Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет інформаційно-аналітичних технологій та менеджменту
(повна назва)

Кафедра прикладної математики
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Провадження механізмів захисту від кібератак
та зловживань у Web-сервісах
(тема)

Виконав:
здобувач 2 року навчання, групи ПМм-23-2
Бородавка В.В.
(прізвище, ініціали)
Спеціальність
113 Прикладна математика
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма
Прикладна математика
(повна назва освітньої програми)
Керівник доц. Бринза Н.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ПМ _____ Сидоров М.В.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет інформаційно-аналітичних технологій та менеджменту
Кафедра прикладної математики
Рівень вищої освіти другий (магістерський)
Спеціальність 113 Прикладна математика
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Прикладна математика
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ПМ _____
(підпис)
“ 25 ” листопада 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Бородавці Владиславу Вячеславовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Провадження механізмів захисту від кібератак та зловживань у Web-сервісах

затверджена наказом по університету від 22 листопада 2024 р. № 1223 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 6 січня 2025 р.

3. Вихідні дані до роботи статистичні, технічні, аналітичні та емпіричні дані, які слугують основою для розробки, впровадження та оцінки ефективності механізмів захисту від кібератак у web-сервісах та системах управління інформаційною безпекою в блокчейні

4. Перелік питань, що потрібно опрацювати в роботі
1. Аналіз предметної області
2. Вибір і обґрунтування методу розв’язання
3. Програмна реалізація
4. Результати обчислювального експерименту
5. Аналіз можливих застосувань

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

1. Актуальність теми роботи
2. Постановка задачі
3. Аналіз предметної області
4. Метод чисельного аналізу
5. Результати обчислювального експерименту

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Підбір та вивчення технічної літератури за темою роботи	25 листопада – 1 грудня 2024 р.	виконано
2	Вибір та обґрунтування методу	2 – 8 грудня 2024 р.	виконано
3	Розробка алгоритму і програми	9 – 22 грудня 2024 р.	виконано
4	Проведення аналітичних досліджень та розрахунків	23 – 29 грудня 2024 р.	виконано
5	Робота над текстом пояснювальної записки	30 грудня 2024 р. – 9 січня 2025 р.	виконано
6	Представлення роботи на рецензію в ЕК	10 січня 2025 р.	виконано

Дата видачі завдання 25 листопада 2024 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Бринза Н.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 113 с., 5 табл., 15 рис., 2 дод., 46 джерел.

WEB-СЕРВІС, БЛОКЧЕЙН, МЕРЕЖА, КІБЕРЗАХИСТ, КІБЕРАТАКА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, МЕХАНІЗМ ЗАХИСТУ, ЕФЕКТИВНІСТЬ, КОМПЛЕКС ЗАХОДІВ.

Об’єкт дослідження – процеси функціонування, розробки, розвитку та впровадження механізмів захисту web-сервісів від кібератак та зловживань, які використовуються для надання різноманітних онлайн-послуг та ресурсів, зокрема методи захисту, що реалізовані за допомогою інструментів фільтрації трафіку, таких як iptables, ipset, fail2ban, та динамічних чорних списків IP-адрес. Основна увага приділяється захисту web-сервісів, побудованих на основі систем управління інформаційною безпекою в блокчейн-мережах.

Мета роботи – розробка та впровадження ефективних механізмів захисту від кібератак та зловживань у web-сервісах. Для досягнення мети проводиться аналіз існуючих рішень, обґрунтовується вибір методів для покращення безпеки, а також розробляється програмна реалізація захисних механізмів та проводиться обчислювальний експеримент для перевірки ефективності.

У роботі використано методи математичного та системного аналізу та порівняння існуючих рішень для захисту web-сервісів від атак на основі блокування та фільтрації небезпечного трафіку. Технічні рішення реалізовані за допомогою налаштування та конфігурації iptables, ipset, fail2ban для створення динамічних чорних списків IP-адрес. Крім того, проведено експериментальне тестування розробленої системи на реальних даних трафіку web-сервісів.

Основним результатом дослідження є впровадження нової стратегії захисту web-сервісів за допомогою поєднання стандартних інструментів фільтрації iptables та ipset з автоматизованою системою реагування на підозрілу активність fail2ban. Новизна роботи полягає в інтеграції цих рішень з блокчейн-

системами, що дозволяє автоматично оновлювати та адаптувати захист у відповідь на поточні загрози. Запропонована система забезпечує виявлення та блокування підозрілих IP-адрес в режимі реального часу.

Результати дослідження рекомендується застосовувати для покращення захисту web-сервісів, що працюють у рамках блокчейн-інфраструктур або мають підвищену загрозу до зловживань і кібератак, зокрема розподілені атаки на відмову в обслуговуванні та brute force. Запропоновані рішення можуть бути інтегровані в існуючі системи управління інформаційною безпекою для підвищення їх ефективності та автоматизації процесів кіберзахисту.

Запропоновані механізми захисту можуть бути застосовані в різних галузях, де використовуються web-сервіси, особливо в фінансових та банківських системах, блокчейн-платформах, системах електронної комерції та в державних установах, що потребують надійного захисту від кібератак. Додатково, технології можуть бути інтегровані в Інтернет речей та інші мережі, де існує потреба у фільтрації трафіку та автоматизації захисних процесів.

Робота є важливою для сучасної кібербезпеки, оскільки вона пропонує інтегровані рішення для захисту web-сервісів від актуальних загроз у реальному часі. Використання динамічних чорних списків IP-адрес у поєднанні з fail2ban дозволяє створювати адаптивні системи захисту, які можуть ефективно протистояти кібератакам, мінімізуючи кількість помилкових блокувань. Це особливо актуально для великих організацій, які постійно стикаються з різними типами загроз.

Запропоновані механізми захисту довели свою ефективність у тестових умовах. У подальшому дослідження можна сфокусувати на підвищенні продуктивності запропонованих рішень для високонавантажених систем, а також на адаптації механізмів захисту до нових типів атак, таких як атаки на основі штучного інтелекту. Також доцільно розглянути можливість інтеграції запропонованої системи зі штучним інтелектом і машинним навчанням, а також з хмарними сервісами платформами для забезпечення масштабованості та гнучкості у використанні.

ABSTRACT

Introductory note: 113 pages, 5 tables, 15 figures, 2 appendixes, 46 sources.

WEB SERVICE, BLOCKCHAIN, NETWORK, CYBER SECURITY, CYBER ATTACK, INFORMATION SECURITY MANAGEMENT SYSTEM, PROTECTION MECHANISM, PERFORMANCE, RANGE OF MEASURES.

The object of research is the processes of operation, development, design and implementation of mechanisms for protecting web-services from cyberattacks and abuse, which are used to provide various online services and resources, in particular, protection methods implemented using traffic filtering tools as iptables, ipset, fail2ban, and dynamic IP blacklists. The focus is on protecting web services built based on information security management systems in blockchain networks.

The purpose of the work is to develop and implement effective mechanisms to protect against cyberattacks and abuse of web-services. To achieve this goal, analysis of existing solutions is carried out, the choice of methods for improving security is justified, and a software implementation of protective mechanisms is developed, and a simulation experiment is conducted to test the effectiveness.

The research uses the methods of system analysis and comparison of existing solutions for protecting web services from attacks based on blocking and filtering malicious traffic. The technical solutions are implemented by setting up and configuring iptables, ipset, fail2ban and creating dynamic blacklists of IP addresses. In addition, the developed system was experimentally tested on real data of web-services traffic.

The main result of the research is the implementation of a new strategy for protecting web-services by combining standard filtering tools iptables and ipset with the automated fail2ban system for reacting to suspicious activity. The innovation of the work is the integration of these solutions with blockchain systems, which allows for automatic updates and adaptation of protection in response to current threats. The proposed system provides real-time detection and blocking of suspicious IP addresses.

The results of the research are recommended to be used to improve the protection of web-services operating within blockchain infrastructures or that are at increased risk of abuse and cyberattacks, including distributed denial-of-service and brute force attacks. The proposed solutions can be integrated into existing information security management systems to increase their efficiency and automate cybersecurity processes.

The proposed protection mechanisms can be applied in various industries where web services are used, especially in financial and banking systems, blockchain platforms, e-commerce systems, and government agencies that need reliable protection against cyberattacks. Additionally, the technologies can be integrated into the Internet of Things and other networks where there is a need to filter traffic and automate security processes.

The work is important for modern cybersecurity because it offers integrated solutions to protect web-services from current threats in real time. The use of dynamic IP blacklists in combination with fail2ban allows creating adaptive protection systems that can effectively resist cyberattacks while minimizing the number of false blockings. This is especially important for large organizations that constantly experience different types of threats.

The proposed protection mechanisms have proven to be effective in test situations. Further research can be focused on improving the performance of the proposed solutions for high-load systems, as well as on adapting the protection mechanisms to new types of attacks, such as artificial intelligence-based attacks. It is also advisable to consider the possibility of integrating the proposed system with artificial intelligence and machine learning, as well as with cloud services platforms to ensure scalability and flexibility in use.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ІТ – інформаційні технології;

КА – кібератаки;

ІБ – інформаційна безпека;

ІС – інформаційна система;

СУІБ – система управління інформаційною безпекою;

БД – база даних;

DoS – Denial of Service;

DDoS – Distributed Denial of Service;

IP – Internet Protocol;

ETC – Ethereum Classic;

PoW – Proof of Work;

PoS – Proof of Stake;

SIEM – Security Information and Event Management;

DMZ – Demilitarized Zone;

VPN – Virtual Private Network;

IDS / IPS – Intrusion Detection Systems and Intrusion Prevention Systems;

SQL – Structured Query Language;

DPoS – Delegated Proof of Stake;

RSA – Rivest–Shamir–Adleman;

ECDSA – Elliptic Curve Digital Signature Algorithm;

SHA – Secure Hash Algorithms;

P2P – Peer-to-peer;

TLS – Transport Layer Security;

DHT – Distributed Hash Table;

LTS – Long-term support.

ВСТУП

Актуальність теми. Сучасні ІТ забезпечують глобальний доступ до ресурсів та сервісів, однак водночас створюють нові можливості для зловмисників, які використовують різноманітні способи для здійснення КА на web-сервіси. Атаки можуть спричинити серйозні наслідки, зокрема втрату конфіденційної інформації, збитки для бізнесу та порушення роботи сервісів. Тому забезпечення надійного захисту від таких атак є важливим завданням у сфері ІБ, а також у сфері системного аналізу для оцінки ефективності забезпечення безпеки.

Актуальність дослідження вразливостей web-сервісів та розробки методів їх усунення зумовлена стрімким зростанням кількості web-сервісів та їх значущості для бізнесу і суспільства. Зі збільшенням масштабів використання web-сервісів пропорційно зростає і кількість їх потенційних вразливостей. За статистикою, понад 60% усіх атак в Інтернеті здійснюються саме через вразливості web-сервісів. Зловмисники використовують такі недоліки для викрадення конфіденційної інформації, впровадження шкідливого програмного забезпечення або злочинного коду на сервери web-додатків. Наявність вразливостей web-сервісів створює передумови для реалізації різноманітних атак, таких як викрадення даних, модифікація інформації, розповсюдження шкідливих програм чи спаму. Наслідки цих дій можуть бути вкрай негативними для бізнесу, зокрема фінансові та репутаційні збитки, та втрата довіри клієнтів. Таким чином, виявлення та усунення вразливостей є важливими для забезпечення безпеки web-середовища, захисту конфіденційної інформації та стабільності функціонування web-сервісів. Наукові дослідження у цій галузі проводяться як в Україні, так і за кордоном. Серед українських вчених, які зробили вагомий внесок у дослідження вразливостей web-сервісів, можна відзначити Степановича В. Ю., професора кафедри програмної інженерії та ІТ Національного авіаційного університету, який спеціалізується на питаннях безпеки програмного забезпечення. Також важливі дослідження проводить Гуцало К. М., кандидат технічних наук, доцент

кафедри ІТ та захисту інформації Львівської політехніки. Серед зарубіжних фахівців у цій сфері слід згадати Джейсона Халперна, доцента кафедри інформаційної безпеки Нью-Йоркського технологічного інституту, та Хуана Хосе Переса, професора університету Ла-Ріоха (Іспанія), які досліджують питання кібербезпеки, зокрема виявлення й усунення вразливостей web-сервісів [1].

Таким чином, питання забезпечення безпеки web-сервісів є ключовим аспектом сучасної кібербезпеки, що вимагає систематичних досліджень та інноваційних підходів. Але у розглянутих наукових працях та публікаціях недостатньо уваги приділяється питанням та дослідженню алгоритмів реагування та відновлення після КА, також не висвітлюються можливості резервування та відновлення інфраструктури після КА, не здійснюється оцінка збитків внаслідок КА. Також немає жодного детального дослідження технічних деталей та механізмів роботи системи захисту від КА та використання різних видів зловмисного програмного забезпечення для атак. Тема є надзвичайно актуальною, і вона постійно вдосконалюється та розширюється відповідно до нових викликів та загроз у сфері ІБ та системного аналізу. А результати даної роботи дозволять запропонувати практичне рішення для підвищення рівня безпеки в ІС та, яке може бути адаптовано та масштабоване відповідно до потреб різних організацій. Адаптивність системи та можливість інтегрувати розвідку загроз у режимі реального часу підвищать її ефективність у протидії КА, що постійно еволюціонують.

Мета і завдання кваліфікаційної роботи. Метою кваліфікаційної роботи є дослідження існуючих механізмів захисту від КА у web-сервісах, розробка нових підходів до їх вдосконалення та впровадження ефективних рішень для забезпечення ІБ. Для досягнення поставленої мети необхідно виконати наступні завдання:

– провести огляд і аналіз сучасного стану задачі захисту web-сервісів від КА та зловживань в СУІБ в блокчейні;

– провести огляд і аналіз існуючих механізмів захисту від КА та зловживань в СУІБ в блокчейні;

– провести аналіз критеріїв вибору механізмів захисту від КА та зловживань в СУІБ в блокчейні;

– провести вибір та обґрунтування методів реалізації механізмів захисту від КА та зловживань в СУІБ в блокчейні;

– програмно реалізувати механізм захисту web-сервісів від КА.

Об'єктом дослідження є процеси функціонування, розробки, розвитку та впровадження механізмів захисту web-сервісів від КА та зловживань, які використовуються для надання різноманітних онлайн-послуг та ресурсів, зокрема методи захисту, що реалізовані за допомогою інструментів фільтрації трафіку, таких як iptables, ipset, fail2ban, та динамічних чорних списків IP-адрес. Основна увага приділяється захисту web-сервісів, побудованих на основі СУІБ в блокчейн-мережах.

Предметом дослідження є розробка механізму захисту від КА, зокрема методу виявлення загроз, їх запобіганню та мінімізації збитків від зловживань. Основна увага приділяється розробці та впровадженню нових технологій, які дозволяють знижувати ризики та підвищувати рівень безпеки web-сервісів.

Методи дослідження. У роботі використовуються методи системного аналізу для вивчення існуючих підходів до забезпечення безпеки, методи моделювання для аналізу КА та їх наслідків, а також методи експериментальних досліджень для тестування та вдосконалення механізмів захисту від КА.

Публікації. Результати, отримані у кваліфікаційній роботі, було представлено на ІІІ Міжнародній науково-практичній конференції «Навчання і викладання: у світі після війни»: Implementing protection mechanisms against cyberattacks in web services (м. Харків, 08 листопада квітня 2024 р.) [2].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

Сучасний розвиток ІТ став невід'ємною складовою життя суспільства. Інформація є одним із найцінніших ресурсів у будь-якому бізнес-процесі, що визначає пріоритетність забезпечення ІБ як ключового аспекту ефективного управління. ІБ включає сукупність заходів, спрямованих на попередження та усунення ризиків несанкціонованого доступу, обробки, модифікації, аналізу, неузгоджених змін або знищення даних. Це комплекс стандартів, методів, технологій та процедур, розроблених для забезпечення захисту конфіденційної інформації.

Проблема захисту інформації від несанкціонованого втручання виникла давно і набула особливої актуальності з розвитком суспільних відносин, появою приватної власності, формуванням державних інституцій та подальшою цифровізацією людської діяльності. З кожним етапом розвитку суспільства значення інформації зростає, що визначає актуальність дослідження обраної теми.

Дослідження теоретичних та практичних аспектів забезпечення ІБ активно здійснюється як вітчизняними, так і зарубіжними науковцями, зокрема Бабенко В., Бойко А., Васильєва Т., Гайдур Г., Гонтарева І., Грищук Р., Затонацька Т., Качинський А., Лєонов С., Кузьменко О., Маргасова В., Онищенко С., Полозова Т., Сороківська О., Хаустова В., Андерсона Р., Веня К., Гордона Л., Гупти М., Кардгольма Л., Кшетрі Н., Лі Дж., Лоєба М., Мура Т., Сінгха А., Сонні З., Стефанідеса Г., Столла М., Цякіса Т., Ши Ю. та інших. Останнім часом питання інформаційної політики та ІБ набуло особливої актуальності. Водночас варто зауважити, що завершення досліджень у цій сфері є малоймовірним через непередбачуваність та динамічний характер змін у бізнес-середовищі, постійний розвиток ІТ та їхній всеосяжний вплив на всі аспекти життєдіяльності суспільства.

Це зумовило наступну постановку мети дипломної роботи – дослідження існуючих механізмів захисту від КА у web-сервісах та в СУІБ в блокчейні, роз-

робка нових підходів до їх вдосконалення та впровадження ефективних рішень для забезпечення ІБ.

1.1 Актуальність та обґрунтування необхідності захисту від кібератак та зловживань в системах управління інформаційною безпекою в блокчейні

У сучасному світі розвиток ІТ є основою багатьох галузей економіки, зокрема фінансової, медичної, логістичної та інших. Однією з ключових технологій, що надають нові можливості для безпечного збереження та передачі інформації, є блокчейн. Ця технологія дозволяє забезпечити прозорість транзакцій, незмінність даних та децентралізовану модель управління, що робить її привабливою для багатьох галузей.

Технологія блокчейн є удосконаленим підходом до організації БД, який забезпечує відкритий обмін інформацією в межах бізнес-мережі. У блокчейні дані зберігаються у вигляді блоків, які утворюють зв’язаний ланцюжок. Інформація в блоках є хронологічно послідовною, оскільки будь-які зміни чи видалення даних неможливі без досягнення консенсусу між учасниками мережі. Завдяки цьому блокчейн можна застосовувати для створення незмінних реєстрів, які використовуються для відстеження замовлень, платежів, рахунків та інших транзакцій. Інформаційна система на основі блокчейну має вбудовані механізми, що запобігають несанкціонованому додаванню транзакцій і забезпечують узгодженість даних у загальному реєстрі [3]. Схематичне зображення структури блокчейну подано на рисунку 1.1.

Варто зазначити, що блокчейн суттєво відрізняється від традиційних баз даних. Він є унікальною системою управління даними, яка має низку розширених можливостей. Основною відмінністю є децентралізований характер управління, який забезпечує довіру до даних без необхідності централізованого контролю. У традиційних БД зазвичай відсутня можливість спільного використання

даних різними компаніями. У блокчейн-мережах кожен учасник має власну копію реєстру, відповідність якої підтримується автоматично. Крім того, у традиційних БД дані можуть бути редаговані або видалені, тоді як у блокчейні внесені дані залишаються незмінними, оскільки система забезпечує високий рівень їх захисту. Як тільки інформація записується до блокчейну, її модифікація стає надзвичайно складною, що підвищує надійність і безпеку збережених даних [4].

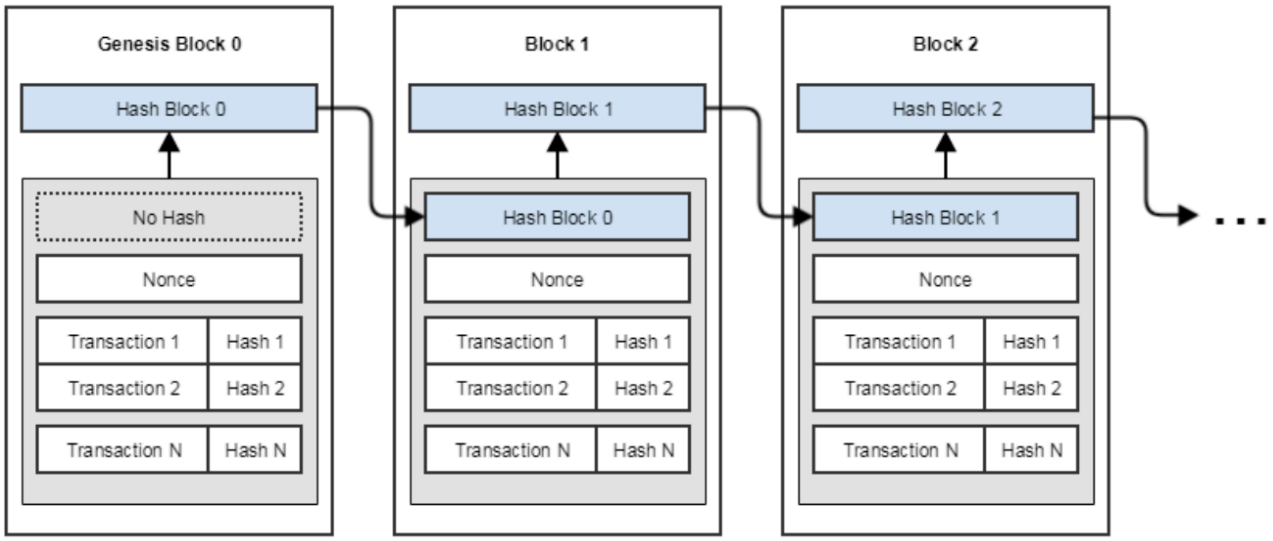


Рисунок 1.1 – Структура блокчейну

Децентралізація в технології блокчейн передбачає передачу контролю та ухвалення рішень від централізованих суб'єктів (окремих осіб, організацій або їхніх груп) до розподіленої мережі. Прозорість децентралізованих блокчейн-систем дозволяє зменшити залежність учасників один від одного, нівелюючи необхідність довіри між ними. Така архітектура обмежує можливість однієї сторони мати надмірний вплив чи контроль, зберігаючи при цьому функціональність мережі. Незмінність даних є ключовою характеристикою блокчейну, що унеможливлює зміну інформації після її внесення до реєстру. У разі помилок у записах для їх корекції додається нова транзакція, при цьому всі попередні транзакції залишаються доступними для перегляду в історії змін. Таким чином, мережа відображає як початковий, так і коригуючий запис. Для підтвердження нових транзакцій система використовує механізми консенсусу, що забезпечу-

ють їх реєстрацію лише за умови схвалення більшістю учасників.

Традиційні БД створюють низку труднощів при веденні обліку фінансових операцій. Наприклад, у випадку продажу нерухомості право власності переходить покупцеві лише після здійснення платежу. Однак сторони можуть окремо реєструвати транзакції, що створює ризики недовіри: продавець може заперечувати отримання коштів, а покупець стверджувати про здійснення платежу, навіть якщо це не відповідає дійсності. Для уникнення подібних суперечок зазвичай залучають довірену третю сторону, яка контролює та підтверджує угоду. Проте централізований посередник ускладнює процес, створюючи єдину точку уразливості, що може призвести до серйозних наслідків для обох сторін у разі порушення функціонування системи. Технологія блокчейн пропонує ефективне вирішення цих проблем через створення децентралізованої, захищеної від несанкціонованого втручання системи для фіксації операцій. У разі угоди з нерухомістю блокчейн забезпечує наявність єдиного реєстру, який синхронізується між покупцем і продавцем у режимі реального часу. Усі транзакції мають бути взаємно схвалені, а будь-які невідповідності у записах миттєво відображаються у всій системі, що підвищує прозорість і довіру до даних. Завдяки своїм властивостям технологія блокчейн здобула широку популярність у різних галузях. Одним із найвідоміших прикладів її застосування є створення цифрової валюти Bitcoin.

Однак, разом із зростанням популярності блокчейну виникають нові виклики у сфері ІБ. Блокчейн, як і будь-яка інша цифрова ІС, стає об’єктом КА і зловживань. Хоча децентралізована природа блокчейну забезпечує певний рівень захисту, вона не є повністю захищеною від різноманітних загроз. Вразливості можуть існувати як на рівні програмного забезпечення, так і на рівні механізмів управління доступом, криптографічних протоколів та мережевої інфраструктури.

Однією з найбільш серйозних загроз є атаки типу «51%», коли зловмисники отримують контроль над більшістю обчислювальних потужностей в мережі блокчейн, що дозволяє їм змінювати транзакції або навіть створювати ду-

блікати цифрових активів. Інші загрози включають фішинг-атаки, злом смарт-контрактів та експлуатацію вразливостей криптографічних алгоритмів. Незахищеність СУІБ може призвести до витоку критичних даних, порушення конфіденційності та значних фінансових втрат.

З огляду на постійний розвиток КА, важливо забезпечити надійні механізми захисту в СУІБ для блокчейну. Це включає в себе постійний моніторинг мережевої активності, впровадження сучасних криптографічних рішень, створення багаторівневих систем автентифікації, а також регулярне оновлення і покращення програмного забезпечення. Зловмисники постійно шукають нові способи обходу захисту, тому актуальність розвитку захисних механізмів в блокчейн-системах залишається на високому рівні. Таким чином, захист від КА та зловживань у блокчейні є важливою складовою для забезпечення надійної роботи систем на основі цієї технології. СУІБ мають постійно адаптуватися до нових викликів, що виникають у кіберпросторі, для збереження високого рівня захисту даних та мінімізації ризиків.

1.2 Аналіз існуючих механізмів захисту від кібератак та зловживань в системах управління інформаційною безпекою в блокчейні

Блокчейн – це неперервний ланцюг з блоків в яких записана інформація, ці блоки створюються постійно з деяким інтервалом. А також в кожному блокові, орім самого першого, є інформація про попередній блок. Якщо це блокчейн, наприклад, криптовалюти Bitcoin, то інформація в блоках буде про транзакції та інші дії з цією криптовалютою. Зв’язок між блоками в блокчейні забезпечується не лише їхньою послідовною нумерацією, але й використанням хеш-сум. Кожен блок містить власну хеш-суму та хеш-суму попереднього блоку, що гарантує цілісність та послідовність ланцюжка. Зміна будь-якої інформації в блоці призводить до зміни його хеш-суми. Для збереження відповідності правилам побудови блокчейн-ланцюжка зміна хеш-суми потребуватиме оно-

влення наступного блоку, що своєю чергою викличе зміну його хеш-суми. У такому випадку попередні блоки залишаються незмінними. Якщо модифікація стосується останнього блоку в ланцюжку, внесення змін може бути відносно простим завданням. Проте, якщо після зміненого блоку вже сформовані наступні блоки, зміна стає надзвичайно трудомістким процесом. Копії блокчейн-ланцюжків зберігаються на багатьох незалежних комп'ютерах, що підвищує стійкість системи до атак. Хоча існує чимало способів атак на блокчейн, спільною рисою таких нападів є те, що чим більше ресурсів зловмисник прагне отримати, тим більше зусиль він має витратити. В результаті, один зловмисник зазвичай не здатний досягти значного успіху, оскільки витрати на атаку переважують потенційну вигоду. Мережа блокчейн складається з вузлів, які виконують різні функції, такі як створення та обробка транзакцій чи надання інших послуг. Наприклад, у мережі Bitcoin вузли забезпечують відправлення та отримання транзакцій, тоді як майнери додають схвалені транзакції до блоків. Кіберзлочинці намагаються виявити вразливості мережі й експлуатувати їх через різні типи атак [5].

Однією з найбільш відомих атак є атака 51%, яка виникає, коли зловмисник отримує контроль над більшістю обчислювальних ресурсів мережі блокчейну, що дозволяє йому маніпулювати транзакціями та порушувати цілісність ланцюжка. Це дозволяє йому контролювати більше 50% майнінгових потужностей і добувати нові блоки швидше за інших учасників. Така перевага дає змогу зловмисникам зупиняти або змінювати порядок підтвердження транзакцій, а також редагувати частини блокчейну і скасовувати вже проведені транзакції [6]. Атака 51% зазвичай порушує протоколи безпеки блокчейну, а її наслідки можуть варіюватися від незначних до дуже серйозних, залежно від обсягу хеш-потужності, що контролює зловмисник. Чим більше обчислювальних ресурсів зловмисник контролює, тим більша ймовірність успішної атаки і більш серйозних збитків [7]. Контролюючи понад 51% потужностей, зловмисник може таємно створювати альтернативні блоки, які будуть вважатися дійсними через домінуючу потужність. Це дозволяє йому скасувати транзакції до їх підтвердже-

ня, що призводить до подвійного витрачання монет. Окрім цього, легальні майнери заробляють менше через те, що зловмисники забирають їхні частки прибутку від оновлення блокчейну. Деякі майнери, збільшуючи свої обчислювальні потужності, можуть ненароком перейти межу в 50% загальної потужності мережі, але це не становить загрози, якщо вони дотримуються правил і не заважають нормальній роботі системи [8]. Проте, якщо учасник використовує свою перевагу для нечесних дій, це вже можна вважати атакою.

Атака Фінні є різновидом «подвійного витрачання», коли угода підтверджується лише одним підтвердженням транзакції [9]. У цьому випадку зловмисник створює транзакцію для оплати товару, паралельно готуючи блок із транзакцією, яка переводить ці кошти на інший власний рахунок, але цей блок не публікує. Як тільки транзакція з оплатою підтверджується одним з майнерів, і товар отримано, зловмисник швидко оприлюднює підготовлений блок. У результаті в мережі утворюються дві блокчейн-гілки однакової довжини. Якщо майнери почнуть підтримувати ту гілку, яка містить транзакцію на рахунок зловмисника, то транзакція, яка передбачала переказ коштів продавцю, буде скасована, і продавець втрачає гроші, оскільки товар уже відправлений [7]. Для захисту від цієї атаки продавець може дочекатися кількох підтверджень транзакції, що знижує ризик, але не гарантує повної безпеки. Якщо зловмисник контролює кілька вузлів мережі, а продавець не чекає достатньої кількості підтверджень, зловмисник може створити довший ланцюжок із транзакцією на свій рахунок. Після публікації цього ланцюжка майнери продовжать працювати з ним, підтримуючи блок з транзакцією на користь зловмисника. Якщо ж обидва ланцюжки мають однакову довжину, майнери повинні вибрати один із них, і в такому випадку ймовірність успіху атаки становитиме 50%.

Атака типу «гонка» або Race Attack відбувається, коли зловмисник здійснює дві транзакції одночасно: транзакцію «А» для оплати покупки та транзакцію «В», яка переводить ті ж кошти на інший свій рахунок. Якщо продавець не чекає підтвердження транзакції й відправляє товар одразу, він ризикує: з 50% ймовірністю транзакція «В» може бути включена в блокчейн без додаткових

дій зловмисника [10]. Ще гірше, зловмисник може збільшити ймовірність успіху атаки, обираючи конкретні вузли для передачі тієї чи іншої транзакції. Принцип цієї атаки схожий на атаку Фінні і також є формою «подвійного витрачання».

Розподілені атаки відмови в обслуговуванні або DDoS хоч і складні у виконанні в умовах блокчейн-мережі, проте залишаються можливими. У разі DDoS-атаки зловмисники прагнуть вивести сервер з ладу шляхом перевантаження його великою кількістю запитів, що призводить до виснаження його обчислювальних ресурсів. Основною метою таких атак є дестабілізація функціонування майнінгових пулів, електронних гаманців, криптовалютних бірж та інших фінансових сервісів. Крім того, блокчейн може бути атакований на прикладному рівні за допомогою DDoS-ботнетів, які здійснюють масовані запити для ускладнення роботи мережі.

Timejacking експлуатує потенційну вразливість у способі обробки часових позначок в мережі Bitcoin. Під час цієї атаки зловмисник змінює часові налаштування вузла, змушуючи його прийняти альтернативний блокчейн. Це можливо, коли зловмисник додає в мережу кілька фальшивих однорангових вузлів із некоректними часовими позначками [11]. Захиститися від такої атаки можна, обмеживши діапазон прийнятних часових значень або використовуючи системний час самого вузла. Значення тимчасової мітки блоку перевіряється не щодо системного часу вузла, а на основі середнього часу його сусідніх вузлів, так званого часу мережі. Час мережі визначається, коли встановлюється нове з’єднання, вузли обмінюються своїми системними часами. Потім кожен вузол обчислює різницю між своїм системним часом і часом сусідів, і з цих відхилень вибирається медіанне значення. Таким чином, системний час вузла плюс медіанне відхилення дорівнює часу мережі. Зловмисник може спотворювати час мережі жертви, підключаючи до неї достатню кількість вузлів, що надсилають системний час, який суттєво відстає. Це призводить до зменшення часу мережі жертви та, відповідно, зниження верхньої межі допустимих значень тимчасових міток блоків для верифікації. Однак, якщо відхилення часу сусіда перевищує 70

хвилин, його дані не враховуватимуться під час обчислення часу мережі. Отже, максимальне зменшення часу мережі для жертви обмежується 70 хвилинами.

Атака маршрутизації або Routing attacks відбувається, коли провайдер змінює напрямок Інтернет-трафіку, використовуючи фальшиві оголошення в системі маршрутизації Інтернету. За допомогою таких атак зловмисник може розділити мережу на два або більше окремих сегменти, які не мають між собою зв'язку. Це унеможливлює взаємодію вузлів з різних частин мережі, що призводить до створення паралельних блокчейнів. Після завершення атаки блоки, здобуті в меншій частині мережі, будуть відкинуті разом із відповідними транзакціями та прибутком майнерів. Також цю атаку можна використовувати для затримки передачі блоку до вузла-жертви на 20 хвилин, що дозволяє зловмиснику залишатися непоміченим [12]. Протягом цього часу жертва не отримує інформації про останній видобутий блок і відповідні транзакції. Наслідки такої атаки залежать від того, хто є жертвою. Якщо це торговець, він стає вразливим до атак з подвійним витрачанням. Якщо це майнер, його обчислювальні ресурси марно витрачаються. А у випадку, якщо жертва – звичайний вузол, він не може брати участь у поширенні останньої версії блокчейну, що впливає на його внесок у роботу мережі.

Атака типу «eclipse» передбачає, що зловмисник контролює значну кількість IP-адрес або використовує розподілену мережу ботнетів. Зловмисник змінює записи в таблиці «випробуваних» вузлів жертви та чекає, поки її вузол буде перезапущено [13]. Після перезапуску всі вихідні з'єднання вузла-жертви спрямовуються на IP-адреси, що контролюються зловмисником. Це призводить до того, що жертва не може отримати необхідні їй транзакції. На перший погляд, атака «eclipse» може здатися схожою на атаку Sybil, оскільки обидві включають поширення фальшивих ресурсів у мережі. Однак їхні кінцеві цілі відрізняються [14]. Під час атаки «eclipse» зловмисник намагається повністю ізолювати жертву, перенаправивши всі її з'єднання до вузлів, які він контролює. Зловмисник створює кільце з підконтрольних IP-адрес, до яких вузол жертви ймовірно підключиться після перезапуску системи. Перезапуск може бути примусовим (на-

приклад, через DDoS-атаку) або статися через інші фактори, які зловмисник може просто чекати.

Атака Sybil є загрозою для безпеки в онлайн-системах, коли одна особа намагається захопити контроль над мережею, створюючи кілька фальшивих облікових записів, вузлів або комп'ютерів. Простий приклад – це ситуація, коли одна людина заводить кілька акаунтів у соціальній мережі. У контексті криптовалют, це може бути ситуація, коли хтось запускає кілька вузлів у блокчейн-мережі одночасно. Назва «Sybil» з'явилася у зв'язку із випадком жінки на ім'я Sybil Dorsett, яка страждала на дисоціативний розлад особистості, також відомий як множинний розлад особистості [15].

Cryptojacking (криптоджекінг) – це один із видів кіберзагроз, що останніми роками набуває все більшого поширення [16]. Ця КА полягає у використанні обчислювальних ресурсів комп'ютера, мобільного телефону, планшета, ноутбука або сервера користувача для несанкціонованого майнінгу криптовалют без його згоди або відома. Основна мета криптоджекінгу – заробіток на криптовалюті за рахунок ресурсів інших людей чи організацій. Ця загроза набуває особливої актуальності у зв'язку з ростом популярності криптовалют, таких як Monero, Bitcoin, Ethereum та інших, а також через збільшення кількості пристроїв, підключених до Інтернету. Для зловмисників це можливість отримувати значні прибутки, використовуючи великі мережі заражених пристроїв для майнінгу [17]. Cryptojacking часто реалізується через приховані скрипти, вбудовані на web-сайти або мобільні додатки. Користувач, відвідуючи заражений web-сайт або завантажуючи скомпрометований додаток, несвідомо запускає процес майнінгу на своєму пристрої. Ресурси процесора та відеокарти використовуються для вирішення складних математичних задач, характерних для криптовалютних мереж, що веде до підвищеного споживання електроенергії та погіршення продуктивності пристроїв. У деяких випадках шкідливе програмне забезпечення може інсталюватися через фішингові атаки або використання вразливостей у програмному забезпеченні. Зловмисники таким чином можуть непомітно захоплювати контроль над пристроями, зокрема серверними система-

ми, що мають великі обчислювальні потужності. Це робить криптоджекінг особливо небезпечним для корпоративних мереж і хмарних платформ.

Усі технології, включно з блокчейном, мають потенційні вектори атак, які кіберзлочинці можуть використовувати для своєї вигоди. В криптовалютному світі однією з відомих є атака Vector 76 або Vector Attack 76. Це форма атаки з подвійним витрачанням, яка експлуатує незначну помилку в системі консенсусу Bitcoin. У результаті зловмисник може отримати кошти та завдати шкоди своїм жертвам [18]. Ця атака виконується, коли шахрайський майнер контролює дві повні мережі вузлів. Один із них (вузол А) він підключає безпосередньо до сервісу обміну, а інший (вузол В) з'єднує з іншими ключовими вузлами в блокчейн-мережі. Для успішного здійснення атаки зловмисник повинен відслідковувати передачу та поширення транзакцій через різні вузли, щоб знати, які з них першими передають операції, і таким чином правильно підключитися як до сервісу обміну, так і до ключових вузлів мережі.

Вразливість подвійного витрачання – це поширений метод атаки на блокчейн, що експлуатує процес перевірки транзакцій. Усі операції в блокчейні повинні пройти верифікацію користувачами для визнання їх дійсними, що займає певний час [19]. Зловмисники можуть скористатися цією затримкою, щоб обдурити систему і використати одні й ті ж монети або токени в кількох транзакціях. З цієї вразливості виникли й інші типи атак, згадані раніше [20]. На відміну від традиційних фінансових установ, блокчейн підтверджує транзакції тільки після досягнення консенсусу між усіма вузлами мережі. Поки блок із транзакцією не перевірений, операція вважається непідтвердженою. Однак процес верифікації займає певний час, що створює можливості для КА. Подібно до підробки грошей, подвійне витрачання призводить до інфляції, збільшуючи кількість дубльованої валюти, яка раніше не існувала. Це призводить до знецінення валюти по відношенню до інших валют чи товарів, знижує довіру користувачів і порушує нормальний обіг та зберігання активів.

Пилові атаки – нещодавно шахраї виявили, що користувачі криптовалют часто не звертають уваги на невеликі суми, які з'являються в їхніх гаманцях. В

результаті вони почали здійснювати так звані «пилові атаки», використовуючи велику кількість IP-адрес і надсилаючи їм кілька сатоші (крихітна частка Bitcoin, кожен Bitcoin складається зі 100 мільйонів сатоші). Після атаки на кілька адрес зловмисники переходять до комбінованого аналізу, щоб визначити, які з них можуть належати одному гаманцю [21]. Основною метою є встановлення зв'язку між атакованими адресами та відповідними компаніями або приватними особами. Якщо ця схема спрацьовує, зловмисники можуть використовувати отриману інформацію для своїх цілей, таких як фішингові атаки або кібервимагання.

Розглянемо приклади успішних атак на блокчейн-мережі та заходи, що були вжиті для їхнього запобігання. У невеликих блокчейн-мережах атаку 51% може здійснити навіть окремий майнер, тоді як у великих мережах із високими вимогами до обчислювальних потужностей це під силу лише великим майнінговим пулам. Наприклад, у 2014 році майнінговий пул GHash.IO досяг 55% обчислювальної потужності мережі Bitcoin. У той час, коли частка пулу досягла 30%, спільнота Bitcoin висловила серйозне занепокоєння, яке посилилося, коли цей показник перевищив критичний поріг у 51%. Представники GHash.IO запевнили, що не планують проводити атаку, оскільки зацікавлені у стабільному розвитку мережі. Вони тимчасово припинили реєстрацію нових учасників і зменшили свій пул до 40%. Незважаючи на ці заходи, до кінця року GHash.IO припинив своє існування. Ймовірною причиною, чому майнери не скористалися можливістю здійснити атаку, було усвідомлення її негативного впливу на ринкову вартість Bitcoin [21].

У 2016 році хакерська група під назвою «Команда 51» успішно атакувала дві криптовалюти на базі Ethereum – Shift і Krypton. В результаті було здійснено подвійне витрачання коштів і викрадено 22 000 монет через біржу Bittrex. Подібна ситуація трапилася 7 січня 2019 року, коли стало відомо про реорганізацію мережі ETC на блоці 10 904 146 із глибиною 3693 блоки, тому припустили, що це була атака подвійного витрачання. Зловмисник орендував обчислювальні потужності на суму 17,5 Bitcoin (192 000 доларів) і вивів 807 260 ETC

(5,6 млн доларів) на кілька гаманців, ймовірно, з біржової адреси. Подальші дії хакера полягали у переміщенні ETC між власними гаманцями та включенні транзакцій у здобуті блоки. Оскільки транзакції зберігалися лише у версії ланцюга, яка належала хакеру, їх було неможливо відстежити. Після конвертації викрадених активів зловмисник опублікував транзакції у блокчейні, що спричинило реорганізацію ланцюга [22].

У грудні 2019 року широкого розголосу набуло відео, яке демонструвало подвійне витрачання Bitcoin у місцях, що його приймають. Ці атаки стали можливими через функцію Replace-By-Fee, яка була включена в суперечливе оновлення протоколу Bitcoin. Схема полягала у надсиланні першої транзакції продавцю, а другої – з вищою комісією, яка замінювала першу. Це дозволяло зловмисникам здійснювати подвійне витрачання, адже продавці приймали непідтверджені транзакції. Подібний інцидент трапився раніше того ж року, коли канадські власники Bitcoin переводили криптовалюту в готівку, не здійснивши фактичного переказу коштів.

Атаки «eclipse» відомі з моменту виникнення перших однорангових мереж. У 2018 році було продемонстровано можливість атаки «eclipse» на мережу Ethereum. Зловмисники могли ізолювати окремий вузол Ethereum і контролювати всі з’єднання цього вузла. Це дозволяло їм впливати на інформацію, яку отримував вузол, та маніпулювати чергою транзакцій (mempool), затримуючи або зовсім не передаючи транзакції в мережу [7]. Атака була успішною завдяки використанню слабких місць у процесі формування з’єднань між вузлами. Зловмисники могли займати всі слоти з’єднань вузла, не дозволяючи йому підключитися до інших вузлів [13]. Вразливість було виправлено після того, як дослідники представили свої знахідки розробникам Ethereum [14]. Зараз ключовим фактором для запобігання атакам «eclipse» є надійний процес вибору однорангових вузлів для мережі. У Ethereum цей процес реалізовано за допомогою протоколу на базі Kademlia, що дозволяє зв’язувати елементи з ключами та зберігати лише в тих парах, чий ідентифікатор вузла близький до пов’язаного з ним ключа. У 2020 році було виявлено вразливість до «eclipse» атак у мережі Stellar,

яка є однією з провідних платформ для створення та передачі цифрових активів. Успішна КА дозволяла зловмисникам впливати на консенсусну мережу Stellar, ізолюючи вузли-учасники. Це дало можливість маніпулювати процесом підтвердження транзакцій і блоків. Ця КА також продемонструвала важливість удосконалення систем захисту вузлів у децентралізованих мережах, які використовують альтернативні механізми консенсусу, як-от Stellar Consensus Protocol.

У 2017 році біржа Bitfinex зазнала масової DDoS-атаки, що стало проблемою для IOTA Foundation, яка запустила свій токен за день до атаки. Через три роки, у лютому 2020 року, Bitfinex знову зазнав DDoS-атаки, лише через день після попередження про схожу атаку.

Coinhive був одним із найвідоміших сервісів для легального майнінгу криптовалюти Monero через web-браузери. Однак, зловмисники швидко почали використовувати цей скрипт для криптоджекінгу без згоди користувачів. Coinhive використовували на тисячах web-сайтів без відома власників або відвідувачів, що призвело до масштабних КА. Успішними жертвами таких КА стали сайти великих корпорацій, державні ресурси та навіть криптовалютні біржі. Coinhive було закрито в 2019 році через негативну репутацію, спричинену зловживанням їхнім продуктом. У лютому 2018 року виявили, що зловмисники отримали доступ до одного з хмарних облікових записів Tesla на Amazon Web Services і використовували сервери компанії для майнінгу криптовалюти. КА була виявлена командою RedLock, яка відзначила, що зловмисники використовували хмарні ресурси Tesla не для крадіжки даних, а для криптоджекінгу [23]. Ця атака показала, як навіть великі компанії можуть стати жертвами через неправильну конфігурацію хмарних ресурсів.

У 2018 році дослідники продемонстрували можливість Sybil-атаки на Whisper (протокол повідомлень у мережі Ethereum, що забезпечує децентралізовану передачу даних між учасниками мережі), створивши безліч підроблених вузлів, які брали участь у комунікації та могли контролювати потік повідомлень. Ця атака виявила слабкість у протоколі, яка полягала у відсутності належного захисту від численних псевдо-ідентичностей. У 2020 році проект Zilliqa,

що використовує шардінг для підвищення масштабованості, також став жертвою Sybil-атаки [15]. Хоча Zilliqa розроблено для децентралізованого виконання смарт-контрактів, зловмисники змогли зареєструвати декілька фальшивих вузлів і порушити процес обробки транзакцій у деяких шардових сегментах. Це поставило під загрозу процес консенсусу в окремих шардових групах. Щоб запобігти атакам Sybil, блокчейн використовує різні алгоритми консенсусу, такі як PoW і PoS, які збільшують вартість цих атак і роблять їх невигідними для потенційних зловмисників. Одне з правил полягає в тому, що можливість створення блоку повинна бути пропорційною загальній обчислювальній потужності механізму PoW, що ускладнює для зловмисників завдання отримання необхідної потужності для створення нового блоку.

У блокчейн-мережах немає довірених вузлів, тому кожен запит передається випадковій кількості вузлів. У разі атаки, жертву оточують фальшиві вузли, які блокують її транзакції, що в кінцевому підсумку відкриває можливості для подвійних витрат. На рисунку 1.2 зображено вузли блокчейн-мережі: помаранчевим кольором позначені вузли, контрольовані зловмисником, зеленим – вузол жертви атаки, а сірим – чесні вузли, які не знаходяться під контролем зловмисника.

Захист інформації в мережі блокчейн є критично важливим, оскільки помилки під час створення або налаштування такої мережі можуть призвести до серйозних проблем. Важливо правильно вибрати модифікації, панелі управління та налаштувати систему відповідно до поставлених цілей. Наприклад, блокчейн, призначений для криптовалюти, не підходить для організації внутрішніх ІС компанії.

Технології блокчейн з різними протоколами можуть забезпечити захист медичних, фінансових та інших персональних даних, водночас дозволяючи їх використання в додатках зі штучним інтелектом. Розглянемо децентралізований блокчейн, який активно використовується в криптовалютах. Переваги таких мереж полягають у відсутності контролю над політикою створення блоків, що дозволяє користувачам мати рівні права на запис та читання інформації, хо-

ча змінювати її вони можуть лише стосовно власних даних. Користувачі мають змогу вибирати, яку інформацію про них можуть бачити інші.

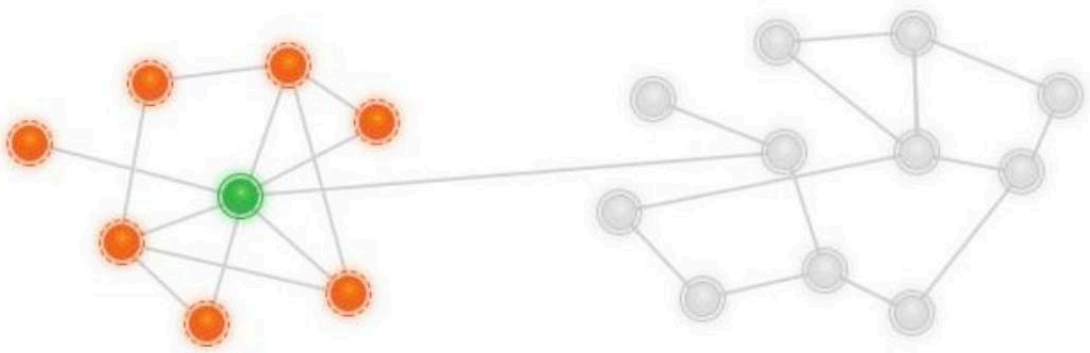


Рисунок 1.2 – Схема вузлів при атаці «Sybil»

Децентралізовані мережі підходять для державних установ або компаній, які мають угоди між собою, оскільки вони допомагають зменшити корупцію та підвищити довіру завдяки прозорості. У таких системах можна переглядати тільки інформацію про транзакції або дії установ. Наприклад, у земельній установі видно, хто придбав ділянку та за яку ціну. Рекомендується мати численні вузли для стабільної роботи мережі та обмежити кількість вузлів, які можуть створювати користувачі.

Користувачам таких мереж слід уважно стежити за тим, щоб їхня особиста інформація не розповсюджувалася. Також не варто користуватися послугами провайдерів, які присвоюють IP-адреси і відстежують дії користувачів, оскільки їхні дані можуть бути вразливими до витоків. Наприклад, для компаній, які прагнуть створити внутрішній блокчейн для моніторингу роботи співробітників, більш підходить централізована мережа, де є керівник, що контролює всі дії з блоками.

У централізованих мережах присутня ієрархія: лише деякі користувачі мають право додавати інформацію, тоді як інші можуть лише переглядати її. Необхідно також проводити регулярні тренінги для користувачів, щоб забезпечити дотримання вимог безпеки. У централізованих системах потрібно слідку-

вати за безпекою мережі, закриваючи її для зовнішніх користувачів.

Захищеність блокчейну залежить від багатьох факторів, і найважливішим є кількість вузлів у мережі: чим їх більше, тим вища безпека. Користувачі отримують два види ключів для шифрування та розшифрування даних, що гарантує їхню безпеку. Прозорість мережі дозволяє виявляти підозрілі зміни та транзакції. Атаки можуть бути спрямовані як на користувачів (наприклад, фішинг), так і на саму мережу.

Кібербезпека також може використовувати блокчейн для підвищення цілісності даних, оскільки в децентралізованій мережі зміни відбуваються лише після підтвердження інформації іншими учасниками. Технологія блокчейн має потенціал значно змінити світ, автоматизуючи численні процеси, що зазвичай займають багато часу, і зменшуючи потребу в зборі зайвої інформації про людей.

1.3 Критерії вибору механізмів захисту від кібератак та зловживань в системах управління інформаційною безпекою в блокчейні

В умовах постійно зростаючих загроз у кіберпросторі, вибір ефективних механізмів захисту для СУІБ в блокчейні стає критично важливим. Системи блокчейн, завдяки своїй децентралізованій природі, мають певні переваги у протидії КА, однак вони не є абсолютно захищеними.

У публікації [24] представлено основні методи виявлення КА, серед яких виділяються сигнатурний аналіз і методи виявлення аномалій. Розглянуто підходи, які можуть бути використані для ідентифікації вторгнень в ІС, а також способи оперативного реагування на такі загрози. Описано різноманітні засоби забезпечення кібербезпеки, зокрема технології систем виявлення та запобігання вторгнень (Intrusion Detection System / Intrusion Prevention System), антивірусне програмне забезпечення та мережеві екрани (файрволи). Проведено аналіз вразливостей ІС і надано рекомендації щодо побудови безпечної інфраструктури,

яка спрямована на запобігання КА і захист даних. Водночас у цій публікації не висвітлено алгоритми реагування на КА та процеси відновлення після них.

У роботі [25] досліджуються негативні наслідки КА на ІС, що є частиною критичної інфраструктури. Увага акцентується на впливі таких атак на системи, які мають важливе значення для функціонування держави, зокрема енергетичні мережі, транспортні системи та комунікаційну інфраструктуру. Проаналізовано потенційні вразливості в цих системах і проведено оцінку ризиків, пов'язаних із можливими КА. Разом із цим, у роботі не розглядаються аспекти відновлення та резервування інфраструктури після таких інцидентів.

У статті [26] детально досліджуються основи ІБ та методи захисту інформації в ІС. Наведено визначення ключових понять і принципів ІБ, а також проаналізовано загрози та ризики, пов'язані із забезпеченням захисту інформації. Особливу увагу приділено послідовності дій, які можуть бути реалізовані під час КА на об'єкти критичної інфраструктури, з метою аналізу їхніх наслідків і визначення типових сценаріїв атак. Описано також методи захисту інформації в хмарних обчислювальних середовищах, однак не розглядаються питання оцінки можливих фінансових та операційних втрат від таких атак.

У науковій роботі [27] розглянуто методи захисту мережевих елементів, зокрема маршрутизаторів, комутаторів і брандмауерів, від КА. Автори акцентують увагу на проблемах виявлення та реагування на кіберінциденти, підкреслюючи важливість використання систем управління інцидентами (SIEM). У праці наведено рекомендації щодо створення ефективних планів реагування на кіберінциденти та забезпечення відновлення функціонування після КА. Значна увага приділена питанням захисту інформації в хмарних обчислювальних середовищах, однак детальний аналіз технічних аспектів механізмів дії та використання шкідливого програмного забезпечення не проводиться.

У статті [28] досліджуються аспекти виявлення вторгнень на основі аномалій і пропонується модель системи виявлення вторгнень, що використовує нейронну мережу, побудовану на основі самоорганізованих карт. Такий підхід дозволяє підвищити ефективність і точність ідентифікації кіберзагроз.

У публікації [29] автори розглядають підходи до виявлення та аналізу КА, пропонуючи модель системи виявлення вторгнень, що використовує нейронну мережу з неконтрольованим глибинним навчанням, зокрема, мережу глибоких переконань (Deep Belief Network) для виявлення кіберінцидентів.

Аналізуючи зазначені вище наукові роботи, можна зробити висновок, що в них розглядаються важливі аспекти виявлення та протидії кіберзагрозам і КА, зокрема використання методів сигнатурного аналізу та виявлення аномалій. Однак ці підходи в умовах комбінованих атак можуть виявитися недостатньо ефективними. Також обговорюється використання моделей нейронних мереж з неконтрольованим глибинним навчанням для аналізу кіберінцидентів і виявлення вторгнень. Водночас, у наукових публікаціях не приділяється достатньо уваги дослідженню алгоритмів реагування та відновлення після кібератак, не розглядаються методи відновлення інфраструктури, а також відсутня оцінка збитків, завданих КА. Крім того, не проводиться детальний аналіз технічних аспектів механізмів роботи та використання різноманітних типів шкідливого програмного забезпечення.

Дослідження вразливостей і методів їх усунення в блокчейні є важливим кроком для забезпечення безпеки та захисту СУІБ. Це дає можливість виявити потенційні загрози та вчасно вжити заходів для їх усунення. Існує безліч методів тестування на вразливості, включаючи сканування, ручний аналіз та тестування на стійкість до зловмисних атак. Після виявлення вразливостей потрібно вжити заходів для їх усунення, що може включати розробку виправлень, налаштування правил безпеки, зміну параметрів сервера і бази даних, а також впровадження додаткових механізмів захисту. Статистичне дослідження поширених вразливостей web-сервісів допомагає з’ясувати, які з них трапляються найчастіше та які заходи слід вжити для їх усунення [30].

Для забезпечення безпеки СУІБ у блокчейні доцільно використовувати різноманітні методи, зокрема застосувати шифрування даних, реалізувати механізми контролю доступу до ресурсів, впровадити процедури перевірки вхідних даних, а також організувати постійний моніторинг активності. Незважаючи

на широкий спектр методів захисту, забезпечення повної безпеки СУІБ в блокчейні залишається складним завданням. Однією з основних проблем є швидкий розвиток нових атак. Зловмисники постійно вдосконалюють свої стратегії, створюючи нові шкідливі програми, здатні обійти існуючі системи захисту. Іншою проблемою є людський фактор: часто користувачі недостатньо усвідомлюють ризики або нехтують базовими правилами безпеки, що може призвести до обходу навіть найсучасніших систем захисту через ненадійні паролі чи інші помилки.

Існує два підходи до вирішення проблеми забезпечення безпеки СУІБ, а саме фрагментарний і комплексний [30, 31]. Фрагментарний підхід передбачає протидію конкретним загрозам у певних умовах. Прикладами такого підходу є використання систем контролю доступу, автономних засобів шифрування та спеціалізованих антивірусних програм. Основною перевагою цього підходу є його спрямованість на окремі загрози. Однак його недоліком є відсутність єдиної захищеної інформаційної системи. Фрагментарні заходи безпеки можуть бути ефективними лише для окремих елементів СУІБ, але незначні зміни в загрозах можуть знизити їхню дієвість. Комплексний підхід, у свою чергу, орієнтований на створення інтегрованого захищеного середовища для обробки інформації в СУІБ, об’єднуючи різні заходи протидії загрозам. Він включає різноманітні методи захисту. Створення такого середовища є перевагою комплексного підходу, оскільки забезпечує високий рівень безпеки. Однак серед його недоліків можна виділити обмеження дій користувачів, чутливість до помилок у налаштуванні засобів захисту та складність управління системою. Важливим елементом комплексного підходу є розробка ефективної політики безпеки, яка регулює роботу захисних засобів СУІБ і враховує всі аспекти обробки інформації. Без такої політики, що передбачає реакцію системи на різні ситуації та можливі загрози, неможливо створити надійну мережеву СУІБ в блокчейні.

Багаторівневий підхід до захисту СУІБ в блокчейні або Defense in Depth передбачає створення кількох послідовних захисних шарів, що використовують різні засоби контролю для досягнення максимального рівня безпеки, рисунок

1.3 [32]. Цей процес починається із зовнішнього рівня та поступово просувається до внутрішніх компонентів системи, аж до ядра – даних. На зовнішньому рівні реалізуються політики та процедури, що регулюють функціонування організації або мережі загалом, включаючи правила доступу, управління паролями та політики використання Інтернет-ресурсів. Наступний рівень забезпечує фізичну безпеку, яка включає використання засобів фізичного контролю, таких як персонал охорони або системи замків, для обмеження доступу до обладнання та приміщень. На подальшому рівні здійснюється захист мережевої інфраструктури від зовнішніх загроз шляхом впровадження таких технологій, як DMZ, VPN, регулярний аудит, тестування на проникнення та аналіз вразливостей.

Поглиблений захист передбачає контроль доступу, автентифікацію та використання інших механізмів для забезпечення безпеки внутрішніх ресурсів. Завершальний етап – захист окремих хостингів та даних за допомогою антивірусних програм, шифрування та файрволів, що забезпечують безпеку окремих ІС та інформації. Така багаторівнева стратегія мінімізує ризик успішних КА, оскільки порушення одного рівня захисту не гарантує доступ до інших. Використання різних технологій і заходів робить систему більш стійкою та надійною.

Рисунок 1.3 – Багаторівневий підхід до побудови системи захисту [14]

У таблиці 1.1 наведена класифікація загроз безпеки СУІБ в блокчейні

[32]. Методи ідентифікації кіберзагроз поділяються на дві ключові категорії: аналіз аномалій у мережевому трафіку та виявлення зловживань.

Таблиця 1.1 – Системна класифікація загроз безпеці

Параметри класифікації	Значення параметрів	Зміст значення параметрів
Види	Фізична цілісність Логічна структура Зміст Конфіденційність Право власності	Знищення (викривлення). Викривлення структури. Несанкціонована модифікація. Несанкціоноване отримання. Привласнення чужого права.
Природа походження	Випадкова Навмисна	Відмови, збої в роботі системи, помилки, стихійні лиха, побічні впливи. Злочинні дії людей.
Передумова появи	Об’єктивні Суб’єктивні	Кількісна недостатність елементів системи, якісна недостатність елементів системи. Розвідувальні органи іноземних держав, промисловий шпіонаж, кримінальні елементи, кіберзлочинні групи, недобросовісні співробітники.
Джерело загроз	Люди Технічні пристрої Моделі, алгоритми, програми Технологічні схеми обробки Зовнішнє середовище	Сторонні особи, користувачі, персонал. Реєстрації, передачі, зберігання, видачі. Загальні, прикладні, допоміжні. Ручні, інтерактивні, внутрішньо машинні, мережеві. Стан середовища (погодні умови та природні катаклізми, побічні шуми, по-бічні сигнали.

Процес визначення кіберзагроз передбачає попередній аналіз інцидентів, що базується на виявлених аномаліях або ознаках зловживань у мережевому

середовищі. Аналіз аномалій дозволяє виявляти суттєві відхилення в мережевому трафіку пристроїв від стандартного профілю їхньої діяльності. Такий профіль створюється на основі статистичних даних та навчальних вибірок, що накопичуються протягом певного періоду експлуатації мережі. Додатково, використання машинного навчання та алгоритмів аналізу даних забезпечує підвищення точності ідентифікації аномалій та зловживань. Ефективність цих методів значною мірою залежить від якості навчальних вибірок, обсягу зібраних даних та правильного налаштування алгоритмів аналізу. Окрім того, аналіз аномалій дозволяє виявляти як відомі, так і нові, невідомі раніше загрози, що підвищує загальний рівень безпеки ІС. Методи виявлення зловживань, у свою чергу, орієнтовані на ідентифікацію шкідливих дій, що відповідають відомим шаблонам або сигнатурам атак. Інтеграція цих підходів у комплексні системи кіберзахисту сприяє створенню багаторівневого захисту, здатного своєчасно реагувати на різноманітні види загроз.

Аналіз телеметричних даних дозволяє виявляти мережеві аномалії шляхом оцінювання ключових характеристик трафіку, без необхідності детального аналізу вмісту кожного пакету. Прикладом таких аномалій можуть слугувати раптове зростання обсягу трафіку з окремої робочої станції або зміни в структурі передачі даних. На рисунку 1.4 [32] представлено блок-схему процесу ідентифікації мережевих аномалій, заснованого на телеметричних даних. Помилки виявлення аномалій поділяються на два типи: хибно-позитивні спрацювання (помилки першого роду) та пропуски істотних подій (помилки другого роду). Зменшення рівня таких помилок потребує впровадження ефективних алгоритмів і точного налаштування системи моніторингу. Крім того, сучасні методи аналізу телеметрії використовують алгоритми машинного навчання, що дозволяє автоматизувати процеси ідентифікації аномалій та підвищити загальну ефективність системи кіберзахисту. Хибна тривога виникає, коли нормальні події помилково визначаються як аномальні, що може призвести до непотрібних дій. Пропуск події, своєю чергою, означає, що система не помічає дійсно аномальних подій, що становить загрозу безпеці.

Рисунок 1.4 – Блок-схема виявлення аномалій [14]

Метод виявлення зловживань у мережевому трафіку має перевагу, оскільки дозволяє ідентифікувати несанкціоновані дії, якщо відомий шаблон трафіку під час атаки [33]. Шаблон атаки є набором правил, що описують конкретну атаку та дозволяють однозначно визначити, чи належить подія до конкретної загрози. Існують значні виклики, пов’язані з ефективним проєктуванням механізмів для визначення правил та можливими труднощами, спричиненими їх великою кількістю. До того ж, цей метод може бути недостатньо дієвим при виявленні нових або модифікованих атак [34]. Для підвищення його ефективності необхідно мати універсальні правила, які охоплюють всі відомі шаблони атак. Важливо регулярно оновлювати ці правила у процесі виявлення нових зразків атак. Інакше система ризикує пропускати нові загрози, які не відповідають встановленим шаблонам.

На основі аналізу різних методів можна зробити висновок, що для забезпечення більш високого рівня захисту інформаційних ресурсів СУІБ в блокчейні доцільно використовувати методи, що базуються на виявленні аномалій, оскільки вони здатні ефективно ідентифікувати кіберзагрози, включно з атаками «нульового дня» (0-day). Основними інструментами захисту від таких загроз є антивірусне програмне забезпечення, яке протидіє шкідливим програмам, системи виявлення та запобігання вторгненням для моніторингу та блокування небажаних активностей, а також файрволи, які контролюють доступ до мере-

жевих ресурсів та захищають від несанкціонованого доступу. Таблиця 1.2 містить основні характеристики систем захисту від кіберзагроз, узагальнені на основі проведеного аналізу.

Таблиця 1.2 – Основні характеристики систем захисту від КА

Функції	Засоби захисту			
	Firewall	IDS/ IPS	Антивірусні програми	SIEM
Дані, що аналізуються	Мережевий трафік	Мережевий трафік	Мережевий трафік, Дані в операційній системі	Дані журналу
Механізм виявлення підозрілої активності	«Список контролю доступу» або Access control list, аналіз зловживань	Аналіз зловживань	Аналіз зловживань аналіз поведінки	Аналіз за прикладами попередніх інцидентів
Оновлення бази для розпізнавання нових загроз	Надається розробником	Надається розробником. Задається користувачем	Надається розробником	Задається користувачем на основі даних
Блокування загрози	Є	Немає	Є	Немає
Синтаксичний аналіз Parsing	Не є необхідним	Частково необхідний	Не є необхідним	Необхідний

Для виявлення та запобігання вторгненням використовуються системи IDS/IPS, причому IDS сповіщає про можливі загрози, а IPS блокує або призупиняє атаки, ґрунтуючись на заздалегідь встановлених правилах. SIEM системи

забезпечують реєстрацію та аналіз подій безпеки в режимі реального часу, відстежуючи активність пристроїв і користувачів, що дозволяє оперативно реагувати на загрози до того, як вони завдадуть шкоди. Програмне забезпечення SIEM збирає інформацію з різних джерел, таких як сервери, контролери доменів та файрволи, і надає її у вигляді звітів. Ці дані можуть використовуватися не лише для забезпечення безпеки, а й для покращення функціонування мережевої інфраструктури.

Головне завдання таких систем полягає в ідентифікації потенційних вразливостей у системі та локалізації наявних загроз. Ця інформація збирається та аналізується за допомогою журналів мережевих пристроїв. Після автоматичного збору даних система проводить класифікацію подій і надсилає сповіщення, якщо виявлені дії обладнання, програм або користувачів можуть бути потенційно небезпечними.

Наприклад, якщо система IDS/IPS виявляє мережеву КА на основі аномалії, автоматизована система може передати команду брандмауеру для блокування IP-адреси, з якої походить підозріла активність, використовуючи дані, отримані від IDS/IPS [35]. У разі, якщо виявлено підозрілу активність без точного підтвердження атаки, система автоматизації може активувати антивірусне програмне забезпечення для прийняття відповідних заходів. Такий підхід дозволяє забезпечити ефективний і скоординований захист, який охоплює різні загрози завдяки взаємодії та обміну інформацією між різними захисними засобами [36].

Розглядаючи концепцію побудови системи захисту від КА, можна запропонувати власну оцінку, яка архітектура – централізована, децентралізована або гібридна – є найбільш підходящою для реалізації цієї системи. Архітектура визначає структуру системи та принципи взаємодії її компонентів.

У централізованій архітектурі всі елементи зосереджені на єдиному сервері, що забезпечує простоту впровадження, але може обмежувати масштабованість і продуктивність, особливо для великих та складних ІКС. Натомість децентралізована архітектура передбачає розподіл компонентів між кількома сер-

верами, що підвищує масштабованість системи, але водночас ускладнює процеси адміністрування та інтеграції. Гібридна архітектура поєднує переваги обох підходів, використовуючи розподіл компонентів між серверами з централізованим управлінням, що дозволяє досягти балансу між ефективністю впровадження та гнучкістю масштабування. Крім того, вибір архітектури залежить від конкретних вимог до системи, таких як продуктивність, рівень безпеки та доступність ресурсів. Оптимальна архітектура також враховує потенційні ризики, пов'язані з кіберзагрозами, забезпечуючи стійкість системи до можливих атак. Гібридна архітектура є оптимальним рішенням для побудови системи захисту від КА, оскільки вона поєднує переваги як централізованого, так і децентралізованого підходів. Ефективність системи захисту можна оцінити за допомогою спеціальної формули [32]:

$$E = \frac{(M - N)}{(M + V + N)} * 100\% * (1 - B), \tag{1.1}$$

де E – ефективність системи;

M – кількість кібератак, виявлених і заблокованих системою;

N – кількість кібератак, попереджених системою;

V – кількість кібератак, які пройшли систему кіберзахисту;

B – відсоток помилкових спрацювань, що генерує система.

Вираз має сенс лише за умов: $M > N \; i \; B \in [0;1)$.

Атаки, про які система кіберзахисту інформує користувачів, є КА, що були виявлені, але не заблоковані в автоматичному режимі. Така система сповіщає про подібні загрози, надаючи користувачам можливість вжити необхідних заходів для їх нейтралізації. До прикладів таких атак належать фішинг, впровадження шкідливого програмного забезпечення чи несанкціоноване проникнення до мережі. Наприклад, система може попередити про фішингову активність шляхом виявлення підозрілих електронних листів або web-ресурсів, а також сигналізувати про наявність шкідливих програм через фіксацію нетипових проце-

сів або змін у файловій системі. Окрім цього, подібні системи можуть використовувати інтелектуальні алгоритми для аналізу поведінки мережевих пристроїв і користувачів, що дозволяє ідентифікувати нові, раніше невідомі загрози. Інтеграція таких функцій забезпечує проактивний підхід до захисту інформаційних систем, мінімізуючи ризики та скорочуючи час реагування на кіберінциденти.

Отже, аналізуючи переваги та недоліки методів виявлення зловживань і мережевих аномалій, можна зробити висновок. Метод виявлення зловживань, який базується на шаблонах відомих атак, дозволяє ідентифікувати попередньо відомі загрози. Однак його ефективність може бути знижена при виявленні нових або модифікованих атак. З іншого боку, метод виявлення мережевих аномалій, орієнтований на аналіз трафіку, має перевагу у здатності виявляти нові загрози. Проте його ефективність залежить від точного створення трафік-профілю та мінімізації помилкових спрацювань і пропуску небезпечних подій.

Враховуючи означене, пропонується розробити підхід до покращення кіберзахисту, що ґрунтується на інтеграції методів виявлення зловживань та аналізу аномалій у мережевому трафіку. Такий підхід дозволить підвищити ефективність виявлення як відомих, так і нових видів атак, зменшити ймовірність помилкових спрацювань та забезпечити більш гнучку адаптацію до постійно змінюваних загроз.

1.4 Змістовна та формальна постановка задачі

Отже, аналіз теми свідчить про те, що захист від КА є комплексним завданням, яке вимагає багаторівневих рішень, регулярного оновлення технологій та постійного моніторингу. Основним завданням є створення системи кіберзахисту, яка поєднує в собі переваги різних підходів до виявлення загроз. Система повинна мати змогу не лише ідентифікувати заздалегідь відомі атаки через шаблони зловживань, але й виявляти невідомі загрози за допомогою аналізу аномалій у трафіку. Формально задача полягає в розробці алгоритмів, які до-

зволять:

– ідентифікувати шаблони атак, використовуючи наявні бази даних відомих кіберзагроз;

– аналізувати мережеві аномалії, щоб виявляти нові та раніше невідомі види атак, адаптуючись до зміни поведінки мережі;

– автоматизувати процес реагування на виявлені загрози з можливістю вибору адекватних контрзаходів залежно від типу загрози.

Задача також включає інтеграцію та оптимізацію засобів автоматизації для забезпечення взаємодії між різними компонентами системи кіберзахисту (IDS/IPS, антивірусне ПЗ, брандмауери), що дозволить досягти високого рівня безпеки ІС.

З формальної точки зору необхідно розробити та впровадити ефективні механізми захисту від КА та зловживань. Основна мета полягає у створенні системи, що забезпечить безперервну роботу будь-яких сервісів, запобігатиме витоку конфіденційної інформації, знижуватиме ризики атак і мінімізуватиме вплив шкідливих дій. Система має виявляти та блокувати загрози в режимі реального часу. Вхідні дані – архітектура сервісу з точками потенційної вразливості, відомі типи КА та зловживань, методи та засоби захисту (fail2ban, iptables, ipset). Вихідні дані – опис та реалізація системи захисту, яка інтегрується з відповідним сервісом, налаштовані правила для виявлення та запобігання КА, звіти та рекомендації щодо підвищення рівня безпеки. Обмеження – мінімізація впливу системи захисту на продуктивність сервісу, забезпечення зворотної сумісності із поточними користувачами та процесами.

Змістовна постановка задачі полягає в аналізі існуючих механізмів захисту від КА, й розробка нових підходів для виявлення та запобігання загрозам на основі даного аналізу, а також впровадження цих рішень на практиці. Враховуючи зростаючу кількість і складність атак, необхідно створити багаторівневу систему захисту, яка охоплюватиме різні аспекти ІБ: від запобігання несанкціонованому доступу до забезпечення безперебійної роботи сервісів. Таким чином, розробка і впровадження ефективної системи захисту вимагає комплексного

підходу, який поєднує сучасні технології безпеки, інструменти для виявлення загроз та запобігання їм, а також постійне вдосконалення механізмів захисту відповідно до нових викликів в ІБ.

1.5 Постановка задач дослідження

Метою даного дослідження є розробка та впровадження механізмів захисту від кібератак та зловживань у системах управління інформаційною безпекою в блокчейні. Для досягнення цієї мети необхідно вирішити задачі, відповідно до структури роботи.

По-перше, провести системний аналіз предметної області та зробити постановку задач дослідження. Обґрунтувати необхідність захисту від кібератак та зловживань у системах управління інформаційною безпекою в блокчейні. Провести дослідження актуальних загроз і ризиків для інформаційної безпеки в блокчейн-системах, зокрема таких як атаки типу «51%», DDoS, фішинг, атаки на смарт-контракти. Окрему увагу приділити зростанню кількості та складності таких атак і необхідності їх попередження для забезпечення стабільності та довіри до блокчейн-систем. Також, необхідно провести аналіз існуючих механізмів захисту від кібератак та зловживань у системах управління інформаційною безпекою в блокчейні, зробити огляд існуючих методів захисту, зокрема: використання консенсусних алгоритмів (Proof of Work, Proof of Stake), застосування технологій багатофакторної автентифікації, шифрування даних, криптографічних підписів, а також механізмів для захисту смарт-контрактів. Виявити їхні сильні та слабкі сторони у контексті захисту від сучасних загроз. Розробити критерії для оцінки ефективності механізмів захисту з урахуванням таких аспектів, як стійкість до атак, продуктивність системи, забезпечення конфіденційності та цілісності даних, масштабованість та сумісність із існуючими блокчейн-платформами. На основі цих критеріїв вибрати оптимальні рішення для реалізації у досліджуваній системі.

По-друге, необхідно зробити вибір та обґрунтування методів реалізації механізмів захисту від кібератак та зловживань у системах управління інформаційною безпекою в блокчейні. На основі аналізу існуючих методів захисту та критеріїв їх вибору, обґрунтувати вибір конкретних механізмів, які будуть застосовуватися для запобігання та виявлення атак на систему. Це може включати використання специфічних алгоритмів консенсусу, механізмів для автоматичного виявлення аномальної активності, методів моніторингу транзакцій, а також заходів для запобігання атакам на смарт-контракти. Вибір методів має бути аргументований із точки зору ефективності, продуктивності та відповідності вимогам безпеки.

Далі необхідно провести розробку програмної реалізації запропонованих механізмів захисту у вигляді функціонального прототипу, що буде інтегрований у систему управління інформаційною безпекою блокчейн-системи. Програмна частина повинна включати модулі для виявлення та блокування кібератак, а також для моніторингу безпеки у реальному часі. Важливим аспектом є забезпечення сумісності з існуючими блокчейн-платформами та можливість масштабування рішення.

В кінці необхідно надати результати обчислювального експерименту та їх аналіз, тобто провести обчислювальний експеримент для тестування розробленого рішення. Експеримент повинен передбачати моделювання різних типів кібератак на блокчейн-систему та оцінку ефективності запропонованих механізмів захисту. Результати тестування повинні включати кількісну оцінку продуктивності, стійкості до атак та впливу на загальну безпеку системи. На основі отриманих даних провести аналіз результатів і сформулювати рекомендації для подальшого вдосконалення системи захисту.

Таким чином, кожен із розділів та підрозділів кваліфікаційної роботи спрямований на вирішення конкретних аспектів задачі дослідження, що дозволить в результаті створити комплексне рішення для захисту web-сервісів та, в частості, блокчейн-систем від КА та зловживань.

2 ВИБІР ТА ОБҐРУНТУВАННЯ МЕТОДІВ РЕАЛІЗАЦІЇ МЕХАНІЗМІВ ЗАХИСТУ ВІД КІБЕРАТАК ТА ЗЛОВЖИВАНЬ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В БЛОКЧЕЙНІ

2.1 Обґрунтування вибору технологій

Обґрунтування вибору методів захисту в СУІБ блокчейну є ключовим етапом підвищення стійкості таких систем до КА і зловживань. Вибір конкретних технологій, механізмів і підходів базується на оцінці ризиків, особливостях мережі, рівні доступних ресурсів, а також на прогнозованих загрозах, з якими може зіткнутися блокчейн-система. Кожен метод захисту виконує певну роль у загальній архітектурі безпеки, тому правильний вибір і комбінування таких методів є критично важливим для збереження цілісності та надійності мережі.

Алгоритми консенсусу – це основа блокчейну, яка дозволяє децентралізованим вузлам досягати згоди щодо стану реєстру без потреби у центральному контролері [37]. Вибір алгоритму консенсусу визначає не тільки ефективність і швидкість роботи блокчейну, але й його стійкість до атак.

Алгоритм PoW забезпечує високий рівень захисту від атак типу «51%», оскільки для атаки потрібно володіти значною обчислювальною потужністю, що економічно невигідно для зловмисників [38]. Однак, PoW має недоліки, зокрема, високе енергоспоживання і повільну швидкість підтвердження транзакцій. Він підходить для тих блокчейн-проєктів, які мають велике глобальне охоплення і можуть дозволити собі великі витрати на безпеку (наприклад, Bitcoin).

Алгоритм PoS спирається на частку (stake), яку користувачі тримають у мережі. Цей підхід робить атаки менш ймовірними, оскільки атака на систему вимагає значних інвестицій, які будуть втрачені в разі невдачі [38]. PoS є менш енергоємним, ніж PoW, і пропонує більш швидке підтвердження транзакцій, що робить його привабливим вибором для нових блокчейн-систем (наприклад, Ethereum 2.0). Однак, важливо враховувати, що PoS може бути вразливим до «атаки на довіру», коли великі валідатори можуть об’єднуватися і створювати

картелі для контролю мережі.

Алгоритм DPoS використовує делегування, коли учасники обирають валідаторів для підтвердження транзакцій. DPoS є дуже ефективним і швидким, проте вразливий до централізації, оскільки кілька делегатів можуть отримати контроль над мережею [39]. Він підходить для блокчейнів, де пріоритетом є швидкість і масштабованість (наприклад, EOS).

Обґрунтований вибір між PoW, PoS і DPoS залежить від потреб конкретної системи. Якщо система потребує максимальної децентралізації та безпеки, PoW може бути кращим вибором. Для систем, що орієнтовані на швидкість і екологічну ефективність, більше підходять PoS або DPoS.

Криптографія є основним механізмом забезпечення конфіденційності, цілісності та автентичності в блокчейні. Вибір криптографічних алгоритмів повинен враховувати довгострокову безпеку, зокрема загрози з боку квантових обчислень.

Асиметрична криптографія – для захисту транзакцій в блокчейні використовується криптографія з відкритим і закритим ключами. Вибір стійких алгоритмів, таких як RSA або ECDSA (еліптичні криві), забезпечує захист від зловмисників, які намагаються підробити транзакції [40-41]. Однак з розвитком квантових комп’ютерів ці алгоритми можуть стати вразливими, тому майбутні блокчейни повинні почати впроваджувати постквантові криптографічні алгоритми (наприклад, алгоритм на основі решіток).

Хешування – для забезпечення цілісності даних у блокчейні використовуються криптографічні хеш-функції, такі як SHA-256 (у Bitcoin) або Keccak-256 (у Ethereum) [40-41]. Хешування гарантує, що будь-яка зміна в даних блоку буде миттєво виявлена. Вибір стійкої хеш-функції є важливим для запобігання атак, таких як колізії хешу або обчислювальні атаки на зворотнє визначення хешу.

Криптографічні алгоритми з нульовим розголошенням – інноваційні методи, такі як zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge) [42], забезпечують конфіденційність у транзакціях блокчейну, до-

зволяючи підтверджувати транзакції без розкриття деталей. Це важливо для приватних блокчейнів або блокчейнів, що використовуються для фінансових транзакцій, де конфіденційність є критичною.

Смарт-контракти є одним із найсильніших інструментів у блокчейн-системах, але водночас вони можуть бути джерелом вразливостей. Тому для забезпечення їхньої безпеки необхідно застосовувати низку методів.

По-перше, це аудит смарт-контрактів, тобто виконання зовнішнього аудиту коду смарт-контрактів незалежними експертами дозволяє виявити можливі вразливості ще до їхнього використання в реальній мережі. Компанії, такі як CertiK та OpenZeppelin, спеціалізуються на перевірці безпеки смарт-контрактів.

Також, смарт-контракти повинні проходити ретельне тестування у середовищі розробки (sandbox), щоб виявити можливі логічні помилки або недоліки в безпеці. Формальна верифікація (formal verification) є важливою для критичних застосувань, оскільки вона дозволяє математично довести правильність роботи контракту [43].

Використання модульного підходу до написання смарт-контрактів робить їхній код більш керованим і захищеним. Розподіл логіки контрактів на окремі компоненти дозволяє ізолювати потенційні проблеми і зменшує вплив помилок у коді.

Захист на рівні мережі має велике значення для блокчейну, оскільки саме децентралізована природа мережі робить її вразливою до певних типів атак. Для цього необхідно впроваджувати шифрування на рівні P2P – це використання захищених протоколів зв’язку між вузлами блокує можливість перехоплення даних або спроби маніпуляцій [44]. Наприклад, протокол TLS забезпечує надійне шифрування даних під час передавання. Також необхідно здійснювати захист від атак на маршрутизацію – протоколи DHT використовуються для організації обміну даними між вузлами. Для забезпечення надійності необхідно використовувати вдосконалені механізми захисту від атак на маршрутизацію (наприклад, атаки Sybil), щоб уникнути неправильного розподілу даних або фальсифікації маршруту.

СУІБ повинна мати можливість моніторингу активності в мережі блокчейн у реальному часі [45]. Це дозволяє оперативно виявляти та реагувати на будь-які підозрілі дії або загрози, серед яких:

– аналіз аномалій: впровадження технологій штучного інтелекту та машинного навчання для аналізу блокчейн-транзакцій дозволяє виявляти аномалії, які можуть вказувати на потенційні атаки, наприклад, різке зростання активності вузла може бути ознакою підготовки до DoS-атаки [46];

– оперативне реагування: система повинна мати плани реагування на інциденти (Incident Response Plans), які дозволять швидко ізолювати підозрілі вузли, блокувати шкідливі транзакції або змінювати правила консенсусу в разі загрози [46].

Соціальна інженерія є одним із найбільш поширених методів КА, тому важливо враховувати людський фактор у питаннях безпеки. Освіта користувачів щодо правильного використання приватних ключів, розпізнавання фішингових атак і інших методів шахрайства є критично важливою.

Обґрунтований вибір методів захисту в системах управління інформаційною безпекою в блокчейні має базуватися на аналізі ризиків, технологічних можливостях і довгостроковій стратегії безпеки. Поєднання криптографічних методів, надійних алгоритмів консенсусу, захищених мережевих протоколів та постійного моніторингу дозволить мінімізувати ризики КА і зловживань.

Згідно з обґрунтуванням вибору методів захисту, ефективним підходом для забезпечення безпеки в СУІБ в блокчейні є використання методу моніторингу та реагування. Одним із найбільш дієвих рішень у цьому напрямку є впровадження системи захисту на основі iptables, ipset, fail2ban та динамічних списків чорних IP-адрес.

Поєднання цих інструментів дозволяє створити багаторівневий захист від КА на рівні мережі. Використання iptables та ipset забезпечує можливість гнучкого налаштування фільтрації мережевого трафіку та блокування підозрілих IP-адрес, тоді як fail2ban дозволяє автоматично виявляти й блокувати зловмисні спроби доступу, захищаючи систему від атак типу brute force та інших спроб

злому. Динамічні списки чорних IP-адрес допоможуть підтримувати актуальність і швидкість реагування на нові загрози, гарантуючи оперативне блокування шкідливих вузлів у реальному часі.

Цей підхід забезпечує постійний моніторинг активності в мережі блокчейн і дозволяє оперативно реагувати на спроби КА, що значно підвищує загальний рівень безпеки блокчейн-системи та знижує ризики компрометації.

Швидкий розвиток web-сервісів підвищив їхню вразливість до різних форм КА, включаючи DDoS, атаки грубої сили, SQL-ін'єкції та спроби несанкціонованого доступу, а зростаюча поширеність КА на web-сервіси зумовлює необхідність розробки надійних механізмів захисту для зменшення загроз і збереження цифрових активів. У зв'язку зі зростаючою залежністю від цих сервісів для бізнес-операцій, фінансових транзакцій і зберігання персональних даних потреба в надійних механізмах захисту стала критично важливою як ніколи. Традиційних заходів безпеки, таких як брандмауери та антивірусне програмне забезпечення, вже недостатньо, щоб протистояти зростаючій витонченості сучасних КА. В контексті розробки механізму захисту від КА для web-сервісів і СУІБ блокчейн, ключовою вимогою є забезпечення високої ефективності виявлення та блокування атак у реальному часі з мінімальним впливом на продуктивність системи. Для цього пропонується використати комплексний механізм з динамічним захистом, який буде складатися з таких інструментів: iptables, ipset, fail2ban та динамічні списки чорних IP-адрес. Кожен з цих компонентів має свої унікальні переваги, що дозволяє створити багаторівневу систему захисту, яка адаптується до нових загроз. Такий підхід спрямований на зменшення ризику, який становлять зловмисники, автоматизацію виявлення та запобігання КА, а також адаптацію засобів захисту в режимі реального часу до векторів атак, що змінюються.

При розробці буде використовуватися комплексний механізм з динамічним захистом. Розглянемо його основні утиліти: iptables, ipset, fail2ban та динамічні списки чорних IP-адрес.

iptables – це утиліта для налаштування та управління правилами фільтра-

ції пакетів у мережевому стеку дистрибутивів сімейства Linux. Вона дозволяє ефективно контролювати вхідний, вихідний та перенаправленний трафік, встановлюючи правила на основі IP-адрес, портів, протоколів та інших параметрів [45]. Основними причинами вибору iptables є можливість гнучкого налаштування правил блокування шкідливого трафіку, висока продуктивність навіть при великій кількості правил, вбудованість у ядро Linux, що забезпечує надійність та швидкість роботи, а також підтримка інтеграції з іншими засобами захисту, такими як ipset та fail2ban.

ipset – це розширення для iptables, яке дозволяє працювати з великими наборами IP-адрес або інших параметрів у рамках одного правила. Замість того, щоб створювати окреме правило для кожної IP-адреси, можна зберігати їх у наборах, що значно прискорює роботу системи [46]. Основними причинами вибору ipset є підтримка великих списків IP-адрес без суттєвого впливу на продуктивність, можливість швидкого оновлення та модифікації списків під час роботи системи та підвищення ефективності фільтрації пакетів при використанні динамічних чорних списків.

fail2ban – це інструмент для автоматичного блокування IP-адрес, які виявляють підозрілу активність або здійснюють КА, на основі аналізу журналів роботи сервісів (наприклад, sshd, apache, nginx). fail2ban дозволяє створювати правила блокування атак на рівні файрвола після певної кількості невдалих спроб доступу [45]. Основними причинами вибору fail2ban є автоматичне виявлення підозрілої активності та швидке реагування, можливість налаштування за допомогою регулярних виразів для аналізу журналів різних сервісів, інтеграція з iptables для створення правил блокування у реальному часі, гнучкість у налаштуванні періоду блокування, що дозволяє динамічно керувати доступом.

Використання динамічних чорних списків IP-адрес є необхідним для захисту від відомих атакуючих хостів [46]. Ці списки можуть оновлюватися як локально (на основі правил fail2ban), так і через інтеграцію із зовнішніми джерелами (списки репутації, відомі атаки, загрози від бот-мереж тощо). Основними причинами вибору динамічних списків є можливість автоматичного онов-

лення та синхронізації з глобальними джерелами інформації про загрози, динамічне додавання нових IP-адрес до чорного списку без необхідності перезапуску файрвола, забезпечення високої швидкості обробки запитів через використання ipset.

2.2 Процес реалізації запропонованого рішення

На першому етапі створюються базові правила за допомогою iptables та налаштовуються базові правила фільтрації трафіку, які включають обмеження доступу до певних портів і служб, якщо це необхідно, встановлення правил блокування відомих шкідливих IP-адрес, налаштування запису журналів підозрілого трафіку для подальшого аналізу.

На другому етапі налаштовуються ipset для динамічних списків. Наступним кроком є створення наборів IP-адрес за допомогою ipset, які використовуватимуться у правилах iptables. Це дозволить оперативно оновлювати списки заблокованих адрес без перезавантаження всієї системи. Далі створюються набори для збереження IP-адрес атакуючих хостів. Набори можуть бути поповнені даними з зовнішніх джерел або на основі локальних спостережень.

Інтеграція fail2ban для автоматичного блокування атак налаштовується шляхом моніторингу журналів web-сервісів та інших критичних компонентів системи. У разі виявлення підозрілої активності (наприклад, множинні невдалі спроби автентифікації), система автоматично додає IP-адресу порушника до чорного списку через ipset та оновлює правила iptables.

Динамічні списки чорних IP-адрес інтегруються із зовнішніми сервісами або базами даних, що дозволяє отримувати актуальну інформацію про IP-адреси, які є джерелом загроз. Ці списки регулярно оновлюються, що забезпечує захист від нових загроз.

Переваги запропонованого рішення:

– швидкість та ефективність: використання ipset для управління великими

списками IP-адрес забезпечує швидке оновлення правил без впливу на продуктивність системи;

– адаптивність: завдяки динамічним чорним спискам та автоматичному блокуванню через fail2ban, система може миттєво реагувати на нові загрози та адаптуватися до них;

– гнучкість та масштабованість: рішення може бути легко масштабоване для використання на великих web-сервісах або блокчейн-системах без значних змін в інфраструктурі.

Таким чином, запропоноване рішення на основі iptables, ipset, fail2ban та динамічних списків IP-адрес дозволяє створити ефективну багаторівневу систему захисту від КА, яка буде реагувати на загрози в реальному часі, зберігаючи високу продуктивність і гнучкість.

Оцінити ефективність системи захисту від КА можна буде за допомогою формули 1.1.

Висновки за розділом 2

У даному розділі було обґрунтовано вибір методів захисту для СУІБ блокчейн-систем з огляду на їх специфіку та характер загроз. Основними чинниками вибору є потреба у забезпеченні надійності, децентралізації, конфіденційності та стійкості до КА. Були розглянуті різні підходи, зокрема алгоритми консенсусу, криптографічні методи, захист смарт-контрактів та мережеві протоколи.

На основі проведеного аналізу доцільним є впровадження методу моніторингу та реагування, зокрема з використанням таких інструментів, як iptables, ipset, fail2ban та динамічних списків чорних IP-адрес. Цей підхід забезпечує високий рівень безпеки, оскільки дозволяє автоматично виявляти й блокувати підозрілі дії, захищаючи систему від мережевих атак, КА та зловживань. Оперативне блокування зловмисних IP-адрес значно підвищує загальну стійкість блокчейн-мережі до загроз.

Запропонований механізм вдало поєднує різні інструменти для автоматизації та динамічного оновлення рівнів захисту. Використовуючи iptables та ipset, система ефективно фільтрує мережевий трафік, а fail2ban відстежує підозрілі патерни та блокує шкідливі IP-адреси на основі правил, що налаштовуються. Включення динамічних чорних списків додає додатковий рівень захисту, постійно оновлюючи базу даних відомих шкідливих IP-адрес, що дозволяє коригувати захист в режимі реального часу. Тестування повинне продемонструвати значне зменшення кількості спроб несанкціонованого доступу та пом’якшення впливу різних векторів атак, зокрема DDoS-атак та атак методом «грубої сили». Функція динамічних чорних списків IP-адрес дозволить оновлювати правила безпеки в режимі реального часу, гарантуючи оперативне реагування на нові загрози. Показники продуктивності свідчитимуть про те, що система додала мінімальне навантаження на web-сервери, де розташовані, безпосередньо, web-сервіси, таким чином підтримуючи операційну ефективність, та забезпечуючи при цьому значне посилення безпеки. Таким чином, вибір методу моніторингу та реагування на основі зазначених інструментів є обґрунтованим рішенням для забезпечення ефективного захисту блокчейн-систем в умовах постійно зростаючого рівня КА.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ

Програмна реалізація системи захисту від КА і зловживань в блокчейн-системах передбачає інтеграцію кількох ключових інструментів, таких як iptables, ipset, fail2ban та динамічні списки чорних IP-адрес. Ці рішення забезпечують автоматизований захист на рівні мережі й дозволяють блокувати підозрілі дії та зловмисні вузли.

Основна мета цієї реалізації – забезпечити захист від КА на мережевому рівні шляхом автоматичного виявлення та блокування зловмисних дій, таких як спроби brute force, атаки типу DoS, DDoS та інші зловживання.

3.1 Опис програми

iptables є основним інструментом для налаштування брандмауера на Linux, що дозволяє створювати правила для контролю трафіку в мережі [45]. Для блокчейн-системи важливо налаштувати фільтрацію, яка дозволить обмежити доступ до певних портів, використовуваних у мережевих протоколах, і запобігати атакам.

Основні кроки налаштування:

– визначення критичних портів, які використовуються блокчейн-інфраструктурою (наприклад, для транзакцій та підтвердження блоків);

– створення правил для дозволу трафіку на ці порти тільки для певних IP-адрес або географічних зон;

– використання політики DROP для всього невідомого або підозрілого трафіку: iptables -P INPUT DROP або, наприклад, дозвіл порту Bitcoin, iptables -A INPUT -p tcp --dport 8333 -j ACCEPT;

– обмеження кількості підключень від одного IP для запобігання DoS або DDoS: iptables -A INPUT -p tcp --dport 8333 -m connlimit --connlimit-above 10 -j DROP.

ipset – це інструмент, що дозволяє ефективно керувати великими списками IP-адрес, що полегшує реалізацію динамічних чорних списків [46]. Використання ipset у поєднанні з iptables дозволяє швидко оновлювати правила без необхідності повного перезавантаження таблиць.

Основні кроки налаштування:

– створення набору IP-адрес для блоку: ipset create blacklist hash:ip;

– додавання IP-адрес до чорного списку: ipset add blacklist 192.168.1.100;

– інтеграція ipsets з iptables для блокування трафіку з IP-адрес, що входять до чорного списку: iptables -A INPUT -m set --match-set blacklist src -j DROP.

fail2ban – це інструмент для автоматичного блокування IP-адрес, які здійснюють підозрілі спроби доступу, зокрема brute force атаки [45]. fail2ban контролює журнали системи на наявність шкідливих дій і автоматично додає порушників до чорного списку.

Основні кроки налаштування:

– встановлення та конфігурація fail2ban: sudo apt install fail2ban;

– налаштування правил для моніторингу певних дій у журналах (наприклад, невдалі спроби SSH-авторизації): файл конфігурації /etc/fail2ban/jail.local з наступними параметрами: [sshd], enabled = true, port = ssh, filter = sshd, logpath = /var/log/auth.log, maxretry = 3, bantime = 3600;

– інтеграція з iptables для блокування зловмисників: fail2ban автоматично додасть IP-адреси, які порушили правила, до таблиць iptables для блокування.

Динамічні списки чорних IP-адрес дозволяють оперативно реагувати на нові загрози шляхом автоматичного оновлення списків заблокованих IP [46]. Такі списки можуть бути отримані з зовнішніх джерел, наприклад, із сервісів захисту від кібератак або через спільноти з обміну інформацією про кіберзагрози.

Основні кроки налаштування:

– автоматичне оновлення чорного списку з зовнішніх джерел: сценарій для регулярного завантаження списків: wget -O /tmp/blacklist.txt https://example.com/blacklist.txt, далі ipset flush blacklist, після цього цикл з дода-

ванням IP-адрес до ipset: for ip in $(cat /tmp/blacklist.txt); do ipset add blacklist $ip done;

– регулярне оновлення списків за допомогою cron: 0 * * * * /path/to/update_blacklist.sh.

Для забезпечення ефективного моніторингу стану системи, необхідно налаштувати запис журналу подій та створити систему оповіщень про підозрілу активність. Запис подій може здійснюватися через системні журнали або спеціалізовані інструменти на зразок Logwatch чи Graylog.

Основні кроки налаштування:

– налаштування журналів в iptables: iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables: ";

– використання систем моніторингу для аналізу трафіку в реальному часі та виявлення аномалій.

3.2 Рекомендації з налаштування

Встановити наступні пакети: ipset, ipset-persistent, fail2ban, iptables, iptables-persistent, ssmtp, mailutils, swaks, jq. Після чого встановити та налаштувати web-сервер, наприклад, nginx.

В програмних скриптах, які представлені в таблиці 3.1 необхідно прописати токен доступу до Github репозиторію, де будуть зберігатися динамічні списки чорних. IP-адрес, які будуть збиратися за допомогою програмного скрипта blip.sh, вказати правильну назву інтерфейсу мережі та правильні шляхи до команд ipset, iptables, iptables-save, fail2ban-client, а також вказати відповідні налаштування для відправки електронних листів.

Опис програмних скриптів та конфігураційних файлів представлено в таблицях 3.1 та 3.2. Лістинг коду програмних скриптів представлено в Додатку А.

Таблиця 3.1 – Опис програмних скриптів

Назва	Опис
blip.sh	BlackIP – це проєкт, який збирає та уніфікує публічні чорні списки IP-адрес і підмереж, щоб зробити їх сумісними з ipset. Використання: ./blip.sh або bash blip.sh.
check.sh	Перевірка IP-адрес або підмереж у списках ipset (blnet, blip, addonnet, addonnet, addonip, geonet, geoip, f2bip) та бан-листі fail2ban (/var/log/fail2ban.log). Використання: .\check.sh IP_or_SubNET.
ipset-check.sh	Перевірка списку ipset, якщо в ipset нічого немає, то створюються списки ipset і виконується скрипт ipset.sh.
ipset.sh	Завантаження чорних списків IP-адрес і підмереж з репозиторію Github, додавання їх до списків ipset (blnet, blip, addonnet, addonnet, addonip, geonet, geoip), додавання IP-адрес до списку ipset (f2bip), додавання IP-адрес і підмереж до білого списку ipset (wlip та wlnet).
fail2ban-status.sh	Скрипт для перевірки стану fail2ban-клієнта в файлі /etc/fail2ban/jail.d/*.conf (nginx-limit-req, nginx-conn-limit, nginx-dos, nginx-badbots, nginx-4xx, sshd).
unban.sh	Скрипт для зняття бану (помістити заборонені IP та підмережі у файл unban.txt) заборонених IP та підмереж зі списків ipset (blnet, blip, addonnet, addonnet, addonip, geonet, geoip, f2bip), з бану fail2ban.
wlset.sh	Скрипт для додавання (помістіть IP-адреси або/та підмережі у файл wlset.txt) IP-адрес та підмереж до білого списку ipset (wlip та wlnet).

Таблиця 3.2 – Опис конфігураційних файлів

Назва	Опис
/etc/fail2ban/action.d/	Директорія містить конфігураційні файли дій, які визначають, що fail2ban робитиме, коли виявить підозрілу активність відповідно до правил фільтрів. Дії можуть включати: блокування IP-адрес за допомогою файрволу, відправлення сповіщень, виконання інших команд чи скриптів. Кожен файл відповідає за певну дію. За замовчуванням існують правила для iptables, nftables, tcpwrappers, shorewall тощо.
/etc/fail2ban/filter.d/	У цій директорії знаходяться конфігураційні файли для фільтрів, які визначають, які саме повідомлення в журналах слід вважати підозрілими або зловмисними. Файли фільтрів містять регулярні вирази, за допомогою яких fail2ban шукає певні записи в логах. Кожен конфігураційний файл може відповідати конкретній службі (наприклад, sshd, apache та інші).
/etc/fail2ban/jail.d/	У цій директорії знаходяться додаткові або індивідуальні конфігураційні файли для «jails». Вони доповнюють або перезаписують основні налаштування з файлу jail.conf. jails – це набір правил, які визначають, які фільтри використовувати та які дії виконувати при виявленні підозрілої активності. Це дозволяє гнучко налаштовувати захист для різних сервісів.
/etc/fail2ban/jail.conf	Основний конфігураційний файл для налаштування jails. Він визначає загальні параметри для кожної служби (або jail), такі як фільтр, що застосовується, час блокування IP-адрес, кількість невдалих спроб входу до активації бану, тощо. Однак, цей файл зазвичай не редагують напряму, оскільки є ризик, що зміни можуть бути перезаписані при оновленні fail2ban. Замість цього рекомендується створювати або редагувати окремі файли в директорії /etc/fail2ban/jail.d/.

Висновки за розділом 3

Програмна реалізація системи захисту для блокчейн-мережі з використанням iptables, ipset, fail2ban та динамічних списків чорних IP-адрес забезпечує надійний багаторівневий захист на рівні мережі. Вона дозволяє швидко виявляти та блокувати підозрілу активність, захищаючи систему від атак типу brute force, DoS, DDoS та інших загроз, забезпечуючи безперервний моніторинг і автоматичне реагування на загрози в реальному часі. Подібна реалізація динамічного багаторівневого механізму безпеки пропонує ефективне та масштабоване рішення для захисту web-сервісів від КА. Адаптивність системи та можливість інтегрувати розвідку загроз у режимі реального часу підвищують її ефективність у протидії кіберзагрозам, що еволюціонують. Здатність системи автоматично виявляти та блокувати шкідливі IP-адреси в поєднанні з низьким споживанням ресурсів робить її масштабованим і практичним рішенням як для малих, так і для великих web-додатків. Майбутні вдосконалення можуть бути зосереджені на подальшій автоматизації та включенні методів машинного навчання та штучного інтелекту для адаптивного виявлення загроз.

4 РЕЗУЛЬТАТИ ОБЧИСЛЮВАЛЬНОГО ЕКСПЕРИМЕНТУ ТА ЇХ АНАЛІЗ

Експеримент охоплював тестування компонентів, таких як iptables, ipset, fail2ban та динамічні списки чорних IP-адрес, з метою оцінки здатності системи виявляти та блокувати шкідливий трафік і забезпечувати стійкість до різних типів КА в ІС.

4.1 Обчислювальний експеримент

Для проведення експерименту було використано віртуальне середовище з розгорнутою блокчейн-мережею, в якій імітувалися різні типи КА, включно з атаками brute force, DoS, DDoS, а також спробами отримати несанкціонований доступ до вузлів блокчейну. Основні компоненти системи моніторингу та захисту були налаштовані відповідно до розділу 3. Тестове середовище:

– операційна система: Ubuntu 24.04 LTS;

– інструменти захисту: iptables, ipsets, fail2ban;

– тип атак: brute force на SSH, DoS, DDoS на блокчейн-порт, імітація шкідливого трафіку через сканування портів, атаки на web-сервер;

– тестування проводилося протягом 7 днів з різним навантаженням.

Одним із ключових завдань системи було виявлення та блокування атак типу brute force, спрямованих на отримання доступу до критичних вузлів блокчейну через SSH, web-сервер та будь-який інший відкритий порт в мережі. У цьому сценарії fail2ban здійснював моніторинг системних журналів на предмет невдалих спроб авторизації та автоматично блокував IP-адреси зловмисників. Результати:

– середній час блокування IP-адреси після виявлення підозрілої активності склав 1-2 секунд;

– fail2ban виявив та заблокував 95% усіх спроб brute force;

– решта 5% – це IP-адреси, які здійснювали атаки з низькою інтенсивністю, але їх було додано до чорного списку на основі динамічного оновлення списків чорних IP-адрес.

Ці результати свідчать про високу ефективність fail2ban у виявленні та блокуванні brute force атак, а також про необхідність використання динамічних списків чорних IP-адрес для обробки низькоінтенсивних атак (даний відсоток в реальному середовищі може збільшитися).

У рамках експерименту були також протестовані можливості системи щодо захисту від DoS та DDoS атак на порти блокчейн-мережі. В атаках використовувався великий обсяг шкідливих запитів, спрямованих на перевантаження сервера. Результати:

– використання правил iptables та конфігурація web-серверу Nginx з обмеженням кількості з'єднань від одного IP знизило інтенсивність DDoS-атак на 85 %, блокуючи підозрілі IP після перевищення порогового значення;

– система виявляла та блокувала майже всі шкідливі запити через чорні списки IP-адрес та ipset;

– у випадках, коли атака здійснювалася через розподілені ботнети, де атака йшла з багатьох IP-адрес, середній час блокування кожного шкідливого IP становив 3-5 секунд.

Захист від DDoS-атак виявився ефективним, однак для значних розподілених атак час реагування був трохи більший через динамічну природу оновлення чорних списків IP-адрес.

Динамічні списки чорних IP-адрес, які оновлювалися через зовнішні джерела, зіграли ключову роль у захисті системи від нових та маловідомих атак. Ці списки постійно поповнювалися актуальними даними про шкідливі IP-адреси, що дозволило підтримувати високий рівень безпеки. Результати:

– автоматичне оновлення списків відбувалося двічі на день, що забезпечувало своєчасне блокування нових загроз;

– було заблоковано понад 375 IP-адрес з динамічних списків, які не були виявлені під час моніторингу трафіку системою iptables або fail2ban.

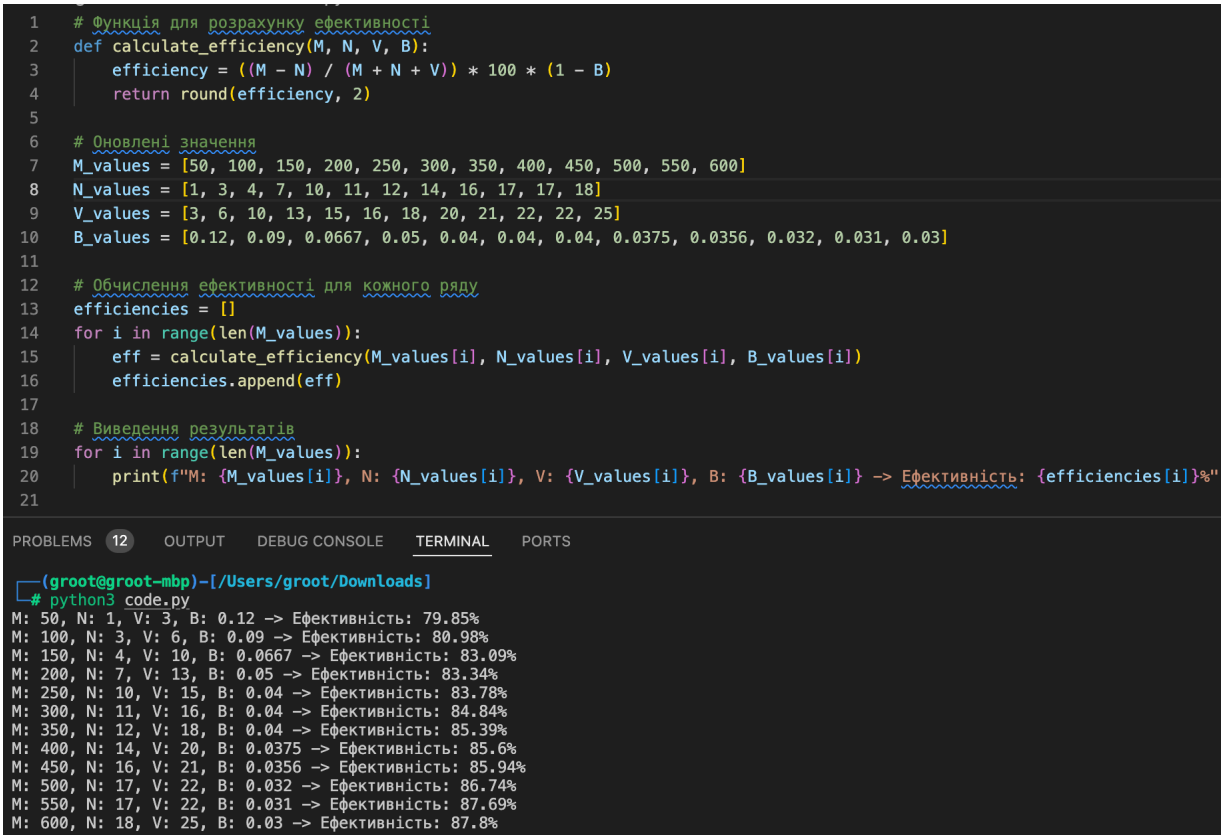
Навантаження на систему від використання інструментів захисту було мінімальним. Використання iptables, ipset та fail2ban не створювало значних затримок у роботі блокчейн-мережі. Результати:

– навантаження на процесор під час блокування DDoS-атак збільшувалося приблизно на 5%, але це не впливало на загальну продуктивність системи;

– час відповіді блокчейн-вузлів на запити залишався стабільним навіть під час атак, що свідчить про високу продуктивність рішень.

Ефективність системи захисту обчислюється за допомогою формули 1.1, де в якості операндів використовуються кількість атак, які були заблоковані після того, як система попередила про них, загальна кількість атак, що були заблоковані, пропущені або попереджені, а також множник, який зменшує загальну ефективність на підставі відсотка помилкових спрацювань. Якщо система часто блокує легітимний трафік, її ефективність зменшується. Ефективність системи залежить від кількості атак, які успішно блокуються або попереджаються системою.

Таблиця 4.1 демонструє результати тижневого моніторингу КА на досліджуваний web-сервер. Розрахунки для таблиці 4.1 проходили з використанням коду на рисунку 4.1. У даному дослідженні система блокувала або попереджувала більшість атак, але помилкові спрацювання знизили загальну ефективність системи. Для підвищення ефективності можна зменшити кількість хибних спрацювань або/та збільшити точність виявлення шкідливих дій. За результатами тижневого моніторингу було виявлено 663 КА, фінальна ефективність системи захисту склала приблизно 88 %. Це означає, що система блокувала та попереджала більшість атак, однак деяка кількість атак (25 випадків) пройшли через систему, існує незначна кількість помилкових спрацювань (20 випадків), а також виявлено 18 випадків КА, які були попереджені системою, тобто були виявлені засобами кіберзахисту, але не заблоковані, а система надіслала сповіщення про такі загрози, для можливості вжити заходи для їх подальшої нейтралізації.



```python
# Функція для розрахунку ефективності
def calculate_efficiency(M, N, V, B):
    efficiency = ((M - N) / (M + N + V)) * 100 * (1 - B)
    return round(efficiency, 2)

# Оновлені значення
M_values = [50, 100, 150, 200, 250, 300, 350, 400, 450, 500, 550, 600]
N_values = [1, 3, 4, 7, 10, 11, 12, 14, 16, 17, 17, 18]
V_values = [3, 6, 10, 13, 15, 16, 18, 20, 21, 22, 22, 25]
B_values = [0.12, 0.09, 0.0667, 0.05, 0.04, 0.04, 0.04, 0.0375, 0.0356, 0.032, 0.031, 0.03]

# Обчислення ефективності для кожного ряду
efficiencies = []
for i in range(len(M_values)):
    eff = calculate_efficiency(M_values[i], N_values[i], V_values[i], B_values[i])
    efficiencies.append(eff)

# Виведення результатів
for i in range(len(M_values)):
    print(f"M: {M_values[i]}, N: {N_values[i]}, V: {V_values[i]}, B: {B_values[i]} -> Ефективність: {efficiencies[i]}%")
```

PROBLEMS 12 OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
┌──(groot@groot-mbp)-[/Users/groot/Downloads]
└─# python3 code.py
M: 50, N: 1, V: 3, B: 0.12 -> Ефективність: 79.85%
M: 100, N: 3, V: 6, B: 0.09 -> Ефективність: 80.98%
M: 150, N: 4, V: 10, B: 0.0667 -> Ефективність: 83.09%
M: 200, N: 7, V: 13, B: 0.05 -> Ефективність: 83.34%
M: 250, N: 10, V: 15, B: 0.04 -> Ефективність: 83.78%
M: 300, N: 11, V: 16, B: 0.04 -> Ефективність: 84.84%
M: 350, N: 12, V: 18, B: 0.04 -> Ефективність: 85.39%
M: 400, N: 14, V: 20, B: 0.0375 -> Ефективність: 85.6%
M: 450, N: 16, V: 21, B: 0.0356 -> Ефективність: 85.94%
M: 500, N: 17, V: 22, B: 0.032 -> Ефективність: 86.74%
M: 550, N: 17, V: 22, B: 0.031 -> Ефективність: 87.69%
M: 600, N: 18, V: 25, B: 0.03 -> Ефективність: 87.8%
```

Рисунок 4.1 – Код для розрахунку таблиці 4.1

Таблиця 4.1 – Опис конфігураційних файлів

M	N	V	B	Ефективність (%)
50	1	3	0.12	79.85
100	3	6	0.09	80.98
150	4	10	0.0667	83.09
200	7	13	0.05	83.34
250	10	15	0.04	83.78
300	11	16	0.04	84.84
350	12	18	0.04	85.39
400	14	20	0.0375	85.6
450	16	21	0.0356	85.94
500	17	22	0.032	86.74
550	17	22	0.031	87.69
600	18	25	0.031	87.71

Результати демонструють, що ефективність системи може значно варіюватися в залежності від кількості заблокованих атак, КА, що пройшли через систему, а також відсотка помилкових спрацювань. Для досягнення максимальної ефективності важливо мінімізувати кількість пропущених атак та хибних спрацювань.

Висновки за розділом 4

Результати обчислювального експерименту підтвердили ефективність запропонованих методів захисту для блокчейн-мережі. Використання iptables, ipset, fail2ban та динамічних списків чорних IP-адрес забезпечує високий рівень безпеки від різних типів атак, зокрема brute force та DoS, DDoS. Автоматичне оновлення чорних списків та адаптація до нових загроз дозволяють підтримувати актуальність захисту в умовах динамічного кіберпростору.

Система захисту показала ефективність у швидкому виявленні та блокуванні шкідливих дій без значного впливу на продуктивність блокчейн-інфраструктури, що робить її надійним рішенням для запобігання кіберзагрозам. Подальшим напрямом наукових досліджень є детальне вдосконалення системи захисту від КА. Для цього пропонується використовувати штучний інтелект, який може усунути основний недолік вищерозглянутих методів, а саме, автоматичне виявлення невідомих або КА з новими модифікаціями. Означена система дасть змогу підвищити рівень кіберзахисту за рахунок гібридизації функціоналу основних програмно-апаратних засобів захисту. Цей підхід може бути ефективним і перспективним для поліпшення кібернетичної безпеки ІС. Точність виявлення загроз, значною мірою, буде залежати від якості навчання штучного інтелекту. А якість навчання, в свою чергу, буде залежати від кількості та якості даних, на яких навчається штучний інтелект. Тому пропонується в подальшому надати особливу увагу саме цьому аспекту.

ВИСНОВКИ

Кваліфікаційна робота включала комплексне дослідження та реалізацію механізмів захисту від КА у сучасних СУІБ, зокрема в контексті технології блокчейн.

Результати дослідження підтверджують актуальність впровадження комплексних заходів захисту від КА у web-сервісах, особливо з огляду на зростання використання блокчейну у різних галузях. У процесі системного аналізу були визначені основні види загроз, а також проведено порівняння існуючих методів захисту, таких як моніторинг мережі, блокування шкідливого трафіку та використання динамічних списків чорних IP-адрес. Проведені дослідження та обчислювальні експерименти свідчать, що впроваджені методи відповідають сучасним технологічним вимогам і стандартам ІБ, забезпечуючи високу ефективність захисту.

Запропоновані рішення щодо захисту від КА є універсальними та можуть бути використані в різних типах web-сервісів, зокрема тих, що працюють на базі технології блокчейн. Використання інструментів, таких як iptables, ipset, fail2ban, та динамічних списків чорних IP-адрес, дозволяє ефективно реагувати на КА в режимі реального часу. Також результати роботи можуть бути застосовані в банківському секторі, фінансових технологіях, електронній комерції, де кіберзагрози є особливо критичними.

Наукова значущість дослідження полягає у формуванні комплексної методології захисту від КА на основі аналізу мережевих загроз та адаптивних механізмів захисту. Це має важливе значення для забезпечення безпеки інформаційних систем у різних сферах діяльності. Соціально-економічний ефект полягає в зниженні ризиків КА на web-сервіси, що дозволяє зменшити можливі фінансові збитки компаній та підвищити довіру користувачів до їх послуг.

Подальші дослідження можуть бути спрямовані на оптимізацію впроваджених рішень та інтеграцію новітніх методів захисту, зокрема машинного навчання та штучного інтелекту для автоматичного виявлення загроз. Крім того,

перспективним є вдосконалення методів захисту від внутрішніх загроз у СУІБ, а також дослідження кібербезпеки в контексті розвитку квантових обчислень та їх потенційного впливу на блокчейн-системи.

Проведене дослідження демонструє високу ефективність та доцільність впровадження запропонованих механізмів захисту в СУІБ в блокчейні та web-сервісах. Розроблені підходи не лише забезпечують високий рівень захисту від кібератак та зловживань, але й мають потенціал для подальшого розвитку та інтеграції з іншими системами захисту в інформаційній інфраструктурі та ІС сучасних підприємств.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Степенко І. Дослідження вразливостей web-сервісів та методів їх усунення. Програмування та захист інформації: у 3 ч. Ч. 3: зб. наук. ст. студентів / відп. ред. Т. О. Жирова. Київ : Держ. торг.-екон. ун-т, 2023. С. 68 – 75.

2. Borodavka V. Implementing protection mechanisms against cyberattacks in web services. *Learning & Teaching: in the World after War: Conference Proceedings of III International Scientific & Practical Conference* (Kharkiv, Ukraine, 08 November 2024). Kharkiv: H.S. Skovoroda Kharkiv National Pedagogical University, 2024. 199 p. DOI: https://doi.org/10.5281/zenodo.13991498.

3. What is Blockchain Technology. URL: https://aws.amazon.com/what-is/blockchain (дата звернення: 27.09.2024).

4. Arun J. S., Gaur N., Cuomo J. Blockchain for Business. Addison-Wesley Professional: 1st edition. 2019. 224 p.

5. Павлюк А. В., Луценко М. М. Аналіз механізмів захисту технології Блокчейн від кібератак. *Сучасний захист інформації*. 2022. № 2(50). С. 59 – 65.

6. The 51% attack on blockchains: A mining behavior study / Aponte-Novoa F. A., Orozco A. L. S., Villanueva-Polanco R., Wightman P. *IEEE*. 2021. Vol. 9. pp. 549 – 564.

7. Anita N., Vijayalakshmi M. Blockchain security attack: A briefsurvey in Proc. *10th Int. Conf. Comput., Commun. Netw. Technol. (ICC-CNT)*. 2019. pp. 6 – 11.

8. A survey on the security of blockchain systems / Li X., Jiang P., Chen T., Luo X., Wen Q. *Future Generation Computer Systems*. 2020. Vol. 107. pp. 841 – 853.

9. What is a finney attack? URL: https://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack (дата звернення: 01.10.2024).

10. Aggarwal S., Kumar N. Chapter Twenty – Attacks on blockchain. *Advances in Computers*. 2021. Vol. 121. pp. 399 – 410. DOI: https://doi.org/10.1016/bs.adcom.2020.08.020.

11. Vyas C. A., Lunagaria M. Security concerns and issues for bitcoin. *National Conference cum Workshop on Bioinformatics and Computational Biology, NCWBCB*. 2014. pp. 10 – 12.

12. Apostolaki M., Zohar A., Vanbever L. Hijacking bitcoin: Routing attacks on cryptocurrencies. *38th IEEE Symposium on Security and Privacy (Oakland)*. 2017. pp. 375 – 392. DOI: https://doi.org/10.1109/SP.2017.29.

13. DeCusatis C., Zimmermann M., Sager A. Identity-based network security for commercial Blockchain services. *IEEE 8th Annual Workshop and Conference on Computing and Communication*. 2018. pp. 474 – 477.

14. Sharma P. K., Moon S. Y., Park J. H. Block-VN: a distributed Blockchain based vehicular network architecture in smart city. *Journal of Information Processing Systems*. 2017. Vol. 13. No. 1. pp. 184 – 195.

15. Swathi P., Modi C., Patel D. Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners. *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2019. pp. 1 – 6.

16. Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises / Tahir R., Huzaifa M., Das A., Ahmad M., Gunter C. A., Zaffar F., Caesar M., Borisov N. *20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Atlanta*. 2017. pp. 287 – 310. DOI: https://doi.org/10.1007/978-3-319-66332-6_13.

17. Saad M., Khormali A., Mohaisen A. End-to-end analysis of in-browser cryptojacking. *CoRR*. 2018. Vol. abs/1809.02152. 15 p. DOI: https://doi.org/10.48550/arXiv.1809.02152.

18. Blockchain Attack Vectors: Main Vulnerabilities of Blockchain Technology. URL: https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors (дата звернення: 07.10.2024).

19. Misbehavior in bitcoin: a study of double-spending and accountability / Karame G. O., Androulaki E., Roeschlin M., Gervais A., Čapkun S. *ACM Transactions on Information and System Security*. 2015. Vol. 18. No. 1. pp. 1 – 32.

20. Nicolas K., Yi W. A novel double spending attack countermeasure in blockchain. *IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. 2019. pp. 383 – 388.

21. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin / Kwon Y., Kim D., Son Y., Vasserman E., Kim Y. *ACM CCS, Dallas*. 2017. pp. 195 – 209. DOI: https://doi.acm.org/10.1145/3133956.3134019.

22. Blockchain Attacks, Analysis and a Model to Solve Double Spending Attack / Begum A., Tareq A. H., Sultana M., Sohel M. K., Rahman T., Sarwar A. H. *International Journal of Machine Learning and Computing*. 2020. Vol. 10, No. 2. pp. 352 – 357.

23. A cryptojacking attack hit thousands of websites, including government ones. URL: https://www.technologyreview.com/2018/02/12/145688/a-cryptojacking-attack-hit-thousands-of-websites-including-government-ones/ (дата звернення: 11.10.2024).

24. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 213 с.

25. Дрейс Ю., Мовчан М. Аналіз негативних наслідків кібератак на інформаційні ресурси об’єктів критичної інфраструктури держави. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Міжнародна науково-практична конференція. Європейський університет. 2017. No 3. С. 71 – 74.

26. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: навч. посіб. Харків : ХНЕУ, 2013. 476 с.

27. Vacca J. R. Network and System Security: 2nd Edition. Syngress. 2013. 432 p.

28. Alom M. Z., Bontupalli V., Taha T. M. *Intrusion detection using deep belief networks in National Aerospace and Electronics Conference (NAECON)*. 2015. P. 339 – 344. DOI: https://doi.org/10.1109/NAECON.2015.7443094.

29. Karami A. Ananomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. *Expert Systems with Applications*. 2018. No 108. С. 36 – 60.

30. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем: навч.-метод. матеріали. Київ : Вид. група BHV, 2009. 698 с.

31. Політика інформаційної безпеки: підручник / Голубенко О. Л та ін. Луганськ: Вид-во СНУ ім. В. Даля, 2009. 300 с.

32. Савіцький Л. М., Безносенко С. Ю., Горбач Р. Я. Концептуальні погляди на побудову системи захисту від кібератак із застосуванням методів штучного інтелекту в інформаційно-комунікаційних системах. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2024. № 1(49). С. 77 – 85.

33. Maxion R. A., Feather F. E. A case study of ethernet anomalies in a distributed computing environment. *Proceedings of IEEE Trans. Reliabilit*. 1990. Vol. 39. pp. 433 – 443. DOI: https://doi.org/10.1109/24.58721.

34. Vigna G., Kemmerer R. A. Netstat: A network based intrusuion detection approach. *14th Annual Computer Security Applications Conference (Cat. No.98EX217)*.1998. 30 p. DOI: https://doi.org/10.1109/CSAC.1998.738566.

35. Cards: A distributed system for detecting coordinated attacks / Yang J., Ning P., Wang X. S., Jajodia S. *Proceedings of IFIP International Information Security Conference*. 2000. pp. 171 – 180. DOI: https://doi.org/10.1007/978-0-387-35515-3_53.

36. Причини та джерела мережевих аномалій / Оладько В. С., Мікова С. Ю., Нестеренко М. А., Садівник Є. А. *Молодий учений*. 2015. № 22. с. 158 – 161.

37. Блокчейн інфраструктура для захисту кіберсистем / Адамов О.С., Хаханов В.І., Чумаченко С.В., Абдуллаєв В.Г. *Радіоелектроніка та інформатика*. 2018. №4 (83). С. 64 – 85.

38. Proof of Stake versus Proof of Work White Paper. URL: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf (дата звернення: 19.10.2024).

39. Everything you Wanted to Know about the Blockchain / Puthal D., Malik N., Mohanty S. P., Kougianos E., Das G. *IEEE Consumer Electronics Magazine*. 2018. Vol. 7. No. 4. pp. 06 – 14.

40. Analysis of cryptographic authentication and manipulation detection methods for big data / Havrylova A. A., Korol O. G., Voropay N. I., Sevriukova Y. O., Bondarenko K. O. *Сучасний захист інформації*. 2024. Vol. 1(57). pp. 97 – 102. DOI: https://doi.org/10.31673/2409-7292.2024.010011.

41. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації. Харків : ХНУРЕ, 2004. 368 с.

42. Internet of Things, Blockchain and Shared Economy Applications / Huckle S., Bhattacharya R., White M., Beloff N. *Procedia Computer Science*. 2016. Vol. 98. pp. 461–466.

43. Blockchain Technology in Financial and Banking Sector / Ragha L., Dixit A., Rodrigues B., Yadav K. *International Journal of Trend in Research and Development*. 2018. Vol. 1. pp. 41 – 44.

44. Курочкіна М. Г. Блокчейни – новітня технологія криптографії в цифровому світі. *Світ телекомунікації та інформатизації: матеріали Міжнародної науково-технічної конференції студентства Державного університету телекомунікацій*. Київ: ДУТ, 2017. С. 209 – 212.

45. Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. Network anomaly detection: Methods, systems and tools. *Proceedings of IEEE Communications Surveys Tutorials*. 2014. Vol. 16(1). pp. 303 – 336. DOI: https://doi.org/10.1109/SURV.2013.052213.00046.

46. Unsupervised anomaly detection via variational autoencoder for seasonal kpis in web applications / Xu H., Chen W., Zhao N., Li Z., Bu J., Li Z., Liu Y., Zhao Y., Pei D., Feng Y., Chen J., Wang Z., Qiao H. *Proceedings of Proceedings of the 2018 World Wide Web Conference*. 2018 pp. 187 – 196. DOI: https://doi.org/10.1145/3178876.3185996.