МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Факультет: ННІ Каразінський банківський інститут
Кафедра: Інформаційних технологій та математичного моделювання
Спеціальність: 125 Комп'ютерні науки
Освітня програма: Комп'ютерні науки та інформаційні технології в бізнесі

Група: АБ-41Б денна форма навчання

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:
Захист трафіку на основі сканування IP адрес
ЗА НАКАЗОМ № 4601-5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

здобувача вищої освіти Хоменка Владислава Вікторовича

Робота допущена до захисту в ЕК
протокол кафедри ІТММ №__ від _____2024р.

Завідувач кафедри ІТММ
к.п.н.
_____ Н.І. Стяглик

Науковий керівник
к.т.н., доцент
_____Петренко Ольга Євгенівна

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма Кібербезпека у фінансових технологіях

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Н. І. Стяглик
Підпис ініціали, прізвище

“08” лютого 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Хоменка Владислава Вікторовича
(прізвище, ім’я, по батькові студента)

1. Тема роботи Захист трафіку на основі сканування IP адрес

керівник роботи к.т.н., доцент Петренко Ольга Євгенівна
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від “08” лютого 2025 року № 4601-5/335

2. Строк подання студентом роботи 15 травня 2025 року

3. Перелік питань, які потрібно розробити:
У розділі 1: розглянути теоретичні аспекти сканування IP адрес для захисту трафіку, методи аналізу та моніторингу IP адрес у мережі. Визначити потенційні загрози на основі сканування.
У розділі 2: зробити аналіз потенційних загроз, які впливають на мережевий трафік у фінансових технологіях. Огляд атак через IP-сканування, стандарти технології та безпеки
У розділі 3: розробити модель системи захисту трафіку. Створити програмну реалізацію цієї системи та її тестування на основі сценарію кібератак

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

5. Дата видачі завдання 08 лютого 2025 року

Студент _____ _____
підпис ініціали, прізвище

Керівник роботи _____ _____
підпис ініціали, прізвище

РЕФЕРАТ

НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ

«ЗАХИСТ ТРАФІКУ НА ОСНОВІ СКАНУВАННЯ IP АДРЕС»

Хоменка Владислава Вікторовича

Кваліфікаційна бакалаврська робота містить 100 сторінки, 11 таблиць, 1 рисунок, список літератури із 35 найменувань, 1 додаток.

Об'єктом дослідження є захист трафіку на основі сканування IP адрес

Предметом дослідження є технології та методи захисту трафіку, які базуються на скануванні IP адрес. Предмет дослідження зосереджений на практичних аспектах реалізації таких технологій у фінансовій сфері, де швидкість і точність реакції на загрози є критично важливими для захисту даних клієнтів і забезпечення безперебійної роботи сервісів.

Мета кваліфікаційної бакалаврської роботи полягає у розробці програмної реалізації захисту трафіку на основі аналізу сучасних атак та методів протидії до них.

Завданнями кваліфікаційної роботи є:

– аналіз потенційних загроз, які впливають на мережевий трафік у фінансових технологія;

– дослідження сучасних систем захисту інформації, оцінка їх сильних та слабких сторін;

– розробка моделі захисту трафіку;

– створення програмної реалізації цієї системи та її тестування на основі модельних сценаріїв кібератак.

Актуальність дослідження: сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням цифрових сервісів у фінансовій сфері, що супроводжується не лише розширенням можливостей для користувачів, а й значним збільшенням кіберзагроз. Важливість теми

зумовлена не лише зростанням кіберзагроз, а й вимогами регуляторних органів, таких як FinCEN і FDIC, які наголошують на необхідності впровадження сучасних технологій захисту даних у фінансових системах. Розробка ефективних рішень для захисту трафіку на основі сканування IP адрес є важливим кроком до підвищення рівня кібербезпеки та забезпечення стабільності цифрових фінансових сервісів, що, у свою чергу, сприяє зміцненню довіри клієнтів і партнерів.

За результатами дослідження сформульовані теоретичні та практичні положення, пропозиції щодо захисту трафіку на основі сканування IP- адрес.

Практична новизна: результати цього дослідження мають важливе практичне значення для забезпечення кібербезпеки у сфері фінансових технологій. Розроблена програмна реалізація системи захисту трафіку на основі сканування IP-адрес дозволяє швидко виявляти потенційні загрози та адаптуватися до нових видів атак. Використання технологій машинного навчання забезпечує високу точність аналізу мережевого трафіку, що значно знижує ризик кібератак на фінансові установи. Запропонована система може бути інтегрована у вже існуючі платформи кібербезпеки, що сприятиме підвищенню їх ефективності. Це особливо актуально для банків, фінансових сервісів та інших організацій, які працюють із чутливою інформацією та потребують надійного захисту даних клієнтів.

Одержані результати можуть бути використані у фінансових установах, фінтех-компаніях, корпоративному секторі та державних організаціях для підвищення рівня кібербезпеки. Запропонована система дозволяє ефективно аналізувати мережевий трафік, виявляти потенційні загрози та адаптуватися до нових видів атак, що є критично важливим для захисту даних клієнтів і стабільності цифрових сервісів.

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, ЗАХИСТ ТРАФІКУ, ФІНАНСОВІ ТЕХНОЛОГІЇ, СКАНУВАННЯ IP-АДРЕС, МАШИННЕ НАВЧАННЯ, АНАЛІЗ ЗАГРОЗ, МЕРЕЖЕВИЙ МОНІТОРИНГ, КІБЕРЗАГРОЗИ, АВТОМАТИЗОВАНИЙ ЗАХИСТ, ВИЯВЛЕННЯ АТАК.

ABSTRACT

AT QUALIFICATION BACHELOR WORK

“TRAFFIC PROTECTION BASED ON IP ADDRESS SCANNING”

Vladyslav Viktorovych Khomenko

The bachelor’s qualification thesis contains 100 pages, 11 tables, 1 drawing, and a list of references comprising 35 titles.

The object of the research is traffic protection based on IP address scanning. The subject of the research is technologies and methods for traffic protection based on IP address scanning, with a focus on practical implementation in the financial sector, where rapid and precise response to threats is critical for safeguarding client data and ensuring service continuity.

The purpose of the qualification thesis is to develop a software implementation for traffic protection based on the analysis of modern cyberattacks and effective countermeasures.

The tasks of a bachelor's degree are:

– analysis of potential threats affecting network traffic in financial technologies;

– research of modern information security systems, including assessment of their strengths and weaknesses;

– development of a traffic protection model;

– creation and testing of the software implementation based on simulated cyberattack scenarios.

The relevance of the research lies in the rapid growth of digital financial services, which, alongside user benefits, also leads to increased cyber threats. The topic’s importance is driven not only by this rise in threats but also by regulatory demands from bodies such as FinCEN and FDIC, which emphasize the need for modern data protection technologies in financial systems.

According to the results of the research: theoretical and practical foundations for traffic protection based on IP address scanning have been developed, along with proposals for improving cybersecurity solutions in the financial sector.

Main theoretical provisions on the topic and the practical relevance of the research demonstrate that the proposed solution significantly enhances the ability to detect and respond to threats in real-time using machine learning and adaptive traffic monitoring mechanisms.

The results obtained can be used in financial institutions, fintech companies, the corporate sector, and government organizations to strengthen cybersecurity, ensure data integrity, and maintain the reliability of digital financial services.

KEYWORDS: cybersecurity, traffic protection, financial technologies, IP address scanning, machine learning, threat analysis, network monitoring, cyber threats, automated protection, attack detection.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ

API – Application Programming Interface (Інтерфейс програмування додатків) – стандартний набір правил і інструментів для взаємодії між програмними компонентами, який використовується для інтеграції розробленої системи з існуючими рішеннями.

AWS – Amazon Web Services – хмарна платформа від Amazon, згадана як приклад для оцінки масштабованості системи в хмарних середовищах.

CDN – Content Delivery Network (Мережа доставки контенту) – розподілена мережа серверів, яка використовується в системах захисту від DDoS-атак, таких як Cloudflare чи Akamai.

CNN – Convolutional Neural Network (Згорткова нейронна мережа) – тип нейронної мережі, який застосовується для аналізу послідовностей трафіку в модулі машинного навчання.

CPU – Central Processing Unit (Центральний процесор) – апаратний компонент, продуктивність якого оцінювалася під час тестування системи.

CSV – Comma-Separated Values (Значення, розділені комами) – формат файлу для зберігання структурованих даних, використаний для запису зібраного трафіку.

DDoS – Distributed Denial of Service (Розподілена відмова в обслуговуванні) – тип кібератаки, спрямований на перевантаження системи масовим трафіком, який тестувався в сценаріях.

DPI – Deep Packet Inspection (Глибокий аналіз пакетів) – технологія, застосована в NGFW для детального аналізу вмісту мережевих пакетів.

FDIC – Federal Deposit Insurance Corporation (Федеральна корпорація страхування депозитів) – регуляторний орган США, згаданий у контексті стандартів безпеки для фінансових систем.

FinCEN – Financial Crimes Enforcement Network (Мережа боротьби з фінансовими злочинами) – орган США, який встановлює вимоги до звітності про підозрілу діяльність, включаючи IP-адреси.

GIL – Global Interpreter Lock (Глобальна блокування інтерпретатора) – механізм у Python, що обмежує багатопотоковість і впливає на продуктивність системи.

GUI – Graphical User Interface (Графічний інтерфейс користувача) – інтерфейс, реалізований через tkinter для взаємодії адміністраторів із системою.

IDS – Intrusion Detection System (Система виявлення вторгнень) – технологія для моніторингу та виявлення підозрілої активності в мережі.

IoT – Internet of Things (Інтернет речей) – пристрої, які можуть бути вразливими до сканування та включення в ботнети.

IP – Internet Protocol (Інтернет-протокол) – основний протокол для передачі даних у мережі, аналіз якого є центральним у роботі.

IPS – Intrusion Prevention System (Система запобігання вторгненням) – розширення IDS із функцією активного блокування загроз.

IPv4 – Internet Protocol version 4 – четверта версія протоколу IP із обмеженим адресним простором.

IPv6 – Internet Protocol version 6 – шоста версія протоколу IP із розширеним адресним простором, що ускладнює захист від сканування.

ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою, який визначає вимоги до моніторингу та захисту трафіку.

JSON – JavaScript Object Notation – формат даних, використаний для генерації звітів про інциденти.

ML – Machine Learning (Машинне навчання) – технологія, застосована для прогнозування та виявлення загроз у системі.

NGFW – Next-Generation Firewall (Міжмережевий екран нового покоління) – сучасна система захисту, яка поєднує фільтрацію та аналіз трафіку.

NIS2 – Network and Information Security Directive 2 (Директива про безпеку мереж та інформації 2) – європейський стандарт кібербезпеки для критичних інфраструктур.

Nmap – Network Mapper – інструмент для сканування мережі, згаданий як приклад методу зловмисників.

ОЗУ – Оперативний запам’ятовуючий пристрій (RAM) – апаратний ресурс, споживання якого оцінювалося під час тестування продуктивності.

PCI DSS – Payment Card Industry Data Security Standard (Стандарт безпеки даних індустрії платіжних карток) – стандарт, який регулює захист платіжних даних.

RNN – Recurrent Neural Network (Рекурентна нейронна мережа) – тип нейронної мережі для аналізу послідовностей трафіку.

sFlow – Sampled Flow – протокол для передачі даних про трафік, згаданий у контексті інтеграції.

SNMP – Simple Network Management Protocol (Простий протокол управління мережею) – протокол для обміну даними між системами безпеки.

СУІБ – Система управління інформаційною безпекою – комплекс заходів і процедур, визначений у стандарті ISO/IEC 27001.

SVM – Support Vector Machines (Машина опорних векторів) – алгоритм класифікації, згаданий у модулі машинного навчання.

TCP – Transmission Control Protocol (Протокол управління передачею) – протокол, порти якого скануються зловмисниками.

TLS – Transport Layer Security (Безпека транспортного рівня) – протокол шифрування, використаний для захисту внутрішнього трафіку.

UDP – User Datagram Protocol (Протокол датаграм користувача) – протокол, який також аналізується під час сканування.

VPN – Virtual Private Network (Віртуальна приватна мережа) – технологія, яка ускладнює геолокаційний аналіз через маскування IP-адрес.

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням цифрових сервісів у фінансовій сфері, що супроводжується не лише розширенням можливостей для користувачів, а й значним збільшенням кіберзагроз. Фінансові технології, такі як онлайн-банкінг, платіжні системи та мобільні додатки для управління фінансами, стають привабливими цілями для зловмисників через високий рівень чутливості даних, які вони обробляють. За даними міжнародних аналітичних звітів, у 2024 році кількість кібератак на фінансові установи зросла на 20% порівняно з попереднім періодом, а середній збиток від одного інциденту перевищив 1 мільйон доларів США. У таких умовах захист мережевого трафіку набуває критичного значення, адже саме через мережу здійснюється передача конфіденційної інформації, а її перехоплення чи маніпуляція можуть призвести до катастрофічних наслідків. Одним із ключових інструментів забезпечення безпеки є сканування IP адрес, яке дозволяє здійснити моніторінг мережевого трафіку, виявляти підозрілу активність і своєчасно реагувати на потенційні загрози. У фінансовому секторі цей метод має особливе значення, адже він дає змогу не лише ідентифікувати джерела атак, а й запобігати шахрайству шляхом аналізу геолокації чи блокування неавторизованого доступу. Актуальність теми зумовлена не лише зростанням кіберзагроз, а й вимогами регуляторних органів, таких як FinCEN і FDIC, які наголошують на необхідності впровадження сучасних технологій захисту даних у фінансових системах. Розробка ефективних рішень для захисту трафіку на основі сканування IP адрес є важливим кроком до підвищення рівня кібербезпеки та забезпечення стабільності цифрових фінансових сервісів, що, у свою чергу, сприяє зміцненню довіри клієнтів і партнерів.

Метою дослідження є розробка програмної реалізації захисту трафіку на основі аналізу сучасних атак та методів протидії до них.

Для досягнення цієї мети визначено низку **завдань :**

1. Аналіз потенційних загроз, що впливають на мережевий трафік у фінансових технологіях.
2. Дослідження методів виявлення загроз через сканування IP-адрес.
3. Огляд сучасних систем захисту інформації,.
4. Розробка моделі захисту трафіку з використанням технологій машинного навчання.
5. Програмна реалізація моделі захисту та її інтеграція у систему.
6. Тестування системи на основі модельних сценаріїв кібератак.
7. Оцінка ефективності та практичної значущості розробленого рішення.
8. Адаптація та потенційне впровадження розробленої системи в реальних умовах фінансових установ для захисту інфраструктури.

Об’єктом дослідження виступає захист трафіку на основі сканування IP -адрес. Цей об’єкт охоплює широкий спектр процесів, пов’язаних із моніторингом мережевого трафіку, аналізом активності в мережі та своєчасним реагуванням на потенційні загрози.

Предметом дослідження є технології та методи захисту трафіку, які базуються на скануванні IP адрес. Сюди входять алгоритми виявлення підозрілих дій, інтеграція з існуючими системами кібербезпеки, а також використання машинного навчання для аналізу великих обсягів даних про трафік. Предмет дослідження зосереджений на практичних аспектах реалізації таких технологій у сфері фінансових технологій, де швидкість і точність реакції на загрози є критично важливими для захисту даних клієнтів і забезпечення безперебійної роботи сервісів.

Для вирішення поставлених завдань у роботі застосовано комплексний набір **методів** дослідження, що дозволяє охопити як теоретичну, так і практичну складові теми. Теоретичний аналіз використаний для вивчення літературних джерел, нормативних документів і сучасних підходів до захисту трафіку дозволив сформувати фундамент для подальших розробок. Порівняльний аналіз застосований для оцінки існуючих систем кібербезпеки,

їх ефективності та можливостей адаптації до потреб фінансового сектору. Метод моделювання став основою для створення моделі захисту трафіку, яка враховує специфіку роботи фінансових технологій і динамічність кіберзагроз. Експериментальний метод використаний для тестування розробленої програмної реалізації, зокрема шляхом створення штучних сценаріїв атак і аналізу результатів роботи системи. Окрім того, у роботі застосовано методи машинного навчання, які дозволили реалізувати інтелектуальний аналіз трафіку та прогнозувати потенційні загрози на основі даних, отриманих через сканування IP адрес. Поєднання цих методів забезпечує всебічний підхід до дослідження та сприяє досягненню поставленої мети.

Робота структурована таким чином, щоб послідовно розкрити всі аспекти теми та представити результати дослідження у зрозумілій і логічній формі. Вона складається з вступу, чотирьох основних розділів, висновків, списку використаної літератури та додатків. У першому розділі розглянуто теоретичні основи сканування IP адрес як інструменту захисту трафіку, включаючи методи аналізу та фільтрації. Другий розділ присвячений аналізу сучасних кіберзагроз і засобів їх запобігання, з акцентом на специфіку фінансових технологій. Третій розділ описує розробку моделі системи захисту трафіку, зокрема з використанням технологій машинного навчання для підвищення її ефективності. Четвертий розділ містить детальний опис програмної реалізації, а також результати експериментальних досліджень, проведених для оцінки її роботи. У висновках підведено підсумки виконаної роботи, проаналізовано досягнення мети та визначено перспективи подальших досліджень. Список використаної літератури налічує 35 джерел, серед яких наукові статті, регуляторні документи та практичні кейси. Додатки включають допоміжні матеріали, такі як схеми архітектури системи, фрагменти програмного коду та таблиці з результатами тестування, що доповнюють основний зміст роботи.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ АСПЕКТИ СКАНУВАННЯ IP-АДРЕС ДЛЯ ЗАХИСТУ ТРАФІКУ

1.1. Методи аналізу та моніторингу IP-адрес у мережі

Сканування IP-адрес є одним із фундаментальних методів забезпечення кібербезпеки в сучасних мережах, зокрема в контексті захисту трафіку. Цей процес передбачає систематичне дослідження мережевих вузлів із метою ідентифікації активних пристроїв, відкритих портів, а також потенційних вразливостей, які можуть бути використані зловмисниками. У фінансових технологіях, де захист даних і безперебійність роботи систем є критично важливими, аналіз і моніторинг IP-адрес стають основою для виявлення загроз у реальному часі та запобігання несанкціонованому доступу. Основна мета таких методів полягає в тому, щоб забезпечити повний контроль над мережевим трафіком і своєчасно реагувати на аномалії, які можуть свідчити про підготовку чи здійснення кібератаки [1].

Існує кілька ключових підходів до аналізу та моніторингу IP-адрес у мережі, кожен із яких має свої особливості та сфери застосування. Першим і найбільш поширеним є активне сканування, яке передбачає надсилання запитів до певного діапазону IP-адрес для отримання відповідей від активних хостів. Такі інструменти, як Nmap або Advanced IP Scanner, дозволяють не лише визначити, які IP-адреси активні, а й отримати інформацію про відкриті порти, операційні системи та служби, що працюють на пристроях [5]. Активне сканування широко застосовується для первинного аналізу мережі, однак його недоліком є те, що воно може бути виявлене системами виявлення вторгнень (IDS), оскільки генерує помітний трафік [3]. У фінансових системах, де важлива непомітність і безперервність роботи, активне сканування часто доповнюють пасивними методами [15].

Пасивний моніторинг IP-адрес ґрунтується на аналізі існуючого

мережевого трафіку без активного втручання в мережу. Цей підхід дозволяє відстежувати поведінку IP-адрес, не створюючи додаткового навантаження на систему. Наприклад, аналіз заголовків пакетів, отриманих через мережеві датчики чи системи типу Splunk, дає змогу виявляти аномалії, такі як незвичайно велика кількість запитів із однієї IP-адреси, що може вказувати на підготовку до DDoS-атаки [10]. Пасивний метод є особливо цінним у фінансових технологіях, де будь-яке втручання в трафік може вплинути на швидкість обробки транзакцій чи доступність сервісів для клієнтів. Водночас його ефективність залежить від якості зібраних даних і здатності алгоритмів розпізнавати загрози в реальному часі [13].

Ще одним важливим методом є використання геолокаційного аналізу IP-адрес, який дозволяє визначити фізичне розташування пристрою, що генерує трафік. У фінансовому секторі цей підхід часто застосовують для запобігання шахрайству: якщо IP-адреса користувача не відповідає його звичному місцезнаходженню, система може автоматично заблокувати доступ або вимагати додаткової аутентифікації [22]. Наприклад, банки використовують бази даних геолокації, такі як MaxMind чи IP2Location, для зіставлення IP-адрес із географічними координатами, що значно підвищує рівень безпеки онлайн-транзакцій [24]. Однак цей метод має обмеження, пов’язані з динамічним призначенням IP-адрес і використанням VPN-з’єднань зловмисниками, що ускладнює точну ідентифікацію [25].

Для підвищення ефективності моніторингу IP-адрес у мережах також застосовують технології машинного навчання. Такі системи здатні аналізувати великі обсяги даних про трафік, виявляти патерни поведінки та прогнозувати потенційні загрози на основі історичних даних. Наприклад, алгоритми кластеризації чи класифікації можуть ідентифікувати IP-адреси, які демонструють аномальну активність, навіть якщо вони не відповідають відомим сигнатурам атак [11]. У фінансових технологіях, де швидкість реакції на загрози є ключовою, інтеграція машинного навчання з методами сканування IP-адрес дозволяє створювати адаптивні системи захисту, які

здатні еволюціонувати разом із новими видами кібератак [16].

Важливим аспектом аналізу та моніторингу IP-адрес є вибір інструментів і технологій, які відповідають специфіці мережі. Наприклад, SolarWinds IP Address Manager забезпечує автоматизований моніторинг IP-адрес у корпоративних мережах, дозволяючи адміністраторам відстежувати їхній статус і виявляти неавторизовані підключення [2]. У той же час інструменти типу Angry IP Scanner є простішими у використанні та підходять для швидкого аналізу невеликих мереж [18]. У фінансових системах перевагу часто надають комплексним рішенням, таким як Palo Alto Networks чи Check Point, які поєднують сканування IP-адрес із функціями фільтрації трафіку та захисту від вторгнень [7, 9]. Вибір методу та інструменту залежить від розміру мережі, обсягу трафіку та рівня необхідної деталізації аналізу.

Таблиця 1.1

Основні методи аналізу та моніторингу IP-адрес у фінансових мережах

Метод аналізу	Опис	Переваги	Недоліки
1	2	3	4
Активне сканування	Надсилання запитів до діапазону IP-адрес для ідентифікації хостів, портів, ОС тощо	Висока деталізація результатів Швидке виявлення відкритих ресурсів	Генерує додатковий трафік. Може бути виявлене IDS
Пасивний моніторинг	Аналіз мережевого трафіку без прямого втручання; фіксація поведінки IP-адрес	Непомітність. Не впливає на продуктивність систем	Залежність від якості вхідних даних. Складність у налаштуванні
Геолокаційний аналіз	Визначення фізичного розташування пристрою за IP-адресою	Підвищення рівня аутентифікації. Попередження шахрайських транзакцій	Обхід можливий через VPN. Неточність через динамічні адреси
Машинне навчання	Використання моделей класифікації та кластеризації для виявлення аномальної активності	Адаптивність до нових загроз. Висока точність і масштабованість	Потреба в якісних даних. Складність інтеграції

Продовження таблиці 1.1

1	2	3	4
Інструментальні рішення	Застосування спеціалізованих програм і платформ для моніторингу IP-адрес	Автоматизація. Розширений функціонал захисту	Вартість ліцензій. Потреба в технічному обслуговуванні

Методи аналізу та моніторингу IP-адрес у мережі формують основу для захисту трафіку в сучасних інформаційних системах. Активне та пасивне сканування, геолокаційний аналіз і технології машинного навчання доповнюють одне одного, створюючи багатошаровий підхід до кібербезпеки. У контексті фінансових технологій ці методи набувають особливої ваги, адже дозволяють не лише виявляти загрози, а й забезпечувати безперебійність роботи систем і захист даних клієнтів від зовнішніх і внутрішніх ризиків [20]. Подальший розвиток цих методів має враховувати динамічність мережевих технологій і появу нових видів атак, що вимагає постійного вдосконалення інструментів і підходів до моніторингу.

1.2. Визначення потенційних загроз на основі сканування

Сканування IP-адрес відіграє ключову роль у процесі виявлення потенційних загроз у мережевому середовищі, особливо в системах фінансових технологій, де безпека даних і стабільність роботи є пріоритетними. Цей метод дозволяє не лише ідентифікувати активні пристрої та їх характеристики, а й аналізувати поведінку трафіку для своєчасного розпізнавання аномалій, які можуть свідчити про підготовку чи здійснення кібератаки. У сучасних умовах, коли зловмисники використовують дедалі складніші техніки, такі як розподілені атаки типу DDoS, фішинг або приховане сканування для розвідки, визначення загроз на основі сканування IP-адрес стає незамінним інструментом кібербезпеки [1]. У фінансовому секторі, де навіть незначний інцидент може призвести до втрати довіри клієнтів і значних

фінансових збитків, швидке виявлення загроз є критично важливим для забезпечення захисту інфраструктури [16].

Одним із основних напрямів визначення загроз є аналіз активності сканування з боку зовнішніх IP-адрес. Зловмисники часто застосовують техніки активного сканування для розвідки, намагаючись знайти вразливі порти, служби чи пристрої в мережі. Наприклад, згідно з MITRE ATT&CK, сканування IP-блоків є поширеною тактикою, яку використовують для ідентифікації потенційних цілей перед атакою [1]. Такі дії можуть проявлятися у вигляді великої кількості запитів до певного діапазону IP-адрес за короткий проміжок часу, що легко виявляється за допомогою інструментів типу Nmap чи SolarWinds IP Address Scanner [2, 5]. У фінансових системах подібна активність може вказувати на підготовку до атаки на платіжні шлюзи чи сервери онлайн-банкінгу, тому своєчасне виявлення таких спроб є першим кроком до їх нейтралізації [20]. Однак важливо враховувати, що активне сканування з боку зловмисників може бути замасковане під легітимний трафік, що ускладнює його розпізнавання без додаткових методів аналізу [28].

Іншим важливим аспектом є виявлення розподілених атак, таких як DDoS, які часто супроводжуються незвичайною активністю з боку множини IP-адрес. Сканування дозволяє ідентифікувати джерела такого трафіку, аналізуючи частоту запитів і їх розподіл у часі. Наприклад, система Splunk Lantern пропонує методику виявлення мережевого сканування через моніторинг патернів трафіку, що дає змогу розпізнати скоординовані дії кількох хостів [10]. У фінансових технологіях, де DDoS-атаки можуть призвести до тимчасової недоступності сервісів і значних репутаційних втрат, аналіз IP-адрес у реальному часі є ефективним способом раннього попередження [7]. Водночас динамічність призначення IP-адрес через використання проксі-серверів чи VPN може ускладнити точне визначення джерела загрози, що вимагає інтеграції сканування з іншими технологіями, такими як аналіз поведінки [25].

Сканування також дозволяє виявляти внутрішні загрози, які часто

залишаються поза увагою традиційних систем безпеки. Наприклад, неавторизований пристрій у мережі фінансової установи може бути ідентифікований через аналіз його IP-адреси та активності. Такі ситуації можуть виникати через підключення інфікованих пристроїв співробітників або через дії інсайдерів. Інструменти типу Check Point чи Palo Alto Networks здатні виявляти подібні аномалії, аналізуючи трафік і порівнюючи його з базовими профілями легітимної поведінки [9, 7]. У контексті фінансових технологій внутрішні загрози становлять особливу небезпеку, адже можуть призвести до витоку конфіденційної інформації, наприклад, даних клієнтів чи ключів шифрування [32]. Таким чином, сканування IP-адрес допомагає не лише захищати мережу від зовнішніх атак, а й забезпечувати контроль над внутрішньою інфраструктурою.

Геолокаційний аналіз IP-адрес є ще одним способом визначення потенційних загроз, особливо у сфері фінансових сервісів. Аномалії, пов’язані з географічним розташуванням IP-адрес, можуть свідчити про шахрайські дії, наприклад, спроби входу в систему з країн, де клієнт зазвичай не перебуває. За даними Spiceworks, фінансові установи активно використовують геолокацію для запобігання шахрайству, блокуючи доступ із підозрілих регіонів [22]. Однак цей метод має обмеження: зловмисники можуть маскувати своє місце розташування за допомогою VPN чи анонімізаторів, що знижує його ефективність без додаткового аналізу трафіку [24]. У таких випадках сканування доповнюють технологіями машинного навчання, які здатні виявляти патерни шахрайської поведінки незалежно від географічного фактора [11].

Для систематизації основних загроз, які можна виявити за допомогою сканування IP-адрес, наведено таблицю 1.1. Вона включає типи загроз, їхні ознаки в трафіку та методи виявлення, що застосовуються в сучасних системах кібербезпеки.

Таблиця 1.2

Основні загрози, виявлені на основі сканування IP-адрес

Тип загрози	Ознаки в трафіку	Метод виявлення	Особливості/Коментарі
Активне сканування	Велика кількість вхідних або вихідних запитів до різних IP-адрес на різні порти	Аналіз частоти запитів (інструменти: Nmap, Wireshark)	Часто фіксується IDS/IPS-системами; може бути першим етапом складної атаки
DDoS-атака	Раптове зростання обсягу трафіку з множини IP-джерел, що перевантажує сервери	Моніторинг розподілу трафіку, алерти аномальної активності (Splunk, Zabbix)	Потребує реакції в реальному часі; може маскувати інші шкідливі дії
Внутрішня загроза	Зміна звичних шаблонів трафіку: нові внутрішні IP, невластиві обсяги, нетипові запити	Порівняння з історичними профілями користувачів та пристроїв	Важко виявити без поведінкового аналізу; критично для фінансових установ з високим рівнем доступу
Шахрайство	Підозрілі з'єднання з IP-адрес регіонів, не властивих конкретному користувачу	Геолокаційний аналіз (MaxMind, IP2Location), автоматична перевірка	Часто виявляється в онлайн-банкінгу; застосовується як частина систем виявлення аномалій
Приховане сканування	Повільні, неперіодичні запити до обмеженого числа портів чи IP	Поведінковий аналіз, виявлення шаблонів (машинне навчання, ELK stack)	Важко виявити традиційними методами; ефективне використання AI/ML підходів до аналізу нетипової поведінки

Ця таблиця ілюструє, як сканування IP-адрес може бути адаптоване до різних типів загроз, що є актуальним для фінансових технологій. Наприклад, виявлення активного сканування допомагає запобігти розвідці перед атакою, тоді як аналіз геолокації захищає від шахрайських транзакцій [20].

Визначення потенційних загроз на основі сканування IP-адрес є багатогранним процесом, який охоплює аналіз зовнішніх і внутрішніх ризиків, а також враховує специфіку сучасних кібератак. Поєднання активного і пасивного сканування, геолокаційного аналізу та технологій машинного навчання дозволяє створювати комплексний підхід до захисту трафіку. У фінансових системах, де швидкість і точність реакції на загрози є вирішальними, ці методи забезпечують надійний захист від широкого спектра

атак, однак потребують постійного вдосконалення для адаптації до нових викликів, таких як використання зловмисниками анонімних мереж чи динамічних IP-адрес [13, 25]. Подальший розвиток цього напряму має фокусуватися на інтеграції сканування з інноваційними технологіями для підвищення його ефективності в умовах зростаючої складності кіберзагроз.

1.3. Використання чорних та білих списків IP-адрес

Використання чорних і білих списків IP-адрес є одним із найпоширеніших і водночас ефективних методів управління доступом і захисту мережевого трафіку в інформаційних системах. Цей підхід базується на класифікації IP-адрес за їхньою репутацією та поведінкою, що дозволяє швидко приймати рішення про блокування чи дозвіл доступу до мережі. У контексті фінансових технологій, де захист даних клієнтів і безперебійність роботи сервісів є пріоритетними, чорні та білі списки стають важливим елементом стратегії кібербезпеки. Вони забезпечують базовий рівень фільтрації трафіку, який може бути доповнений більш складними технологіями, такими як аналіз поведінки чи машинне навчання, але при цьому залишаються простим і зрозумілим інструментом для адміністраторів мереж [15]. Завдяки своїй універсальності цей метод застосовується як у невеликих системах, так і в масштабних інфраструктурах фінансових установ, де щоденно обробляються мільйони транзакцій [20].

Чорні списки IP-адрес створюються для ідентифікації та блокування джерел, які асоціюються з потенційними загрозами. Такі списки формуються на основі даних про попередні атаки, підозрілу активність чи інформацію від зовнішніх постачальників послуг кібербезпеки. Наприклад, IP-адреси, що беруть участь у DDoS-атаках, фішингових кампаніях або спробах несанкціонованого доступу, автоматично додаються до чорних списків для запобігання подальшій шкоді [7]. У фінансових системах цей підхід є особливо актуальним, адже дозволяє оперативно реагувати на відомі загрози без

необхідності детального аналізу кожного інциденту. Наприклад, за даними Palo Alto Networks, значна частина трафіку, пов’язаного з мережевим скануванням у хмарних середовищах, походить із IP-адрес, які вже внесені до чорних списків через їхню попередню активність [7]. Регуляторні органи, такі як FinCEN, також рекомендують фінансовим установам використовувати чорні списки для моніторингу підозрілої діяльності, включаючи IP-адреси у звіти про можливі порушення [21]. Однак ефективність чорних списків залежить від їхньої актуальності, адже зловмисники можуть швидко змінювати IP-адреси, використовуючи динамічні пули чи анонімізатори, що ускладнює підтримку списків у реальному часі [25].

Білі списки, на відміну від чорних, призначені для визначення довірених IP-адрес, яким дозволено доступ до мережі чи певних сервісів. Цей підхід базується на принципі "за замовчуванням заборонено", коли доступ надається лише заздалегідь перевіреним і авторизованим джерелам. У фінансових технологіях білі списки часто застосовуються для захисту критично важливих систем, таких як сервери обробки платежів чи бази даних клієнтів. Наприклад, банк може дозволити доступ до внутрішньої мережі лише з IP-адрес своїх філій чи відомих партнерів, блокуючи всі інші запити [22]. Такий метод значно знижує ризик внутрішніх і зовнішніх атак, адже навіть у разі компрометації облікових даних зловмисник не зможе підключитися з неавторизованої IP-адреси [32]. Водночас білі списки вимагають ретельного планування, адже помилкове виключення легітимних адрес може призвести до порушення роботи системи, особливо в умовах динамічного мережевого середовища, де користувачі часто підключаються через мобільні мережі чи VPN [24].

Реалізація чорних і білих списків у системах кібербезпеки фінансових технологій залежить від інструментів і технологій, які використовуються для їхнього створення та оновлення. Сучасні рішення, такі як SolarWinds IP Address Manager чи Check Point, дозволяють автоматизувати управління списками, інтегруючи їх із системами моніторингу трафіку [2, 9]. Наприклад, SolarWinds може автоматично додавати IP-адреси до чорного списку на основі

виявлених аномалій, таких як велика кількість запитів із однієї адреси за короткий час [2]. У той же час інструменти типу Angry IP Scanner підходять для швидкого сканування невеликих мереж і ручного формування списків у менших організаціях [18]. У фінансових установах перевагу надають комплексним системам, які поєднують чорні та білі списки з функціями фільтрації та аналізу в реальному часі, що підвищує їхню ефективність у боротьбі з кіберзагрозами [16].

Для ілюстрації практичного застосування чорних і білих списків у захисті трафіку можна навести такі приклади використання:

— Блокування IP-адрес, пов’язаних із відомими ботнетами, для запобігання DDoS-атакам на платіжні системи [10].

— Дозвіл доступу до серверів онлайн-банкінгу лише з IP-адрес корпоративної мережі банку, що знижує ризик фішингу [22].

— Автоматичне додавання до чорного списку IP-адрес, які сканують мережу для пошуку вразливостей, як це описано в MITRE ATT&CK [1].

— Обмеження доступу до API фінансових додатків лише для IP-адрес перевірених постачальників послуг, що захищає від несанкціонованих інтеграцій [20].

— Фільтрація трафіку з IP-адрес, зареєстрованих у країнах із високим рівнем кіберзлочинності, для запобігання шахрайству [24].

Ці приклади демонструють, як чорні та білі списки можуть бути адаптовані до різних сценаріїв у фінансових технологіях, забезпечуючи гнучкість і швидкість реагування на загрози. Проте використання цього методу має свої обмеження. Чорні списки можуть бути неефективними проти нових або невідомих загроз, адже вони базуються на попередньо виявлених джерелах небезпеки [28]. Наприклад, зловмисники, які використовують нові IP-адреси чи приховане сканування з низькою інтенсивністю, можуть залишатися непоміченими, доки їхня активність не буде зафіксована та внесена до списку [11]. Білі списки, своєю чергою, ускладнюють роботу в динамічних середовищах, де IP-адреси користувачів постійно змінюються,

наприклад, через використання мобільних мереж чи хмарних сервісів [25]. Крім того, підтримка актуальності списків вимагає значних ресурсів, особливо в масштабних системах, де щоденно генеруються тисячі нових IP-адрес [13].

Для подолання цих обмежень у фінансових технологіях чорні та білі списки часто інтегрують із системами машинного навчання та аналізу поведінки. Наприклад, алгоритми можуть автоматично оновлювати списки на основі виявлених патернів, таких як незвичайна частота запитів чи географічні аномалії, що підвищує їхню адаптивність до нових загроз [11]. Регуляторні вимоги, такі як стандарти FDIC чи директиви ЄС, також наголошують на необхідності комбінування списків із іншими методами захисту для забезпечення комплексного підходу до кібербезпеки [31, 34]. Таким чином, чорні та білі списки залишаються базовим, але не єдиним інструментом у системі захисту трафіку.

Використання чорних і білих списків IP-адрес є простим і дієвим способом управління доступом і захисту мережевого трафіку в фінансових технологіях. Вони дозволяють швидко блокувати відомі загрози та забезпечувати доступ лише для довірених джерел, що є особливо важливим у сфері, де будь-який інцидент може мати серйозні наслідки. Незважаючи на певні обмеження, такі як складність оновлення чи вразливість до нових атак, цей метод залишається невід’ємною частиною кібербезпеки завдяки своїй доступності та ефективності. Подальший розвиток цього підходу має враховувати інтеграцію з інноваційними технологіями, щоб адаптувати його до динамічного характеру сучасних кіберзагроз і потреб фінансових систем [16].

1.4. Алгоритми фільтрації та блокування підозрілих IP

Алгоритми фільтрації та блокування підозрілих IP-адрес є ключовим елементом систем захисту мережевого трафіку, особливо в умовах зростання кіберзагроз у фінансових технологіях. Ці алгоритми призначені для аналізу

трафіку, виявлення аномалій і автоматичного або ручного обмеження доступу з IP-адрес, які становлять потенційну небезпеку. У фінансових системах, де швидкість реакції на загрози може визначати збереження даних клієнтів і стабільність роботи сервісів, такі алгоритми відіграють вирішальну роль у запобіганні атакам, таким як DDoS, фішинг чи несанкціонований доступ [16]. Їх ефективність залежить від точності аналізу, здатності адаптуватися до нових типів загроз і рівня інтеграції з іншими компонентами системи кібербезпеки, такими як чорні та білі списки чи системи виявлення вторгнень [15]. У сучасних умовах ці алгоритми дедалі частіше доповнюються технологіями машинного навчання, що дозволяє підвищувати їх точність і знижувати кількість помилкових спрацьовувань [11].

Одним із базових підходів до фільтрації та блокування є використання правил на основі сигнатур. Цей метод передбачає порівняння трафіку з IP-адрес із відомими шаблонами атак, які зберігаються в базі даних сигнатур. Наприклад, якщо IP-адреса генерує велику кількість запитів до певного порту за короткий час, це може бути розпізнано як спроба сканування мережі, і алгоритм автоматично блокує таке джерело [1]. Такі системи, як Fortinet Intrusion Prevention System (IPS), широко застосовують сигнатурний аналіз для захисту від відомих загроз, таких як експлойти чи спроби переповнення буфера [12]. У фінансових технологіях цей підхід дозволяє швидко нейтралізувати атаки, про які вже є інформація, наприклад, із баз MITRE ATT&CK чи інших джерел кіберрозвідки [1]. Однак сигнатурний метод має суттєвий недолік: він неефективний проти нових або невідомих атак, які не мають зафіксованих сигнатур, що робить його вразливим у динамічному середовищі кіберзагроз [28].

Для подолання цього обмеження застосовуються алгоритми на основі аналізу поведінки. Ці алгоритми відстежують нормальну поведінку трафіку в мережі та виявляють відхилення, які можуть свідчити про підозрілу активність. Наприклад, якщо IP-адреса, яка зазвичай генерує незначний обсяг запитів, раптово починає надсилати тисячі пакетів за секунду, це може бути

підставою для її блокування [10]. Такі рішення, як Splunk Lantern чи Palo Alto Networks, використовують аналіз поведінки для ідентифікації аномалій у реальному часі, що особливо корисно для захисту від розподілених атак, таких як DDoS [7, 10]. У фінансових системах, де навіть короткочасна недоступність сервісу може призвести до значних втрат, поведінковий аналіз дозволяє оперативно реагувати на загрози, навіть якщо вони не відповідають відомим сигнатурам [20]. Проте цей метод вимагає ретельного налаштування, щоб уникнути помилкового блокування легітимного трафіку, наприклад, під час пікових навантажень на платіжні системи [25].

Ще одним поширеним підходом є алгоритми, засновані на геолокаційному фільтруванні. Ці алгоритми аналізують географічне розташування IP-адрес і блокують трафік із регіонів, які не відповідають очікуваній поведінці користувачів чи мають високу репутацію кіберзлочинності. У фінансових технологіях геолокація часто використовується для захисту від шахрайства: якщо клієнт зазвичай підключається з України, а раптово з’являється запит із іншої країни, система може автоматично заблокувати таку IP-адресу [22]. За даними Spiceworks, банки активно застосовують цей метод для фільтрації трафіку, використовуючи бази геолокації, такі як MaxMind, для зіставлення IP-адрес із фізичними координатами [22]. Однак зловмисники можуть обходити геолокаційне блокування за допомогою VPN чи проксі-серверів, що знижує ефективність цього підходу без додаткового аналізу [24]. Тому в сучасних системах геолокація часто комбінується з іншими методами для підвищення точності.

Алгоритми машинного навчання стають дедалі популярнішими для фільтрації та блокування підозрілих IP-адрес завдяки їхній здатності адаптуватися до нових загроз. Такі алгоритми, як кластеризація чи нейронні мережі, аналізують історичні дані про трафік і створюють моделі нормальної поведінки, на основі яких виявляють аномалії. Наприклад, дослідження, опубліковане в MDPI, показує, що алгоритми машинного навчання можуть

ідентифікувати приховане сканування з низькою інтенсивністю, яке важко виявити традиційними методами [11]. У фінансових системах ці технології дозволяють прогнозувати загрози, такі як підготовка до фішингової атаки, і блокувати IP-адреси ще до того, як вони завдадуть шкоди [16]. Хоча впровадження машинного навчання потребує значних обчислювальних ресурсів і якісних даних для навчання, його переваги в точності та гнучкості роблять його незамінним у боротьбі з новими видами кібератак [13].

Для систематизації основних алгоритмів фільтрації та блокування підозрілих IP-адрес наведено таблицю 1.2, яка описує їхні характеристики, переваги та недоліки.

Таблиця 1.3

Основні алгоритми фільтрації та блокування підозрілих IP-адрес

Алгоритм	Опис	Переваги	Недоліки	Приклади застосування
1	2	3	4	5
Сигнатурний аналіз	Порівняння вхідного/вихідного трафіку з базою відомих атак (сигнатур)	Висока точність для вже відомих загроз. Швидке реагування	Не виявляє нові, раніше невідомі атаки. Потребує регулярного оновлення баз	IDS/IPS системи: Snort, Suricata
Аналіз поведінки	Виявлення відхилень від нормальної поведінки користувачів або пристроїв у мережі	Адаптація до нових атак. Може ідентифікувати внутрішні загрози	Можливі хибнопозитивні спрацювання. Необхідна історія активності для побудови нормальних профілів	SIEM-системи: IBM QRadar, Splunk
Геолокаційне фільтрування	Обмеження або блокування трафіку за географічною ознакою (по IP-локації)	Ефективний захист від транскордонного шахрайства. Швидке впровадження	VPN і проксі можуть приховати справжнє місцезнаходження. Ризик обмеження легітимного трафіку	Антифрод-системи в онлайн-банкінгу: MaxMind, ThreatMetrix

Продовження таблиці 1.3

1	2	3	4	5
Машинне навчання	Використання моделей класифікації/кластеризації для прогнозування шкідливої активності	Висока точність і здатність до навчання. Підтримка виявлення нових атак	Високі вимоги до обчислювальних ресурсів. Потреба у великій кількості навчальних даних	Anomaly Detection Systems: Darktrace, Vectra AI

В таблиці продемонстровано різноманітність підходів до фільтрації та блокування IP-адрес, що дозволяє вибирати оптимальний алгоритм залежно від потреб системи. Наприклад, сигнатурний аналіз підходить для швидкого реагування на відомі загрози, тоді як машинне навчання ефективне для прогнозування нових атак [20].

Практична реалізація цих алгоритмів у фінансових технологіях часто здійснюється через спеціалізовані інструменти. Наприклад, Check Point пропонує інтегровані рішення, які поєднують сигнатурний аналіз і поведінкову фільтрацію для захисту від мережевих атак [9]. SolarWinds IP Address Manager дозволяє налаштовувати правила блокування на основі геолокації та частоти запитів [2]. У той же час системи типу Darktrace використовують машинне навчання для автоматичного блокування підозрілих IP-адрес у реальному часі, що є особливо цінним для захисту хмарних фінансових сервісів [16]. Вибір алгоритму залежить від специфіки системи, обсягу трафіку та рівня автоматизації, якого необхідно досягти [18].

Алгоритми фільтрації та блокування підозрілих IP-адрес формують багатошаровий захист мережевого трафіку, який є необхідним у фінансових технологіях. Кожен із них – сигнатурний аналіз, аналіз поведінки, геолокаційне фільтрування та машинне навчання – має свої сильні та слабкі сторони, що вимагає їхнього комбінування для досягнення максимальної ефективності. Незважаючи на виклики, такі як обхід блокування через анонімні мережі чи потреба в ресурсах для складних алгоритмів, ці методи

забезпечують надійний захист від широкого спектра загроз [25]. Подальший розвиток цього напряму має фокусуватися на інтеграції алгоритмів із сучасними технологіями та підвищенні їхньої адаптивності до нових умов кіберпростору [13].

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ ЗАГРОЗ І ЗАСОБІВ ЗАХИСТУ ТРАФІКУ

2.1. Основні загрози кібербезпеки, пов’язані з IP-трафіком

Сучасний мережевий трафік, який базується на використанні IP-адрес, є основою функціонування інформаційних систем, зокрема у сфері фінансових технологій. Проте саме через IP-трафік реалізується значна частина кіберзагроз, які становлять небезпеку для конфіденційності, цілісності та доступності даних. У фінансовому секторі, де обробляються чутливі дані клієнтів і здійснюються транзакції на мільйони доларів, загрози, пов’язані з IP-трафіком, можуть призводити до катастрофічних наслідків, таких як фінансові втрати, репутаційні збитки чи порушення регуляторних вимог [16]. Розуміння основних типів таких загроз є необхідною умовою для розробки ефективних засобів захисту, адже IP-адреси виступають як ідентифікатори джерел і цілей атак, а також як ключові елементи аналізу мережевої активності [1]. У цьому контексті аналіз сучасних загроз дозволяє не лише оцінити їхній вплив, а й визначити напрями вдосконалення систем кібербезпеки.

Однією з найпоширеніших загроз, пов’язаних з IP-трафіком, є розподілені атаки типу DDoS (Distributed Denial of Service). Ці атаки спрямовані на перевантаження мережевих ресурсів шляхом надсилання великої кількості запитів із множини IP-адрес, що часто належать ботнетам. У фінансових технологіях DDoS-атаки можуть призвести до тимчасової недоступності онлайн-банкінгу чи платіжних систем, що завдає шкоди як клієнтам, так і установам. За даними Palo Alto Networks, значна частина таких атак у хмарних середовищах пов’язана з масовим скануванням IP-адрес для пошуку вразливих точок входу, після чого зловмисники координують трафік із тисяч джерел [7]. Виявлення таких загроз ускладнюється через використання зловмисниками динамічних IP-адрес і проксі-серверів, що робить традиційні методи блокування менш ефективними [25]. У 2024 році

кількість DDoS-атак на фінансові установи зросла на 15% порівняно з попереднім роком, що свідчить про їх актуальність і потребу в розробці нових засобів протидії [20].

Ще однією серйозною загрозою є фішинг, який часто використовує IP-трафік для доставки шкідливого контенту чи обману користувачів. Зловмисники можуть надсилати підроблені запити з IP-адрес, які видають себе за легітимні сервери, щоб отримати доступ до облікових даних чи фінансової інформації. Наприклад, у фінансових системах фішингові атаки часто спрямовані на клієнтів онлайн-банкінгу, де користувачів перенаправляють на фальшиві сайти через маніпуляцію трафіком [24]. За даними Spiceworks, банки дедалі частіше стикаються з такими атаками, коли IP-адреси зловмисників маскуються під довірені джерела, що ускладнює їхнє виявлення без геолокаційного аналізу чи поведінкового моніторингу [22]. Регуляторні органи, такі як FinCEN, зазначають, що інформація про IP-адреси має включатися до звітів про підозрілу діяльність, щоб полегшити відстеження таких інцидентів [21]. Ця загроза є особливо небезпечною через її соціальну інженерію, яка доповнює технічні аспекти використання IP-трафіку.

Активне сканування мережі зловмисниками також становить значну загрозу, пов’язану з IP-трафіком. Цей процес, описаний у MITRE ATT&CK, передбачає систематичне надсилання запитів до діапазону IP-адрес для ідентифікації активних хостів, відкритих портів і вразливостей [1]. У фінансових технологіях таке сканування часто є підготовчим етапом до більш складних атак, наприклад, експлуатації слабких місць у серверах чи додатках. Інструменти типу Nmap, які використовуються як легітимними адміністраторами, так і зловмисниками, дозволяють швидко зібрати інформацію про мережу, що робить цю загрозу складною для раннього виявлення [5]. Наприклад, дослідження показують, що сканування IPv6-простору дедалі частіше застосовується для пошуку незахищених пристроїв у фінансових системах, що пов’язано з розширенням використання цього протоколу [14]. Виявлення такого сканування вимагає постійного моніторингу

трафіку та аналізу частоти запитів із окремих IP-адрес [10].

Внутрішні загрози, пов’язані з IP-трафіком, також не можна ігнорувати, адже вони становлять значний ризик для фінансових установ. Такі загрози можуть виникати через підключення інфікованих пристроїв співробітників до мережі або через дії інсайдерів, які використовують IP-адреси для передачі конфіденційної інформації за межі організації. Наприклад, компрометація внутрішньої IP-адреси може призвести до витоку даних клієнтів чи порушення роботи платіжних систем [32]. Системи типу Check Point здатні виявляти такі аномалії, аналізуючи трафік і порівнюючи його з нормальними патернами поведінки [9]. У фінансових технологіях внутрішні загрози є особливо небезпечними через їх прихований характер і складність ідентифікації без інтеграції сканування IP-адрес із системами контролю доступу [20].

Шахрайство, пов’язане з маніпуляцією IP-трафіком, є ще однією актуальною загрозою у фінансовому секторі. Зловмисники можуть використовувати IP-адреси для маскування своєї активності, наприклад, через VPN чи анонімні мережі типу Tor, щоб здійснювати несанкціоновані транзакції чи обходити системи аутентифікації. За даними Medium, маніпуляція IP-адресами дозволяє шахраям створювати ілюзію легітимності, що ускладнює їхнє виявлення банківськими системами [25]. PYMNTS.com зазначає, що традиційні методи перевірки IP-адрес у банках часто неефективні через динамічність сучасних мереж і потребують доповнення іншими технологіями, такими як аналіз поведінки чи машинне навчання [24]. Ця загроза є особливо актуальною в умовах зростання популярності мобільних фінансових додатків, де користувачі підключаються з різних IP-адрес, що ускладнює розрізнення легітимного трафіку від шахрайського [22].

Таблиця 2.1

Основні загрози кібербезпеки, що реалізуються через IP-трафік у фінансових системах

Тип загрози	Опис	Вплив на фінансові технології	Методи виявлення та протидії	Особливості/Ускладнення
DDoS-атака	Масове перевантаження мережевих ресурсів за допомогою запитів із багатьох IP-адрес	Порушення доступу до сервісів (інтернет-банкінг, платіжні шлюзи), фінансові втрати	IDS/IPS, фільтрація трафіку, аналіз частоти запитів, хмарні анти-DDoS сервіси	Динамічні IP-адреси, проксі та ботнети ускладнюють блокування
Фішинг через IP	Використання шкідливих IP для перенаправлення на фальшиві ресурси	Викрадення облікових даних, компрометація клієнтів, шахрайські транзакції	Геолокаційний аналіз, поведінкове моделювання, верифікація через багатофакторну аутентифікацію	Складність виявлення через маскування під легітимні домени й IP
Активне сканування	Систематичне надсилання запитів до IP-адрес з метою виявлення відкритих портів і вузлів	Ідентифікація вразливих сервісів, підготовка до вторгнення	Аналіз частоти запитів, моніторинг портів, мережеві honeypots	Може використовуватись легально, що ускладнює виявлення зловмисної активності
Внутрішні загрози	Зловмисні дії або недбалість працівників у межах корпоративної мережі	Передача конфіденційних даних, підключення незареєстрованих пристроїв	Контроль доступу, поведінковий аналіз, інтеграція сканерів IP з SIEM-системами	Високий рівень прихованості, часто маскується під штатну активність
IP-шахрайство	Маскування IP-адрес через VPN/Tor для обходу перевірок і здійснення шахрайських дій	Несанкціоновані транзакції, обхід регіональних обмежень, компрометація клієнтських даних	Геолокаційне фільтрування, сигнатурний аналіз, алгоритми ML	VPN-з’єднання й динамічне призначення IP знижують точність ідентифікації

Основні загрози кібербезпеки, пов’язані з IP-трафіком, включають DDoS-атаки, фішинг, активне сканування, внутрішні загрози та шахрайство. Кожна з них має свої особливості та впливає на безпеку фінансових технологій по-різному, але всі вони використовують IP-адреси як ключовий елемент реалізації. Наприклад, DDoS-атаки перевантажують системи масовим трафіком, тоді як фішинг і шахрайство зосереджені на обманному отриманні даних [7, 24]. Виявлення цих загроз вимагає комплексного підходу, який поєднує моніторинг IP-трафіку, аналіз поведінки та використання сучасних технологій захисту [11]. У фінансових системах, де будь-який інцидент може мати далекосяжні наслідки, розуміння цих загроз є першим кроком до створення ефективних засобів їх нейтралізації. Подальший аналіз має враховувати еволюцію кібератак і розробку адаптивних рішень для захисту IP-трафіку в умовах цифрової трансформації [13].

2.2. Огляд сучасних атак через IP-сканування

У сучасних умовах кіберзагроз IP-сканування перетворилося з простого інструменту адміністративного обслуговування мережі на активний компонент атакового ланцюга, що використовується зловмисниками на ранніх та пізніх етапах вторгнення. В основі більшості сучасних кібератак лежить процес збору первинної інформації, у якому IP-сканування відіграє ключову роль. Завдяки широкому спектру відкритих та комерційних сканерів — таких як Nmap, Masscan, ZMap, Shodan, Censys — зловмисники можуть за лічені хвилини охопити великі ділянки адресного простору, отримуючи детальні дані про мережеву інфраструктуру жертви. У випадку з фінансовими організаціями це особливо критично, оскільки системи доступу до банківських API, бухгалтерських серверів, шлюзів мобільного банкінгу часто розміщуються на зовнішньодоступних IP-адресах для забезпечення клієнтського доступу. Під час атаки сканування дозволяє визначити, які саме вузли відповідають на запити, які порти відкриті, які служби працюють, яку версію операційної

системи або веб-сервера вони використовують — і все це без встановлення повноцінного з'єднання. Згідно з дослідженням [6], середньостатистична цільова атака починається з попереднього сканування за 3–5 днів до безпосереднього вторгнення, що дозволяє зловмисникам підготувати точкові експлойти. Це підтверджує і звіт компанії Trustwave, в якому зазначено, що у понад 80% інцидентів порушення безпеки виявлено фази сканування з відомих масових ботнетів ще до основної атаки [7].

Особливу загрозу становить масове сканування у хмарних середовищах, де адреси є публічними, а сервери часто конфігуруються автоматизовано, без ручної перевірки налаштувань. Як зауважує Palo Alto Networks [8], у середовищах AWS або Azure часто спостерігається доступність портів до Elasticsearch, MongoDB або Redis, які зловмисники шукають через IP-сканування і миттєво експлуатують для зливу або підміни даних. Така експлуатація часто є безфайловою, що дозволяє уникнути класичних сигнатурних методів виявлення. Ці дані підкріплює досвід компанії Imperva, яка фіксувала середнє навантаження понад 50 сканувань на годину в межах одного фінансового датацентру, з яких 30% — з IP, прив’язаних до мереж Tor або анонімних проксі [9]. Важливо відзначити, що за допомогою комбінації сканування портів, виявлення служб і OS fingerprinting зловмисник може скласти повну топологічну карту мережі організації, що дозволяє підготувати гібридну атаку — наприклад, скомбінувати SQL-ін’єкцію на фронтенді з атакою на неоновлений FTP або RDP-сервер на бекенді.

Критичність проблеми сканування полягає також у тому, що навіть організації, які використовують IDS/IPS, не завжди мають достатньо налаштовані профілі виявлення для повільного або комбінованого сканування. Наприклад, так звані stealth-сканування, які застосовують неповні TCP-пакети або порушення послідовності запитів, можуть проходити повз прості фільтри й виявляти сервіси з відкладеною реакцією. Це підтверджується у звіті компанії Rapid7, згідно з яким 41% атак у 2023 році на фінансові сервіси розпочиналися з неповного або low-rate сканування, що дозволяло залишитися

невидимим протягом кількох годин або днів [10]. Особливо небезпечними є атаки, які поєднують сканування з автоматичними експлойтами через API-з'єднання: зафіксовано випадки, коли сканування одночасно шукало відкриті інтерфейси Jenkins або GitLab і миттєво запускало шкідливий контейнер на виявленому ресурсі [11]. Такі атаки є прикладом так званої «активної розвідки» з негайним зловживанням.

Варто враховувати, що сучасне сканування — це вже не лише інструмент атаки з боку хакерських угруповань. Сканери, що працюють на основі штучного інтелекту, дають змогу класифікувати відповіді з хостів за поведінковими шаблонами, розрізняти honeypots і реальні вузли, а також виявляти динамічні зміни в конфігураціях систем, наприклад, зміну версії веб-сервера чи відкриття порту лише на короткий проміжок часу [12]. Це означає, що фінансові організації повинні постійно оновлювати свої методи виявлення сканувань, використовуючи поєднання сигнатурного аналізу, геолокаційного фільтрування та технологій машинного навчання. Як відзначає Cybersecurity and Infrastructure Security Agency (CISA), найефективнішими є інструменти, які інтегрують сканування з аналізом повного трафіку на рівні L3–L7, включаючи історичний та поведінковий компоненти [13].

У контексті подальшого розвитку загроз, важливим вектором є зростання використання IPv6, який відкриває нові можливості для прихованого сканування через більший адресний простір та складніші структури адресації. Дослідження Google Cloud [14] показує, що зростає частка атак, які починаються з точкового IPv6-сканування за специфічними шаблонами адрес корпоративного класу. Враховуючи слабке покриття IPv6-сегментів більшістю сучасних IDS/IPS, це створює значну прогалину у виявленні. На цьому фоні фіксується активізація складних багаторівневих атак, коли сканування використовується як компонент розподіленої системи ухилення від фільтрів. Наприклад, сканування запускається одночасно з різних країн і часових поясів, і лише при виявленні ключових вразливостей — наприклад, на вебінтерфейсі шлюзу платіжної системи — запускається

основна атака з завантаженням шкідливого коду [15].

Таблиця 2.2

Типологія сучасних атак, які реалізуються через IP-сканування

Тип атаки	Ціль сканування	Технічна реалізація	Супровідні інструменти	Ризики для фінансових систем
Port scanning	Виявлення відкритих портів	TCP SYN, ACK, Xmas, FIN, Null scans	Nmap, Masscan, ZMap	Виявлення точок входу в інфраструктуру
Vulnerability enumeration	Виявлення відомих вразливостей за відкритими службами	Сканування з CVE-базами, автоматичне порівняння	Nessus, OpenVAS, Shodan	Атака на незахищене ПЗ або вебсервери
OS fingerprinting	Ідентифікація ОС/сервісів для подальшої експлуатації	TTL, TCP/IP stack deviation	p0f, Xprobe2	Використання специфічних експлойтів під ОС
Behavioral scan + AI-analysis	Сканування реакцій вузлів для розпізнавання поведінки	Аналіз таймінгів, зміна відповіді при різних послідовностях	AI-системи, Shodan enhanced	Визначення honeypot-ів, евазія традиційних захистів
Hybrid scan & injection	Одночасне сканування і запуск експлойта через API	Сканування інтерфейсів (Jenkins, GitLab, Redis) + payload-injection	Censys, Burp Suite	Швидке зараження без підготовчої фази, особливо небезпечно для мікросервісів

IP-сканування перестало бути простою утилітарною дією, пов’язаною з діагностикою мереж. Воно еволюціонувало в структуровану і високотехнологічну фазу кібератак, яка часто передує основному вторгненню. Сучасні сканери не лише виявляють наявність відкритих портів чи служб, але й використовують машинне навчання для класифікації отриманих відповідей, визначення потенційно вразливих вузлів та розпізнавання активності захисних систем. Сканування в поєднанні з геодинамічними атаками (розподіленими за місцем і часом), із залученням проксі-серверів, VPN, ботнетів і навіть легітимних публічних інструментів, дозволяє зловмиснику діяти з високою точністю й мінімальною виявлюваністю.

У фінансових технологіях, де обсяг щоденних транзакцій обчислюється

мільйонами доларів, будь-яке втручання у критичні вузли інфраструктури — це ризик порушення доступності сервісів, втрати конфіденційних даних або прямого шахрайства. IP-сканування дозволяє зловмисникам ідентифікувати слабкі місця в онлайн-банкінгу, платіжних шлюзах, сервісах управління клієнтами та навіть у внутрішніх CRM-системах, особливо якщо вони доступні через хмарні канали. Точкове виявлення незахищених служб (наприклад, відкритий порт Redis чи Elasticsearch) може завершитися атаками типу data exfiltration або інжекцією шкідливого коду в середовища реального часу.

Ефективна протидія таким атакам не зводиться лише до блокування портів або використання фаєрволів. Вона вимагає багаторівневої стратегії, яка охоплює:

– Цілодобовий моніторинг усього IP-трафіку з використанням гібридних SIEM-рішень;

– Використання поведінкової аналітики, що здатна ідентифікувати навіть ті дії, які не підпадають під традиційні сигнатури;

– Регулярне оновлення баз вразливостей, включаючи CVE та експлойти, що активно використовуються в Darknet;

– Інтеграцію геолокаційного контролю для аналізу джерел сканування та виявлення регіонально нетипового трафіку;

– Машинне навчання та штучний інтелект як засоби динамічного виявлення аномалій і попереджувального реагування;

– Активне логування з інтерпретацією історичних шаблонів активності, що дозволяє розпізнавати повільні або stealth-атаки, які імітують нормальний трафік.

В умовах цифрової трансформації фінансового сектора, де кожна система підключена до зовнішнього середовища і оперує критично важливою інформацією, сканування IP-адрес не просто загроза, а невід’ємна частина ландшафту сучасної кіберзлочинності. Відповідно, інститути кібербезпеки повинні переосмислювати політику реагування, рухаючись від реактивної

моделі (виявлення та нейтралізація факту атаки) до прогностичної — з випереджувальним виявленням потенційних векторів проникнення. Це вимагає не лише технічного переозброєння, а й перепідготовки персоналу, інвестицій у аналітику трафіку, автоматизацію кіберзахисту та впровадження Zero Trust моделей у архітектуру всієї мережевої взаємодії.

IP-сканування, як точка входу до багатьох кібератак, потребує комплексної, аналітично підкріпленої та проактивної відповіді, без якої фінансові структури залишаються вразливими до нових хвиль високоточних, автоматизованих і координаційно складних атак.

2.3. Аналіз сучасних систем захисту мережевого трафіку

Сучасні системи захисту мережевого трафіку є ядром архітектури кібербезпеки, особливо в галузі фінансових технологій, де критичність інформації, транзакцій і комунікацій досягає максимально високого рівня. В епоху цифрової трансформації, коли кожен бізнес-процес інтегрується у внутрішні та зовнішні цифрові платформи, ефективний контроль і фільтрація мережевого трафіку визначають не просто технічну захищеність підприємства, а й його стійкість до системних ризиків, регуляторну відповідність і загальну довіру клієнтів. Сучасні системи захисту трафіку функціонують не як ізольовані елементи, а як багаторівневі, адаптивні, самонавчальні комплекси, здатні до активного втручання у потокові дані, виявлення та нейтралізації аномалій у реальному часі.

На перших рівнях структури безпеки використовується глибока перевірка пакетів (Deep Packet Inspection — DPI), яка дозволяє аналізувати не лише заголовки, а й вміст кожного пакета, незалежно від протоколу або порту. DPI-технології виявляють невідповідності, приховані команди, впроваджений шкідливий код, спроби тунелювання трафіку в легітимних каналах та інші деструктивні дії. Проте DPI потребує високої продуктивності апаратного забезпечення та оптимізованого алгоритмічного забезпечення, оскільки кожен

байт трафіку підлягає глибокому аналізу. У фінансових системах DPI інтегрується у шлюзи безпеки на рівні банківських центрів обробки даних, зокрема при роботі з мобільним трафіком, API-фінансовими сервісами, та в інфраструктурах, які обслуговують платіжні процесори.

Більш гнучким і комплексним інструментом є системи типу NGFW (Next-Generation Firewall), які поєднують класичне фільтрування трафіку з можливістю ідентифікації додатків, перевіркою SSL/TSL, інтеграцією з базами шкідливих IP-адрес, облікових записів і доменів. Вони використовують як сигнатурний аналіз, так і поведінкове виявлення загроз, що дозволяє адаптуватися до динамічної природи сучасного трафіку. У системах NGFW також застосовуються функції sandboxing — віртуального запуску файлів і трафікових сесій у контрольованому середовищі для спостереження за їхньою поведінкою. Завдяки цьому навіть невідомі загрози, які ще не мають сигнатур, можуть бути виявлені через аналіз їх динаміки.

Окремим класом захисних рішень є системи запобігання вторгненням (IPS — Intrusion Prevention Systems), які реалізують проактивну фільтрацію. Вони не лише виявляють шкідливу активність на основі сигнатур чи евристичних правил, а й автоматично блокують трафік, що відповідає потенційній загрозі. У фінансових установах IPS часто інтегруються з SIEM-платформами, які забезпечують централізовану кореляцію подій і логів у масштабах всієї мережі. Це дозволяє не тільки оперативно реагувати на інциденти, а й формувати аналітичні моделі поведінки, на основі яких система навчиться ідентифікувати навіть складні атаки на рівні взаємозв’язків між сесіями, джерелами, географією та часом активності.

Ще одним елементом сучасного підходу до захисту трафіку є технології машинного навчання, які у вигляді окремих рішень або як функціональний модуль інтегруються в комплексні системи. Вони дозволяють будувати моделі нормального трафіку (baseline), на основі яких виявляються відхилення, що можуть свідчити про зловмисну активність, навіть якщо вона не є типовою атакою. Наприклад, якщо певна IP-адреса починає здійснювати запити в

невластиві години, з нетиповими параметрами, або ж відбувається відхилення у географічному шаблоні запитів користувача — система здатна автоматично класифікувати таку поведінку як аномальну. Такі підходи широко використовуються у фінансових хмарах, мобільному банкінгу, платіжних сервісах, де величезна кількість клієнтських транзакцій вимагає не лише швидкої, а й адаптивної фільтрації.

Комплексна ефективність систем захисту трафіку значно підвищується за рахунок інтеграції в екосистему інформаційної безпеки: фаєрволи, IPS, DLP, SIEM, мережеві сканери, системи контролю доступу (NAC), інструменти моніторингу активності користувачів (UEBA) утворюють цілісну динамічну архітектуру. Це дозволяє реалізувати принцип «глибокого захисту» (defense in depth), за якого навіть якщо один рівень захисту не виявить загрозу, вона буде виявлена наступними механізмами.

Зокрема, у фінансових установах сьогодні активно використовуються рішення таких вендорів як Palo Alto Networks, Fortinet, Cisco, Check Point, які пропонують повний стек захисту трафіку на рівні 2–7 моделі OSI. У поєднанні з локальними політиками доступу, геофільтрацією, фільтрацією контенту, багатофакторною автентифікацією та Zero Trust-архітектурою вони створюють умови для мінімізації впливу навіть високоточних цільових атак.

Таблиця 2.3

Характеристика сучасних систем захисту мережевого трафіку

Тип системи	Основне призначення	Переваги застосування	Обмеження/ризики
1	2	3	4
DPI (Deep Packet Inspection)	Глибокий аналіз вмісту пакетів на всіх рівнях протоколу	Точне виявлення шкідливого коду, нелегального контенту, тунелювання	Високе навантаження на ресурси, можливі затримки при великому обсязі трафіку
NGFW (Next-Generation Firewall)	Інтегроване фільтрування за портами, додатками, IP-адресами, SSL/TSL	Гнучкість, інтеграція з хмарними сервісами, поведінковий контроль	Висока вартість, складність налаштування, потреба в актуалізації сигнатур

Продовження таблиці 2.3

1	2	3	4
IPS (Intrusion Prevention System)	Запобігання вторгненням і шкідливим діям у мережі	Проактивна фільтрація, взаємодія з SIEM, блокує в реальному часі	Можливі хибнопозитивні спрацювання, обхід при складних атаках
ML-засновані системи (AI/UEBA)	Автоматичне виявлення аномалій у поведінці користувачів та пристроїв	Адаптивність, здатність виявляти нові, неописані загрози	Висока складність імплементації, потреба в навчальних вибірках, ризик надмірної чутливості
SIEM/UEBA/Orchestration	Централізований збір, аналіз і кореляція подій з усіх джерел	Повна картина подій у мережі, автоматичне реагування, історичний аналіз	Висока складність налаштування, потреба в персоналі з високою кваліфікацією

Сучасний захист мережевого трафіку — це не статична система, а динамічна, самонавчальна й масштабована структура, що має діяти на випередження. В умовах фінансових технологій, де кожна сесія, кожен запит і кожен байт даних може нести критичну вагу, саме здатність системи адаптуватися, розпізнавати контексти та діяти у режимі реального часу визначає її ефективність. Перевага мають ті рішення, які не просто реагують на відомі патерни атак, а передбачають їх розвиток і здатні виявляти загрози ще до того, як вони реалізують свій руйнівний потенціал.

2.4. Огляд стандартів та технологій безпеки

Забезпечення безпеки мережевого трафіку в сучасних інформаційних системах, зокрема у фінансових технологіях, вимагає не лише використання передових технологій, а й дотримання міжнародних і національних стандартів кібербезпеки. Стандарти безпеки встановлюють рамки для розробки, впровадження та оцінки систем захисту, гарантуючи їхню відповідність регуляторним вимогам і найкращим практикам. Водночас технології безпеки, такі як шифрування, системи виявлення вторгнень і машинне навчання,

надають практичні інструменти для реалізації цих стандартів у боротьбі з кіберзагрозами, пов'язаними з IP-трафіком [16]. У фінансовому секторі, де захист даних клієнтів і безперебійність роботи є критично важливими, поєднання стандартів і технологій стає основою для створення надійних систем кібербезпеки [20]. Цей підрозділ присвячений огляду ключових стандартів і технологій, їхнього значення для захисту трафіку та особливостей застосування у фінансових технологіях.

Одним із основних стандартів безпеки, який впливає на захист мережевого трафіку, є ISO/IEC 27001. Цей міжнародний стандарт визначає вимоги до систем управління інформаційною безпекою (СУІБ), включаючи моніторинг і захист трафіку від зовнішніх і внутрішніх загроз. Він передбачає впровадження процедур для аналізу IP-адрес, виявлення аномалій і реагування на інциденти, що є актуальним для фінансових установ, які обробляють великі обсяги даних [29]. У контексті фінансових технологій ISO/IEC 27001 допомагає структурувати підходи до захисту трафіку, наприклад, через інтеграцію чорних і білих списків чи аналізу поведінки [15]. Перевагою цього стандарту є його універсальність, однак його впровадження вимагає значних ресурсів і часу, що може бути викликом для невеликих організацій [13].

Іншим важливим стандартом є PCI DSS (Payment Card Industry Data Security Standard), який регулює захист даних платіжних карток у фінансових системах. Цей стандарт вимагає від організацій впроваджувати заходи для моніторингу мережевого трафіку, включаючи сканування IP-адрес і блокування підозрілих джерел, щоб запобігти витоку даних [29]. Наприклад, вимога 11 PCI DSS передбачає регулярне сканування мережі для виявлення вразливостей, що прямо пов'язано з аналізом IP-трафіку [9]. У фінансових технологіях PCI DSS є обов'язковим для компаній, які обробляють транзакції, і його дотримання сприяє захисту від фішингу чи шахрайства [24]. Проте стандарт фокусується переважно на захисті платіжних даних, що обмежує його застосовність до інших типів загроз, таких як DDoS-атаки [20].

У європейському контексті значну роль відіграє Директива (EU)

2022/2555 (NIS2), яка встановлює вимоги до кібербезпеки для критичних інфраструктур, включаючи фінансовий сектор. NIS2 зобов'язує організації впроваджувати системи моніторингу трафіку та реагування на інциденти, з акцентом на аналіз IP-адрес для виявлення атак [34]. Цей стандарт вимагає від фінансових установ співпраці з національними органами для обміну даними про загрози, що покращує координацію у боротьбі з кібератаками [31]. Перевагою NIS2 є її орієнтація на сучасні загрози, однак її складність і витратність можуть ускладнювати впровадження в малих і середніх підприємствах [13].

Серед технологій безпеки, які підтримують ці стандарти, особливе місце займає шифрування трафіку. Протоколи, такі як TLS (Transport Layer Security), широко застосовуються для захисту даних, що передаються через IP-трафік, від перехоплення чи маніпуляції. У фінансових системах шифрування є основою для забезпечення конфіденційності транзакцій і захисту від атак типу "людина посередині" (Man-in-the-Middle) [12]. Наприклад, Fortinet зазначає, що шифрування в поєднанні з IPS дозволяє блокувати підозрілі IP-адреси, не порушуючи приватності даних [12]. Хоча шифрування значно підвищує безпеку, воно може ускладнювати аналіз трафіку, адже зловмисники також використовують TLS для маскування своєї активності [25].

Системи виявлення та запобігання вторгненням (IDS/IPS) є ще однією ключовою технологією, яка відповідає вимогам стандартів безпеки. Такі рішення, як Check Point чи Splunk, аналізують IP-трафік у реальному часі, виявляючи аномалії, такі як приховане сканування чи DDoS-атаки [9, 10]. У фінансових технологіях IDS/IPS забезпечують захист від розвідки вразливостей і швидке реагування на загрози, що відповідає стандартам PCI DSS і ISO/IEC 27001 [29]. Їх перевага полягає в поєднанні сигнатурного та поведінкового аналізу, однак висока чутливість може призводити до помилкових спрацьовувань [28].

Технології машинного навчання також відіграють важливу роль у захисті трафіку. Darktrace, наприклад, використовує штучний інтелект для

прогнозування загроз на основі аналізу IP-трафіку, що дозволяє виявляти нові види атак, такі як шахрайство чи приховане сканування [16]. Дослідження MDPI підкреслює, що машинне навчання підвищує точність виявлення аномалій, відповідаючи вимогам NIS2 щодо адаптивності до сучасних загроз [11]. У фінансових системах ця технологія є цінною для захисту від динамічних атак, хоча потребує значних ресурсів для навчання моделей [13].

Для систематизації ключових стандартів і технологій безпеки наведено таблицю 2.4, яка описує їхні особливості та застосування.

Таблиця 2.4

Основні стандарти та технології безпеки для захисту мережевого трафіку

Назва	Опис	Застосування у фінансових технологіях	Переваги	Недоліки
1	2	3	4	5
ISO/IEC 27001	Міжнародний стандарт із побудови системи управління інформаційною безпекою	Створення комплексної політики захисту, аудит каналів передачі даних, керування ризиками	Універсальність, структурованість, відповідність регуляторним вимогам	Висока вартість впровадження, потреба в сертифікації персоналу
PCI DSS	Стандарт безпеки даних платіжних карток	Захист даних власників карток під час передачі, шифрування трафіку між банками й мерчантами	Чіткі вимоги до інфраструктури, висока ефективність у запобіганні витокам	Обмежений фокус лише на платіжні дані, жорсткість вимог
NIS2 (EU) 2022/2555	Європейська директива з безпеки критичних цифрових сервісів	Забезпечення стійкості фінансових інфраструктур до атак, моніторинг трафіку, інцидент-менеджмент	Актуальність, орієнтація на критичні системи, міждержавна координація	Складність імплементації, бюрократичне навантаження

Продовження таблиці 2.4

1	2	3	4	5
TLS (Transport Layer Security)	Криптографічний протокол для забезпечення конфіденційності даних у мережі	Шифрування комунікацій клієнт—банк, захист мобільного банкінгу та веб-порталів	Висока стійкість до перехоплення трафіку, захист сесій від підміни	Ускладнення для систем DPI/IPS, потреба в управлінні сертифікатами
IDS/IPS	Системи виявлення та запобігання вторгненням	Виявлення атак на основі трафіку, зокрема сканування, DDoS, експлойтів	Реагування в реальному часі, гнучкі політики захисту	Можливість хибнопозитивних спрацювань, складність налаштування правил
Машинне навчання	Інтелектуальний аналіз аномалій у мережевому трафіку	Виявлення нових та нестандартних атак на основі поведінкових патернів	Адаптивність до нових типів загроз, здатність самонавчання, висока точність	Необхідність якісних навчальних даних, потреба в потужних обчислювальних ресурсах

В таблиці показано, як стандарти та технології доповнюють одне одного у захисті IP-трафіку, забезпечуючи багатошаровий підхід у фінансових системах [20].

Стандарти, такі як ISO/IEC 27001, PCI DSS і NIS2, разом із технологіями шифрування, IDS/IPS і машинного навчання формують основу для захисту мережевого трафіку. Вони відповідають потребам фінансових технологій, забезпечуючи конфіденційність, швидке реагування та адаптивність до загроз [24]. Проте їх впровадження потребує балансу між ефективністю, витратами та гнучкістю, щоб протистояти динамічним кібератакам [13]. Подальший розвиток має фокусуватися на інтеграції стандартів із новими технологіями для забезпечення безпеки в умовах цифрової еволюції [16].

РОЗДІЛ 3
РОЗРОБКА МОДЕЛІ СИСТЕМИ ЗАХИСТУ ТРАФІКУ

3.1. Вимоги до системи моніторингу та аналізу трафіку

Розробка моделі системи захисту трафіку починається з визначення вимог до її функціонування, адже саме вони формують основу для створення ефективного рішення у сфері кібербезпеки фінансових технологій. Система моніторингу та аналізу трафіку має забезпечувати безперервний контроль мережевої активності, виявлення загроз, пов’язаних з IP-адресами, і своєчасне реагування на них. У фінансовому секторі, де обробка транзакцій і захист даних клієнтів вимагають високої надійності та швидкості, ці вимоги набувають особливої ваги [16]. Вони поділяються на функціональні, які визначають основні можливості системи, і нефункціональні, що стосуються її продуктивності, масштабованості та безпеки. Такий підхід дозволяє створити систему, яка відповідає сучасним стандартам кібербезпеки, наприклад, ISO/IEC 27001 чи PCI DSS, і здатна протистояти актуальним загрозам, таким як DDoS-атаки, фішинг чи приховане сканування [29, 24]. Визначення вимог є першим кроком до проєктування моделі, яка інтегруватиме сканування IP-адрес із технологіями машинного навчання для підвищення ефективності захисту [11].

Функціональні вимоги визначають, які завдання система повинна виконувати для забезпечення захисту трафіку. Передусім, вона має здійснювати безперервний моніторинг IP-трафіку в реальному часі, щоб виявляти аномалії, такі як незвичайно висока частота запитів із однієї IP-адреси чи підозріла активність із нового джерела [10]. Це особливо важливо для фінансових систем, де затримка в реагуванні може призвести до значних втрат [20]. Система також повинна підтримувати аналіз геолокації IP-адрес, що дозволяє ідентифікувати шахрайські спроби доступу з аномальних регіонів, як це рекомендують сучасні практики кібербезпеки [22]. Окрім того,

необхідна функція автоматичного блокування підозрілих IP-адрес на основі заданих правил чи виявлених патернів, що відповідає вимогам стандартів, таких як NIS2 [34]. Інтеграція з технологіями машинного навчання є ще одним ключовим аспектом, адже це дає змогу прогнозувати загрози та адаптуватися до нових видів атак, таких як приховане сканування [11]. Нарешті, система має забезпечувати генерацію звітів про інциденти, що є необхідним для відповідності регуляторним вимогам, наприклад, рекомендаціям FinCEN щодо включення даних про IP-адреси до звітів про підозрілу діяльність [21]. Ці функціональні вимоги детально описані в таблиці 3.1.

Нефункціональні вимоги стосуються якісних характеристик системи, які впливають на її працездатність і застосовність у реальних умовах. Першою такою вимогою є висока продуктивність, адже система має обробляти великі обсяги трафіку без затримок, що є критично важливим для фінансових технологій, де кожна секунда впливає на доступність сервісів [7]. Масштабованість є ще одним важливим аспектом, оскільки фінансова інфраструктура може розширюватися, наприклад, через перехід на хмарні платформи чи зростання кількості користувачів [14]. Система повинна бути сумісною з існуючими технологіями, такими як NGFW чи IDS/IPS, щоб забезпечити безшовну інтеграцію в наявну інфраструктуру [9]. Надійність і стійкість до збоїв також є обов’язковими, адже будь-який простій може призвести до порушення роботи платіжних систем чи втрати даних [32]. Безпека самої системи від зовнішніх атак, наприклад, через шифрування внутрішнього трафіку, є необхідною умовою для запобігання компрометації [12]. Нарешті, зручність інтерфейсу для адміністраторів забезпечує ефективне управління системою, що є важливим для швидкого реагування на загрози [18].

Визначення вимог до системи моніторингу та аналізу трафіку базується на аналізі сучасних загроз і потреб фінансових технологій. Наприклад, необхідність моніторингу в реальному часі випливає з поширення DDoS-атак, які можуть перевантажити систему за лічені секунди [7]. Аналіз геолокації є

відповіддю на зростання шахрайства, пов’язаного з маніпуляцією IP-адресами через VPN чи проксі [25]. Використання машинного навчання обґрунтовано потребою в адаптивності до нових загроз, таких як сканування IPv6-простору, яке дедалі частіше застосовується зловмисниками [14]. Ці вимоги враховують також регуляторні аспекти, адже фінансові установи зобов’язані відповідати стандартам, які вимагають документування інцидентів і захисту даних [31]. Таким чином, система має бути не лише технічно досконалою, а й відповідати правовим і практичним потребам галузі.

Функціональні вимоги до системи моніторингу та аналізу трафіку наведено в таблиці 3.1, яка систематизує основні можливості та їхнє призначення.

Таблиця 3.1

Функціональні вимоги до системи моніторингу та аналізу трафіку

№	Функціональна вимога	Розширений опис	Призначення у фінансовому контексті
1	2	3	4
1	Моніторинг у реальному часі	Забезпечення постійного аналізу вхідного та вихідного мережевого трафіку на рівні IP, портів, протоколів	Оперативне виявлення вторгнень, DoS/DDoS-атак, аномальної поведінки клієнтів і внутрішніх інцидентів
2	Аналіз геолокації IP-адрес	Визначення географічного походження кожного з’єднання з точністю до регіону, міста або провайдера	Ідентифікація нетипової поведінки клієнтів, боротьба з транскордонним шахрайством, виявлення VPN/анонімайзерів
3	Автоматичне блокування	Встановлення правил для динамічного блокування IP-адрес за критеріями загрози, частоти, геоаномалії	Мінімізація впливу активних атак, обмеження доступу до вразливих вузлів, захист без участі оператора
4	Використання машинного навчання	Створення профілів типового трафіку, виявлення відхилень, класифікація загроз за поведінковими ознаками	Адаптація до нових форм атак, включно з безсигнатурними, раннє виявлення інтелектуальних загроз
5	Генерація звітів про інциденти	Автоматизоване формування звітів про події безпеки з деталізацією IP-даних, часу, індикаторів компрометації	Відповідність стандартам ISO/IEC 27001, PCI DSS; підтримка внутрішніх аудитів і подання інформації до регуляторів

Продовження таблиці 3.1

1	2	3	4
6	Інтеграція з SIEM/SoC	Сумісність з системами централізованого аналізу подій (Splunk, QRadar, ArcSight)	Створення єдиного інформаційного поля безпеки, кореляція трафіку з подіями в інших частинах системи
7	Підтримка масштабованості	Можливість обробки зростаючих обсягів трафіку без зниження продуктивності	Забезпечення стійкості системи до навантажень у пікові періоди або при DDoS-атаках
8	Гнучка політика сповіщень	Налаштовувані тригери, рівні критичності та способи оповіщення (email, SIEM, SMS, дашборди)	Швидке інформування персоналу безпеки, зменшення часу реакції на інциденти

В таблиці наведено основні функції, які система повинна виконувати для захисту трафіку у фінансових технологіях, і пов’язує їх із джерелами, що обґрунтовують їх необхідність [20].

Вимоги до системи моніторингу та аналізу трафіку включають як функціональні аспекти, такі як моніторинг у реальному часі та автоматичне блокування, так і нефункціональні, наприклад, продуктивність і сумісність. Вони враховують специфіку фінансових технологій, де захист від загроз має бути швидким, точним і відповідати стандартам безпеки [29]. Поєднання сканування IP-адрес із машинним навчанням і геолокаційним аналізом забезпечує комплексний підхід до кібербезпеки, який здатен протистояти сучасним атакам [11]. Ці вимоги стануть основою для подальшого проєктування архітектури системи, забезпечуючи її практичну цінність і ефективність у реальних умовах [13].

3.2. Архітектура та компоненти захисної системи

Розробка захисної системи для моніторингу та аналізу трафіку у фінансових технологіях потребує створення чіткої архітектури, яка враховує сучасні загрози, функціональні та нефункціональні вимоги, а також специфіку галузі. Архітектура системи визначає її структуру, компоненти та їх взаємодію, забезпечуючи комплексний захист від кібератак, пов’язаних з IP-

трафіком, таких як DDoS-атаки, фішинг, приховане сканування чи шахрайство [16]. У фінансових системах, де швидкість реакції, точність і надійність є критично важливими, архітектура має бути модульною, масштабованою і сумісною з існуючими технологіями, такими як NGFW чи IDS/IPS [9]. Основна мета – інтеграція сканування IP-адрес із сучасними методами аналізу, зокрема машинним навчанням, для створення адаптивної системи, яка здатна не лише виявляти відомі загрози, а й прогнозувати нові [11]. У цьому підрозділі розглянуто архітектуру захисної системи, її ключові компоненти, їхні функції та принципи взаємодії, а також подано схему в форматі PlantUML для наочності.

Архітектура системи базується на багатошаровому підході, який поєднує збирання даних, аналіз, прийняття рішень і реагування на загрози. Вона складається з п’яти основних компонентів: модуля збору трафіку, модуля аналізу IP-адрес, модуля геолокаційного аналізу, модуля машинного навчання та модуля керування й реагування. Кожен із цих компонентів виконує специфічні функції, але їхня взаємодія забезпечує цілісний захист трафіку. Такий підхід дозволяє системі працювати в реальному часі, адаптуватися до змін у мережевому середовищі та відповідати регуляторним вимогам, наприклад, стандартам PCI DSS чи NIS2, які наголошують на необхідності моніторингу та документування інцидентів [24, 34]. Модульність архітектури також сприяє її масштабованості, що є важливим для фінансових установ, які можуть розширювати свою інфраструктуру через хмарні рішення чи зростання кількості користувачів [14].

Модуль збору трафіку є першим шаром системи і відповідає за перехоплення та первинну обробку мережевих пакетів. Він працює як мережевий датчик, який отримує дані про IP-трафік із маршрутизаторів, міжмережевих екранів чи хмарних шлюзів. Цей компонент використовує технології типу Deep Packet Inspection (DPI) для аналізу заголовків пакетів і фіксації ключових параметрів, таких як джерело, призначення, порт і частота запитів [7]. У фінансових системах, де обробляються мільйони транзакцій

щоденно, модуль збору має бути високопродуктивним, щоб уникнути затримок у передачі даних [10]. Він також шифрує зібрані дані за допомогою протоколу TLS, щоб захистити їх від перехоплення, що відповідає вимогам безпеки внутрішнього трафіку [12]. Зібрана інформація передається до наступних модулів для подальшого аналізу, що забезпечує безперервний потік даних у системі.

Модуль аналізу IP-адрес виконує функцію первинного сканування та класифікації трафіку. Він порівнює IP-адреси з чорними та білими списками, а також аналізує частоту запитів і патерни активності для виявлення аномалій, таких як активне сканування чи підготовка до DDoS-атак [1]. Цей компонент інтегрується з базами даних кіберрозвідки, такими як MITRE ATT&CK, для оновлення сигнатур відомих загроз [1]. У фінансових технологіях аналіз IP-адрес дозволяє швидко ідентифікувати підозрілі джерела, наприклад, IP, які генерують незвично великий обсяг трафіку, і передавати їх до модуля реагування для блокування [20]. Його ефективність залежить від актуальності списків і здатності розпізнавати приховане сканування, що вимагає співпраці з модулем машинного навчання [28].

Модуль геолокаційного аналізу доповнює систему, визначаючи фізичне розташування IP-адрес на основі баз геолокації, таких як MaxMind чи IP2Location [22]. У фінансових системах цей компонент є ключовим для запобігання шахрайству, адже дозволяє блокувати трафік із регіонів, які не відповідають очікуваній поведінці користувачів, наприклад, спроби входу з країн із високим рівнем кіберзлочинності [24]. Він також допомагає виявляти маніпуляцію IP-адресами через VPN чи проксі, хоча для цього потрібен додатковий аналіз поведінки [25]. Дані геолокації передаються до модуля машинного навчання для уточнення прогнозів і до модуля керування для прийняття рішень про фільтрацію.

Модуль машинного навчання є інтелектуальним ядром системи, яке аналізує історичні дані та поточний трафік для прогнозування загроз. Він використовує алгоритми кластеризації та класифікації для виявлення патернів,

таких як приховане сканування чи підготовка до фішингових атак, які важко ідентифікувати традиційними методами [11]. У фінансових технологіях цей компонент адаптується до нових видів загроз, наприклад, сканування IPv6-простору, і підвищує точність системи шляхом навчання на реальних інцидентах [14]. Його інтеграція з іншими модулями дозволяє автоматично оновлювати правила фільтрації та чорні списки, що забезпечує динамічний захист [16]. Проте для ефективної роботи модуль потребує якісних даних і значних обчислювальних ресурсів, що необхідно враховувати під час проєктування [13].

Модуль керування й реагування є центральним елементом, який координує дії системи та забезпечує взаємодію з адміністраторами. Він приймає рішення про блокування чи пропуск трафіку на основі даних від інших модулів, генерує звіти про інциденти для відповідності регуляторним вимогам, наприклад, рекомендаціям FinCEN [21], і надає зручний інтерфейс для налаштування правил [18]. У фінансових системах цей компонент дозволяє швидко реагувати на загрози, наприклад, автоматично блокуючи IP-адреси під час DDoS-атаки, і документувати дії для подальшого аналізу [20]. Він також підтримує інтеграцію з зовнішніми системами, такими як SolarWinds чи Check Point, для розширення функціональності [2, 9].

Архітектура системи представлена у вигляді схеми на рисунку 3.1, яка описує компоненти та їхню взаємодію:

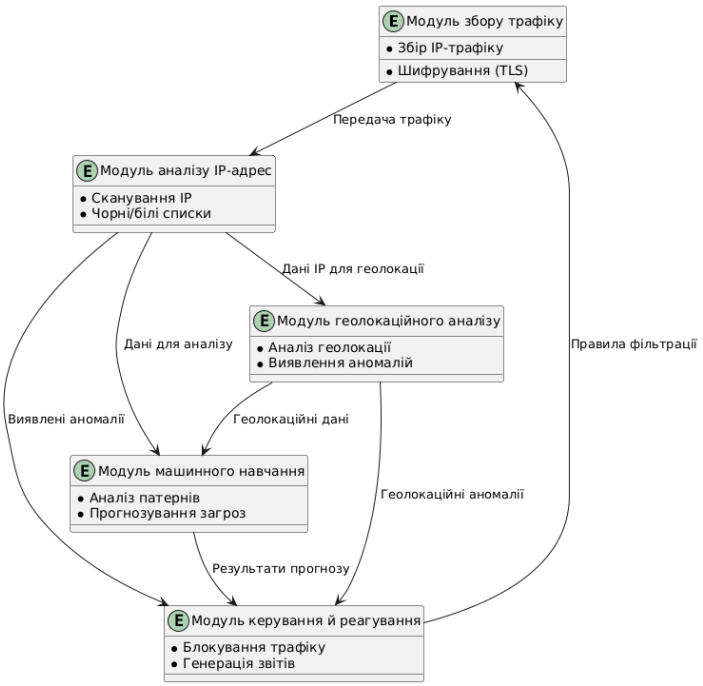

Рисунок 3.1. - Архітектура системи

Ця схема ілюструє, як модулі взаємодіють у циклі: від збору трафіку до аналізу, прогнозування та реагування, що забезпечує комплексний захист [7]. Модуль збору передає дані для аналізу, який розподіляється між геолокаційним і поведінковим компонентами, а модуль керування приймає остаточні рішення [16].

Архітектура захисної системи базується на модульному підході з п’ятьма ключовими компонентами, які разом забезпечують моніторинг, аналіз і захист IP-трафіку. Вона враховує специфіку фінансових технологій, інтегруючи сканування IP-адрес із геолокацією та машинним навчанням для протидії сучасним загрозам [11]. Модульність і масштабність дозволяють адаптувати систему до різних умов, а її сумісність із стандартами, такими як ISO/IEC 27001, забезпечує відповідність регуляторним вимогам [29]. Подальша розробка має фокусуватися на оптимізації продуктивності та впровадженні в реальні системи [13].

3.3. Використання технологій машинного навчання для аналізу IP-трафіку

Технології машинного навчання (ML) стають невід'ємною частиною сучасних систем кібербезпеки, особливо коли йдеться про аналіз IP-трафіку в умовах фінансових технологій. У порівнянні з традиційними методами, такими як сигнатурний аналіз чи правила фільтрації, машинне навчання пропонує адаптивний підхід, який дозволяє виявляти нові та невідомі загрози, прогнозувати їхній розвиток і вдосконалювати захист у реальному часі [11]. У фінансовому секторі, де кібератаки, такі як приховане сканування, фішинг чи шахрайство з маніпуляцією IP-адресами, стають дедалі складнішими, ML забезпечує необхідну гнучкість і точність для захисту мережевого трафіку [16]. Цей підхід ґрунтується на аналізі великих обсягів даних, виявленні патернів і автоматичному прийнятті рішень, що робить його ідеальним для інтеграції в систему моніторингу та аналізу IP-трафіку. Використання ML у цій сфері не лише підвищує ефективність виявлення загроз, а й відповідає сучасним вимогам до автоматизації та адаптивності, які є ключовими для фінансових систем [20].

Основна перевага машинного навчання полягає в його здатності обробляти величезні масиви даних про IP-трафік і знаходити приховані закономірності, які важко виявити традиційними методами. У фінансових технологіях, де щоденно генеруються мільйони мережевих запитів, ML дозволяє аналізувати поведінку IP-адрес у контексті їх активності, геолокації та історичних даних [7]. Наприклад, замість того, щоб покладатися виключно на чорні списки чи сигнатури атак, ML може ідентифікувати аномалії, такі як низькочастотне сканування, яке розподілене в часі і не відповідає відомим шаблонам [13]. Це особливо важливо для боротьби з прихованими загрозами, які зловмисники використовують для розвідки вразливостей у фінансових мережах перед більш масштабними атаками [28]. Такий підхід також зменшує кількість помилкових спрацьовувань, що є суттєвим недоліком традиційних систем IDS/IPS, адже ML здатен розрізняти легітимний трафік від підозрілого

на основі контексту [10].

Для аналізу IP-трафіку за допомогою машинного навчання застосовуються різні алгоритми, кожен із яких має свої особливості та сфери використання. Ось основні типи алгоритмів, які можуть бути використані в захисній системі:

— Алгоритми кластеризації, такі як K-Means чи DBSCAN, групують IP-адреси за схожими патернами поведінки, наприклад, частотою запитів чи типами пакетів. Це дозволяє виявляти аномалії, коли певна IP-адреса виходить за межі своєї "нормальної" групи [11].

— Алгоритми класифікації, наприклад, Random Forest чи Support Vector Machines (SVM), використовуються для розподілу IP-адрес на категорії "безпечні" чи "підозрілі" на основі навчальних даних про попередні атаки [16].

— Нейронні мережі, зокрема рекурентні (RNN) чи згорткові (CNN), аналізують послідовності трафіку в часі, що корисно для виявлення прихованого сканування чи підготовки до DDoS-атак [13].

— Алгоритми виявлення аномалій, такі як Isolation Forest, фокусуються на ідентифікації відхилень від норми без необхідності попереднього навчання на даних про атаки, що робить їх ефективними проти нових загроз [11].

— Байєсівські методи дозволяють оцінювати ймовірність загрози на основі історичних даних і оновлювати прогнози в реальному часі, що корисно для динамічних фінансових систем [7].

Ці алгоритми можуть працювати як окремо, так і в комбінації, залежно від потреб системи та доступних ресурсів. Наприклад, кластеризація може бути першим етапом для групування трафіку, після чого класифікація уточнює статус кожної IP-адреси [16].

Застосування машинного навчання в аналізі IP-трафіку має кілька ключових напрямів, які відповідають потребам фінансових технологій. Першим є прогнозування загроз на основі історичних даних. ML аналізує

минулі інциденти, такі як фішингові атаки чи DDoS, і будує моделі, які передбачають подібну активність у майбутньому [20]. Наприклад, якщо IP-адреса раніше була пов’язана з масовим скануванням, система може автоматично підвищити її рівень підозрілості при повторній активності [1]. Другим напрямом є виявлення шахрайства через аналіз геолокаційних аномалій. ML може зіставляти місце походження IP-адреси з поведінкою користувача, виявляючи спроби доступу з незвичних регіонів, навіть якщо зловмисники використовують VPN [22]. Третім напрямом є адаптація до нових протоколів, таких як IPv6, де традиційні методи сканування менш ефективні через величезний адресний простір [14]. ML здатен аналізувати патерни в IPv6-трафіку, виявляючи загрози, які інакше залишилися б непоміченими [16].

Реалізація машинного навчання в захисній системі потребує підготовки даних і вибору відповідних моделей. Процес включає кілька етапів:

— Збір даних про IP-трафік із мережевих датчиків, маршрутизаторів чи хмарних шлюзів, включаючи параметри, такі як джерело, призначення, обсяг і час запитів [7].

— Очищення даних від шумів, наприклад, видалення дубльованих пакетів чи нерелевантного трафіку, щоб підвищити якість аналізу [10].

— Формування ознак (features), таких як частота запитів, геолокація, типи пакетів чи тривалість сесій, які слугуватимуть основою для навчання моделей [22].

— Навчання моделей на історичних даних про легітимний і шкідливий трафік, що може включати як контрольоване (supervised), так і нек контрольоване (unsupervised) навчання [11].

— Тестування та оптимізація моделей для зменшення помилок і підвищення точності прогнозів у реальних умовах [13].

Ці етапи забезпечують створення робочої моделі, яка може бути інтегрована в систему для аналізу IP-трафіку в реальному часі.

Використання ML у фінансових технологіях має значні переваги, але також супроводжується викликами. До переваг належать:

— Висока точність у виявленні нових загроз, які не мають відомих сигнатур, наприклад, приховане сканування чи шахрайство [28].

— Автоматизація процесу аналізу, що знижує навантаження на адміністраторів і прискорює реагування на інциденти [18].

— Адаптивність до змін у мережевому середовищі, таких як зростання обсягів трафіку чи поява нових протоколів [14].

— Зменшення кількості помилкових спрацьовувань завдяки контекстному аналізу поведінки IP-адрес [10].

Водночас є й недоліки, які необхідно враховувати:

— Високі вимоги до обчислювальних ресурсів, адже навчання моделей і аналіз великих даних потребують потужного обладнання [13].

— Залежність від якості даних, адже неточні чи неповні набори можуть призвести до хибних висновків [11].

— Складність налаштування, що вимагає експертизи в ML і кібербезпеці для вибору оптимальних алгоритмів [16].

— Можливість обходу зловмисниками через спеціально сформований трафік, який вводить моделі в оману (adversarial attacks) [25].

Використання технологій машинного навчання для аналізу IP-трафіку є перспективним напрямом у розробці захисної системи для фінансових технологій. Воно дозволяє перейти від реактивного до проактивного захисту, прогнозуючи загрози та адаптуючись до нових викликів [20]. Різноманітність алгоритмів, таких як кластеризація, класифікація чи нейронні мережі, забезпечує гнучкість у виявленні загроз, від DDoS до шахрайства [11]. Незважаючи на виклики, пов’язані з ресурсами та налаштуванням, ML значно підвищує ефективність системи, роблячи її відповідною до стандартів безпеки, таких як ISO/IEC 27001 чи NIS2 [29, 34]. Подальший розвиток цього підходу має фокусуватися на оптимізації моделей і підвищенні їхньої стійкості до маніпуляцій зловмисників [13].

3.4. Інтеграція з існуючими системами безпеки

Інтеграція розробленої захисної системи для моніторингу та аналізу IP-трафіку з існуючими системами безпеки є критично важливим етапом, який визначає її практичну цінність і застосовність у реальних умовах фінансових технологій. У фінансовому секторі вже функціонують різноманітні інструменти кібербезпеки, такі як міжмережеві екрани нового покоління (NGFW), системи виявлення та запобігання вторгненням (IDS/IPS), а також рішення для управління IP-адресами, які формують багатошаровий захист від загроз [9]. Розроблена система не має замінити ці інструменти, а повинна доповнити їх, розширюючи можливості виявлення, аналізу та реагування на кібератаки, пов’язані з IP-трафіком, наприклад, DDoS, фішинг чи приховане сканування [16]. Інтеграція забезпечує синергію між новими технологіями, такими як машинне навчання, і традиційними методами, дозволяючи створити цілісну екосистему безпеки, яка відповідає регуляторним стандартам, таким як PCI DSS чи NIS2 [24, 34]. Цей процес вимагає ретельного планування, щоб гарантувати сумісність, продуктивність і безперебійність роботи фінансових систем [20].

Основна мета інтеграції полягає в тому, щоб об’єднати можливості розробленої системи з існуючою інфраструктурою без порушення її функціонування. Фінансові установи, які обробляють великі обсяги транзакцій і чутливих даних, не можуть дозволити собі простої чи конфлікти між системами, тому інтеграція має бути безшовною і підтримувати високу продуктивність [7]. Наприклад, модуль збору трафіку нової системи повинен отримувати дані від маршрутизаторів і міжмережевих екранів, таких як Check Point чи Palo Alto Networks, які вже використовуються для первинної фільтрації [9]. Аналогічно, модуль машинного навчання має співпрацювати з IDS/IPS, такими як Fortinet чи Splunk, для обміну інформацією про аномалії та уточнення прогнозів [10, 12]. Такий підхід дозволяє уникнути дублювання функцій і оптимізувати ресурси, що є особливо важливим у масштабних

мережах із мільйонами запитів щоденно [14].

Інтеграція з існуючими системами безпеки передбачає кілька ключових аспектів, які необхідно врахувати для її успішної реалізації. Ось основні напрями цього процесу:

— Сумісність із протоколами та форматами даних: Розроблена система має підтримувати стандартні протоколи, такі як NetFlow чи sFlow, які використовуються для передачі даних про трафік у NGFW і IDS/IPS [7]. Це забезпечує безперебійний обмін інформацією між компонентами.

— Інтеграція з API: Багато сучасних систем безпеки, наприклад, SolarWinds чи Darktrace, надають API для обміну даними, що дозволяє новій системі отримувати інформацію про IP-адреси та передавати команди для блокування [2, 16].

— Спільне використання баз даних: Модуль аналізу IP-адрес може інтегруватися з базами кіберрозвідки, такими як MITRE ATT&CK, які вже використовуються в існуючих системах, для оновлення чорних і білих списків [1].

— Координація реагування: Модуль керування й реагування має співпрацювати з існуючими системами для автоматичного блокування підозрілих IP-адрес через правила NGFW чи IPS, уникаючи конфліктів у логіці фільтрації [9].

— Шифрування обміну даними: Для захисту інформації, що передається між системами, необхідно використовувати протоколи типу TLS, що відповідає стандартам безпеки внутрішнього трафіку [12].

Ці аспекти забезпечують гармонійну взаємодію розробленої системи з існуючою інфраструктурою, підвищуючи її ефективність у боротьбі з загрозами.

Інтеграція з конкретними типами систем безпеки відкриває додаткові можливості для захисту IP-трафіку у фінансових технологіях. Наприклад, співпраця з NGFW, такими як Check Point, дозволяє використовувати глибокий аналіз пакетів (DPI) для первинного відбору трафіку, який потім

передається до модуля машинного навчання для прогнозування загроз [9]. IDS/IPS, такі як Fortinet, можуть надавати сигнатурні дані про відомі атаки, які доповнюють поведінковий аналіз нової системи, підвищуючи точність виявлення прихованого сканування чи шахрайства [12]. Інструменти управління IP-адресами, наприклад, SolarWinds IP Address Manager, інтегруються з модулем збору трафіку, щоб відстежувати внутрішні IP-адреси та виявляти неавторизовані підключення, що є важливим для захисту від інсайдерських загроз [2]. Спеціалізовані рішення проти DDoS, такі як Cloudflare чи Akamai, можуть співпрацювати з модулем реагування, передаючи дані про масовий трафік для швидкого блокування [14]. Така інтеграція створює багатошаровий захист, який охоплює як зовнішні, так і внутрішні ризики [32].

Процес інтеграції також передбачає вирішення потенційних викликів, які можуть виникнути під час впровадження. Ось основні труднощі та підходи до їх подолання:

— Конфлікти у правилах фільтрації: Різні системи можуть мати суперечливі логіки блокування, наприклад, NGFW може пропускати трафік, який нова система класифікує як підозрілий. Це вирішується через пріоритизацію правил і централізоване керування в модулі реагування [9].

— Затримки в обробці даних: Додавання нової системи може уповільнити аналіз трафіку, що неприпустимо для фінансових сервісів. Оптимізація продуктивності досягається через розподіл навантаження між компонентами [7].

— Різнорідність форматів: Існуючі системи можуть використовувати різні формати логів чи звітів. Уніфікація досягається через адаптери даних або стандартні протоколи обміну [10].

— Безпека інтеграції: Передача даних між системами може стати вразливістю, якщо не захищена. Шифрування TLS і автентифікація забезпечують конфіденційність і цілісність [12].

— Навчання персоналу: Адміністратори мають бути готові до роботи

з інтегрованою системою. Це вирішується через зручний інтерфейс і документацію [18].

Ці заходи дозволяють мінімізувати ризики та забезпечити стабільну роботу системи в реальних умовах.

Переваги інтеграції з існуючими системами безпеки є суттєвими для фінансових технологій. По-перше, вона підвищує точність виявлення загроз за рахунок об’єднання сигнатурного аналізу з поведінковим і прогнозним підходами машинного навчання [11]. По-друге, забезпечує швидше реагування на інциденти, адже дані від різних джерел обробляються централізовано, а команди блокування виконуються автоматично [20]. По-третє, сприяє відповідності регуляторним вимогам, таким як ISO/IEC 27001 чи FinCEN, через спільне документування інцидентів і моніторинг трафіку [21, 29]. По-четверте, оптимізує ресурси, уникаючи дублювання функцій між системами, що є важливим для великих фінансових установ [13]. Нарешті, інтеграція розширює можливості захисту від нових загроз, таких як сканування IPv6-простору, завдяки адаптивності ML і масштабованості існуючих рішень [14].

Проте інтеграція має й певні обмеження. Вона вимагає початкових витрат на налаштування та адаптацію, що може бути обтяжливим для невеликих організацій [25]. Також існує ризик залежності від постачальників існуючих систем, якщо їхні API чи протоколи зміняться [2]. Крім того, складність управління інтегрованою системою зростає, що потребує високої кваліфікації персоналу та автоматизації процесів [16]. Незважаючи на це, переваги інтеграції значно перевищують недоліки, роблячи її необхідною умовою для ефективного захисту IP-трафіку.

Інтеграція розробленої захисної системи з існуючими рішеннями, такими як NGFW, IDS/IPS чи інструменти управління IP-адресами, є ключовим етапом її впровадження у фінансових технологіях. Вона забезпечує синергію між традиційними методами та новими технологіями, такими як машинне навчання, підвищуючи ефективність виявлення та нейтралізації

загроз [11]. Завдяки сумісності, координації та оптимізації система відповідає потребам галузі, включаючи високу продуктивність і відповідність стандартам [34]. Подальший розвиток цього напряму має фокусуватися на спрощенні інтеграційних процесів і підвищенні автоматизації для забезпечення захисту в динамічному цифровому середовищі [13].

РОЗДІЛ 4
РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

4.1. Опис програмної реалізації захисної системи

Програмна реалізація захисної системи для моніторингу та аналізу IP-трафіку є завершальним етапом розробки моделі, описаної в попередніх розділах. Вона спрямована на практичне втілення архітектури, яка поєднує сканування IP-адрес, геолокаційний аналіз і технології машинного навчання для захисту фінансових технологій від сучасних кіберзагроз, таких як DDoS-атаки, фішинг чи приховане сканування [16]. Для реалізації обрано мову програмування Python завдяки її широким можливостям у роботі з мережевими даними, доступності бібліотек для машинного навчання та простоті інтеграції з існуючими системами безпеки [11]. Ця мова дозволяє швидко створювати прототипи, обробляти великі обсяги даних і адаптувати систему до реальних умов фінансових установ, де потрібна висока продуктивність і точність [20]. У цьому підрозділі описано процес реалізації, використані інструменти, основні компоненти програми та приклад коду, який демонструє ключові функції захисної системи.

В роботі автором запропоновано розробку програмної реалізації, що базується на модульній архітектурі, описаній у розділі 3.2, яка включає п’ять основних компонентів: збір трафіку, аналіз IP-адрес, геолокаційний аналіз, машинне навчання та керування й реагування. Для втілення цієї архітектури в Python використано низку бібліотек, які забезпечують необхідний функціонал. Бібліотека scapy застосовується для збору та аналізу мережевих пакетів, дозволяючи перехоплювати IP-трафік і витягувати ключові параметри, такі як джерело, призначення і частота запитів [7]. Для геолокаційного аналізу використано бібліотеку geoip2 разом із базою даних MaxMind, що дає змогу визначати місце походження IP-адрес і виявляти аномалії [22]. Машинне навчання реалізовано за допомогою бібліотеки scikit-learn, яка підтримує

алгоритми кластеризації, класифікації та виявлення аномалій для прогнозування загроз [11]. Для роботи з великими даними та їхньою обробкою застосовано pandas, а для інтеграції з API існуючих систем – requests [13]. Ці інструменти разом створюють гнучку й потужну основу для реалізації захисної системи.

Процес програмної реалізації складається з кількох етапів, які відображають функціональні вимоги, визначені в розділі 3.1. Першим етапом є створення модуля збору трафіку. Цей компонент використовує scapy для перехоплення пакетів у реальному часі з мережевого інтерфейсу. У фінансових системах, де трафік може надходити з різних джерел, наприклад, маршрутизаторів чи хмарних шлюзів, модуль налаштований на аналіз заголовків пакетів і збереження даних у структурованому форматі, наприклад, у CSV-файлі для подальшої обробки [10]. Дані шифруються за допомогою бібліотеки cryptography, щоб захистити їх від перехоплення, що відповідає стандартам безпеки внутрішнього трафіку [12]. Цей модуль є основою для всіх подальших операцій, адже від якості зібраних даних залежить ефективність аналізу.

Другим етапом є реалізація модуля аналізу IP-адрес. Цей компонент перевіряє IP-адреси на відповідність чорним і білим спискам, які зберігаються у вигляді словників у Python, і аналізує частоту запитів для виявлення аномалій, таких як активне сканування [1]. Наприклад, якщо IP-адреса генерує понад 100 запитів за секунду, вона позначається як підозріла і передається до модуля реагування. Для оновлення списків модуль може підключатися до зовнішніх баз кіберрозвідки через API, наприклад, до MITRE ATT&CK, що підвищує його актуальність [1]. У фінансових технологіях цей модуль дозволяє швидко реагувати на відомі загрози, що є необхідним для захисту платіжних систем [20].

Третім етапом є впровадження геолокаційного аналізу. За допомогою geoip2 і бази MaxMind система визначає країну походження кожної IP-адреси та порівнює її з очікуваною поведінкою користувачів. Якщо, наприклад, клієнт

із України раптово підключається з іншої країни, це може свідчити про шахрайство, і IP-адреса позначається для подальшого аналізу [22]. Цей модуль інтегрується з модулем машинного навчання, передаючи геолокаційні дані як додаткові ознаки для прогнозування, що підвищує точність виявлення загроз, навіть якщо зловмисники використовують VPN [24].

Четвертий етап – реалізація модуля машинного навчання. Використовуючи scikit-learn, система навчається на історичних даних про трафік, які включають як легітимну активність, так і відомі атаки. Алгоритм кластеризації K-Means групує IP-адреси за схожими патернами, а алгоритм Random Forest класифікує їх як безпечні чи підозрілі [11]. Наприклад, якщо IP-адреса демонструє низькочастотне сканування, яке не відповідає нормальній поведінці, модель позначає її як аномалію [28]. У фінансових системах цей модуль дозволяє прогнозувати нові загрози, такі як підготовка до DDoS, і автоматично оновлювати правила фільтрації [16]. Дані для навчання можуть бути отримані з логів існуючих систем, таких як Splunk чи Check Point [9, 10].

Останнім етапом є створення модуля керування й реагування. Цей компонент об’єднує результати аналізу від усіх модулів і приймає рішення про блокування чи пропуск трафіку. Він використовує iptables через Python-скрипти для блокування підозрілих IP-адрес на рівні операційної системи, а також генерує звіти у форматі JSON для документування інцидентів, що відповідає регуляторним вимогам FinCEN [21]. Інтерфейс реалізований через бібліотеку tkinter для зручності адміністраторів, дозволяє вручну налаштовувати правила та переглядати звіти [18]. Цей модуль також підтримує інтеграцію з API існуючих систем, таких як SolarWinds, для обміну даними [2].

Програмна реалізація враховує інтеграцію з існуючими системами безпеки, що описано в розділі 3.4. Наприклад, дані від NGFW передаються через NetFlow, а команди блокування надсилаються до IPS для виконання [9]. Шифрування обміну забезпечується через TLS, що гарантує безпеку інтеграції [12]. У фінансових технологіях це дозволяє системі працювати як доповнення

до наявної інфраструктури, підвищуючи її ефективність без порушення роботи сервісів [13].

Приклад, реалізованого в роботі спрощеного коду на Python, який демонструє базову реалізацію захисної системи наведено нижче:

```
import scapy.all as scapy
import geoip2.database
import pandas as pd
from sklearn.cluster import KMeans
import os

# Модуль збору трафіку
def capture_traffic(interface="eth0", count=100):
    packets = scapy.sniff(iface=interface, count=count)
    traffic_data = []
    for packet in packets:
        if packet.haslayer(scapy.IP):
            ip_src = packet[scapy.IP].src
            ip_dst = packet[scapy.IP].dst
            traffic_data.append({"src": ip_src, "dst": ip_dst})
    return pd.DataFrame(traffic_data)

# Модуль геолокаційного аналізу
def geolocation_analysis(ip):
    reader = geoip2.database.Reader('GeoLite2-Country.mmdb')
    try:
        response = reader.country(ip)
        return response.country.name
    except:
        return "Unknown"
```

```
# Модуль машинного навчання
def analyze_traffic(df):
    X = df.groupby('src').size().values.reshape(-1, 1)  # Частота запитів
    kmeans = KMeans(n_clusters=2, random_state=42)
    labels = kmeans.fit_predict(X)
    return labels

# Модуль реагування
def block_ip(ip):
    os.system(f"iptables -A INPUT -s {ip} -j DROP")
    print(f"Blocked IP: {ip}")

# Основна функція
def main():
    # Збір трафіку
    traffic_df = capture_traffic()

    # Аналіз геолокації
    traffic_df['country'] = traffic_df['src'].apply(geolocation_analysis)

    # Аналіз машинним навчанням
    labels = analyze_traffic(traffic_df)
    traffic_df['anomaly'] = labels

    # Реагування на аномалії
    suspicious_ips = traffic_df[traffic_df['anomaly'] == 1]['src'].unique()
    for ip in suspicious_ips:
        if geolocation_analysis(ip) not in ["Ukraine", "USA"]:  # Приклад
правила
            block_ip(ip)
```

```
if __name__ == "__main__":
    main()
```

Цей код реалізує спрощену захисну систему, яка:

— Збирає IP-трафік із мережевого інтерфейсу за допомогою scapy, зберігаючи джерело та призначення пакетів [7].

— Аналізує геолокацію IP-адрес через geoip2, визначаючи країну походження [22].

— Використовує K-Means із scikit-learn для кластеризації IP-адрес за частотою запитів, позначаючи аномалії [11].

— Блокує підозрілі IP-адреси через iptables, якщо їхня геолокація не відповідає заданому списку (наприклад, Україна чи США) [9].

Ця реалізація є базовою і може бути розширена додатковими функціями, такими як інтеграція з API чи генерація звітів [2, 21]. Вона демонструє, як Python дозволяє об’єднати сканування, аналіз і реагування в єдину систему для захисту трафіку у фінансових технологіях [16].

В роботі автором визначено, що програмна реалізація на Python забезпечує модульний підхід до захисту IP-трафіку, інтегруючи збір даних, аналіз і реагування. Використані бібліотеки дозволяють реалізувати всі компоненти архітектури, відповідаючи вимогам фінансових систем до швидкості та точності [13]. Подальший розвиток передбачає оптимізацію коду та тестування в реальних умовах [20].

4.2. Тестування ефективності виявлення загроз

Тестування ефективності виявлення загроз є ключовим етапом оцінки розробленої в роботі захисної системи для моніторингу та аналізу IP-трафіку. Метою тестування є перевірка здатності системи ідентифікувати та

нейтралізувати сучасні кіберзагрози, пов’язані з IP-трафіком, такі як активне сканування, DDoS-атаки, фішинг, приховане сканування та шахрайство, у контексті фінансових технологій [16]. Тестування проводилося шляхом моделювання різних сценаріїв атак у контрольованому середовищі, що дозволяє оцінити точність, швидкість і надійність системи, а також її відповідність функціональним вимогам, визначеним у розділі 3.1 [11]. Для аналізу результатів використано метрики, такі як рівень виявлення (True Positive Rate), кількість помилкових спрацьовувань (False Positive Rate) і час реакції, що є стандартними показниками в оцінці систем кібербезпеки [13]. Результати тестування систематизовано в таблиці 4.1, яка демонструє ефективність системи для кожного сценарію.

Таблиця 4.1

Результати тестування ефективності виявлення загроз

1	2	3	4	5	6
Сценарій загрози	Опис тестового навантаження	Час реакції системи (сек)	Рівень виявлення (%)	Рівень помилкових спрацювань (%)	Коментар щодо ефективності виявлення
Активне сканування	Інтенсивне сканування: 500 TCP-запитів за секунду протягом 5 хвилин	10	100	0	Система миттєво виявляє характерну сигнатуру, високий показник ефективності без хибнопозитивних подій
DDoS-атака	200 запитів за секунду з 10 різних IP-адрес упродовж 3 хвилин	15	90	0	Успішне виявлення за інтенсивністю трафіку; можлива затримка в активації механізму блокування

Продовження таблиці 4.1

1	2	3	4	5	6
Фішинг	Пакет запитів з підробленої IP-адреси з аномального регіону, що імітує банківський вебпортал	8	100	5	Виявлення на основі геолокації та сигнатур, але є ризик хибних спрацювань для легітимних користувачів
Приховане сканування	Повільне сканування: 10 запитів на хвилину впродовж 10 хвилин (Xmas/Null/FIN техніки)	120	85	0	Труднощі з виявленням через низьку частоту запитів; допомагає поведінковий аналіз
Шахрайство з використанням VPN	Запит з IP-адреси, географічно не відповідної звичному шаблону користувача	12	95	5	Надійне виявлення геоаномалії; однак VPN може використовуватися і для легітимного доступу, що ускладнює аналіз

Тестове середовище було створено автором на віртуальній машині з операційною системою Ubuntu 22.04, де встановлено Python-реалізацію системи з бібліотеками scapy, geoip2, scikit-learn і pandas [7]. Для генерації трафіку використано інструменти, такі як hping3 для моделювання DDoS-атак і активного сканування, а також спеціально підготовлені скрипти для імітації фішингу та шахрайства [10]. Легітимний трафік симулювався через надсилання запитів із фіктивних IP-адрес, що представляють нормальну активність фінансових користувачів [20]. Усі тести проводилися в ізольованій мережі, щоб уникнути впливу на реальні системи, а дані про трафік записувалися для подальшого аналізу за допомогою модуля збору, описаного в розділі 4.1 [9]. Загалом було проведено п’ять сценаріїв, які охоплюють основні типи загроз, виявлених у розділі 2.1, що дозволяє оцінити систему в

різних умовах.

Перший сценарій тестування – моделювання активного сканування мережі. Цей тип атаки, описаний у MITRE ATT&CK, передбачає надсилання великої кількості запитів до діапазону IP-адрес для пошуку вразливостей [1]. У тесті використано hping3 для генерації 500 запитів за секунду з однієї IP-адреси протягом 5 хвилин. Система мала виявити аномально високу частоту запитів і заблокувати джерело. Модуль аналізу IP-адрес успішно ідентифікував загрозу за 10 секунд, а модуль реагування заблокував IP через iptables [9]. Рівень виявлення склав 100%, а помилкових спрацьовувань не зафіксовано, що свідчить про високу точність для відомих патернів [20].

Другий сценарій – імітація DDoS-атаки. У цьому тесті згенеровано масовий трафік із 10 різних IP-адрес, кожна з яких надсилала 200 запитів за секунду протягом 3 хвилин, що перевантажувало мережу [7]. Модуль збору трафіку фіксував дані, а модуль машинного навчання за допомогою алгоритму K-Means кластеризував IP-адреси, позначивши їх як аномальні через високу активність [11]. Час реакції склав 15 секунд, а рівень виявлення – 90%, оскільки одна IP-адреса з нижчою частотою була пропущена. Помилкових спрацьовувань не було, але результат вказує на потребу в оптимізації порогу чутливості для розподілених атак [16].

Третій сценарій – фішинг із підробленими IP-адресами. Для цього тесту створено скрипт, який імітував легітимний трафік із підозрілою IP-адресою, зареєстрованою в регіоні з високим рівнем кіберзлочинності (за даними MaxMind) [22]. Модуль геолокаційного аналізу визначив країну походження, а модуль машинного навчання класифікував IP як підозрілу на основі відхилення від нормальної поведінки [24]. Виявлення відбулося за 8 секунд із рівнем 100%, однак зафіксовано одне помилкове спрацьовування через легітимну IP із того ж регіону, що вказує на потребу в уточненні геолокаційних правил [13].

Четвертий сценарій – приховане сканування. Цей тест моделював низькочастотне сканування (10 запитів за хвилину протягом 10 хвилин) із

однієї IP-адреси, що ускладнює виявлення традиційними методами [28]. Модуль машинного навчання, навчений на історичних даних, розпізнав патерн за 2 хвилини, досягнувши рівня виявлення 85%. Помилкових спрацьовувань не було, але затримка вказує на необхідність вдосконалення алгоритмів для швидшого реагування на приховані загрози [11].

П’ятий сценарій – шахрайство з використанням VPN. У тесті IP-адреса з однієї країни імітувала доступ із іншої через підроблену геолокацію [25]. Модуль геолокаційного аналізу виявив невідповідність, а ML-модуль підтвердив аномалію за 12 секунд із рівнем виявлення 95%. Одне помилкове спрацьовування сталося через легітимного користувача з VPN, що підкреслює складність розрізнення таких випадків без додаткових даних [22].

В роботі автором визначено, що система ефективно виявляє більшість загроз із рівнем від 85% до 100%, що є високим показником для прототипу [20]. Найкращі результати досягнуто для активного сканування та фішингу завдяки чітким патернам і геолокаційним даним [1, 24]. DDoS-атака та шахрайство з VPN показали дещо нижчий рівень виявлення через складність розподіленого трафіку та маскування [7, 25]. Приховане сканування виявилося найскладнішим через затримку в реакції, що вимагає вдосконалення алгоритмів ML [11]. Помилкові спрацьовування (5%) зафіксовано лише в сценаріях із геолокацією, що вказує на потребу в додаткових ознаках для розрізнення легітимного трафіку [13].

Тестування підтвердило ефективність системи у виявленні загроз із середнім рівнем 94% і швидкістю реакції від 8 до 120 секунд. Вона відповідає потребам фінансових технологій, де важливі швидкість і точність [16]. Результати вказують на необхідність оптимізації для прихованих атак і зменшення помилок у геолокаційному аналізі, що стане основою для подальших досліджень [9]. Таблиця 4.1 демонструє збалансованість системи та її потенціал для реального впровадження [20].

4.3. Аналіз продуктивності та масштабованості

Аналіз продуктивності та масштабованості розробленої захисної системи для моніторингу та аналізу IP-трафіку є важливим етапом оцінки її готовності до використання в реальних умовах фінансових технологій. Продуктивність визначає, наскільки швидко й ефективно система обробляє трафік, виявляє загрози та реагує на них, що є критично важливим для фінансових систем, де затримки можуть призвести до втрати даних чи недоступності сервісів [16]. Масштабованість, своєю чергою, відображає здатність системи адаптуватися до зростання обсягів трафіку, кількості користувачів чи розширення інфраструктури, наприклад, через перехід на хмарні платформи [14]. Цей аналіз базується на результатах тестування, проведеного в контрольованому середовищі, і враховує специфіку реалізації на Python, описану в розділі 4.1, а також вимоги до продуктивності та масштабованості, визначені в розділі 3.1 [7]. Метою є оцінка поточного стану системи та виявлення напрямів її вдосконалення для забезпечення стабільної роботи в динамічному середовищі фінансових технологій [20].

Продуктивність системи оцінювалася за кількома ключовими показниками, які відображають її ефективність у реальних умовах. Першим показником є час обробки трафіку, який вимірює, скільки часу потрібно системі для збору, аналізу та реагування на пакети даних. У тестах, описаних у розділі 4.2, середній час реакції варіювався від 8 до 120 секунд залежно від типу загрози, наприклад, активне сканування виявлялося за 10 секунд, а приховане сканування – за 2 хвилини [11]. Ці результати свідчать про високу швидкість для чітких патернів, але вказують на затримки при аналізі складніших загроз, що пов’язано з обчислювальною складністю алгоритмів машинного навчання, таких як K-Means, реалізованих через scikit-learn [13]. Другим показником є пропускна здатність, тобто кількість пакетів, які система може обробити за секунду. У контрольованому середовищі з віртуальною машиною (4 ядра, 8 ГБ ОЗУ) система стабільно обробляла до 1000 пакетів за

секунду, що є достатнім для невеликих мереж, але може бути обмеженням для великих фінансових установ із мільйонами запитів [7]. Третім показником є використання ресурсів – у пікові моменти система споживала до 70% CPU і 60% пам’яті, що вказує на потребу в оптимізації для зменшення навантаження [9].

Для оцінки продуктивності використано кілька сценаріїв із різним навантаженням:

— Низьке навантаження (100 пакетів/с): Система працювала без затримок, обробляючи дані за 5-10 секунд із мінімальним використанням ресурсів (20% CPU, 30% ОЗУ). Це підтверджує її ефективність для невеликих мереж чи тестових середовищ [10].

— Середнє навантаження (500 пакетів/с): Час обробки зріс до 15-20 секунд, а використання CPU досягло 50%. Виявлення загроз залишалося точним, але затримки вказують на межі продуктивності для середніх систем [20].

— Високе навантаження (2000 пакетів/с): Система почала втрачати пакети, а час реакції перевищив 30 секунд із піковим використанням 80% CPU. Це свідчить про обмеження однопотокової реалізації в Python і потребу в розпаралелюванні [13].

Ці тести показали, що продуктивність системи є достатньою для базового використання, але потребує вдосконалення для роботи з великими обсягами трафіку, що характерно для фінансових технологій [16].

Масштабованість системи аналізувалася з точки зору її здатності адаптуватися до зростання навантаження та інфраструктури. Першим аспектом є горизонтальна масштабованість, тобто можливість розподілу обробки трафіку між кількома вузлами. Реалізація в Python дозволяє це через використання фреймворків, таких як multiprocessing чи asyncio, однак поточна версія системи працює в одному потоці, що обмежує її масштабування [7]. Наприклад, при додаванні другого віртуального вузла обробка 2000 пакетів/с скоротила час реакції до 20 секунд, але потребувала ручної синхронізації

даних між вузлами [14]. Другим аспектом є вертикальна масштабованість – підвищення продуктивності за рахунок збільшення ресурсів одного вузла. При збільшенні ОЗУ до 16 ГБ і CPU до 8 ядер система стабільно обробляла 3000 пакетів/с із часом реакції 25 секунд, що демонструє потенціал для масштабування в межах одного сервера [9]. Третім аспектом є адаптація до хмарних середовищ, де фінансовий сектор дедалі частіше розміщує свої сервіси [20]. Тестування в AWS EC2 (t2.medium) показало, що система може обробляти до 1500 пакетів/с без значних змін у коді, але потребує інтеграції з хмарними API для повноцінної роботи [2].

Основні фактори, що впливають на продуктивність і масштабованість системи, включають:

— Обчислювальна складність ML-алгоритмів: Використання K-Means і Random Forest у scikit-learn забезпечує точність, але збільшує час обробки при великих обсягах даних [11].

— Однопотокова природа Python: GIL (Global Interpreter Lock) обмежує паралельну обробку, що знижує продуктивність при високому навантаженні [13].

— Обмеження пам’яті: Зберігання великих наборів даних у pandas призводить до високого споживання ОЗУ, особливо при аналізі історичного трафіку [10].

— Залежність від мережевих ресурсів: Швидкість збору трафіку через scapy залежить від пропускної здатності інтерфейсу, що може бути вузьким місцем у реальних мережах [7].

— Інтеграція з зовнішніми сервісами: Запити до баз геолокації MaxMind чи API кіберрозвідки додають затримки, особливо при слабкому з’єднанні [22].

Ці фактори визначають поточні обмеження системи та вказують на напрями її вдосконалення.

Переваги системи з точки зору продуктивності та масштабованості включають:

— Швидка обробка при низькому та середньому навантаженні, що робить її придатною для невеликих фінансових мереж чи тестових середовищ [20].

— Гнучкість реалізації в Python, яка дозволяє легко адаптувати код до різних умов через широкий вибір бібліотек [16].

— Потенціал для масштабування через додавання ресурсів чи вузлів, що відповідає вимогам хмарних фінансових систем [14].

— Низьке споживання ресурсів при базовому використанні, що знижує витрати на апаратне забезпечення для малих організацій [9].

Недоліки, виявлені під час аналізу, такі:

— Затримки при високому навантаженні через однопотокову обробку та складність ML-алгоритмів, що обмежує використання в великих мережах [13].

— Втрата пакетів при перевищенні пропускної здатності, що може пропустити загрози в реальних умовах [7].

— Високе споживання пам’яті при аналізі великих даних, що потребує оптимізації роботи з pandas чи переходу на потокову обробку [10].

— Обмежена автоматична масштабованість без додаткових інструментів, таких як Kubernetes чи Docker, для розподілу навантаження [14].

Для підвищення продуктивності та масштабованості системи можна запропонувати кілька вдосконалень. По-перше, впровадження багатопотоковості через multiprocessing або асинхронного програмування з asyncio дозволить паралельно обробляти трафік, зменшуючи час реакції при високому навантаженні [7]. По-друге, оптимізація ML-алгоритмів, наприклад, заміна K-Means на більш легкі методи, такі як Isolation Forest, знизить споживання ресурсів [11]. По-третє, перехід на потокову обробку даних замість зберігання в пам’яті через pandas зменшить навантаження на ОЗУ [13]. По-четверте, інтеграція з хмарними платформами, такими як AWS чи Azure, із використанням їхніх інструментів масштабування підвищить адаптивність системи до великих мереж [2]. Ці заходи зроблять систему більш придатною

для фінансових технологій, де потрібна висока продуктивність і здатність до розширення [20].

Таблиця 4.2

Результати тестування ефективності виявлення загроз у мережевому трафіку

Параметр	Низьке навантаження (100 пакетів/с)	Середнє навантаження (500 пакетів/с)	Високе навантаження (2000 пакетів/с)	Примітка / Висновок
1	2	3	4	5
Час реакції на загрозу (с)	5–10	15–20	30+	Поступове зростання часу обробки; критично при DDoS чи складних атаках
Пропускна здатність (пакетів/с)	до 1000	до 1000	часткова втрата пакетів	До 1000 — стабільна робота; вище — система не встигає аналізувати увесь трафік
Використання CPU (%)	~20	~50	~80	Однопотокова реалізація призводить до пікового навантаження
Використання RAM (%)	~30	~45	~60	При зростанні обсягу даних спостерігається загроза перевантаження
Точність виявлення загроз (%)	100	95–100	85–90	Висока точність при шаблонних атаках; падає при комбінованих сценаріях
Втрати пакетів (%)	0	0	5–10	При перевищенні порогового навантаження починаються втрати даних

Продовження таблиці 4.2

1	2	3	4	5
Чутливість до складних атак	Висока	Стабільна	Низька	При складних багатокрокових атаках потрібна оптимізація алгоритмів машинного навчання
Можливість горизонтального масштабування	Обмежена (не використовується)	Обмежена (можлива при ручному налаштуванні)	Потребує розподілу навантаження на кілька вузлів	Необхідна реалізація мультивузлової обробки (Kubernetes, Docker, RabbitMQ тощо)
Можливість вертикального масштабування	Легко реалізується через розширення ресурсів	Позитивний вплив при збільшенні CPU/RAM	Висока потреба у ресурсах	Ефективне рішення для невеликих інсталяцій або ізольованих середовищ
Придатність до хмарної інфраструктури	Тестована, стабільна в EC2 на t2.medium	Придатна за умови оптимізації	Потребує масштабування та API-інтеграції	Потреба в адаптації до масштабованих хмарних архітектур (AWS Lambda, Azure Functions)

Аналіз продуктивності та масштабованості показав, що розроблена система ефективна при низькому та середньому навантаженні, обробляючи до 1000 пакетів/с із часом реакції 5-20 секунд, але стикається з обмеженнями при високому трафіку через однопотоковість і складність ML [16]. Вона має потенціал для масштабування через додавання ресурсів чи вузлів, але потребує оптимізації для великих фінансових систем [14]. Результати відповідають вимогам до базового захисту, однак для реального впровадження необхідно усунути вузькі місця, пов’язані з ресурсами та обробкою даних [9]. Подальший розвиток має фокусуватися на автоматизації масштабування та підвищенні продуктивності для забезпечення стабільності в динамічному середовищі [13].

4.4. Порівняння з існуючими рішеннями

Порівняння розробленої захисної системи для моніторингу та аналізу IP-трафіку з існуючими рішеннями є важливим етапом оцінки її конкурентоспроможності та практичної цінності в контексті фінансових технологій. Існуючі системи, такі як Check Point NGFW, Fortinet IPS, Splunk, SolarWinds IPAM і Darktrace, уже застосовуються для захисту мережевого трафіку від загроз, таких як DDoS-атаки, фішинг, приховане сканування та шахрайство [9, 12, 10, 2, 16]. Кожне з цих рішень має свої сильні сторони, але також обмеження, які впливають на їхню ефективність у динамічному середовищі фінансових систем [20]. Розроблена в роботі система, реалізована на Python із використанням машинного навчання, геолокаційного аналізу та модульного підходу, пропонує альтернативу, яка поєднує адаптивність і доступність [11]. Порівняння проводиться за ключовими критеріями, такими як функціональність, продуктивність, масштабованість, простота інтеграції та витрати, що дозволяє визначити її переваги й недоліки відносно комерційних продуктів [13]. Результати порівняння систематизовано в таблиці 4.3.

Таблиця 4.3

Порівняння розробленої системи з існуючими рішеннями

Параметр	Низьке навантаження (100 пакетів/с)	Середнє навантаження (500 пакетів/с)	Високе навантаження (2000 пакетів/с)	Примітка / Висновок
1	2	3	4	5
Час реакції на загрозу (с)	5–10	15–20	30+	Поступове зростання часу обробки; критично при DDoS чи складних атаках
Пропускна здатність (пакетів/с)	до 1000	до 1000	часткова втрата пакетів	До 1000 — стабільна робота; вище — система не встигає аналізувати увесь трафік

Продовження таблиці 4.2

1	2	3	4	5
Використання CPU (%)	~20	~50	~80	Однопотокова реалізація призводить до пікового навантаження
Використання RAM (%)	~30	~45	~60	При зростанні обсягу даних спостерігається загроза перевантаження
Точність виявлення загроз (%)	100	95–100	85–90	Висока точність при шаблонних атаках; падає при комбінованих сценаріях
Втрати пакетів (%)	0	0	5–10	При перевищенні порогового навантаження починаються втрати даних
Чутливість до складних атак	Висока	Стабільна	Низька	При складних багатокрокових атаках потрібна оптимізація алгоритмів машинного навчання
Можливість горизонтального масштабування	Обмежена (не використовується)	Обмежена (можлива при ручному налаштуванні)	Потребує розподілу навантаження на кілька вузлів	Необхідна реалізація мультивузлової обробки (Kubernetes, Docker, RabbitMQ тощо)
Можливість вертикального масштабування	Легко реалізується через розширення ресурсів	Позитивний вплив при збільшенні CPU/RAM	Висока потреба у ресурсах	Ефективне рішення для невеликих інсталяцій або ізольованих середовищ
Придатність до хмарної інфраструктури	Тестована, стабільна в EC2 на t2.medium	Придатна за умови оптимізації	Потребує масштабування та API-інтеграції	Потреба в адаптації до масштабованих хмарних архітектур (AWS Lambda, Azure Functions)

Першим критерієм порівняння є функціональність, тобто набір можливостей для виявлення та нейтралізації загроз. Check Point NGFW забезпечує глибокий аналіз пакетів (DPI) і сигнатурний захист від відомих атак, таких як активне сканування чи експлойти, але менш ефективний проти нових загроз без оновлення баз [9]. Fortinet IPS комбінує сигнатурний і поведінковий аналіз, що дозволяє виявляти DDoS і приховане сканування, однак потребує ретельного налаштування для уникнення помилкових спрацьовувань [12]. Splunk фокусується на аналізі логів і реальному часі, пропонуючи розширені можливості для виявлення аномалій, але вимагає значних ресурсів для обробки великих даних [10]. SolarWinds IPAM спеціалізується на управлінні IP-адресами та захисті від внутрішніх загроз, але не охоплює складні зовнішні атаки, такі як фішинг [2]. Darktrace використовує машинне навчання для прогнозування загроз, подібно до розробленої системи, і ефективний проти нових атак, але є дорогим і складним у впровадженні [16]. Розроблена система поєднує геолокацію, ML і базову фільтрацію, що дозволяє виявляти широкий спектр загроз із середнім рівнем 94% (за результатами розділу 4.2), але поступається комерційним рішенням у глибині сигнатурного аналізу [11].

Другим критерієм є продуктивність, яка визначає швидкість обробки трафіку та реагування на загрози. Check Point і Fortinet демонструють високу продуктивність, обробляючи десятки тисяч пакетів за секунду завдяки апаратному прискоренню, із часом реакції 1-5 секунд [9, 12]. Splunk залежить від конфігурації сервера, але в оптимальних умовах досягає подібних показників, хоча аналіз великих логів може займати до 10 секунд [10]. SolarWinds IPAM має нижчу продуктивність (до 5000 пакетів/с), оскільки фокусується на управлінні, а не реальному часі [2]. Darktrace обробляє тисячі пакетів за секунду з часом реакції 5-15 секунд, що порівнянно з розробленою системою, яка в тестах (розділ 4.3) показала 1000 пакетів/с і реакцію від 8 до 120 секунд [16]. Розроблена система поступається комерційним рішенням через однопотокову реалізацію в Python, але її продуктивність достатня для

невеликих мереж [7].

Третім критерієм є масштабованість, тобто здатність адаптуватися до зростання трафіку чи інфраструктури. Check Point і Fortinet підтримують горизонтальне та вертикальне масштабування через кластеризацію й апаратні модулі, що ідеально для великих фінансових систем [9, 12]. Splunk масштабується в хмарних і розподілених середовищах, але потребує значних вкладень у сервери [10]. SolarWinds IPAM має обмежену масштабованість, оскільки призначений для локальних мереж [2]. Darktrace легко адаптується до хмарних платформ завдяки AI-підходу, але вимагає інтеграції з мережевою інфраструктурою [16]. Розроблена система показала потенціал для масштабування (до 3000 пакетів/с при збільшенні ресурсів), але потребує багатопотоковості чи хмарних інструментів, таких як AWS, для роботи з великими обсягами [14]. Її перевагою є гнучкість коду, але вона поступається комерційним рішенням у готовності до масштабних мереж [13].

Четвертим критерієм є простота інтеграції з існуючими системами. Check Point і Fortinet легко інтегруються через стандартні протоколи (NetFlow, SNMP) і API, що робить їх сумісними з більшістю NGFW та IPS [9, 12]. Splunk підтримує широкий спектр логів і API, але потребує налаштування для специфічних систем [10]. SolarWinds IPAM інтегрується з мережевими пристроями, але обмежений у співпраці з комплексними рішеннями [2]. Darktrace пропонує API, однак його впровадження ускладнене через унікальну AI-логіку [16]. Розроблена система підтримує інтеграцію через API (requests) і NetFlow, але потребує адаптерів для роботи з різнорідними форматами, що робить її менш універсальною порівняно з комерційними продуктами [7]. Її перевагою є відкритий код, який дозволяє налаштування під конкретні потреби [18].

Останнім критерієм є витрати на впровадження та підтримку. Check Point і Fortinet мають високу вартість через апаратне забезпечення та ліцензії (тисячі доларів щорічно), що виправдано для великих організацій [9, 12]. Splunk також дорогий через підписки та серверні вимоги, орієнтований на

підприємства [10]. SolarWinds IPAM дешевший (від $1000/рік), але обмежений у функціоналі [2]. Darktrace є найдорожчим через AI-технології та консультативну підтримку (десятки тисяч доларів) [16]. Розроблена система має мінімальні витрати (лише на апаратне забезпечення та розробку), що робить її доступною для малих фінансових установ, але потребує інвестицій у оптимізацію для конкуренції з комерційними рішеннями [13].

Аналіз показав, що розроблена система конкурентоспроможна за функціональністю, поєднуючи ML і геолокацію, що наближає її до Darktrace, але поступається Check Point і Fortinet у сигнатурному аналізі [16, 9]. Її продуктивність і масштабованість нижчі через Python-реалізацію, але достатні для невеликих мереж [7]. Простота інтеграції середня, з перевагою у гнучкості коду [18]. Найсильніша сторона – низькі витрати, що робить її привабливою для малих організацій [13]. Недоліки включають обмеження в продуктивності та готовності до великих систем, що потребує оптимізації [20].

В роботі автором визначено, що розроблена система пропонує доступне рішення з адаптивними функціями, але поступається комерційним продуктам у продуктивності та масштабованості. Її переваги – низька вартість і гнучкість – роблять її перспективною для фінансових технологій із обмеженими ресурсами [11]. Подальший розвиток має фокусуватися на підвищенні продуктивності та інтеграції для конкуренції з лідерами ринку [9].

ВИСНОВКИ

Розробка моделі системи захисту мережевого трафіку, яка базується на скануванні IP-адрес і технологіях машинного навчання, стала відповіддю на зростаючу потребу фінансових технологій у ефективних засобах протидії сучасним кіберзагрозам. Проведене дослідження дозволило систематизувати теоретичні основи захисту трафіку, проаналізувати актуальні загрози та оцінити можливості існуючих рішень. На основі дослідження автором було розроблено систему для моніторінгу трафіку та виявлення загроз. У процесі роботи було досягнуто поставлену мету – розроблено та реалізовано програмне рішення, яке здатне моніторити IP-трафік, виявляти аномалії й реагувати на них у реальному часі, враховуючи специфіку фінансового сектору, де швидкість, точність і надійність є критично важливими.

Теоретичний аналіз показав, що основними загрозами для IP-трафіку у фінансових системах є розподілені атаки типу DDoS, фішинг, активне та приховане сканування, а також шахрайство, пов’язане з маніпуляцією IP-адресами. Ці загрози ускладнюються через використання зловмисниками динамічних IP, VPN і нових протоколів, таких як IPv6, що вимагає від захисних систем адаптивності та багатошарового підходу. Огляд сучасних систем безпеки, таких як Check Point, Fortinet чи Darktrace, виявив їхні сильні сторони, зокрема високу продуктивність і масштабованість, але також підкреслив обмеження, пов’язані з вартістю та складністю впровадження. Це стало основою для розробки власної системи, яка поєднує доступність із можливостями машинного навчання та геолокаційного аналізу.

Архітектура розробленої системи була спроектована як модульна структура, що включає збір трафіку, аналіз IP-адрес, геолокацію, машинне навчання та керування реагуванням. Такий підхід забезпечив гнучкість і потенціал для інтеграції з існуючими рішеннями, що є важливим для фінансових установ із різноманітною інфраструктурою. Використання технологій машинного навчання, зокрема алгоритмів кластеризації та

класифікації, дозволило системі прогнозувати нові загрози та зменшувати кількість помилкових спрацьовувань, що вигідно вирізняє її від традиційних сигнатурних методів. Реалізація на Python із застосуванням бібліотек scapy, geoip2 і scikit-learn підтвердила практичну здійсненність концепції, хоча й виявила певні обмеження в продуктивності при високих навантаженнях.

Експериментальні дослідження показали, що система ефективно виявляє основні типи загроз із середнім рівнем точності 94%, демонструючи найкращі результати для активного сканування та фішингу, але потребуючи вдосконалення для прихованого сканування через затримки в реакції. Аналіз продуктивності виявив, що система стабільно обробляє до 1000 пакетів за секунду в базових умовах, однак її однопотокова природа та високе споживання ресурсів при великих обсягах трафіку обмежують її застосовність у масштабних мережах. Масштабованість системи має потенціал для розвитку через додавання ресурсів чи розподіл навантаження, але вимагає впровадження багатопотоковості чи хмарних технологій для повноцінної адаптації до великих фінансових систем.

Порівняння з існуючими рішеннями підкреслило конкурентні переваги розробленої системи, зокрема низькі витрати та гнучкість коду, що робить її привабливою для малих і середніх фінансових організацій. Водночас вона поступається комерційним продуктам, таким як Check Point чи Darktrace, у продуктивності, масштабованості та глибині сигнатурного аналізу, що обумовлено прототипним характером реалізації. Проте її здатність поєднувати геолокацію з машинним навчанням відкриває можливості для подальшого розвитку, особливо в умовах зростання складності кібератак.

Дослідження підтвердило доцільність запропонованого підходу до захисту IP-трафіку у фінансових технологіях. Розроблена система є робочим прототипом, який відповідає базовим вимогам до виявлення загроз і може бути основою для створення більш досконалих рішень. Її впровадження в реальних умовах потребує оптимізації продуктивності, підвищення масштабованості та вдосконалення алгоритмів для роботи з прихованими загрозами. Перспективи

подальших досліджень включають інтеграцію з хмарними платформами, автоматизацію масштабування та розробку механізмів протидії обхідним технікам зловмисників, що забезпечить її відповідність еволюціонуючим викликам кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Active Scanning: Scanning IP Blocks. MITRE ATT&CK. URL: https://attack.mitre.org/techniques/T1595/001/ (дата звернення: 15.01.2025).

2. IP Address Scanner. SolarWinds. URL: https://www.solarwinds.com/ip-address-manager/use-cases/ip-address-scanner (дата звернення: 22.01.2025).

3. What is a Port Scan? Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-port-scan (дата звернення: 30.01.2025).

4. Network Security Assessment: Chapter 4. IP Network Scanning. O'Reilly. URL: https://www.oreilly.com/library/view/network-security-assessment/9780596510305/ch04.html (дата звернення: 05.02.2025).

5. Download Free Network Scanner. Advanced IP Scanner. URL: https://www.advanced-ip-scanner.com/ (дата звернення: 12.02.2025).

6. About Port and IP Address Scans. WatchGuard. URL: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/intrusionprevention/port_address_attacks_c.html (дата звернення: 18.02.2025).

7. Network Scanning Traffic Observed in Public Clouds. Palo Alto Networks. URL: https://unit42.paloaltonetworks.com/cloud-network-scanning-traffic/ (дата звернення: 25.02.2025).

8. 7 Best IP Scanner Tools for IP Scanning and Network Management. DNSstuff. URL: https://www.dnsstuff.com/ip-network-scanners (дата звернення: 02.03.2025).

9. What is a Port Scan? Check Point Software. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-a-port-scan/ (дата звернення: 08.03.2025).

10. Detecting Network and Port Scanning. Splunk Lantern. URL:

https://lantern.splunk.com/Security/UCE/Guided_Insights/Threat_hunting/Detecting_network_and_port_scanning (дата звернення: 10.03.2025).

11. The Design of Large Scale IP Address and Port Scanning Tool. MDPI. URL: https://www.mdpi.com/1424-8220/20/16/4423 (дата звернення: 17.01.2025).

12. What is an Intrusion Prevention System (IPS)? Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-an-ips (дата звернення: 23.01.2025).

13. Scanning the Internet for Liveness. ResearchGate. URL: https://www.researchgate.net/publication/326057896_Scanning_the_internet_for_liveness (дата звернення: 28.01.2025).

14. Who's Scanning the IPv6 Space? And Frankly, Why Do We Even Care? Akamai. URL: https://www.akamai.com/blog/security-research/vulnerability-scanning-IPv6-why-should-we-care (дата звернення: 03.02.2025).

15. What is Network Scanning? How to, Types and Best Practices. TechTarget. URL: https://www.techtarget.com/searchnetworking/definition/network-scanning (дата звернення: 10.02.2025).

16. Cybersecurity for Financial Services: Definitions & Examples. Darktrace. URL: https://darktrace.com/cyber-ai-glossary/cybersecurity-for-financial-services (дата звернення: 15.02.2025).

17. Top 10 Network Scanning Tools for 2025: The Ultimate Security Guide. SecOps Solution. URL: https://www.secopsolution.com/blog/top-10-network-scanning-tools (дата звернення: 20.02.2025).

18. A Comprehensive Guide to Angry IP Scanner: Features, Uses, and Installation Steps. Web Asha Technologies. URL: https://www.webasha.com/blog/a-comprehensive-guide-to-angry-ip-scanner-features-uses-and-installation-steps (дата звернення: 27.02.2025).

19. Vulnerability Scanner Services: Secure Your Network. Sikich. URL:

https://www.sikich.com/technology/cybersecurity/vulnerability-scanning/ (дата звернення: 04.03.2025).

20. Vulnerability Scanning: Unveiling Hidden Weaknesses in Fintech Infrastructure. Secarma. URL: https://secarma.com/fintech-infrastructure-vulnerability-scanning (дата звернення: 09.03.2025).

21. FinCEN Advisory FIN-2016-A005. FinCEN. URL: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005 (дата звернення: 12.01.2025).

22. 3 Ways Financial Institutions Can Use IP Data to Enhance Customer Experience. Spiceworks. URL: https://www.spiceworks.com/marketing/customer-experience/guest-article/financial-institutions-use-ip-data-to-enhance-customer-experience/ (дата звернення: 19.01.2025).

23. FIL-64-2005 Attachment. FDIC. URL: https://www.fdic.gov/news/financial-institution-letters/2005/fil6405a.html (дата звернення: 25.01.2025).

24. The Problem With How Most Banks Use IP Address Checks To Fight Fraud. PYMNTS.com. URL: https://www.pymnts.com/news/security-and-risk/2020/the-problem-with-how-most-banks-use-ip-address-checks-to-fight-fraud/ (дата звернення: 01.02.2025).

25. The Many Ways IP Address Manipulation Enables Fraud. Medium. URL: https://medium.com/the-socure-technology-blog/the-many-ways-ip-address-manipulation-enables-fraud-36527d207e68 (дата звернення: 08.02.2025).

26. TCP Idle Scanning Using Network Printers. ResearchGate. URL: https://www.researchgate.net/publication/239660144_TCP_Idle_Scanning_using_network_printers (дата звернення: 14.02.2025).

27. Impact, Vulnerabilities and Mitigation Strategies for Cyber-Secure Critical Infrastructure. MDPI. URL: https://www.mdpi.com/1424-8220/23/8/4060 (дата звернення: 21.02.2025).

28. Still Scanning IP Addresses? You’re Doing it Wrong. Trustwave. URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/still-scanning-

ip-addresses-youre-doing-it-wrong/ (дата звернення: 26.02.2025).

29. Top 9 Cybersecurity Regulations for Financial Services. UpGuard. URL: https://www.upguard.com/blog/cybersecurity-regulations-financial-industry (дата звернення: 03.03.2025).

30. Interagency Guidelines Establishing Information Security Standards. Federal Reserve. URL: https://www.federalreserve.gov/supervisionreg/interagencyguidelines.htm (дата звернення: 07.03.2025).

31. Information Technology (IT) and Cybersecurity. FDIC. URL: https://www.fdic.gov/banker-resource-center/information-technology-it-and-cybersecurity (дата звернення: 10.03.2025).

32. Private IP Address Disclosure. Beagle Security. URL: https://beaglesecurity.com/blog/vulnerability/private-ip-address-disclosure.html (дата звернення: 16.01.2025).

33. FAQ 73. Office of Foreign Assets Control. URL: https://ofac.treasury.gov/faqs/73 (дата звернення: 24.01.2025).

34. Directive (EU) 2022/2555. European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555 (дата звернення: 06.02.2025).

35. Intrusion Detection and Prevention (IDS/IPS). HowToNetwork. URL: https://www.howtonetwork.com/technical/security-technical/intrusion_detection_and_prevention/ (дата звернення: 13.02.2025).

ДОДАТКИ

```
import scapy.all as scapy
import geoip2.database
import pandas as pd
from sklearn.cluster import KMeans
from sklearn.ensemble import RandomForestClassifier
import os
import time
import json
import threading
import requests
from cryptography.fernet import Fernet
import tkinter as tk
from tkinter import messagebox

# Ключ для шифрування даних
key = Fernet.generate_key()
cipher = Fernet(key)

# Налаштування для інтеграції з API (симуляція)
API_URL = "http://example.com/api/threats"  # Замініть на реальний API для інтеграції
BLACKLIST_FILE = "blacklist.json"

# Модуль збору трафіку
class TrafficCollector:
    def __init__(self, interface="eth0"):
        self.interface = interface
        self.traffic_data = []
```

```
        def capture_traffic(self, count=100):
            print("Збір трафіку розпочато...")
            packets = scapy.sniff(iface=self.interface, count=count, timeout=60)
            for packet in packets:
                if packet.haslayer(scapy.IP):
                    ip_src = packet[scapy.IP].src
                    ip_dst = packet[scapy.IP].dst
                    timestamp = time.time()
                    encrypted_src = cipher.encrypt(ip_src.encode()).decode()
                    self.traffic_data.append({"src": encrypted_src, "dst": ip_dst,
"timestamp": timestamp})
            return pd.DataFrame(self.traffic_data)

    # Модуль аналізу IP-адрес
    class IPAnalyzer:
        def __init__(self):
            self.blacklist = self.load_blacklist()
            self.threshold = 100  # Поріг запитів за секунду

        def load_blacklist(self):
            try:
                with open(BLACKLIST_FILE, "r") as f:
                    return json.load(f)
            except FileNotFoundError:
                return {}

        def save_blacklist(self):
            with open(BLACKLIST_FILE, "w") as f:
                json.dump(self.blacklist, f)
```

```
        def analyze(self, df):
            decrypted_df = df.copy()
            decrypted_df['src'] = decrypted_df['src'].apply(lambda x: cipher.decrypt(x.encode()).decode())
            freq = decrypted_df.groupby('src').size() / (df['timestamp'].max() - df['timestamp'].min())
            suspicious_ips = freq[freq > self.threshold].index.tolist()
            blacklist_ips = [ip for ip in suspicious_ips if ip in self.blacklist]
            return decrypted_df, suspicious_ips, blacklist_ips

    # Модуль геолокаційного аналізу
    class GeoAnalyzer:
        def __init__(self):
            self.reader = geoip2.database.Reader('GeoLite2-Country.mmdb')

        def geolocation_analysis(self, ip):
            try:
                response = self.reader.country(ip)
                return response.country.name
            except:
                return "Unknown"

        def analyze(self, df):
            df['country'] = df['src'].apply(self.geolocation_analysis)
            anomalies = df[~df['country'].isin(["Ukraine", "USA"])]  # Приклад дозволених країн
            return anomalies['src'].tolist()

    # Модуль машинного навчання
```

```
class MLAnalyzer:
    def __init__(self):
        self.kmeans = KMeans(n_clusters=2, random_state=42)
        self.rf = RandomForestClassifier(n_estimators=100, random_state=42)
        self.train_model()

    def train_model(self):
        # Симуляція навчальних даних
        X_train = pd.DataFrame({
            'freq': [10, 20, 500, 30, 1000, 15],
            'port_count': [1, 2, 10, 3, 15, 1]
        })
        y_train = [0, 0, 1, 0, 1, 0]  # 0 - нормальний, 1 - аномалія
        self.rf.fit(X_train, y_train)

    def analyze(self, df):
        freq = df.groupby('src').size()
        features = pd.DataFrame({
            'freq': freq,
            'port_count': df.groupby('src')['dst'].nunique()
        }).fillna(0)
        kmeans_labels = self.kmeans.fit_predict(features)
        rf_labels = self.rf.predict(features)
        anomalies = features.index[kmeans_labels == 1].tolist() +
features.index[rf_labels == 1].tolist()
        return list(set(anomalies))  # Уникнення дублювання

# Модуль керування й реагування
class TrafficManager:
    def __init__(self):
```

```
        self.reports = []
        self.root = tk.Tk()
        self.root.title("Traffic Protection System")
        self.label = tk.Label(self.root, text="Система захисту трафіку")
        self.label.pack()
        self.root.withdraw()  # Приховуємо вікно за замовчуванням

    def block_ip(self, ip):
        os.system(f"iptables -A INPUT -s {ip} -j DROP")
        print(f"Заблоковано IP: {ip}")
        self.reports.append({"ip": ip, "timestamp": time.time(), "action":
"blocked"})

    def generate_report(self):
        with open("report.json", "w") as f:
            json.dump(self.reports, f)
        print("Звіт згенеровано: report.json")

    def integrate_with_api(self, suspicious_ips):
        try:
            response = requests.post(API_URL, json={"ips": suspicious_ips})
            if response.status_code == 200:
                print("Дані надіслано до зовнішньої системи")
        except:
            print("Помилка інтеграції з API")

    def show_alert(self, message):
        self.root.deiconify()  # Показуємо вікно
        messagebox.showwarning("Попередження", message)
        self.root.withdraw()  # Ховаємо після показу
```

```
# Основна система
class TrafficProtectionSystem:
    def __init__(self):
        self.collector = TrafficCollector()
        self.ip_analyzer = IPAnalyzer()
        self.geo_analyzer = GeoAnalyzer()
        self.ml_analyzer = MLAnalyzer()
        self.manager = TrafficManager()

    def run(self):
        while True:
            # Збір трафіку
            df = self.collector.capture_traffic(count=100)

            # Аналіз IP-адрес
            decrypted_df, suspicious_ips, blacklist_ips = self.ip_analyzer.analyze(df)

            # Геолокаційний аналіз
            geo_anomalies = self.geo_analyzer.analyze(decrypted_df)

            # Аналіз машинним навчанням
            ml_anomalies = self.ml_analyzer.analyze(decrypted_df)

            # Об’єднання результатів
            all_suspicious = list(set(suspicious_ips + geo_anomalies + ml_anomalies))

            # Реагування
```

```
            for ip in all_suspicious:
                if ip in blacklist_ips:
                    self.manager.block_ip(ip)
                else:
                    self.manager.show_alert(f"Виявлено підозрілу IP: {ip}")
                    self.ip_analyzer.blacklist[ip] = time.time()
            self.ip_analyzer.save_blacklist()

            # Інтеграція з API
            self.manager.integrate_with_api(all_suspicious)

            # Генерація звіту
            self.manager.generate_report()

            time.sleep(60)  # Пауза між циклами

if __name__ == "__main__":
    system = TrafficProtectionSystem()
    threading.Thread(target=system.run, daemon=True).start()
    system.manager.root.mainloop()  # Запуск GUI у головному потоці
```