системи містять чутливі дані користувачів, зокрема їхні фінансові транзакції, історію підключень та персональні ідентифікаційні відомості, що робить їх привабливою мішенню для кібератак та несанкціонованого доступу. Традиційні методи захисту не завжди гарантують достатній рівень безпеки, особливо з урахуванням постійного вдосконалення атак та методів зламу криптографічних алгоритмів. У зв'язку з цим актуальним є дослідження та впровадження ефективних методів шифрування, зокрема потокового шифру RC4, який відзначається високою швидкістю обробки даних та можливістю реалізації у ресурсозалежних системах. Застосування цього алгоритму в білінгових системах дозволяє мінімізувати ризики несанкціонованого доступу, збереження цілісності та конфіденційності інформації, що є ключовим завданням у забезпеченні безпеки сучасних інформаційних технологій. Актуальність дослідження також полягає в необхідності адаптації криптографічних методів до нових загроз, які виникають через розвиток технологій і збільшення обсягів даних, що потребують захисту в умовах постійно змінюваного кіберпростору.

Метою статті є дослідження сучасних методів захисту персональних даних у білінгових системах телекомунікаційних і мережевих сервісів шляхом використання криптографічного алгоритму RC4, зокрема через аналіз аспектів забезпечення конфіденційності, цілісності та автентичності даних користувачів, фінансових транзакцій і історії підключень, дослідження переваг і недоліків потокового шифру RC4, оцінку його стійкості до атак і можливостей оптимізації для підвищення ефективності в умовах реального використання, а також розробку рекомендацій щодо впровадження цього алгоритму з метою запобігання несанкціонованому доступу та модифікації білінгової інформації.

Об'єктом дослідження є процес шифрування персональних даних в білінгових системах із використанням алгоритму RC4.

Предмет дослідження – підходи до розробки, реалізації та оцінки ефективності застосування алгоритму шифрування RC4 для забезпечення конфіденційності та безпеки персональних даних у білінгових системах, а також порівняння цього алгоритму з іншими методами шифрування з точки зору швидкості, надійності та рівня захисту інформації в умовах специфіки роботи білінгових систем.

Аналіз попередніх досліджень. Алгоритм RC4 є однією з найбільш використовуваних криптографічних технологій для шифрування персональних даних у білінгових системах. Розроблений Роном Рівестом, він забезпечує високу швидкість шифрування та ефективний захист даних при передачі через мережу [1]. Однак, хоча RC4 має переваги, вчені, зокрема Елія Крейн і Аді Шамір, вказують на вразливості, такі як небезпека повторного використання ключів, що може призвести до атак на шифрування [2]. Брюс Шнайєр наголошує на важливості регулярної зміни ключів та використання додаткових протоколів для посилення безпеки [3]. Шаул Розенберг підкреслює необхідність належного управління ключами та їх частого оновлення для мінімізації вразливостей [4]. Попри ефективність RC4, для його

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

безпечного використання в білінгових системах необхідно поєднувати алгоритм з іншими заходами захисту даних.

Виклад основного матеріалу. Технологічні досягнення, особливо у сфері систем безпеки даних, значно покращили процес захисту інформації, що є важливим аспектом у сучасному світі. Проблеми безпеки, які сьогодні викликають значне занепокоєння, включають засоби захисту даних, безпеку мереж, безпеку віртуалізації, цілісність застосунків та управління ідентичністю, які використовуються в різноманітних сервісах. Процес захисту даних спрямований на запобігання крадіжці або перехопленню даних хакерами, кракерами, кардерами, фрікерами та іншими зловмисниками. Захист даних на комп'ютерах може забезпечити захист інформації від несанкціонованого доступу. Надсилання даних або інформації без належного захисту несе в собі ризик перехоплення, тому для забезпечення безпеки даних необхідно використовувати криптографічні методи.

Інтернет речей (IoT) є комерційною революцією, і впровадження пристроїв IoT в підприємствах сприяє успіху в управлінні даними, а також в загальному успіху організацій. Використання систем бізнес-аналізу є не лише технологічним, а й соціальним рішенням для поліпшення комунікації та надання швидкого доступу до інформації. У той же час, удосконалення безпеки бізнес-інформації може призвести до технологічних і нетехнічних збитків, загроз та порушень принципів безпеки бізнес-інформації.

Основною метою цього дослідження є вивчення впливу безпеки даних на впровадження систем бізнес-аналізу. Техніка шифрування потоком RC4 широко використовується завдяки своїй простоті реалізації в різних додатках і підтвердженій безпеці для використання. Шифрування з використанням техніки Rivest Code 4 (RC4) є одним з численних моделей та підходів, що доступні для захисту даних. Результатом цього дослідження є використання програми шифрування потоком RC4, при цьому кількість оригінальних символів (відкритий текст), успішно зашифрованих, дорівнює кількості зашифрованих символів (шифротекст), що дозволяє зберігати введені дані в зашифрованому вигляді в базі даних, забезпечуючи таким чином безпеку та конфіденційність даних [3].

Найбільш широко використовуваним програмним забезпеченням для шифрування потоком є RC4, також відоме як ARCFOUR (підозрюваний RC4). RC4 також використовується в відомих протоколах, таких як SSL (Secure Sockets Layer), що захищає інтернет-трафік, і WEP, що забезпечує безпеку бездротових мереж. Безпека повідомлень, даних або інформації в процесі передачі або зберігання даних є однією з найважливіших складових комп'ютерної та комп'ютерної мережевої комунікації і стала однією з рушійних сил розвитку криптографічних технологій. Криптографія – це техніка кодування даних, яка підтримує два основні елементи інформаційної безпеки: секретність і конфіденційність. Техніка шифрування потоком RC4 широко застосовується через свою простоту реалізації в різноманітних додатках і підтверджену безпеку для використання. У сучасному світі захист персональних даних є надзвичайно важливим аспектом, оскільки дані можуть бути конфіденційними і вимагають відповідного захисту для збереження своєї конфіденційності. Криптографія є одним із основних способів забезпечення захисту даних, і одним з алгоритмів, який активно використовується для шифрування даних, є алгоритм шифрування потоком RC4. Цей метод є ефективним засобом для забезпечення конфіденційності та автентичності даних і дозволяє покращити аспекти безпеки інформації, що передається або зберігається в інформаційних системах, таких як білінгові системи. Криптографія є науковою галуззю, яка вивчає методи кодування та захисту даних за допомогою різних алгоритмів. Зокрема, текстові дані, що містять літери, цифри та символи, є типовими для обробки в рамках криптографії, і одним з основних завдань є перетворення таких даних у шифротекст, щоб унеможливити їх розкриття особами, які не мають відповідних прав доступу. Проте однією з проблем є те, що шифрування даних іноді може збільшувати їх обсяг, що створює труднощі для ефективного зберігання і передачі

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

інформації. Для вирішення цієї проблеми використовуються такі методи шифрування, як блочні шифри та поточні шифри, до яких належить й RC4 [1–2, 4].

Захист даних може бути здійснений двома основними способами: перший – це налаштування прав доступу для кожного користувача в базі даних, а другий – це забезпечення безпеки самих даних, що зберігаються в базі даних, шляхом їх шифрування. У випадку білінгових систем для Інтернет-кафе всі дані зазвичай зберігаються в базі даних MySQL, що значно полегшує моніторинг активності користувачів, зокрема кількості споживачів і тривалості їх використання послуг. Така система дозволяє легко реєструвати транзакції і здійснювати контроль за доступом до інтернет-ресурсів у реальному часі. Алгоритм шифрування потоком RC4 є одним з найбільш широко використовуваних методів для шифрування даних. Він дозволяє перетворювати оригінальні дані на певні символи, що робить їх недоступними для осіб, які не мають відповідного ключа для дешифрування. Алгоритм шифрування RC4 простий у реалізації та ефективний у застосуванні в різних інформаційних системах, таких як білінгові системи. Для його реалізації достатньо використовувати стандартні апаратні специфікації, такі як процесор мінімум Pentium III, оперативну пам’ять 64 MB, жорсткий диск 5 GB та відеокарту з роздільною здатністю SVGA.

Для розробки програм, що реалізують цей алгоритм, зазвичай використовуються програмні засоби, такі якPython, C#, або Java, а також операційні системи Windows 98 SE, Windows ME або Windows XP. Програма, що реалізує шифрування потоком RC4, зазвичай включає в себе процес генерації псевдовипадкових байтів за допомогою ключа, які потім підлягають операціям XOR з відкритим текстом для отримання шифротексту. Для дешифрування шифротексту достатньо повторно застосувати операцію XOR з тими ж псевдовипадковими байтами, що дозволяє відновити оригінальний текст. Таким чином, алгоритм RC4 є ефективним методом шифрування даних, що застосовується для захисту конфіденційної інформації в білінгових системах і інших додатках, що вимагають високого рівня безпеки даних. Для забезпечення безпеки в білінгових системах важливо враховувати, що ефективність алгоритму RC4 залежить від належного управління ключами та регулярного оновлення цих ключів, оскільки їх повторне використання може призвести до вразливостей. Сучасні підходи до шифрування даних рекомендують комбінувати RC4 з іншими методами захисту, такими як багатофакторна аутентифікація та використання більш складних протоколів, наприклад, TLS. Хоча RC4 є швидким і ефективним алгоритмом, його вразливості можуть бути усунуті за допомогою гібридних рішень, що включають в себе також алгоритми шифрування AES для підвищення безпеки. Крім того, при розробці систем з використанням RC4 важливо також враховувати можливість атак типу криптоаналізу, тому використання додаткових захисних механізмів є необхідним для зниження ризиків. Враховуючи сучасні вимоги до безпеки, застосування алгоритму RC4 слід обмежити, а для критичних додатків – використовувати новітні криптографічні стандарти, що відповідають міжнародним вимогам.

Алгоритм шифрування потоком RC4 є потужним інструментом для захисту персональних даних у білінгових системах, адже він дозволяє ефективно шифрувати інформацію, забезпечуючи її конфіденційність. У процесі шифрування використовуються кілька ключових компонентів: відкритий текст (plaintext), який підлягає шифруванню, та ключ (key), що забезпечує унікальність і безпеку перетворення даних. Наприклад, відкритий текст може мати вигляд: 101 110 107 114 105 112 115 105 (в Ascii-форматі), що представляє собою послідовність чисел, яка відповідає певним символам, таким як літери і цифри, що є частиною конфіденційних даних. Ключ для шифрування, який використовується в алгоритмі RC4, може бути довільної довжини і забезпечує унікальність шифрування для кожної конкретної сесії. Залежно від довжини ключа, RC4 генерує псевдовипадкові байти, які потім комбінуються з відкритим текстом для створення шифротексту. Цей процес гарантує, що дані, що передаються в білінговій системі, залишаються захищеними від сторонніх осіб, навіть у випадку перехоплення інформації. Важливим аспектом є те, що алгоритм RC4 використовує метод шифрування потоком, що дозволяє обробляти дані послідовно, не збільшуючи їх розмір, що є

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

важливим фактором у реальному часі при обробці великої кількості запитів. Завдяки високій швидкості шифрування та дешифрування RC4 є ідеальним для використання в білінгових системах, де необхідно швидко і безпечно обробляти транзакції. Крім того, цей алгоритм забезпечує високу гнучкість, оскільки може бути адаптований до різних умов і типів даних, що дозволяє ефективно захищати як текстову, так і числову інформацію [1-2].

Для забезпечення шифрування використовують певний ключ, наприклад, слово «computer», що у Ascii-форматі виглядає як: 107 111 109 112 117 116 101 114. Цей ключ є важливим елементом, оскільки він генерує псевдовипадкові байти, які потім використовуються для шифрування відкритого тексту. Кожен з елементів відкритого тексту підлягає операціям XOR з відповідними байтами ключа, генерованими з ключа, що створює шифротекст. Це забезпечує захист даних, оскільки навіть якщо зловмисник отримає доступ до шифротексту, без відповідного ключа він не зможе відновити оригінальну інформацію. Процес шифрування потоком RC4 дозволяє ефективно обробляти великі обсяги даних, що особливо важливо для білінгових систем, де потрібно швидко і безпечно передавати персональні дані клієнтів, такі як історія транзакцій або особисті реквізити. Оскільки алгоритм працює з потоком байтів, його легко адаптувати до різних типів даних, що робить його гнучким для використання в різних секторах. Ключові особливості RC4 включають простоту його реалізації, високу швидкість виконання та здатність до обробки даних без значного збільшення їх обсягу, що робить його ідеальним для середовищ з обмеженими ресурсами, таких як білінгові системи. Важливо, що забезпечення безпеки даних через RC4 має також враховувати належну обробку ключів, щоб уникнути їх компрометації та збереження конфіденційності при передачі інформації.

У білінгових системах, де важливо забезпечити захист персональних даних користувачів, алгоритм RC4 дозволяє перетворювати чутливу інформацію в такий вигляд, який неможливо зчитати без правильного ключа для дешифрування. Таким чином, цей метод шифрування є ефективним способом забезпечення конфіденційності та цілісності даних, що обробляються у реальному часі в рамках білінгових процесів. Алгоритм RC4 забезпечує захист даних завдяки тому, що він генерує псевдовипадкові байти, які комбінуються з оригінальними даними через операцію XOR. Цей процес дозволяє перетворювати відкриті дані, такі як інформація про транзакції або особисті дані користувачів, у шифротекст, що неможливо відновити без ключа. Важливим аспектом використання RC4 є його здатність до обробки великих обсягів даних за короткий проміжок часу, що робить його ідеальним для високопродуктивних білінгових систем, де потрібна швидкість і ефективність [1, 3]. Крім того, шифрування за допомогою RC4 допомагає захистити інформацію при її передачі через мережу, забезпечуючи надійний захист від несанкціонованого доступу під час обробки даних. Використання алгоритму RC4 в білінгових системах дозволяє зменшити ризики, пов’язані з витоком особистої інформації клієнтів, оскільки навіть якщо дані будуть перехоплені, вони залишатимуться недоступними без ключа дешифрування.

Наведена форма використовується для виконання процесу перемикання використання між комп’ютерами в рамках білінгових систем, що дозволяє ефективно контролювати доступ до ресурсів та забезпечити безпеку персональних даних за допомогою алгоритму RC4, як показано на зображенні нижче (рис.1). Така функціональність дозволяє здійснювати динамічне розподілення завдань між комп’ютерами, що забезпечує надійний захист інформації під час її обробки та зберігання. Процес перемикання між комп’ютерами у білінгових системах сприяє ефективному використанню обчислювальних ресурсів та забезпечує високий рівень захисту персональних даних за допомогою алгоритму RC4. Важливою перевагою є можливість контролювати доступ до критичних даних, що дозволяє знизити ризики несанкціонованого доступу до конфіденційної інформації. Використання RC4 для шифрування даних забезпечує їхню безпеку, оскільки алгоритм дозволяє перетворювати інформацію в незрозумілий формат, що неможливо дешифрувати без відповідного ключа.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

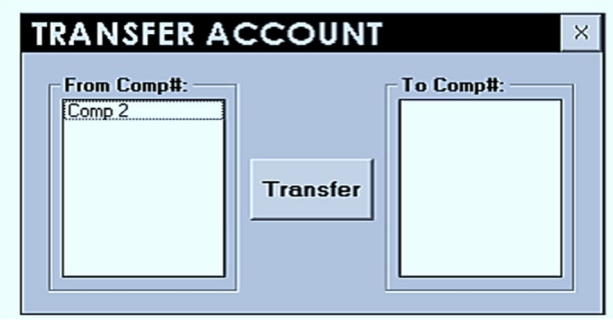


Рис. 1. Форма передачі облікового запису в білінговій системі для шифрування та захисту персональних даних

Джерело: розроблено автором

Цей підхід є особливо важливим для білінгових систем, де динамічне перемикання між комп'ютерами забезпечує рівномірне навантаження та ефективне використання ресурсів без шкоди для безпеки. Розподілення завдань між комп'ютерами дозволяє скоротити час обробки запитів та покращити загальну продуктивність системи, водночас підтримуючи високий рівень захисту даних [2, 4]. Застосування алгоритму RC4 також забезпечує цілісність даних, що важливо при обробці персональної інформації клієнтів у реальному часі. Це дає змогу відстежувати активність користувачів та контролювати доступ до чутливої інформації, запобігаючи її несанкціонованому використанню.

Наступна форма використовується для перегляду зашифрованої інформації в рамках білінгових систем, що дозволяє забезпечити захист персональних даних за допомогою алгоритму RC4, як показано на зображенні нижче (рис. 2).

Рис. 2. Результати шифрування персональних даних за допомогою алгоритму RC4 в білінговій системі

Джерело: розроблено автором

Такий процес дозволяє адміністратору або авторизованому користувачу переглядати дані, що були зашифровані для забезпечення конфіденційності, гарантуючи, що тільки ті, хто має відповідні права доступу та ключі для дешифрування, можуть отримати розшифровану інформацію [1-2]. Форма забезпечує ефективне управління доступом до зашифрованих даних, що є важливим елементом для захисту конфіденційної інформації у білінгових системах. Використання алгоритму RC4 гарантує високий рівень безпеки, оскільки дані шифруються за допомогою ключа, який відомий лише авторизованим особам, що знижує ризик

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

несанкціонованого доступу. Процес шифрування допомагає зберегти цілісність і конфіденційність даних протягом всього процесу їх зберігання та обробки, що є важливим для уникнення витоку інформації. Важливим аспектом є те, що для перегляду зашифрованих даних необхідно мати правильний ключ дешифрування, що забезпечує додатковий рівень захисту від несанкціонованих запитів. Алгоритм RC4 є надзвичайно ефективним для шифрування та дешифрування персональних даних у реальному часі, що особливо важливо для білінгових систем, де швидкість обробки даних є критичною. Водночас, цей підхід гарантує, що лише уповноважені користувачі можуть отримувати доступ до розшифрованої інформації, зберігаючи високий рівень безпеки та відповідність стандартам захисту персональних даних. Така система дозволяє легко інтегрувати механізми аудиту, що дають змогу відстежувати та контролювати всі операції з конфіденційною інформацією. Завдяки використанню RC4, білінгові системи можуть надавати захищений доступ до інформації про клієнтів, що є критично важливим для підтримки довіри до системи та забезпечення юридичних вимог щодо захисту персональних даних [3].

Ця форма використовується для перегляду розшифрованої інформації в білінгових системах, що дозволяє отримати доступ до персональних даних після їх обробки за допомогою алгоритму RC4, як показано на зображенні нижче (рис. 3). Такий підхід забезпечує ефективне управління доступом до конфіденційної інформації, дозволяючи лише авторизованим користувачам переглядати дані після їх успішного дешифрування, що гарантує захист від несанкціонованого доступу.

Рис. 3. Результати дешифрування персональних даних за допомогою алгоритму RC4

Джерело: розроблено автором

Цей механізм дозволяє адміністраторам білінгових систем здійснювати контроль за доступом до розшифрованих даних, забезпечуючи високий рівень безпеки та конфіденційності персональної інформації клієнтів. Завдяки використанню алгоритму RC4, дані, що зберігаються в зашифрованому вигляді, можуть бути доступні лише тим користувачам, які мають відповідні ключі для дешифрування, що є важливим аспектом для запобігання витоку чутливої інформації. Алгоритм RC4 забезпечує швидке та ефективне шифрування і дешифрування даних, що є критично важливим у реальному часі для забезпечення безперервності обслуговування користувачів у білінгових системах. Оскільки персональні дані часто використовуються для здійснення фінансових операцій або обробки платіжних відомостей, їх захист є важливою складовою частиною загальної безпеки системи. Дешифрування даних відбувається на основі алгоритму RC4, який дозволяє зберегти

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

цілісність і конфіденційність інформації протягом всього процесу її обробки. Технологія дешифрування, реалізована в системах, дозволяє надійно відновлювати оригінальні дані без втрат, що особливо важливо при роботі з фінансовими даними клієнтів. Використання алгоритму RC4 дозволяє автоматизувати процес дешифрування, зменшуючи ймовірність помилок або зловживань з боку несанкціонованих користувачів, оскільки доступ до даних отримують лише уповноважені особи. Це також дозволяє забезпечити відповідність вимогам щодо захисту персональних даних, що є важливою частиною законодавчих норм у багатьох країнах. Впровадження таких підходів у білінгових системах підвищує довіру користувачів до сервісу та гарантує високий рівень захисту персональних даних.

Наведена форма використовується для перегляду інформації про підключених клієнтів у білінгових системах, що дозволяє адміністратору або авторизованим користувачам отримувати доступ до даних клієнтів після їх шифрування за допомогою алгоритму RC4, як показано на зображенні нижче (рис. 4). Така функціональність забезпечує ефективне управління доступом до персональних даних, дозволяючи відстежувати активність користувачів системи в режимі реального часу та гарантує безпеку і конфіденційність інформації під час її обробки [1, 4].

Рис. 4. Користувачі, які підключені до білінгової системи для обробки персональних даних

Джерело: розроблено автором

Наведена форма є важливим інструментом для підтримки безпеки даних у білінгових системах, оскільки вона дозволяє адміністраторам точно визначати, хто має доступ до конфіденційної інформації клієнтів. Алгоритм RC4 застосовується для шифрування особистих даних, що забезпечує надійний захист від несанкціонованого доступу. Після шифрування дані можна безпечно передавати через мережу, при цьому лише ті користувачі, які мають відповідні ключі для дешифрування, можуть отримати доступ до оригінальної інформації. Це особливо важливо в контексті білінгових систем, де велика кількість клієнтів взаємодіє з системою та надає персональні дані, які потребують захисту. Алгоритм RC4 є популярним через свою швидкість і ефективність при шифруванні великих обсягів даних, що особливо важливо для швидкого оброблення запитів у реальному часі. Завдяки використанню цієї технології можна знизити ризики, пов’язані з витоками персональної інформації або зловмисними атаками на бази даних. У системах білінгу, де кожен запис клієнта містить чутливу інформацію, захист за допомогою RC4 дозволяє забезпечити конфіденційність і цілісність даних під час їх обробки та зберігання. Крім того, система моніторингу дозволяє адміністраторам стежити за кожним підключенням до системи в реальному часі, що полегшує виявлення підозрілої активності або спроб несанкціонованого доступу. Завдяки інтеграції таких механізмів, як шифрування RC4, з білінговими системами, організації можуть забезпечити надійний захист своїх клієнтських даних, водночас гарантуючи швидкість та зручність обробки запитів. Це також дозволяє підвищити довіру користувачів до системи, оскільки вони можуть бути впевнені, що їх персональні дані надійно захищені від зловмисників [2–3].

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Наявність надійного шифрування в білінгових системах є критично важливим для запобігання несанкціонованому доступу до персональних даних, таких як імена, адреси, номери рахунків і фінансові транзакції. Завдяки алгоритму RC4, який забезпечує високий рівень безпеки, системи можуть захищати такі дані навіть під час їх передачі через незахищені мережі. Алгоритм шифрування RC4 працює шляхом перетворення відкритих даних у зашифровані за допомогою ключа, що забезпечує унікальність кожного сеансу шифрування. Це дозволяє мінімізувати ймовірність того, що дані можуть бути дешифровані без належних прав доступу. Особливістю RC4 є його здатність шифрувати дані в реальному часі, що є важливим для забезпечення оперативної обробки клієнтських запитів без шкоди для безпеки. Проте варто зазначити, що алгоритм RC4 має свої обмеження і, зокрема, вимагає постійного оновлення ключів для підтримки високого рівня безпеки. У білінгових системах це може бути реалізовано через регулярну зміну ключів шифрування, що дозволяє знизити ризики зловмисних атак. Крім того, важливо також застосовувати додаткові методи захисту, такі як багаторівнева аутентифікація, для забезпечення максимального рівня безпеки. В результаті, інтеграція алгоритму RC4 в білінгові системи не тільки забезпечує надійний захист даних, але й дозволяє компаніям підвищити ефективність їхніх бізнес-процесів, оптимізуючи час обробки запитів. На додачу, використання таких технологій сприяє зміцненню репутації компанії серед клієнтів, які можуть бути впевнені в захищеності своїх персональних даних.

Висновки. Алгоритм RC4 може бути ефективно використаний як техніка захисту даних від атак з боку несанкціонованих осіб. Однак, через виявлені вразливості та слабкості, пов’язані з криптоаналізом, в сучасних системах безпеки його використання обмежується. Для більш надійного захисту даних зараз рекомендується використовувати сучасні алгоритми шифрування, такі як AES (Advanced Encryption Standard), що забезпечує високу стійкість до атак. Використання довгого ключа, без сумніву, підвищує рівень безпеки, оскільки збільшується складність дешифрування інформації, але для підвищення рівня захисту важливо комбінувати його з іншими методами, такими як регулярне оновлення ключів та застосування складніших протоколів шифрування, таких як TLS (Transport Layer Security). У контексті безпеки білінгових систем, що працюють з персональними даними користувачів, основна увага має бути приділена забезпеченню конфіденційності даних, що стосуються інтернет-активності користувачів. Це можна досягти через використання сучасних механізмів шифрування та багатофакторної аутентифікації для захисту доступу до інформації. Для розробки програмного забезпечення, яке забезпечує захист даних інтернет-білінгу, доцільно використовувати сучасні мови програмування, такі як Python, C#, або Java, які підтримують новітні криптографічні бібліотеки та протоколи безпеки.

Список використаних джерел

1. Rivest, S. RC4 Algorithm: Description and Cryptographic Usage / R. Rivest // Journal of Cryptographic Engineering. – 2010. – Vol. 8. – P. 25–38.

2. Krein, E. Vulnerabilities of the RC4 Algorithm and Its Impact on Data Security / E. Krein// Cryptography and Communications. – 2020. – Vol. 12. – P. 121–134.

3. Schneier, B. Using RC4 in Critical Systems: Recommendations for Enhanced Security / B. Schneier // Computer Security and Cryptography Journal. – 2020. – Vol. 19. – P. 57–72.

4. Rosenberg, S. Key Management and Its Role in RC4 Security / S. Rosenberg // International Journal of Information Security and Privacy. – 2021. – Vol. 7. – P. 45–58.

Роботу виконано під науковим керівництвом д-ра екон. наук, професора
ЧУБАЄВСЬКОГО В. І.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

КОМБІНОВАНИЙ ПІДХІД ДО ВИКОРИСТАННЯ СИСТЕМ СКАНУВАННЯ ВРАЗЛИВОСТЕЙ ДЛЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ШЕВЯКОВ Н. С., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У цій статті розглядається комбінований метод аудиту інформаційної безпеки комп'ютерних мереж із застосуванням систем сканування вразливостей. Досліджено, як інтеграція таких інструментів, як Nmap, Nessus, OpenVAS, Masscan, OSSEC і Lynis, сприяє виявленню загроз на різних рівнях мережевої інфраструктури. Проведено аналіз їхньої ефективності у задачах сканування портів, виявлення вразливостей, перевірки конфігурацій і моніторингу систем. Експерименти, проведені на тестовій платформі Kali Linux, показали, що використання комбінованого підходу покращує якість і деталізацію аудиту. У висновках наведено практичні поради щодо вибору оптимальних комбінацій інструментів залежно від специфіки організації, а також окреслено перспективні напрями для подальших досліджень.

This article examines a combined method of auditing information security of computer networks using vulnerability scanning systems. It is investigated how the integration of tools such as Nmap, Nessus, OpenVAS, Masscan, OSSEC and Lynis helps to detect threats at different levels of the network infrastructure. Their effectiveness in port scanning, vulnerability detection, configuration checking and system monitoring is analyzed. Experiments conducted on the Kali Linux test platform have shown that using a combined approach improves the quality and detail of the audit. The conclusions provide practical advice on choosing the optimal combinations of tools depending on the specifics of the organization, and also outline promising areas for further research.

Актуальність. У сучасному світі інформаційні технології є основою роботи бізнесу, державних структур і критичної інфраструктури, але кількість кіберзагроз зростає щороку в геометричній прогресії, створюючи серйозні виклики для безпеки систем. Системи сканування вразливостей, такі як Nmap, Nessus чи OpenVAS, дозволяють виявляти загрози, але їхні обмеження роблять комбінований підхід необхідним для комплексного захисту. В Україні це питання є особливо актуальним через зростання гібридних загроз у контексті геополітичної ситуації. Глобальні тренди, зокрема ускладнення атак і підвищення вимог до захисту даних, підкреслюють важливість такого підходу, який дозволяє організаціям адаптувати інструменти до своїх потреб, ефективно реагувати на сучасні виклики та готуватися до майбутніх загроз. Таким чином, розробка комбінованого підходу до використання систем сканування вразливостей є актуальним завданням, що має як теоретичне, так і практичне значення для забезпечення інформаційної безпеки в цифровому світі.

Метою статті є розробка комбінованого підходу до використання систем сканування вразливостей для аудиту інформаційної безпеки комп'ютерних мереж. Дослідження спрямоване на оцінку ефективності інтеграції інструментів у виявленні загроз, аналізі конфігурацій і моніторингу систем. Завдання включають порівняння їхніх можливостей за критеріями точності, швидкості та повноти охоплення, а також формулювання рекомендацій для оптимального поєднання в різних сценаріях аудиту.

Об'єктом дослідження є комп'ютерні мережі, що підлягають аудиту інформаційної безпеки, зокрема локальні мережі організацій, серверні системи та гібридні інфраструктури з активними пристроями й сервісами, де необхідно виявляти вразливості та забезпечувати захист від кібератак.

Предмет дослідження є комбінований підхід до використання систем сканування вразливостей, таких як Nmap, Nessus, OpenVAS, OSSEC і Lynis, у процесі аудиту

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

інформаційної безпеки, включаючи методи їх інтеграції, оцінку ефективності та взаємодію для підвищення якості виявлення загроз.

Аналіз попередніх досліджень. Практика проведення аудитів інформаційної безпеки та використання спеціалізованих інструментів є усталеною, що відображено в технічних керівництвах, таких як NIST Special Publication 800-115 [1]. Попередні дослідження та огляди часто фокусуються на ключових інструментах аудиту. Наприклад, у статті B. Alotaibi та A. Al-Qahtani, опублікованій в International Journal of Network Security & Its Applications (IJNSA), Nmap детально аналізується як потужний засіб для розвідки мережі та ідентифікації сервісів [2].

Хоча ці основні інструменти є важливими компонентами аудиту відповідно до загальних методологій, описаних у NIST SP 800-115 [4], дана робота досліджує ефективність комбінованого підходу. Такий підхід інтегрує зазначені та інші спеціалізовані інструменти (наприклад, для аудиту конфігурацій, моніторингу логів), оскільки оцінка синергії від таких конкретних поєднань для підвищення якості аудиту потребує додаткового вивчення.

Викладення основного матеріалу. Перш ніж перейти до огляду систем сканування вразливостей, важливо окреслити ключові поняття, які лежать в основі аудиту інформаційної безпеки та цієї роботи:

Вразливість – це слабкість в інформаційній системі, процедурах забезпечення безпеки, внутрішніх контролях або в процесі реалізації, яку може використати джерело загрози [3, с. 18].

Аудит безпеки – процес аналізу системи для виявлення ризиків, перевірки відповідності стандартам захисту та розробки рекомендацій щодо їх усунення. Проведення аудиту дозволяє не лише ідентифікувати слабкі місця, а й розробити ефективні рекомендації щодо їх усунення, що сприяє підвищенню рівня безпеки організації [4].

Для проведення аудиту комп'ютерних систем важливо обрати інструменти; ці інструменти називаються сканерами виявлення вразливостей – системами, призначеними для швидкого визначення хостів, їхніх характеристик та пов'язаних уразливостей, що робить їх невід'ємною частиною цього процесур [5]. Схема, представлена на Рис. 1, ілюструє розподіл сканерів за основними областями їхнього застосування в аудиті інформаційної безпеки.

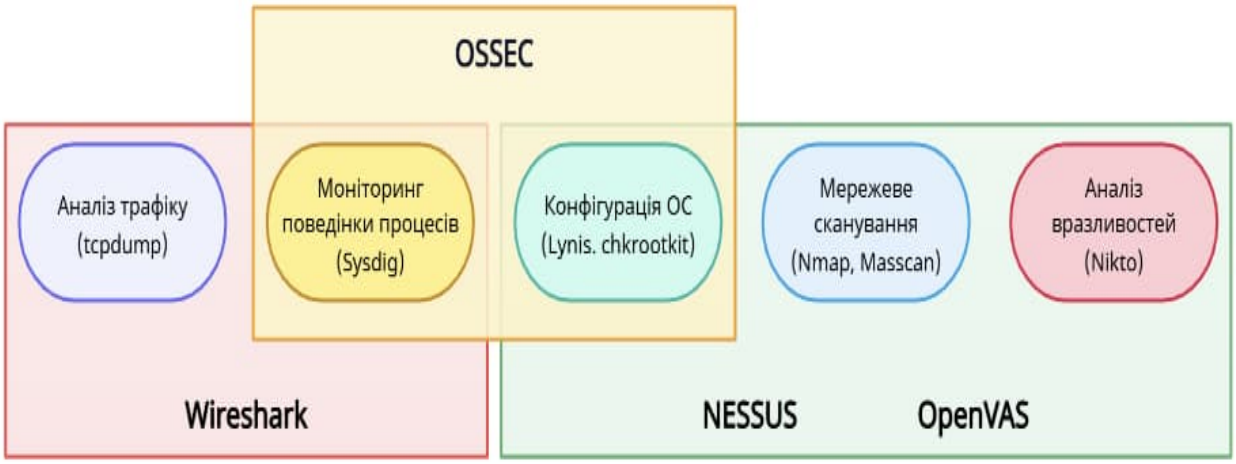


Рис. 1. Розподіл сканерів за областями із зазначенням багатофункціональності

Джерело: розроблене автором в середовищі Creately

Як показано на схемі, ефективне виявлення загроз вимагає комплексного підходу, адже жоден окремий інструмент не може охопити всі аспекти безпеки через свою спеціалізацію на певних типах вразливостей. Саме тому подальше дослідження зосереджується на комбінованому використанні систем сканування, що дозволяє компенсувати недоліки окремих засобів і забезпечити більш повну оцінку стану інформаційної безпеки. Розглядаються різні

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

варіанти комбінування інструментів, які відповідають потребам як базового аудиту для невеликих систем, так і комплексного аналізу для складних IT-інфраструктур.

Перший набір інструментів, призначений для проведення базового аудиту інформаційної безпеки. Він включає чотири компоненти: Nmap, OpenVAS, та Lynis. Цей набір розроблено для оцінки стану мережевої інфраструктури та операційних систем з метою виявлення вразливостей і недоліків конфігурації. Його застосування доцільне в умовах обмежених ресурсів, коли необхідно отримати попередні дані про безпеку без залучення складних або комерційних рішень.

Таблиця 1

Опис інструментів для базового аудиту

Назва інструменту	Призначення та можливості	Ключові характеристики	Рекомендована область застосування
Nmap	Використовується для сканування мережі, визначає відкриті порти та активні служби. Це дозволяє отримати первинну інформацію про структуру мережі та потенційні точки ризику.	Використання безкоштовних інструментів або їх версій із відкритим кодом, що знижує фінансові витрати. Сумісність із операційними системами Linux і Windows, що забезпечує можливість застосування в різних середовищах. Можливість швидкого розгортання та отримання результатів, що є важливим для аналізу.	Організації з обмеженими ресурсами, де відсутня можливість впровадження комплексних систем безпеки. Попередня оцінка стану інформаційної безпеки перед проведенням детального аудиту. Навчальні або дослідницькі проекти, спрямовані на вивчення базових методів аналізу вразливостей.
OpenVAS	Використовується для сканування мережі, визначає відкриті порти та активні служби. Це дозволяє отримати первинну інформацію про структуру мережі та потенційні точки ризику.		
Lynis	Програма для аудиту конфігурації Linux-систем. Вона аналізує параметри безпеки ОС і пропонує рекомендації для їх вдосконалення.		

Джерело: розроблене автором

Хоча Комбінація 1 дозволяє виконати базову оцінку, вона не заміняє поглиблений аудит із використанням спеціалізованих інструментів, але її можна ефективно використовувати проти поверхневих вразливостей, тобто такі які існують незалежно від інших[1, с. 28]. Її ефективність залежить від кваліфікації користувача та правильності інтерпретації отриманих даних. У майбутніх дослідженнях доцільно розглянути можливість інтеграції додаткових інструментів для підвищення точності аналізу. Вона є практичним рішенням для аудиту інформаційної безпеки, забезпечує базовий рівень аналізу мережевих і системних вразливостей, що може слугувати основою для подальшого вдосконалення захисту. Застосування цього набору є доцільним у контексті ресурсоефективного підходу до забезпечення безпеки даних.

Другий набір призначений для детального аудиту інформаційної безпеки на рівні мережі та систем. Він складається з чотирьох компонентів: Nmap, Nessus, Lunis, OSSEC. Цей набір орієнтований на організації, які потребують глибокого аналізу вразливостей, моніторингу безпеки в реальному часі та управління системними процесами.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Таблиця 2

Опис інструментів для розширеного аудиту

Назва інструменту	Призначення та можливості	Ключові характеристики	Рекомендована область застосування
Nmap	Завдяки можливості виконання складних мережевих скриптів (NSE), Nmap може забезпечувати базову оцінку захищеності мережі та виявлення аномалій	Поєднання безкоштовних і комерційних інструментів для підвищення точності аналізу. Можливість моніторингу в реальному часі для оперативного реагування на загрози. Підтримка детального управління системними процесами, особливо в Windows-середовищі. Вимагає значних ресурсів для налаштування та підтримки, особливо в великих мережах. Використання комерційних інструментів (наприклад, Nessus) пов'язане з додатковими витратами	Організацій середнього розміру з розгалуженою мережевою інфраструктурою. Компаній, які потребують регулярного моніторингу та звітів для відповідності стандартам безпеки. Системних адміністраторів, відповідальних за безпеку систем
Nessus	Комерційний інструмент для виявлення вразливостей із розширеною базою даних загроз і можливістю створення детальних звітів із рекомендаціями		
Lynis	Виявляє можливі уразливості на рівні ОС, що дозволяє запобігти загрозам ще на етапі налаштування інфраструктури		
OSSEC	Система моніторингу безпеки (HIDS), що аналізує журнали подій		

Джерело: розроблене автором

Комбінація 2 є ефективним рішенням для організацій, які прагнуть забезпечити високий рівень безпеки завдяки детальному аналізу вразливостей і моніторингу систем. Вона дозволяє не лише виявляти загрози, а й оперативно на них реагувати.

Третій набір інструментів для комплексного аудиту інформаційної безпеки охоплює конфігурації систем, аналіз мережевого трафіку та виявлення вразливостей. Він включає шість компонентів: Nmap, Nessus, QualysGuard, Lynis, OSSEC та Wireshark. Цей набір призначений для організацій із високими вимогами до безпеки, де потрібен максимальний контроль над інфраструктурою та ефективне виявлення загроз на різних рівнях системи.

Таблиця 3

Опис інструментів для комплексного аудиту

Назва інструменту	Призначення та можливості	Ключові характеристики	Рекомендована область застосування
Nmap	Для детального сканування мережі. Забезпечує повну картину мережевої інфраструктури.	Максимальне охоплення: від мережевого сканування до аналізу конфігурацій і моніторингу в реальному часі. Автоматизація та звітність: QualysGuard і Nessus забезпечують автоматизований аудит і детальні звіти.	Великих організацій із розвиненою інфраструктурою, де потрібен повний контроль над безпекою. Компаній із критичними даними, які потребують регулярного моніторингу та аналізу
QualysGuard	Хмарний сервіс для автоматизованого аудиту вразливостей. Для автоматизованого аудиту вразливостей, аналізує конфігурації, програмне забезпечення та порівнює їх із сучасними стандартами безпеки.		

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Назва інструменту	Призначення та можливості	Ключові характеристики	Рекомендована область застосування
OSSEC	Для моніторингу в реальному часі та виявлення аномалій. включаючи підозрілі процеси та rootkits	Підтримка різних платформ: інструменти охоплюють як Linux (Lynis, OSSEC), так і Windows	
Wireshark	Для глибокого аналізу мережевого трафіку, дозволяє виявляти слабкі протоколи, аномалії та спроби атак	Глибокий аналіз: Wireshark і OSSEC дозволяють виявляти приховані загрози на рівні трафіку та поведінки	Організацій, що прагнуть відповідати міжнародним стандартам безпеки (наприклад, стандарти серії ISO 27000)
Nessus	Для глибокого аналізу вразливостей із детальними звітами, також проводить аналіз системних налаштувань, слабких паролів та інших критичних недоліків із використанням розширеної бази даних загроз		
Lynis	Для аудиту конфігурації Linux-систем, що аналізує параметри безпеки ОС і пропонує рекомендації для їх вдосконалення		

Джерело: розроблене автором

Для забезпечення ефективного аудиту інформаційної безпеки важливо дотримуватися логічного порядку застосування інструментів у кожній комбінації.

Рис. 2. Набір для базового сканування

Джерело: розроблене автором у середовищі Creately

Перша комбінація інструментів застосовується послідовно, розширюючи аналіз від мережевого рівня до конфігурації ОС. Спочатку Nmap швидко сканує мережу, виявляючи активні хости, відкриті порти та базові сервіси. На основі цих даних OpenVAS проводить комплексне сканування вразливостей у сервісах та перевіряє конфігурації мережевих пристроїв. Завершує процес Lynis, який аудитує налаштування операційної системи, виявляючи недоліки та надаючи рекомендації. Такий підхід забезпечує охоплення основних рівнів безпеки: мережевого, програмного та системного.

Рис. 3. Розширене сканування мережі та системи

Джерело: розроблене автором у середовищі Creately

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Друга комбінація розширює першу, інтегруючи OSSEC для моніторингу в реальному часі. Nmap забезпечує базове сканування мережі (топологія, порти). Потім Nessus виконує детальний аналіз вразливостей, використовуючи розширену базу даних для виявлення програмних і конфігураційних недоліків. Lynis проводить глибокий аудит налаштувань ОС. На завершення, OSSEC здійснює постійний моніторинг поведінки системи, дозволяючи оперативно виявляти аномалії та потенційні атаки. Такий підхід забезпечує комплексну оцінку безпеки, поєднуючи попередження загроз та оперативне реагування.

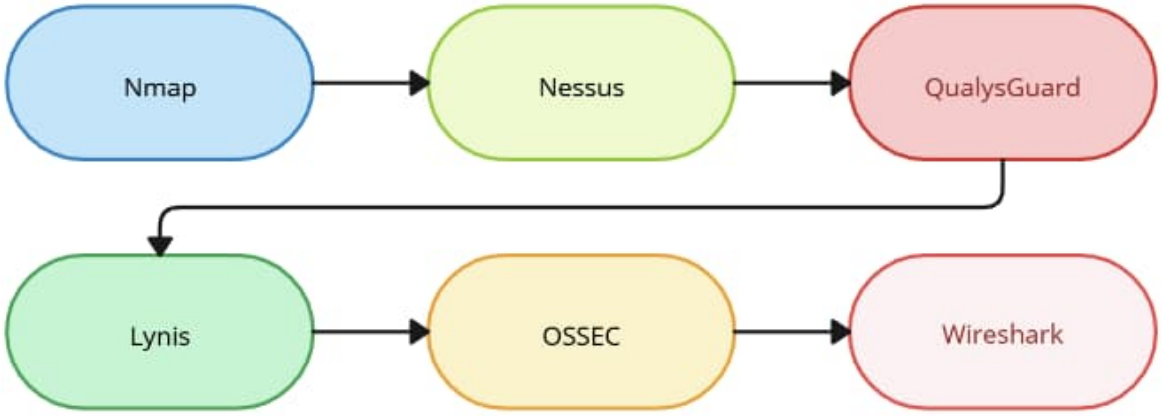


Рис. 4. Комплексне сканування мережі та системи

Джерело: розроблене автором у середовищі Creately

Третя комбінація представляє найбільш комплексний підхід до аудиту безпеки, охоплюючи всі критичні аспекти – від мережевого сканування до аналізу трафіку. Як і в попередніх варіантах, Nmap використовується для сканування мережі, що встановлює базову карту активних пристроїв і відкритих портів. Nessus проводить детальний аналіз вразливостей, використовуючи свою розширену базу даних для виявлення потенційних загроз у знайдених сервісах. Для доповнення цієї оцінки в рамках хмарного підходу використовується QualysGuard, що забезпечує автоматизований аудит конфігурацій та порівняння з сучасними стандартами безпеки. Lynis знову входить до процесу для детального аудиту налаштувань операційної системи, а OSSEC слугує системою моніторингу, яка забезпечує оперативне реагування на аномалії у поведінці системи. Завершує комплекс Wireshark, який дозволяє в режимі реального часу аналізувати мережевий трафік, виявляючи слабкі протоколи, аномалії та потенційні спроби атак. Цей послідовний підхід забезпечує максимально повну оцінку стану інформаційної безпеки, поєднуючи глибокий аналіз вразливостей із постійним моніторингом та аналізом мережевого трафіку.

Переглянувши представлені види комбінацій інструментів та визначивши їх правильний порядок використання, можна перейти до практичної частини дослідження. Тестування проводилось на тестовій системі Kali Linux 2025.1a у середовищі віртуальної машини VirtualBox 7.1.6.

Спеціально для тестування у системі було навмисно створено певну кількість вразливостей, щоб оцінити точність виявлення інструментами та ефективність їх роботи.

Серед вразливостей були налаштовані:

- Відкриті порти з потенційними вразливостями (22/TCP, 80/TCP, 443/TCP, 21/TCP, 23/TCP, 3306/TCP).
- Простий пароль «1111» для користувача спеціально створеного для оцінки точності та тестування «Test1».
- Налаштовані вразливі сервіси, зокрема FTP, SSH та Telnet із застарілими версіями програмного забезпечення.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

- Дозволений анонімний доступ до FTP та Telnet.
- Використання незахищених протоколів передачі даних (HTTP, FTP, Telnet).
- Відсутність налаштувань контролю цілісності та обмеження доступу в SSH.
- Генерація подій перевищення лімітів входу.
- Вимкнення механізмів захисту типу SELinux.
- Встановлення вразливого застарілого пакету програмного забезпечення з відкритими CVE.

Таблиця 4

Результати тестування системи набором інструментів для базового сканування

Інструмент	Команда	Результат сканування	Знайдені вразливості або помилки	Час виконання
Nmap(v7.94)	nmap -p 1-65535 -T4 -A -v 192.168.56.1/24	Виявлено 6 відкритих портів	21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 80/tcp (http), 443/tcp (https), 3306/tcp (mysql),).	2 хвилини 12 секунд
OpenVAS (v23.16.1)	omp -u admin -w adm444 -T «Full and fast» –t 192.168.56.1/24	Виявлено базові вразливост	Ненадійний пароль для Test1, застаріла версія FTP, неправильні налаштування SSH, помилкові конфігурації сервісів з використанням застарілих протоколів FTP, SSH, Telnet.	3 хвилини 29 секунд
Lynis(v3.0.9)	lynis audit system	Виявлено 5 проблем конфігурації	Вимкнені оновлення Вимкнений SELinux Відсутній пароль для root Увімкнені невикористовувані служби (FTP, Telnet) Відсутність інструментів контролю цілісності	3 хвилин 51 секунда

Джерело: розроблене автором

Проведене тестування системи виявило лише частину наявних вразливостей. Загальний час виконання базового аудиту склав 11 хвилин 32 секунди. Хоча інструменти успішно ідентифікували відкриті порти, слабкий пароль, застарілі версії сервісів та деякі проблеми конфігурації, значна кількість вразливостей залишилась невиявленою. Результати демонструють, що базовий аудит надає лише поверхневу оцінку безпеки системи. Для виявлення всіх наявних вразливостей та забезпечення комплексного захисту необхідно переходити до розширеного сканування з використанням додаткових інструментів та методів глибокого аналізу.

Таблиця 5

Результати тестування системи набором інструментів для розширеного сканування

Інструмент	Команда	Результат сканування	Знайдені вразливості або помилки	Час виконання
Nmap (v7.94)	nmap -p 1-65535 -T4 -A -v 192.168.56.1/24	Виявлено 6 відкритих портів	21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 80/tcp (http), 443/tcp (https), 3306/tcp (mysql),)	2 хвилини 12 секунд
Nessus (v10.8.3)	/opt/nessus/sbin/nessuscli scan --policy «Basic Vulnerability Scan» --target <target_ip> --format html	Проведено детальний аналіз сервісів із зазначенням потенційних загроз	Простий пароль для Test1, застаріла версія FTP, неналежні налаштування SSH, невірні конфігурації сервісів із використанням старих протоколів FTP, SSH, Telnet	4 хвилин 37 секунд

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Інструмент	Команда	Результат сканування	Знайдені вразливості або помилки	Час виконання
Lynis(v3.0.9)	lynis audit system	Виявлено 5 проблем конфігурації	Вимкнені оновлення Вимкнений SELinux Відсутній пароль для root Увімкнені невикористовувані служби (FTP, Telnet) Відсутність інструментів контролю цілісності	3 хвилин 51 секунда
OSSEC (v4.11.1)	ossec-logtest	Виявлено 2 аномалії у логах	Перевищення лімітів входу, що свідчить про спроби brute-force атак або інші ознаки несанкціонованого доступу	3 хвилини 02 секунди

Джерело: розроблене автором

Проведене розширене сканування з використанням комбінації інструментів дозволило виявити більшу кількість вразливостей за загальний час 13 хвилин 42 секунди. Розширене сканування дозволило виявити більше потенційних вразливостей системи, особливо пов'язаних із спробами несанкціонованого доступу, що не було виявлено під час базового сканування.

Таблиця 6

Результати тестування системи набором інструментів для комплексного сканування

Інструмент	Команда	Результат сканування	Знайдені вразливості або помилки	Час виконання
Nmap (v7.94)	nmap -p 1-65535 -T4 -A -v 192.168.56.1/24	Виявлено 6 відкритих портів	21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 80/tcp (http), 443/tcp (https), 3306/tcp (mysql),).	2 хвилини 12 секунд
Nessus (v10.8.3)	/opt/nessus/sbin/nessuscli scan --policy «Basic Vulnerability Scan» --target <target_ip> --format html	Проведено детальний аналіз сервісів із зазначенням потенційних загроз	Простий пароль для Test1, застаріла версія FTP, неналежні налаштування SSH, невірні конфігурації сервісів із використанням старих протоколів FTP, SSH, Telnet.	4 хвилин 37 секунд
QualysGuard (v6.4)	qualysscan -target <target_ip> -policy «Default Policy»	Виявлено 8 вразливостей	Неправильна конфігурація, використання застарілих протоколів, неналежне шифрування та інші невідповідності, що можуть призводити до компрометації системи.	7 хвилин 27 секунд
Lynis(v3.0.9)	lynis audit system	Виявлено 5 проблем конфігурації	Відсутність регулярних оновлень Вимкнений SELinux Слабкі паролі, зокрема для root Увімкнені невикористовувані служби (FTP, Telnet) Відсутність інструментів контролю цілісності	5 хвилин 51 секунда
OSSEC (v4.11.1)	ossec-logtest	Виявлено 2 аномалії у логах	Перевищення лімітів входу, що свідчить про спроби brute-force атак або інші ознаки несанкціонованого доступу.	3 хвилини 02 секунди

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Інструмент	Команда	Результат сканування	Знайдені вразливості або помилки	Час виконання
Wireshark (v4.4.5-1)	tshark -i eth0 -f «tcp port 80 or tcp port 21 or tcp port 23» -a duration:600	Виявлено 2 випадки передачі незашифрованих даних	По протоколах HTTP, FTP та Telnet Виявлено випадки передачі незашифрованих даних , що може призводити до перехоплення конфіденційної інформації	10 хвилин

Джерело: розроблене автором

Комплексне сканування системи за допомогою 6 спеціалізованих інструментів дозволило виявити значно ширший спектр вразливостей. Загальний час виконання всіх перевірок склав 33 хвилини 09 секунд. Комплексне сканування дозволило виявити майже всі навмисно створені вразливості системи, демонструючи переваги використання різнопланових інструментів для забезпечення всебічного аналізу безпеки інформаційних систем.

Тепер, після тестувань, потрібно визначити ефективність виявлення кожного набору інструментів Pn. Це дозволить оцінити, наскільки ефективно кожен набір інструментів справляється із завданням виявлення різної складності та кількості вразливостей.

$$P_n = \frac{TP}{TP+FP}, \quad (6)$$

де TP *(True Positive)* – вірно виявлена вразливість, FP *(False Positive)* – хибно класифіковані вразливості., Обрахунки запишемо у вигляді таблиці:

Таблиця 7

Результати розрахунку ефективності для досліджуваних наборів інструментів

Набір інструментів	TP	TF	P_n
Базове сканування (Nmap, OpenVAS, Lynis)	6	1	0.8571
Розширене сканування (Nmap, Nessus, Lynis, OSSEC)	7	1	0,875
Комплексне сканування (Nmap, Nessus, Lynis, OSSEC, QualysGuard)	9	2	0,8181

Джерело: розроблене автором

Висновки. Дослідження встановило, що комбінований підхід до використання сканерів вразливостей значно підвищує ефективність аудиту безпеки комп'ютерних мереж. Інтеграція інструментів дозволяє виявляти загрози на різних рівнях інфраструктури – від відкритих портів і слабких паролів до аномалій у системних логах і трафіку.

Отримані результати свідчать, що комбінований підхід є оптимальним рішенням для комплексного захисту інформаційних систем, сприяючи як виявленню вразливостей, так і оперативному реагуванню на потенційні загрози. Перспективними напрямами подальшого розвитку є автоматизація цього підходу та його тестування на реальних системах для підвищення зручності й масштабованості.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаних джерел

1. SP 800-115. Technical guide to information security testing and assessment. Replaces SP 800-42 (10/15/2003); effective from 2008-09-30. Official edition. Gaithersburg : National Institute of Standards and Technology (NIST), 2008. 80 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
2. A comprehensive analysis of network scanning and security assessment tool. International journal of network security & its applications. 2024. Vol. 16, no. 6. P. 101–112. URL: https://doi.org/10.5121/ijnsa.2024.16607
3. SP 800-30 Rev 1. Guide for conducting risk assessments. Replaces SP 800-30 (07/01/2002); effective from 2012-09-17. Official edition. Gaithersburg: National Institute of Standards and Technology (NIST), 2012. 95 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
4. Security audit - Glossary | CSRC. *NIST Computer Security Resource Center | CSRC*. URL:https://csrc.nist.gov/glossary/term/security_audit
5. Vulnerability scanning - Glossary | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/glossary/term/vulnerability_scanning
6. Lakhtin I., Mykhailenko D., Nariezhnii O. Comparison of commercial web application vulnerability scanners and open source scanners. Computer science and cybersecurity. 2022. No. 2. P. 41–49. URL: https://doi.org/10.26565/2519-2310-2022-2-05

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВОЇ Ю. Є.

МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД АТАК ЛОГІЧНИХ ВИСНОВКІВ НА КОМЕРЦІЙНОМУ ПІДПРИЄМСТВІ

ШЕРШЕНЬ Д. С., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека систем електронних комунікацій в економіці»

У статті розглядаються проблеми захисту персональних даних у сучасних умовах, коли спостерігається зростання випадків порушень безпеки та компрометації конфіденційності користувачів. Піддано критиці існуючі моделі, в яких треті сторони збирають і контролюють великі обсяги персональних даних. Як приклад потенційно надійного рішення для збереження конфіденційності, в статті розглядається застосування блокчейн-технології для створення децентралізованої системи управління персональними даними, що дозволяє користувачам володіти та контролювати свої дані без необхідності довіряти третім сторонам. Описано протокол, який перетворює блокчейн на автоматизовану систему управління доступом, в якій транзакції використовуються не лише для фінансових операцій, а й для передачі інструкцій щодо збереження, запиту та обміну даними.

The article discusses the issues of personal data protection in the modern context, where there is an increase in security breaches and compromises of user privacy. It critiques existing models in which third parties collect and control large volumes of personal data. As a potentially reliable solution for maintaining privacy, the article examines the application of blockchain technology to create a decentralized personal data management system, allowing users to own and control their

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

data without the need to trust third parties. A protocol is described that transforms blockchain into an automated access control system, where transactions are used not only for financial operations but also for transferring instructions related to the storage, querying, and exchange of data.

Актуальність. З огляду на постійне впровадження нових технологій збору, обробки та зберігання персональних даних, комерційні підприємства мають дедалі більше зобов'язань щодо захисту інформації про своїх клієнтів, співробітників та партнерів. Особливу небезпеку становлять атаки, що ґрунтуються на логічних висновках, під час яких зловмисники можуть отримати доступ до конфіденційної інформації, здійснивши аналіз неявних зв'язків і взаємозалежностей між даними. Враховуючи, що комерційні підприємства зазвичай зберігають величезні обсяги даних, що містять як особисту, так і фінансову інформацію, захист від таких атак стає надзвичайно важливим для запобігання витоку даних, репутаційних втрат і юридичних наслідків. Атаки логічних висновків можуть бути надзвичайно складними для виявлення та запобігання, оскільки вони не потребують прямого доступу до даних, а лише маніпулювання доступною інформацією для здобуття конфіденційних даних. Тому розробка та впровадження ефективних методів захисту персональних даних від атак логічних висновків є нагальною необхідністю для забезпечення кібербезпеки підприємств та збереження довіри їхніх клієнтів і партнерів.

Метою статті є дослідження методів захисту персональних даних від атак логічних висновків на комерційних підприємствах шляхом аналізу основних загроз, оцінки ефективності існуючих підходів до забезпечення конфіденційності та цілісності даних у процесі їх зберігання, обробки та передачі, а також розробки рекомендацій щодо впровадження комплексних заходів кіберзахисту в рамках систем управління інформаційною безпекою.

Об'єктом дослідження є процес захисту персональних даних на комерційних підприємствах від атак логічних висновків, який включає виявлення потенційних загроз, аналіз методів приховування та анонімізації даних, оцінку ефективності криптографічних і політик доступу, а також розробку заходів щодо підвищення рівня інформаційної безпеки.

Предмет дослідження – підходи, методи та інструменти забезпечення захисту персональних даних від атак логічних висновків на комерційних підприємствах, що включають застосування алгоритмів анонімізації, диференційної приватності, криптографічних методів, політик контролю доступу та інших технологій кібербезпеки для мінімізації ризиків несанкціонованого вилучення прихованої інформації.

Аналіз попередніх досліджень. В. Демиденко у своїй роботі зосереджується на методах захисту персональних даних в умовах динамічного розвитку інформаційних технологій, підкреслюючи важливість впровадження ефективних засобів захисту від атак логічних висновків. На його думку, ключовим аспектом є використання адаптивних систем, які дозволяють постійно оновлювати захисні механізми у відповідь на нові загрози, що виникають у реальному часі [1]. Однак він не враховує всі аспекти взаємодії між різними типами даних, що можуть бути використані для здійснення атак логічних висновків. Зокрема, не аналізуються ризики, пов'язані з використанням уразливих елементів у корпоративних базах даних, що можуть стати основою для виведення чутливої інформації.

П. Хендерсон вивчає підходи до використання технології блокчейн для захисту персональних даних від атак, зокрема від витоків інформації через атаки логічних висновків [2]. Він стверджує, що децентралізація даних може знизити рівень загрози від несанкціонованого доступу. Проте його дослідження не охоплює інтеграцію таких технологій у вже існуючі корпоративні системи, що обмежує практичну цінність цієї концепції для комерційних підприємств, які працюють з великими масивами даних.

A. Zhang, досліджуючи захист даних у сфері фінансових технологій, наголошує на важливості застосування методів диференціації даних для зменшення ефективності атак

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

логічних висновків [3]. Він пропонує використовувати алгоритми для створення псевдодані, що ускладнюють виведення реальних зв'язків між даними. Однак він не враховує вплив цього підходу на ефективність бізнес-операцій, що може призвести до значного сповільнення обробки запитів, особливо в реальному часі.

J. Müller акцентує увагу на використанні алгоритмів машинного навчання для виявлення і запобігання атак логічних висновків у великих масивах даних комерційних підприємств [4]. Він пропонує використовувати інтеграцію штучного інтелекту для автоматичного виявлення аномалій і непередбачуваних патернів у даних. Проте його дослідження не враховує проблеми адаптації таких систем до різноманіття даних, які можуть бути збережені в базах даних підприємства, що ускладнює процес їх інтеграції.

В. Ковальчук в українських дослідженнях, присвячених захисту персональних даних, підкреслює важливість використання багатофакторної аутентифікації і шифрування даних як основних методів захисту від атак логічних висновків на комерційних підприємствах [5]. Водночас він звертає увагу на важливість комплексного підходу, що включає регулярне оновлення політик безпеки та проведення тренінгів для співробітників підприємства, щоб зменшити ймовірність успішного проведення атак. Однак його робота не розглядає в повному обсязі питання захисту даних у рамках співпраці з третіми сторонами, що може бути критичним в умовах глобалізації бізнесу.

Таким чином, сучасні підходи до захисту персональних даних вказують на необхідність інтеграції багатьох технологій та методів для ефективного запобігання атакам логічних висновків на комерційних підприємствах. Водночас дослідження не завжди охоплюють всі аспекти практичної реалізації таких методів, що вимагає подальших розробок і впровадження нових інструментів захисту.

Виклад основного матеріалу. Методи захисту персональних даних на комерційних підприємствах набувають все більшого значення у зв'язку з постійним зростанням обсягів зібраної та оброблюваної інформації. Сучасний бізнес, активно використовуючи персональні дані для персоналізації послуг, прогнозування тенденцій та оптимізації процесів прийняття рішень, стикається з проблемами безпеки, оскільки централізоване зберігання та аналіз величезних обсягів даних створюють потенційні ризики витоку та несанкціонованого доступу. Зокрема, атаки логічних висновків дозволяють зловмисникам ідентифікувати приховані зв'язки між, на перший погляд, анонімними даними, що може призвести до порушення конфіденційності та втрати контролю над персональною інформацією.

Різні методи захисту, зокрема анонімізація даних, такі як анонімність, розмаїтість та близькість, спрямовані на ускладнення ідентифікації окремих записів, однак дослідження показують, що навіть такі підходи можуть бути скомпрометовані у випадку обробки великих масивів даних із високою розмірністю. Крім того, методи диференційної приватності дозволяють додавати шум до обчислювальних процесів перед обміном інформацією, що мінімізує ризик відтворення вихідних даних, але при цьому може впливати на точність аналітики. Іншим перспективним напрямком є використання криптографічних підходів, зокрема повністю гомоморфного шифрування, що забезпечує можливість обробки зашифрованих даних без їх розшифрування, проте такі методи залишаються ресурсомісткими та не завжди ефективними у комерційному середовищі.

Застосування технології блокчейн та децентралізованих систем управління персональними даними розглядається як один із можливих варіантів вирішення проблеми довірених обчислень, оскільки дозволяє користувачам зберігати контроль над власною інформацією без необхідності покладатися на централізовані організації. Використання блокчейну в поєднанні з офчейн-сховищами може забезпечити баланс між конфіденційністю та доступністю даних для бізнес-процесів. У межах цієї концепції реалізується механізм управління доступом до персональних даних, що базується на смарт-контрактах і криптографічних механізмах авторизації [1, 3]. Таким чином, розвиток методів захисту персональних даних на комерційних

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

підприємствах потребує комплексного підходу, що поєднує правові, організаційні та технічні заходи, включаючи передові методи анонімізації, криптографічного захисту та децентралізованого управління інформацією, аби ефективно протидіяти атакам логічних висновків та іншим загрозам у цифровому середовищі.

У роботі розглядаються актуальні питання захисту персональних даних користувачів, які взаємодіють із сторонніми сервісами, з особливим акцентом на мобільні платформи, де програмні застосунки постійно здійснюють збір, обробку та зберігання великого обсягу персональної інформації без повного контролю та усвідомлення з боку користувачів. Однією з ключових проблем є те, що мобільні додатки, отримуючи доступ до конфіденційних даних (наприклад, геолокації, контактів, записів дзвінків), роблять це без можливості гнучкого налаштування дозволів у режимі реального часу, що ускладнює управління інформаційною безпекою.

Запропонована система забезпечує кілька рівнів захисту від типових загроз конфіденційності, зокрема гарантує право власності користувача на його персональні дані, надаючи можливість контролювати доступ до них шляхом чітко визначених правил авторизації та делегування дозволів. Особливу увагу приділено прозорості та можливості аудиту: користувач може у будь-який момент переглянути, які дані збираються та як саме вони використовуються [4]. Важливим аспектом є впровадження гнучкої системи контролю доступу, що дозволяє змінювати або відкликати надані раніше дозволи без необхідності повного видалення облікового запису. Такий механізм може значно покращити сучасні системи управління дозволами в мобільних застосунках, при цьому зберігаючи надійність та безпеку через використання блокчейн-технологій.

Архітектура запропонованого рішення включає три ключові компоненти: мобільних користувачів, які встановлюють застосунки; сервіси, що розробляють та впроваджують ці застосунки для обробки персональних даних у комерційних та аналітичних цілях (наприклад, для персоналізації реклами чи покращення клієнтського досвіду); а також вузли мережі, які підтримують блокчейн та розподілене сховище даних, забезпечуючи механізми контролю доступу та збереження інформації.

Система реалізує два основних типи транзакцій у блокчейні: T_{access}, що керує правами доступу, та T_{data}, яка використовується для зберігання та запиту даних. Наприклад, при першому встановленні мобільного застосунку для захисту конфіденційності користувача генерується спільний ідентифікатор (користувач-сервіс), який записується у блокчейн разом із початковими дозволами через транзакцію T_{access}. Далі зібрані персональні дані, такі як GPS-координати чи дані сенсорів, шифруються за допомогою спільного ключа та записуються у блокчейн транзакцією T_{data}. При цьому у відкритому реєстрі зберігається лише хеш SHA-256 даних, тоді як самі дані передаються у розподілене офчейн-сховище.

Для отримання доступу до персональної інформації користувач або сервіс надсилає запит T_{data} з відповідним ідентифікатором, після чого блокчейн перевіряє цифровий підпис та чинні дозволи. Якщо права доступу підтверджені, запитувані дані надаються у відповідь. Користувач у будь-який момент може змінити рівень дозволів або відкликати доступ до раніше переданої інформації, оновивши транзакцію T_{access}.

Спільний ідентифікатор ID для пари «користувач-сервіс» формується за допомогою хеш-функції на основі ідентифікаторів користувача та сервісу:

$$ID = H(user_{id},\ service_{id}), \tag{1}$$

де $user_{id}$ – унікальний ідентифікатор користувача, $service_{id}$ – унікальний ідентифікатор сервісу, H – криптографічна хеш-функція (наприклад, SHA-256). Це забезпечує генерацію унікального ідентифікатора, що є важливим для запису даних у блокчейн.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Персональні дані, наприклад, GPS-координати D_{gps}, шифруються за допомогою спільного ключа K і записуються у блокчейн через транзакцію T_{data}:

$$D_{encrypted} = E_K(D_{gps}), \tag{2}$$

де E_K – криптографічна функція шифрування за допомогою спільного ключа K, D_{gps} – необроблені GPS-координати.

Обчислення хешу для зберігання у блокчейні:

$$H(D_{encrypted}) = SHA\text{–}256(D_{encrypted}), \tag{3}$$

де H – хеш-функція SHA-256 для отримання короткої ідентифікації шифрованих даних, яка записується у блокчейн.

Транзакція T_{data} записується у блокчейн, що містить хеш зашифрованих даних:

$$T_{\text{data}} = \{ID, H(D_{encrypted})\}, \tag{4}$$

Користувач або сервіс надсилає запит на доступ до даних через транзакцію T_{data}з відповідним ідентифікатором ID:

$$T_{\text{data}} = \{ID,\ signature\}, \tag{5}$$

де $signature$ – цифровий підпис для підтвердження запиту користувача або сервісу.

Блокчейн перевіряє цифровий підпис і відповідні права доступу. Якщо права доступу підтверджені, система надає дані:

$$if\ permissions_valid(ID) = True \Rightarrow Access\ Granted, \tag{6}$$

де $permissions_valid(ID)$– цифровий підпис для підтвердження запиту користувача або сервісу.

Користувач може оновити рівень дозволів через транзакцію T_{access}:

$$T_{\text{access}} = \{ID, \{new_permissions\}\}, \tag{7}$$

де $new_permissions$ – новий набір дозволів для доступу до даних. Наведені моделі ілюструють процес забезпечення захисту персональних даних у системі, використовуючи блокчейн для зберігання хешів зашифрованих даних та управління правами доступу через транзакції T_{access} і T_{data}.

Офчейн-сховище реалізоване за допомогою розподіленої хеш-таблиці (DHT) на основі Kademlia, що забезпечує масштабованість та стійкість до відмов завдяки розподіленій реплікації даних між вузлами (рис.1). Для забезпечення довготривалого зберігання використовується механізм LevelDB з інтеграцією до блокчейну. Альтернативно можуть використовуватися централізовані хмарні рішення для збереження даних, однак вони потребують певного рівня довіри до сторонніх постачальників послуг [2, 4-5]. Це дозволяє забезпечити надійність і безпеку зберігання даних, зменшуючи залежність від єдиного постачальника послуг. Водночас, система залишається гнучкою, оскільки дозволяє вибір між децентралізованими та централізованими підходами в залежності від вимог до безпеки та доступності.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

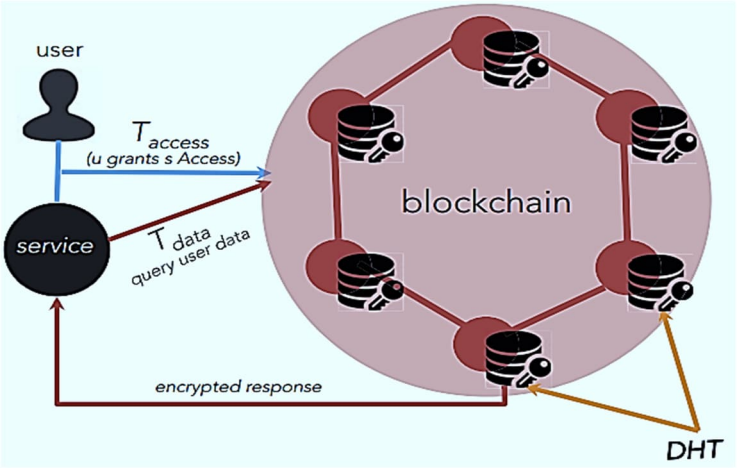


Рис. 1. Огляд децентралізованої платформи для захисту персональних даних

Джерело: розроблено автором в середовищі Canva

Розподілені хеш-таблиці, зокрема Kademlia, забезпечують ефективне зберігання і пошук даних у розподіленій мережі вузлів. Ключове поняття в Kademlia – це хеш-ідентифікатор k, який використовується для визначення місцезнаходження даних у мережі. Дані D зберігаються на вузлах мережі відповідно до їх хеш-ідентифікатора k, де k розраховується як хеш-значення:

$$k = H(D), \tag{8}$$

де D – дані, що зберігаються в мережі (наприклад, зашифровані дані), H – хеш-функція (наприклад, SHA-256). Кожен вузол має унікальний ідентифікатор id_{node}, і дані D зберігаються на найближчому до хешу k вузлі, що має ідентифікатор id_{node} з мінімальною відстанню по метриці XOR:

$$d_{node} = XOR(k, id_{node}), \tag{9}$$

де d_{node} – відстань між хешем даних k та ідентифікатором вузла id_{node}, XOR – побітова операція «виключаюче АБО». Для забезпечення стійкості до відмов дані реплікуються на кількох вузлах. Кількість реплік можна описати через функцію RRR:

$$R(D) = \{d_1, d_2, \dots, d_n\}, \tag{10}$$

де $R(D)$ – множина вузлів, на яких зберігаються репліки даних D, n – кількість реплік.

Для захисту персональних даних комерційних підприємств від атак логічних висновків впроваджується мережевий протокол, який використовує криптографічні механізми в децентралізованій платформі. Це забезпечує шифрування даних, цифровий підпис і контроль доступу, унеможливлюючи несанкціоноване втручання.

Фундаментальною складовою цього протоколу є система ідентифікації користувачів, що базується на використанні псевдоідентичностей, які дозволяють кожному суб'єкту створювати унікальні ключові пари, необхідні для автентифікації та шифрування переданих даних. Для посилення рівня безпеки в межах системи реалізовано концепцію складених ідентичностей, що передбачає створення спільного облікового запису для двох або більше суб'єктів, де одна сторона має повний контроль над даними, а інші – обмежений доступ відповідно до наданих дозволів. Основною перевагою такої архітектури є можливість

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

безпечного зберігання та передачі даних, оскільки навіть у випадку перехоплення інформації сторонніми особами її дешифрування є неможливим без відповідних криптографічних ключів.

Структурно протокол функціонує на базі блокчейну, який виступає не лише як розподілена книга обліку транзакцій, а й як захищене середовище зберігання критично важливих контрольних записів, що гарантує їхню незмінність та захист від фальсифікації. З метою оптимізації процесу управління даними блокчейн використовується для збереження лише хеш-ідентифікаторів файлів, тоді як самі дані розміщуються у розподіленій базі даних, що значно зменшує навантаження на систему та покращує швидкість доступу до інформації. Управління доступом до персональних даних у цій системі здійснюється за допомогою спеціальних транзакцій, які розподіляються на два основні типи: транзакції доступу, що містять набір дозволів, які користувач надає конкретному сервісу, та транзакції даних, які забезпечують можливість виконання операцій читання та запису інформації відповідно до визначених правил безпеки [1-2]. Такий механізм дозволяє користувачам самостійно контролювати, хто та в якому обсязі може отримати доступ до їхніх персональних даних, а також забезпечує автоматизоване оновлення дозволів у разі зміни політики конфіденційності.

З точки зору захисту інформації протокол ґрунтується на комбінації кількох криптографічних методів, які забезпечують цілісність і конфіденційність даних на всіх етапах їхнього зберігання та передачі. Зокрема, симетричне шифрування використовується для безпечного кодування переданої інформації, тоді як цифровий підпис дозволяє перевіряти автентичність транзакцій і гарантувати, що дані не були підроблені під час передачі. Додатково впроваджений механізм хешування, який використовується для створення унікальних ідентифікаторів даних, забезпечує їхню незмінність, що особливо важливо для підтримки захисту від атак, спрямованих на модифікацію або фальсифікацію інформації.

Однією з ключових переваг цього підходу є те, що навіть у разі компрометації одного з вузлів мережі або отримання зловмисником доступу до частини розподіленої бази даних, розкриття повного масиву інформації стає неможливим через розділення даних на окремі блоки, кожен із яких зашифрований унікальним ключем. Більше того, використання механізму складених ідентичностей дозволяє обмежити потенційні наслідки атаки, оскільки кожен користувач має окремий набір криптографічних ключів для взаємодії з кожним сервісом, що унеможливлює масштабний витік даних навіть у випадку компрометації окремого облікового запису [3, 5]. Таким чином, запропонований мережевий протокол є комплексним рішенням, що забезпечує багаторівневий захист персональних даних на комерційних підприємствах, запобігаючи несанкціонованому доступу, маніпуляції інформацією та можливості її аналізу методами логічного висновку, гарантуючи при цьому прозоре управління дозволами, децентралізований контроль автентичності та високу стійкість до потенційних загроз.

Методи захисту персональних даних від атак логічних висновків на комерційному підприємстві вимагають нових підходів і технологій, що забезпечують не тільки конфіденційність, а й ефективність обробки даних. Перспективні розширення технології блокчейну можуть відіграти ключову роль у розвитку більш зрілих і надійних розподілених обчислювальних платформ, які дозволять захистити персональні дані від таких атак. Від зберігання даних до їх обробки блокчейн може стати основою для створення більш безпечних і ефективних рішень, які здатні покращити захист інформації в умовах сучасних загроз.

Один з основних викликів при використанні блокчейну для захисту персональних даних полягає у його публічному характері. Більшість існуючих рішень обмежуються зберіганням посилань на зашифровані дані, що обмежує прямий доступ до них, але не гарантує повної безпеки при обробці інформації. Крім того, сторонні сервіси, маючи доступ до необроблених даних, можуть зберігати їх для подальшого аналізу, що створює нові вектори ризику.

Один із можливих шляхів вирішення цієї проблеми – це забезпечення обробки даних без їх безпосереднього доступу. Для цього можна використати методи розподілених

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

обчислень, такі як розподіл даних на частини за допомогою методу розподілу секретів Шаміра. Це унеможливлює відновлення даних без наявності ключових компонентів. Безпечні багатосторонні обчислення можуть бути використані для обробки інформації без її розкриття [1, 4-5]. Такий підхід дозволяє виконувати обчислення без відновлення вихідних даних, що підвищує рівень конфіденційності і безпеки.

Прикладом такого рішення може бути система електронного голосування на основі блокчейну. У разі використання мобільного застосунку для голосування виборці передають свої голоси в зашифрованому вигляді. Після завершення голосування результати аналізуються за допомогою розподіленої мережі, де вузли виконують обчислення в межах MPC-протоколу. Важливо, що жоден вузол не має доступу до всього масиву голосів, а результати голосування безпечно зберігаються в блокчейні. Це забезпечує конфіденційність голосів та захист від маніпуляцій.

Однак у класичних блокчейн-системах, таких як Bitcoin, усі вузли вважаються однаково ненадійними, і їхній вплив на ухвалення рішень визначається тільки обчислювальними ресурсами. Це створює певні недоліки, такі як високі енергетичні витрати, затримки в обробці транзакцій і вразливість до атак типу «Сібіл». Для вдосконалення механізмів захисту можна ввести нову динамічну метрику довіри, яка базується на історії дій вузлів. Рівень довіри до кожного вузла оцінюється на основі ймовірності його коректної поведінки в майбутньому. Це дозволяє зменшити ймовірність атак і надавати більшу вагу рішенням надійних вузлів, що підвищує ефективність мережі.

Таке підвищення довіри до вузлів дозволяє ефективно обробляти транзакції, але може створити нові ризики, такі як маніпуляції з довірою. Однак для мінімізації цих ризиків можна застосовувати стратегії, наприклад, випадковий вибір вузлів для верифікації кожного блоку з урахуванням їхнього рівня довіри, але з рівномірним розподілом голосів. Це допоможе уникнути концентрації влади в руках окремих учасників і забезпечить більш справедливий розподіл відповідальності. Загалом, застосування технологій блокчейну, зокрема методів безпечних багатосторонніх обчислень та вдосконалених моделей довіри, дозволяє побудувати більш ефективні і безпечні механізми захисту персональних даних, зменшуючи ризики атак логічних висновків, оптимізуючи ресурси та підвищуючи стійкість до маніпуляцій з боку зловмисників.

Висновки. З огляду на виклики захисту персональних даних від атак логічних висновків у комерційних підприємствах, очевидно, що сучасні методи зберігання та обробки даних потребують удосконалення. Блокчейн, інтегрований з рішеннями для зберігання поза мережею, надає користувачам повний контроль над їхніми даними, гарантуючи при цьому високий рівень безпеки та прозорості. Завдяки цьому підходу, компанії можуть зосередитись на ефективному використанні даних без ризиків зловживань та витоків інформації. Децентралізовані платформи дозволяють спростити прийняття юридичних та регуляторних рішень щодо чутливих даних, автоматично забезпечуючи їх виконання через вбудовані в блокчейн нормативи. Така система не тільки підвищує рівень захисту, але й забезпечує більшу довіру між користувачами та компаніями, створюючи основу для подальшого розвитку інноваційних рішень у сфері обробки персональних даних.

Список використаних джерел

1. Демиденко, В. Методи захисту персональних даних в умовах динамічного розвитку інформаційних технологій / В. Демиденко // Наукові праці. – 2020. – Т. 22, № 3. – С. 78–85.

2. Henderson, P. Blockchain-based Personal Data Protection against Logical Inference Attacks / P. Henderson // Journal of Cybersecurity and Data Privacy. – 2019. – Vol. 10, No. 2. – P. 45–50.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

3. Zhang, A. Differentiating Data for Preventing Logical Inference Attacks / A. Zhang // International Journal of Security and Privacy. – 2020. – Vol. 14, No. 5. – P. 204–211.

4. Müller, J. Machine Learning Algorithms for Detecting Logical Inference Attacks in Commercial Data Systems / J. Müller // Journal of Artificial Intelligence and Data Security. – 2021. – Vol. 18, № 1. – P. 102–108.

5. Ковальчук, В. Захист персональних даних від атак логічних висновків на комерційних підприємствах / В. Ковальчук // Інформаційна безпека України. – 2019. – Т. 14, № 4. – С. 34–40.

Роботу виконано під науковим керівництвом канд. техн. наук, професора
ХОХЛАЧОВОЇ Ю. Є.

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПОШИРЕНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДО КВАНТОВИХ АТАК

ШОСТАК Л. В., 2 курс 9м група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті розглянуто вразливості поширених алгоритмів шифрування з урахуванням перспектив появи потужних квантових обчислювальних пристроїв. Висвітлено теоретичне підґрунтя виникнення квантових атак, зокрема алгоритму Шора й алгоритму Гровера, та проаналізовано їхній вплив на стійкість поширених криптосистем. Розглянуто останні дослідженя у галузі постквантової криптографії, зокрема програму Національного Інституту Стандартів і Технологій Сполучених Штатів Америки із відбору перспективних алгоритмів. Зроблено висновки щодо нагальної потреби модернізації криптографічних стандартів і впровадження гібридних рішень.

The article examines the vulnerabilities of commonly used encryption algorithms, taking into account the prospects of powerful quantum computing devices. It highlights the theoretical background of quantum attacks, particularly Shor's algorithm and Grover's algorithm, and analyzes their impact on the security of common cryptosystems. The latest research in post-quantum cryptography is reviewed, including the National Institute of Standards and Technology program for selecting promising algorithms. Conclusions emphasize the urgent need to modernize cryptographic standards and introduce hybrid solutions.

Актуальність. У сучасному світі захист інформації відіграє критичну роль у багатьох сферах діяльності – від державної безпеки та банківської сфери до електронної комерції та комунікаційних сервісів. На сьогодні найбільш поширеними методами забезпечення цілісності, конфіденційності та автентичності даних є криптографічні алгоритми, зокрема асиметричні (RSA – Rivest–Shamir–Adleman, ECC – Elliptic-curve cryptography) та симетричні (AES – Advanced Encryption Standard, 3DES – Triple Data Encryption Standard) [1]. Проте з появою квантових обчислень традиційні криптосистеми можуть стати вразливими до атак, що використовують квантові алгоритми.

Квантовий комп'ютер, завдяки явищу суперпозиції й заплутаності, здатен розв'язувати певні класичні криптографічні задачі в значно коротший час, порівняно зі звичайним комп'ютером. Найбільш відомим прикладом є алгоритм Шора, який дає змогу здійснювати розкладання великих чисел на прості множники за поліноміальний час, замість

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

експоненційного, фактично руйнуючи безпеку RSA й інших алгоритмів із подібною математичною основою [2]. Ця загроза є настільки серйозною, що багато країн та наукових організацій уже активно інвестують у дослідження постквантових алгоритмів шифрування, аби встигнути перейти на нові криптосистеми до настання «квантової переваги».

Тобто, актуальність теми зумовлена перспективою реальної втрати криптостійкості сучасних інформаційних систем. Це може призвести до витоку конфіденційної інформації, фінансових збитків, загроз державній безпеці та інших негативних наслідків.

Метою дослідження є комплексний аналіз основних поширених алгоритмів шифрування (RSA, ECC, AES) у контексті їхньої потенційної вразливості до атак, що застосовують квантові обчислення, а також формування рекомендацій щодо переходу до постквантових схем захисту.

Предметом дослідження є криптографічна безпека інформаційних систем, у яких використовуються класичні (не постквантові) алгоритми шифрування.

Об'єктом дослідження є процеси проведення квантових атак на поширені криптосистеми (RSA, ECC, AES) та методи оцінювання криптостійкості за умови прогресу у квантових обчисленнях.

Аналіз попередніх досліджень і публікацій.

Peter W. Shor: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, 1994. Класична робота, у якій уперше запропоновано алгоритм Шора для факторизації та обчислення дискретного логарифма на квантовому комп'ютері.

Michael A. Nielsen, Isaac L. Chuang: Quantum Computation and Quantum Information, 2000. Одна з найвпливовіших фундаментальних монографій, дає детальний огляд від квантової механіки до квантових обчислень та інформації, в тому числі про квантову криптографію.

Jiang Zhang, Dingyi Pei, Yupu Hu: Quantum Cryptography and Secret-Key Distillation, 2007. Робота присвячена розвитку квантової криптографії та методам дистиляції секретного ключа, що забезпечують безпеку зв'язку на квантовому рівні.

Peter Schwabe, Douglas Stebila, Thom Wiggers: Post-Quantum TLS Without Handshake Signatures, 2022. Описує постквантову альтернативу сучасному протоколу TLS – протокол KEMTLS. Публікація включає аналіз безпеки, ефективності та швидкодії.

Горбенко І.Д., Качко О.Г.: Основні положення та результати порівняння властивостей електронних підписів постквантового періоду, 2021. Порівнює алгоритми підписів (включаючи Falcon та SPHINCS+) з позиції продуктивності, стійкості та придатності до імплементації.

Калушка М.М.: Алгоритми гібридного шифрування, 2024. Містить поради з комбінування класичних та постквантових криптографічних рішень в перехідний період.

Горбенко І.Д., Потій О.В.: Постквантова криптографія та механізми її реалізації, 2016. Розглядаються класи постквантових алгоритмів, сценарії загроз, і надаються рекомендації щодо їх впровадження в IT-інфраструктуру.

Виклад основного матеріалу.

Станом на 2025 рік найпоширенішими алгоритмами шифрування залишаються відносно старі:

Таблиця 1

Поширені алгоритми шифрування

Алгоритм	Тип	Типова довжина ключа, біт	Рік стандартизації	Найчастіша сфера застосування
AES	Симетричний блоковий шифр	128, 192, 256	1998 (Rijndael); стандарт 2001	TLS, VPN, дискове та файлове шифрування (BitLocker, VeraCrypt)

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Алгоритм	Тип	Типова довжина ключа, біт	Рік стандартизації	Найчастіша сфера застосування
RSA	Асиметричний (криптосистема з відкритим ключем)	2048–4096	1977	Безпечний обмін ключами, цифрові підписи (SSL/TLS, S/MIME, PGP), банківські системи
ECDH	Асиметричний на еліптичних кривих	256, 384	1985	Банки, е-комерція, VPN
ECDSA	Асиметричний на еліптичних кривих	256	1999	Блокчейн, електронні підписи, SSL
ECIES	Асиметричний на еліптичних кривих	256	2004	хмарні сервіси, месенджери, VPN
ChaCha20	Симетричний потоковий шифр	256 біт (як правило з 96-бітним nonce)	2008	Мобільні та ресурсообмежені пристрої, швидке шифрування трафіку (TLS 1.3, VPN), часто разом із Poly1305 (AEAD)
ДСТУ 4145-2002	Асиметричний на еліптичних кривих	128, 192, 256 біт	2002	Електронні цифрові підписи (ЕЦП)
ДСТУ 7624:2014 («Калина»)	Симетричний блоковий шифр	128, 256, 512 біт	2014	Шифрування даних у держустановах, банківській сфері
ДСТУ 7564:2014 («Купина»)	Геш-функція	256, 384, 512 біт (вихідний хеш)	2014	Контроль цілісності даних, цифрові підписи

Джерело: розроблено автором

Сучасні комп'ютери оперують бітами, що можуть набувати лише двох значень – 0 або 1. Квантові комп'ютери використовують квантові біти (кубіти), які окрім 0 або 1, також можуть перебувати в суперпозиції цих станів, що дає змогу обробляти більшу кількість інформації паралельно.

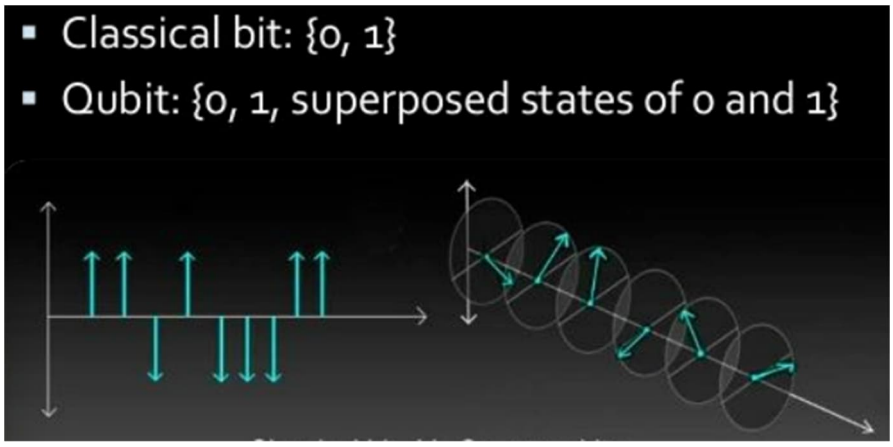


Рис. 1. Класичний та квантовий біти

Джерело: https://devopedia.org/qubit

У загальному розумінні квантова атака – це криптографічна атака, що використовує обчислювальні можливості квантових комп'ютерів для зламу або послаблення стійкості

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

класичних криптографічних алгоритмів. Основними квантовими алгоритмами, що можуть незабаром використовуватися для квантових атак і становити практичну небезпеку для сучасних криптосистем є алгоритм Шора та алгоритм Гровера.

Вразливість RSA – Алгоритм Шора.

Алгоритм RSA базується на складності розкладання великих (1024, 2048, 4096 біт) чисел на прості множники. Алгоритм Шора – це квантовий алгоритм, що дозволяє розкладати великі числа на множники набагато швидше, ніж класичні алгоритми. Він базується на ідеї перетворення задачі факторизації до пошуку періоду функції в арифметиці за модулем заданого числа. Квантовий комп'ютер обчислює цей період за допомогою перетворення Фур'є та принципу квантової паралельності, а вже потім з отриманим періодом класично відновлюються множники. Для класичних алгоритмів факторизації час O для розкладання числа N зростає експоненційно:

-Метод перебору та Метод Ферма: $O\left(\sqrt{N}\right)$;

-Метод Лемана: $O\left(N^{1/3}\right)$;

-Метод квадратичних форм Шенкса та Алгоритм Полларда: $O\left(N^{1/4}\right)$.

Квантовий алгоритм Шора розв'язує цю задачу за поліноміальний час: $O(log^3 N)$[2].

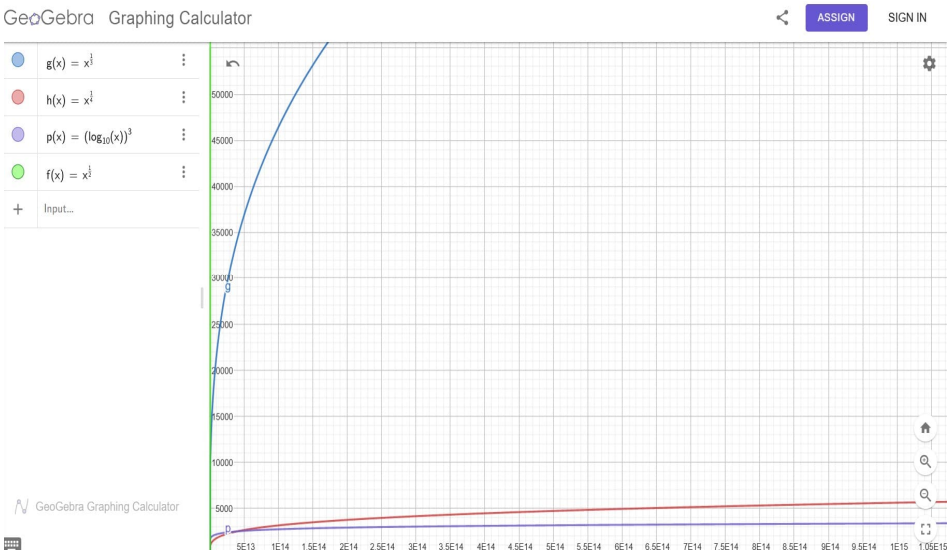


Рис. 2. Умовне зображення швидкодії алгоритмів факторизації. Зелений колір – методи перебору та Ферма, синій – метод Лемана, червоний – Шенкса та Полларда, фіолетовий – алгоритм Шора. Вісь абсцис – число N, вісь ординат – час факторизації O

Джерело: розроблено автором у середовищі Geogebra Graphing Calculator.

Таким чином, зловмисник зоже отримати приватний ключ за відомим відкритим ключем і цілком зламати систему шифрування або електронного підпису [2, с. 15]. Тобто, RSA-1024 стає слабким за наявності квантового комп'ютера з кількома тисячами кубітів, здатних працювати стабільно (що відповідає умовам корекції помилок і т.ін.); RSA-2048 теж у зоні ризику, хоча потребує потужнішого квантового пристрою, але поточні оцінки вказують на можливість його зламу такими пристроями протягом десятиліття чи двох [3, с. 7]; RSA-4096 вважається більш надійним, однак при подальшому прогресі в технологіях квантових обчислень і він не гарантує абсолютної безпеки.

Вразливість ECC – Алгоритм Шора.

Криптосистеми на основі еліптичних кривих (ECC) – наприклад, ECDSA, ECDH, ECIES, ДСТУ 4145-2002 – вважаються більш ефективними, ніж RSA, за

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

однакових рівнів безпеки. Проте вони також базуються на математично складній задачі (логарифм на еліптичних кривих), яка може бути розв'язана квантовим алгоритмом Шора за поліноміальний час [5, с. 21].

Це можливо завдяки тому, що насправді алгоритм Шора призначений не тільки для факторизації, а загалом розв'язує задачу прихованої підгрупи в абелевих групах. Дискретний логарифм, як і факторизація, належить до цього ж класу задач. [7]

Тобто ECC-256, ECC-384, ECC-521 вразливі до таких самих фундаментальних загроз, як і RSA, хоч і потребують іншої конкретної реалізації алгоритму Шора.

Загалом, ECC-256 вважається приблизним еквівалентом безпеки з RSA-3072 у класичному контексті, але в квантовому сценарії обидві схеми мають аналогічні проблеми. Збільшення розміру ключа ECC покращує безпеку, проте квантова атака залишається поліноміальною. Тому, як і у випадку з RSA, ведуться дослідження щодо переходу на новітні криптографічні схеми (на основі граток або кодів), аби мати рівень квантової стійкості, що гарантує захист від зламу на десятиліття вперед.

Вразливість AES, ChaCha20, ДСТУ 7624:2014 («Калина»), ДСТУ 7564:2014 («Купина») – Алгоритм Гровера.

Алгоритм Гровера використовує квикористовує ефект квантової суперпозиції та «віддзеркалення» (інверсію та дифузію) амплітуди станів, аби поступово збільшувати ймовірність єдиного шуканого елемента серед можливих. Це дозволяє досягти прискорення пошуку з $O(N)$ у класичній моделі до $O(\sqrt{N})$ у квантовій. [4]. Тобто шифр AES-128 за квантових умов матиме ефективну безпеку рівня приблизно 64 біт. Хоча це все ще велике число, зниження рівня безпеки вдвічі – дуже суттєвий фактор.

AES-128 у квантовій парадигмі прирівнюється до безпеки 64-бітного ключа. Це є фактично загрозою, але все ж таки злам 64-бітного шифру теж не є миттєвим процесом, хоча значно простішим за 128-бітний перебір у класичному середовищі [1, с. 45].

AES-256 та Chacha-20 з погляду квантових обчислень відповідатиме рівню 128 біт, що вважається досить надійним для сучасних стандартів. Саме тому багато спеціалістів рекомендують у перспективі переходити на AES-256, щоб забезпечити достатній рівень захисту навіть з урахуванням застосування алгоритму Гровера.

Геш-функція ДСТУ 7564:2014 («Купина») як і будь-яка інша класична геш-функція уразлива до алгоритму Гровера. Зазвичай, щоб підібрати передобраз *X*, для якого *H(X)=Y*, потрібно 2^n спроб для n-бітного гешу. У квантовому випадку алгоритм Гровера зменшує складність до $2^{n/2}$.

З 2017 року Національний інститут стандартів і технологій США (NIST) проводить масштабну програму стандартизації постквантової криптографії. На різних етапах ця програма розглянула низку варіантів криптосистем, що мають потенціал протистояти квантовим атакам. Найуспішнішими типами систем виявилися:

-Граткові (Lattice-based): Crystals-Kyber, SABER, Dilithium, Falcon

-Кодові (Classic McEliece),

-Мультиваріантні (Rainbow, GeMSS),

-На основі геш-функцій Hash-based (SPHINCS+).

На момент написання статті окремі алгоритми вже відібрані для стандартизації (наприклад, Crystals-Kyber та Crystals-Dilithium), тоді як інші проходять додаткові етапи оцінювання [3; 5]. Однією з проблем є розмір ключів (особливо для кодових алгоритмів) та швидкодія: не всі запропоновані методи однаково зручні для впровадження в обмежених середовищах (IoT), мобільних пристроях чи великомасштабних дата-центрах.

Міжнародні організації (ISO, IEEE) також беруть участь у дискусії. Хоча поки що не існує обов'язкових до виконання міжнародних стандартів саме з постквантової криптографії, велика частина експертів орієнтується на рекомендації NIST як найбільш цілісні та авторитетні.

На практиці перехід до нових криптографічних схем не може бути одномоментним. Це багаторічний процес, що включає оцінку ризиків: визначення, які дані потребують довгострокового захисту. Якщо інформація має бути таємною 10–20 років, треба вже зараз

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

планувати її захист постквантовими методами. Одночасне використання традиційних та постквантових алгоритмів у TLS, VPN та інших протоколах (наприклад, комбінація ECDH+Kyber) дозволить підтримувати сумісність зі старими системами і водночас забезпечити «захист наперед». Також потрібна підготовка сертифікаційних центрів (CA) до випуску сертифікатів, що включають постквантові схеми. Можливе поступове збільшення розміру ключів і застосування гібридних сертифікатів (X.509). Аудит криптографічних бібліотек дозволить перевірити, які саме алгоритми вбудовані у програмні платформи (OpenSSL, BoringSSL, mbedTLS тощо), чи є підтримка Kyber, Dilithium тощо.

Оскільки квантова криптографія – нова галузь, що вимагає від спеціалістів додаткових знань і досвіду, будуть необхідні інвестиції у навчання персоналу та розробників.

Великий виклик полягає у тому, що багато організацій (банки, державні установи, медичні заклади) мають складну інфраструктуру, яка не оновлювалася десятиріччями. Тому впровадження постквантових рішень вимагає чіткої стратегії та співпраці з фахівцями з IT-безпеки.

На сьогодні реальні квантові процесори, створені IBM, Google, Intel, Rigetti, IonQ та іншими компаніями, мають десятки чи сотні кубітів. Проте більшість з них є шумними (Noisy Intermediate-Scale Quantum – NISQ) і не здатні вирішувати великі криптографічні задачі. Тим не менш, прогрес у цій галузі йде швидко, і деякі експерти вважають, що досягнення порогу в тисячі стабільних кубітів може статися впродовж наступних 5–10 років.

Як тільки квантові комп'ютери вийдуть на рівень декількох тисяч або навіть мільйонів кубітів (із корекцією помилок), злам розглянутих алгоритмів стане цілком реальним. При цьому історично зафіксовані перехоплені зашифровані повідомлення зможуть бути розкриті ретроспективно. Тобто атака може бути відкладена в часі до моменту, коли з'явиться достатньо потужний комп'ютер. Це особливо небезпечно для даних, цінність яких зберігається десятки років (дипломатична, військова, медична інформація та ін.). Отже, необхідність захисту в майбутньому спонукає до вже сьогоднішнього переходу на схеми шифрування, що вважаються квантостійкими.

Сучасні поширені алгоритми шифрування (RSA, ECC, AES-128) уразливі до атак, які використовують квантові алгоритми (Шора, Гровера). RSA та ECC можуть бути зламані за поліноміальний час за наявності достатньо потужного квантового комп'ютера, тоді як ефективна безпека AES із довжиною ключа 128 біт знижується до 64 біт.

Прогрес квантових обчислень свідчить, що протягом найближчих 5–20 років імовірний вихід квантових процесорів із достатньою кількістю кубітів для зламу традиційних криптосистем. Це становить серйозну загрозу для довгострокового зберігання та передавання секретних даних.

NIST та інші організації пропонують переходити на постквантові (lattice-based, code-based тощо) або гібридні криптосхеми. Зокрема, алгоритми Crystals-Kyber і Crystals-Dilithium уже рекомендовані як перспективні стандарти.

Практична реалізація квантових стійких рішень потребує ретельного планування, включаючи аудит чинних систем, оновлення криптографічних бібліотек, випуск нових сертифікатів і поступову інтеграцію в протоколи безпеки (TLS, VPN).

Подальші дослідження у цій галузі мають охоплювати створення більш ефективних постквантових алгоритмів із меншими ключами та більшою швидкодією, вивчення механізмів корекції помилок у квантових обчисленнях для визначення реальних ресурсів, потрібних для зламу RSA чи ECC та розробку гібридних протоколів безпеки, які могли б гарантувати стійкість як до класичних, так і до квантових атак.

Загалом, розглянута проблематика свідчить про нагальну потребу готуватися до квантового виклику вже сьогодні. Вчасна модернізація криптосистем допоможе уникнути масових компрометацій і збитків, пов'язаних із неконтрольованим зламом критично важливої інформації.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаних джерел

1. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 2015. 784 с.
2. Chen L., Jordan S., Liu Y.-K. et al. Report on Post-Quantum Cryptography. NIST, 2022. 36 с.
3. NIST Post-Quantum Cryptography Standardization. National Institute of Standards and Technology (NIST). URL: https://csrc.nist.gov/projects/post-quantum-cryptography (дата звернення 10.03.2025)
4. Grover L.K. A fast quantum mechanical algorithm for database search // Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. – 1996. – С. 212–219.
5. Bernstein D. J., Buchmann J., Dahmen E. Post-Quantum Cryptography. Springer, 2009. 266 с.
6. Hoffstein J., Pipher J., Silverman J.H. NTRU: A ring-based public key cryptosystem // Algorithmic Number Theory. – Springer, 1998. – С. 267–288.
7. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. 10th Anniversary Edition. – Cambridge University Press, 2010. – С. 217–232.

Роботу виконано під науковим керівництвом канд. техн. наук, ст. наук. співроб., доцента ЗВЄРЄВА В. П.

АРХІТЕКТУРА НАДІЙНОГО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ: ПРИНЦИПИ, МОДЕЛІ ТА МЕХАНІЗМИ РЕАЛІЗАЦІЇ

ЮРЧЕНКО Д. О., 2 курс 6мз група ФІТ ДТЕУ,
освітня програма «Безпека інформаційних і комунікаційних систем в економіці»

У статті розглянуто проблему забезпечення надійності технічного захисту інформації (ТЗІ) в умовах зростаючих кіберзагроз. Проаналізовано основні принципи побудови надійної архітектури ТЗІ, зокрема, принципи мінімальних привілеїв, глибокого захисту, розділення обов'язків, відмовостійкості, адаптивності та масштабованості. Розглянуто різні моделі архітектури ТЗІ та проведено їх порівняльний аналіз. Запропоновано практичні рекомендації щодо вибору та реалізації механізмів захисту, а також наведено приклад впровадження архітектури ТЗІ для малого виробничого підприємства.

The article addresses the problem of ensuring the reliability of technical information protection (TIP) in the face of growing cyber threats. The basic principles of building a reliable TIP architecture are analyzed, including the principles of least privilege, defense in depth, separation of duties, fault tolerance, adaptability and scalability. Various models of TIP architecture are considered and a comparative analysis is performed. Practical recommendations are proposed for the selection and implementation of security mechanisms, as well as an example of the implementation of TIP architecture for a small manufacturing enterprise.

У сучасному цифровому ландшафті, що характеризується експоненційним зростанням кількості та складності кіберзагроз, питання надійності технічного захисту інформації (ТЗІ) набуває першорядної актуальності. Збереження конфіденційності, цілісності та доступності критично важливих даних є фундаментальною вимогою для стабільного функціонування будь-якої організації, незалежно від її розміру чи галузевої приналежності. Збільшення кількості кібератак, їхня різноманітність та потенційні наслідки зумовлюють необхідність

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

переосмислення традиційних підходів до захисту інформації та переходу до більш надійних і стійких архітектур ТЗІ.

Водночас, забезпечення надійності архітектури ТЗІ є складною багатогранною проблемою, що вимагає комплексного підходу. Недостатньо простого впровадження окремих засобів захисту; необхідно створити цілісну систему, здатну ефективно протистояти різноманітним загрозам. Крім того, архітектура ТЗІ повинна бути адаптивною, здатною еволюціонувати разом із зміною ландшафту загроз та потреб організації. Важливим аспектом є також відмовостійкість, що забезпечує безперервне функціонування системи захисту навіть у разі виходу з ладу окремих компонентів.

Мета статті - визначення ключових принципів, що лежать в основі побудови надійної архітектури ТЗІ.

Об'єктом дослідження є моделі та механізми архітектури ТЗІ інформаційних систем підприємств.

Предметом дослідження є методи та технології побудови архітектури ТЗІ інформаційних систем у захищеному середовищі.

Аналіз попередніх досліджень. У сфері надійності технічного захисту інформації (ТЗІ) дослідження варіюються від моделювання захисту даних у відкритих каналах [1] до практичної побудови захищених мереж [6]. Черненко Р.М. [1] зосереджується на IoT-мережах, підкреслюючи їхню вразливість.

Важливим є реконфігурування засобів захисту [2], що дає змогу адаптуватися до нових загроз. Гільгурт С.Я. та Чемерис О.А. [2] наголошують на гнучкості та ефективності. Не слід ігнорувати фізичний захист [3].

Ковальчук І. [4] описує ключові принципи захищених систем. Руденко В.М. [5] підкреслює потребу постійного вдосконалення. Закаржевський А. [6] розглядає захищені мережі на основі загальнодоступних каналів.

Поповський В.В. [7] аналізує архітектуру телекомунікацій. Кучук Г.А. [8] вивчає управління потоками даних у критичних системах. Воробієнко П.П. [9] дає основи телекомунікацій.

Медхі Д. та Рамасамі К. [10] досліджують маршрутизацію та безпеку. Поповський В.В. [11] розглядає математичні основи.

Вуд Ч.К. [12] дає перелік елементів для оцінки безпеки. Бріл А.Е. [13] вивчає вбудовування засобів керування. Кропаткін Ф. та Куссеров Р.П. [14] описують принципи управління активами. Макбет С. [15] вивчає самоорганізацію даних.

Виклад основного матеріалу. В основі побудови ефективної системи технічного захисту інформації (ТЗІ) лежать фундаментальні теоретичні принципи та концепції, що визначають підходи до проектування, реалізації та управління безпекою інформаційних систем. Розуміння основних понять і визначень є необхідною передумовою для розробки надійної архітектури ТЗІ, здатної протистояти сучасним загрозам інформаційній безпеці.

У контексті нашої статті, під архітектурою ТЗІ розуміється структурована сукупність компонентів, засобів і методів захисту інформації, організованих у певну систему з метою забезпечення безпеки інформаційних активів організації. Архітектура ТЗІ визначає способи взаємодії між компонентами системи захисту, розподіл функцій між ними, а також правила і процедури управління безпекою.

Ключовим критерієм ефективності архітектури ТЗІ є її надійність, яка характеризується здатністю системи захисту безперебійно виконувати свої функції в умовах різних загроз і несприятливих факторів. Надійність ТЗІ оцінюється за допомогою таких критеріїв, як доступність, що відображає здатність авторизованих користувачів отримувати доступ до інформаційних ресурсів у необхідний час; цілісність, що гарантує неможливість несанкціонованої модифікації інформації; та конфіденційність, що забезпечує захист

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

інформації від несанкціонованого розкриття. Показники надійності ТЗІ можуть включати середній час між збоями, ймовірність безвідмовної роботи та час відновлення після збою.

Ефективність архітектури ТЗІ безпосередньо залежить від її здатності протистояти існуючим загрозам інформаційній безпеці. Загрози можуть бути внутрішніми (пов'язані з діями співробітників організації) або зовнішніми (пов'язані з діями зловмисників), випадковими або навмисними, технічними або організаційними. До основних загроз належать вірусні атаки, хакерські вторгнення, витік інформації, соціальна інженерія, DDoS-атаки, та інші. Вплив загроз на надійність ТЗІ може проявлятися у порушенні доступності, цілісності або конфіденційності інформації, що призводить до фінансових втрат, репутаційних ризиків та інших негативних наслідків.

Для забезпечення надійної архітектури ТЗІ необхідно дотримуватися певних принципів, які визначають підходи до проектування та реалізації системи захисту. Серед найважливіших принципів слід виділити:

Принцип мінімальних привілеїв (Principle of Least Privilege), який передбачає надання користувачам та процесам тільки тих прав і дозволів, які необхідні для виконання їхніх безпосередніх обов'язків. Це дозволяє обмежити потенційний збиток у разі компрометації облікового запису або системи.

Принцип глибокого захисту (Defense in Depth), який полягає у застосуванні декількох рівнів захисту, кожен з яких повинен компенсувати недоліки інших. Це дозволяє підвищити стійкість системи до атак, оскільки зловмиснику необхідно подолати кілька бар'єрів, щоб досягти своєї мети.

Принцип розділення обов'язків (Separation of Duties), який передбачає розподіл критичних функцій між декількома співробітниками або процесами. Це дозволяє запобігти зловживанням владою та знизити ризик помилок або навмисних дій, що можуть завдати шкоди інформаційній безпеці.

Принцип відмовостійкості (Fault Tolerance), який забезпечує безперервну роботу системи захисту навіть у разі виходу з ладу окремих компонентів. Це досягається за допомогою резервування, дублювання, використання відмовостійких технологій та інших методів.

Принцип адаптивності та масштабованості (Adaptability and Scalability), який дозволяє системі захисту адаптуватися до змін у ландшафті загроз та потреб організації. Архітектура ТЗІ повинна бути гнучкою та здатною масштабуватися, щоб відповідати зростаючим вимогам до безпеки.

Крім перерахованих вище, існують й інші важливі принципи, такі як мінімізація площі атаки (зменшення кількості потенційних вразливостей), простота (чим простіша система, тим легше її захистити), та модульність (можливість додавати та видаляти компоненти системи без порушення її функціонування). Дотримання цих принципів дозволяє створити надійну та ефективну архітектуру ТЗІ, здатну забезпечити безпеку інформаційних активів організації в умовах сучасних кіберзагроз.

Ефективний захист інформаційних активів вимагає оптимального вибору моделі архітектури технічного захисту інформації (ТЗІ), що відповідає конкретним потребам, ризикам та наявним ресурсам. Існує декілька моделей, кожна з яких має свої переваги та недоліки, і застосовується в різних умовах.

Однією з класичних є модель захищеного контуру, що ізолює критичні системи за допомогою фізичних і логічних бар'єрів, суворих політик безпеки та контролю за потоками даних. Вона ефективна для захисту особливо цінної інформації, проте складна та дорога у впровадженні.

Альтернативою є модель сегментованої мережі, що розділяє мережу на сегменти з різними рівнями захисту. Міжмережеві екрани та системи виявлення вторгнень ізолюють сегменти, обмежуючи розповсюдження загроз та полегшуючи управління безпекою.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Сучасний підхід - модель нульової довіри (Zero Trust), що не довіряє жодному користувачу чи пристрою за замовчуванням. Кожен запит на доступ перевіряється та авторизується на основі контексту, ідентифікації та політик. Модель Zero Trust ефективно захищає від внутрішніх та зовнішніх загроз, але вимагає значних інвестицій та змін в організації.

Окрім цього, використовується хмарна архітектура безпеки, що застосовує хмарні сервіси для захисту інформації. Вона може знизити витрати та підвищити гнучкість, але вимагає ретельної оцінки безпеки хмарних провайдерів.

Оцінка моделей вимагає порівняльного аналізу за критеріями надійності. Важливо оцінити їхню стійкість до різних видів атак, таких як віруси, хакерські атаки, витоки інформації, соціальна інженерія та DDoS. Також необхідна оцінка ефективності механізмів захисту, таких як міжмережеві екрани, системи виявлення вторгнень, шифрування та контроль доступу. Необхідно враховувати складність впровадження та підтримки, а також визначити переваги та недоліки кожної моделі.

Вибір моделі залежить від конкретних вимог та умов, включаючи тип інформації, ризики, бюджет та існуючу інфраструктуру. Чим цінніша інформація, тим вищі вимоги до безпеки. Необхідно оцінити ймовірність та збитки від загроз. Вартість впровадження різних моделей може значно відрізнятися. Модель повинна бути сумісною з наявною інфраструктурою.

Рекомендації щодо вибору моделі різняться для різних організацій. Малим підприємствам може бути достатньо сегментованої мережі та базових засобів захисту. Великим організаціям може знадобитися Zero Trust або поєднання моделей для багаторівневого захисту. Важливо переглядати та адаптувати модель у відповідь на зміни в ландшафті загроз.

Реалізація надійної архітектури технічного захисту інформації (ТЗІ) вимагає комплексного застосування різноманітних механізмів, які забезпечують конфіденційність, цілісність та доступність інформаційних активів. Ці механізми охоплюють різні аспекти безпеки, від автентифікації та авторизації користувачів до захисту мережі та даних.

Одним з ключових елементів забезпечення безпеки є автентифікація та авторизація. Для підтвердження особи користувача, що намагається отримати доступ до системи, застосовується багатофакторна автентифікація (MFA), яка вимагає надання кількох різних типів доказів, таких як пароль, одноразовий код з мобільного пристрою або біометричні дані. Це значно ускладнює процес несанкціонованого доступу до облікового запису. Після успішної автентифікації визначаються права доступу користувача до різних ресурсів системи. Для цього часто використовується контроль доступу на основі ролей (RBAC), який визначає рівень доступу на основі посади або ролі користувача в організації. Централізоване управління ідентифікаційними даними та доступом (IAM) дозволяє ефективно керувати обліковими записами користувачів, правами доступу та політиками безпеки.

Для захисту мережевої інфраструктури використовуються різні механізми. Міжмережеві екрани (Firewalls) фільтрують мережевий трафік на основі заданих правил, блокуючи несанкціонований доступ до внутрішніх ресурсів. Системи виявлення та запобігання вторгненням (IDS/IPS) аналізують мережевий трафік у реальному часі для виявлення та блокування шкідливих дій. Для забезпечення безпечного віддаленого доступу до мережі використовуються віртуальні приватні мережі (VPN), які створюють зашифрований канал зв'язку між користувачем та мережею. Мережева сегментація та мікросегментація дозволяють розділити мережу на окремі сегменти, кожен з яких має свій рівень захисту та політику доступу. Це дозволяє обмежити розповсюдження загроз у мережі у разі компрометації одного з сегментів.

Захист даних є критично важливим аспектом забезпечення надійної архітектури ТЗІ. Шифрування даних (Data Encryption) використовується для перетворення даних у нечитабельний формат, що робить їх незрозумілими для неавторизованих осіб. Захист від

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

витоку даних (DLP) запобігає несанкціонованому копіюванню або передачі конфіденційних даних за межі організації. Регулярне резервне копіювання та відновлення даних (Backup and Recovery) забезпечує можливість відновлення даних у разі втрати або пошкодження. Керування правами доступу до даних (DRM) дозволяє контролювати, хто має доступ до даних і що вони можуть з ними робити.

Окрім перелічених вище, існують й інші важливі механізми забезпечення надійності. Моніторинг та аудит безпеки дозволяють відстежувати події в системі та виявляти підозрілу активність. Управління вразливостями передбачає виявлення та усунення вразливостей в програмному забезпеченні та апаратних засобах. Реагування на інциденти безпеки включає розробку та впровадження планів дій у разі виникнення інцидентів безпеки. Тестування на проникнення (Penetration Testing) дозволяє перевірити ефективність системи захисту шляхом моделювання реальних атак.

Застосування перелічених механізмів в комплексі дозволяє створити надійну архітектуру ТЗІ, здатну забезпечити захист інформаційних активів організації від різноманітних загроз. Важливо враховувати, що вибір конкретних механізмів залежить від специфічних потреб та ризиків організації.

Успішне створення надійної архітектури технічного захисту інформації (ТЗІ) потребує ретельного планування, виділення ресурсів та врахування специфіки організації. Нижче наведено практичні рекомендації та приклад для малого виробничого підприємства.

Процес впровадження ТЗІ зазвичай складається з декількох етапів. Спочатку необхідно провести оцінку ризиків та визначити потреби, аналізуючи інформаційні активи, виявляючи загрози та оцінюючи їхню ймовірність. На основі цього визначаються вимоги до архітектури ТЗІ. Далі відбувається проектування архітектури ТЗІ, розробляється концептуальна модель, визначаються компоненти системи, їхні функції та зв’язки, враховуючи потреби, ризики та обмеження. Наступний етап - вибір та впровадження механізмів захисту, таких як міжмережеві екрани, системи виявлення вторгнень, антивіруси, шифрування та контроль доступу. Потім проводиться тестування та аудит безпеки, перевіряючи ефективність архітектури, виявляючи слабкі місця та вразливості. Заключний етап – моніторинг та підтримка, що включає постійний контроль, реагування на інциденти, оновлення ПЗ та зміни в політиках безпеки.

Для успішної реалізації ТЗІ необхідні ресурси та кваліфікований персонал. Важливо мати достатній бюджет на обладнання, ПЗ та оплату фахівців з інформаційної безпеки. Персонал повинен володіти необхідними знаннями та навичками для проектування, впровадження, налаштування та підтримки системи захисту.

Інтеграція нової архітектури з існуючими системами може бути складною. Необхідно враховувати сумісність компонентів та вплив змін на бізнес-процеси. Рекомендується використовувати відкриті стандарти та залучати фахівців з досвідом роботи з існуючими системами.

Розглянемо приклад для малого виробничого підприємства, яке виготовляє металоконструкції та має локальну мережу з комп’ютерами бухгалтерського обліку, конструкторського бюро та виробничого цеху, підключену до Інтернету.

Вибираються наступні механізми захисту: міжмережевий екран (Firewall) для захисту від зовнішніх загроз, антивірусне ПЗ для захисту від вірусів, система резервного копіювання даних для відновлення у разі втрати, контроль доступу на основі ролей (RBAC) для обмеження доступу до конфіденційних даних, шифрування даних для захисту даних, що передаються по мережі, та багатофакторна автентифікація для доступу до критичних систем.

Обґрунтування вибору полягає в наступному: міжмережевий екран захищає від хакерських атак, антивірус запобігає зараженню вірусами, система резервного копіювання дозволяє швидко відновити дані, RBAC обмежує доступ до конфіденційної інформації, шифрування захищає дані, що передаються, а MFA підвищує безпеку доступу до критичних систем.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Для оцінки ефективності необхідно провести тестування на проникнення, аудит безпеки та моніторинг системи. На основі результатів необхідно внести зміни до архітектури та політик безпеки для покращення захисту інформації.

В умовах зростання кіберзагроз забезпечення надійності технічного захисту інформації (ТЗІ) є критичним. Для побудови надійної архітектури ТЗІ необхідно враховувати фундаментальні принципи, такі як мінімальні привілеї, глибокий захист, розділення обов'язків, відмовостійкість, адаптивність та масштабованість. Існують різні моделі архітектури ТЗІ, кожна з яких має свої переваги та недоліки, а вибір оптимальної моделі залежить від конкретних потреб, ризиків та обмежень організації. Реалізація надійної архітектури ТЗІ вимагає комплексного застосування різноманітних механізмів, що забезпечують автентифікацію, авторизацію, захист мережі та даних. Впровадження ТЗІ має відбуватися поетапно, з урахуванням необхідних ресурсів, кваліфікації персоналу та інтеграції з існуючими системами. Для малого виробничого підприємства оптимальним може бути поєднання міжмережевого екрану, антивірусного програмного забезпечення, системи резервного копіювання даних, контролю доступу на основі ролей, шифрування даних та багатофакторної автентифікації.

У сучасному цифровому середовищі, де кількість і складність кіберзагроз постійно зростає, забезпечення надійного технічного захисту інформації (ТЗІ) стає першочерговим завданням для будь-якої організації. Для стабільного функціонування необхідно забезпечити конфіденційність, цілісність та доступність інформації, що потребує переосмислення традиційних підходів до захисту та переходу до стійких і адаптивних архітектур ТЗІ.

Ефективна архітектура ТЗІ повинна базуватися на фундаментальних принципах, серед яких пріоритетними є принцип мінімальних привілеїв, принцип глибокого захисту, принцип розділення обов'язків, принцип відмовостійкості, а також принцип адаптивності та масштабованості. Дотримання цих принципів дозволяє створити комплексну систему захисту, здатну протистояти різноманітним загрозам.

Принцип мінімальних привілеїв обмежує доступ користувачів лише до необхідних ресурсів, знижуючи ризик несанкціонованого доступу. Принцип глибокого захисту забезпечує багаторівневу безпеку, що ускладнює проникнення зловмисників. Принцип розділення обов'язків гарантує, що критичні функції виконуються різними особами або системами, що підвищує контроль. Принцип відмовостійкості забезпечує роботу системи навіть у разі збою окремих її компонентів. Принцип адаптивності та масштабованості дозволяє системі швидко реагувати на нові загрози та змінюватися відповідно до розвитку організації.

Існує декілька моделей архітектури ТЗІ, зокрема модель захищеного контуру, модель сегментованої мережі, модель нульової довіри (Zero Trust) та хмарна архітектура безпеки. Вибір оптимальної моделі залежить від специфічних потреб організації, оцінки ризиків, наявних ресурсів та характеристик інформаційних активів.

Реалізація надійної архітектури ТЗІ вимагає комплексного застосування різноманітних механізмів, що забезпечують автентифікацію та авторизацію користувачів, захист мережевої інфраструктури (міжмережеві екрани, системи виявлення вторгнень, віртуальні приватні мережі) та захист даних (шифрування, захист від витоку даних, резервне копіювання).

Впровадження ТЗІ є поетапним процесом, що включає оцінку ризиків, проектування архітектури, вибір та впровадження механізмів захисту, тестування та аудит безпеки, а також моніторинг та підтримку. Успішне впровадження потребує наявності кваліфікованого персоналу та достатніх ресурсів, а також врахування сумісності з існуючими системами.

Для малих підприємств, зокрема виробничих, ефективною стратегією може бути комбінація базових механізмів захисту, таких як міжмережевий екран, антивірусне програмне забезпечення, система резервного копіювання, контроль доступу на основі ролей, шифрування даних та багатофакторна автентифікація. Регулярне тестування та аудит системи дозволять вчасно виявити та усунути слабкі місця в архітектурі ТЗІ.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Для підтримки актуальності та ефективності архітектури ТЗІ слід регулярно проводити аудит безпеки, тестування на проникнення та аналіз вразливостей. Це дозволяє виявляти слабкі місця в системі захисту та вживати відповідні заходи для їх усунення. Аудити повинні включати як технічні аспекти, так і аналіз політик безпеки, процедур та прав доступу, що гарантує всебічну перевірку захищеності організації. Крім того, регулярне тестування на проникнення дає змогу перевірити стійкість інфраструктури до атак, що використовують новітні методи та технології. Всі виявлені вразливості повинні бути оперативно виправлені, а результати аудиту – використовуватись для оновлення стратегій безпеки та усунення потенційних загроз у майбутньому.

Особливу увагу слід приділяти захисту даних, що зберігаються в хмарних середовищах. Використання хмарних сервісів потребує ретельного вибору провайдера та забезпечення відповідного рівня безпеки даних, включаючи шифрування, контроль доступу та резервне копіювання. Оскільки хмарні сервіси надають високу гнучкість та масштабованість, це також створює нові виклики щодо управління конфіденційністю та безпекою даних. Важливо встановити чіткі політики управління доступом до чутливої інформації, визначити, хто має доступ до яких даних, та забезпечити їх постійну охорону через багатоетапне шифрування. Крім того, необхідно гарантувати надійне резервне копіювання та відновлення даних у разі їх втрати або компрометації, а також дотримання нормативно-правових вимог та стандартів безпеки, встановлених для хмарних сервісів.

Отже, архітектура надійного технічного захисту інформації є критично важливим елементом забезпечення стабільного та безпечного функціонування будь-якої організації в сучасному цифровому середовищі. Її побудова вимагає комплексного підходу, що базується на фундаментальних принципах, таких як мінімізація привілеїв, глибокий захист, розділення обов’язків, відмовостійкість, адаптивність та масштабованість.

Вибір оптимальної моделі архітектури ТЗІ (захищений контур, сегментована мережа, Zero Trust, хмарна архітектура безпеки) залежить від специфічних потреб організації, оцінки ризиків, наявних ресурсів та характеристик інформаційних активів.

Реалізація надійної архітектури ТЗІ потребує застосування різноманітних механізмів, включаючи автентифікацію та авторизацію, захист мережевої інфраструктури, захист даних, моніторинг безпеки та реагування на інциденти.

Успішне впровадження та підтримка ефективної архітектури ТЗІ вимагають наявності кваліфікованого персоналу, достатніх ресурсів, постійного моніторингу, регулярного аудиту безпеки, а також навчання та підвищення обізнаності персоналу щодо правил інформаційної безпеки. Організації, які приділяють достатню увагу ТЗІ, можуть значно зменшити ризик кібератак, захистити свої інформаційні активи та забезпечити безперервність бізнес-процесів.

Список використаних джерел

1. Черненко Р.М. Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей: дис. ... д-ра філософії / Р.М. Черненко. – Київ: Київський столичний університет імені Бориса Грінченка, 2024. – 200 с.
2. Гільгурт С.Я., Чемерис О.А. Реконфігуровні сигнатурні засоби захисту інформації комп’ютерних систем: монографія / С.Я. Гільгурт, О.А. Чемерис. – Київ: Академперіодика, 2022. – 297 с.
3. Жеребко О.В. Методи фізичного захисту інформації в інформаційно-комунікаційних системах: дипломна робота магістра / О.В. Жеребко. – Київ: Національний авіаційний університет, 2024. – 122 с.
4. Ковальчук І. Принципи проектування захищених інформаційних систем // Матеріали VI Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання». – Тернопіль: ТНТУ, 2023. – С. 152–153.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

5. Руденко В.М. Засоби удосконалення комплексу технічного захисту інформації: пояснювальна записка кваліфікаційної роботи / В.М. Руденко. – Київ: Київський національний університет імені Тараса Шевченка, 2023. – 76 с.

6. Закаржевський А. Методологія побудови захищених інфокомунікаційних мереж спеціального призначення на базі каналів загального доступу // *Інформаційні та комунікаційні технології, електроніка та електротехніка*. – 2023. – Вип. 3, № 2. – С. 53–63.

7. Поповський В.В., Лемешко О.В., Ковальчук В.К., Плотніков М.Д., Картушин Ю.П. Телекомунікаційні системи та мережі. Структура й основні функції: монографія / В.В. Поповський, О.В. Лемешко, В.К. Ковальчук, М.Д. Плотніков, Ю.П. Картушин. – Харків: ХНУРЕ, 2018. – 564 с.

8. Кучук Г.А. Інформаційні технології управління інтегральними потоками даних в інформаційно-телекомунікаційних мережах систем критичного призначення: монографія / Г.А. Кучук. – Харків: ХУПС, 2013. – 264 с.

9. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: підручник / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – Київ: САММІТ-Книга, 2010. – 708 с.

10. Медхі Д., Рамасамі К. Маршрутизація в мережах: алгоритми, протоколи та архітектури / Д. Медхі, К. Рамасамі. – Амстердам: Morgan Kaufmann Publishers, 2007. – 788 с.

11. Математичні основи теорії телекомунікаційних систем / за ред. В.В. Поповського. – Харків: СМІТ, 2006. – 564 с.

12. Вуд Ч.К. Комп’ютерна безпека: комплексний контрольний перелік елементів / Ч.К. Вуд. – Лондон: Комп’ютери і безпека, 2015. – 320 с.

13. Бріл А.Е. Вбудовування засобів керування в структуровані інформаційні системи / А.Е. Бріл. – Нью-Йорк: Yourdon Press, 2016. – 290 с.

14. Кропаткін Ф., Куссеров Р.П. Принципи управління для захисту активів / Ф. Кропаткін, Р.П. Куссеров. – Нью-Йорк: Yourdon Press, 2015. – 310 с.

15. Макбет С. Самоорганізуюче управління даними та знаннями, створеними користувачами / С. Макбет. – IEEE Communications, 2018. – Т. 30, № 3. – С. 237–264.

Роботу виконано під науковим керівництвом PhD, старшого викладача
ШЕСТАКА Я. І.

Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Електронне наукове видання

ПРОГРАМУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ

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

Частина 2

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
252Е-2025