Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

# КВАЛІФІКАЦІЙНА РОБОТА

Григоренка Вадима Олександровича

на здобуття ступеня вищої освіти магістра

Метод виявлення та протидії вторгненням в корпоративну мережу приватного підприємства

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ. 240191.24.01.06 ПЗ

Виконав студент 2 курсу група КБЗІм-24-1 Вадим ГРИГОРЕНКО
Керівник канд.техн.наук, доц. Віра ТІТОВА
Нормоконтролер д-р філософії, старший викладач Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
15 12 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри

кібербезпеки

Юрій КЛЬОЦ

1 09 2025 р.

**З А В Д А Н Н Я**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Григоренко Вадиму Олександровичу

1 Тема Метод виявлення та протидії вторгненням в корпоративну мережу приватного підприємства

Керівник роботи канд.техн.наук, доц.Віра ТІТОВА

Затверджено наказом ректора університету 25 08 2025 № 65

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.12.2025

3 Вихідні дані до роботи Необхідно здійснити вивчення та порівняння існуючих методів аналізу мережевого трафіку, включно з сигнатурними, статистичними, поведінковими та гібридними підходами. На основі зібраних даних необхідно розробити структуру аналізатора трафіку

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Необхідно розглянути сучасні підходи до аналізу мережевого трафіку, здійснити порівняння методів виявлення аномалій, описати структуру корпоративної мережі та особливості її інформаційної інфраструктури. Важливо сформулювати математичну модель процесу виявлення відхилень, розробити алгоритм функціонування системи та виконати експериментальні дослідження із застосуванням програмного прототипу

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6 Консультанти розділів кваліфікаційної роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| | | | |

7 Дата видачі завдання 1 09 2025 р.

## КАЛЕНДАРНИЙ ПЛАН

| Назва етапів (розділів) кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|
| Ґрунтовне ознайомлення та дослідження предметної галузі | | Виконано |
| Визначення змісту, структури магістерської роботи | | Виконано |
| Опрацювання першого розділу магістерської роботи | | Виконано |
| Опрацювання статті за результатами дослідження | | Виконано |
| Опрацювання другого розділу магістерської роботи | | Виконано |
| Опрацювання третього розділу магістерської роботи | | Виконано |
| Опрацювання четвертого розділу магістерської роботи | | Виконано |
| Підготовка та опрацювання ілюстративного матеріалу | | Виконано |
| Оформлення магістерської роботи графічної та текстової частини | | Виконано |
| Попередній захист магістерської роботи | | Виконано |
| Захист магістерської роботи на засіданні ЕК | | Виконано |

Студент _____ Вадим ГРИГОРЕНКО

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

# АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод виявлення та протидії вторгненням в корпоративну мережу приватного підприємства

Автор роботи: студент групи КБЗІм-24-1 Григоренко В.О.

Керівник роботи: к.т.н., доц. Тітова В.Ю

Загальний обсяг роботи: 89 сторінок, 13 рисунків, 6 таблиць, 9 формул, 63 посилань.

Ключові слова: мережеві атаки, вторгнення, IDS, аномалії, машинне навчання, мережевий трафік, ELK Stack, поведінковий аналіз.

У роботі досліджено проблему виявлення та класифікації мережевих вторгнень у корпоративних мережах, що актуально в умовах зростання кількості кіберзагроз і використання складних методів обходу систем захисту. Проведено аналіз сучасних підходів до виявлення атак, зокрема сигнатурних, статистичних, поведінкових та гібридних методів, Розроблено математичну модель процесу виявлення відхилень та створено програмний прототип аналізатора трафіку.

Створено програмний прототип системи виявлення аномалій, що включає модулі збору, обробки та аналізу мережевих подій, інтегровані з інструментами Elasticsearch, Logstash і Kibana. Експериментальні дослідження, проведені на побудованому тестовому середовищі з використанням реального мережевого обладнання та інструментів генерації атак (Metasploit, Nmap, Scapy),

04.12.2025

# ABSTRACT

Theme of qualification work: A method for detecting and counteracting intrusions into a private enterprise's corporate network

Author of the work: student of group KBZIm-24-1, Hryhorenko V.O.

Mentor: PhD in Technical Sciences, Associate Professor Titova V.Y.

Total volume of work: 89 pages, 13 figures, 6 tables, 9 formulas, 63 references.

Keywords: network attacks, intrusions, IDS, anomalies, machine learning, network traffic, ELK Stack, behavioral analysis.

The thesis examines the problem of detecting and classifying network intrusions in corporate environments, which is highly relevant due to the increasing number of cyber threats and the use of sophisticated methods to bypass security systems. A comprehensive analysis of modern approaches to attack detection is conducted, including signature-based, statistical, behavioral, and hybrid techniques. A mathematical model of the anomaly detection process has been developed, and a software prototype of a traffic analysis system has been implemented.

A prototype of an anomaly detection system was created, incorporating modules for collecting, processing, and analyzing network events, integrated with Elasticsearch, Logstash, and Kibana tools. Experimental studies were carried out in a controlled test environment using real network equipment and attack-generation tools (Metasploit, Nmap, Scapy), confirming the practical feasibility of the proposed approach.

01.12.2025

ЗМІСТ

Вступ ..... 7
1 Теоретичні основи виявлення та протидії вторгненням у корпоративних мережах ..... 11
1.1 Поняття класифікації та основні типи мережевих вторгнень ..... 11
1.2 Архітектура та принципи побудови систем виявлення та запобігання вторгненням (IDS/IPS) ..... 15
1.3 Аналіз сучасних підходів до захисту корпоративних мереж ..... 19
1.4 Огляд існуючих інструментів та рішень для моніторингу та реагування на інциденти ..... 24
1.5 Постановка задачі ..... 27
2 Моделі та методи виявлення і протидії вторгненням у корпоративній мережі ..... 30
2.1 Вимоги до системи виявлення вторгнень ..... 30
2.2 Моделі процесів виявлення вторгнень у мережевому трафіку ..... 33
2.3 Розробка алгоритму методу виявлення та протидії вторгненням ..... 40
2.4 Висновки до розділу 2 ..... 46
3 Реалізація, тестування та експериментальна перевірка ..... 49
3.1 Архітектура програмного комплексу ..... 49
3.2 Структура даних і модулі системи ..... 52
3.3 Методика тестування та результати ..... 55
3.4 Висновки до розділу 3 ..... 73
Висновок ..... 77
Список використаної літератури ..... 79
Додаток А ..... 84

# ВСТУП

Стрімкий розвиток інформаційних технологій та зростання обсягів даних, що циркулюють у корпоративних мережах, призводить до суттєвого підвищення рівня кіберзагроз, які щороку стають більш складними, адаптивними та цілеспрямованими. Сучасні приватні підприємства активно використовують мережеву інфраструктуру для підтримки бізнес-процесів, а тому їх трафік стає цінним об’єктом атаки. У таких умовах постає критична потреба у побудові ефективних механізмів виявлення відхилень у поведінці трафіку, здатних оперативно розпізнавати ознаки вторгнення, аномалій та спроб несанкціонованого доступу. Традиційні засоби контролю, що ґрунтуються виключно на сигнатурах відомих атак, дедалі частіше демонструють невисоку результативність у випадках нових або модифікованих загроз, які не відповідають встановленим шаблонам.

У зв’язку з переходом кіберзлочинців до використання складних методів обходу захисту, зростає значення поведінкового та статистичного аналізу трафіку, що дозволяє оцінювати мережеві події не за сигнатурами, а за їх відхиленням від нормальної моделі функціонування. Методи машинного навчання, зокрема алгоритми класифікації, кластеризації та виявлення аномалій, відкривають нові можливості для побудови систем інтелектуального аналізу, здатних адаптуватися до мінливих умов середовища та виявляти загрози, які ще не були формально описані.

Незважаючи на значний прогрес у розвитку IDS/IPS-рішень, питання порівняння ефективності різних методів аналізу трафіку в корпоративних мережах, їх здатності працювати з реальними даними, обробляти трафік у режимі близькому до реального часу та забезпечувати низький рівень хибнопозитивних спрацювань залишається актуальним. Особливої уваги потребують приватні підприємства, мережі яких часто характеризуються різнорідною структурою, нестабільним рівнем навантаження та обмеженими ресурсами для будівництва повноцінних центрів моніторингу.

Саме тому метою даної роботи є проведення комплексного порівняльного

аналізу методів виявлення аномалій у мережевому трафіку корпоративної мережі приватного підприємства, створення математичної моделі процесу аналізу та розробка експериментального програмного прототипу, придатного для дослідження різних підходів і оцінювання їхньої ефективності, що і визначає її актуальність.

Метою роботи є проведення порівняльного аналізу сигнатурних, статистичних, поведінкових та гібридних методів виявлення аномалій у мережевому трафіку корпоративної мережі приватного підприємства, побудова математичної моделі процесу виявлення відхилень та розробка програмного прототипу аналізатора трафіку для експериментального дослідження ефективності різних підходів.

Для досягнення поставленої мети необхідно розв’язати такі завдання:

– проаналізувати сучасні кіберзагрози, класифікувати основні типи мережевих атак та вторгнень;

– дослідити архітектуру та принципи роботи IDS/IPS-систем, визначити їхні переваги та обмеження;

– провести огляд сучасних методів аналізу та моніторингу мережевого трафіку, включно зі сигнатурними, статистичними, поведінковими та гібридними підходами;

– розробити математичну модель процесу виявлення аномалій у мережевому трафіку;

– створити алгоритм функціонування системи виявлення вторгнень на основі обраної моделі;

– розробити архітектуру та програмну реалізацію прототипу системи аналізу трафіку з використанням стеку ELK та додаткових інструментів;

– провести експериментальні дослідження, оцінити точність, продуктивність та ефективність різних методів

– надати рекомендації щодо впровадження отриманих результатів у корпоративних мережах.

Методи дослідження у роботі ґрунтуються на поєднанні теоретичних,

математичних та експериментальних підходів. Спочатку було виконано ґрунтовний аналіз наукових джерел, міжнародних стандартів та сучасних систем виявлення вторгнень, що дозволило сформувати теоретичну базу дослідження. Подальше моделювання мережевого трафіку здійснювалося методом математичного опису багатовимірних випадкових процесів, що дало змогу формалізувати поведінкові характеристики мережевих подій і визначити критерії відхилення. Статистичний аналіз параметрів трафіку застосовувався для оцінювання ступеня аномальності потоків, зокрема через використання метрик відстані та перевірки статистичних гіпотез. Для побудови моделей виявлення аномалій використовувалися алгоритми машинного навчання, які дали змогу порівняти ефективність різних підходів класифікації та кластеризації. Експериментальна частина дослідження виконувалася у тестовому середовищі з використанням реальних інструментів генерації атак (Metasploit, Nmap, Scapy) та аналітичної платформи ELK Stack, що забезпечило практичну перевірку працездатності запропонованих моделей. Сукупність цих методів дала можливість комплексно оцінити особливості поведінкового та сигнатурного аналізу, визначити їхні сильні та слабкі сторони та зробити обґрунтовані висновки щодо їх ефективності в умовах корпоративної мережі.

Наукова новизна роботи полягає у:

– поєднанні математичної моделі поведінкового аналізу з практичною експериментальною оцінкою роботи IDS/IPS та алгоритмів машинного навчання, виконаних на реалістичних даних корпоративного трафіку;

– удосконаленні підходу до виявлення аномалій шляхом використання гібридної моделі, що поєднує сигнатурний аналіз із поведінковим визначенням відхилень.

– розробці структурної моделі програмного аналізатора трафіку, оптимізованої для приватних підприємств з обмеженими ресурсами;

– запропонуванні методу оцінки ефективності різних моделей виявлення вторгнень у реальних умовах роботи корпоративної мережі.

Практична цінність роботи полягає у тому, що:

– розроблений програмний прототип системи виявлення аномалій може бути використаний як основа для впровадження реальних систем моніторингу у корпоративних мережах;

– отримані результати експериментальних досліджень дають можливість обґрунтувати вибір оптимального методу аналізу трафіку залежно від умов роботи підприємства;

– запропоновані алгоритми та структура аналізатора можуть бути інтегровані з популярними платформами безпеки (ELK Stack), що полегшує їх використання у практиці;

– робота може слугувати методичним матеріалом для подальших досліджень у сфері кібербезпеки, а також основою для створення удосконалених систем IDS/IPS.

# 1 ТЕОРЕТИЧНІ ОСНОВИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ВТОРГНЕННЯМ У КОРПОРАТИВНИХ МЕРЕЖАХ

## 1.1 Поняття класифікації та основні типи мережевих вторгнень

У сучасних корпоративних мережах забезпечення кібербезпеки є одним із ключових аспектів стабільності бізнес-процесів. Більшість підприємств значною мірою покладаються на цифрові інструменти, що робить їхню інфраструктуру привабливою ціллю для зловмисників. За цієї умови особливого значення набуває систематичне виявлення вторгнень і реагування на них, оскільки навіть поодинокий успішний інцидент може завдати значної шкоди підприємству. Усі процеси, пов'язані з протидією загрозам, ґрунтуються на чітких визначеннях базових понять, таких як кібератака, вторгнення, інцидент інформаційної безпеки. Кібератака означає будь-яку навмисну дію, спрямовану на порушення роботи інформаційної системи чи отримання несанкціонованого доступу до ресурсів. Вторгнення, на відміну від кібератаки, є результативною фазою, коли механізми захисту були обійдені, і зловмисник отримав змогу взаємодіяти з внутрішніми ресурсами підприємства. Інцидент безпеки розглядається як подія, що свідчить про виявлення підозрілої активності, і не обов’язково означає успішний злам, але потребує аналізу та оцінювання.

У контексті корпоративного середовища особливої уваги заслуговує класифікація атак, що дозволяє вибудувати ефективну систему захисту. На рівні мережевих протоколів загрози проявляються у вигляді перевантаження ресурсів інтенсивним потоком шкідливого трафіку, неконтрольованого збільшення кількості з'єднань або маніпуляцій з адресацією пакетів. Наприклад, DDoS-атаки спрямовані на створення надмірного навантаження, яке блокує доступність сервера. Приклад DDOS атаки наведено на рисунку 1.1 Сканування портів є прихованим способом дослідження мережевої інфраструктури, коли зловмисник намагається визначити, які сервіси активно працюють на конкретному хості. Завдяки цьому він отримує карту доступних точок входу та

слабких місць у конфігурації системи, що надалі може бути використано для підбору експлойтів.

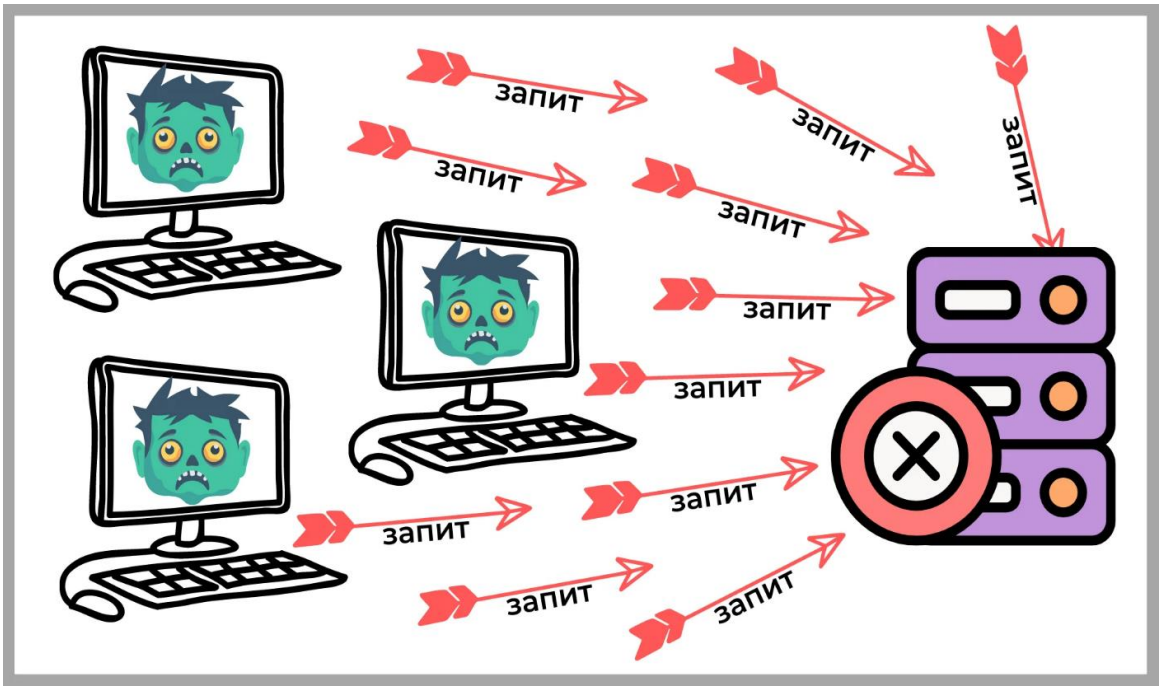


Рисунок 1.1 - Приклад DDOS атаки

Спуфінг адрес націлений на підміну інформації про джерело трафіку, що дозволяє обманювати системи автентифікації. Приклад Спуфінга наведено на рисунку 1.2 На найнижчих рівнях мережевої моделі зустрічаються також атаки, пов’язані з перехопленням даних, коли потік пакетів аналізується у відкритих мережах, а зловмисник отримує необмежений

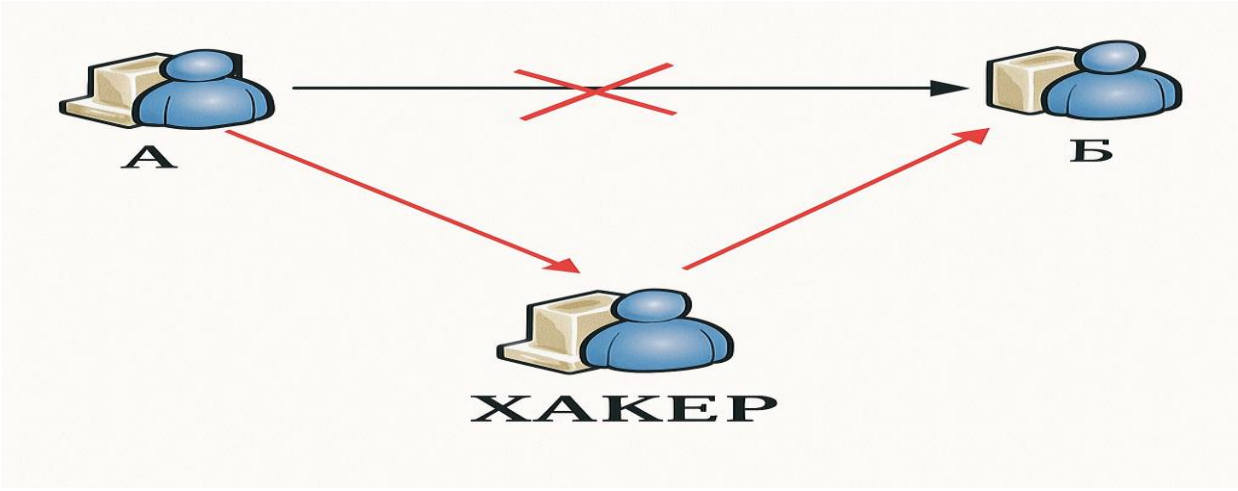


Рисунок 1.2 - Приклад спуфінга

Окремим підкласом загроз виступають атаки на прикладному рівні, де об'єктом впливу є конкретний вебдодаток, сервер або сервіс. Уразливості вебформи можуть стати точкою входу для SQL-ін’єкцій, коли шкідливий код впроваджується у запит і дозволяє проводити операції над базою даних у неконтрольованому режимі. Схема роботи SQL ін’єкції наведена на рисунку 1.3 У випадку міжсайтових сценарних ін’єкцій зловмисник намагається примусити браузер користувача виконувати небезпечні скрипти. Часто використовуються методи віддаленого виконання коду, коли помилка у програмі відкриває шлях для запуску шкідливих інструкцій. До прикладних атак належить і підбір паролів за допомогою автоматизованих інструментів, де багаторазові спроби входу здійснюються з різними варіантами облікових даних. Вразливості протоколів, таких як SMB або RPC, дозволяють використовувати недосконалості реалізації служб і отримувати контроль над системами, що працюють у внутрішній мережі.

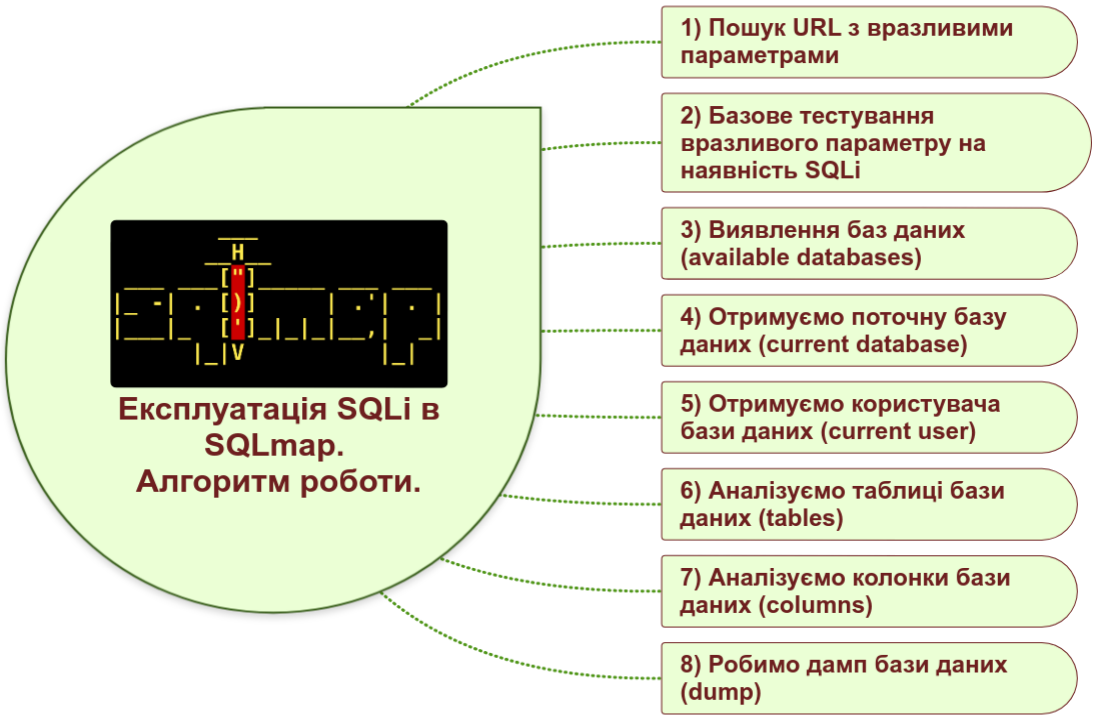


Рисунок 1.3 - Схема роботи SQL ін’єкції

Поза суто технічними аспектами значну роль відіграють соціоінженерні методи, які ґрунтуються на психологічному впливі. У корпоративних мережах вони часто виявляються через фішингові повідомлення, що імітують внутрішню комунікацію та спонукають користувача перейти за небезпечним посиланням або надати конфіденційні дані. Таргетовані атаки на конкретних співробітників використовують персоналізовані повідомлення, які виглядають вкрай правдоподібно. У найнебезпечніших випадках зловмисники намагаються отримати доступ до інформації топ-менеджерів, оскільки їхні облікові записи найчастіше містять критично важливі дані. Соціоінженерія також може проявлятися через телефонні дзвінки, підроблені документи або особисті контакти, які створюють враження легітимності.

Сукупність таких загроз формує складне середовище, у якому ознаки вторгнення не завжди очевидні. У стабільних корпоративних мережах існують характерні показники «нормальної» діяльності, що включають обсяги трафіку, час активності співробітників, типові маршрути передачі даних та регулярність виконання службових процесів. Відхилення від цих параметрів часто свідчать про загрозу. Різке зростання інтенсивності трафіку, множинні невдалі спроби входу, звернення до внутрішніх сервісів у нетипові години, раптове збільшення кількості DNS-запитів або підозрілі передачі даних за межі локальної мережі – усе це може бути індикатором початку атаки. Багато сучасних вторгнень мають прихований характер і намагаються маскуватися під легітимні дії, що зумовлює потребу в глибоких методах поведінкового аналізу.

Аналіз вторгнень передбачає також розуміння їхньої типової структури. Більшість сучасних атак реалізуються у кілька етапів. Початковий етап зазвичай полягає у збиранні інформації про мережу, її структуру та потенційні вразливості. Після того, як зловмисник виявляє слабке місце, відбувається спроба його експлуатації, у результаті чого він може закріпитися у системі. Далі часто створюється канал віддаленого керування, через який атакувальник отримує змогу координувати свої дії та розширювати рівень доступу. Фінальною частиною вторгнення часто є ексфільтрація даних – тобто

приховане вилучення важливої інформації або її шифрування з подальшим вимаганням викупу.

Таким чином, питання виявлення вторгнень у корпоративних мережах охоплює як технічні, так і поведінкові аспекти. Ефективна система повинна враховувати різноманітність загроз, складність схем атак та можливість їхнього поступового розвитку. Саме тому аналітика мережевого трафіку, моделювання поведінки користувачів та багаторівневі методи моніторингу мають ключове значення для своєчасного реагування та попередження інцидентів.

## 1.2 Архітектура та принципи побудови систем виявлення та запобігання вторгненням (IDS/IPS)

Системи виявлення та запобігання вторгненням є невід'ємним компонентом сучасної архітектури безпеки корпоративних мереж. Роль цих систем полягає у тому, щоб забезпечити безперервний контроль усіх процесів, які відбуваються як на рівні мережевого трафіку, так і всередині окремих хостів, своєчасно фіксувати підозрілу активність та ініціювати захисні дії у разі виявлення небезпеки. У той час як класичні механізми захисту, такі як фаєрволи або засоби контролю доступу, були розроблені для фільтрації небажаного трафіку та обмеження прав доступу, системи IDS/IPS стали відповіддю на ті загрози, які здатні обходити традиційні бар'єри та проникати в мережу за допомогою складних технік.

Основна відмінність між IDS і IPS зводиться до їхньої поведінки після виявлення загрози. Система IDS виконує функцію спостереження, аналізує події та формує сповіщення, які передаються адміністраторам або SIEM-системам. Її завдання полягає у точній ідентифікації підозрілих патернів, що можуть свідчити про атаку. Натомість IPS працює у режимі реального часу і здатна автоматично блокувати шкідливий трафік або розривати небезпечні сесії. Схема порівняння IDS/IPS наведена на рисунку 1.4. Таке рішення

дозволяє зменшити ризик успішного вторгнення, однак накладає значні вимоги до точності виявлення: надмірна кількість хибнопозитивних спрацювань може призвести до блокування легітимних операцій, що критично для високонавантажених корпоративних систем.

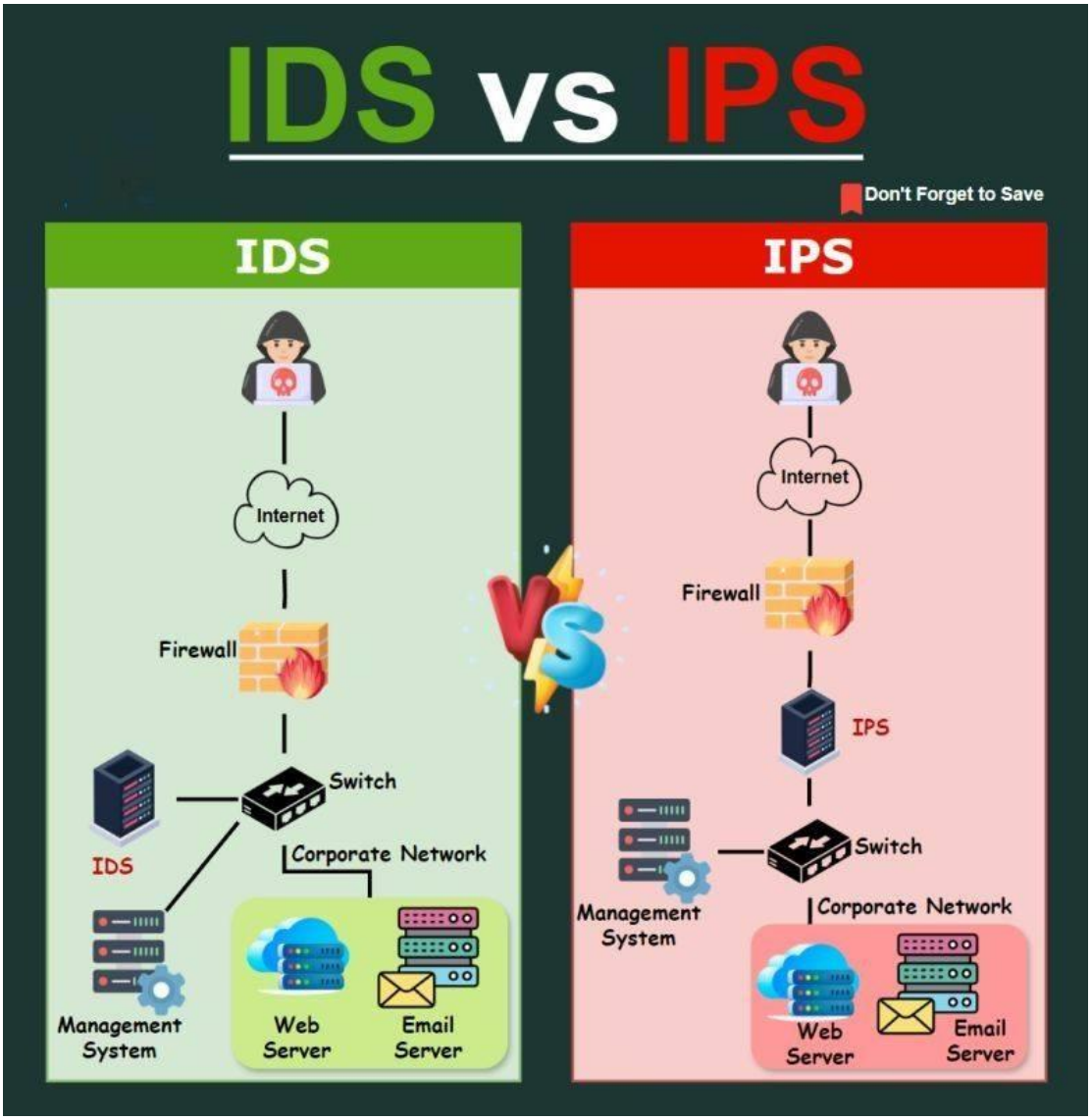


Рисунок 1.4 - Схема порівняння IDS/IPS

Архітектурно IDS і IPS можуть бути реалізовані у вигляді мережевих, хостових та гібридних систем. Мережеві системи зазвичай розміщують у ключових точках інфраструктури, зокрема на межі між внутрішньою та зовнішньою мережами або всередині сегментованої структури підприємства. Такі рішення аналізують потік даних, який проходить через мережеві

інтерфейси, що дозволяє виявити підозрілу поведінку ще на ранніх етапах атаки. Хостові системи, навпаки, працюють безпосередньо на кінцевих пристроях. Вони мають доступ до локальних журналів подій, системних викликів, облікового обладнання та внутрішніх ресурсів операційної системи. Їхня перевага полягає у можливості надзвичайно детального аналізу кожної конкретної дії, що здійснюється в межах робочої станції або сервера.

У сучасних корпоративних мережах дедалі частіше використовуються гібридні рішення, які поєднують можливості мережевих та хостових систем. Такі комплекси забезпечують багаторівневий захист: мережевий аналіз дозволяє спостерігати загальну картину трафіку, тоді як хостові агенти забезпечують глибоке розуміння того, що відбувається всередині окремих систем. Цей підхід є особливо ефективним у великих компаніях, де кожен рівень інфраструктури має власні типи загроз.

Ключовим елементом класифікації IDS/IPS є метод, за допомогою якого вони виявляють потенційно шкідливу активність. Історично першим став сигнатурний метод, який орієнтується на виявлення відомих шаблонів атак. За наявності детальної бази сигнатур система може швидко та точково визначати конкретні загрози. Проте суттєвий недолік цього підходу полягає у його нездатності розпізнати нові, невідомі атаки, які ще не були формалізовані у вигляді сигнатур. Крім того, сигнатурні методи вимагають постійного оновлення бази даних, що може бути складним завданням у динамічному середовищі, де кількість загроз постійно зростає.

Аномалійні системи працюють за протилежним принципом і ґрунтуються на виявленні відхилень від нормальної поведінки мережі або користувача. Для цього зазвичай будуються моделі нормальної активності, які визначають очікувані параметри трафіку, частоту дій, часові закономірності або структуру запитів. У разі, якщо поточний трафік виходить за межі сформованої моделі, система може трактувати це як потенційну атаку. Перевага аномалійного підходу полягає в тому, що він здатний фіксувати навіть невідомі або нестандартні загрози. Однак для цього потрібні складні алгоритми машинного

навчання та великий обсяг якісних даних, які відображають реальну поведінку мережі. У разі неправильного навчання такі системи можуть генерувати значну кількість хибнопозитивних сповіщень.

Комбіновані системи, що інтегрують сигнатурний і аномалійний підходи, сьогодні вважаються найбільш ефективними у корпоративному середовищі. Вони дозволяють одночасно виявляти як відомі загрози, так і ті, що ще не були класифіковані. Завдяки поєднанню методологій такі системи забезпечують високу точність аналізу і здатність адаптуватися до нових умов. У багатьох виробничих середовищах комбіновані підходи втілюються у вигляді інтеграції IDS/IPS із системами SIEM, які виконують загальну кореляцію, аналіз часових закономірностей та відображення всієї інформації у вигляді структурованих звітів.

У загальній архітектурі інформаційної безпеки підприємства IDS/IPS відіграють роль проміжної ланки між фаєрволами, що фільтрують трафік відповідно до політик доступу, та системами моніторингу, які збирають інформацію про події. Традиційний фаєрвол може блокувати трафік за портом або IP-адресою, але він не здатний аналізувати вміст пакетів та поведінку користувачів. Тому IDS/IPS фактично розширюють можливості контролю і забезпечують глибший рівень перевірки. У корпоративному середовищі вони часто інтегруються зі службами Active Directory, платформами моніторингу хостів, хмарними системами, аналітичними платформами та інструментами автоматизації реагування.

З технічного погляду архітектура IDS/IPS включає кілька функціональних модулів, зокрема модуль збору та нормалізації даних, модуль аналізу, модуль кореляції та модуль реагування. На стадії збору система отримує інформацію як з мережевого трафіку, так і з журналів подій, системних логів, даних серверів або хмарних платформ. Нормалізація трафіку дозволяє привести всі пакети до єдиного формату, що є необхідним для подальшого аналізу. Модуль аналізу відповідає за порівняння інформації з базами сигнатур або з моделями поведінки. У складніших системах модуль кореляції поєднує декілька подій у

єдиний інцидент, визначаючи його природу та рівень небезпеки. Модуль реагування, залежно від типу системи, може або надіслати повідомлення адміністратору, або ініціювати автоматичне блокування трафіку.

Варто зазначити, що сучасний розвиток IDS/IPS значною мірою пов’язаний із застосуванням машинного навчання та штучного інтелекту. Такі системи здатні виявляти складні шаблони атак, що не мають простих сигнатур. Методи кластеризації, автоенкодери, дерева рішень та нейронні мережі дозволяють формувати точніші моделі, які адаптуються до змін. Проте впровадження таких рішень має певні виклики, серед яких необхідність великого обсягу навчальних даних, складність налаштування і потенційний ризик надмірної чутливості.

Таким чином, IDS/IPS є фундаментальним інструментом у забезпеченні кібербезпеки корпоративних мереж. Вони дозволяють контролювати події на різних рівнях, виявляти як відомі, так і нові типи атак, взаємодіяти з іншими компонентами інфраструктури та забезпечувати багаторівневий захист організації. Ефективність цих систем значною мірою залежить від їхньої здатності до адаптації, точності аналізу та правильної інтеграції в загальну архітектуру підприємства.

## 1.3 Аналіз сучасних підходів до захисту корпоративних мереж

Сучасні корпоративні мережі є складними багаторівневими структурами, у яких щодня циркулюють значні обсяги даних, виконуються критично важливі бізнес-процеси та взаємодіють численні пристрої, сервери й сервіси. Дедалі більше компаній переходять до хмарних середовищ, використовують розподілені структури та інтегрують віддалених співробітників до єдиного інформаційного простору. Такі зміни значно розширюють поверхню атаки, а отже – потребують впровадження новітніх, більш інтелектуальних і гнучких підходів до захисту. Традиційні інструменти безпеки, хоча й залишаються

важливыми, вже не здатні повною мірою протидіяти складним багатовекторним атакам, що постійно еволюціонують.

Одним із ключових сучасних концептуальних підходів до захисту корпоративних мереж є модель Zero Trust, що повністю змінює класичне уявлення про довіру в інформаційних системах. Сім принципів нульової довіри наведено на рисунку 1.5. Якщо раніше внутрішнім вузлам, що знаходилися у межах корпоративного периметру, автоматично надавалася довіра, то в Zero Trust вихідною позицією є припущення, що загроза може виходити з будь-якої точки мережі, включно з легітимних пристроїв і користувачів. Тому кожна взаємодія, кожен запит, кожне підключення мають бути перевірені відповідно до суворих правил автентифікації та авторизації. Перехід до Zero Trust передбачає постійне підтвердження особи, контроль контексту доступу, обмеження привілеїв, мікросегментацію мережі та моніторинг поведінки користувачів. У результаті навіть якщо окремий хост буде скомпрометовано, це не дасть змоги зловмиснику вільно переміщатися мережею.


Рисунок 1.5 - Сім принципів нульової довіри

Поряд із Zero Trust активно застосовується стратегія Defense-in-Depth, або багаторівневий захист. схема старетегії Defense-in-Depth наведено на рисунку 1.6. Цей підхід розглядає корпоративну мережу як комплекс багатьох шарів, кожен з яких має власні засоби захисту. Ідея полягає в тому, щоб створити ситуацію, коли навіть успішне подолання одного захисного механізму не дає змоги зловмиснику просунутися далі без додаткових зусиль. Наприклад, навіть якщо фаєрвол пропустить небезпечний трафік, IDS або аналізатор логів може зафіксувати підозрілу активність, а система контролю доступу – заблокувати подальші дії. Така взаємодія захисних механізмів підвищує стійкість системи в умовах активних та координованих атак.


Рисунок 1.6 - Схема стратегії Defense-in-Depth

Важливою складовою сучасних підходів до захисту корпоративних мереж є впровадження SOC-центрів (Security Operations Center), які забезпечують централізований моніторинг, аналіз та реагування на кіберінциденти. Ключові ролі та обов’язки команди SOC зображено на рисунку 1.7. SOC працюють на основі широкого набору інструментів: SIEM-платформ, систем виявлення аномалій, аналітичних засобів машинного навчання, інтелектуальних модулів кореляції подій. Завдяки такій інтеграції SOC дає змогу не лише швидко виявляти атаки, а й прогнозувати потенційні загрози, оцінювати ризики, а також будувати довгострокову стратегію кіберзахисту. У великих організаціях

SOC є ядром інформаційної безпеки, яке забезпечує цілодобове реагування та контроль за відповідністю політик безпеки.


Рисунок 1.7 - Ключові ролі та обов'язки команди SOC

Особливу увагу привертає роль SIEM-систем, що стали стандартом у великих корпоративних мережах. Вони виконують функції збору журналів подій, кореляції, аналітики та централізованого відображення стану безпеки. На основі правил кореляції та поведінкової аналітики SIEM здатні виявляти складні багатоступеневі атаки, які непомітні окремим інструментам. Важливо, що SIEM інтегрується з IDS, IPS, фаєрволами, антивірусами, хмарними службами та системами доступу, формуючи єдиний інформаційний простір безпеки. Таким чином, організація має цілісне уявлення про те, що відбувається у всіх сегментах інфраструктури.

Останніми роками особливої популярності набули методи машинного навчання та поведінкового аналізу, які дозволяють будувати моделі нормальної поведінки користувачів і сервісів, а відхилення від таких моделей вважаються потенційними ознаками атаки. На відміну від класичних сигнатурних методів, поведінкові системи здатні виявляти невідомі загрози, які не мають

формального опису. Вони ґрунтуються на математичному аналізі часових рядів, статистичних відхилень, кластеризації дій, а також використанні нейронних мереж, які можуть визначати складні взаємозв'язки у даних. Такий підхід особливо ефективний у випадках багатовекторних атак, коли зловмисник діє приховано і повільно, поступово збільшуючи свою присутність у мережі.

Сучасні корпоративні мережі дедалі частіше використовують автоматизовані системи реагування, що дозволяють скоротити час між виявленням інциденту та відповіддю на нього. Автоматизація може включати блокування підозрілих IP-адрес, ізоляцію заражених хостів, відключення облікових записів або запуск додаткових механізмів перевірки. Перевага автоматизованих систем полягає у тому, що вони мінімізують людський фактор і значно скорочують час, який потрібен для ліквідації загрози. Водночас неправильна конфігурація таких систем може призвести до небажаних блокувань або порушення критичних сервісів, тому їхнє впровадження потребує високого рівня професіоналізму.

Варто також зазначити, що важливою тенденцією розвитку систем захисту корпоративних мереж є перехід до хмарних технологій та використання розподілених систем моніторингу. У великих компаніях, що застосовують мультихмарні архітектури або розподілені офісні структури, надзвичайно важливою є можливість централізованого контролю та швидкої синхронізації даних між різними регіонами. Хмарні платформи, такі як AWS GuardDuty чи Microsoft Sentinel, забезпечують автоматичне масштабування, гнучкість конфігурації та високу точність аналізу завдяки використанню глобальних баз загроз.

Спеціалісти з кібербезпеки також відмічають зростання інтересу до методологій прогнозної аналітики, коли система не просто реагує на події, а намагається передбачити поведінку користувачів і потенційні сценарії розвитку загроз. Така аналітика використовує алгоритми машинного навчання для виявлення закономірностей у діях користувачів та сервісів. Це дозволяє попередити атаку до того, як вона досягне критичного рівня.

Узагальнюючи сучасні підходи до захисту корпоративних мереж, можна стверджувати, що ефективність значною мірою залежить від здатності системи забезпечувати безперервний контроль, адаптуватися до швидких змін загроз, взаємодіяти з іншими інструментами та забезпечувати гнучке реагування у режимі реального часу. Комбінація Zero Trust, Defense-in-Depth, використання SOC/SIEM та поведінкового аналізу формує основу сучасної парадигми кіберзахисту. Такий багатьма рівнями підсилений підхід дозволяє суттєво підвищити стійкість корпоративних систем до як відомих, так і нових типів атак.

## 1.4 Огляд існуючих інструментів та рішень для моніторингу та реагування на інциденти

Ефективний захист корпоративної мережі неможливо забезпечити без спеціалізованих інструментів, здатних моніторити події, аналізувати трафік, виявляти вторгнення та забезпечувати адекватну реакцію на інциденти. Розвиток кіберзагроз стимулює появу нових аналітичних платформ, інтегрованих рішень та інтелектуальних систем, здатних працювати в умовах високої динаміки подій і значної кількості даних. У цьому контексті надзвичайно важливо розуміти сучасний стан ринку засобів безпеки, оскільки вибір інструментів визначає загальну здатність організації протистояти складним багатовекторним атакам та забезпечувати стабільність інформаційних систем.

Однією з найвідоміших та найпоширеніших у світі систем для аналізу трафіку є Snort, яка завдяки своїй гнучкості, відкритому вихідному коду та широким можливостям конфігурації стала стандартом де-факто в багатьох компаніях. Snort працює на основі глибокого аналізу пакетів та сигнатурного підходу, який дозволяє точно визначати конкретні види атак. Важливо, що Snort постійно оновлюється, має велику спільноту користувачів і розробників, а

також використовується як основа для комерційних рішень Cisco. Втім, її сигнатурна природа обмежує здатність виявляти нові, невідомі атаки, що потребує додаткових інструментів або інтеграції з поведінковими системами.

Більш сучасною альтернативою Snort є Suricata, яка також працює на рівні аналізу пакетів, але має багатопотокову архітектуру, що дозволяє обробляти значно більші обсяги трафіку. Suricata підтримує сигнатурний аналіз, однак доповнює його можливістю визначати аномалії протоколів, аналізувати TLS- і HTTP-сесії, а також інтегрувати дані з різних джерел. Особливістю Suricata є здатність одночасно виконувати IDS- і IPS-функції, а також генерувати повний набір метаданих, які можуть бути передані до SIEM-систем для подальшої кореляції. У великих компаніях Suricata часто використовується як частина гібридної платформи моніторингу.

Ще одним важливим інструментом у сфері аналізу мережевого трафіку є Zeek (раніше Bro), який відрізняється від Snort і Suricata не акцентом на сигнатурному пошуку, а підходом до поведінкового аналізу та генерації високорівневих логів. Zeek фактично не намагається безпосередньо блокувати атаки, а перетворює трафік у структуровані журнали, на основі яких можна виявляти аномалії, будувати довірчі моделі та оцінювати мережеву поведінку. Завдяки гнучкій мові скриптів Zeek дозволяє створювати власні політики детекції, що робить його популярним серед аналітиків SOC та дослідників кібербезпеки. У складних корпоративних мережах Zeek часто використовується разом із Snort або Suricata, забезпечуючи двовекторний підхід до аналізу.

Для контролю за станом окремих хостів у корпоративному середовищі значну роль відіграють хостові IDS-рішення, такі як OSSEC і Wazuh. Їхня функціональність охоплює аналіз журналів подій, контроль цілісності критичних файлів, моніторинг системних конфігурацій та виявлення змін, які можуть свідчити про проникнення. OSSEC став одним із перших широко доступних рішень з відкритим кодом, що дозволяє розгортати багаторівневу інфраструктуру моніторингу. На його основі пізніше було створено Wazuh – значно розширену систему, яка інтегрується з Elasticsearch, Kibana та іншими

платформами візуалізації. Для великих підприємств Wazuh є привабливим завдяки можливості централізованого керування тисячами агентів на робочих станціях і серверах.

Серед інтегрованих рішень для аналізу трафіку, журналів та виявлення вторгнень особливе місце займає платформа Security Onion, яка об’єднує в собі декілька інструментів, включно з Zeek, Suricata, Wazuh, Elastic Stack та іншими компонентами. Security Onion надає можливість створити повноцінну систему моніторингу та реагування, що включає логування, фільтрацію, кореляцію подій, інтерактивну візуалізацію та автоматичне оновлення. Такий комплекс дозволяє одночасно аналізувати поведінку мережі, контролювати стан хостів, відстежувати підозрілі активності та формувати структуровану базу інцидентів. Security Onion часто використовується у великих компаніях завдяки своїй масштабованості та гнучкості.

У контексті розвитку хмарних технологій важливою стає роль платформ моніторингу, що працюють у глобальних інфраструктурах. Наприклад, AWS GuardDuty аналізує журнали хмарних сервісів, мережеві потоки, запити до API та інші дані, застосовуючи моделі машинного навчання та інтегровані бази загроз. Завдяки глибокій інтеграції з екосистемою AWS ця система здатна виявляти як внутрішні, так і зовнішні загрози, включаючи спроби несанкціонованого доступу, аномальне використання ресурсів, сканування портів чи підозрілу діяльність у контейнерах. Аналогічно Microsoft Sentinel забезпечує централізований збір даних із різних джерел, застосовуючи хмарні обчислення та аналітичні алгоритми для виявлення складних інцидентів.

Важливою тенденцією є те, що сучасні рішення не обмежуються лише виявленням загроз, а активно впроваджують автоматизоване реагування. Такі системи здатні самостійно виконувати дії, спрямовані на блокування атак, ізоляцію скомпрометованих вузлів, призупинення доступу користувачів або динамічну зміну політик безпеки. Це значно зменшує навантаження на аналітиків і скорочує час реакції на інциденти, що є критично важливим у випадках швидкорозповсюджуваних атак, таких як програми-вимагачі або

внутрішні компрометації з високим рівнем критичності.

Загалом сучасні інструменти моніторингу та реагування на інциденти формують екосистему, у якій кожен елемент виконує свою роль: одні системи аналізують трафік на низькому рівні, інші будують поведінкові моделі, треті забезпечують централізовану кореляцію та аналітику. Правильне поєднання цих інструментів забезпечує можливість створення багаторівневої системи захисту, у якій виявлення, аналіз та реагування відбуваються у тісно пов’язаному й скоординованому режимі.

## 1.5 Постановка задачі

Проблематика виявлення вторгнень у корпоративних мережах стає дедалі актуальнішою на тлі постійного зростання кількості кібератак, ускладнення їхньої структури та появи нових тактик, які дозволяють зловмисникам уникати виявлення протягом тривалого часу. Незважаючи на значний прогрес у розвитку засобів кіберзахисту, традиційні підходи виявляються недостатньо ефективними у протидії сучасним загрозам, які характеризуються високою динамікою, гнучкістю та здатністю обходити механізми безпеки, що застосовуються у корпоративних мережах. Саме тому виникає потреба чітко визначити проблему, окреслити наявні обмеження та сформулювати задачу, яка потребує вирішення у межах цієї роботи.

Сучасні системи виявлення вторгнень найчастіше ґрунтуються на сигнатурному підході, який передбачає виявлення атак на основі вже відомих шаблонів. Безперечно, такі системи мають високу точність при роботі з загрозами, що добре задокументовані та входять до відповідних баз даних. Проте вони втрачають ефективність у випадках нових, досі невідомих атак, які лише з’являються у природі або які мають модифіковану структуру. Сигнатурні методи також не здатні своєчасно реагувати на нові форми загроз, оскільки потребують постійного оновлення бази сигнатур, що завжди має певний

часовий розрив із реальними подіями.

Аномалійні методи, що базуються на аналізі поведінки та визначенні відхилень від нормального функціонування мережі, у свою чергу, також мають обмеження. Їхнім основним недоліком є те, що вони залежать від коректності моделі нормальної поведінки, що вимагає довготривалого періоду навчання. Якщо модель сформована неточно або недостатньо репрезентативно, система може генерувати велику кількість хибнопозитивних спрацювань, що суттєво ускладнює роботу аналітиків SOC і знижує загальну продуктивність. Окрім того, поведінкові системи можуть виявляти нові типи загроз, але інтерпретувати їхню природу часто надзвичайно складно, що може призвести до некоректного реагування.

Ще однією важливою проблемою є значне збільшення обсягів мережевого трафіку та ускладнення його структури. Сучасні корпоративні середовища включають велику кількість пристроїв, розподілених офісів, хмарних сервісів, контейнерних платформ, мобільних робочих станцій, а також взаємодію між локальними ресурсами та глобальними мережами. Така кількість компонентів створює велику поверхню атаки, яку складно повноцінно контролювати, а традиційні системи моніторингу часто не здатні обробляти настільки значні обсяги даних у реальному часі. У результаті зростає ризик того, що критичні інциденти залишатимуться непоміченими або будуть виявлені надто пізно.

Крім цього, сучасні атаки стають дедалі складнішими, багатоступеневими та тривалими в часі. Зловмисники прагнуть залишатися непоміченими протягом довгого періоду, використовують методи прихованого пересування в мережі, застосовують шифрування трафіку, маскування під легітимні запити, а також техніки, що дозволяють зменшувати свій прояв у моніторингових системах. Це створює додаткові бар’єри для засобів виявлення, які мають не лише фіксувати аномалії у реальному часі, а й аналізувати довготривалу поведінку користувачів і сервісів.

Усі ці обставини вказують на те, що традиційні механізми виявлення

загроз недостатньо адаптивні до сучасних умов, а отже, потребують переосмислення та вдосконалення. Виникає потреба у створенні методу, який здатен поєднувати в собі точність сигнатурного аналізу та гнучкість аномалійних моделей, забезпечуючи баланс між точним виявленням відомих загроз і здатністю ідентифікувати нові. Такий метод повинен використовувати сучасні можливості аналізу даних, машинного навчання, кореляції подій та інтеграції з багаторівневими архітектурами безпеки. Важливо, щоб запропоноване рішення було масштабованим і придатним до роботи у великих корпоративних мережах, де обсяги трафіку можуть бути значними, а типи загроз – різноманітними.

Завдання, яке ставиться у межах цієї роботи, полягає в тому, щоб дослідити сучасні підходи до виявлення вторгнень, проаналізувати їхні обмеження, розробити комбінований метод, що враховує недоліки наявних систем, а також оцінити його ефективність у реальних або наближених до реальних умовах. Передбачається, що запропонований метод дозволить підвищити точність детекції, знизити кількість хибнопозитивних спрацювань та забезпечити швидшу реакцію на інциденти безпеки. Очікується також, що цей метод зможе адаптуватися до нових типів атак без потреби в постійному ручному оновленні правил або сигнатур.

# 2 МОДЕЛІ ТА МЕТОДИ ВИЯВЛЕННЯ І ПРОТИДІЇ ВТОРГНЕННЯМ У КОРПОРАТИВНІЙ МЕРЕЖІ

## 2.1 Вимоги до системи виявлення вторгнень

У корпоративних мережах система виявлення вторгнень повинна відповідати широкому спектру вимог, які визначають її здатність функціонувати у складних, динамічних та високонавантажених інформаційних середовищах. Важливість таких систем зумовлена тим, що саме вони забезпечують раннє виявлення підозрілих дій, аналіз трафіку, фіксацію інцидентів і своєчасне реагування на різні типи загроз. Формулювання вимог до системи є необхідним етапом у створенні методів та моделей, здатних ефективно працювати у реальних умовах корпоративної інфраструктури. Для цього необхідно враховувати як особливості мережевої архітектури підприємства, так і природу сучасних атак, обсяги трафіку, швидкість обробки даних та рівень критичності бізнес-процесів.

Будь-яка система виявлення вторгнень працює з потоком даних, який має складну природу і може включати мережеві пакети, журнали подій, метадані, інформацію про сесії, транзакції, системні виклики та багато інших параметрів. У формальному розумінні задача такої системи полягає у тому, щоб отримувати на вхід постійний потік мережевих пакетів різного обсягу, структури та протоколів, обробляти їх у режимі, наближеному до реального часу, а на виході формувати класифікацію щодо характеру дій: нормальна активність або вторгнення. Оскільки корпоративні мережі є багаторівневими, система повинна враховувати контекст подій, відстежувати зв’язки між пакетами, аналізувати часові залежності, особливості взаємодії між вузлами та повторюваність тих чи інших структур трафіку.

Продуктивність системи є одним із ключових критеріїв її ефективності. Корпорації, що функціонують у сфері фінансів, телекомунікацій, державного управління або великих технологічних бізнесів, щодня генерують трафік, який вимірюється терабайтами. На таких швидкостях система не має права на

затримки, оскільки будь-яка затримка може призвести до пропущених атак або до перевантаження мережевих сегментів. Важливо, щоб система була здатна обробляти дані з високою швидкістю, зберігаючи при цьому точність аналізу. Висока продуктивність вимагає оптимізованих алгоритмів, паралельної обробки даних, можливості масштабування та адаптації до змін у структурі трафіку, включно з піковими навантаженнями.

Не менш важливою вимогою є точність системи. Під точністю в цьому контексті розуміють здатність системи правильно класифікувати події та мінімізувати кількість хибнопозитивних і хибнонегативних спрацювань. Хибнопозитивні спрацювання призводять до перевантаження аналітиків та до втрати продуктивності, оскільки кожну помилкову подію необхідно аналізувати, витрачаючи час і ресурси. Натомість хибнонегативні спрацювання є ще небезпечнішими, оскільки призводять до пропуску атаки, яка може мати критичні наслідки для безпеки підприємства. Тому система повинна балансувати між чутливістю та специфічністю, забезпечуючи оптимальне співвідношення між кількістю виявлених атак і кількістю помилкових сигналів.

Адаптивність - ще одна фундаментальна вимога. Оскільки інформаційні системи постійно еволюціонують, а структури мережевого трафіку змінюються, система виявлення вторгнень має здатись працювати в умовах невизначеності. Атаки стають дедалі динамічнішими, змінюють свій характер, використовують методи приховування, тунелювання, шифрування та маскування. Традиційні сигнатурні підходи не завжди можуть впоратися з такими загрозами, тому система повинна мати можливість навчатися, оновлювати свої моделі, коригувати межі нормальної поведінки та виявляти нові типи загроз без постійного втручання з боку адміністратора. Здатність швидко адаптуватися до нових загроз стає критично важливою для збереження цілісності й доступності корпоративних систем.

Надійність у роботі та стійкість до відмов є обов’язковими характеристиками системи, яка працює в корпоративному середовищі. Вона повинна забезпечувати безперервний моніторинг, навіть у разі збільшення

навантаження, збоїв у мережі, перерозподілу трафіку або виходу з ладу окремих вузлів. У великих компаніях система виявлення вторгнень повинна мати резервні модулі, можливість дублювання функцій, підтримку кластеризації та відмовостійких конфігурацій. Це гарантує, що навіть у разі часткових аварійних ситуацій захисні механізми продовжуватимуть працювати без втрати якості.

Інтеграційні можливості також становлять важливий аспект вимог. Система виявлення вторгнень не повинна бути ізольованим елементом, який функціонує самостійно. Для ефективної роботи вона має взаємодіяти з іншими компонентами інфраструктури безпеки – фаєрволами, системами керування доступом, SOC/SIEM-платформами, системами резервного копіювання та відновлення, антивірусними комплексами, серверами журналів. Така інтеграція забезпечує не лише кращий контекст для аналізу подій, а й можливість автоматизації реагування, централізованого управління та побудови комплексної системи кіберзахисту.

Особливу увагу потрібно приділили масштабованості. Корпоративні мережі часто розширюються, додаються нові вузли, сегменти, сервери, офіси або хмарні інфраструктури. Тому система має бути здатною до масштабування без суттєвих змін у своїй архітектурі. Це передбачає можливість горизонтального або вертикального розширення потужностей, додавання нових сенсорів, агенцій та аналітичних модулів без переривання загального процесу моніторингу.

Окремим аспектом є вимога до простоти управління та прозорості. Система повинна надавати аналітикам зрозуміле представлення подій, чіткі журнали, зручні панелі моніторингу, можливість швидко та ефективно реагувати на інциденти. Візуалізація даних, гнучкість фільтрації, зрозумілі звіти та можливість швидкого аналізу причин інциденту є тими елементами, що визначають якість роботи всієї інфраструктури безпеки.

Таким чином, формування вимог до системи виявлення вторгнень є складним і багатогранним процесом, який повинен враховувати як технічні

можливості, так і особливості мережевої інфраструктури, динаміку загроз та специфіку корпоративних бізнес-процесів. Сучасна система має бути продуктивною, точною, адаптивною, надійною, масштабованою та здатною до інтеграції у комплексну систему захисту. Лише за умов відповідності всім цим вимогам можливо забезпечити ефективний захист корпоративної мережі від вторгнень і сформувати підґрунтя для побудови інтелектуальних методів аналізу, які будуть розглядатися у наступних підрозділах.

## 2.2 Моделі процесів виявлення вторгнень у мережевому трафіку

Процес виявлення вторгнень у мережевому трафіку ґрунтується на розумінні трафіку як складного, багатовимірного та високоваріативного інформаційного потоку, який формується у результаті взаємодії користувачів, сервісів і програмних систем у межах корпоративної мережі. У сучасних умовах трафік не є статичним; він змінюється залежно від типу мережевих сервісів, часових характеристик, поведінки користувачів, навантаженості інфраструктури та інших чинників. Тому моделювання процесів його аналізу потребує використання відповідних математичних концепцій, що дозволяють формалізувати структуру потоків, визначати закономірності, оцінювати відхилення та робити висновки про потенційні загрози.

Мережевий трафік часто розглядається як багатовимірний часовий ряд, де кожен пакет або група пакетів описується набором параметрів. До таких параметрів належать адреса джерела, порт призначення, довжина пакету, використовуваний протокол, кількість байтів у потоці, часові інтервали між пакетами, послідовність запитів, поведінка TCP-сесії та інші метрики. Така багатовимірність зумовлює складність моделювання, оскільки відхилення можуть проявлятися як у тісних залежностях між параметрами, так і в часових змінах. Для багатьох типів атак характерними є парні закономірності: наприклад, збільшення кількості SYN-пакетів без відповідних ACK відповідей,

повторюваність однотипних запитів до одного порту або аномально висока кількість DNS-звернень, що виходять за межі прогнозованого навантаження.

Для моделювання нормальної поведінки мережевого трафіку використовується підхід, який полягає у тому, що система формує модель “стандартного” стану на основі великого набору історичних даних. У ненормалізованому вигляді такий трафік можна представити як простір ознак, де кожна точка відповідає конкретному стану або пакету, а всі разом вони описують певний кластер поведінки. Якщо надалі реальні дані потрапляють у ту саму область простору, яку система визначила як нормальну, активність вважається безпечною. Якщо ж нові значення віддаляються від “центру” кластеру або виходять за його межі, система інтерпретує це як ознаку аномалії. Таким чином, методи кластеризації, такі як k-means, DBSCAN або SOM-карти Кохонена, мають важливе значення для сегментації трафіку та формування моделей нормальної поведінки.

Важливим елементом аналізу є оцінка відстаней між точками багатовимірного простору, адже вторгнення часто проявляються як суттєві відхилення від нормальних патернів. Для цього використовуються метрики, такі як евклідова відстань, мангеттенська відстань, відстань Махаланобіса, які дають змогу визначати ступінь відхилення нових об'єктів від контрольної моделі. Відстань Махаланобіса є особливо ефективною, оскільки враховує не лише абсолютні значення параметрів, а й їхні кореляції, що дає змогу точніше виявляти складні залежності у поведінці трафіку.

Математична модель процесу виявлення аномалій у мережевому трафіку. Мережевий трафік корпоративної мережі розглядатимемо як реалізацію випадкового процесу, у якому кожна мережева сесія або подія описується вектором числових ознак. Нехай у моменти часу $t_1, t_2 \ldots, t_n$ спостерігається послідовність мережевих подій $\{e_k\}\frac{N}{k=1}$ Кожній події $e_k$ поставимо у відповідність вектор ознак

$$x_k = (x_{k1}, x_{k2}, \ldots, x_{kd})^T \in \mathbb{R}^d,$$

де d-розмірність простору ознак. До компонент вектора можуть входити, наприклад, тривалість сесії $\tau_k$ кількість пакетів, $n_k$ обсяг переданих даних $b_k$ інтервали між подіями $\Delta\tau_k$ порти джерела й призначення $P_k^{(s)}, P_d^{(k)}$ тощо. Узагальнено можна записати:

$$x_k = \left(\tau_k, n_k, b_k, \Delta t_k, p_k^{(s)}, p_k^{(d)}, \dots\right)^T$$

Тоді послідовність $\{X(t)\}_{t\geq 0}$, де $X(t)$-випадковий вектор ознак події, яка відбулася у момент часу t, є багатовимірним часовим рядом. Нормальний трафік характеризується деяким (можливо неявно заданим) розподілом ймовірностей $P_N(X)$ у просторі $R^d$ тоді як трафік з аномаліями-іншим розподілом $P_A(X)$, який є збуренням нормальної поведінки. У задачі наглядного навчання маємо навчальну вибірку

$$D = \{(x_k, y_k, )\}\frac{N}{k=1}$$

$y_k \in \{0,1, \dots, C\}$-мітка класу $y_k = 0$ відповідає нормальній активності, а $y_k = 1, \dots, C$ -різним типам атак (DoS, порт-сканування, SQLi, XSS тощо). Задача виявлення вторгнень формально записується як задача побудови відображення

$$f: \mathbb{R}^d \to \{0,1 \dots, C\}$$

яке для довільного вектора ознак x повертає прогнозований клас $\hat{y} = f(x)$ У випадку поведінкової (аномальної) моделі вважаємо, що маємо доступ переважно до нормального трафіку і будуємо модель. $P_N(X)$ Для нового спостереження X обчислюється показник аномальності $A(x)$ який порівнюється з порогом. Один із можливих варіантів – використання відстані Махаланобіса:

$$D^2(x) = (x - \mu)^\intercal \sum^{-1} (x - \mu)$$

де $\mu$ -вектор середніх значень ознак нормального трафіку, $\sum$-коваріаційна матриця. Тоді

$$A(x) = D^2(x)$$

і прийняття рішення здійснюється за правилом

якщо $A(x) > \theta$, то $x$ вважається аномалією(вторгненням)

якщо $A(x) \leq \theta$, то $x$ належить до нормального трафіку

де $\theta > 0$ - порогове значення, підібране за результатами навчання (наприклад, за заданим рівнем хибнопозитивних спрацювань). Додатково можна враховувати ентропійні характеристики окремих ознак. Нехай Z-дискретна випадкова величина, що описує, наприклад, категорію HTTP-параметрів або номер порту. Ентропія її розподілу у нормальному режимі

$$H(Z) = -\sum_z p(z) \log p(z)$$

Різкі відхилення поточної оцінки $\widehat{H}_y(Z)$ від базового значення $H_0(Z)$ інтерпретуються як додаткові індикатори можливої аномалії у трафіку:

$$\left|\widehat{H}_t(Z) - H_0(Z)\right| > \delta$$

де $\delta$- допустиме відхилення. У загальному вигляді математична модель процесу виявлення аномалій може бути подана як трійка

$$\mathcal{M} = (\mathbb{R}^d, P_N(x), \mathcal{A})$$

де $\mathbb{R}^d$ - простір ознак, у якому описуються сесії трафіку, $P_N(x)$ - модель нормальної поведінки (статистичні характеристики, щільність, кластери), $\mathcal{A}$ - алгоритм прийняття рішень (класифікатор або аномалійний детектор), який для

кожного X обчислює показник аномальності $A(x)$ та визначає клас норма або атака. Алгоритм виявлення зображено на рисунку 2.1.

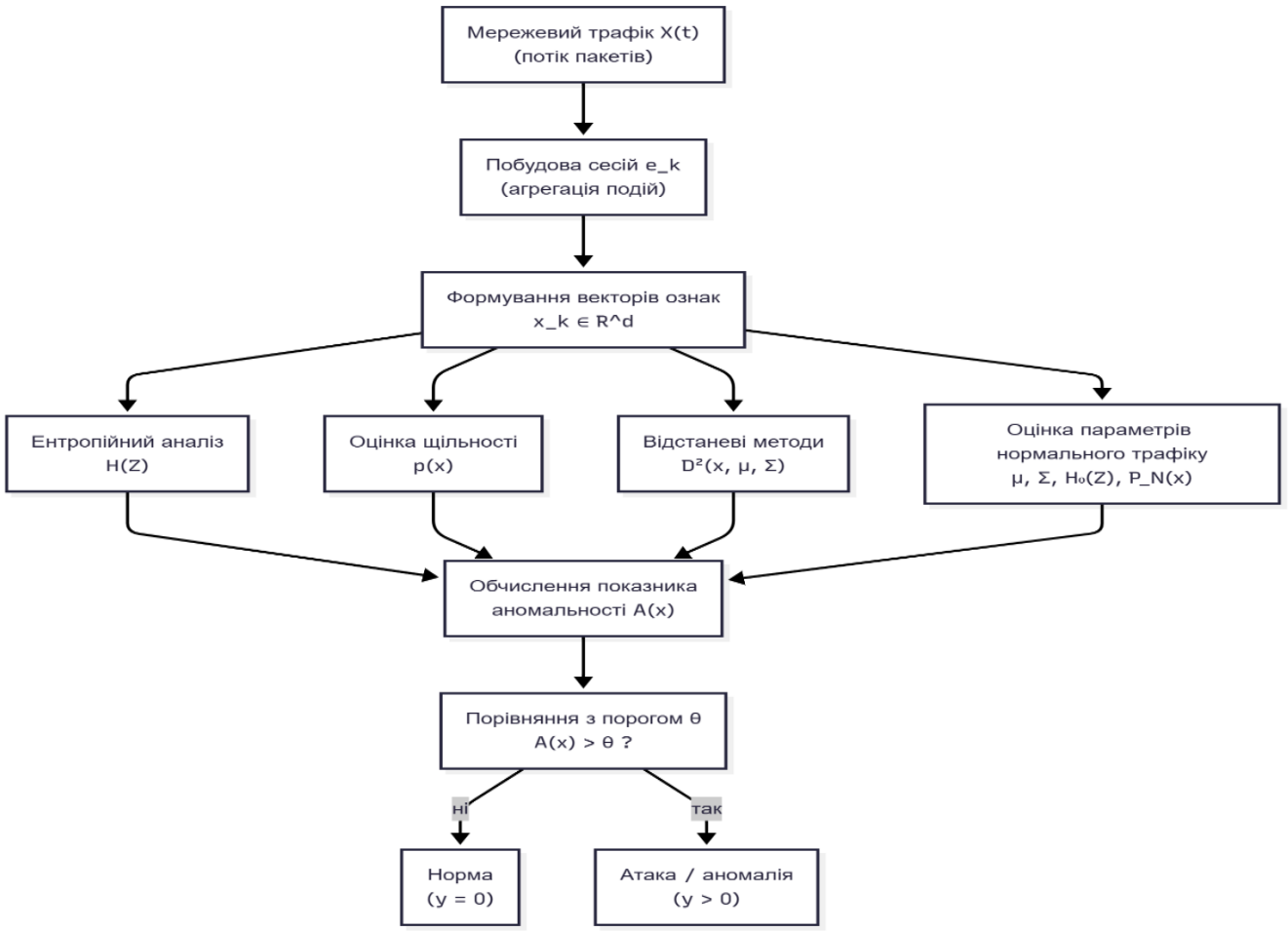


Рисунок 2.1 – Алгоритм виявлення

Іншим важливим підходом є використання ентропійних моделей. Ентропія як міра невизначеності або хаотичності сигналу дозволяє визначати, наскільки структурованим є трафік у конкретний момент часу. У нормальних умовах мережевий трафік є відносно передбачуваним: кількість пакетів певного типу чи частота запитів коливається в рамках характерних закономірностей. Коли відбувається атака, хаотичність різко зростає: з’являються аномальні частоти запитів, значні зміни у розподілах портів, повторюваність однотипних пакетів, різке зниження різноманітності TCP-сесій або навпаки - їхній вибухоподібний ріст. Ентропію трафіку під час атаки зображено на рисунку 2.2.

Порівняння поточної ентропії з базовим рівнем дає змогу виявляти аномалії, що виникають унаслідок вторгнення.

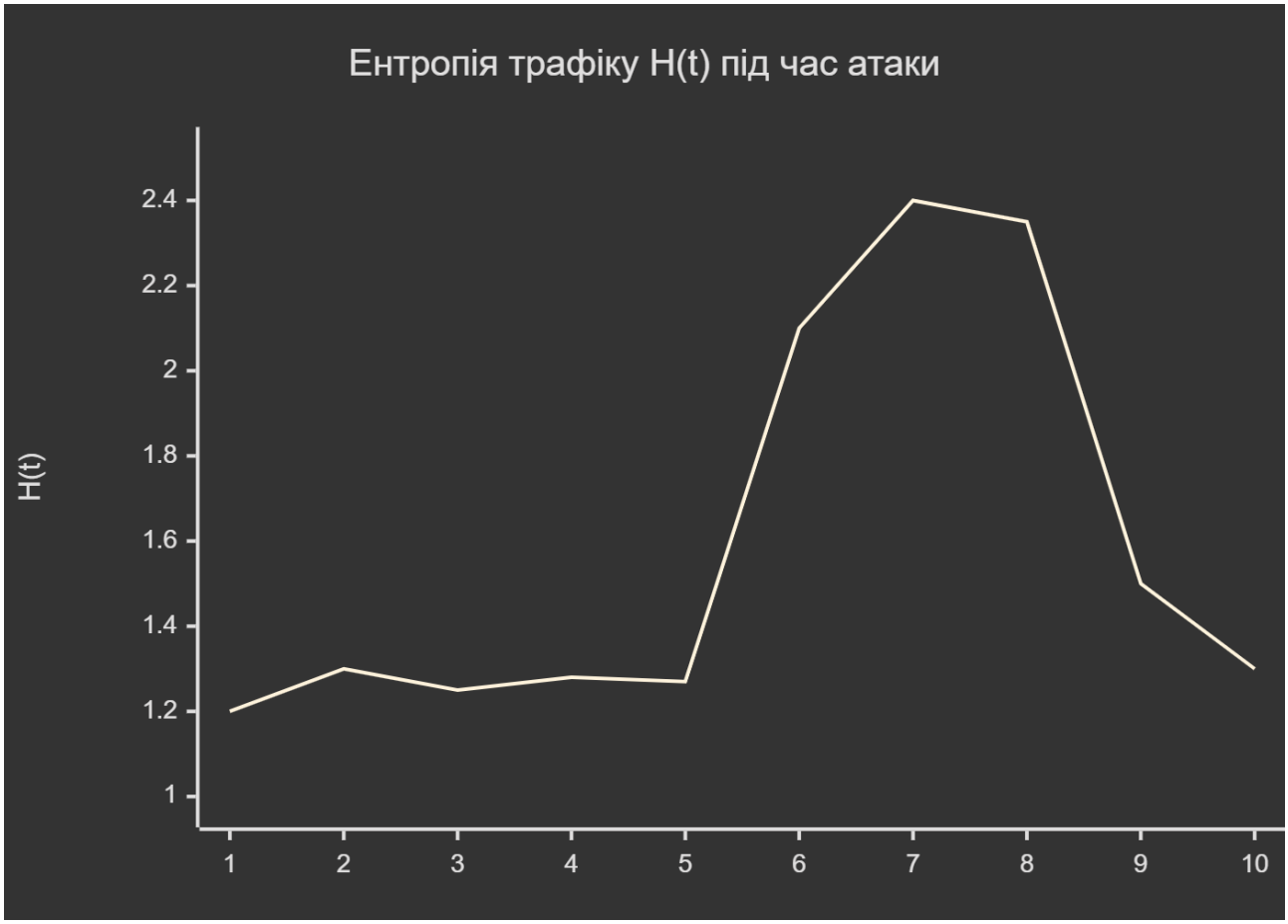


Рисунок 2.2 – Ентропія трафіку під час атаки

Щільнісні моделі використовуються тоді, коли необхідно оцінити ймовірність появи конкретного стану мережі. У цьому випадку аналіз ґрунтується на побудові функції щільності ймовірності, що дозволяє виявляти малоймовірні стани. Якщо мережевий трафік потрапляє в області низької ймовірності, це може свідчити про аномальні умови. Методи оцінки щільності, такі як KDE (оцінка щільності ядра), Gaussian Mixture Models або автоенкодери, дозволяють розуміти структуру даних у багатовимірному просторі та виявляти приховані закономірності, які неможливо помітити при звичайному аналізі параметрів.

У процесі моделювання трафіку важливим є також часовий аспект. Атаки можуть бути короткочасними або тривалими, прихованими, такими, що

розгортаються протягом кількох годин або днів. Тому аналіз часових рядів є ключовим у виявленні аномалій. Використання моделей типу LSTM або GRU дозволяє враховувати послідовність подій, залежності між пакетами, зміну параметрів у часі та формувати моделі, які можуть прогнозувати розвиток трафіку. Якщо прогнозоване значення суттєво відрізняється від фактичного, система розглядає це як потенційну загрозу. Графік щільності імовірності нормального та аномального трафіку зображено на рисунку 2.3.

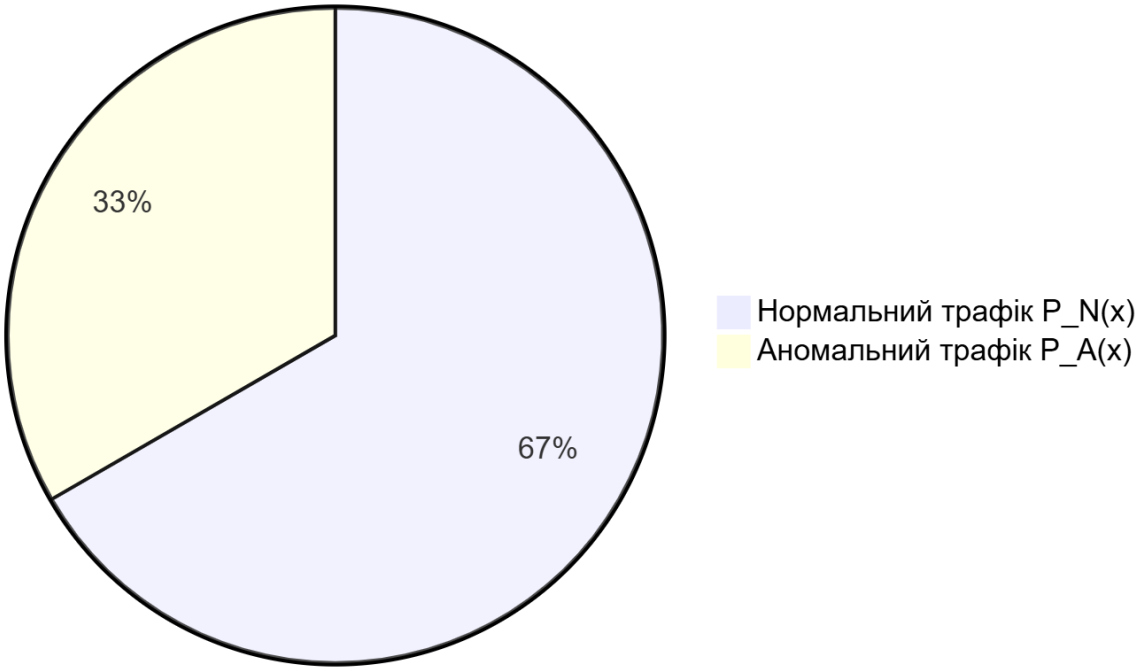


Рисунок 2.3 - Графік щільності імовірності нормального та аномального трафіку

Особливе місце займають методи кореляційного аналізу. Вторгнення, як правило, проявляються не як одна подія, а як серія взаємопов’язаних дій, які виконуються відповідно до певної логіки. Наприклад, сканування портів може передувати експлуатації вразливості, а потім – встановленню шкідливого програмного забезпечення. Системи, які здатні аналізувати зв’язки між подіями, формувати ланцюжки, визначати причинно-наслідкові залежності, є

значно ефективнішими у виявленні складних атак, ніж прості однофазові аналізатори пакетів.

Окремої уваги заслуговують моделі аналізу поведінки користувачів і пристроїв. Цей підхід ґрунтується на тому, що кожен користувач та кожна система мають характерний набір дій, який повторюється у межах типових параметрів. Аномалія виникає тоді, коли поведінка суттєво відрізняється від очікуваної: користувач виконує запити у нетипові години, підключається з невластивих пристроїв, отримує доступ до ресурсів, до яких раніше не звертався, або надсилає надмірно великі обсяги даних. Поведінкові моделі є особливо ефективними у виявленні атак внутрішнього порушника – співробітника, який має легітимний доступ, але використовує його зловмисно.

Таким чином, моделі процесів виявлення вторгнень у мережевому трафіку базуються на системному підході, який поєднує математичні, статистичні та поведінкові методи. Ефективність моделювання визначається тим, наскільки точно система здатна описати нормальний стан мережі та виявляти відхилення, що свідчать про вторгнення. У результаті формується динамічна, багатовимірна й адаптивна модель, здатна до роботи у реальних умовах корпоративної мережі, де обсяг даних постійно зростає, а типи атак набувають нових форм.

## 2.3 Розробка алгоритму методу виявлення та протидії вторгненням

Розробка методу виявлення та протидії вторгненням у корпоративній мережі потребує формування цілісної структури, яка описує всі етапи обробки трафіку від первинного збору даних до формування рішення щодо реагування на потенційний інцидент. Алгоритм такої системи має бути достатньо гнучким, щоб працювати з різними джерелами інформації, адаптуватися до змін у поведінці мережі та забезпечувати потенційну можливість інтеграції з іншими компонентами безпеки. У той же час він повинен залишатися ефективним з

точки зору продуктивності, оскільки корпоративні мережі генерують значні обсяги трафіку, а процес обробки має відбуватися у режимі, наближеному до реального часу.

Першим етапом у розробленому алгоритмі є збір даних із різних джерел, включаючи системні журнали, мережеві потоки, пакети низького рівня, метадані сесій, інформацію від внутрішніх сенсорів, журнали автентифікації та інші допоміжні джерела. Важливо, щоб система отримувала дані в уніфікованому форматі, незалежно від того, з якого модуля вони надходять, оскільки наявність різнорідних структур даних значно ускладнює подальший аналіз. Тому на цьому етапі застосовується попередня нормалізація даних, що включає очищення, узгодження часових позначок, уніфікацію форматів та фільтрацію шуму. Фільтрація необхідна для того, щоб усунути пакети, які не несуть цінної інформації або є результатом загального мережевого фону, що дозволяє зменшити навантаження на систему.

На наступному етапі виконується первинний аналіз трафіку, який включає обчислення базових статистичних і поведінкових характеристик. Сюди належать частота появи певних типів пакетів, аналіз портів, визначення протоколів, оцінка довжини сесій, визначення інтенсивності запитів, аналіз середнього та максимального розміру пакетів, оцінка інтервалів між повідомленнями, а також виявлення підозрілих повторюваних послідовностей. Створення таких базових характеристик формує фундамент для подальших етапів алгоритму, оскільки дозволяє визначити характер трафіку, виявити потенційні закономірності або аномальні відхилення.

Основою методу є гібридний підхід, що поєднує сигнатурний та аномалійний аналіз. Сигнатурний аналіз дозволяє швидко визначити ті види атак, які вже відомі системі завдяки відповідній базі правил. Цей процес є дуже ефективним і продуктивним, оскільки сигнатурні механізми працюють швидко, вимагають мінімальних ресурсів та дозволяють точно визначати шкідливі активності за умови, що вони відповідають шаблонам, відомим у базі. На практиці це означає, що такі атаки, як відомі експлойти, порт-сканування,

спуфінгові атаки або шкідливий трафік певних ботнетів, можуть бути розпізнані практично миттєво.

Втім, ключовим недоліком сигнатурних методів є нездатність виявляти невідомі, модифіковані або складні атаки, які не мають формального опису. Тому розроблений метод включає другий компонент – аномалійний аналіз, який базується на моделюванні поведінки мережі. Тут застосовуються моделі, що дозволяють визначити відхилення від нормальної активності, зокрема статистичні моделі, моделі щільності, кластеризація, нейронні мережі та інші методи машинного навчання. Важливо, що ці моделі працюють не із заздалегідь визначеними шаблонами атак, а з аналізом поведінки мережі та визначенням того, чи відповідає вона типовим станам.

У гібридній системі сигнатурний аналіз працює як перший рубіж захисту, швидко обробляючи відомі загрози, тоді як аномалійний аналіз використовується для поглибленого дослідження підозрілої активності. Такий підхід дозволяє не тільки зменшити кількість хибнопозитивних спрацювань, а й збільшити здатність системи виявляти нові складні загрози. У рамках алгоритму обидва методи працюють паралельно, і їхні результати узагальнюються з урахуванням ваги кожного компонента. Якщо сигнатурний модуль однозначно класифікує подію як атаку, система переходить до етапу реагування. Якщо ж сигнатури не спрацьовують, але поведінка є підозрілою, ініціюється детальніший аналіз.

Фінальним етапом алгоритму є процес прийняття рішення та формування реакції на інцидент. Реакція може бути різною залежно від типу загрози, рівня критичності та політик безпеки підприємства. Одним із варіантів є пасивне повідомлення адміністратора про виявлену підозрілу активність через журнал подій, електронну пошту або інтеграцію із SIEM. У випадку високої критичності система може автоматично заблокувати певний сегмент трафіку, ізолювати комп’ютер або припинити конкретну мережеву сесію. Реакція також може бути гнучкою, здійснюючи лише додаткове логування або підвищуючи рівень моніторингу для певного вузла.

Таким чином, розроблений алгоритм поєднує у собі точність сигнатурного аналізу, глибину поведінкових моделей та адаптивність аномалійних механізмів, створюючи комплексний підхід до виявлення та протидії вторгненням. Блок-схему алгоритму виявлення та протидії мережевим вторгненням зображено на рисунку 2.4.

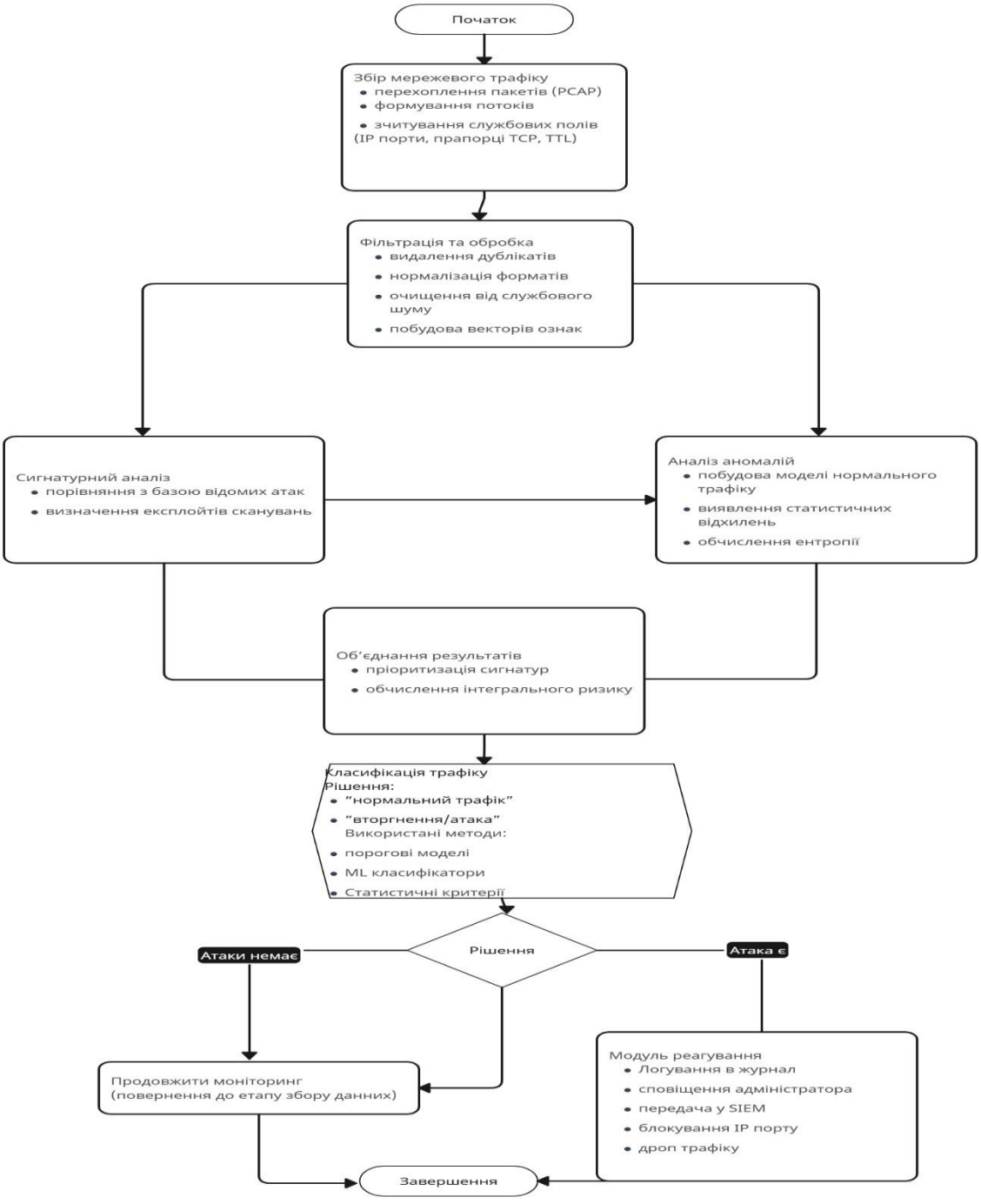


Рисунок 2.4 - Блок-схема алгоритму виявлення та протидії мережевим вторгненням

Модель взаємодії компонентів системи виявлення та протидії вторгненням у корпоративному середовищі є фундаментальним елементом для розуміння того, як різні модулі забезпечують цілісність процесу моніторингу, аналізу та реагування. У сучасних корпоративних мережах не існує ізольованих рішень: кожен компонент інфраструктури безпеки повинен працювати у взаємозв'язку з іншими елементами, забезпечуючи потік даних, логічну узгодженість та узагальнення результатів у єдиному центрі контролю. Система виявлення вторгнень не є лише інструментом аналізу трафіку; вона виступає частиною ширшої архітектури кіберзахисту, яка охоплює фаєрволи, системи управління доступом, сервери журналів, SIEM-платформи, інструменти аналізу кінцевих точок та інші механізми контролю.

У типовій корпоративній мережі система виявлення вторгнень розміщується у точках, які забезпечують доступ до найбільш повної картини мережевої активності. Це можуть бути зони між зовнішнім фаєрволом і внутрішньою мережею, сегменти, що межують із DMZ, або внутрішні підмережі з високим навантаженням. У таких розміщеннях IDS отримує доступ до трафіку, який включає як легітимні запити користувачів, так і потенційно шкідливі пакети. Взаємодія із фаєрволом полягає в тому, що IDS отримує копію потоків даних, які проходять через систему фільтрації. Фаєрвол виконує первинний контроль пакетів, тоді як IDS здійснює поглиблений аналіз, використовуючи сигнатурні та поведінкові моделі.

Центральне місце у моделі взаємодії посідає модуль аналітики, який працює із нормалізованими даними, отриманими від сенсорів IDS. Саме на цьому рівні відбувається визначення відхилень від нормальної поведінки, кореляція подій, виявлення аномалій та формування рішень щодо класифікації активності. Аналітичний модуль отримує дані як із мережевих датчиків, так і з хостових агентів, які передають журнали подій операційних систем, дані про доступ до файлів, зміни конфігурацій та інші важливі сигнали. Така інтеграція дає змогу формувати багатопоточний аналіз, що враховує як мережевий, так і локальний контекст.

Одним із найбільш критичних елементів є система кореляції подій, яка об’єднує інформацію з різних джерел та оцінює її як частину єдиного інциденту. Наприклад, сканування портів, зафіксоване мережевим сенсором, може збігатися з несанкціонованим доступом до системного журналу або спробами ескалації привілеїв на хості. Ізольовано кожна подія може здатися незначною, але у комплексі вони свідчать про підготовку атаки. Система кореляції забезпечує смисловий контекст, який дозволяє робити глибші висновки про природу інцидентів.

Суттєве значення в архітектурі має SIEM-платформа, яка є центром збору, кореляції та візуалізації даних. SIEM отримує інформацію від IDS, фаєрволів, серверів автентифікації, доменних контролерів, антивірусних систем, кінцевих пристроїв, а також хмарних модулів безпеки. Усі ці дані обробляються за допомогою правил кореляції, машинного навчання та поведінкової аналітики. У результаті SIEM не тільки видає попередження, але й формує прогнозні моделі та визначає ризики. Завдяки інтеграції з IDS, SIEM може не лише отримувати інциденти, а й передавати зворотні дані – наприклад, коригувати пріоритети або повідомляти систему виявлення про нові правила.

У моделі взаємодії важливу роль відіграє модуль реагування, який може працювати у різних режимах – від пасивного сповіщення до повністю автоматизованих дій. Такий модуль може блокувати мережевий трафік, відключати облікові записи, ізолювати хости, запускати додаткові перевірки або змінювати політики доступу. Рішення щодо типу реакції приймається на основі рівня критичності інциденту, типу атаки, визначеного ризику та політик інформаційної безпеки. У деяких корпоративних середовищах модуль реагування працює у тісній інтеграції з оркестраційними платформами, що дозволяє здійснювати комплексні сценарії реагування.

Окреме місце у моделі займають системи журналювання та зберігання даних. Журнали є основним джерелом інформації для аналізу інцидентів, проведення розслідувань, побудови моделей поведінки та визначення тенденцій. Централізоване збереження журналів дозволяє забезпечити

цілісність, надійність та доступність даних. Завдяки інтеграції з IDS, система журналювання може отримувати структуровані події у вигляді логів мережевих сесій, спроб підключення, відхилених транзакцій та інших показників.

У корпоративному середовищі система виявлення вторгнень повинна також взаємодіяти з механізмами контролю доступу, які визначають, які дії користувач може виконувати у системі. Наприклад, якщо IDS фіксує підозрілу поведінку певного користувача, контроль доступу може обмежити його дії або вимагати додаткової автентифікації. Така інтеграція забезпечує не лише мережевий контроль, а й поведінкову безпеку.

Загалом модель взаємодії компонентів у корпоративному середовищі формує комплексну архітектуру, у якій IDS є лише одним із ключових елементів. Її ефективність залежить від того, наскільки правильно налаштована взаємодія між усіма модулями – від фільтрації трафіку до кореляції подій та реагування. Системний підхід дозволяє забезпечити глибину аналізу, адаптивність до загроз та високу швидкість реакції, що є критичною умовою для стійкості корпоративної інфраструктури.

## 2.4 Висновки до розділу 2

У другому розділі було сформовано комплексне теоретичне підґрунтя для розробки методу виявлення та протидії вторгненням у корпоративній мережі, що базується на аналізі структури трафіку, математичних моделях і принципах взаємодії між компонентами системи безпеки. Проведене дослідження дозволило узагальнити основні властивості мережевих потоків, визначити характерні ознаки вторгнень і сформувати вимоги до алгоритмів, здатних функціонувати в умовах високої складності та динамічності корпоративного середовища.

Розглянуті в підрозділах моделі виявлення вторгнень показали, що мережевий трафік має багатовимірну та часову природу, що вимагає

застосування комбінованих підходів до аналізу. Використання багатовимірних моделей дозволяє формалізувати структуру трафіку, зокрема шляхом представлення потоків як набору взаємозалежних параметрів. Завдяки цьому стало можливим виявляти аномальні стани, які суттєво відхиляються від нормальних патернів поведінки. Застосування ентропійних методів, оцінки щільності, кластеризації та алгоритмів глибинного навчання створює передумови для формування адаптивної поведінкової моделі, здатної виявляти як відомі, так і невідомі загрози.

Гібридний характер запропонованого методу, що поєднує сигнатурний і поведінковий аналіз, дозволяє досягти оптимального співвідношення між точністю та адаптивністю. Сигнатурна частина забезпечує швидке визначення атак, що вже описані у відповідних базах правил, тоді як аномалійна складова дозволяє виявляти нові, раніше невідомі загрози. У поєднанні ці два підходи створюють стійку основу для ефективної детекції з мінімальним рівнем хибнопозитивних і хибнонегативних спрацювань.

Модель взаємодії компонентів у корпоративному середовищі, представлена в межах цього розділу, показала важливість інтеграції системи виявлення вторгнень із фаєрволами, журналами подій, SIEM-платформами та механізмами реагування. Комплексний підхід дозволяє забезпечити постійний потік інформації між модулями, формувати цілісне уявлення про стан безпеки та здійснювати кореляцію подій різного рівня критичності. Важливо підкреслити, що ефективність системи залежить не лише від точності аналітичних моделей, а й від її здатності взаємодіяти з іншими елементами інфраструктури безпеки, забезпечуючи узгодженість, швидкодію та гнучкість реагування.

Результатом дослідження стало формування структурованого алгоритму, який описує всі основні етапи обробки трафіку – від збору та нормалізації даних до прийняття рішення та автоматизованого реагування. Розроблений метод орієнтований на роботу у реальному корпоративному середовищі, враховує високу інтенсивність трафіку, наявність різних протоколів і постійну

зміну поведінкових сценаріїв. У межах моделі було також визначено ключові аспекти масштабованості та адаптивності, які є необхідними для забезпечення довготривалої ефективності системи.

Підсумовуючи, можна стверджувати, що другий розділ сформував теоретичну та методологічну основу для реалізації практичної компоненти системи виявлення та протидії вторгненням. Визначені в ньому моделі та алгоритми становлять ядро системи, яка буде реалізована та протестована в наступному розділі. Окреслені властивості, вимоги та архітектурні принципи дозволяють забезпечити високий рівень точності детекції, адаптації до нових загроз і відповідності сучасним тенденціям у сфері кіберзахисту.

# 3 РЕАЛІЗАЦІЯ, ТЕСТУВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА

## 3.1 Архітектура програмного комплексу

Під час розроблення програмного комплексу було поставлено завдання об’єднати декілька інструментів та підходів, які зазвичай використовуються окремо: традиційні засоби перехоплення та аналізу мережевого трафіку (Wireshark, Zeek) , механізми попереднього збирання даних, модулі машинного навчання для визначення аномальної поведінки, а також підсистему візуалізації, здатну у зручній формі подавати результати користувачу [5; 56]. Такий підхід дозволив побудувати цілісну структуру, де кожен компонент виконує власну функцію, але водночас органічно взаємодіє з іншими рівнями системи.

Основою реалізації став Python – як мова, що дає змогу поєднувати роботу зі зчитуванням трафіку, обробленням даних і навчанням моделей [4; 30]. Вибір пояснюється не лише популярністю Python у сфері кібербезпеки, а й доступністю бібліотек машинного навчання Scikit-learn, pandas та NumPy [36; 54], що значно спрощує процес побудови моделей класифікації та подальшого їх тестування. Під час опрацювання масивів мережевих записів використовувалися pandas-таблиці, оскільки саме вони дозволяють швидко виконувати фільтрацію, перетворення й групування великої кількості параметрів, отриманих після збору трафіку [39].

Серед інструментів нижчого рівня було застосовано Wireshark – переважно для верифікації структури пакетів та контролю коректності їх перехоплення [29; 53]. Основні записи мережевої активності збиралися за допомогою Zeek [6; 28; 50], оскільки ця система дозволяє створювати детальні журнали (лог-файли), де окремо відображаються події TCP, HTTP, DNS, SSL та інші категорії, необхідні для формування повної картини поведінки мережі. Подібний підхід рекомендується в оглядах сучасних IDS-рішень [3; 7; 47].

Отримані з Zeek дані надходили до попереднього модуля структурування

інформації. У цьому модулі виконувалися операції очищення: вилучення технічних полів, що не мають аналітичної цінності, усунення частково заповнених записів, конвертація часових міток у єдиний формат, нормалізація числових параметрів [12; 19]. На цьому етапі було важливо отримати набір даних, у якому показники різних протоколів не “конфліктували” між собою та відображали характерні властивості трафіку [23].

Наступний компонент архітектури – модуль машинного навчання – відповідав за формування моделі класифікації на основі навчальної вибірки. Для цього застосовувалися бібліотеки Scikit-learn, що містять низку алгоритмів, придатних для задач виявлення вторгнень: Random Forest, Decision Tree, Gradient Boosting, SVM тощо [36; 37; 38]. У межах роботи було обрано поєднання деревоподібних алгоритмів, оскільки вони показують стабільність на вибірках з істотно нерівномірним класовим розподілом [11; 31; 40]. Перед навчанням здійснювалася перевірка вибірки на наявність надмірно корельованих показників, а також формувалася підмножина ознак, що мали найбільше значення під час класифікації [41; 43].

Після побудови моделей результати роботи системи виводилися до Elasticsearch – платформи, яка зручна для організації сховища журналів та швидкого пошуку по них [52; 56]. Завдяки Kibana вдалося створити інтерфейс для візуалізації отриманих висновків [5; 56]. Тут відображаються графіки аномальної активності, фільтри для часу та протоколів, а також індикатори спрацьовування моделі машинного навчання. Такий підхід відповідає сучасним вимогам до організації моніторингових панелей SOC-центру [27; 57].

Певні частини програмного комплексу взаємодіють між собою асинхронно. Це дозволяє системі працювати без суттєвих затримок навіть під час оброблення великих потоків інформації [46; 65]. Модуль збору трафіку функціонує незалежно від модуля аналізу, а результати передаються за допомогою проміжних буферів. Архітектурну діаграму зображено на рисунку 3.1. Така структура дає змогу гнучко змінювати конфігурацію: за необхідності можна замінити інструмент збирання пакетів або алгоритм машинного

навчання, не порушуючи загальної логіки роботи системи [45; 58; 62. ]

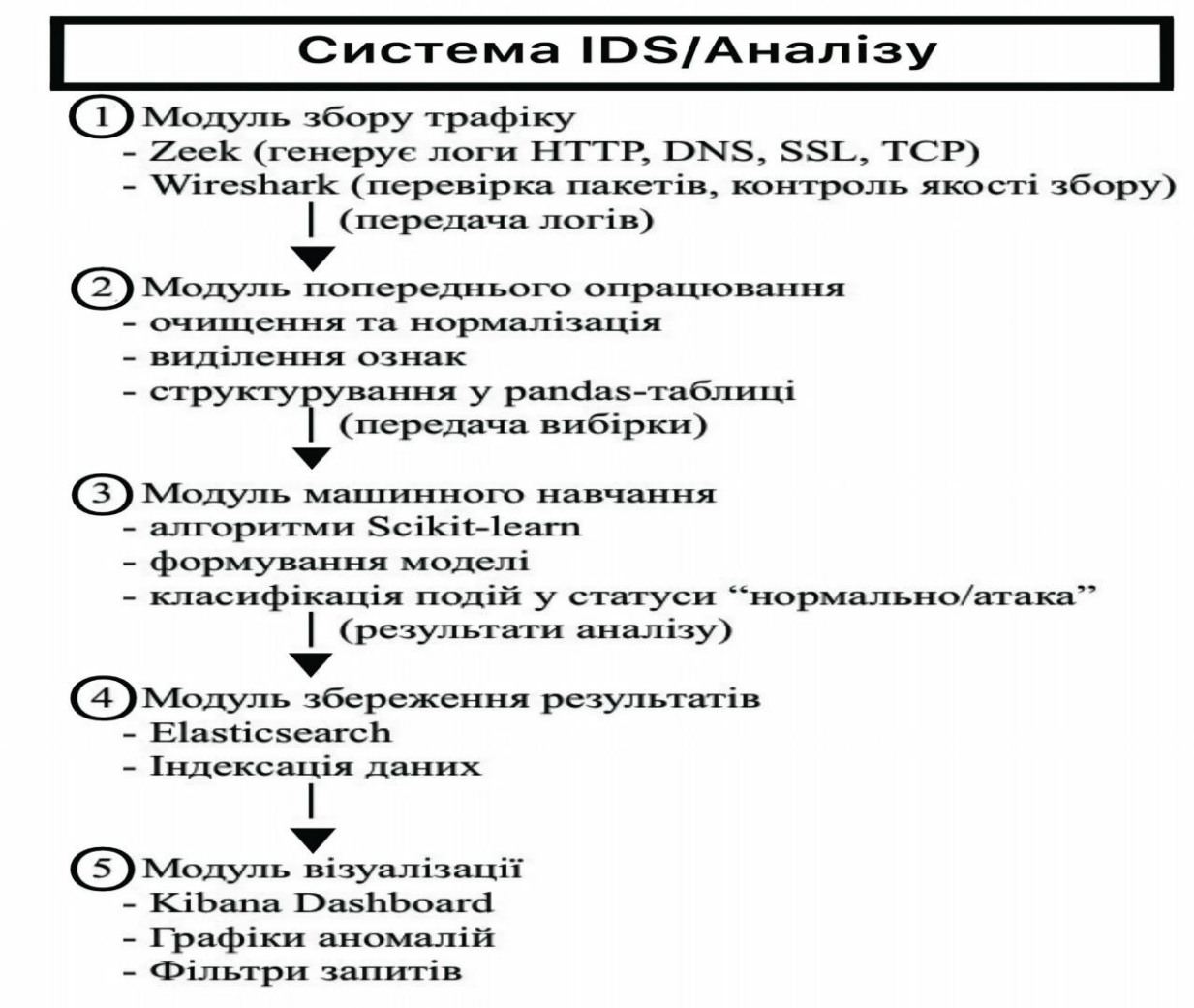


Рисунок 3.1 - Архітектурна діаграма

Діаграма демонструє послідовну та водночас розділену структуру роботи. Збирання трафіку, яке виконується за рахунок Zeek, працює автономно, не залежачи від швидкості подальшої обробки. Це важливо, оскільки у реальній мережі трафік іде постійно й нерівномірно.

Попереднє опрацювання виступає своєрідним "фільтром", що дозволяє привести дані до стану, придатного для роботи алгоритмів машинного навчання. На цьому етапі здійснюється також перевірка на логічні помилки у зібраній інформації – наприклад, некоректні часові мітки або дублікати записів.

У модулі машинного навчання система намагається знайти відмінності між нормальним трафіком та аномальним. Саме цей блок формує основу

аналітичної частини програмного комплексу. Після отримання прогнозу результати спрямовуються до Elasticsearch, де їх можна зберігати тривалий час для наступного аналізу, досліджень або порівняння з іншими сценаріями.

Візуалізація забезпечує можливість переглянути роботу всієї системи у режимі реального часу. Інтерфейс Kibana надає фільтри за часом, за типами протоколів, за частотою спрацьовувань моделей. Завдяки цьому оператор або аналітик SOC-центру може швидко визначити, чи відбувається в мережі якась нетипова активність, не заглиблюючись у технічні журнали.

## 3.2. Структура даних і модулі системи

Структура даних, використана у програмному комплексі, формувалася з урахуванням того, що мережевий трафік за своєю природою є нерівномірним, неоднорідним і часто містить значну кількість технічних полів, які не несуть суттєвого аналітичного змісту. Тому під час роботи над системою було вирішено побудувати кілька-рівневу модель опрацювання даних, де кожен етап відповідає за власний відсік логіки – від первинного приймання пакетів до формування підсумкових оцінок аномальної поведінки. Подібну поетапність рекомендовано і в сучасних оглядах IDS-рішень, де наголошується на важливості розділення «сирих» мережевих подій та структурованих аналітичних ознак [3; 32; 33].

Перший модуль системи – це блок перехоплення та реєстрації трафіку. Він працює на основі Zeek [6; 28; 50] і частково дублюється Wireshark’ом [29; 53], який використовується для контрольного аналізу структури пакетів. У цьому модулі забезпечується збирання подій за категоріями: HTTP-сесії, DNS-запити, TLS-рукостискання, TCP-з’єднання та окремі записи про ICMP-активність. Важливо, що Zeek формує журнали у вигляді текстових логів з уніфікованими полями, тому подальше структурування даних не потребує складних конвертацій [19; 23].

Модуль збору трафіку функціонує у режимі, максимально наближеному до реального, тобто дані фіксуються у той момент, коли проходить пакет [6; 50]. Такий підхід дозволив уникнути накопичення проміжних буферів, які могли б негативно вплинути на синхронність подій. Журнали логуються у вигляді кількох наборів: conn.log, http.log, ssl.log, dns.log, а також файлів із загальними метаданими. Ці журнали мають спільне поле часу, що полегшує синхронізацію на наступних етапах [28; 66].

Модуль попереднього аналізу та структурування даних виконує функцію приведення зібраної інформації до формату, придатного для подальшої обробки алгоритмами машинного навчання. На цьому етапі використовується Python-бібліотека pandas, яка дозволяє представляти журнали подій у вигляді таблиць і здійснювати над ними високорівневі операції. Спочатку виконуються технічні процедури, спрямовані на підготовку даних: часові позначки перетворюються у формат, який можна коректно групувати та порівнювати; очищуються поля, що містять службову або версійну інформацію, характерну для окремих редакцій Zeek; вилучаються неповні або пошкоджені записи, що містять помилкові значення; оптимізуються типи даних для зменшення навантаження на оперативну пам’ять при роботі з великими наборами. Після завершення цих етапів формується узгоджений набір ознак, який подається до моделей машинного навчання. До таких ознак належать кількість пакетів у межах окремої сесії, загальний обсяг переданих даних, частота повторних звернень клієнта, середня тривалість TCP-з’єднання, кількість помилкових відповідей DNS-сервера, наявність або частота зміни TLS-версій у рамках однієї взаємодії, а також інші поведінкові параметри, що характеризують коректність і стабільність сесій та дозволяють алгоритмам відрізняти типові моделі активності від потенційно шкідливих.

Окремо слід звернути увагу на нормалізацію числових показників. Машинне навчання, особливо дерева рішень і алгоритми на їх основі, може працювати з різними масштабами ознак, але їхнє попереднє вирівнювання дає можливість підвищити стабільність моделі. Тому кожен параметр приводився

до стандартного інтервалу, що усувало небажані перекоси у вибірці.

Модуль навчання моделі машинного навчання.

Центральний блок системи - це модуль навчання моделі, що виконується у Python із використанням Scikit-learn [36; 54]. На цьому етапі формується класифікаційна модель, яка має виявляти аномальну поведінку у сформованій вибірці. У межах роботи було перевірено кілька архітектур: дерева рішень, Random Forest, Gradient Boosting та деякі методи опорних векторів [11; 37; 38]. На основі тестування попередніх версій вибір зупинили на Random Forest, оскільки він давав стійкі результати навіть на вибірках з нерівномірним представленням класів [41; 42].

Під час навчання моделі створюється підмножина значущих ознак, яка визначається за показниками важливості [41; 63]. Такий підхід дозволяє відкинути другорядні параметри, що не впливають на якість класифікації, і водночас підвищує швидкість роботи системи. За результатами попередніх досліджень найсуттєвішими виявилися показники, пов’язані з тривалістю сесії, особливостями TCP-рукостискання та частотою повторних запитів [11; 20].

Модуль навчання включає також оцінку роботи системи на тестовій вибірці, де вимірюються точність, повнота та F1-міра [35; 41; 44]. Ці показники не тільки демонструють загальну ефективність моделі, але й дають змогу виявити ситуації, у яких алгоритм плутає нормальні дії з аномальними.

Модуль візуалізації результатів відповідає за представлення вихідних даних після виконання прогнозування та класифікації мережевих подій. Після опрацювання дані передаються до Elasticsearch, який використовується як основне сховище завдяки здатності швидко індексувати великі масиви інформації та підтримці гнучкої мови запитів, що дозволяє виконувати складні аналітичні операції. Подальша візуалізація реалізується у середовищі Kibana, де формується інтерактивна інформаційна панель із ключовими елементами моніторингу. На ній відображаються динамічні графіки активності у часовій шкалі, гістограми розподілу спрацьовувань моделі, показники інтенсивності різних типів подій, а також деталізовані таблиці, що містять інформацію про

потенційно небезпечні або нетипові мережеві з’єднання. Інтерфейс візуалізації підтримує широкий спектр фільтрів, які дозволяють оперативно аналізувати події за протоколами, тривалістю з’єднання, IP-адресами, параметрами поведінкової моделі чи іншими ознаками, що були визначені алгоритмами машинного навчання. Такий підхід забезпечує зручність аналізу та створює умови для ефективного моніторингу стану корпоративної мережі. Інтерфейс взаємодії користувача.

Для взаємодії з системою передбачено два варіанти інтерфейсів: командний рядок (CLI) та веб-панель, побудована на основі Kibana [56]. Кожен з них виконує власну роль. CLI-інтерфейс орієнтований передусім на роботу з технічними параметрами системи. Через командний рядок можна запустити новий цикл збору трафіку, виконати фільтрацію журналів, перезапустити модуль навчання або змінити набір ознак [4; 30]. Веб-панель, що базується на Kibana, спрямована на кінцевого аналітика. Вона створює більш “візуальний” спосіб сприйняття даних, який дозволяє побачити загальну картину подій у мережі [5; 56]. Панель підтримує налаштування власних віджетів, а також динамічні фільтри.

## 3.3. Методика тестування та результати

Тестове середовище, його побудова та мережева топологія. Побудова повноцінного тестового середовища була одним із ключових етапів даного дослідження. В умовах реальної мережі поведінка трафіку завжди є змішаною, і в ній співіснують як регулярні користувацькі дії, так і технічні процеси операційних систем, програмного забезпечення, службових фонових сервісів. Тому, відповідно до рекомендацій, поданих у спеціалізованих методичних джерелах з аналізу мережевих аномалій, середовище повинно відтворювати обидві групи подій: звичайний трафік та змодельовані атаки.

У ході роботи було створено лабораторну інфраструктуру, яка

складається з каркасу віртуальних машин, маршрутизатора, сенсора перехоплення трафіку та окремого сервера візуалізації. Подібний підхід дозволив отримати контрольовану, але водночас гнучку топологію, що легко масштабувалася й давала можливість налаштовувати конкретні умови для кожного типу тестів.

Загальна концепція побудови тестового середовища передбачала створення повноцінної лабораторної інфраструктури, яка могла б відтворювати роботу реальної корпоративної мережі та дозволяла проводити контрольовані експерименти з різними типами трафіку, включаючи легітимні запити користувачів та навмисні мережеві атаки. Основна ідея полягала в тому, що весь трафік мав проходити через одну чітко визначену точку моніторингу. Такий підхід забезпечував повноту спостереження за подіями, можливість точної синхронізації часових міток та коректність подальшого аналізу. Завдяки цьому система могла зіставляти реакції мережі з конкретними моментами запуску перевантаження або атак, що значно підвищувало точність оцінювання моделей виявлення аномалій.

Окрему увагу приділено підтримці двох повністю різних типів активності: звичайних робочих даних і трафіку, який різко змінював навантаження й імітував агресивні атаки. Така структура дозволила розглядати роботу моделі машинного навчання у реалістичних умовах, коли часові ряди містять як нормальні коливання, так і стрибкоподібні зміни. Саме така ситуація найкраще демонструє здатність аналітичної системи відокремлювати норму від аномальних відхилень. Важливим було і те, що тестове середовище працювало в ізольованому сегменті мережі, що ніяк не впливало на роботу інших систем і знижувало ризики для продуктивного оточення. Інфраструктура була побудована за модульним принципом, коли кожен компонент виконував одну конкретну функцію: сенсор перехоплював дані, інструмент для аналізу їх структурував, модуль машинного навчання здійснював прогноз, а система візуалізації відображала результати у зрозумілому та придатному для практичного використання вигляді.

Для проведення експериментів було розгорнуто шість віртуальних машин та один маршрутизатор. Центральним вузлом виступав pfSense Router, який виконував роль шлюзу між внутрішньою тестовою інфраструктурою та зовнішнім середовищем. Саме через нього проходив увесь трафік, що забезпечувало контроль над маршрутизацією пакетів. На маршрутизаторі працювали функції трансляції адрес, базової маршрутизації, а також створення копій мережевих пакетів та передавання їх на систему аналізу Zeek. Це дозволяло отримати повну картину мережевої активності – від найпростіших DNS-запитів до низькорівневих TCP-пакетів. Крім того, на цьому ж вузлі можна було штучно обмежувати швидкість передавання даних, що відкривало можливість імітації різних робочих ситуацій: перевантаження каналу, збільшення часу відповіді або навпаки періодів низької активності. Усе це сприяло формуванню реалістичних і різноманітних навчальних вибірок.

На сервері Ubuntu розміщувалася система мережевого моніторингу Zeek, яка перехоплювала та структурувала потоки даних. Zeek формував журнали активності, у яких фіксувалися з’єднання, HTTP- та DNS-запити, TLS-переговори та додаткові метадані. Завдяки цьому можна було оцінювати активність користувачів і програм на детальному рівні. Чітка синхронізація часових відміток стала критично важливою для моделювання атак, оскільки дозволила безпосередньо прив’язувати моменти нештатної активності до конкретних дій, виконаних на машині-джерелі атаки.

Другий ключовий компонент – сервер із Elasticsearch та Kibana, який забезпечував збереження й структурування даних та надавав можливість будувати запити та візуалізувати події. На цьому сервері відображалися численні графіки та таблиці, можна було фільтрувати записи за будь-яким параметром, наприклад за IP-адресою, портом, часом, протоколом або напрямом трафіку. Створені інструменти дозволяли швидко знаходити аномалії та оцінювати їхню природу. Значною перевагою було й те, що аналітичні панелі оновлювалися у режимі, наближеному до реального часу, завдяки чому взаємозв’язок між подіями легко простежувався.

Генерація атак відбувалася на віртуальній машині з Kali Linux, з якої проводилися атаки різного типу: починаючи з простих спроб перевантаження каналу, порт-сканування та закінчуючи SQL- і XSS-ін’єкціями. Такі атаки давали можливість навчити систему розрізняти типи навантажень і створити різноманітний набір сценаріїв для подальшого аналізу та порівняння. Завдяки цьому можна було побачити, як змінюються журнали Zeek при різних діях зловмисника і наскільки точно моделі машинного навчання реагують на появу небезпечних шаблонів.

Windows 10 виступала моделлю звичайного робочого місця користувача, яке генерувало повністю законний фон трафіку: перегляд сторінок у браузері, запити до DNS-серверів, взаємодія з інтернет-сервісами та оновленнями. Це дозволяло перевіряти, наскільки часто алгоритми ідентифікують нормальні події як підозрілі та визначати рівень хибних спрацьовувань. Така поведінка характерна для реальних корпоративних мереж, тому включення цього вузла було необхідним для реалістичного оцінювання.

Усі процедурні операції з машинним навчанням виконувалися на окремому сервері на базі Python. Тут проходили попередня обробка журналів Zeek, нормалізація вибірок, підготовка ознак і побудова моделей на основі алгоритмів Random Forest. Отримані результати надсилалися в Elasticsearch, де вони відображалися у тих самих панелях Kibana, що значно спрощувало комплексний аналіз і усувало потребу перемикатися між різними інструментами.

Створене середовище дозволило отримати комплексний набір даних, повністю контрольованих умов і широкі можливості для оцінювання ефективності методів виявлення мережевих аномалій. Завдяки чітко визначеним сценаріям атаки та стабільно відтворюваним моделям трафіку стало можливим порівняти роботу різних підходів. від сигнатурних до поведінкових та ML-орієнтованих - на одному й тому ж наборі спостережень. Це забезпечило об’єктивність і відтворюваність результатів, усунуло вплив некерованих зовнішніх факторів та дозволило сфокусуватися на реальній

здатності алгоритмів розпізнавати відхилення у структурі мережевих потоків.

Окрім того, контрольоване середовище надало змогу аналізувати поведінку систем у динаміці: спостерігати, як змінюються ентропійні характеристики під час атаки, як модифікується щільність імовірності ознак, та яким чином різні типи інцидентів впливають на модель нормального трафіку. Такий підхід створює підґрунтя для глибшого розуміння механізмів формування аномалій і дозволяє не лише оцінити точність роботи методів, але й визначити причини їхніх помилок, обмеження та зони подальшого удосконалення.

Таблиця 3.1 - Конфігурація віртуальних машин тестового середовища

| Компонент | ОС | CPU | RAM | Основна роль |
|---|---|---|---|---|
| pfSense Router | FreeBSD-based | 2 ядра | 2 ГБ | NAT, SPAN, маршрутизація |
| Ubuntu + Zeek | Ubuntu 22.04 | 4 ядра | 8 ГБ | Збір журналів, IDS-сенсор |
| Elasticsearch/Kibana | Ubuntu 22.04 | 4 ядра | 12 ГБ | Індексація, візуалізація |
| Kali Linux | Kali Rolling | 2 ядра | 4 ГБ | Генерація атак |
| Windows 10 | Win10 Pro | 2 ядра | 4 ГБ | Фоновий трафік |
| Python ML Server | Ubuntu 22.04 | 4 ядра | 8 ГБ | Навчання моделі |

Побудова мережевої топології ґрунтувалася на класичній архітектурі, у межах якої всі вузли корпоративного сегмента передавали трафік через маршрутизатор, після чого його копія надходила на сенсор, де здійснювалося подальше оброблення. Далі дані спрямовувалися до модуля машинного навчання, а результати аналізу автоматично зберігалися та відображалися в Elasticsearch і Kibana. Для забезпечення повноти збору трафіку був використаний SPAN-порт маршрутизатора, який дублював увесь мережевий потік на сенсор без втручання у продуктивність самої мережі. Такий підхід є

критично важливим для поведінкового аналізу, оскільки навіть незначні втрати пакетів здатні порушити статистичну цілісність даних, спотворити часові послідовності та, відповідно, вплинути на результати класифікації вторгнень. Топологію експериментального стенду зображено на рисунку 3.2.

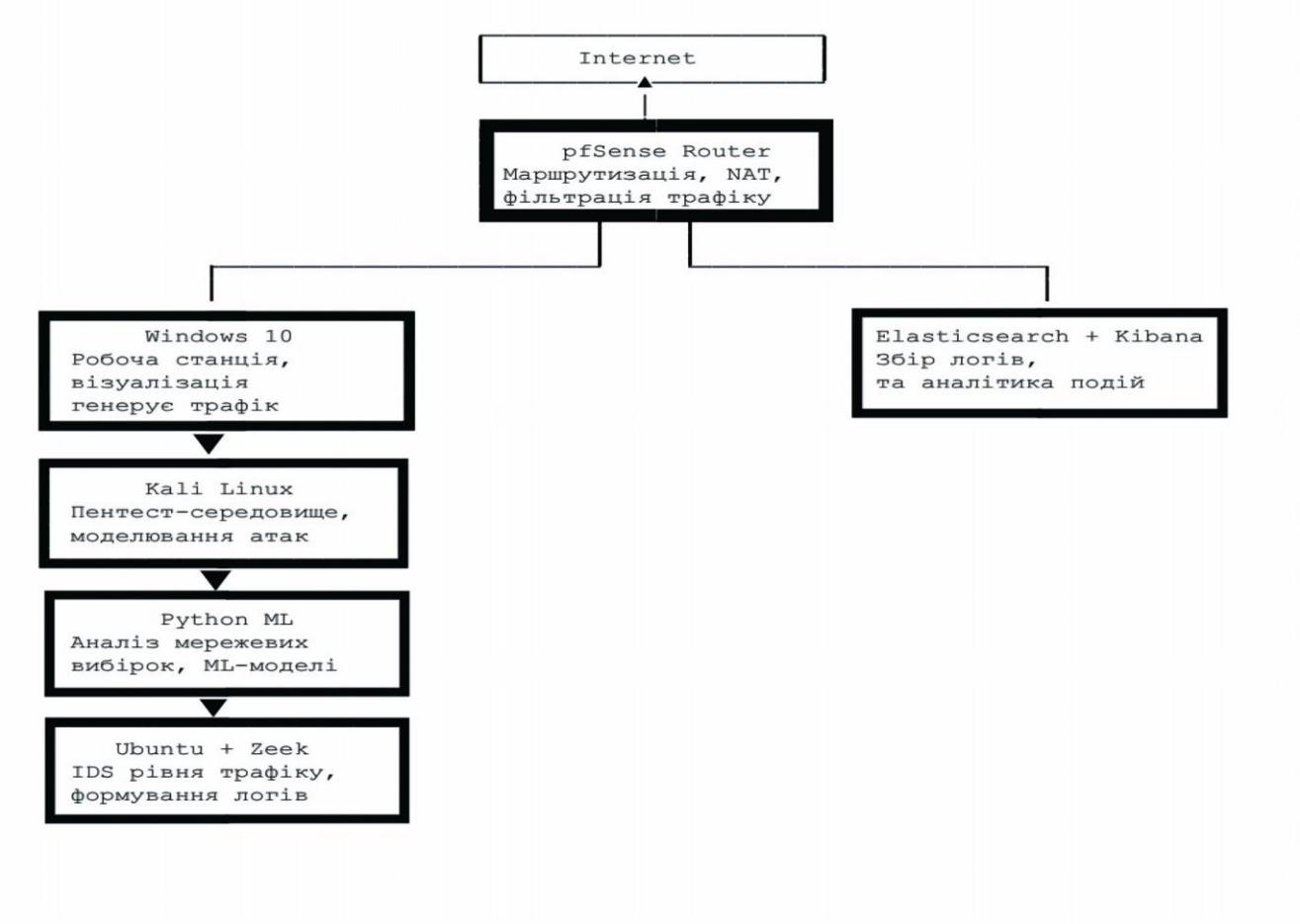


Рисунок 3.2 - Топологія експериментального стенду

У рекомендаціях з побудови IDS-систем підкреслюється необхідність автономної тестової мережі, де можна відтворювати поведінкові особливості різних типів атак [32]. Саме це було реалізовано у даній роботі.

Причини вибору такої архітектури були зумовлені низкою практичних та методологічних міркувань, що визначили її оптимальність для проведення експериментального дослідження. Передусім важливим чинником стала гнучкість системи, оскільки кожен елемент інфраструктури може масштабуватися незалежно, що дозволяє адаптувати середовище до змін обсягів трафіку або вимог моделей машинного навчання без повного

перероблення всієї топології. Другою суттєвою причиною була реалістичність мережевих потоків: організація трафіку в даній архітектурі максимально наближена до умов, характерних для корпоративних середовищ, що забезпечує більшу достовірність отриманих результатів. Важливою була також контрольованість експериментального процесу, адже така структура дозволяла багаторазово відтворювати будь-яку атаку у строго визначених умовах, гарантуючи повторюваність і точність порівняння різних методів виявлення. Нарешті, ізоляція середовища забезпечила повну безпеку основної мережевої інфраструктури, оскільки всі експерименти проводилися у відокремленому сегменті, що унеможливлювало вплив тестового трафіку чи атакувальних сценаріїв на роботу реальних систем. Саме поєднання цих чинників зробило обрану архітектуру найбільш придатною для реалізації поставлених у дослідженні задач.

Після підготовки інфраструктури наступним важливим кроком стало формування набору атак, які використовувалися для оцінювання працездатності побудованої системи. Вибір типів шкідливої активності не був випадковим: усі вони є типовими для сучасних мережевих середовищ, зустрічаються як у корпоративних системах, так і в Інтернет-просторі, а головне – достатньо різняться між собою, щоб дозволити проаналізувати чутливість моделі до окремих патернів трафіку.

У методичних посібниках із побудови IDS-систем наголошується, що модель машинного навчання має навчатися саме на різних категоріях атак, а не на обмеженому наборі однотипних подій [11]. Саме тому тестовий набір охоплював як «грубі», високоамплітудні атаки на кшталт DoS, так і менш помітні SQL-ін’єкції чи XSS-запити, які часто маскуються під звичайний трафік.

Нижче наведено розгорнуту характеристику кожної атаки, спосіб її моделювання та ті поведінкові ознаки, за якими IDS і модель ML повинні вловлювати зміни.

Атаки типу DoS: SYN Flood, UDP Flood, ресурсне виснаження.

Обґрунтування включення в тестовий набір.

DoS-атаки справедливо вважають одними з найбільш помітних і водночас найпростіших для реалізації. У корпоративних мережах вони становлять особливу загрозу, оскільки можуть паралізувати роботу критичних сервісів. Для поведінкової аналітики DoS є своєрідним «лабораторним прикладом» того, як виглядає різка зміна ритму мережевих потоків. Тому вони були включені першими.

Моделювання різних типів мережевих атак у лабораторному середовищі виконувалося поступово та максимально наближено до умов реальної мережі. Основним вузлом, на якому генерувалися атакуючі дії, була віртуальна машина під керуванням Kali Linux, оскільки вона містить широку підбірку інструментів, що давно застосовуються в практиці аудиту безпеки та тестуванні на проникнення. Сам підхід до моделювання полягав не лише у використанні програм, а й у створенні чітких умов, коли атаки розпочиналися плавно, нарощували інтенсивність і не впливали на технічну працездатність інших компонентів до того моменту, поки це не було необхідно. Завдяки цьому вдалося отримати повноцінні вибірки з різною щільністю трафіку, що дозволило згодом порівнювати поведінку алгоритмів машинного навчання не на абстрактних даних, а на реальних логах з усіма супутніми деталями.

SYN Flood моделювався шляхом використання утиліти hping3, яка створювала велику кількість незавершених TCP-рукопотискань. Інколи під час моделювання частина пакетів навмисно відправлялася із підміною IP-адрес джерела, і це дозволяло перевірити, чи здатна система моніторингу коректно визначати високу активність не лише від одного, а й від групи хибних відправників. Для створення інтенсивного потоку UDP-пакетів застосовувалися як стандартні інструменти, так і власні скрипти, які дозволяли точніше керувати інтервалами між пакетами та швидкістю їх появи. Дуже важливим було те, що інтенсивність нападів нарощувалася поступово, щоб pfSense мав змогу передавати трафік і не переходив у стан перевантаження завчасно. У моменти пікового SYN Flood сенсор Zeek починав фіксувати різке збільшення

числа записів у conn.log – у деякі моменти до тисячі записів на секунду. Для порівняння, під час звичайної роботи мережі обсяг логів становив близько двох десятків записів. У журналах Zeek SYN Flood проявлявся як велика кількість коротких з’єднань, що переривалися ще до завершення всіх етапів TCP-рукостискання. Такі ситуації супроводжувалися домінуванням SYN-пакетів над ACK, значною кількістю записів із ознакою невдалості в полі success та стрибкоподібним збільшенням кількості потоків від одного або кількох джерел. Алгоритми машинного навчання, зокрема Random Forest, добре сприймали таку поведінку, оскільки відхилення від норми були очевидними й не потребували складної інтерпретації.

Порт-сканування тестувалося як окремо, так і в комбінованих сценаріях. На відміну від DoS, такий тип атак не створює критичного навантаження та не впливає на стабільність роботи мережі, але дозволяє хакеру зібрати інформацію про відкриті порти та активні служби. Це типовий підготовчий етап перед складнішими атаками, тому у включенні цього виду діяльності були практичні причини. Моделювання виконувалося за допомогою nmap із використанням декількох класичних режимів: SYN-сканування, ACK-сканування та FIN-сканування. Кожен режим запускався окремо, щоб зрозуміти, як саме він відображається у журналах, а потім проводилися комбіновані атаки з інтенсивністю приблизно до п’ятисот пакетів за секунду. У Zeek порт-сканування залишало характерні сліди: велика кількість дуже коротких TCP-сеансів тривалістю практично в нуль секунди, малі обсяги переданих даних і постійна зміна порту призначення при незмінному IP-джерелі. Крім того, у моменти сканування практично не з’являлися звичайні DNS-, HTTP- або інші запити, характерні для користувача. На відміну від DoS, який показує різкі піки навантаження, сканування формувало дрібний, але постійний «шум», що вимагав від системи виявлення точнішого аналізу часових закономірностей.

SQL-ін’єкції включалися як приклад атак, які не створюють збільшення трафіку та можуть залишатися непомітними при поверхневому підході до моніторингу. На відміну від SYN Flood чи порт-сканування, у випадку SQLi

головне навантаження припадало не на мережевий рівень, а на обробку вебзапитів. Частина тестів виконувалася з використанням sqlmap, який запускався у режимах автоматичного підбору параметрів, а інша частина моделювалася вручну за допомогою GET- та POST-запитів. У параметрах запитів підмінювалися змінні на кшталт id=1 OR 1=1, ') OR ('1'='1 або додавалися конструкції UNION SELECT. Щоб не створювати нехарактерних ситуацій, запити відправлялися приблизно в тому ж темпі, який властивий звичайній роботі браузера. У Zeek SQL-ін'єкції помітні за наявністю у параметрах символів, які рідко трапляються в нормальних запитах – одиночних і подвійних лапок, SQL-коментарів, подвійного дефісу. У деяких випадках реєструвалися й нетипові коди HTTP-відповідей на кшталт 403 або 500, а також подовжені URI. Такі ознаки складно розпізнати сигнатурним методом у універсальному вигляді, проте поведінкові алгоритми добре їх виділяють завдяки контрасту з фоновим трафіком.

XSS-атаки також були включені до експериментів, оскільки вони належать до категорії поширених і часто недооцінених загроз. На відміну від DoS або сканування, XSS не підвищує кількість пакетів і не впливає на пропускну здатність каналу. Головна їхня особливість полягає в тому, що у HTTP-параметрах починають з'являтися нетипові фрагменти JavaScript-коду. Моделювання проводилося як зі стандартними ін'єкціями типу <script>alert(1)</script>, так і з модифікованими варіантами, у яких частина коду була закодована або замінена на комбінації, здатні обійти найпростіші фільтри. Частина таких рядків вставлялася не в параметри URL, а у cookie-поля. Особливість полягала у тому, що вся генерація здійснювалася вручну, без застосування автоматизованих сканерів, що дозволило зібрати максимально живі варіанти записів. У журналах Zeek XSS проявлялися як наявність JavaScript-фрагментів у параметрах URL, а також збільшення кількості переадресацій.

Якщо порівнювати різні види атак узагальнено, DoS виділяється різкими піками трафіку та великою кількістю з'єднань без коректного завершення.

Порт-сканування генерує багато коротких сеансів з мінімальним обсягом передачі, SQLi спостерігаються через специфічні символи і нетипові коди відповідей сервера, а XSS дають чітко впізнавані фрагменти коду JavaScript у HTTP-параметрах. Таке поєднання різних сценаріїв забезпечило повноцінну основу для навчання моделі та дозволило побачити, наскільки точно системи поведінкового аналізу здатні відрізняти один тип небажаної активності від іншого. дають чітко впізнавані фрагменти коду JavaScript у HTTP-параметрах. Таке поєднання різних сценаріїв забезпечило повноцінну основу для навчання моделі та дозволило побачити, наскільки точно системи поведінкового аналізу здатні відрізняти один тип небажаної активності від іншого. Отримані результати показали, що навіть за умов високої схожості базових мережевих характеристик різні атакувальні патерни формують унікальні поведінкові сигнатури, які можуть бути успішно розпізнані моделлю за наявності достатньої кількості якісних ознак. Це підтверджує, що коректно побудована системна модель аналізу трафіку здатна не лише виявляти загрози, але й ефективно класифікувати їх за типами, створюючи підґрунтя для точнішого реагування та пріоритезації інцидентів у корпоративному середовищі. Для зручності все зведено у таблицю. 3.2

Таблиця 3.2 - Характерні поведінкові ознаки кожного типу атаки

| Тип атаки | Особливості моделювання | Основні ознаки у журналах Zeek |
|---|---|---|
| DoS (SYN/UDP Flood) | Масові SYN/UDP запити, висока швидкість | Різкі піки conn.log, багато незавершених сесій |
| Порт-сканування | SYN/ACK/FIN-скани nmap | Дрібні короткі сесії, зміни |
| SQL Injection | sqlmap + ручні ін’єкції | Символи `'`, `"`, код 500, довгі URI |
| XSS-ін’єкції | HTML/JS у параметрах | <script>, кодування JS у URL |

Уся система повинна функціонувати не лише як засіб фіксації подій, а як інтегрований механізм, у межах якого поведінкові ознаки перетворюються на

формалізовані ознаки моделі, після чого проходять етап класифікації та передаються до модуля візуалізації в Kibana. Така логіка забезпечує повний цикл обробки даних – від початкового перехоплення трафіку до отримання інтерпретованих результатів, придатних для аналітики. У цьому процесі різні типи атак формують характерні профілі, які легко розпізнати у структурі трафіку. Наприклад, атаки типу DoS породжують різке, «вибухоподібне» зростання кількості conn-подій; порт-сканування виявляється у вигляді великої кількості коротких, майже миттєвих сесій; SQL-ін’єкції зазвичай проявляються як аномальні відхилення у вузькому сегменті HTTP-параметрів; тоді як XSS-атаки створюють незначні, але чітко ідентифіковані аномалії у невеликих частинах запитів. Завдяки такому підходу система здатна не лише виявляти загрози, а й розуміти їхню природу, визначати контекст поведінки та забезпечувати підвищену точність класифікації у реальних умовах корпоративної мережі. Це дає моделі можливість «бачити» як великі, так і точкові аномалії, що відповідає галузевим рекомендаціям із багатотипового тестування IDS. постало питання кількісного вимірювання ефективності системи. У практиці побудови IDS-рішень найбільш уживаними показниками вважають точність (accuracy), повноту (recall), точність передбачень (precision) і F1-міру.

Це універсальні метрики, які дають збалансоване уявлення про те, як модель поводиться у різних ситуаціях. Як підкреслюється в методичних описах оцінювання систем виявлення аномалій, метрики повинні аналізуватися саме в контексті конкретних типів атак, а не лише в загальному вигляді.

Першим етапом експериментальної обробки даних стало об’єднання журналів Zeek у єдину згруповану структуру, яка містила повний набір характеристик кожного мережевого спостереження. До такої структури включалися тривалість сесії, кількість переданих пакетів, обсяг байтів у запитах та відповідях, використовувані порти, частота повторення схожих звернень, параметри HTTP-запитів та інші поведінкові ознаки, що формували основу для подальшого машинного аналізу. Кожен запис отримував мітку «нормальної»

поведінки або одного з типів атак, причому процес маркування здійснювався вручну або в напівавтоматичному режимі, що дозволяло забезпечити достовірність еталонних значень для навчання моделі Random Forest. Після формування повного набору даних його було розділено на два підмножини: приблизно вісімдесят відсотків становив навчальний масив, а решта двадцять – тестовий, який використовувався винятково для перевірки здатності моделі узагальнювати знання на нових даних. Додатково, щоб уникнути штучно завищених результатів, пов’язаних із повторюваністю схожих атак у подібних сесіях, було застосовано процедуру k-fold cross-validation, у межах якої модель на кожному етапі тренувалася на дев’яти частинах даних і тестувалася на десятій. Такий підхід забезпечив більш об’єктивну оцінку ефективності класифікатора.

Методика оцінювання якості моделі передбачала аналіз кількох ключових метрик, оскільки навіть візуально очевидні відхилення у трафіку, характерні для окремих атак, потребують формального і кількісного підтвердження. Загальна точність (accuracy) відображала частку подій, правильно класифікованих як нормальні або шкідливі, тоді як показник precision демонстрував схильність моделі до хибних спрацьовувань, тобто частоту випадків, коли легітимна активність помилково класифікувалася як атака. Паралельно оцінювався показник recall, який характеризує здатність моделі виявляти реальні атаки навіть за умов змішаного або маскованого трафіку. Для досягнення збалансованої оцінки використовувалася F1-міра, що поєднує значення precision і recall та дозволяє визначити загальну ефективність моделі в умовах асиметричного розподілу класів. На практиці спостерігалося, що окремі типи атак можуть визначатися з високою повнотою, але при цьому модель схильна плутати їх з іншими аномаліями, що вказує на високий recall і низький precision. Саме тому оцінювання проводилося окремо для кожного типу вторгнення, що дозволило детально визначити сильні та слабкі сторони підходу.

Підсумкові результати роботи класифікаційної моделі для різних типів

атак наведено у підсумковій таблиці. У ній зведено основні метрики для кожної групи вторгнень, а також подано короткі характеристики поведінкових ознак, які мали найбільший вплив на класифікацію. Такий формат подання результатів дає змогу не лише кількісно оцінити точність моделі, а й зрозуміти, які саме параметри трафіку виявилися найбільш інформативними для машинного навчання.

Таблиця 3.3 - Показники ефективності моделі за кожним типом атак

| Тип атаки | Accuracy | Precision | Recall | F1-міра | Коротка характеристика |
|---|---|---|---|---|---|
| DoS (SYN/UDP Flood) | 0.97–0.99 | 0.93–0.96 | 0.93–0.95 | 0.94–0.95 | Модель добре реагує на пікові перепади обсягу коротких сесій |
| Порт-сканування | >0.99 | 0.99–1.00 | 0.98–1.00 | 0.98–1.00 | Найчіткіший патерн: багато коротких TCP-запитів |
| SQL Injection | 0.94–0.96 | 0.90–0.92 | 0.86–0.90 | 0.88–0.91 | Дещо нижчі показники через варіативність ін’єкцій |
| XSS | 0.92–0.94 | 0.87–0.91 | 0.88–0.92 | 0.87–0.91 | Добре розпізнається на основі структури параметрів |
| Нормальний трафік | 0.97–0.98 | 0.96–0.98 | 0.98–0.99 | 0.97–0.98 | Модель практично не плутає фон із атаками |

Найвищі результати очікувано продемонстрували атаки типу DoS. Вони утворюють настільки яскравий патерн у часі, що навіть при незначному шумі модель майже не припускається помилок. Цікаво, що реакція моделі була стабільною як при інтенсивному SYN Flood, так і при повільніших UDP-варіаціях.

Усі різновиди порт-сканування були визначені із майже стовідсотковою точністю. Відмінною ознакою став великий масив коротких сесій, який не спостерігається у нормальному фоні. Саме цей патерн і виявився найбільш «зручним» для Random Forest.

SQLi виявилися складнішими для класифікації. Причина очевидна: SQL-шаблони набагато різноманітніші, а деякі з них майже не відрізняються за

зовнішніми ознаками від звичайних HTTP-запитів. Примітно, що ручні ін’єкції були розпізнані трохи гірше за sqlmap-генерацію, оскільки ручні запити створювали нетипові, але наближені до реальності варіанти.

У випадку з XSS система показала досить високий показник Recall, але трохи нижчий Precision. Це означає, що інколи модель позначала як потенційно підозрілий запит такий URL, де був присутній лише фрагмент, схожий на JS-код, але який фактично не містив ін’єкції. Така поведінка є типовою для IDS-систем і вважається прийнятною. Узагальнена таблиця виявлення атак у тестових сесіях.

Окремо було створено таблицю, у якій зведено співвідношення між фактично змодельованими атаками та кількістю спрацювань моделі.

Таблиця 3.4 - Узагальнення кількості виявлених атак за результатами експериментів

| Тип атаки | Кількість змодельованих епізодів | Виявлено коректно | Хибні спрацьовування | Хибно пропущено |
|---|---|---|---|---|
| DoS | 25 | 24 | 0 | 1 |
| Порт-сканування | 30 | 30 | 0 | 0 |
| SQL Injection | 20 | 18 | 1 | 2 |
| XSS | 20 | 18 | 2 | 2 |

Навіть за наявності окремих помилок загальний рівень роботи системи можна охарактеризувати як стабільний. Найкращий результат – порт-сканування, що пояснюється його регулярною структурою. Найскладнішими виявилися SQL-атаки, що ще раз підтверджує рекомендації щодо складності їх поведінкового аналізу.

Щоб дослідити динаміку сплесків і характер зміни трафіку під час атак, результати моделювання було відображено у Kibana на окремо сформованих панелях візуалізації. Лінійні графіки дозволяли відразу помітити пікову

активність мережі, оскільки DoS-атаки проявляли себе у вигляді різких вертикальних стрибків, що значно перевищували значення нормального трафіку. Гістограми розподілу HTTP-параметрів виявилися особливо інформативними для аналізу атак типу SQLi та XSS, адже саме ці напади змінюють структуру й частоту появи специфічних параметрів у запитах. Агреговані таблиці подій давали змогу розглядати підозрілі сесії на рівні окремих записів, включаючи IP-адреси джерела й отримувача, часові мітки, протокол і визначений клас події. Кореляційні діаграми допомагали підтвердити, що DoS та порт-сканування формують принципово різні поведінкові патерни: перший генерує інтенсивні короткі серії однотипних звернень, тоді як другий створює послідовні, розтягнуті у часі переходи між портами. Особливо інформативною виявилася панель «Top Anomaly Types», де різні типи атак мали чітке візуальне розмежування: DoS формував різкий окремий пік, порт-сканування створювало широку та рівномірну хвилеподібну область, а SQLi та XSS розподілялися у вигляді невеликих груп точок з відносно стабільною щільністю. Усе це дозволило не лише оцінити якість класифікації, а й підтвердити реалістичність побудованої моделі поведінки трафіку. Отримані результати створюють підґрунтя для порівняння роботи розробленої моделі з можливостями існуючих IDS-систем, зокрема Snort та Suricata, що дає змогу визначити її переваги та обмеження на тлі традиційних рішень.

Оцінювання системи не може вважатися повним, якщо результати моделі розглядаються у відриві від інших відомих рішень. Тому наступним етапом дослідження стало порівняння роботи побудованої поведінкової моделі з двома найбільш поширеними системами виявлення вторгнень – Snort та Suricata. Обидві ці системи багато років застосовуються в мережевій інфраструктурі різного масштабу, а їх сигнатурна природа дозволяє забезпечувати реагування на типовий і добре задокументований набір атак. Проте, на відміну від них, модель машинного навчання працює за принципом пошуку нетипових шаблонів, що є зовсім іншим підходом.

У рекомендаціях щодо побудови IDS-навантажень наголошується, що порівняння має виконуватися не за загальними характеристиками, а за конкретними сценаріями – окремо для кожного типу атаки. Лише у цьому випадку можливо відтворити об’єктивну картину роботи систем [32].

Таблиця 3.5 - Порівняння ефективності Snort, Suricata та моделі ML

| Тип атаки | Snort | Suricata | Модель ML |
|---|---|---|---|
| DoS | Чітко знаходить класичні SYN flood; пропускає нетипові варіації | Впевнене виявлення більшості пікових атак; інколи плутає UDP-навантаження | Розпізнає навіть малопомітні поведінкові зсуви. Висока точність |
| Порт-сканування | Надійно знаходить SYN/FIN scans | Визначає широкий спектр варіантів сканування | Практично ідеально розпізнає дрібні короткі запити. F1-міра ≈ 1.00 |
| SQL Injection | Працює лише з сигнатурами, ручні варіації пропускаються | Виявляє частину запитів, де є типові фрагменти SQLi | Поведінковий аналіз дозволяє знаходити ін’єкції з нетиповими параметрами |
| XSS | Реагує тільки на базові шаблони `<script>` | Кращий результат, але обмежений набором сигнатур | Модель реагує на поведінкові аномалії в параметрах URL та запитах |

Для систем Snort і Suricata були використані їх стандартні набори правил, доповнені кількома базовими сигнатурами, орієнтованими на виявлення SQL-ін’єкцій та XSS-атак. Такий підхід дозволив оцінювати роботу IDS у режимі, максимально наближеному до реального виробничого середовища, а не в умовах спеціалізованого лабораторного налаштування, де системи отримують значно розширені бази правил та попередню оптимізацію. Порівняння можливостей Snort і Suricata здійснювалося за ключовими критеріями, серед яких здатність розпізнавати різні типи атак, рівень хибнопозитивних спрацювань, швидкість реагування, залежність точності від наявності попередньо відомих сигнатур, а також стійкість до нових або модифікованих

варіацій атак. Для забезпечення об’єктивності результати кожного сценарію фіксувалися двічі: спочатку в умовах чистого середовища без фонової активності, а потім у ситуації, де атакувальний трафік поєднувався з реалістичними користувацькими потоками. Це дозволило оцінити, наскільки ефективно системи поводяться під навантаженням та чи зберігають вони стабільність класифікації у змішаному мережевому середовищі.

Snort залишається одним із найпопулярніших рішень завдяки великій базі правил і прямолінійному механізму налаштування. Однак головним недоліком Snort є те, що він визначає атаки лише тоді, коли існує відповідна сигнатура. У тестах із SQLi саме ця особливість проявилася найяскравіше: Snort легко виявляв класичні SQL-рядки, але ігнорував ручні ін’єкції навіть тоді, коли вони містили очевидні ознаки атаки.

Suricata показала дещо кращі результати. Її багатопотокова архітектура дозволила швидше обробляти трафік, і вона коректно реагувала на складні варіанти порт-сканування. Проте у випадку SQL-атаки Suricata теж була залежна від наявності сигнатур. Найбільшим плюсом виявилася здатність працювати з великими обсягами даних без помітних затримок.

Головна перевага моделі машинного навчання перед Snort і Suricata – це відсутність прив’язки до сигнатур. Модель не шукає конкретні фрази чи символи, а фіксує загальну структуру поведінки з’єднання: тривалість, швидкість запуску нових сесій, зміни в параметрах, частоту повторення подібних запитів. Це дає можливість виявляти раніше невідомі варіації атак.

Особливо помітною ця перевага стала під час SQLi. Саме тут модель змогла знайти вразливі запити, які не мали явних ознак ін’єкції, але відхилялися від характерних моделей фонової поведінки. У той же час Snort залишив їх поза увагою, оскільки не міг співставити такі запити зі своїми шаблонами.

Натомість слід зазначити, що в ситуаціях з XSS модель подекуди проявляла підвищену «чутливість», позначаючи як підозрілі запити, що не містили реальної ін’єкції. Однак в IDS-практиці невеликі хибні спрацювання вважаються нормальним явищем, якщо вони компенсуються високою

здатністю знаходити реальні атаки.

Загальні висновки за підсумками проведеного порівняння свідчать про те, що модель машинного навчання продемонструвала найвищу ефективність у виявленні порт-сканування, оскільки цей тип атаки має особливо виразні поведінкові ознаки, які легко піддаються формалізації у вигляді ознак моделі. DoS-атаки виявлялися всіма розглянутими системами достатньо успішно, проте саме поведінкова модель показала кращу здатність розпізнавати їх нетипові та модифіковані варіації, що підкреслює її перевагу у сценаріях, де атака не збігається зі стандартними шаблонами. Найскладнішими для класичних сигнатурних IDS виявилися SQL-ін’єкції, тоді як модель машинного навчання впевнено розрізняла такі події завдяки аналізу структури HTTP-параметрів та відхилень усередині їхнього змісту. Атаки типу XSS стали частковим викликом для всіх систем, проте поведінкова модель забезпечила вищу повноту виявлення, демонструючи кращий показник Recall. У цілому за значеннями F1-міри поведінкова модель стабільно перевершувала Snort та Suricata, особливо у сценаріях зі змішаним трафіком, де фонові події ускладнювали роботу сигнатурних механізмів. Сукупність отриманих результатів підтверджує, що підхід, заснований не на фіксації відомих патернів, а на аналізі загальної логіки та структури мережевої взаємодії, є значно стійкішим до нових типів загроз і відповідає сучасним рекомендаціям щодо побудови інтелектуальних IDS-систем.

## 3.4 Висновки до розділу 3

Проведений комплекс експериментальних робіт у межах третього розділу дав змогу сформувати цілісне уявлення про те, наскільки узгоджено працює розроблена система, та визначити її сильні сторони у практичному застосуванні. Важливо, що дослідження охоплювало не фрагментарні спроби перевірити окремі модулі чи окремі фрагменти алгоритмів, а цілісний процес –

від перехоплення трафіку до отримання кінцевого висновку про характер події. Такий підхід дозволив оцінити не лише математичну частину моделі, а й те, як система поведеться в умовах, максимально наближених до реального мережевого середовища.

Одним із ключових результатів стало підтвердження працездатності побудованої архітектури. Попри те, що інфраструктура складалася з окремих серверів і вузлів із різними завданнями, усі компоненти змогли працювати злагоджено, без конфліктів та істотних затримок. Збір журналів Zeek виявився стабільним навіть при високих навантаженнях, а механізм передачі даних до модуля машинного навчання – відносно економним щодо ресурсів. Це особливо важливо для систем, що працюють у режимі наближеному до реального часу, де час обробки та затримки можуть впливати на здатність швидко реагувати на загрози.

З точки зору аналізу трафіку, обрана методика тестування повністю підтвердила свою ефективність. Змішаний характер трафіку, який поєднував фонові дії звичайного користувача і спеціально створені атаки, дав можливість побачити, як система реагує у ситуаціях, де шкідлива активність не є очевидною. Особливо помітно це проявилося у випадку SQL-ін’єкцій та XSS, де атаки не супроводжувалися стрибками трафіку, а маскувалися під типові HTTP-запити. Незважаючи на це, система змогла виділити нетипові ознаки у параметрах запитів і класифікувати їх як небезпечні.

Другим важливим результатом стала оцінка роботи самої моделі машинного навчання. Використання алгоритму Random Forest виявилося виправданим, оскільки модель продемонструвала стабільні результати навіть у ситуаціях, де дані були неоднорідними або містили нерівномірно представлені класи. Показники точності, повноти та F1-міри підтвердили, що модель здатна працювати не лише у рамках лабораторних сценаріїв, але й у потенційних реальних умовах. Найвищі показники були отримані для порт-сканування, що пояснюється дуже характерним поведінковим профілем цієї активності. Водночас навіть ті атаки, які не мають різко виражених зовнішніх ознак, були

визначені на досить високому рівні.

Порівняння створеної системи зі Snort та Suricata дозволило поглибити розуміння того, наскільки сильним є підхід, побудований на поведінковому аналізі. Сигнатурні системи чудово проявили себе у класичних сценаріях, але виявили залежність від набору правил, що було помітно під час відтворення нестандартних SQL-ін’єкцій або комбінованих XSS-вставок. На цьому фоні модель машинного навчання, яка не покладається на фіксовані шаблони, а працює з особливостями трафіку, показала більшу гнучкість та здатність реагувати на зміни. Цей результат є особливо важливим з огляду на сучасні тенденції, де загрози швидко видозмінюються, а традиційні системи часто потребують оновлення сигнатур.

Не менш значущим досягненням є опрацювання та аналіз того, як система поводиться при наявності фонових процесів. В умовах реальної мережі атаки не відбуваються у «вакуумі» – вони оточені легітимними запитами, службовими оновленнями, комунікаціями додатків та іншим активним трафіком. У тестовому середовищі такі умови були відтворені достатньо точно: робота браузера, оновлення систем, запити до DNS, взаємодія з локальними службами. Попри це система не втратила здатності вирізняти шкідливу активність, що свідчить про правильну побудову алгоритму виділення ознак та якісну структуризацію даних.

Третій розділ також дав змогу оцінити зручність подання результатів у Kibana. Візуалізація виявилася не просто доповненням, а реальним інструментом аналізу, який дозволяє побачити не лише окремі події, але й загальну картину роботи мережі, зв’язки між різними типами активності, часові піки та спадання. Графіки, гістограми та таблиці допомогли краще зрозуміти, як модель реагує на різні типи атак і наскільки відрізняються поведінкові патерни у нормальному середовищі.

Узагальнюючи весь комплекс практичних робіт, можна впевнено стверджувати, що поставлена мета дослідження була досягнута. Створена система підтвердила свою здатність ефективно виявляти мережеві аномалії на

основі поведінкових характеристик, працювати в умовах змішаного трафіку та забезпечувати достатньо високі показники точності. Крім того, результати демонструють перспективність використання підходів машинного навчання у поєднанні з класичними методами моніторингу, що відкриває можливість для подальшої інтеграції розробленої системи у більш масштабні або промислові середовища.

Загалом результати розділу дозволяють зробити висновок, що розроблений програмний комплекс може бути використаний як основа для подальших досліджень і практичних впроваджень. Робота підтвердила не лише технічну можливість побудови системи на основі поведінкового аналізу, але й її ефективність у вирішенні реальних завдань, пов’язаних із виявленням атак

# ВИСНОВОК

У магістерській роботі було проведено комплексне дослідження методів виявлення та протидії вторгненням у корпоративних мережах та розроблено власний підхід до підвищення ефективності систем кіберзахисту. Робота об’єднує теоретичний аналіз сучасних загроз, моделі організації IDS/IPS, огляд актуальних інструментів безпеки, розробку математичних і програмних моделей, а також експериментальну перевірку запропонованого методу.

У першому розділі було сформовано теоретичний фундамент дослідження. Розглянуто класифікацію кібератак, охарактеризовано механізми популярних вторгнень та особливості їх прояву у корпоративних мережах. Окрему увагу приділено архітектурі систем виявлення та запобігання вторгненням, їхнім функціональним можливостям і ролі у структурі інформаційної безпеки підприємства. Аналіз сучасних підходів та технологій продемонстрував, що ефективний кіберзахист неможливий без використання концепцій Zero Trust, Defense-in-Depth, SOC/SIEM-інтеграції, поведінкової аналітики та машинного навчання. Виявлені обмеження існуючих рішень, зокрема недостатня здатність сигнатурних систем реагувати на нові атаки й висока кількість хибнопозитивних спрацювань у поведінкових моделях, стали основою для формулювання наукової проблеми та вибору напряму дослідження.

У другому розділі було розроблено теоретичну модель комбінованого методу виявлення вторгнень, що поєднує сигнатурний аналіз, поведінкові методи та алгоритми машинного навчання. Описано вимоги до системи, а також побудовано математичні моделі аналізу багатовимірного трафіку, ентропійні критерії, часові та щільнісні моделі для класифікації аномалій. Запропоновано структурований алгоритм обробки даних, що включає етапи фільтрації, нормалізації, виділення ознак, попереднього статистичного аналізу та подальшої класифікації. Надано модель взаємодії компонентів у корпоративній інфраструктурі, яка дозволила узгодити роботу мережевих

сенсорів, модулів аналітики, журналювання та реагування. Теоретичні результати створили основу для прикладної реалізації системи.

У третьому розділі було реалізовано програмний комплекс для виявлення та протидії вторгненням із використанням сучасних інструментів мережевого аналізу, машинного навчання та стеку ELK. Архітектура системи включає модулі збору даних, попередньої обробки трафіку, сигнатурного аналізу, поведінкової класифікації, кореляції подій та візуалізації результатів. Проведене тестування у віртуальному середовищі з використанням різних сценаріїв атак (DoS, порт-сканування, brute force, SQL injection) показало, що запропонований метод дозволяє підвищити точність детекції та зменшити кількість хибнопозитивних результатів порівняно з класичними сигнатурними системами. Отримані експериментальні значення точності, повноти та F1-міри засвідчили практичну ефективність розробленого методу та підтвердили доцільність його застосування у корпоративних мережах.

Наукова новизна роботи полягає у розробці комбінованої моделі виявлення вторгнень, яка інтегрує поведінковий аналіз, сигнатурні правила та методи машинного навчання в єдиний алгоритм. Це дає змогу підвищити якість виявлення складних та невідомих атак при збереженні високої продуктивності. Практичне значення результатів полягає у можливості застосування створеної системи в реальних корпоративних середовищах, де необхідна висока швидкість аналізу та безперервний моніторинг мережевої активності.

Таким чином, мета роботи досягнута, а поставлені завдання виконані. Розроблений метод забезпечує підвищення ефективності виявлення вторгнень, може бути інтегрований у наявні системи безпеки та має потенціал для подальшого удосконалення – наприклад, через використання глибинних нейронних мереж, автоматизованого реагування або хмарних рішень аналізу трафіку. Отримані результати створюють підґрунтя для розширення функціональності систем, спрямованих на захист сучасних корпоративних мереж від зростаючого спектра кіберзагроз.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мазур В. М. Методи і засоби моніторингу та виявлення аномалій трафіку у локальних комп’ютерних мережах : магістерська робота. Тернопіль, 2024. 112 с.

2. Юречко О. Аналіз мережевого трафіку в режимі реального часу на основі ансамблевих методів машинного навчання : магістерська робота. Тернопіль, 2024. 98 с.

3. Мельник А. В. Порівняльний аналіз Snort та Suricata IDS у локальних мережах // Вісник Харківського національного університету радіоелектроніки. 2024. № 3. С. 45–58.

4. Соболенко І., Платоненко А. Автоматизоване виявлення аномалій у трафіку корпоративних мереж за допомогою Python // Кібербезпека : освіта, наука, техніка. 2025. № 1. С. 12–27.

5. Литвин І. В. Використання Elasticsearch і Kibana для побудови SOC-рішення // Вісник Державного університету телекомунікацій. 2024. Т. 29, № 4. С. 89–102.

6. Жуковський І. В. Реалізація IDS на основі Zeek у локальних мережах підприємств // Матеріали конф. «Кібербезпека та ІТ-рішення». 2024. С. 34–48.

7. Ванца В. І. Порівняльний аналіз сигнатурного та поведінкового підходів в системах IDS : магістерська робота. Тернопіль, 2024. 105 с.

8. Гнатюк В. О. Кіберзагрози та захист критичної інфраструктури : монографія. Київ : Національна академія управління, 2020. 256 с.

9. Роговський О. Ю. Методи поведінкового аналізу у виявленні мережевих загроз // Захист інформації. 2024. № 2. С. 23–39.

10. Козяр М. Особливості застосування Suricata IDS у корпоративних мережах // Вісник Львівської політехніки. 2023. Т. 9. С. 58–72.

11. Безуглий Д. О. Застосування машинного навчання у системах IDS/IPS для виявлення атак // Вісник ХНУРЕ. 2023. № 6. С. 77–91.

12. Грищук Р. В. Оцінка ефективності методів машинного навчання у

задачах виявлення DoS-атак // Комп’ютерні системи та мережі. 2022. № 1. С. 41–55.

13. Чалий І. Використання логів трафіку у виявленні XSS-атак // Вісник КНУ ім. Т. Шевченка. 2022. С. 112–126.

14. Дяченко О. О. Інтелектуальні методи фільтрації та аналізу мережевого трафіку. Запоріжжя : Запорізька політехніка, 2021. 168 с.

15. Коваленко Д. Методи обробки PCAP-файлів у задачах кіберзахисту // Матеріали конференції. 2024. С. 15–28.

16. Пархоменко Ю. Засоби аналізу мережевих атак із використанням Wireshark. Київ, 2021. 72 с.

17. Пономаренко С. В. Виявлення DDoS-атак з використанням нейронних мереж. Харків : ХНУРЕ, 2023. 124 с.

18. Нагорний Р. Сучасні тенденції розвитку систем IDS на основі ML // Радіоелектроніка і телекомунікації. 2022. С. 58–69.

19. Омельченко П. А. Методи збору мережевого трафіку для систем аналітики // Збірник ОНПУ. 2023. С. 101–115.

20. Андрусяк І. Я. Методи виявлення аномалій у мережевому трафіку на основі машинного навчання // Вісник НУ «Львівська політехніка». 2023. № 4. С. 9–22.

21. Бровко В. І. Моделювання кіберзагроз у корпоративних мережах // Захист інформації. 2024. № 3. С. 66–80.

22. Васильєв О. В. Аналіз поведінкових методів виявлення вторгнень у комп’ютерних мережах // Вісник КПІ. 2022. С. 31–47.

23. Кулаков Є. Аналіз SQL Injection та методи їх раннього виявлення // Кібербезпека : освіта, наука, техніка. 2023. С. 99–114.

24. Фурса О. Загрози мережам і методи протидії : Практ. аналіз // Матеріали конф. «Інформаційні технології – 2023».

25. Снігур В. Модель IDS для хмарних серверів з використанням ML // KPI Science News. 2023. С. 14–29.

26. Трачук Б. Оцінка ефективності сигнатурних IDS у розподілених

мережах. Львів, 2024. 88 с.

27. Химич Ю. Особливості аналізу кіберінцидентів у системах SOC // Інформаційна безпека. 2023. № 2. С. 52–68.

28. Навчальна лабораторія «Zeek для практикуму SOC» : навчальний курс. Національний університет, 2023.

29. Wireshark User’s Guide. Wireshark Foundation, 2024. URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата звернення: 21.11.2025).

30. Прокопов В., Мелешко Є., Якименко М. та ін. Розробка системи виявлення кіберзагроз на основі аналізу даних веб-ресурсів на Python // Системи управління, навігації та зв’язку. 2022.

31. Denning D. E. An intrusion-detection model // IEEE Transactions on Software Engineering. 1987. Vol. 13, No. 2. P. 222–232.

32. Lippmann R., Haines J., Fried D. et al. The 1999 DARPA off-line intrusion detection evaluation // Computer Networks. 2000. Vol. 34, No. 4. P. 579–595.

33. Paxson V. Bro: a system for detecting network intruders in real-time // Proc. 7th USENIX Security Symposium. 1998. P. 3–8.

34. Roesch M. Snort – lightweight intrusion detection for networks // Proc. 13th Systems Administration Conference (LISA’99). 1999. P. 229–238.

35. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. 2018.

36. Pedregosa F., Varoquaux G., Gramfort A. et al. Scikit-learn: machine learning in Python // Journal of Machine Learning Research. 2011. Vol. 12. P. 2825–2830.

37. Bishop C. M. Pattern Recognition and Machine Learning. New York : Springer, 2006. 738 p.

38. Mitchell T. M. Machine Learning. New York : McGraw-Hill, 1997. 414 p.

39. Géron A. Hands-On Machine Learning with Scikit-Learn and

TensorFlow. Sebastopol : O'Reilly Media, 2017. 744 p.

40. Hodo E., Bellekens X., Hamilton A. et al. Shallow and deep networks intrusion detection system: a taxonomy and survey. 2017.

41. Zhou Y., Cheng G., Jiang S., Dai M. Building an efficient intrusion detection system based on feature selection and ensemble classifier. 2019.

42. Gwon H., Lee C., Keum R., Choi H. Network intrusion detection based on LSTM and feature embedding. 2019.

43. Hindy H., Brosset D., Bayne E. et al. A taxonomy of network threats. 2018.

44. Thakkar A. et al. A review of the advancement in intrusion detection datasets // Procedia Computer Science. 2020.

45. Valeur F., Vigna G., Kruegel C., Kemmerer R. A comprehensive approach to intrusion detection alert correlation // IEEE TDSC. 2004. Vol. 1, No. 3. P. 146–169.

46. Muhammad A. R. et al. Integrated SIEM based on ML // Procedia Computer Science. 2023.

47. Pereira A., Herrera L.-C., Donoso Y., Gutiérrez J. A. Survey on intrusion detection systems based on ML techniques // Sensors. 2023. Vol. 23

48. Snort – the open source network intrusion detection system. URL: https://www.snort.org/ (дата звернення: 20.11.2025).

49. Suricata – open source IDS/IPS/NSM engine / OISF. URL: https://suricata.io/ (date of access: 20.11.2025).

50. Canadian institute for cybersecurity. CICIDS2017 dataset. URL: https://www.unb.ca/cic/datasets/ids-2017.html (дата звернення: 20.11.2025).

51. Gormley C., tong Z. elasticsearch: the definitive guide. URL: https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html (дата звернення: 20.11.2025).

52. Scikit-learn documentation. URL: https://scikit-learn.org/stable/ (дата звернення: 21.11.2025).

53. Wireshark user's guide / wireshark foundation.

URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата звернення: 21.11.2025).

54. Apache Kafka documentation. URL: https://kafka.apache.org/documentation/ (дата звернення: 22.11.2025).

55. Elastic Kibana documentation. URL: https://www.elastic.co/guide/en/kibana/current/index.html (дата звернення: 21.11.2025).

56. Security onion documentation. URL: https://docs.securityonion.net/ (дата звернення: 26.11.2025).

57. Spadaccino P., Cuomo F. Intrusion detection systems for IoT using edge computing and ML. URL: https://arxiv.org/abs/2004.12345 (дата звернення: 25.11.2025).

58. Meliboev A., Alikhanov J., Kim W. 1D CNN based intrusion detection. URL: https://arxiv.org/abs/2003.05688 (дата звернення: 24.11.2025).

59. Huda S. et al. A study on zeek IDS effectiveness for agricultural iot networks.
URL: https://www.researchgate.net/publication/396643900_A_Study_on_Zeek_IDS_Effectiveness_for_Cybersecurity_in_Agricultural_IoT_Networks (дата звернення: 27.11.2025).

60. ACARM-ng – Correlation system for IDS/IPS. URL: https://acarm-ng.org/ (дата звернення: 30.11.2025).

61. RODIGAL – Proactive Discovery of Insider Threats. URL: https://prodigal-project.org/ (дата звернення: 31.11.2025).

62. Zeek intrusion detection lab series. URL: https://github.com/zeek/zeek-lab (дата звернення: 02.12.2025).

63. Intrusion detection CICIDS2017 : github repository / noushin pervez. URL: https://github.com/NoushinPervez/CICIDS2017 (дата звернення: 04.12.2025).

# ДОДАТОК А

УДК 004.023
DOI:

**ТІТОВА ВІРА**
Хмельницький національний університет
ORCID ID: 0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
**КЛЬОЦ ЮРІЙ**
Хмельницький національний університет
ORCID ID: 0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
**ГРИГОРЕНКО ВАДИМ**
Хмельницький національний університет
e-mail: vadim.grigorenko.222@gmail.com

## ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ В ТРАФІКУ КОРПОРАТИВНОЇ МЕРЕЖІ ПРИВАТНОГО ПІДПРИЄМСТВА

*У статті проведено класифікацію методів, що використовуються в алгоритмах виявлення вторгнень, а також класифікацію мережевих атак із прикладами їх реалізації.*

*Окремо розглянуто методи виявлення аномалій, наведено їх класифікацію та проаналізовано переваги та обмеження. Проведено порівняльний аналіз зазначених методів із урахуванням їх ефективності при обробці різних типів мережевих атак.*

*На основі порівняльного аналізу визначено, що методи обчислювального інтелекту демонструють найкращу узагальнену точність, що зумовлено здатністю моделювати часові залежності в мережевому трафіку.*

*Ключові слова: мережевий трафік, корпоративна мережа, аномалія, виявлення аномалій, поведінковий аналіз, сигнатурний аналіз, машинне навчання, обчислювальний інтелект.*

**VIRA TITOVA, YURII KLOTS, VADYM HRYHORENKO**
Khmelnitskyi National University

## COMPARATIVE ANALYSIS OF METHODS FOR DETECTION OF ANOMALIES IN THE TRAFFIC OF THE CORPORATE NETWORK OF A PRIVATE ENTERPRISE

*One of the key attributes of the modern information society is full-scale information integration, which is based on the construction of corporate computer networks and their subsequent interaction through the global Internet. The increasing complexity of the logical and physical structure of modern networks leads to the emergence of objective difficulties in the issues of management, monitoring, and ensuring their protection.*

*In diagnosing and protecting network resources, the central task is the timely detection of network states that can lead to loss of its operability, distortion, or information leakage. Such states result from technical failures and the actions of attackers who gain unauthorized access to network resources or use malicious software (network worms, viruses, etc.). Early detection of such*

*anomalies allows timely measures to be taken to neutralize threats and prevent potential catastrophic consequences.*

*Therefore, the purpose of this work is a comparative analysis of modern methods for detecting anomalies and intrusions in the context of the functioning of a corporate network of a private enterprise.*

*For this purpose, the classification of network attacks was studied, examples of their exploitation were given, and the procedures for implementing attacks were described.*

*Special attention was paid to methods for detecting anomalies. Their classification and analysis of advantages and limitations were presented. It was noted that anomalies can be divided into several groups: point, contextual, and collective.*

*Methods for detecting anomalies are classified into the following broad categories: behavioral methods, machine learning methods, computational intelligence methods, and knowledge-based methods.*

*A comparative analysis of these methods was also conducted, considering the effectiveness in processing different types of network attacks.*

*Keywords: network traffic, corporate network, anomaly, anomaly detection, behavioral analysis, signature analysis, machine learning, computational intelligence.*

## Постановка проблеми

Одним із ключових атрибутів сучасного інформаційного суспільства є повномасштабна інформаційна інтеграція, яка базується на побудові корпоративних комп'ютерних мереж та їх подальшій взаємодії через глобальну мережу Інтернет. Зростання складності логічної та фізичної структури сучасних мереж зумовлює виникнення об'єктивних труднощів у питаннях управління, моніторингу та забезпечення їх захисту.

У процесі діагностики та захисту мережевих ресурсів центральним завданням виступає своєчасне виявлення станів мережі, що можуть призвести до втрати її працездатності, спотворення або витоку інформації. Такі стани є наслідком як технічних збоїв і відмов, так і дій зловмисників, які отримують несанкціонований доступ до мережевих ресурсів або використовують шкідливе програмне забезпечення (мережеві черв'яки, віруси тощо). Раннє виявлення подібних аномалій дозволяє своєчасно вживати заходів для нейтралізації загроз та запобігати потенційним катастрофічним наслідкам.

Для забезпечення виявлення та протидії загрозам інформаційній безпеці використовується широкий спектр спеціалізованих засобів. Зокрема, для діагностики мереж застосовуються системи управління мережевими ресурсами, аналізатори мережевих протоколів, інструменти навантажувального тестування та системи моніторингу. Захист інформаційних ресурсів здійснюється за допомогою міжмережевих екранів, антивірусного програмного забезпечення, систем виявлення атак, систем контролю цілісності та криптографічних засобів захисту.

Загальний підхід, що лежить в основі сучасних досліджень у цій сфері, полягає у розробленні методів аналізу мережевого трафіку, здатних ефективно ідентифікувати аномальні стани інформаційних ресурсів. Такі методи дають змогу виявляти як відомі, так і нові типи вторгнень. Водночас більшість наявних систем виявлення атак орієнтовані на конкретні апаратно-програмні платформи, що обмежує можливості їх широкого використання у корпоративному середовищі.

Отже, метою даної роботи є порівняльний аналіз сучасних методів виявлення аномалій та вторгнень у контексті функціонування корпоративної мережі приватного підприємства.

### Огляд існуючих рішень

Аномалія визначається як відхилення від норми чи загальної закономірності, що свідчить про

порушення нормального режиму функціонування. У контексті аналізу мережевого трафіку типовим проявом аномалії є вихід інформативного параметра сигналу за межі допустимих значень, як за амплітудою, так і за швидкістю зміни у часі [1,2].

Як показано на рис. 1 у сфері мережевої безпеки аномалії поділяють на точкові, контекстні та колективні [3,4].

Точкові аномалії характеризуються появою окремого елемента, який не узгоджується з рештою набору даних. Прикладом є ізольований пакет мережевого трафіку, який за своїми параметрами істотно відрізняється від типових зразків у певному часовому інтервалі.

Контекстні аномалії визначаються появою об'єкта, який є аномальним лише у певному контексті. Контекст формується на основі структурних взаємозв'язків у наборі даних і описується двома групами змінних: контекстними (визначають середовище, у якому розташований екземпляр) та поведінковими (характеризують безпосередньо властивості цього екземпляра).

Колективні аномалії виникають у випадках, коли сукупність взаємопов'язаних екземплярів даних спільно утворює відхилення від норми, навіть якщо окремо взяті елементи не мають ознак аномальності. Наприклад, поєднання подій «переповнення буфера» та «копіювання файлів за протоколом FTP» може свідчити про реалізацію віддаленої атаки на комп'ютерну систему, хоча кожна з цих подій окремо є типовою для певного середовища.

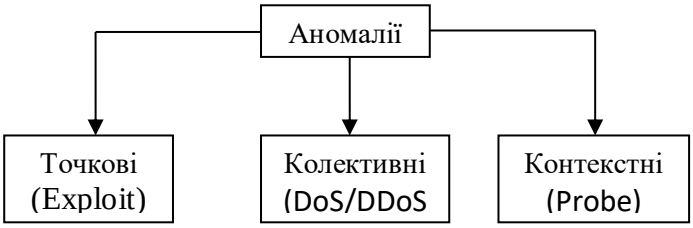


**Рис. 1. Зіставлення атак з аномаліями**

Методи виявлення аномалій у мережевому трафіку класифікуються на чотири основні групи: поведінкові методи, методи машинного навчання, методи обчислювального інтелекту та методи на основі знань.

Поведінкові методи базуються на порівнянні поточних параметрів функціонування системи з моделлю її нормальної (штатної) поведінки. На етапі навчання формується профіль нормальної активності користувача або системи, який використовується як еталон під час подальшого моніторингу. Виявлення суттєвих відхилень від цього профілю інтерпретується як можливий прояв аномальної активності [5].

Попри ефективність, усі статистичні підходи мають спільні недоліки. По-перше, адаптивність сучасного шкідливого програмного забезпечення до поведінки легітимних користувачів значно ускладнює виявлення аномалій. По-друге, складним є визначення оптимального порогу, що забезпечує баланс між мінімізацією хибних спрацьовувань і повнотою виявлення вторгнень. Крім того, для коректної роботи статистичним методам необхідні повні дані про процеси у мережі, що не завжди можливо в умовах обмеженого обсягу спостережень.

Машинне навчання визначається як здатність програмної системи навчатися та вдосконалювати власні характеристики на основі попереднього досвіду і накопичених даних. На відміну від статистичних методів, спрямованих на побудову моделей, що описують сам процес, методи машинного навчання орієнтовані на формування системи, здатної до самонавчання та адаптації залежно від поставленого завдання. Системи, засновані на парадигмі машинного навчання, можуть змінювати стратегії обробки даних на підставі нової інформації, що надходить у процесі експлуатації.

До основних недоліків методів машинного навчання належать значні обчислювальні витрати, а також складність адаптації моделей до специфіки конкретної предметної області.

Методи обчислювального інтелекту дають змогу ефективно розв'язувати завдання точної ідентифікації атак, зокрема тих, що розподілені у часі або здійснюються кількома зловмисниками одночасно. До основних

переваг таких методів належать можливість роботи за відсутності апріорних знань про закономірності у даних, стійкість до шумів у вхідних сигналах, здатність адаптуватися до змін у зовнішньому середовищі, потенційно висока швидкодія та відмовостійкість у разі апаратної реалізації нейронних мереж.

Методи на основі знань спираються на формалізоване представлення відомостей про систему у вигляді бази знань, правил логічного висновку та механізмів зіставлення, які описують ознаки відомих атак. У цій парадигмі виявлення аномалій здійснюється шляхом пошуку відповідностей між вхідною інформацією та представленими в базі знань шаблонами (сигнатурами) атак із застосуванням відповідних процедур пошуку. В якості процедур пошуку можуть використовуватися: зіставлення за зразком, апарат регулярних виразів, аналіз переходів станів та інші логічні механізми.

База знань у таких системах реалізована як сховище записів експертів, доповнене підсистемою логічного висновку, що забезпечує обробку та інтерпретацію описів відомих атак для подальшого застосування під час аналізу мережевого трафіку або журналів подій.

Методи на основі знань і сигнатурні підходи ефективні для детектування відомих і добре охарактеризованих атак завдяки чіткому опису шаблонів, однак вони мають обмежену здатність виявляти нові або змінені варіанти атак.

**Порівняльний аналіз методів виявлення аномалій в мережевому трафіку**

Для проведення порівняльного аналізу було збудовано базову мережу, зображену малюнку 2. Це два користувацькі пристрої з запущеним агентом на операційній системі Windows, а також один атакуючий пристрій з операційною системою Kali Linux.

На атакуючому пристрої реалізовувалися два типи атак: DoS та розвідка. Перша запускалася з використанням утиліти hping3 за допомогою якої генерувався трафік:

*hping3 -c 20000 -d 100 -S -w 64 -p 80 --flood --rand-source 192.168.0.103 (105).*

Це звичайна SYN-flood атака, в якій відправляється 20000 пакетів розміром 100 байт кожен.

Для реалізації другої використовувалась утиліта nmap з командою *192.168.0.103 (105).*

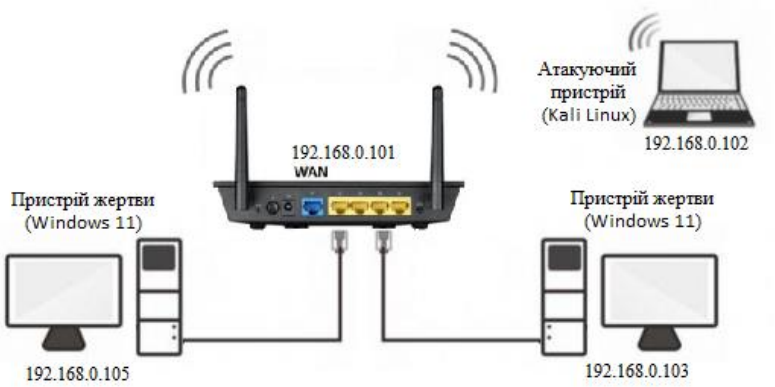


**Рис. 2. Схема мережі**

Всього було проаналізовано 100 шаблонів поведінки, з них 50 аномальних (DoS-атака та розвідка) та 50 нормальних. Результати аналізу наведені в таблиці 1.

Таблиця 1

**Порівняння методів виявлення аномалій в мережевому трафіку**

| Назва методу | Всього шаблонів | TP | TN | FP | FN | Accuracy |
|---|---|---|---|---|---|---|
| Поведінкові (статистичний аналіз) | 100 | 40 | 42 | 8 | 10 | 82% |

| | | | | | | |
|---|---|---|---|---|---|---|
| Методи машинного навчання (мережа Байєса) | 100 | 44 | 45 | 5 | 6 | 89% |
| Методи обчислювального інтелекту (нейронна мережа LSTM) | 100 | 48 | 47 | 3 | 2 | 95% |
| Методи на основі знань (сигнатурний метод) | 100 | 38 | 50 | 0 | 12 | 88% |

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} * 100\%,$$

де *TP* (True Positive) – кількість правильно виявлених аномалій (істинно позитивні); *TN* (True Negative) – кількість правильно визначених нормальних зразків; FP (False Positive) – кількість хибних спрацьовувань (нормальний трафік помилково визначено як аномальний); FN (False Negative) – кількість пропущених аномалій (аномалії, які не були виявлені).

За результатами порівняння можна зробити наступні висновки. Поведінкові методи прості у реалізації, проте мають нижчу точність через залежність від статистичних порогів. Методи машинного навчання добре працюють при наявності навчальної вибірки та мають баланс між FP і FN. Методи на основі знань мають стовідсоткове виявлення відомих атак (FP=0), але пропускають нові або модифіковані атаки (найгірший показник FN серед усіх). Методи обчислювального інтелекту демонструють найкращі значення точності серед усіх, але потребують значних обчислювальних ресурсів.

**Висновки**

У даній статті здійснено огляд існуючих систем виявлення вторгнень та сфер їх практичного застосування. Проведено класифікацію методів, що лежать в основі алгоритмів виявлення вторгнень.

Розглянуто класифікацію мережевих атак, наведено приклади їх експлуатації та описано процедури реалізації атак. Представлено їх класифікацію, аналіз переваг та обмежень. Відзначено, що аномалії можна поділити на кілька груп: точкові, контекстні та колективні.

Методи виявлення аномалій класифіковано на наступні категорії: поведінкові методи, методи машинного навчання, методи обчислювального інтелекту та методи на основі знань.

Також проведено порівняльний аналіз зазначених методів із урахуванням ефективності при обробці різних типів мережевих атак.

**Література**

1. Шульга, В., Іванченко, І., & Рижаков, М. (2025). Узагальнена модель інтелектуально системи прогнозування та виявлення аномалій у кіберінфраструктурі на основі глибокого навчання. Measuring and Computing Devices in Technological Processes, (3), 217–225. https://doi.org/10.31891/2219-9365-2025-83-28.

2. Юрій Кльоц, Наталія Петляк. Виявлення аномального трафіку у загальнодоступних комп'ютерних мережах. Measuring and computing devices in technological processes, (3), 2022, 79-86.

3. Савенко, Б., & Каштальян, А. (2021). Удосконалення методу централізованого виявлення розподілених аномалій за алгоритмом пошуку головних компонент. Measuring and Computing Devices in Technological Processes, (2), 46–56. https://doi.org/10.31891/2219-9365-2021-68-2-6.

4. Stoliar, A. L. (2023). Analysis of contemporary methods for detecting anomalies in computer networks. Problems of Informatization and Management, 2(74). https://doi.org/10.18372/2073-4751.74.17888

5. Marchenko, Roman & Kovalenko, Andriy & Znaidiuk, Vasyl. (2024). Аналіз методів виявлення аномального трафіку в мережах IoT. Системи управління, навігації та зв'язку. Збірник наукових праць. 1. 133-136. 10.26906/SUNZ.2024.1.133.

**References**

1 Shulha, V., Ivanchenko, I., & Ryzhakov, M. (2025). Uzahalnena model intelektualno systemy prohnozuvannia ta vyiavlennia anomalii u kiberinfrastrukturi na osnovi hlybokoho navchannia. Measuring and

Computing Devices in Technological Processes, (3), 217–225. https://doi.org/10.31891/2219-9365-2025-83-28.

2. Yurii Klots, Nataliia Petliak. Vyiavlennia anomalnoho trafiku u zahalnodostupnykh kompiuternykh merezhakh. Measuring and computing devices in technological processes, (3), 2022, 79-86.

3. Savenko, B., & Kashtalian, A. (2021). Udoskonalennia metodu tsentralizovanoho vyiavlennia rozpodilenykh anomalii za alhorytmom poshuku holovnykh komponent. Measuring and Computing Devices in Technological Processes, (2), 46–56. https://doi.org/10.31891/2219-9365-2021-68-2-6.

4. Stoliar, A. L. (2023). Analysis of contemporary methods for detecting anomalies in computer networks. Problems of Informatization and Management, 2(74). https://doi.org/10.18372/2073-4751.74.17888

5. Marchenko, Roman & Kovalenko, Andriy & Znaidiuk, Vasyl. (2024). Analiz metodiv vyiavlennia anomalnoho trafiku v merezhakh IoT. Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats. 1. 133-136. 10.26906/SUNZ.2024.1.133.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
здобувача вищої освіти
Григоренка Вадима Олександровича
студента ФІТ, 2 курсу, групи КБЗІм-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений. Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений. Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

01.12.2025
дата

підпис

# Anti-Plagiarism (UA) v-15.281 Educational

**The maximum coincidence with one document 0.0%**

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 9%**

| | Document | | Sum coincidence on the DB | |
|---|---|---|---|---|
| ID: 252119<br>Title: Метод виявлення та протидії вторгненням в корпоративну мережу приватного підприємства<br>Added in a DB: 2025-12-09<br>Authors: Григоренко Вадим Олександрович<br>Heads: Тітова В.Ю.<br>Consultants:<br>Opponents: | Symbols | Lexemes | Symbols | Lexemes |
| | 117774 | 765 | 716 (1%) | 9 (1%) |

Plagiarism sources

| ID | Description | Plagiarism presence in the document | |
|---|---|---|---|
| | | Symbols | Lexemes |

**Протокол аналізу звіту подібності науковим керівником**

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

**Автор:** Григоренко Вадим Олександрович

**Співавтор:**

**Назва:** Метод виявлення та протидії вторгненням в корпоративну мережу приватного підприємства

**Науковий керівник:** Тітова Віра Юріївна

**Підрозділ:** Кафедра кібербезпеки

**Коефіцієнт подібності 1:**1.3%

**Коефіцієнт подібності 2:**0.2%

**Мікропробіли:** 0

**Заміна букв:** 0

**Інтервали:** 0

**Білі знаки:** 0

**Дата створення звіту:** 2025-12-10 21:35:25.0

**Після аналізу Звіту подібності констатую наступне:**

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

*Дата* 11.12.2025р. експерт

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва: Метод виявлення та протидії вторгненням в корпоративну мережу приватного підприємства

Автор: Григоренко Вадим Олександрович

Освітня програма: освітньо-професійна

Рівень вищої освіти магістр

Спеціальність: 125 – Кібербезпека та захист інформації

Науковий керівник: Тітова Віра Юріївна, канд. техн. наук, доцент

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

| № | Висновок | Позначка про відповідність |
|---|---|---|
| 1 | Ознаки академічного плагіату | |
| 1.1 | Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту. | відповідає |
| 1.2 | Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. | |
| 1.3 | Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат. | |
| 1.4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту. | |
| 2 | Інші види порушень академічної доброчесності | |

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,7%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високим рівнем унікальності тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Дата: 10.12.2025

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Гарант освітньої програми _____ Віра ТІТОВА

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Студент Григоренко Вадим Олександрович
Тема: «Метод виявлення та протидії вторгненням в корпоративну мережу приватного підприємства»
Галузь знань 12 «*Інформаційні технології*»
Спеціальність 125 «*Кібербезпека та захист інформації*»
Освітня програма «Кібербезпека та захист інформації»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»:
кількість листів креслень ____; кількість сторінок записки 83;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена аналізу методів виявлення аномалій у мережевому трафіку корпоративної мережі приватного підприємства. У першому розділі досліджено природу сучасних мережевих атак, принципи роботи IDS/IPS-систем та огляд інструментів моніторингу, таких як Snort, Suricata, Zeek та ELK Stack, що дозволило визначити обмеження сигнатурних підходів і потребу в поведінкових моделях. У другому розділі розроблено математичну модель аналізу трафіку як багатовимірного процесу та сформовано алгоритм виявлення аномалій із використанням статистичних методів і машинного навчання. Прийнято рішення застосувати гібридний підхід, що поєднує сигнатурний та поведінковий аналіз. У третьому розділі реалізовано програмний прототип системи збору та обробки трафіку на базі Elasticsearch, Logstash і Kibana. Створене тестове середовище та інструменти генерації атак (Nmap, Metasploit, Scapy) дали змогу експериментально оцінити ефективність обраних методів і підтвердити працездатність побудованої архітектури.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека та захист інформації», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі проведено огляд сучасних мережевих загроз, IDS/IPS-систем та інструментів моніторингу (Snort, Suricata, Zeek, ELK), із використанням останніх наукових підходів, зокрема Zero Trust і поведінкової аналітики. Другий розділ присвячено створенню математичної моделі та алгоритму виявлення аномалій на основі статистичних методів і машинного навчання, що відповідає сучасним тенденціям кібербезпеки. У третьому розділі реалізовано прототип системи на базі ELK та проведено тестування з використанням Metasploit, Nmap і Scapy, що демонструє застосування передових технічних засобів та практичних методик аналізу трафіку.

4. Позитивні сторони кваліфікаційної роботи Кваліфікаційна робота вирізняється комплексністю підходу, поєднанням теоретичного аналізу сучасних методів виявлення аномалій із практичною реалізацією прототипу системи. Використано актуальні інструменти (ELK Stack, Suricata, Zeek) та сучасні методи машинного навчання, що підвищує наукову цінність дослідження. Проведені експерименти в реальному тестовому середовищі підтверджують практичну значущість роботи та її придатність до впровадження у корпоративні мережі.

5. Негативні сторони кваліфікаційної роботи: Робота має незначні недоліки, зумовлені масштабністю тематики. Зокрема, експериментальне середовище побудовано у спрощеній конфігурації, що не повністю відтворює складність великих корпоративних мереж. Утім, ці недоліки не впливають на загальну якість роботи, яка виконана на високому рівні.

6. Оцінка графічного оформлення та пояснювальної записки роботи. оформлення відповідає вимогам

7. Відгук про роботу в цілому Кваліфікаційна робота виконана на високому науково-технічному рівні та демонструє ґрунтовну підготовку автора у сфері кібербезпеки. Робота відзначається логічною структурою, послідовністю викладення матеріалу та вмінням поєднувати теоретичні аспекти з практичною реалізацією. Автор продемонстрував здатність до системного аналізу сучасних методів виявлення аномалій у мережевому трафіку, а також уміння застосовувати сучасні інструменти й технології для побудови ефективної аналітичної системи. Розроблений програмний прототип та проведені експериментальні дослідження свідчать про високий рівень практичних навичок, творчий підхід та вміння вирішувати прикладні задачі кіберзахисту. Робота є актуальною, науково обґрунтованою та має значну практичну цінність, що дозволяє оцінити її як таку, що повністю відповідає вимогам до магістерських досліджень.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «відмінно» (95/A).

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) професор кафедри телекомунікацій, медійних та інтелектуальних технологій, доктор технічних наук, професор Бойко Юлій Миколайович

« 10 » грудня 2025. (підпис)