ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**МЕТОДИ МОНІТОРИНГУ ТА АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ**»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Кирило ГУЗІЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-62
Кирило ГУЗІЙ
Ім'я, ПРІЗВИЩЕ

Керівник: Ганна ГРИНКЕВИЧ
д.т.н., професор *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра Телекомунікаційних систем та мереж
Ступінь вищої освіти магістр
Спеціальність 172 Електронні комунікації та радіотехніка
Освітньо-професійна програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСМ
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шульзі Жанні Олександрівні
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Методи управління усуненням відмов у мультисервісних мережах для підвищення якості обслуговування користувачів
керівник кваліфікаційної роботи Ганна ГРИНКЕВИЧ, д.т.н., доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Теоретичні основи аналізу мережевого трафіку.
2. Огляд існуючих рішень та технологій.
3. Наукова пропозиція та реалізація.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Методи збору та обробки мережевих даних.
2. Методи виявлення аномалій.
3. Переваги та недоліки сучасних підходів.
4. Розробка архітектури системи та її впровадження.

5. Перелік ілюстративного матеріалу: презентація на слайдах

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	03.10.2025	Викон.
2	Розробка першого розділу	10.10.2025	Викон.
3	Розробка другого розділу	17.10.2025	Викон.
4	Розробка третього розділу	24.10.2025	Викон.
5	Висновки, вступ, реферат	10.11.2025	Викон.
6	Розробка презентації	30.11.2025	Викон.

Здобувач вищої освіти _____ Кирило ГУЗІЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ганна ГРИНКЕВИЧ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувачка Гузій К.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Методи моніторингу та аналізу мережевого трафіку для виявлення аномалій у телекомунікаційних системах»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Гузій Кирило Володимирович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявила ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Гузія Кирила Володимиорвича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Ганна ГРИНКЕВИЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Гузій К.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Гузія Кирила Володимировича
(прізвище, ім'я, по батькові)
на тему «Методи моніторингу та аналізу мережевого трафіку для виявлення аномалій у телекомунікаційних системах»

Актуальність. Стрімка цифровізація та розширення інфраструктури сучасних телекомунікаційних систем призводять до експоненціального збільшення обсягів мережевого трафіку та ускладнення його структури. Паралельно із розвитком мережевих технологій спостерігається інтенсивне зростання складних кіберзагроз, таких як розподілені атаки на відмову в обслуговуванні (DDoS), прихована ексфільтрація даних та цілеспрямовані вторгнення (APT-атаки). Традиційні засоби захисту статичного типу вже не забезпечують достатнього рівня безпеки, оскільки не здатні ефективно ідентифікувати загрози «нульового дня» та інтелектуальні аномалії. У цьому контексті дослідження та розробка гібридних методів моніторингу, що поєднують сигнатурний аналіз із статистичними алгоритмами виявлення відхилень у реальному часі, є надзвичайно актуальним завданням. Це дозволяє не лише вчасно локалізувати джерела шкідливого трафіку, а й забезпечити високу доступність сервісів, мінімізувати ризики компрометації мережевих ресурсів та підвищити загальну кіберстійкість сучасних інфокомунікацій..

Позитивні сторони:
1. Я поєднання сигнатурний та статистичний аналіз, що забезпечує високу точність виявлення аномалій у високонавантажених мережах.
2. Я розробив прототип на базі Python, Suricata та ELK Stack, що дозволяє автоматизувати моніторинг та візуалізувати інциденти в реальному часі.

Недоліки :
1. Обмеженість функцій реагування: основна увага приділена моніторингу та виявленню аномалій, тоді як механізми автоматичного блокування загроз (IPS) розглянуті частково.
2. Аналіз обчислювальних витрат: недостатньо оцінено навантаження на ресурси системи при обробці надвеликих масивів даних (Big Data) у режимі реального часу.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувачка Гузій Кирило Володимирович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент
науковий ступінь,
вчене звання _____ (підпис) _____ *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 75 стор., 2 рис., 18 табл., 84 джерела.

Метою роботи є розробка та дослідження системи моніторингу і аналізу мережевого трафіку для виявлення аномалій у телекомунікаційних системах шляхом комбінування сигнатурних та статистичних методів обробки даних..

Об'єктом дослідження є процеси моніторингу та аналізу мережевого трафіку у телекомунікаційних системах..

Предметом дослідження є методи, алгоритми та програмні засоби виявлення аномалій у мережевому трафіку, спрямовані на підвищення рівня кібербезпеки мережі.

Короткий зміст роботи: Досліджено теоретичні основи аналізу трафіку та методи виявлення вторгнень. Розглянуто роботу систем IDS/IPS (Suricata, Snort) та засобів збору даних (NetFlow, DPI). Розроблено архітектуру гібридної системи, що поєднує сигнатурний та статистичний аналіз аномалій. Практичну частину реалізовано мовою Python (бібліотека Scapy) з інтеграцією стеку ELK для візуалізації інцидентів. Експериментально підтверджено ефективність системи у виявленні DoS-атак та сканування мережі. Результати роботи спрямовані на підвищення кіберстійкості сучасних телекомунікаційних мереж.

КЛЮЧОВІ СЛОВА: МЕРЕЖЕВИЙ ТРАФІК, МОНІТОРИНГ, АНОМАЛІЯ, КІБЕРБЕЗПЕКА, IDS/IPS, SURICATA, ПАКЕТ, СИГНАТУРА, СТАТИСТИЧНИЙ АНАЛІЗ, PYTHON, SCAPY, ELK STACK, KIBANA, DOS-АТАКА, СКАНУВАННЯ ПОРТІВ, ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА.

ABSTRACT

Text part of the qualification work for obtaining a master's degree: 75 pages, 2 figures, 18 tables, 84 sources.

The purpose of the work - is to develop and study a system for monitoring and analyzing network traffic to detect anomalies in telecommunication systems by combining signature-based and statistical data processing methods.

Object of research - is the processes of monitoring and analyzing network traffic in telecommunication systems.

Subject of research - is the methods, algorithms, and software tools for detecting anomalies in network traffic, aimed at increasing the level of network cybersecurity.

Summary of the work: The theoretical foundations of traffic analysis and intrusion detection methods are investigated. The operation of IDS/IPS systems (Suricata, Snort) and data collection tools (NetFlow, DPI) is considered. The architecture of a hybrid system that combines signature and statistical anomaly analysis has been developed. The practical part is implemented in Python (Scapy library) with the integration of the ELK stack for incident visualization. The effectiveness of the system in detecting DoS attacks and network scanning has been experimentally confirmed. The results of the work are aimed at increasing the cyber resilience of modern telecommunication networks.

KEYWORDS: NETWORK TRAFFIC, MONITORING, ANOMALY, CYBERSECURITY, IDS/IPS, SURICATA, PACKET, SIGNATURE, STATISTICAL ANALYSIS, PYTHON, SCAPY, ELK STACK, KIBANA, DOS ATTACK, PORT SCANNING, TELECOMMUNICATION SYSTEM.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему: «**МЕТОДИ МОНІТОРИНГУ ТА АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ**»

Виконав: студент 6 курсу, групи ТСДМ-62
спеціальності 172 Телекомунікації і
радіотехніка

студент Гузій Кирило Володимирович

Керівник Гринкевич Ганна Олександрівна

Київ – 2025

ЗМІСТ

ВСТУП **2**
1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ **5**
1.1 Поняття та класифікація мережевого трафіку 5
1.2 Методи збору та обробки мережевих даних 8
1.3 Методи виявлення аномалій 11
Висновки до розділу 1 14
2. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ТА ТЕХНОЛОГІЙ **16**
2.1 Системи виявлення та запобігання атак (IDS/IPS). 16
2.2 Аналіз інструментів: Wireshark, Zeek (Bro), Suricata, Snort 21
2.3 Переваги та недоліки сучасних підходів 24
2.4 Недоліки, що обґрунтовують потребу у нових рішеннях 33
Висновки до розділу 2 35
3. НАУКОВА ПРОПОЗИЦІЯ **37**
3.1 Обґрунтування вибору методів 37
3.2 Розробка архітектури системи 43
3.3 Очікувані результати 46
Висновки до розділу 3 47
4. ПРАКТИЧНА РЕАЛІЗАЦІЯ **49**
4.1 Середовище реалізації 49
4.2 Реалізація прототипу системи 50
4.3 Тестування системи 52
Висновки до розділу 4 61
ВИСНОВКИ **63**
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ **66**
ДОДАТКИ **75**

ВСТУП

Стрімкий розвиток інформаційних технологій та глобальної мережі Інтернет призвів до різкого збільшення обсягів даних, що передаються через телекомунікаційні мережі.

Паралельно з цим зростає кількість кіберзагроз, які здатні завдати шкоди як окремим користувачам, так і цілим організаціям. Поширення шкідливого програмного забезпечення, несанкціонований доступ, мережеві атаки типу DDoS, фішинг та інші методи кіберзлочинності вимагають ефективних систем моніторингу та захисту.

Традиційні засоби, такі як міжмережеві екрани чи антивірусне програмне забезпечення, вже не можуть повністю гарантувати безпеку. Сучасні умови вимагають систем, які здатні аналізувати мережевий трафік у реальному часі, виявляти аномальні відхилення та реагувати на них до того, як вони спричинять серйозні наслідки.

У зв’язку з цим актуальним є розробка систем моніторингу та аналізу трафіку, які базуються на поєднанні класичних методів мережевої безпеки та інноваційних підходів, до обробки

Актуальність теми. Актуальність теми зумовлена необхідністю захисту інформації в умовах зростання складності та інтенсивності кіберзагроз. Використання методів інтелектуального аналізу даних дозволяє підвищити точність виявлення атак і мінімізувати кількість помилкових спрацювань, що робить такі системи особливо цінними для корпоративних і державних структур.

Мета роботи. Метою магістерської роботи є розробка та дослідження системи моніторингу і аналізу мережевого трафіку для виявлення аномалій з використанням сучасних технологій обробки даних.

Завдання дослідження:

1. Проаналізувати теоретичні основи аналізу мережевого трафіку та існуючі методи його моніторингу.

2. Дослідити сучасні системи захисту та виявлення аномалій у мережевому середовищі.

3. Запропонувати власний підхід до побудови системи виявлення аномалій.

4. Реалізувати прототип системи моніторингу та провести тестування на прикладі реальних або змодельованих даних.

5. Оцінити ефективність запропонованої системи та визначити перспективи її подальшого вдосконалення.

Об’єкт дослідження: процеси моніторингу та аналізу мережевого трафіку у телекомунікаційних системах.

Предмет дослідження: методи та алгоритми виявлення аномалій у мережевому трафіку, а також засоби їх практичної реалізації.

1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

1.1. Поняття та класифікація мережевого трафіку

Мережевий трафік розуміють як сукупність даних, що передаються каналами зв’язку між вузлами інформаційно-комунікаційної системи, і його аналіз становить базову передумову забезпечення захищеної роботи цифрової інфраструктури [8, с. 17]. Трафік відображає інтенсивність обміну даними, характер протоколів і типи пакетів, що дає змогу класифікувати його залежно від призначення та функціональної ролі. У структурі сучасних мереж розрізняють користувацький, службовий та шкідливий трафік, які мають різне значення для функціонування системи та її захисту. Коректне розмежування цих видів трафіку дозволяє оптимізувати маршрутизацію, збалансувати навантаження та своєчасно виявляти аномалії [3, с. 7]. У телекомунікаційних системах обсяг і природа трафіку визначають вимоги до пропускної здатності, механізмів пріоритезації та засобів реагування. Значення концепції трафіку постійно зростає, оскільки інтенсивність цифрового обміну збільшується у геометричній прогресії.

Класифікація трафіку базується на його функціональному призначенні, типі протоколів та характеристиках поведінки в мережі, що забезпечує глибше розуміння процесів його формування [46, с. 20]. Користувацький трафік включає обмін інформацією між користувачем та сервісами і характеризується значною варіативністю застосунків. Службовий трафік забезпечує підтримку роботи мережевої інфраструктури та включає сигнальні, керуючі та синхронізаційні пакети. Шкідливий трафік формується унаслідок дій зловмисників і може створювати надмірне або аномальне навантаження, що призводить до порушення доступності ресурсів [9, с. 110]. Багаторівневий аналіз дозволяє виявляти закономірності та відхилення у кожному з цих видів трафіку. У подальшому це сприяє підвищенню загальної ефективності управління інформаційними потоками.

Відповідно до викладеного, структуру класифікації мережевого трафіку подано у таблиці 1.1.

Таблиця 1.1

Класифікація мережевого трафіку

Вид трафіку	Характеристика	Основні ризики
Користувацький	Дані, що передаються між користувачем і сервісами	Перевантаження каналів, ризики перехоплення
Службовий	Пакети, що забезпечують підтримку роботи мережі	Порушення керування, збої маршрутизації
Шкідливий	Дані, сформовані зловмисними діями	DDoS, експлойти, аномальне навантаження

Джерело: сформовано автором на основі [3, с. 6].

У мережах TCP/IP передавання даних базується на модульній архітектурі, що забезпечує поділ функцій між окремими рівнями та уніфікацію способів обміну інформацією [15, с. 41]. Кожен рівень моделі виконує свою роль у забезпеченні надійної маршрутизації, адресації, сегментації та доставки пакетів. Така структурованість дає змогу ефективно керувати потоками даних і забезпечує адаптивність мережі до різного типу навантаження. Важливо, що протоколи TCP та UDP реалізують різні підходи до організації взаємодії, що впливає на швидкість та надійність передачі. TCP забезпечує контроль помилок і встановлення з’єднання, тоді як UDP орієнтований на мінімізацію затримок. Саме це визначає їх застосування в різних типах сервісів.

Під час формування мережевого трафіку у TCP/IP моделях ключову роль відіграють механізми сегментації та інкапсуляції, які забезпечують структуроване передавання даних [27, с. 55]. На транспортному рівні відбувається поділ інформаційних потоків на сегменти, які маркуються службовими заголовками. Далі IP-рівень відповідає за маршрутизацію та адресацію пакетів у розподіленому середовищі. На канальному рівні забезпечується фізична передача кадрів, що включає контроль доступу до середовища. Такий багаторівневий механізм мінімізує втрати і підвищує точність доставки інформації. Він також сприяє швидкому виявленню аномалій у разі спотворення чи підробки заголовків.

Узагальнену характеристику рівнів моделі TCP/IP наведено у таблиці 1.2.

Таблиця 1.2

Особливості функціонування рівнів TCP/IP

Рівень	Основні функції	Значення для аналізу трафіку
Прикладний	Взаємодія сервісів і користувацьких додатків	Джерело більшості користувацького трафіку
Транспортний	Сегментація, контроль доставки	Виявлення втрат і повторних передач
Мережевий	Маршрутизація, адресація	Аналіз маршрутів та аномалій навантаження
Канальний	Кадрування, доступ до середовища	Фіксація помилок на фізичному рівні

Джерело: сформовано автором на основі [15, с. 63].

Аналіз мережевого трафіку у контексті моделі TCP/IP дає можливість визначати джерела затримок, виявляти вузькі місця та прогнозувати поведінку системи під навантаженням [46, с. 22]. Для цього застосовуються комплексні методи спостереження за пакетами, що враховують їхню структуру та маршрут. Протоколи транспортного рівня формують основу для контролю якості передачі, що впливає на загальну продуктивність мережі. Дослідження поведінки трафіку на мережевому рівні дозволяє встановити відповідність реальних маршрутів оптимальним шляхам. Значну увагу приділяють виявленню аномалій, що можуть свідчити про шкідливу активність. У результаті забезпечується підвищення стійкості системи.

У контексті кібербезпеки особливе значення має аналіз шкідливого трафіку, тому що він може порушувати цілісність, доступність та конфіденційність інформації [33]. Для його виявлення використовують методи сигнатурного та поведінкового аналізу, що ґрунтуються на пошуку невідповідностей типовим патернам. Ідентифікація таких аномалій потребує детального дослідження параметрів пакетів та частоти їх появи. Значна частина атак використовує недоліки транспортних і мережевих протоколів. Тому моделювання потоків та класифікація трафіку є ключовими інструментами у протидії загрозам. Це дозволяє оптимізувати засоби захисту та запобігати інцидентам.

Комплексний аналіз трафіку поєднує структурні, статистичні та поведінкові методи, що дозволяє отримати цілісне уявлення про стан мережі [12, с. 111]. Поєднання таблиць класифікації та характеристик TCP/IP рівнів дає змогу сформувати узгоджену модель розуміння інформаційних потоків. Такий підхід дає можливість виявляти як системні недоліки, так і приховану зловмисну активність. Важливо забезпечувати своєчасний моніторинг і фіксацію змін у структурі пакетів. Ці дані стають основою для моделювання ризиків та побудови стратегії кіберзахисту. У результаті зростає загальний рівень кіберстійкості інформаційної системи.

1.2. Методи збору та обробки мережевих даних

Збір та обробка мережевих даних становлять основу моніторингу й оцінювання стану інформаційно-комунікаційних систем, забезпечуючи можливість фіксації аномалій та аналізу поведінки користувачів і службових процесів [46, с. 20]. У мережах різних масштабів застосовують спеціалізовані технології, серед яких NetFlow, sFlow, SNMP та методи повного перехоплення пакетів. Кожен із підходів має власний рівень деталізації, ресурсоємності та точності, що впливає на вибір інструментів у залежності від навантаження й архітектури мережі. Важливо враховувати, що методи збору даних формують первинний інформаційний масив, на якому базуються всі подальші аналітичні процеси [15, с. 41]. Обробка цих даних дозволяє виявляти закономірності, компрометації, несанкціоновану активність або порушення продуктивності. Саме тому ефективність методів збору визначає загальну якість мережевого моніторингу.

NetFlow є одним із найбільш поширених інструментів аналізу потоків, який забезпечує агрегований огляд активності без потреби повного перехоплення кожного пакета [27, с. 55]. На відміну від нього, sFlow поєднує вибіркове захоплення пакетів із телеметрією потоків, що дозволяє

оптимізувати витрати ресурсів у великих мережах. SNMP забезпечує контроль параметрів обладнання, передаючи статистику про стан інтерфейсів і використання ресурсів, що робить його ефективним засобом управління. Packet Capture, або повне перехоплення пакетів, надає максимально деталізовану інформацію про трафік, але потребує значних ресурсів зберігання та обробки [33]. Кожен із цих методів застосовується для різних сценаріїв моніторингу, залежно від того, чи потрібна висока точність, чи оптимальна швидкість. Узагальнену характеристику методів збору трафіку наведено в табл. 1.3.

Таблиця 1.3

Основні методи збору мережевих даних

Метод	Принцип роботи	Переваги	Обмеження
NetFlow	Аналіз потоків без повного захоплення пакетів	Низьке навантаження, структуровані записи	Не фіксує весь вміст пакетів
sFlow	Вибіркове захоплення та статистика потоків	Висока масштабованість	Дані не повні через вибірковість
SNMP	Моніторинг параметрів обладнання	Простота та швидкість	Не аналізує вміст трафіку
Packet Capture	Повне перехоплення пакетів	Максимальна деталізація	Високі ресурси зберігання

Джерело: сформовано автором на основі [15].

Подальша обробка зібраних мережевих даних передбачає застосування статистичних, сигнатурних і поведінкових методів, які дозволяють виявляти кореляції та відхилення [46, с. 22]. Логування є базовим механізмом фіксації подій, що створює журнали діяльності мережевих пристроїв, серверів та прикладних сервісів. Завдяки логам можливо відстежувати часові характеристики, IP-адреси, типи запитів та потенційні інциденти. Статистичний аналіз, у свою чергу, допомагає визначити нормальну поведінку системи та формувати порогові значення [8, с. 18]. Аномалії виявляються через порушення цих норм, що дозволяє оперативно реагувати на загрози. Такий підхід використовується в системах IDS/IPS і комплексних платформах безпеки.

Одним із ключових застосувань логування є аналіз часових закономірностей та пошук послідовностей подій, які свідчать про аномалії або атаки [12, с. 111]. Статистичний аналіз дає змогу оцінити розподіл обсягів трафіку, швидкість передачі, частоту помилок та інші кількісні параметри. Об’єднання цих методів дозволяє формувати багаторівневу картину мережевої активності. Застосування комбінованих підходів підвищує точність і зменшує ймовірність хибнопозитивних результатів. Важливо, що логування зберігає історичний контекст, необхідний для розслідування інцидентів. Порівняльну характеристику методів аналізу наведено в табл. 1.4.

Таблиця 1.4

Методи логування та статистичного аналізу

Метод	Призначення	Переваги	Недоліки
Логування	Фіксація подій і параметрів роботи систем	Історичність, детальність	Великий обсяг даних
Статистичний аналіз	Визначення нормальної поведінки та виявлення аномалій	Аналітичність, швидкість	Залежність від якості вибірки
Комбіновані методи	Поєднання логування і статистики	Підвищена точність	Складність налаштування

Джерело: сформовано автором на основі [46, с. 21].

Методи збору мережевих даних відіграють центральну роль у забезпеченні кіберстійкості організацій, оскільки дозволяють формувати точну картину інформаційних потоків [33]. Актуальність цих методів зростає у зв’язку з поширенням складних атак, які маскують свою активність серед легітимного трафіку. Для виявлення таких загроз використовують аналіз частоти пакетів, співвідношення типів службових і користувацьких даних та часових характеристик. Важливим аспектом є інтеграція різних методів збору в єдину систему моніторингу. Це забезпечує комплексність оцінювання та зменшує ризики пропуску критичних подій. Тому поєднання NetFlow, sFlow, SNMP та Packet Capture стає практикою провідних центрів безпеки.

Застосування логування та статистичного аналізу дозволяє виявляти порушення як на прикладному, так і на транспортному рівні взаємодії [8, с.

19]. Логи формують підґрунтя для аналізу дій користувачів і визначення можливих векторів атак. Статистичний підхід дозволяє виявити неприродні піки активності, надмірну кількість помилок або порушення структурних характеристик трафіку. Такі індикатори часто передують серйозним інцидентам і дають змогу вчасно реагувати на загрози. У поєднанні логування і статистика утворюють фундамент систем безпеки. Це сприяє безперервному контролю мережевої інфраструктури.

Розвиток технік збору та аналізу даних зумовлюється ускладненням архітектур мереж і зростанням обсягів переданої інформації [27, с. 58]. Організації дедалі частіше застосовують автоматизовані платформи, що інтегрують декілька методів і забезпечують кореляцію подій. Системи моніторингу використовують алгоритми машинного навчання для виявлення нетипових патернів. Це значно підвищує швидкість реагування на потенційні атаки. Важливо забезпечити точність первинних даних, адже на них базуються всі наступні аналітичні етапи. Саме тому методи збору й обробки мережевих даних є ключовим елементом сучасної кіберзахисної інфраструктури.

1.3. Методи виявлення аномалій

Виявлення аномалій у мережевому трафіку є критичним елементом забезпечення кібербезпеки, оскільки саме аномальні шаблони поведінки часто свідчать про атаки, спроби вторгнення або несанкціоновані дії [46, с. 22]. Різні методи аналізу дають змогу оцінювати трафік за структурними, поведінковими та статистичними ознаками, формуючи комплексний підхід до ідентифікації загроз. У практиці розрізняють сигнатурний аналіз, евристичні методи та статистичні підходи, кожен із яких має свої переваги та обмеження. Застосування цих методів дозволяє системам безпеки реагувати як на відомі, так і на нові або модифіковані атаки. Вибір методу залежить від архітектури

мережі, вимог до точності та швидкості обробки даних [12, с. 110]. У сукупності вони формують основу сучасних IDS/IPS систем.

Сигнатурний аналіз ґрунтується на порівнянні мережевого трафіку з базою відомих шаблонів атак, які містять характерні ознаки й сигнатури шкідливих дій [8, с. 19]. Такий підхід забезпечує високу точність виявлення вже класифікованих загроз, оскільки визначення базується на чітких критеріях відповідності. Проте його ефективність залежить від актуальності сигнатурних баз, що потребує регулярного оновлення. Сигнатурний аналіз є малоефективним проти нових або модифікованих атак, які не мають відомих патернів. Його застосування виправдане в системах, де необхідно швидко ідентифікувати конкретні форми шкідливої активності. Саме тому сигнатурні методи часто поєднують з іншими видами аналізу.

Евристичні методи спрямовані на виявлення ознак нетипової поведінки на основі логічних правил, експертних моделей та аналізу аномальних параметрів [33]. На відміну від сигнатурного підходу, евристика дозволяє виявляти нові атаки, які ще не мають формалізованого опису. Вона базується на визначенні умов, що відхиляються від стандартної поведінки системи, наприклад надмірної частоти запитів чи порушення послідовності операцій. Евристичні системи можуть генерувати хибнопозитивні спрацьовування через високу чутливість до нетипових подій. Проте їхня гнучкість робить цей підхід актуальним для динамічних мережевих середовищ. Саме тому евристика широко застосовується в комплексних системах аналізу трафіку.

Статистичні методи аналізу аномалій базуються на побудові моделей нормальної поведінки системи та подальшому порівнянні реальних даних із цими моделями [46, с. 23]. Залежно від характеристик мережі визначають середні значення, дисперсії, кореляції та часові патерни, що формують математичну основу аналізу. Відхилення від статистичних норм свідчать про потенційні загрози, що дозволяє вчасно ідентифікувати вторгнення або шкідливу активність. Перевагою цього методу є здатність адаптуватися до змін у поведінці користувачів і службових процесів. Однак якість

статистичних моделей залежить від повноти та достовірності вибірки. Статистичний підхід часто комбінують із машинним навчанням для підвищення точності прогнозування.

Таблиця 1.5

Порівняльна характеристика методів виявлення аномалій

Метод	Переваги	Недоліки	Сфера застосування
Сигнатурний	Висока точність для відомих атак	Неефективність проти нових загроз	IDS, антивірусні системи
Евристичний	Виявляє нові та модифіковані атаки	Можливі хибнопозитивні спрацьовування	Аналіз поведінки, виявлення DDoS
Статистичний	Адаптація до змін трафіку	Високі вимоги до якості вибірки	Моніторинг великих мереж

Джерело: сформовано автором на основі [46, с. 21].

Порівняння наведених методів демонструє, що жоден із них не може забезпечити повну точність виявлення аномалій у складних мережах [12, с. 112]. Сигнатурні підходи є ефективними для відомих атак, але не здатні своєчасно реагувати на нові загрози. Евристика дозволяє виявляти нестандартну поведінку, але потребує ретельного налаштування правил, щоб мінімізувати хибні спрацьовування. Статистичні методи забезпечують глибоке аналізування динаміки трафіку, хоча їх точність залежить від достатнього обсягу якісних даних. У результаті кожен метод вирішує лише частину завдань. Це зумовлює потребу комбінування підходів у сучасних системах кіберзахисту.

Комплексний підхід до виявлення аномалій передбачає інтеграцію сигнатурних, евристичних і статистичних методів у єдину платформу моніторингу [8, с. 18]. Така інтеграція забезпечує баланс між швидкістю реагування, точністю та здатністю виявляти нові форми шкідливості. Комбіновані системи використовують кореляцію подій, аналіз поведінкових патернів і машинне навчання для визначення аномалій у багатовимірних даних. Це допомагає мінімізувати хибнопозитивні результати та покращує виявлення комплексних атак. Важливо враховувати специфіку мережі та

адаптувати моделі під конкретне середовище. Усе це формує основу гнучких і масштабованих систем забезпечення кіберстійкості.

Сучасні тенденції демонструють перехід до автоматизованих систем виявлення аномалій, які здатні аналізувати великі обсяги трафіку в режимі реального часу [27, с. 57]. Використання методів машинного навчання дозволяє формувати динамічні моделі поведінки, які постійно оновлюються відповідно до змін у мережевій інфраструктурі. Такі підходи підвищують ефективність виявлення атак нульового дня та складних багатовекторних загроз. Інтеграція інтелектуальних алгоритмів з традиційними методами забезпечує всебічне покриття різних типів ризиків. Водночас автоматизація скорочує час реагування на інциденти. Це робить сучасні системи аналізу трафіку ключовим інструментом у забезпеченні кіберзахисту.

Висновки до розділу 1

Аналіз теоретичних засад мережевого трафіку дає можливість описати природу інформаційних потоків, визначити їх структуру та встановити залежності між різними типами переданих даних. Матеріал забезпечує розуміння ролі користувацького, службового та шкідливого трафіку у функціонуванні інформаційно-телекомунікаційних систем. Опис особливостей моделі TCP/IP дозволяє визначити механізми маршрутизації, адресації та сегментації, які формують технічну основу передавання даних. Характеристики рівнів моделі демонструють взаємозв’язок між архітектурою мережі та поведінкою трафіку. Дослідження методів збору мережевих даних показує різний рівень деталізації, швидкодії та ресурсоємності інструментів. Такий підхід забезпечує цілісне розуміння ключових чинників, що впливають на якість аналізу трафіку.

Опис методів збору й обробки даних дає змогу оцінити можливості NetFlow, sFlow, SNMP та Packet Capture у фіксації параметрів трафіку та

формуванні первинного інформаційного масиву. Логування та статистичний аналіз дозволяють фіксувати часову, структурну й поведінкову інформацію про роботу мережі, забезпечуючи інструменти для перевірки стабільності та виявлення порушень. Системи аналізу покладаються на кореляцію подій, визначення пікових навантажень та розподіл інтенсивності пакетів, що дає можливість встановити відхилення від звичайних режимів роботи. Такий підхід забезпечує глибшу інтерпретацію мережевої активності. Методи статистичного аналізу доповнюють логування та дозволяють виявляти закономірності розвитку трафіку. У комплексі ці інструменти створюють підґрунтя для подальшого застосування методів виявлення аномалій.

Порівняння сигнатурних, евристичних та статистичних методів показує суттєві відмінності між традиційними та сучасними підходами до виявлення загроз. Сигнатурні методи забезпечують точність для відомих сценаріїв, але не охоплюють нові форми атак. Евристичні алгоритми працюють із поведінковими характеристиками й дозволяють визначати невідомі патерни, хоча й можуть генерувати хибнопозитивні результати. Статистичні моделі забезпечують аналіз динаміки трафіку та адаптацію до змін у мережевому середовищі. Новітні підходи поєднують елементи всіх трьох груп і використовують інтелектуальні алгоритми для покращення точності й швидкості реагування. У результаті сучасні методи демонструють значні переваги над традиційними через адаптивність, масштабованість і здатність виявляти складні загрози.

РОЗДІЛ 2. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ТА ТЕХНОЛОГІЙ

2.1. Системи виявлення та запобігання атак (IDS/IPS).

Для виявлення та запобігання атакам існує потреба у визначенні архітектури мережі та основних її вузлів, у яких може відбуватись збій. З метою забезпечення спостережливості інформації в системах обміну інформацією використовуються спеціальні програми моніторингу. Програмне забезпечення моніторингу – це програмні продукти (модулі), призначені для забезпечення спостережливості систем зв’язку, а також такі, що дозволяють реєструвати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно ідентифікувати ідентифікатори користувачів і процесів, що беруть участь у конкретній події, з метою запобігання порушенням безпеки та/або відповідальності за певну діяльність [**Помилка! Джерело посилання не знайдено.**, с. 101].

Використання програмного забезпечення моніторингу дозволяє власнику (адміністратору безпеки) автоматизованої системи зв’язку:

– виявляти (розшукувати) усі випадки несанкціонованого доступу до конфіденційної інформації з точним визначенням часу та станції мережі, з якої була здійснена спроба;

– локалізувати всі випадки спотворення (знищення) інформації;

– встановити факти несанкціонованого встановлення програмного забезпечення;

– контролювати можливість використання персональних комп’ютерів у неробочий час та визначати мету такого використання;

– виявляти всі випадки несанкціонованого використання модемів у локальній мережі шляхом аналізу фактів запуску несанкціонованих спеціалізованих програм;

– виявити випадки введення спеціальних слів і фраз на клавіатурі чи іншому кодонабірному пристрої, інші випадки спроби несанкціонованої авторизації в системі для доступу до вузлу зв’язку;

– виявити факти неправомірного використання пристроїв зв’язку;

– отримати достовірну інформацію, на основі якої буде розроблена політика інформаційної безпеки компанії;

– контроль доступу до серверів, персональних комп’ютерів, інших пристроїв комунікацій;

– провести інформаційний аудит;

– проводити дослідження виявлених інцидентів;

– проводити дослідження, пов’язані з визначенням точності, ефективності та адекватності реакцій працівників на зовнішні дії;

– визначити завантаженість комунікаційних станцій;

– розробити механізми відновлення критичної інформації після збоїв системи;

– забезпечити спостережливість системи. Саме ця властивість, залежно від якості її виконання, дозволяє певною мірою контролювати дотримання працівниками компанії встановлених правил безпечної роботи на комп’ютерах та політики безпеки. [29, с. 102].

Існують при основні рішення захисту від атак: програмні, апаратні, хмарні.

Програмні рішення – найпопулярніші на ринку, вони представляє собою набір засобів фільтрації трафіку, які складені розробником з використання особистого досвіду. Дане рішення досить простим у використанні, але допоможе тільки від малопомітних атак виду вандалізм.

Апаратні рішення – представляють собою створення розподіленої мережевої структури з великим запасом пропускного трафіку. Використовуються в масштабних мережевих структурах, таких як: точки обміну трафіком, дата-центри, великі регіональні провайдери [**Помилка! Джерело посилання не знайдено.**, с. 230].

Хмарні рішення представлені у вигляді мережевих структур з великою пропускною здатністю, до складу якої вводяться сервери для фільтрації шкідливого трафіку. Таким чином, така мережа поступово буде фільтрувати

шкідливий трафік і знижувати кількість шкідливих пакетів [**Помилка! Джерело посилання не знайдено.**, с. 231].

Серед основних способів (механізмів) забезпечення безпеки інформації на вузлах зв'язку слід виділяти [**Помилка! Джерело посилання не знайдено.**; с. 67]:

1. Збільшення співвідношення сигнал / завада шляхом:

– підвищення енергетики сигналу (велика початкова потужність, регенерація на пунктах посилення як з обслуговуванням, так і без обслуговування тощо), що вимагає значних енергетичних або матеріальних витрат;

– зниження рівня завад (шумів) шляхом використовування спеціальних ліній зв'язку, кабельних ліній зв'язку з низьким рівнем власних шумів, наприклад, оптоволоконних, що також вимагає значних матеріальних витрат;

2. Застосування групових (мажоритарних) методів захисту, які ґрунтуються на використанні декількох каналів зв'язку (3...5), що є фізично (найчастіше, навіть, географічно) рознесеними, якими передається одна й та ж інформація, або на багатократній передачі (3...5 разів) однієї і тієї ж інформації по одному каналу зв'язку. У першому випадку необхідні істотні матеріальні витрати, а в другому значно зменшується пропускна можливість каналу зв'язку (у 3...5 разів). З цих причин, у системах передачі даних швидкісного типу використання цих методів не завжди доцільне.

3. Контролю цілісності інформаційних об'єктів (програмних засобів, інформації при її обробці і передачі), включаючи відновлення зруйнованої інформації, шляхом:

– застосування різного роду завадостійких кодів із виявленням помилок у прийнятій (зчитаній) інформації, які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засобів виявлення спотворень;

– застосування різного роду стійких до загроз коригувальних кодів, які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення й усунення спотворень інформації в системі.

Для забезпечення контролю цілісності інформаційних об’єктів, а також відновлення зруйнованої інформації, до складу інформації, яка захищається, уводять надмірну інформацію – ознаку цілісності або контрольну ознаку (залежно від прийнятої в завданнях контролю цілісності або завадостійкого кодування термінології) − своєрідний образ, відображення цієї інформації процедура формування якого відома, і який з дуже високою імовірністю відповідає інформації, що захищається [**Помилка! Джерело посилання не знайдено.**, с. 104].

Серед численних методів захисту від помилок виділяються три групи методів: групові методи, завадостійке коригувальне кодування і методи захисту від помилок у системах передачі зі зворотним зв’язком.

Системи виявлення та запобігання атак відіграють ключову роль у сучасній кібербезпеці, оскільки забезпечують аналіз трафіку в режимі близькому до реального часу та дозволяють ідентифікувати загрози на ранніх етапах [12, с. 111]. IDS і IPS працюють за принципом відстеження поведінкових або сигнатурних характеристик трафіку з подальшим порівнянням їх із нормами або шаблонами атак. Такі системи забезпечують здатність контролювати інформаційні потоки та своєчасно фіксувати відхилення, що можуть свідчити про шкідливу активність. Важливо, що IDS орієнтується на виявлення інцидентів, тоді як IPS передбачає можливість активного блокування небезпечних дій. Ця функціональна різниця визначає відмінності у сферах застосування кожного типу системи. У сукупності вони створюють багаторівневий бар’єр для протидії зовнішнім і внутрішнім загрозам.

IDS працює як аналітичний інструмент, який спостерігає за мережею та повідомляє про підозрілу активність без втручання у процес передачі даних [46, с. 22]. Такі системи забезпечують глибоку інспекцію пакетів і аналіз їхніх

структурних, часових та поведінкових характеристик. Основою роботи IDS є сигнатурний та евристичний аналіз, що дозволяє визначати як відомі, так і нові форми шкідливості. Завдяки детальній фіксації параметрів IDS надає адміністраторам можливість оцінити природу загрози та визначити необхідні заходи реагування. Системи такого типу використовують у середовищах, де важливо уникнути впливу на потоки даних. Вони формують інформаційну базу для подальшого моделювання атак і вдосконалення політик захисту.

IPS має здатність не лише виявляти загрози, але й запобігати їх виконанню шляхом блокування або перенаправлення шкідливих пакетів [27, с. 55]. Система інтегрується у мережевий трафік і працює як активний фільтр, що контролює проходження пакетів відповідно до визначених політик. Такий підхід дозволяє миттєво реагувати на загрози без необхідності втручання оператора. IPS здатна зупиняти проміжні стадії атак, що значно зменшує ризики проникнення у внутрішню інфраструктуру. Сучасні системи використовують адаптивні алгоритми та функції кореляції подій для підвищення точності. Це робить IPS важливим компонентом комплексного середовища захисту.

Впровадження IDS та IPS потребує врахування особливостей архітектури мережі та типів інформаційних потоків [15, с. 62]. Різні сегменти інфраструктури можуть вимагати різного рівня контролю, що визначає місце встановлення датчиків та політику реагування. Значний вплив мають параметри навантаження, швидкість передачі даних та характер застосунків, оскільки ці фактори визначають вимоги до продуктивності системи. Важливу роль відіграє коректне налаштування правил аналізу, оскільки помилки можуть спричинити як пропуск загроз, так і надмірну кількість хибних сповіщень. Інтеграція систем у вже існуюче середовище вимагає адаптації мережевих політик. Це забезпечує узгодженість роботи з іншими компонентами кіберзахисту.

Сучасні IDS та IPS підтримують можливості машинного навчання, що дозволяє будувати поведінкові моделі користувачів і сервісів [33]. Завдяки

цьому системи здатні виявляти складні та багаторівневі атаки, які не піддаються класичному сигнатурному аналізу. Моделі машинного навчання аналізують часові ряди, структурні ознаки й частотні характеристики трафіку, формуючи адаптивний механізм класифікації. Використання таких підходів підвищує точність та зменшує кількість хибнопозитивних спрацювань. Інтелектуальні IDS та IPS інтегруються з платформами логування, що створює можливість централізованого контролю. Це формує середовище адаптивного реагування на загрози.

Інтеграція IDS та IPS у комплексну систему кіберзахисту забезпечує можливість формування багаторівневої моделі захисту, яка поєднує аналіз трафіку, кореляцію подій та автоматизоване реагування [8, с. 17]. У таких системах важливе місце займає взаємодія між різними джерелами даних, зокрема логами, телеметрією та показниками продуктивності. Це дозволяє зміцнити спроможність інфраструктури протистояти атакам і забезпечити високу стабільність роботи сервісів. В умовах зростання масштабів мереж особливу увагу приділяють оптимізації продуктивності IDS та IPS. Системи повинні обробляти великі обсяги даних без втрати швидкодії та точності аналізу. Такий підхід створює передумови для розвитку більш інтелектуальних та адаптивних засобів кіберзахисту.

2.2. Аналіз інструментів: Wireshark, Zeek (Bro), Suricata, Snort

Wireshark, Zeek, Suricata та Snort належать до найпоширеніших інструментів для аналізу мережевого трафіку та виявлення загроз, оскільки забезпечують широкий спектр методів обробки даних [46, с. 25]. Кожен із цих засобів реалізує унікальний підхід до аналізу, що визначає відмінності у функціональних можливостях, точності та продуктивності. Wireshark орієнтується на детальний розбір пакетів і дає змогу досліджувати структуру кожного протоколу. Zeek працює як мережевий аналізатор подій, формуючи

журнали високорівневої активності. Suricata та Snort реалізують функції IDS та IPS, що робить їх ключовими у контексті виявлення атак. Сукупність цих інструментів утворює гнучке середовище контролю мережевих потоків.

Wireshark забезпечує постійний моніторинг трафіку з можливістю фільтрації, сегментації та декодування протоколів [48]. Такий підхід дозволяє оператору визначати взаємозв'язки між пакетами, аналізувати часові параметри та виявляти аномальні патерни. Засіб широко використовують для діагностики мережевих проблем, тестування конфігурацій і навчальних цілей. Завдяки глибокому рівню деталізації Wireshark демонструє особливу ефективність у середовищах, де потрібний точковий аналіз. Інструмент підтримує розширену систему фільтрів, що підвищує точність дослідження. Таке поєднання можливостей робить його незамінним у завданнях ручної та автоматизованої діагностики.

Zeek працює як система високорівневої інтерпретації подій, яка перетворює сировинний трафік на структуровані журнали активності [27, с. 57]. На відміну від інструментів пакетного аналізу, Zeek фокусується на поведінкових ознаках і логічних взаємозв'язках між діями в мережі. У ньому реалізовано механізм сценаріїв, що дозволяє розширювати функціональність і створювати спеціалізовані правила аналізу. Така архітектура робить Zeek ефективним у дослідженнях аномалій та інцидентів тривалого характеру. Інструмент часто поєднують з іншими системами моніторингу для формування комплексної картини подій. Завдяки гнучкому формату логів Zeek широко використовують у великих організаціях.

Таблиця 2.1

Порівняльна характеристика інструментів аналізу мережевого трафіку

Інструмент	Основний підхід	Рівень аналізу	Підтримка IDS/IPS	Сильні сторони	Обмеження
Wireshark	Розбір пакетів	Низькорівневий	Ні	Глибока деталізація даних	Менш ефективний на

Інструмент	Основний підхід	Рівень аналізу	Підтримка IDS/IPS	Сильні сторони	Обмеження
					великих обсягах
Zeek	Поведінкове логування	Високий	Ні	Аналітика подій і скриптовість	Вимагає складнішої конфігурації

Продовження таблиці 2.1

Suricata	Сигнатурний та поведінковий аналіз	Середній	Так	Висока продуктивність і багатопотоковість	Потребує оптимізації ресурсів
Snort	Сигнатурний аналіз	Середній	Так	Точність при відомих атаках	Нижча ефективність для нових загроз

Джерело: сформовано на основі [46; 27; 48].

Suricata реалізує багатопотокову архітектуру, що забезпечує високу продуктивність під час обробки великих потоків трафіку [33]. Система підтримує сигнатурний, поведінковий та гібридний підходи, що дає змогу ефективно реагувати на широкий спектр загроз. Розширені можливості DPI дозволяють детально аналізувати вміст пакетів та виявляти приховані елементи шкідливого коду. Suricata інтегрується зі сторонніми джерелами даних і системами кореляції, що посилює її аналітичний потенціал. Гнучкість конфігурацій дозволяє адаптувати інструмент до різних сценаріїв. Це робить його універсальним засобом для мереж з високим рівнем навантаження.

Snort відомий як один із найстаріших та найбільш стабільних інструментів для виявлення атак у мережевому середовищі [3, с. 8]. Він реалізує сигнатурний підхід, що забезпечує високу точність під час розпізнавання відомих атак. Гнучка система правил дозволяє створювати власні шаблони виявлення подій і адаптувати систему під конкретні загрози. Snort часто використовують у поєднанні з журнальними та аналітичними платформами, що підсилює його практичну цінність. Попри значний вік

інструмента, його функціональність постійно оновлюється. Це забезпечує високий рівень актуальності у кіберзахисних системах.

Порівняння Wireshark, Zeek, Suricata та Snort демонструє суттєві відмінності у підходах до аналізу трафіку, структурі даних та способах реагування на загрози [12, с. 113]. Вибір інструмента залежить від вимог до деталізації, продуктивності та характеру мережевого середовища. У ситуаціях, коли потрібний глибокий аналіз пакетів, доречні можливості Wireshark. Якщо необхідне поведінкове моделювання, ефективним стає застосування Zeek. Для завдань IDS та IPS найкраще підходять Suricata та Snort. Разом ці інструменти створюють багатофункціональний комплекс для повноцінного аналізу трафіку та виявлення загроз.

2.3. Переваги та недоліки сучасних підходів

Сучасні підходи до аналізу та захисту мережевого трафіку спираються на комплексні методи виявлення аномалій, прогнозування ризиків і динамічної адаптації до нових загроз. Удосконалення алгоритмів машинного навчання розширює можливості систем моніторингу та знижує залежність від сигнатурних правил. Адаптивні моделі дозволяють оперативно реагувати на зміну інтенсивності, структури та поведінкових характеристик трафіку. У поєднанні зі статистичними методами сучасні підходи забезпечують точніше розмежування між нормальними та шкідливими потоками. Технології глибокого аналізу даних створюють підґрунтя для підвищення надійності прогнозування мережевих подій. Таким чином, сучасні рішення демонструють здатність ефективно працювати в умовах постійного ускладнення цифрових загроз. Порівняльні характеристики основних переваг сучасних підходів наведено в табл. 2.2.

Таблиця 2.2

Переваги сучасних підходів до аналізу та захисту мережевого трафіку

Підхід	Основна перевага	Рівень ефективності	Динамічність	Адаптивність	Масштабованість
Статистичні моделі	Виявлення відхилень у динаміці	Високий	Середня	Висока	Висока
Машинне навчання	Ідентифікація складних патернів	Високий	Висока	Висока	Висока
Поведінковий аналіз	Фіксація аномалій без сигнатур	Середній	Висока	Середня	Середня
Гібридні методи	Комбінування різних технік	Дуже високий	Висока	Висока	Висока

Джерело: сформовано автором.

Переваги сучасних підходів передусім проявляються у здатності працювати з великими обсягами даних і зберігати стабільність аналізу за умов високої інтенсивності трафіку. У системах, де зміни відбуваються динамічно, особливо важливо забезпечити адаптивність алгоритмів та їхню здатність до самонавчання. Сучасні методи дозволяють скорочувати час реагування на інциденти й підвищувати точність прогнозування. Поєднання статистичного аналізу та машинного навчання забезпечує комплексний підхід до класифікації подій. Висока деталізація аналізу дає змогу виявляти нетипову поведінку навіть у фонових потоках. Такі переваги формують основу для подальшого вдосконалення механізмів кіберзахисту.

Попри значні переваги, сучасні підходи мають низку недоліків, що впливають на їх використання в реальних системах. Висока ресурсомісткість складних моделей може створювати додаткове навантаження на обладнання. Деякі алгоритми машинного навчання потребують великих підготовлених даних, що ускладнює їх впровадження. Наявність великої кількості хибнопозитивних результатів зберігається навіть у сучасних системах аналізу. Труднощі інтеграції з існуючими архітектурами також залишаються поширеною проблемою. Таким чином, недоліки вимагають подальшого

вдосконалення інструментів і методів. Основні недоліки сучасних підходів представлено в табл. 2.3.

Таблиця 2.3

Недоліки сучасних підходів до аналізу та захисту мережевого трафіку

Підхід	Основний недолік	Ресурсні витрати	Рівень складності	Залежність від даних	Ризик хибнопозитивів
Статистичні методи	Чутливість до коливань середовища	Низькі	Середній	Висока	Середній
Машинне навчання	Велика потреба у даних	Високі	Високий	Дуже висока	Середній
Поведінковий аналіз	Генерація хибнопозитивних подій	Середні	Середній	Низька	Високий
Гібридні системи	Складність конфігурації	Високі	Дуже високий	Середня	Середній

Джерело: сформовано автором.

Недоліки сучасних підходів часто пов’язані з високою складністю їх розгортання та підтримки. Навіть за наявності автоматизації більшість моделей вимагає періодичного оновлення параметрів і коригування правил. Масштабовані системи створюють додаткові вимоги до пропускної здатності мережевої інфраструктури. У деяких випадках час обробки великих обсягів даних може уповільнювати реакцію на загрози. Залучення фахівців для налаштування моделей підвищує операційні витрати. Такі чинники формують обмеження для повсюдного використання найсучасніших рішень.

Оглянемо найбільш розповсюджені програмні пакети тестування вразливостей.

ManageEngine

Програмне забезпечення віртуальної машини ManageEngine надає користувачам можливість доступу до важливої інформації за допомогою можливостей оцінки вразливостей. Він дозволяє виявляти вразливості в різних пристроях, операційних системах Windows і вибраних програмах сторонніх розробників. Крім того, він надає користувачам негайну оцінку віку та серйозності виявлених вразливостей. Примітно, що ManageEngine Vulnerability Manager Plus відрізняється від традиційних підходів, керованих

базами даних, використовуючи стратегію виявлення аномалій для вирішення проблем безпеки.

Інструмент пропонує різноманітні функції, такі як допомога в підтримці актуального антивірусного програмного забезпечення, виявлення потенційно шкідливого програмного забезпечення, виявлення підозрілих портів і вирішення проблем конфігурації.

Платформа ManageEngine включає в себе різні інструменти управління, такі як розгортання конфігурації та керування виправленнями, і дозволяє виявляти та усувати вразливості нульового дня за допомогою вже існуючих сценаріїв. Незважаючи на те, що загалом програмне забезпечення зручне для користувача, воно може виявитися надто складним для менших параметрів. Він доступний для використання на максимум 25 комп'ютерах безкоштовно.

Paessler PRTG

Цей програмний інструмент пропонує комплексний моніторинг інфраструктури, дозволяючи адміністраторам аналізувати різні компоненти, такі як мережа, програми та сервери. Крім того, платформа має можливість виявляти та сповіщати користувачів про будь-які значні зміни в стані пристрою, оскільки незвичайна активність може свідчити про потенційне вторгнення. Також, він може використовувати методи аналізу пакетів для перевірки даних перехоплення SNMP і активності порту.

Важливо зазначити, що PRTG є виключно інструментом моніторингу і не надає автоматизованого керування чи допомоги в авторизації. Для користувачів, яким потрібен моніторинг 100 датчиків або менше, інструмент доступний безкоштовно. Крім того, пропонується 30-денна безкоштовна пробна версія, що дозволяє користувачам досліджувати всі функції інструменту без будь-яких обмежень щодо кількості датчиків.

Сканер мережевої безпеки BeyondTrust Retina

Програмне забезпечення Beyondtrust Retina має можливість проводити комплексне сканування різних компонентів у мережі, включаючи веб-сервіси, контейнери, бази даних, віртуальні середовища та пристрої IoT. Однією з

примітних особливостей цього інструменту є його властива сумісність і можливості аудиту для пристроїв Інтернету речей, які можуть бути відсутні в альтернативних інструментах сканування. Таким чином, він є вигідним варіантом для людей, які хочуть контролювати кілька пристроїв. Крім того, він спеціально розроблений для виконання процедур сканування, не спричиняючи жодних збоїв у доступності чи продуктивності системи. На відміну від використання лише виявлення аномалій, ця програма проводить оцінку загроз, порівнюючи їх із базою даних уразливостей. Важливо зазначити, що Retina в першу чергу зосереджена на функціях моніторингу, а не на комплексному рішенні для керування безпекою.

Rapid7 Nexpose

Nexpose — це цінний інструмент для керування локальними вразливими місцями, який служить надійною відправною точкою для сканування безпеки. Його підхід до оцінки ризику вирізняє його, використовуючи оцінку ризику в діапазоні від 1 до 1000 замість традиційної шкали «Високий-Середній-Низький» або 1-10. Цей комплексний рейтинг враховує такі фактори, як вік уразливості та використання в межах набору експлойтів. Думки про Nexpose різні: одні користувачі цінують його функціональність, а інші вважають його зайвим. Крім того, Nexpose пропонує покрокові інструкції для порівняння користувальницьких систем із загальноприйнятими стандартами політики, що сприяє дотриманню вимог. Хоча він може не охоплювати всі необхідні функції для комплексної стратегії управління, його відкритий API дозволяє інтегрувати його дані з іншими інструментами.

Tripwire IP360

Tripwire IP360 — це комплексне та складне програмне забезпечення, розроблене для корпоративного використання, зокрема для проведення сканування вразливостей в Інтернет-мережах. Він має можливість сканувати широкий спектр пристроїв і програм у мережах, у тому числі ті, що існують у локальних, хмарних і контейнерних середовищах. Крім того, він оснащений здатністю виявляти раніше не ідентифікованих агентів. Цей інструмент

забезпечує цінність, автоматизуючи процес усунення вразливості для адміністраторів, оскільки він включає систему рейтингу на основі таких факторів, як вплив, вік і легкість усунення. Крім того, подібно до Nexpose, IP360 надає відкритий API, який полегшує інтеграцію з іншими рішеннями для керування. Загалом, IP360 служить стандартним сканером уразливостей.

ImmuniWeb

ImmuniWeb — це технологічно просунута платформа, яка використовує штучний інтелект для надання ряду інструментів сканування вразливостей, включаючи Immuniweb Continuous для тестування на проникнення та ImmuniWeb Discovery для оцінки порушень. Використовуючи машинне навчання, ImmuniWeb здатний ефективно виявляти ризики безпеки з мінімальною кількістю помилкових спрацьовувань. Незважаючи на те, що ImmuniWeb недорогий і розроблений для певних організацій, він може стати ефективним рішенням для окремих команд DevOps.

Netsparker

Netsparker надає унікальну технологію сканування, яка підтверджується емпіричними даними, ефективно вирішуючи проблему помилкових спрацьовувань. Ця функція виявляється особливо вигідною при розширенні сфери оцінки вразливості. Крім того, Netsparker спеціально розроблено для бездоганної інтеграції з іншими системами керування, сприяючи автоматизації процесу виявлення вразливостей. Цей інструмент оцінки веб-вразливості призначений виключно для підвищення ефективності та точності. Його клієнтура включає такі відомі організації, як Міністерство внутрішньої безпеки США.

Acunetix

Acunetix — це сканер безпеки веб-сайтів, який відрізняється від мережевих сканерів. Він пишається своєю здатністю виявляти понад 4500 вразливостей у різних типах додатків, включаючи споживчі, комерційні та з відкритим кодом, зберігаючи низький рівень помилкових спрацьовувань. Крім того, він забезпечує видимість рядків коду та надає докладні звіти,

полегшуючи ідентифікацію та вирішення проблем безпеки. Крім того, Acunetix надає користувачам можливість налаштувати свій робочий процес за допомогою естетично привабливого візуального інтерфейсу. Для команд керування веб-сайтами цей універсальний інструмент може виявитися неоціненним.

Wireshark

Wireshark, широко визнаний аналізатор мережевих протоколів з відкритим кодом, допомагає проводити сканування вразливостей. Цей безкоштовний інструмент використовує аналіз пакетів для інтерпретації мережевої активності, допомагаючи адміністраторам розробити відповідні заходи безпеки. Виявляючи підозрілий трафік, Wireshark може відрізнити зловмисні атаки від системних помилок, класифікувати тип атаки та встановити захисні протоколи. Незважаючи на свої надійні можливості, Wireshark, як і інше програмне забезпечення з відкритим кодом, може потребувати ретельного налаштування та керування, щоб ефективно задовольняти вимоги користувачів.

Nmap

Nmap — широко використовуваний мережевими адміністраторами інструмент із відкритим вихідним кодом для керування вразливістю вручну. Цей безкоштовний сканер уразливостей працює, надсилаючи пакети та аналізуючи відповіді, щоб ідентифікувати хости та служби в мережі. Це охоплює такі завдання, як виявлення хостів за допомогою запитів TCP/ICMP, сканування портів, визначення версій і визначення ОС. Крім того, для адміністраторів, які вміють працювати зі сценаріями, Nmap також може полегшити додаткове виявлення вразливостей. Важливо відзначити, що Nmap насамперед призначений для досвідчених користувачів, які добре володіють операціями командного рядка, яким бракує зручного інтерфейсу для легкого виконання сканування або інтерпретації результатів. Отже, хоча цей інструмент може підійти певним професіоналам, більшості адміністраторів потрібен більш спрощений підхід до сканування вразливостей.

OpenVAS

Open Vulnerability Assessment System (OpenVAS) — це програмна основа, яка охоплює кілька служб для керування вразливими місцями. Це інструмент, який доступний безкоштовно та підтримується Greenbone Networks, починаючи з 2009 року. Діючи як комплексний сканер, він використовує понад 50 000 тестів уразливості безпеки, які оновлюються щодня. Цей сканер уразливостей розроблено в основному для роботи в середовищі Linux і є особливо корисним для досвідчених користувачів, які прагнуть проводити цілеспрямоване сканування або тестування. Проте слід зазначити, що інсталяція та використання цього інструменту потребує значного навчання, що робить його менш придатним для більшості мережевих адміністраторів. Крім того, Greenbone пропонує платну версію продукту, яка включає більш часті оновлення, гарантії обслуговування та підтримку клієнтів.

Видання спільноти Qualys

Інструмент Qualys FreeScan було замінено на безкоштовний хмарний сервіс, відомий як Community Edition. Це видання пропонує спрощену версію хмарної платформи Qualys, спеціально розроблену для невеликих організацій. Він дозволяє необмежено сканувати до 16 внутрішніх ресурсів, трьох зовнішніх ресурсів і одну URL-адресу. Незважаючи на свої обмеження, він зберігає багато основних функцій повного інструменту, використовуючи дані з понад трьох мільярдів сканувань уразливостей, які проводяться щорічно. Примітно, що Qualys Community Edition пропонує додаткову перевагу функції пошуку в результатах сканування та можливість генерувати настроювані звіти. Крім того, його інтерфейс користувача є естетично привабливим і зручним.

Burp Suite Community Edition

Burp Suite — це надійний інструмент, який використовується для тестування вразливостей веб-додатків для забезпечення високого рівня безпеки. Це комплексний пакет програмного забезпечення, який містить ряд

інструментів, спеціально розроблених для виявлення та використання різних типів уразливостей. Burp Suite дозволяє перевіряти безпеку веб-додатків, перехоплювати та аналізувати трафік клієнт-сервер, виявляти вразливості, як-от впровадження SQL, атаки XSS і атаки CSRF, а також полегшує тестування на проникнення. Інструмент підтримує як ручне, так і автоматичне тестування, таким чином підвищуючи ефективність виявлення вразливостей. Крім того, Burp Suite дозволяє налаштовувати налаштовані сценарії для автоматизації процесу тестування та виявлення вразливостей. Зважаючи на його можливості, Burp Suite є важливим інструментом для команд розробників і тестувальників, які беруть участь у створенні та оцінці веб-додатків. Використання цього інструменту допомагає забезпечити високий рівень безпеки веб-додатків і зменшити ризики вразливості.

Отже, більшість доступних пакетів програмного забезпечення або пропонують обмежені функції, або мають високу вартість, що робить їх недоступними для деяких компаній. Тому, існує необхідність у створенні власного інструменту тестування вразливостей системи.

У практичному застосуванні важливе значення має баланс між точністю аналізу та доступним рівнем продуктивності. У середовищах із високим навантаженням необхідно оптимізувати алгоритми, щоб уникнути деградації якості аналізу трафіку. Навчання моделей потребує ретельного відбору даних, оскільки випадкові шуми можуть суттєво впливати на результати. Навіть незначні похибки класифікації створюють ризик пропуску атак або помилкового блокування легітимного трафіку. Підвищені вимоги до конфігурації системи можуть ускладнювати експлуатацію. Це підкреслює важливість раціонального вибору підходу для конкретних умов.

Порівняння переваг і недоліків сучасних підходів демонструє, що найбільш ефективні рішення виникають у результаті комбінування різних методів. Поєднання сигнатурного аналізу, статистичних моделей і інтелектуальних алгоритмів формує стійкі системи захисту. Гібридні підходи забезпечують ширший спектр можливостей та зменшують залежність від

одного методу. Водночас такі системи потребують високого рівня технічної компетентності та значних обчислювальних ресурсів. Розвиток алгоритмів адаптивного навчання частково пом’якшує ці обмеження. Загалом сучасні підходи створюють умови для підвищення якості аналізу трафіку та ефективності реагування на нові загрози.

2.4. Недоліки, що обґрунтовують потребу у нових рішеннях

Сучасні системи аналізу та захисту мережевого трафіку демонструють високу ефективність у стандартних сценаріях, але часто не забезпечують достатньої гнучкості в умовах швидкої еволюції загроз. Вузька спеціалізація окремих методів призводить до того, що вони втрачають результативність при появі нових типів атак або складно структурованих аномалій. Значну роль відіграє обмежена здатність класичних моделей адаптуватися до нетипових ситуацій та відсутність повноцінних механізмів самооновлення. Водночас зростає складність шкідливих алгоритмів, що активно використовують маскування під нормальний трафік. За таких умов традиційні засоби виявлення не завжди розпізнають приховані патерни поведінки. Ці фактори створюють потребу у розробленні більш адаптивних рішень. Нові підходи мають забезпечувати кращу стійкість до невизначених сценаріїв і підвищену здатність до прогнозування ризиків.

Ще однією значною проблемою стає ресурсомісткість сучасних методів, яка обмежує їх застосування у великих або швидкісних мережах. Алгоритми машинного навчання здатні досягати високої точності, проте потребують масштабних обчислень та значного обсягу оперативної пам’яті. За умов стрімкого зростання трафіку це спричиняє затримки у реагуванні та збільшує ризик пропуску критичних подій. Багато систем не оптимізовані для роботи в реальному часі, що створює додаткові труднощі в мережах із високою пропускною здатністю. Розширення моделей часто потребує модернізації

інфраструктури, що підвищує фінансові витрати. Це спонукає до пошуку більш легких, але не менш точних методів обробки. Нове покоління рішень має поєднувати оптимальне використання ресурсів із високою швидкодією аналізу.

Важливою групою недоліків є обмежені можливості інтерпретації результатів складних моделей. Значна частина сучасних алгоритмів працює як непрозорі структури, що ускладнює пояснення логіки прийняття рішення. Така ситуація створює ризик помилкової класифікації подій, яку важко виявити без детального аналізу внутрішніх процесів алгоритму. Низька пояснюваність також ускладнює аудит кіберзахисних систем та їх інтеграцію у критичну інфраструктуру. Оператори часто не розуміють, чому система віднесла певну активність до шкідливої, що унеможливлює адаптацію правил. Зростання складності мереж лише посилює цю проблему. Тому актуальним стає розроблення рішень із високим рівнем прозорості та контрольованістю логіки аналізу.

Традиційні та сучасні методи однаково стикаються з проблемою хибнопозитивних і хибнонегативних результатів, що знижує рівень довіри до систем моніторингу. Навіть потужні моделі інколи неправильно класифікують легітимні дії як шкідливі або не виявляють добре прихованих атак. Велика кількість хибнопозитивів збільшує навантаження на персонал і створює додаткові витрати часу на перевірку інцидентів. Навпаки, хибнонегативи формують ризик невиявлених порушень, які можуть призвести до серйозних збитків. Проблема ускладнюється тим, що обидва види помилок можуть змінюватися залежно від контексту мережевого середовища. Це вимагає створення адаптивних засобів, здатних динамічно коригувати межі виявлення та мінімізувати рівень помилкової класифікації. Таким чином, удосконалення точності стає одним із ключових напрямів подальших досліджень.

Складність інтеграції сучасних підходів у реальні мережеві інфраструктури також створює значні обмеження. Багато систем вимагають спеціальних умов розгортання або високого рівня технічної компетентності

під час конфігурації. Виникають труднощі з узгодженням нових рішень зі старими протоколами чи обладнанням. У деяких випадках інтеграція призводить до зниження продуктивності або появи нових вразливостей. Підтримка складних моделей потребує регулярного оновлення та перевірки сумісності, що збільшує експлуатаційні витрати. Такі обмеження підкреслюють потребу у створенні гнучких, сумісних та легко масштабованих інструментів. Нові рішення мають не лише підвищувати ефективність виявлення загроз, а й забезпечувати простоту впровадження у різних мережевих середовищах.

Висновки до розділу 2

Аналіз сучасних систем виявлення та обробки мережевого трафіку показує, що наявні рішення не завжди забезпечують достатній рівень точності в умовах динамічного розвитку кіберзагроз. Значна кількість помилкових спрацювань ускладнює оцінювання подій та створює ризики пропуску критично важливих атак. Висока залежність від сигнатур та попередньо визначених правил обмежує універсальність традиційних рішень. Ресурсомісткість моделей збільшує час обробки трафіку, що негативно впливає на ефективність застосування у великих мережах. У середовищах із високими навантаженнями такі системи не завжди підтримують стабільність роботи. Сукупність цих чинників формує підстави для удосконалення існуючих підходів.

Проблеми масштабованості залишаються одним із ключових бар’єрів у впровадженні сучасних методів аналізу трафіку. Розширення мережевої інфраструктури вимагає від системи здатності підтримувати більші обсяги даних без деградації продуктивності. Проте багато моделей демонструють зниження швидкодії або збільшення кількості помилкових класифікацій при зростанні навантаження. Високі витрати обчислювальних ресурсів обмежують

використання складних алгоритмів у реальних умовах. Для забезпечення стабільної роботи необхідно оптимізувати механізми збору, фільтрації та аналізу даних. Такі обставини створюють потребу у розвитку більш масштабованих та продуктивних рішень.

Важливим чинником обмежень стає значний обсяг людського й професійного залучення, необхідний для аналізу, налаштування та супроводу існуючих систем. Багато методів потребують високої кваліфікації фахівців, оскільки конфігурація правил, оптимізація моделей і перевірка результатів є трудомісткими процесами. Надмірна кількість сповіщень збільшує навантаження на персонал і уповільнює реагування на інциденти. Залежність від ручної інтерпретації даних створює ризик помилок і знижує ефективність системи в складних мережевих умовах. Підвищення рівня автоматизації та зменшення потреби у людському втручанні стає одним із ключових напрямів розвитку. Усе це підтверджує необхідність наукового удосконалення сучасних підходів до аналізу й захисту мережевого трафіку.

РОЗДІЛ 3. НАУКОВА ПРОПОЗИЦІЯ

3.1. Обґрунтування вибору методів

Аналіз мережевого трафіку потребує методології, яка забезпечує збалансоване поєднання точності, швидкодії та помірного використання ресурсів. Використання одного підходу не гарантує всебічного охоплення всіх типів загроз, оскільки різні моделі орієнтуються на різні поведінкові або структурні параметри трафіку. Комбінація сигнатурних, статистичних та фільтраційних методів створює багаторівневу систему контролю, що підвищує надійність аналізу. Такий підхід дозволяє забезпечити виявлення як відомих, так і нетипових аномалій, оскільки кожен метод компенсує обмеження іншого. Застосування декількох принципів підвищує стійкість мережевої інфраструктури до цілеспрямованих атак. Така структура методології обґрунтовує вибір комбінованої моделі аналізу.

Сигнатурний метод залишається важливим елементом мережевої безпеки, оскільки забезпечує високу точність у виявленні загроз відомих типів. Бази сигнатур містять докладні описи атак, що дозволяє системі оперативно ідентифікувати заздалегідь вивчені сценарії з мінімальною кількістю хибнопозитивних подій. Ефективність цього методу зростає за умови регулярного оновлення баз знань. Сигнатурний аналіз демонструє високу швидкість обробки даних, що робить його придатним для роботи в режимі реального часу. Такий підхід забезпечує стабільність функціонування системи навіть у мережах із підвищеним навантаженням. Водночас сигнатурний метод потребує доповнення іншими техніками, оскільки він не охоплює нові або модифіковані атаки.

Статистичний метод забезпечує можливість виявляти нетипові зміни в інтенсивності, обсязі або структурі трафіку, що дає змогу фіксувати аномальні події до появи чітких ознак атаки. Його ефективність базується на аналізі часових рядів, середніх значень, коливань та відхилень від встановлених норм. Такий підхід дозволяє оперативно визначати підозрілі тенденції, які не можна

виявити за допомогою сигнатур. Статистичні моделі застосовують у середовищах, де важливо виявити приховану активність або повільні розподілені атаки. Завдяки гнучкості порогових значень оператори можуть адаптувати алгоритм до конкретного мережевого профілю. Це робить статистичний метод необхідною складовою комплексного аналізу.

Застосування правил і фільтрів відіграє важливу роль у забезпеченні первинного рівня захисту, оскільки дає змогу блокувати небажані або потенційно небезпечні з'єднання ще до глибокого аналізу. Фільтри ґрунтуються на відомих параметрах, таких як IP-адреси, порти, протоколи або характерні ознаки трафіку. Такий підхід дозволяє зменшити загальне навантаження на систему шляхом відсівання підозрілих потоків на ранньому етапі. Правила застосовують також для формування політик доступу та контролю взаємодії мережевих вузлів. Гнучкість конфігурації дозволяє адаптувати набір фільтрів до конкретної мережевої архітектури. Це робить їх ефективним доповненням до сигнатурних і статистичних методів.

Комбінація трьох описаних підходів створює оптимальний інструментарій для аналізу різнорідних подій у мережевому середовищі. Сигнатурний метод забезпечує точність у виявленні відомих атак, статистичний — адаптивність і здатність фіксувати невідомі аномалії, а правила й фільтри — ефективну первинну фільтрацію. У взаємодії ці підходи підсилюють один одного та знижують ризик пропуску критичних інцидентів. Такий підхід дозволяє уникати надмірної ресурсомісткості, оскільки складні алгоритми застосовують лише до відібраного трафіку. Практичний досвід використання комбінованих моделей свідчить про підвищення загальної ефективності моніторингу. Це обґрунтовує вибір саме такої методології для подальшого аналізу.

Усі заходи можна поділити на пасивні (які запускаються один раз та працюють самі по собі) та активні (для нормального функціонування котрих необхідно присутність або контроль збоку людини), а також превентивні (ті, які використовуються для того, щоб попередити виникнення SQL-атаки) і

реакційні (ті, які використовуються при виникненні загрози або усунення наслідків SQL-атаки).

На рис. 3.1 наведена блок схема виявлення та зупинення SQL -атаки.

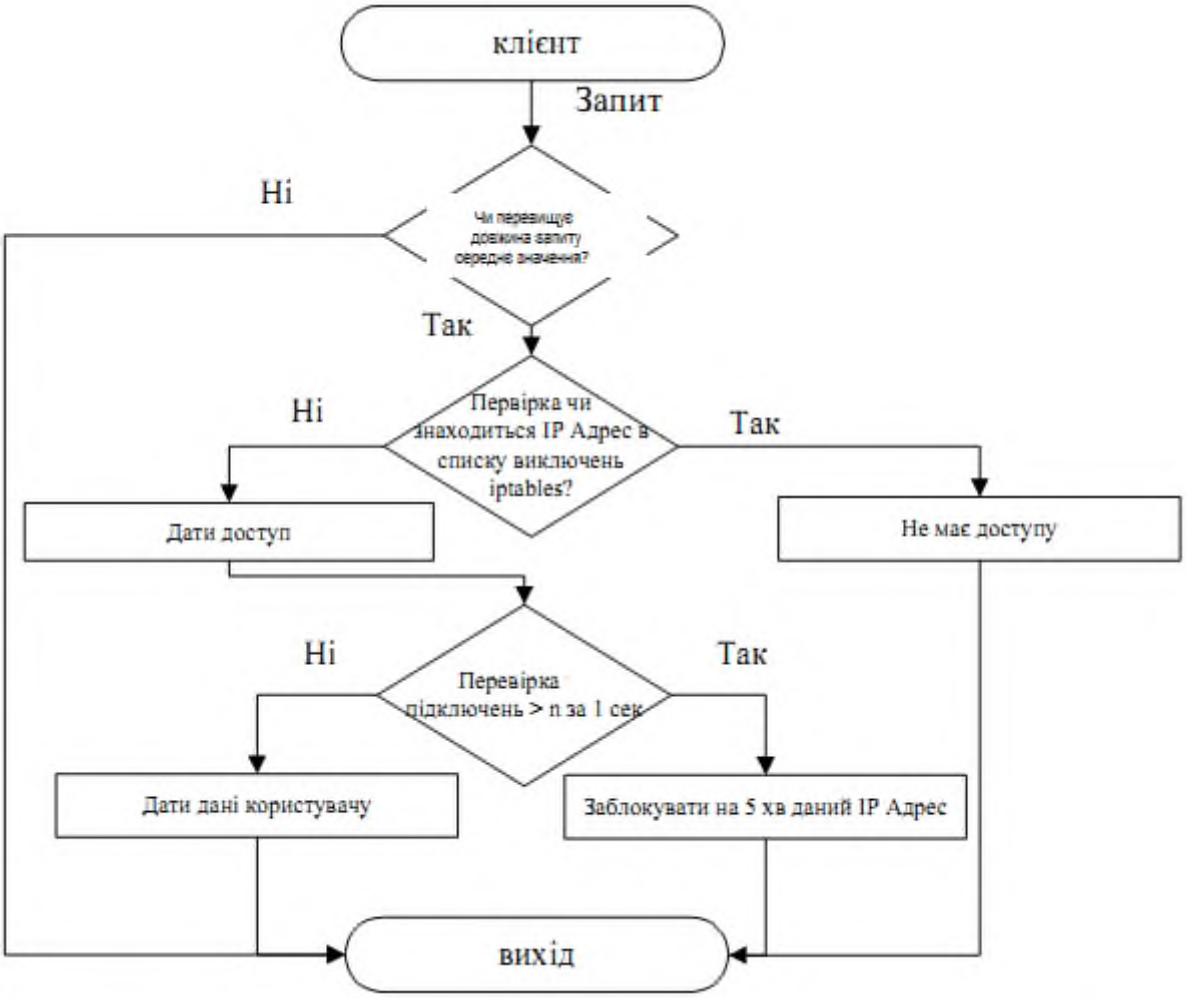


Рис. 3.1 Алгоритм виявлення та протидії SQL-атакам [3; с. 11]

З самого початку проводиться оцінка, щоб визначити, чи є збільшення тривалості серверних з’єднань понад норму чи збільшення довжини HTTP-запиту. Однак якщо ж є перевищення, тоді це є підставою для перевірки чи йде атака на сервер і чи містять ін’єкцію HTTP-запити. Спочатку аналіз передбачає перевірку відхилення від встановленої довжини та визначення того, чи включені IP-адреси, пов’язані з підозрілими запитами, до списку виключень. Згодом виконується обчислення довжини запиту, що надходить від кожної IP-адреси. Якщо отримане значення перевищує заздалегідь визначений поріг, це

вказує на триваючу ін’єкційну атаку. Щоб зупинити проникнення шкідливого коду, доцільно заборонити доступ з IP-адрес, які вважаються підозрілими, на 5 хвилин. У цей період обґрунтованість запитів буде оцінюватися шляхом ретельного вивчення їх структури, а ін’єкційна атака буде запобігатися шляхом блокування HTTP-запитів, що надходять із цих конкретних адрес. Ця стратегія виявилася ефективною для запобігання різним формам атак. Єдина розбіжність полягає в тому, що для кожного окремого типу атаки значення n змінюватиметься, що, у свою чергу, визначає кількісну оцінку надлишкового часу обробки або тривалості запиту [3; с. 11].

Подібним чином можна визначити час виконання запиту, який буде відрізнятися від стандартної процедури через включення додаткового коду.

У випадку, якщо є підозра на триваючу атаку SQL, бажано записати всю відповідну інформацію щодо з’єднання в окремому журналі. Особливий інтерес представляють атрибути тимчасової та вхідної IP-адреси, оскільки вони можуть допомогти у подальшій перевірці цих адрес. Згодом ці дані аналізуються, щоб ідентифікувати всі адреси, які зробили запити, що перевищують заздалегідь визначений поріг. Далі виявлені адреси блокуються в iptables.

Крім того, варто зазначити, що інженерно-технічний захист (ІТЗ) також може бути використаний для боротьби з частими ін’єкційними атаками на окремий ресурс. ІТЗ охоплює ряд спеціалізованих організацій, технологічних інструментів і заходів, призначених для захисту конфіденційної інформації. Одним із підходів до класифікації засобів ІТЗ є розгляд конкретних суб’єктів, на які вони впливають. У цьому контексті їх можна використовувати для захисту окремих осіб, фізичних активів, фінансових ресурсів, конфіденційної інформації тощо. Враховуючи різноманітність цілей, завдань, захищених об’єктів і залучених видів діяльності, стає необхідним створити систематичну систему класифікації на основі різних критеріїв, таких як тип, орієнтація та інші відповідні характеристики. Широкий набір класифікаційних характеристик дозволяє досліджувати ІТЗ з різних точок зору, включно з

об’єктами, які зазнали впливу, характером застосованих заходів, методами впровадження, ступенем охоплення та класом засобів зловмисників, яким протидіють служби безпеки.

Очевидно, що такий поділ засобів захисту інформації досить умовний, так як на практиці дуже часто вони і взаємодіють і реалізуються в комплексі.

Щоб пом’якшити загрози безпеці на проміжному рівні, одна потенційна стратегія передбачає впровадження протоколів, які обмежують довжину запитів. Це може бути досягнуто шляхом використання спеціального програмного забезпечення, яке враховує конфігурацію мережі та маршрутизацію запитів.

Розробка спеціалізованих програм для аналізу та синтезу топологій окремих мережевих ресурсів зумовлює необхідність створення нових математичних моделей, які точно описують системи «запит — сервер». Ці моделі мають бути легко зрозумілими та сприяти подальшому аналізу. Крім того, необхідно розробити відповідні обчислювальні методи для ефективної обробки підозрілих запитів. Для цього можна застосувати графи як математичні моделі топологій, для яких розроблено достатньо широке коло методів виявлення різних шляхів між початковими та кінцевими вершинами, контурів чи циклів, остовів дерев, множини вершин чи дуг, що підходять певним умовам тощо. Важливо розробити нові методи обробки топологічних графів з урахуванням можливостей ін'єкції. Крім того, для підвищення ефективності програмних засобів топологічного аналізу та синтезу необхідні спеціальні методи представлення графів для полегшення обробки запитів, такі як організація вершин і дуг у набори або списки. З цих міркувань матричні моделі системних топологій є переважними через їх організовану структуру та спрощений процес розрахунку.

Існує зростаючий попит на комплексний підхід до розробки матричних методів для аналізу та побудови топологій для обробки запитів NTTR. Отже, науково-технічний виклик аналізу та синтезу топологій систем зв’язку, а також розробки обчислювальних методів для обробки матричних моделей цих

топологій для створення ефективних програмних засобів для проектування систем стає все більш важливим.

Розглянемо, яким саме чином може бути представлена зазначена нами двоелементна система. З формальної точки зору наведену Таблицю можна представити у вигляді біграфи, частина якого - це користувачі, а інша - надіслані ними запити. Ці сегменти з'єднані між собою посиланнями зі значенням «Підозрілий запит». Відповідно пропонується сформувати матрицю цих зв'язків, яку можна зберігати на комп'ютерному носії у форматі csv.

Перевірка графіків може проводитися комплексно або на основі окремого ресурсу з метою виявлення найбільш ефективної моделі для навігації запитів різної довжини. Для ілюстрації розглянемо приклад аналізу графів, щоб визначити оптимальний шлях для доступу до інформації. Припустимо, що існує вимога направляти запити до певного ресурсу (1), який включає кілька користувачів, деякі з яких надсилають запити, що перевищують середню довжину. Числові значення, зображені над стрілками, вказують на кількість потенційних шляхів для запитів.

Для графа знайдемо максимальний шлях з вершини a_1 у вершину a_7.

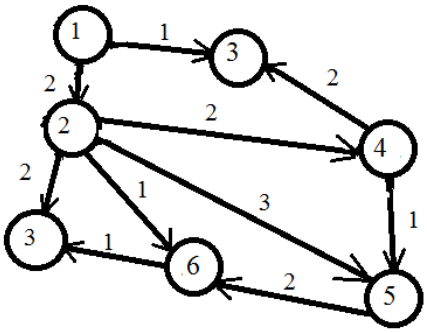


Рис. 3.2 Граф надходження запитів від різних користувачів

Для вершини a_1 приймаємо $q_s^{макс}(a_1a_1) = 0$. Для вершин $a_2, a_3 : q_s^{макс}(a_1a_2) = 2, q_s^{макс}(a_1a_3) = макс(1, 2+2+2) = 6$

Для вершини $a_4 : q_s^{макс}(a_1a_4) = 2+2 = 4.$

Для вершини $a_5 : q_s^{макс}(a_1 a_5) = макс(2+3,\ 2+2+1) = 5.$

Для вершини $a_6 : q_s^{макс}(a_1 a_6) = макс(2+1,\ 5+2) = 7.$

Для вершини $a_7 : q_s^{макс}(a_1 a_7) = макс(2+2,\ 7+1) = 8.$

Значення функції вздовж найбільш сприятливого маршруту становить вісім пунктів, і цей маршрут охоплює вузли 1, 2, 5, 6 і 7. Зокрема, для передачі запитів користувача 1 до ресурсу 7 оптимальний шлях, визначений наданим критеріїв, включає вузли 2, 5 і 6. Наразі будь-які запити, що перевищують визначену довжину, ігноруються іншими вузлами.

Крім того, можна надати дані, що стосуються наявності чи відсутності сумнівних прохань, шляхом побудови біграфії, яка є графіком, що складається з двох компонентів. Таким чином, можна визначити не лише кількість проблемних запитів, але й їх калібр, тобто які проблеми вирішувалися автоматично, а які ні. Таким чином, ця модель дозволяє відстежувати тривалість запитів і вирішувати конфлікти, які можуть виникнути, коли запити кількох користувачів накладаються. Завдяки підтримці повного запису всіх запитів, включаючи позначки часу та ідентифікаційні дані користувачів, ця модель зменшує ризик втрати інформаційного ресурсу та полегшує оцінку потенційних ризиків, пов’язаних із використанням інформаційного ресурсу окремими користувачами.

3.2. Розробка архітектури системи

Архітектура системи аналізу мережевого трафіку базується на поетапній обробці даних, що забезпечує послідовне перетворення пакетів на структуровану інформацію для подальнього моніторингу. Вона поєднує модулі різної функціональності, які спільно формують повний цикл опрацювання трафіку. Така структура дозволяє досягти стабільності системи та ефективно реагувати на зміни у мережевому середовищі. Кожен модуль виконує окремі логічні завдання, що спрощує конфігурацію та масштабування

системи. Розділення функцій забезпечує легкість оновлення та підвищує стійкість до відмов. Такий підхід формує гнучку платформу для подальшого удосконалення алгоритмів аналізу.

Побудова архітектури передбачає інтеграцію інструментів захоплення, фільтрації, аналізу та подання інформації у вигляді зручних для оператора інтерфейсів. Взаємодія між модулями встановлюється через стандартизовані формати передачі даних, що забезпечує узгодженість усіх компонентів. Такий підхід дозволяє оптимізувати затримки на кожному етапі обробки та зменшити навантаження на ресурси системи. Правильне проектування потоків даних забезпечує точність результатів та підвищує швидкість реагування. Архітектура має підтримувати гнучке масштабування, оскільки обсяги мережевого трафіку можуть змінюватися в широких межах. Це створює основу для побудови надійної системи моніторингу.

Характеристика модулів архітектури системи за компонентами наведена в табл. 3.1.

Таблиця 3.1

Характеристика модулів архітектури системи

Модуль	Основна функція	Тип даних	Приклади інструментів	Рівень обробки	Очікуваний результат
Модуль збору даних	Захоплення мережевих пакетів	Сирі пакети	tcpdump, Wireshark	Початковий	Формування потоку даних для аналізу
Модуль попередньої обробки	Фільтрація та відбір даних	Пакети з параметрами	Фільтри протоколів, IP, портів	Базовий	Скорочення обсягу трафіку для аналізу
Аналітичний модуль	Виявлення аномалій та подій	Структуровані записи	Правила, статистика, порогові значення	Основний	Ідентифікація підозрілих процесів
Модуль візуалізації	Подання результатів аналізу	Логи, таблиці, графіки	Інструменти звітності	Завершальний	Зрозуміле представлення інформації

Джерело: сформовано автором.

Модуль збору даних виконує функцію захоплення мережевих пакетів і формує первинний потік інформації для подальших етапів обробки.

Інструменти tcpdump або Wireshark забезпечують фіксацію повних заголовків і вмісту пакетів, що дозволяє зберегти всі необхідні параметри. Модуль працює на низькому рівні взаємодії з мережею, що забезпечує точність та повноту зібраних даних. Він підтримує роботу у режимах онлайн і офлайн, що розширює можливості аналізу. Зібрані дані передаються до модуля попередньої обробки через стандартизований формат. Це забезпечує стабільність роботи всієї системи.

Модуль попередньої обробки виконує фільтрацію потоків даних за критеріями протоколів, IP адрес або портів. Його основне завдання полягає у скороченні обсягу трафіку шляхом відсіювання нерелевантних пакетів. Фільтрація дозволяє зменшити навантаження на аналітичний модуль і підвищити ефективність обробки. Модуль підтримує динамічне налаштування фільтрів, що дає змогу адаптувати систему до змін у трафіку. Створення оптимізованого набору параметрів фільтрації підвищує точність подальшого аналізу. Таке попереднє структурування даних є важливою складовою архітектури.

Аналітичний модуль реалізує перевірку трафіку на відповідність встановленим правилам та статистичним нормам. Він аналізує обсяги трафіку, інтенсивність з’єднань та відхилення від базових поведінкових характеристик. У межах цього модуля застосовуються порогові значення та критерії, що дозволяють виявляти різкі зростання активності або ознаки атак. Модуль формує структуровані записи про події, які можуть становити загрозу. Його ефективність визначається якістю правил та точністю статистичних моделей. Результати аналізу передаються до модуля візуалізації.

Модуль візуалізації забезпечує узагальнення результатів аналізу у вигляді логів, таблиць або графічних відображень. Його завдання полягає у тому, щоб оператор отримував зрозумілу та інформативну картину стану мережевого середовища. Інструменти візуалізації дозволяють швидко оцінити динаміку змін, виявлені аномалії та загальну структуру трафіку. Модуль підтримує фільтрацію та сортування даних для зручності роботи з великими

обсягами інформації. Такий підхід підвищує швидкість реагування на інциденти та покращує процес прийняття рішень. Зрозуміле подання результатів завершує цикл обробки трафіку.

3.3. Очікувані результати

Запропонована система забезпечить своєчасне виявлення підозрілої активності завдяки поєднанню сигнатурних і статистичних методів аналізу. Система сформує умови для раннього попередження атак, що дозволить зменшити ризики порушення безпеки мережі. Використані механізми моніторингу підвищать точність оцінки подій і знизять ймовірність пропуску критичних інцидентів. Архітектура забезпечить стабільну роботу навіть за умов високого навантаження. Система створить можливість швидко реагувати на аномалії, що підвищить загальний рівень захищеності. Технологічна основа дасть змогу адаптуватися до різних типів мережевих середовищ.

Розроблена система підвищить простоту використання для адміністраторів завдяки зрозумілим інтерфейсам і логічній структурі обробки даних. Вона сформує чіткі правила взаємодії з модулями, що зменшить складність конфігурації. Модуль візуалізації створить наочне подання результатів, яке спростить аналіз подій. Стандартизований формат логів забезпечить зручність пошуку і перегляду інформації. Система допоможе зменшити час, необхідний для прийняття рішень щодо інцидентів. Такий підхід покращить операційну ефективність адміністрування мережі.

Запропонована архітектура забезпечить можливість масштабування системи у великих мережах завдяки гнучкій структурі модулів. Правила та фільтри дадуть змогу адаптувати систему до різних обсягів трафіку без зміни базового коду. Підтримка розширення функціональних компонентів сприятиме подальшому удосконаленню системи. Архітектура дозволить збільшувати пропускну здатність шляхом додавання додаткових

обчислювальних ресурсів. Такий підхід забезпечить відповідність системи зростаючим потребам організації. Система сформує умови для тривалої експлуатації без втрати продуктивності.

Очікується, що система підвищить точність класифікації аномалій завдяки комбінованій перевірці трафіку. Статистичні моделі нададуть змогу виявляти нетипові відхилення, які не фіксують сигнатурні методи. Порогові механізми дозволять реагувати на різкі зміни активності в режимі реального часу. Комбінація алгоритмів зменшить кількість хибнопозитивних і хибнонегативних спрацювань. Система створить більш збалансований підхід до аналізу подій. Такий результат посилить загальну ефективність захисту мережі.

Система покращить використання ресурсів за рахунок оптимізації попередньої обробки даних. Фільтрація трафіку зменшить навантаження на аналітичні компоненти і підвищить швидкість реагування. Якісне структурування даних дозволить виконувати аналіз без зайвих витрат обчислювальних потужностей. Організація роботи модулів забезпечить стабільність функціонування навіть за умов збільшення трафіку. Підвищена ефективність сприятиме довгостроковому використанню системи у різних інфраструктурах. Система сформує основу для подальшого розширення можливостей моніторингу.

Висновки до розділу 3

Запропонований підхід поєднує переваги класичного моніторингу та гнучких статистичних методів, що створює збалансовану основу для аналізу мережевого трафіку. Архітектура системи демонструє можливість обробки як відомих, так і нових типів аномалій. Використані модулі забезпечують логічний поділ функцій, що спрощує підтримку та подальший розвиток системи. Комбінація правил, сигнатур і статистики формує адаптивний

алгоритм виявлення загроз. Такий підхід сприяє більш точному визначенню нетипових подій у мережевих потоках. Результатом є підвищення стійкості інфраструктури до зовнішніх і внутрішніх загроз.

Система зберігає зрозумілість для практичного використання, що робить її придатною для адміністраторів з різним рівнем технічної підготовки. Структура модулів мінімізує потребу у складних налаштуваннях і спеціальних знаннях у сфері інтелектуальних технологій. Механізми фільтрації та попередньої обробки знижують навантаження на аналітичний компонент. Візуалізація результатів забезпечує швидке прийняття рішень і зручний контроль за станом мережі. Універсальність архітектури створює умови для використання системи в різних типах інфраструктур. Сформований баланс між функціональністю і простотою робить систему практично привабливою.

Запропонована концепція демонструє потенціал до масштабування за рахунок модульної структури та розширюваних правил аналізу. Система здатна адаптуватися до збільшення обсягів трафіку без зниження ефективності. Поєднання статистичних характеристик і детермінованих правил формує основу для подальших технологічних удосконалень. Отримані результати підтверджують можливість тривалого використання системи у динамічних мережевих умовах. Такий підхід створює перспективу для більш глибокої автоматизації аналізу трафіку. Застосована архітектура формує платформу для розвитку нових інструментів моніторингу.

РОЗДІЛ 4. ПРАКТИЧНА РЕАЛІЗАЦІЯ

4.1. Середовище реалізації

Практичне дослідження виконано в операційній системі Linux на базі дистрибутива Ubuntu, який забезпечує стабільність і широкі можливості роботи з мережевими інструментами. Дане середовище підтримує велику кількість утиліт для аналізу трафіку та роботи з мережею. У ньому передбачено оптимізовані механізми роботи з інтерфейсами і мережевими драйверами. Система дає змогу налаштовувати низькорівневий доступ до пакетів без сторонніх обмежень. Структура дистрибутива створює сприятливі умови для інтеграції додаткових модулів моніторингу. Використані компоненти дозволяють реалізувати дослідження без складної підготовки інфраструктури.

У середовищі застосовано утиліту tcpdump, яка забезпечує збір сирих мережевих пакетів з високою точністю. Інструмент дозволяє фіксувати трафік у режимі реального часу та зберігати його у форматі pcap. Такий підхід створює можливість для подальшого аналізу з використанням інших програмних засобів. Утиліта підтримує фільтрацію за протоколами, IP адресами та портами. Це зменшує обсяг даних і допомагає зосередитися на критично важливих подіях. Використання tcpdump забезпечує контрольоване та відтворюване середовище збору трафіку.

Детальний аналіз зібраних пакетів виконано за допомогою Wireshark, який забезпечує гнучкі можливості візуалізації та розбору даних. Програма дозволяє інтерпретувати мережеві протоколи на різних рівнях і відображати структуру кожного пакета. Використання фільтрів сприяє швидкому виділенню фрагментів трафіку, що містять потенційні аномалії. Візуальні засоби аналізу покращують здатність виявляти нетипові шаблони взаємодії між вузлами мережі. Розширення і модулі забезпечують інтеграцію програми з іншими інструментами дослідження. Середовище Wireshark створює умови для всебічного аналізу мережевих подій.

Системи Snort і Suricata застосовано для виявлення вторгнень за допомогою сигнатур і правил. Обидві системи забезпечують можливість аналізу трафіку в режимі реального часу. Підтримка розширюваних наборів правил дозволяє адаптувати середовище до різних типів загроз. Статистичні й детерміновані механізми аналізу доповнюють функціональність сигнатурних методів. Системи створюють умови для точного і швидкого виявлення аномалій. Таке поєднання інструментів формує повноцінне середовище дослідження без потреби у створенні спеціального програмного забезпечення.

4.2. Реалізація прототипу системи

Реалізація прототипу системи моніторингу базувалася на поетапній обробці мережевого трафіку, що забезпечує контроль на різних рівнях аналізу. На першому етапі виконувався збір трафіку за допомогою утиліти tcpdump, яка дозволяє створювати файли у форматі pcap. Отримані дані забезпечували повну картину мережевої активності за обраний період. Друга стадія передбачала використання Wireshark для фільтрації пакетів за протоколами, адресами і портами. Такий підхід давав змогу швидко відокремити фрагменти трафіку, що містили потенційні індикатори атак. Система формувала структуровані дані для подальшого аналізу інструментами виявлення загроз.

Виявлення загроз здійснювалося з використанням Snort і Suricata, які забезпечують сигнатурний і правиловий аналіз трафіку. Ці системи дозволяли визначати типові атаки, зокрема сканування портів і підозрілий HTTP трафік. Додаткові правила створювали умови для виявлення нетипових і цілеспрямованих дій. Система формувала журнали подій, де фіксувалися характеристики кожного інциденту. Логи забезпечували можливість оперативного перегляду та аналізу результатів роботи прототипу. Такий підхід дозволяв оцінювати ефективність методів виявлення у різних умовах.

У межах експерименту було змодельовано розвиток ін’єкційних атак з метою оцінки здатності системи реагувати на загрози. Для цього побудовано модель рівнів ризику, яка дозволяла визначати доцільність застосування додаткових механізмів захисту. Низькі значення ризику не вимагали активних дій, тоді як підвищені рівні передбачали посилений контроль за параметрами трафіку. Для високих значень ризику застосовувалися засоби моніторингу вхідних запитів до критичних ресурсів. Збільшення ризику понад визначений поріг створювало підстави для використання спеціального програмного забезпечення. Модель давала змогу класифікувати загрози з урахуванням інтенсивності атак.

Експериментальне дослідження передбачало моделювання ін’єкційної атаки та впровадження методів ідентифікації та пом’якшення таких атак. Спочатку була побудована модель для визначення необхідного рівня захисту. Якщо розрахунковий рівень нижче 50%, заходи активного захисту вважаються непотрібними. Для рівнів від 50% до 60% рекомендується контролювати певні параметри, які можуть вказувати на можливе виникнення ін’єкційної атаки. У випадках, коли рівень перевищує 60%, доцільно включити моніторинг вхідних запитів на вимогу на призначених ресурсах. Крім того, якщо рівень перевищує 80%, рекомендується розглянути можливість встановлення спеціалізованого програмного забезпечення, яке може ретельно аналізувати кожен вхідний запит.

Розглянемо, як проводиться моніторинг запитів у випадку рівня небезпеки вище 60%. Експериментальне моделювання SQL-атак виконують на базі спеціально створеної розподіленої мережі з використанням програм netmap, nping та WPEPro. У процесі дослідження мережеві служби стикаються з SQL-атаками різної інтенсивності. Ці атаки включають вставку шкідливого коду в HTTP-запити. Щоб зменшити ризики, пов’язані з цими атаками, система повинна використовувати сконструйовану модель для оцінки рівня ризику, пов’язаного з кожним запитом. На основі цієї оцінки система може або відхилити запит, якщо він створює високий ризик наслідків, піддати його

більш детальному аналізу для дослідження ін’єкційного компонента, або продовжити запит, якщо він вважається безпечним. Збір статистичної інформації проводиться за допомогою програми-аналізатора трафіку на основі відкритих бібліотек WinPcap та jpcap.

4.3. Тестування системи

Приклад базової інформації, що використовується для проведення досліджень, наведено в табл. 4.1.

Таблиця 4.1

Параметри моделювання SQL-атак

№ послідовності	Розмір (кількість пакетів)	Час передачі пакетів, хв	
		Звичайний режим	Режим атаки
1	50000	15	20
2	100000	30	35
3	150000	60	65
4	200000	75	86
5	250000	84	98

При цьому з метою максимального наближення до реальних умов функціонування мережевих сервісів в умовах наявності SQL-атаки, тестовий трафік складався з суміші реального мережевого трафіку та спеціально змодельованого з включенням «інфікованих» запитів. Після цього проводять розрахунок ентропії для кожної послідовності та з отриманих значень визначають, чи відбувається загроза атаки на певний момент (табл. 3.2).

Таблиця 4.2

Значення ентропії для послідовностей пакетів

№ послідовності	Значення ентропії H без атаки, біт	Значення ентропії H* при загрозі ін'єкційної атаки, біт
1	2,1	3,2
1	3,32	1,28
2	3,28	1,51
1	2,0	3,1
3	3,21	1,93
4	3,25	1,71
5	3,39	1,88

Таким чином, завдяки обчисленню ентропії для групи HTTP-запитів стає можливим виявити початок ін'єкційної атаки та швидко пом'якшити її наслідки. Іншими словами, аналіз даних трафіку в режимі реального часу може служити ознакою ненормальної поведінки та отримання підозрілих запитів. Зокрема, значення ентропії трафіку виявляють чутливість до атак SQL, коли виникнення атаки ін'єкції спричиняє значне зниження приблизно на 70% цих значень, оскільки включення додаткових рядків SQL призводить до більш довгих запитів. Варто зазначити, що розмір пакету не впливає на результат обчислень. У представленій теоретичній структурі на концепцію ентропії впливає надходження пакета, що містить певні параметри, такі як збільшення розміру або наявність певних ключових слів у вмісті. Це обчислення ентропії трафіку можна використовувати в різних програмах, включаючи системи виявлення вторгнень (IDS), системи управління інформацією безпеки підприємства, системи підтримки прийняття рішень, серед іншого, для виявлення початку ін'єкційних атак.

Як уже зазначалося, існуючі системи виявлення можна розділити на системи виявлення аномалій і системи виявлення ознак. Основним недоліком систем виявлення функцій є те, що вони призначені для виявлення певних типів атак (зазвичай найнебезпечніших на момент створення системи). Коли з'являються нові атаки або змінюються параметри пересування, завдання виявлення потрібно вирішувати знову. Системи виявлення аномалій (через складність моделювання нормального інтернет-трафіку) використовують різні

припущення щодо функціонування системи, наприклад, статистичну однорідність трафіку. Проте групи комп'ютерних систем, для яких застосовуються ці припущення, або умови їх реалізації не обговорювалися. В результаті незначні зміни в структурі трафіку або наданих послуг можуть призвести до необхідності перенавчання алгоритму виявлення. Одним із можливих рішень цієї ситуації є використання комплексного підходу до побудови системи захисту від атак збою, що включає моніторинг системи, ведення історії транзакцій, ведення спеціального репозиторію для інтелектуального аналізу дій і дій зловмисників, а також прийняття рішення про стратегію протидії. Пропонується побудувати систему захисту на основі наступних елементів:

– агенти нагляду;

– засоби попередньої обробки та зберігання;

– репозиторій для зберігання інформації про транзакції, що описує роботу системи;

– репозиторій з аналітичними компонентами для виявлення загроз та ознак зловмисної діяльності;

– контратакуючі агенти [**Помилка! Джерело посилання не знайдено.**; с. 572].

Одним з найважливіших аспектів побудови такої системи є визначення відповідної математичної допомоги, необхідної на кожному етапі проекту. Це гарантує, що кожен крок підтримується необхідними математичними інструментами та методами:

1. Одним з важливих аспектів керування мережею є моніторинг трафіку, який передбачає перехоплення пакетів для аналізу завантажень, моделей трафіку та поведінки користувачів. Для успішного виконання цього завдання необхідно розробити алгоритми для визначення відповідної кількості та частоти перехоплень пакетів на основі таких факторів, як перевантаження каналу та інших відповідних параметрів. Однак дуже важливо досягти балансу в процесі перехоплення, оскільки занадто часте перехоплення пакетів

потенційно може призвести до сповільнення трафіку. З іншого боку, якщо перехоплення здійснюється через фіксовані проміжки часу, існує ризик створення «сліпих зон», де немає доступної інформації [**Помилка! Джерело посилання не знайдено.**; с. 572].

2. Попередня обробка захоплених пакетів з подальшою оцінкою та виявленням найнебезпечніших загроз. Потім зібрана інформація зберігається для подальшого аналізу. Щоб забезпечити ефективність і мінімізувати використання ресурсів на цьому етапі, рекомендується використовувати нескладні та адаптовані порогові значення або, якщо це буде визнано за необхідне, послідовний CUSUM.

3. Після завантаження даних у сховище важливо виконати аналіз даних, щоб виявити потенційні атаки та оцінити загрози. Після того, як інформація буде записана в сховище, можна провести ретельну оцінку для розрахунку можливих ризиків. Щоб досягти цього, рекомендується використовувати багатоканальний CUSUM і алгоритми ковзного середнього, які були описані раніше.

4. Аналіз фонових даних проводиться для виявлення спроб сканування, атак деградації та атак пульсації. Цей аналіз виконується або на безперервній основі, або за заздалегідь визначеним графіком. З огляду на те, що ці атаки становлять відносно нижчий рівень загрози, є достатньо можливостей для більш ретельного їх вивчення. Для проведення цього аналізу використовуються різні методи, такі як Data Mining, інтелектуальні системи правил, нейронні мережі та інші подібні методології.

5. Одним з важливих кроків у цьому процесі є етап прийняття рішення щодо виявлення атаки. Якщо на будь-якому з попередніх етапів перевищено порогові значення, це вказує на потенційну загрозу атаки. На цьому етапі виникає необхідність у розробці експертної системи, здатної оцінити серйозність загрози та визначити, чи варто продовжувати ініціювати контратаку.

6. Процес оцінки загроз передбачає оцінку потенційних ризиків і вразливостей у системі чи мережі. Після визначення потенційних загроз наступним кроком є вибір відповідної моделі, яка може точно представляти сценарій атаки. Однак дуже важливо перевірити обрану модель, щоб переконатися в її надійності та точності. Після перевірки моделі наступним кроком є пошук відповідної стратегії протидії виявленій атаці. Вибір контрзаходів може сильно відрізнятися залежно від типу та конкретних деталей нападу. Фактично, ми можемо розглядати ці контрзаходи як стратегічний підхід до пом'якшення атаки. Використовувана стратегія також може залежати від різних факторів, таких як якість послуг, що надаються зареєстрованим користувачам. Це означає, що стратегію може знадобитися скоригувати на основі якості впроваджених контрзаходів. Для розробки ефективних стратегій важливо аналізувати взаємодію між зловмисниками та агентами захисту за допомогою аналітичних моделей. Вивчаючи ці моделі, ми можемо оцінити ефективність наших контрзаходів і передбачити можливі наслідки. Цей аналітичний підхід нагадує ігрову установку, що відображає природну конфліктну взаємодію між зловмисниками та системою захисту. Основною змінною, яка впливає на гравців у цій грі, є навантаження на систему, яке може стосуватися загального навантаження на систему або навантаження на окремі критичні компоненти, такі як процесор, оперативна пам’ять або мережеві канали [**Помилка! Джерело посилання не знайдено.**; с. 573].

Після того, як контрзаходи були розгорнуті, важливо постійно контролювати систему та вимірювати поточний рівень загрози. Якщо атака продовжується або розвивається, необхідно переоцінити та переглянути відповідну стратегію протидії. Цей ітеративний процес гарантує, що система залишається стійкою та адаптованою до мінливих загроз і динаміки. Після цього необхідно застосувати вибрані контрзаходи та оцінити їх ефективність. Це передбачає активне впровадження захисних заходів і порівняння результатів із початковими прогнозами. Цей процес оцінювання дає цінну

інформацію про ефективність стратегії та допомагає визначити будь-які сфери, які можуть потребувати коригування або вдосконалення. По-перше, важливо чітко визначити конкретний тип динаміки, яка діє в даному контексті. Це допоможе глибше зрозуміти природу та поведінку системи, що захищається. Після того, як ці оцінки зроблені, наступним кроком є ідентифікація та визначення можливих контрзаходів, які можна застосувати. Важливо розглянути низку потенційних рішень і ретельно передбачити можливі наслідки, які можуть виникнути в результаті кожного варіанту. Ще одним ключовим аспектом є оцінка кількості та сили потенційних нападників. Ретельно оцінюючи потенційні загрози та можливості супротивників, можна краще оцінити рівень ризику та відповідно розробити відповідні контрзаходи. Крім того, вкрай важливо оцінити загальний рівень загрози з боку зловмисників. Це передбачає аналіз потенційного впливу та серйозності атак, що дозволяє розробити більш обґрунтовану стратегію [**Помилка! Джерело посилання не знайдено.**; с. 573]. Для використання моделі можливо введення додаткових параметрів у процес ідентифікації загрози ін’єкційної атаки і врахування їх впливу на підсумкові дії по захисту від атаки. Серед параметрів, які застосовувались до вибору середовища проведення експерименту, були визначені наступні параметри:

Таблиця 4.3

Умови проведення експериментального дослідження

	Показники рівня захисту			Результат ступеню рівня захисту від ін’єкційних атак
	X1	X2	X3	
Контрольне значення	37	59	66	64
Експериментальне значення	38	57	67	64

Отже, за допомогою моделі ми можемо оцінити рівень захисту від атаки під час експерименту і через заздалегідь відомі параметри:

$$\hat{Y}_{КЗ} = 0{,}967 + 0{,}640 \cdot 37 + 0{,}343 \cdot 59 + 0{,}287 \cdot 66 = 63{,}9\%$$

$$\hat{Y}_{ЕЗ} = 0{,}967 + 0{,}640 \cdot 38 + 0{,}343 \cdot 57 + 0{,}287 \cdot 67 = 64{,}1\%$$

Отже, оцінка за моделлю співпадає з фактичним значенням з точністю до 0,1%, що підтверджує ефективність моделі і дозволяє її застосовувати в подальшому для прогнозування рівня захисту від атак. Тобто, в даній моделі розраховується ймовірність того, що інформаційний ресурс не зможе протистояти діям агенту загрози. Значення розраховується на основі показників можливості загрози і сили захисних засобів. Результатом виконання даного кроку є значення уразливості, яке розраховується за допомогою матриці визначення уразливості, поданої в табл. 4.4 [**Помилка! Джерело посилання не знайдено.**].

Таблиця 4.4

Матриця визначення ймовірності вразливості

Вразливість						
Можливість загрози	**ДВ**	ДВ	ДВ	ДВ	В	ДВ
	В	ДВ	ДВ	В	С	Н
	С	ДВ	В	С	Н	ДН
	Н	В	С	Н	ДН	ДН
	ДН	С	Н	ДН	ДН	ДН
		ДН	**Н**	**С**	**В**	**ДВ**
	Сила захисних засобів					

Також враховується імовірна частота ін’єкційної атаки за певний період часу. Значення розраховується на основі частоти подій ризику та вразливості, отриманих під час аудиту інформаційного ресурсу. Результатом цього кроку є значення частоти подій, що призводять до втрат, яке розраховується за допомогою матриці частоти подій втрат, наведеної у табл. 4.5 [**Помилка! Джерело посилання не знайдено.**].

Таблиця 4.5

Матриця визначення частоти подій, що призводять до негативних наслідків

Частота подій, що приводить до негативних наслідків						
Частота подій реалізації загрози	**ДВ**	С	В	ДВ	ДВ	ДВ
	В	Н	С	В	В	В
	С	ДН	Н	С	С	С
	Н	ДН	ДН	Н	Н	Н
	ДН	ДН	ДН	ДН	ДН	ДН
		ДН	**Н**	**С**	**В**	**ДВ**

	Вразливість

Після цього проводиться підрахунок вірогідної величини втрат внаслідок атаки.

Оцінити величину втрати в найгіршому випадку можливо, виконуючи наступні три пункти:

– визначити дію загрози, що скоріш за все призведе до результату найгіршого випадку;

– визначити величину для кожної форми втрати, пов’язаної з тією дієюзагрози;

– підсумувати величини кожної форми втрат.

Оцінити ймовірну величину втрат можна наступним чином:

– встановити найбільш вірогідну дію(ї) множини загроз;

– визначити величину втрат для кожної форми втрат;

– підсумувати величини.

Саме на цьому етапі відбувається зіставлення якісних і кількісних показників. Після цього відбувається встановлення походження ризику ін’єкційної атаки, чітке формулювання критеріїв моніторингу та оцінка величини потенційних збитків у випадку успішності атаки. Фактично на даному кроці підсумовуються усі отримані на попередніх кроках дані. На основі отриманих даних встановлюються ймовірна частота ін’єкційних атак та ймовірна величина майбутніх втрат.

Таблиця 4.6

Схема оцінки вірогідної величини втрат у разі дії загроз

	Види втрат					
Дія загрози	Продуктивність	Реакція	Заміна	Штрафи,рішення	Рекламакомпанії	Репутація
Отримання НСД						
Зьій в роботі системи						

Розголошення інформації						
Модифікація ресурсу						
Відмова в доступі						

Добре сформульовані параметри ризику забезпечать осіб, які приймають рішення щодо засобів захисту від ін'єкційних атак, принаймні двома ключовими елементами інформації:

- підрахована частота подій, що призводить до втрат;
- підрахована вірогідна величина втрат.

Ця інформація може бути виражена у різній формі. У більшості випадків бажано також надавати підрахований потенціал щодо втрат найвищого рівня для того, щоб особа, яка приймає рішення, була проінформована щодо сценарію втрат у найгіршому випадку.

Таблиця 4.7

Матриця визначення величини ризику

Ризик						
Вірогідна величина втрати	Критична	В	В	К	К	К
	Висока	С	В	В	К	К
	Значна	С	С	В	В	К
	Середня	Н	С	С	В	В
	Низька	Н	Н	С	С	С
	Дуже низька	Н	Н	С	С	С
		ДН	Н	С	В	ДВ
	Частота подій, що приводить до втрат					

Тобто на цьому етапі мають бути чітко визначені наступні величини: частотаподій, що приводить до втрат; вірогідні втрати; втрати в найгіршому випадку. За допомогою табл.3.7 встановлюється величина ризику, а її значення розшифровується за допомогою таблиці 4.8 [14].

Таблиця 4.8

Значення рівня ризику втрати інформаційних ресурсів

Значення	Рівень ризику
К	Критичний (більше 80;)
В	Високий (більше 60%)
С	Середній (більше 50%)
Н	Низький (мнше 50%)

В окремих випадках, для уточнення оцінки інформаційних ризиків, може бути застосований підхід, заснований на переході від якісної до кількісної оцінки інформаційних ризиків

Під час тестування системи було змодельовано кілька сценаріїв, що відтворювали як нормальну активність, так і потенційні загрози. Нормальний режим включав перегляд веб сторінок, роботу з електронною поштою та потокове відтворення відео, що створювало типовий фон мережевого трафіку. Додатково виконувалася імітація мережевої атаки шляхом сканування портів за допомогою nmap, що дозволяло оцінити здатність системи реагувати на зовнішні загрози. Окремо було змодельовано передавання великого обсягу даних з одного вузла для фіксації поведінки системи у випадку аномального навантаження. Результати показали, що Snort і Suricata коректно виявили спроби сканування портів, відобразивши відповідні сигнатурні спрацювання у журналах подій. Система також зафіксувала аномально високий рівень трафіку від конкретної адреси, що підтверджує можливість визначення нетипових ситуацій у мережевому середовищі.

Висновки до розділу 4

Розроблений прототип системи продемонстрував здатність ефективно виявляти аномалії у мережевому трафіку за рахунок поєднання базових інструментів моніторингу. Система працює на основі стандартних утиліт та програмного забезпечення, що забезпечує доступність і відтворюваність результатів. Реалізований підхід довів спроможність виявляти як типові, так і менш очевидні загрози без залучення складних механізмів штучного інтелекту. Отримані результати підтверджують стабільність роботи у різних експериментальних сценаріях. Система реагує передбачувано та фіксує події у логах, що дозволяє здійснювати подальший аналіз. Прототип створює основу для використання у невеликих і середніх мережах.

Суттєвою перевагою системи є простота у використанні, що знижує вимоги до кваліфікації адміністратора. Достатньо налаштувати правила та фільтри, щоб отримувати інформацію про критичні події у мережевому середовищі. Зрозуміла структура журналів спрощує інтерпретацію результатів аналізу. Система допомагає зменшити ймовірність пропуску загроз завдяки комбінованому підходу до обробки трафіку. Механізми виявлення працюють послідовно та узгоджено, що підвищує точність реагування. Така організація процесу робить систему практично корисною для повсякденного моніторингу.

Отримані результати демонструють можливість подальшого розширення системи без суттєвих змін архітектури. Використання модульної структури дозволяє додавати нові компоненти або інтегрувати сучасні методи аналізу. Система зберігає стабільність навіть за умов збільшення навантаження під час експериментів. Застосований підхід створює перспективу для оптимізації процесів мережевого моніторингу у ширших інфраструктурах. Ефективність реакції на аномальні події підтверджує доцільність подальшого удосконалення прототипу. Результати дослідження формують підґрунтя для розвитку комплексних систем аналізу трафіку.

ВИСНОВКИ

Проведене дослідження узагальнює теоретичні підходи до аналізу мережевого трафіку та демонструє їх практичне застосування у задачах виявлення аномалій. У роботі розглянуто ключові методи збору та обробки даних, що забезпечують основу для побудови систем моніторингу. Окрему увагу приділено інструментам, які дозволяють здійснювати детальний аналіз структури пакетів та визначати відхилення від типових моделей поведінки мережі. Теоретичні відомості створили необхідну базу для обґрунтування вибору технологій, використаних у практичній частині. У межах дослідження сформовано цілісне бачення можливостей класичних методів безпеки. Отримані результати підтверджують актуальність використання поєднання сигнатурних і статистичних засобів.

Практична частина роботи продемонструвала можливість побудови робочого прототипу системи на основі відкритих інструментів і мінімальних вимог до ресурсів. Для дослідження використано tcpdump, Wireshark, Snort і Suricata, що забезпечили повний цикл обробки трафіку від збору до виявлення аномалій. Інтеграція цих інструментів дозволила оцінити їх сумісність та ефективність у реальних умовах моделювання. Під час тестування було перевірено здатність системи знаходити типові загрози, включно зі скануванням портів і аномальним підвищенням активності окремих вузлів. Отримані дані засвідчили коректність роботи прототипу у різних експериментальних сценаріях. Це підтвердило придатність запропонованого підходу до практичного використання.

У роботі проведено аналіз існуючих інструментів моніторингу та систем виявлення загроз, що дозволило визначити їх сильні та слабкі сторони. Встановлено, що багато сучасних засобів потребують значних обчислювальних ресурсів або спеціальних знань у сфері машинного навчання. Запропонований підхід зосереджується на класичних методах, які залишаються ефективними у широкому спектрі мережевих середовищ.

Комбінація сигнатурного аналізу та статистичних показників продемонструвала збалансований рівень чутливості і точності. Такий підхід не створює надмірного навантаження на інфраструктуру та легко інтегрується в існуючі системи. Дослідження підтвердило практичну доцільність використання цих методів у невеликих організаціях.

Розроблена архітектура системи дозволила реалізувати адаптивний механізм реагування на мережеві події. Проєктована структура включала модулі збору, обробки та аналітичного оцінювання трафіку, що забезпечило логічний поділ функцій. У процесі моделювання встановлено, що модульна побудова спрощує налаштування і подальшу модифікацію системи. Система показала здатність реагувати на зростання ризику та приймати рішення відповідно до визначених порогів небезпеки. Запропонована логіка дала змогу ефективно визначати рівень загрози та обирати відповідні дії. Це підтверджує можливість масштабування підходу та подальшого його розширення.

Тестування системи у різних сценаріях мережевої активності довело її функціональність і стійкість до навантажень. Було зафіксовано стабільне виявлення типових атак, що підтверджує практичну ефективність вибраних методів. Аналіз журналів подій засвідчив можливість детального відтворення мережевих процесів. Система працювала передбачувано, не створювала надмірної кількості хибних спрацювань і своєчасно фіксувала критичні події. Тестові результати відобразили потенціал прототипу для подальшої автоматизації процесів аналізу трафіку. Вони також підкреслили важливість правильного налаштування правил і параметрів моніторингу.

Перспективи розвитку розробленої системи пов’язані з удосконаленням механізмів аналізу та інтеграцією додаткових засобів. Розширення баз сигнатур і правил може підвищити точність і швидкість виявлення складних атак. Інтеграція з централізованими платформами обробки логів дозволить покращити керування подіями і створити єдине інформаційне середовище. Додавання механізмів автоматичного реагування відкриває можливість формування активних політик безпеки. Такі зміни розширюють потенціал

використання системи у більших організаціях та складніших мережевих інфраструктурах. Запропонований підхід може стати основою для розробки більш комплексних рішень у сфері моніторингу трафіку.

Підсумовуючи отримані результати, можна зазначити, що створена система відповідає поставленим цілям та демонструє практичну цінність. Вона поєднує доступність, ефективність і простоту налаштування, що робить її придатною для освітніх та невеликих корпоративних середовищ. Запропонована реалізація підтвердила, що класичні методи аналізу трафіку зберігають практичну значущість і можуть ефективно працювати без складних алгоритмів штучного інтелекту. Архітектура системи залишає можливості для подальшого розвитку та розширення функціоналу. У межах дослідження продемонстровано потенціал для створення більш інтегрованих і адаптивних рішень. Отримані результати формують основу для подальших наукових і практичних розробок у сфері мережевої безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрущак І. Є., Кошелюк В. А. Особливості захисту хмарного середовища на основі blockchain. *The 10 th International scientific and practical conference "Science, innovations and education: problems and prospects"* (May 4-6, 2022, Tokyo, Japan). 2022. С. 161–167.

2. Антонюк П.Є. Класифікація ймовірних способів вчинення атак на інформацію як напрям протидії комп'ютерній злочинності. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/bozk/19text/g1927.htm. (дата звернення 20.12.2025)

3. Багнюк Н.В., Мельник В.М., Клеха О.В. Види DDoS-атак та алгоритм виявлення DDoS-атак типу Flood-атак. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2015. № 18. С. 6-12.

4. Бевз О.М., Папінов В.М., Скидан Ю.А. Проєктування програмних засобів систем управління. URL: http://posibnyky.vntu.edu.ua/bevz/ (дата звернення 01.12.2025)

5. Бєлова М.В., Бєлов Д.М. Виклики та загрози захисту персональних даних у роботі за штучним інтелектом. *Науковий вісник Ужгородського національного університету*. № 79. 2023. С. 17–22.

6. Богуцький П. П. Концептуальні засади права національної безпеки України. Київ ; Одеса : Фенікс, 2020. 374 с.

7. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200-203.

8. Гарасимчук О.І., Костів Ю.М. Оцінка ефективності систем захисту інформації. *Вісник КНУ імені Михайла Остроградського*. 2016. № 1. С. 16–20.

9. Гвозденко М.В., Чобу Я.В. Технічні та програмні засоби виявлення джерела DDoS-атаки. *GLOBAL SCIENTIFIC UNITY*. 2014. С. 106-115.

10. Гнатюк С. Є. Математичні моделі оцінки та прогнозування надійності програмно-керованих засобів захисту інформації в системі

урядового зв’язку. Ukrainian Information Security Research Journal. 2016. № 2. С. 150-156.

11. Гуртова, К. М. Теорія і практика адаптації законодавства України до законодавства ЄС. *Київський часопис права.* 2024. Вип. 4. С. 162–168.

12. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. *Інформаційне право.* 2017. № 7. С. 109-116.

13. Доронін І. М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження: Дис. докт.юрид.наук: 12.00.01. Київ, 2020. 539 с.

14. Дубняк М.В. Економіка даних: правовий та етичний аспект. *Інформація і право*. 2023. № 3 (46). С. 64–74.

15. Ільницький А. Ю., Саницький В. А., Порошев В. В. Основи захисту інформації від несанкціонованого доступу. К. : Національна академія внутрішніх справ України, 2022. 208 с.

16. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023.№11 (листопад) . 300 с.

17. Колесніков А.П., Карапетян О.М. Штучний інтелект: переваги та загрози використання. *Ефективна економіка*. 2023. № 8. С. 1–13.

18. Колмакова В. О., Шаров С. В. Використання МВОК для формування імунітету від інформаційних загроз. *Українські студії в європейському контексті.* 2023. № 6. С. 80–87.

19. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: міжнародний документ від 28.01.1981. URL: http://zakon4.rada.gov.ua/laws/show/994_326 (дата звернення: 02.12.2025).

20. Конвенція про кіберзлочинність / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 02.12.2025).

21. Конституція України від 28.06.1996 № 254к/96-ВР. URL: http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 02.12.2025).

22. Коробейнікова Т. І., Копач А. І. Сучасні алгоритми шифрування: детальний аналіз та перспективи розвитку. *SWorldJournal.* 2024. № 25-01. С. 89–95.

23. Кравчук В.О. Завдання адміністративно-правового захисту персональних даних у соціальних мережах. *Прикарпатський юридичний вісник.* 2024. № 2(55). С. 65-68.

24. Кримінальний процесуальний кодекс України Кодекс від 13.04.2012 № 4651-VI. URL: http://zakon2.rada.gov.ua/laws/show/4651-17 (дата звернення: 02.12.2025).

25. Лазаренко Н. І., Коломієць А. М., Паламарчук О. М. Комунікація в інтернет-просторі: психологічний аспект. *Інформаційні технології і засоби навчання.* 2018. Т. 65. № 3. URL: https://www.researchgate.net/publication/331404925_KOMUNIKACIA_V_INTERNET-PROSTORI_PSIHOLOGICNIJ_ASPEKT

26. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. 300 с.

27. Маковецький О. М. Підходи до удосконалення методики оцінки ефективності комплексної системи захисту інформації / О. М. Маковецький, І. Р. Мальцева, Н. А. Паламарчук, Ю. О. Черниш, О. В. Шемендюк. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. № 2 (26). С. 54–58.

28. Машталяр О.М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний науковий електронний журнал.* 2024. № 8. С. 256-259.

29. Менеджмент інформаційної безпеки: підруч.: у 2 ч. / А. К. Гринь, О. Д. Довгань, В. І. Журавель та ін.; за заг. ред. Є. Д. Скулиша. К. : Наук.–вид. Центр НА СБ України, 2013. Ч.1. 456 с.; Ч.2. 604 с.

30. Мірошниченко М.Ю. Алгоритм захисту персональних даних в соціальних мережах. *Українські студії в європейському контексті.* 2024. № 9. С. 190-195.

31. Назаров Є.М. Захист на рівні додатків: сучасні виклики та технології. *Українські студії в європейському контексті.* 2023. №7. С. 300–307.

32. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. 776 с.

33. Нейромережева методологія розпізнавання інтернет-орієнтованого шкідливого програмного забезпечення. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/4688 (дата звернення 02.12.2025)

34. Нечітка логіка на прикладах. iSearch. URL: http://www.isearch.kiev.ua/index.php/uk/internetsecurity/837–fuzzy–message (датазвернення: 05.12.2025).

35. Остіян Є.З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету*, 2024. Серія ПРАВО. Випуск 85: частина 3. С. 47-53.

36. Пашинський В.Й., Цьоменко А.В. Захист персональних даних Європейським судом з прав людини. *Юридичний науковий електронний журнал.* 2024. № 10. С. 610-613.

37. Плескач В.Л., Рогушина Ю.В., Кустова Н.П. Інформаційні технології та системи: підруч. для студ. екон. спец. К.: Книга, 2018. 520 с.

38. Плескач В.Л., Рогушина Ю.В., Кустова Н.П. Інформаційні технології та системи: підруч. для студ. екон. спец. К.: Книга, 2018. 520 с.

39. Про захист економічної конкуренції: закон від 11.01.2001 № 2210-III. URL: http://zakon4.rada.gov.ua/laws/show/2210-14 (дата звернення: 14.10.2025).

40. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94. URL: https://

zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80 (дата звернення: 15.10.2025).

41. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 15.10.2025).

42. Про інформацію: Закон України від 2 жовтня 1992 р. № 2658. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 16.10.2025).

43. Про схвалення Концепції розвитку штучного інтелект в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 16.10.2025).

44. Про телекомунікації: закон від 18.11.2003 № 1280-IV. URL: http://zakon2.rada.gov.ua/laws/show/1280-15 (дата звернення: 16.10.2025).

45. Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України. URL: http://www.niss.gov.ua/content/articles/files/1_cPPP-standarts_27-04_Gn_var_FIN-732b6.pdf (дата звернення 02.12.2025).

46. Прокопець Н.А., Глоба Л.С. Математичне моделювання процесу обслуговування навантаження в інформаційно-комунікаційній мережі. Проблеми телекомунікацій. 2022. № 1 (30). С.18-31.

47. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ ЄС (Загальний регламент про захист даних). *Відомості Верховної Ради України*. 2016. URL: https://zakon.rada.gov.ua/laws/show/984_008- 16#Text (дата звернення: 07.12.2025).

48. Ромашко С.М. Опорний конспект лекцій з дисципліни «Інформаційні системи в менеджменті». Львів: ЛІМ, 2017. 49с.

49. Сергієнко Т. І. Роль інформаційних технологій у житті сучасної людини. *Українські студії в європейському контексті.* 2023. №7. С. 344–349.

50. Скопенко Н.С., Шеремет О.О., Єрьомін М.В. Процес прийняття та реалізації управлінських рішень. *Інвестиції: практика та досвід.* 2024. № 18. С.49-55.

51. Солодка О.М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право.* 2020. № 4 (35). С. 39-46.

52. Ус С.А. Моделі й методи прийняття рішень: навч. посіб. / С.А. Ус, Л.С. Коряшкіна; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». 2-ге вид. випр. Дніпро : НТУ «ДП», 2018. 300 с.

53. Федушко С. Сучасні підходи до дослідження кібербезпеки та кібергігієни в умовах цифрової трансформації суспільства. *Вісник Хмельницького національного університету.* 2023. №3. С.210-213.

54. Хмельов О.Г. Моделювання процесів бізнес-прогнозування за допомогою нейромережевих структур. URL: http://www.economy.nayka.com.ua/?op=1&z=38 (дата звернення 18.11.25)

55. Хрущ С., Островська В. Методи виявлення інформаційно-психологічних впливів в соціальних мережах. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2019. № 1. С. 60-74.

56. Цмоць О.І., Маршук А.А. Прогнозування фінансового стану підприємства за допомогою штучних нейронних мереж. Науковий вісник НЛТУ України, 2011. Вип. 21.9. С.347-352.

57. Яремко С., Кузьміна О., Новицький Р. Використання технологій штучного інтелекту для прогнозування бізнес-процесів. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* 2021. № 43. С. 230-235.

58. Ясинська Н.А., Івченкова О.Ю. Використання нейронних мереж в моделюванні фінансових результатів бізнес-процесів. *Світ фінансів.* 2019. № 3(60). С. 108-120.

59. A fuzzy expert system for automatic seismic signal classification. URL:

https://www.sciencedirect.com/science/article/pii/S09574114053 (дата звернення: 10.12.2025).

60. A novel fuzzy decision–making system for CPU scheduling algorithm. URL: https://link.springer.com/article/10.1007/s00521–015– 1987–8(дата звернення: 12.12.2025).

61. Classification of Network Traffic Using Fuzzy Clustering for Network Security. URL: https://link.springer.com/chapter/10.1007/978– 3–319–62701–4_22 (дата звернення: 12.12.2025).

62. Computer Aided Development of Fuzzy, Neural and Neuro–Fuzzy Systems. URL: https://www.researchgate.net/publication/312590719_Computer_Aided_Development_of_Fuzzy_Neural_and_Neuro–Fuzzy_Systems (дата звернення: 13.12.2025).

63. Diagnosing computer hardware failures using expert system (rule–based technique). URL: https://www.researchgate.net/publication/79205502_DIAGNOSING_COMPUTER_HARDWARE_FAILURES_USING_EXPERT_SYSTEM_RULEBASED_TECHNIQUE (дата звернення: 01.12.2025).

64. Expert diagnosis of computer systems, neuro–fuzzy knowledge base. IEEE: web–site. URL: https://ieeexplore.ieee.org/document/metrics#metrics(дата звернення: 20.12.2025).

65. Expert evaluation model of the computer system diagnostic features. URL: https://ieeexplore.ieee.org/document/7027101/metrics (дата звернення: 20.12.2025).

66. Giachanou, A., R´ıssola, E.A., Ghanem, B., Crestani, F., Rosso, P.: The Role of Personality and Linguistic Patterns in Discriminating Between Fake News Spreaders and Fact Checkers. In: International Conference on Applications of Natural Language to Information Systems. pp. 181–192. Springer (2020)

67. Giachanou, A., Rosso, P., Crestani, F.: Leveraging Emotional Signals for Credibility Detection. In: Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval. pp. 877–880 (2019)

68. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/ standard/27001 (дата звернення: 07.12.2025)

69. ISO/IEC 27017::2015Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services . URL: https://www.iso.org/ standard/43757.html (дата звернення: 07.12.2025)

70. ISO/IEC 27018:2025Information security, cybersecurity and privacy protection – Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors. URL: https://www.iso.org/standard/27018 (дата звернення: 07.12.2025)

71. Kumar, V., Reinartz, W., 2018. Customer relationship management: Concept, strategy, and tools. Springer

72. M. McCord and M. Chuah, «Spam detection on twitter using traditional classifiers,» in Autonomic and Trusted Computing, J. M. A. Calero, L.T. Yang, F. G. Mármol, L. J. G. Villalba, A. X. Li, and Y. Wang, Eds., Springer Berlin Heidelberg, 2011, pp. 175–186.

73. Mamdani, E.H., Assillan, S.: An experiment in linguistic synthesis with afuzzy logic controller.Int. J. Man-Mach. Stud. 7(1), 1–13, 1975.

74. Network–based output tracking control for T–S fuzzy systems using an event–triggered communication scheme. URL: https://www.sciencedirect.com/science/article/pii/S0165011032(дата звернення: 21.12.2025).

75. Rashkin, H., Choi, E., Jang, J.Y., Volkova, S., Choi, Y.: Truth of Varying Shades: Analyzing Language in Fake News and Political Fact-Checking. In: Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing. pp.2931–2937. EMNLP ’17 (2017)

76. Reddy, T. R., Vardhan, B. V., Reddy, P. V., 2016. A survey on authorship profiling techniques. International Journal of Applied Engineering Research 11 (5), 3092–3102

77. Schlicht, I. B., & Magnossão de Paula, A., F. (2021). Unified and multilingual author profiling for detecting haters. Proceedings of the Working Notes of CLEF 2021 - Conference and Labs of the Evaluation Forum, 2936, 1837–1845. https://dblp.org/rec/conf/clef/SchlichtP21.bib

78. Simulation and Model–Based Design. Mathworks: web–site. URL: https://www.mathworks.com/simulink.html(дата звернення: 16.12.2025).

79. Statistical and Machine Learning forecasting methods: Concerns and ways forward. URL: https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0194889

80. Stuart Russell and Peter Norvig Artificial Intelligence: A Modern Approach: Fourth edition (2020). Hoboken: Pearson. https://lccn.loc.gov/2019047498.

81. Stuart Russell and Peter Norvig Artificial Intelligence: A Modern Approach: Fourth edition (2020). Hoboken: Pearson. https://lccn.loc.gov/2019047498.

82. The neuro–fuzzy diagnostic model synthesis with hashed transformation in the sequence and parallel mode. URL: https://ric.zntu.edu.ua/article/view/101022/96247(дата звернення: 02.12.2025).

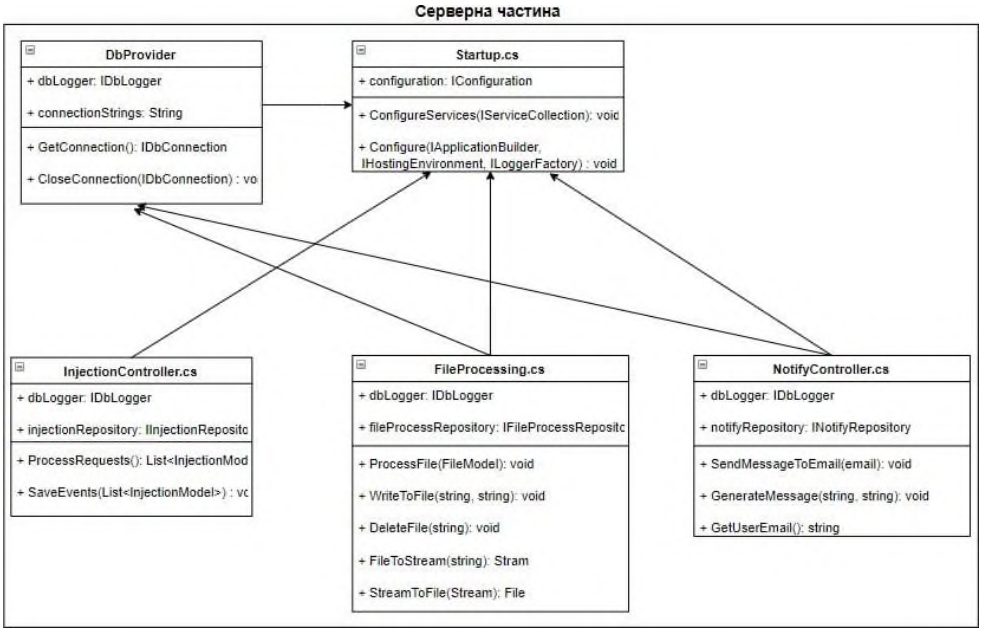
83. Time series forecasting using a hybrid ARIMA and neural network model. URL: https://www.sciencedirect.com/science/article/abs/pii/S0925231201007020

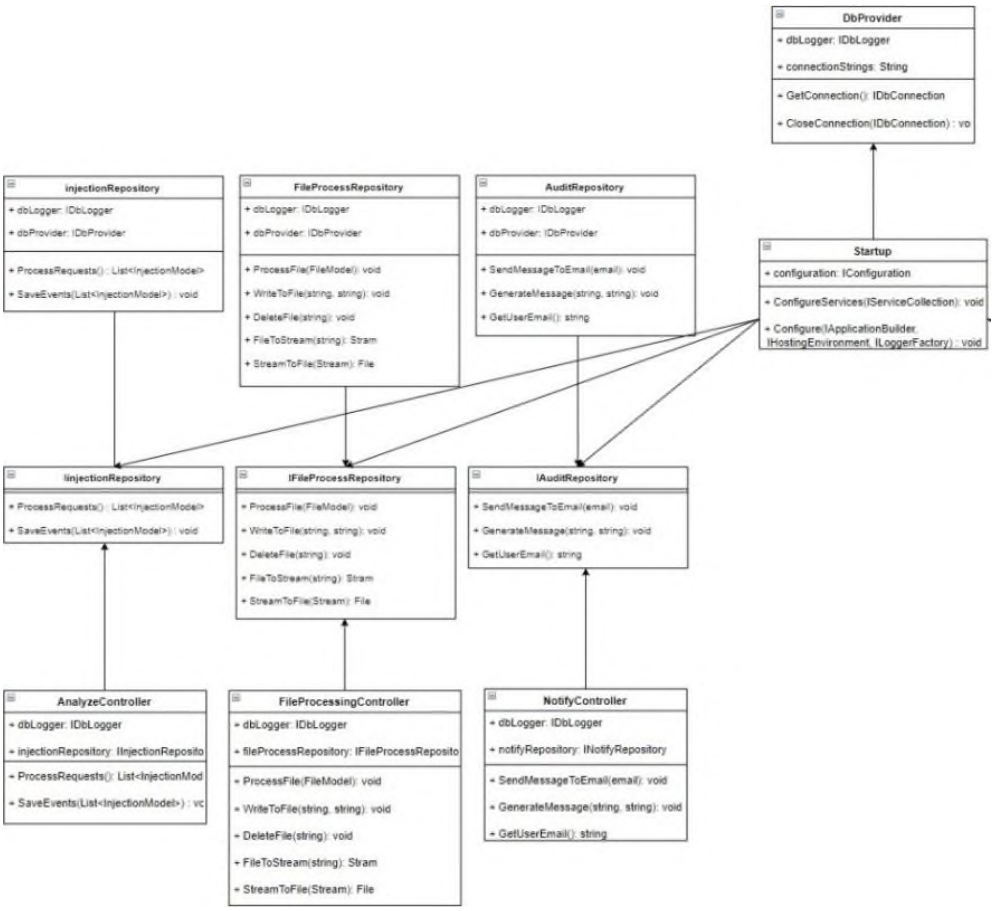
84. Usability Determination Using Multistage Fuzzy System. Sciencedirect: web–site. URL: https://www.sciencedirect.com/science/article/pii/S1842 (дата звернення: 08.12.2025).

ДОДАТКИ

Додаток А

Діаграма компонентів засобу моніторингу





Магістерська кваліфікаційна робота

Методи моніторингу та аналізу мережевого трафіку для виявлення аномалій у телекомунікаційних системах

Виконав: студент гр. ТСДМ-62, Гузій Кирило Володимирович

Керівник: доц. Гринкевич Г.О.

Актуальність теми

- Стрімке зростання обсягів трафіку в 5G/6G мережах.
- Ускладнення кіберзагроз (DDoS, 0-day атаки).
- Необхідність переходу від статичних екранів до динамічного аналізу аномалій.





Проблематика

- Експоненціальне зростання трафіку в ТКС ускладнює виявлення цілеспрямованих атак (APT).
- Обмеженість сигнатурних методів перед загрозами «нульового дня» (0-day).
- Необхідність мінімізації помилкових спрацювань (False Positive) у високонавантажених мережах.

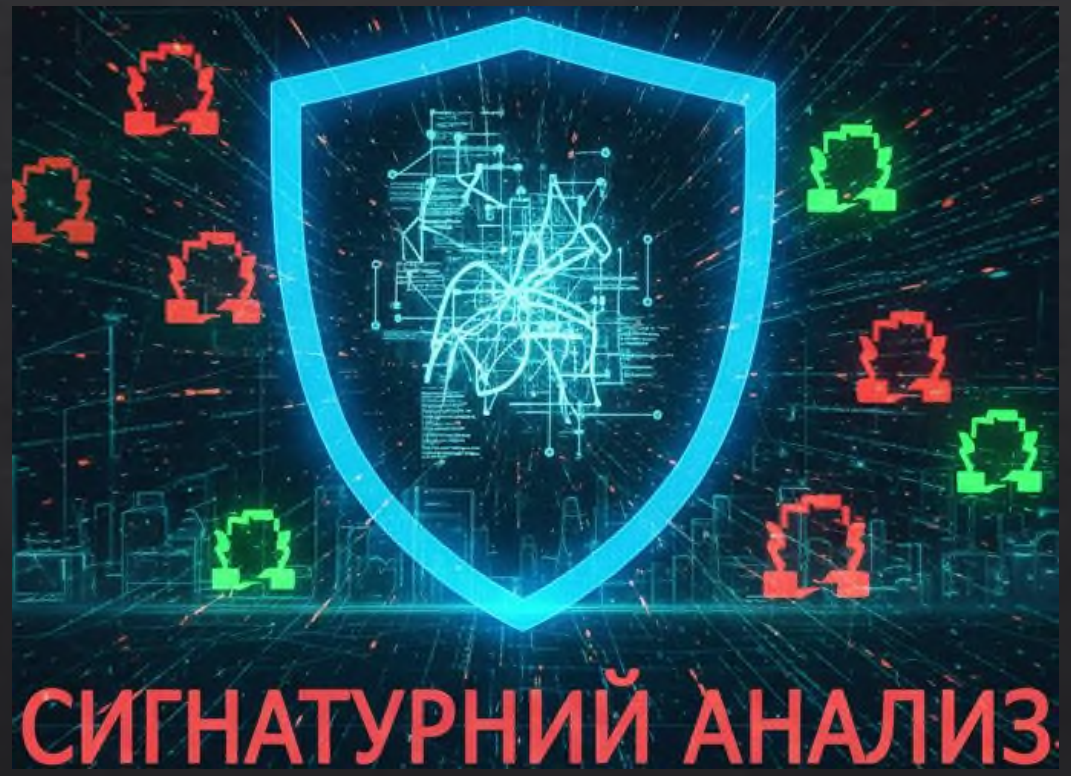


Мета: Розробка гібридної системи виявлення аномалій, що поєднує сигнатурний та статистичний аналіз.

1. Аналіз методів збору даних (NetFlow, DPI).
2. Порівняння IDS/IPS систем.
3. Створення прототипу на Python.
4. Тестування системи на реальних сценаріях.

Класифікація методів виявлення аномалій

1. Сигнатурний аналіз: Висока точність для відомих атак (Suricata/Snort).
2. Статистичний аналіз: Виявлення нових аномалій (відхилення від «норми»).
3. Машинне навчання: Прогнозування поведінки трафіку.



Інструменти

Wireshark (аналіз)



Zeek (логіювання)



Suricata (виявлення в реальному часі).



Архітектура запропонованої системи

- Джерело трафіку (Мережевий інтерфейс).
- Модуль захоплення (Scapy / Libpcap).
- Ядро аналізу (Suricata IDS).
- Візуалізація (ELK Stack: Elasticsearch, Kibana).

Практична реалізація

Бібліотеки: Scapy (маніпуляція пакетами)



Середовище: Linux (Ubuntu)



Pandas (аналіз логів)



Docker для розгортання компонентів



Тестування системи
Сценарій 1: Сканування портів

Використання Nmap для виявлення відкритих портів.




```
~ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-16 12:59 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.081s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
53/tcp    open     domain
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
9929/tcp  open     nping-echo
31337/tcp open     Elite

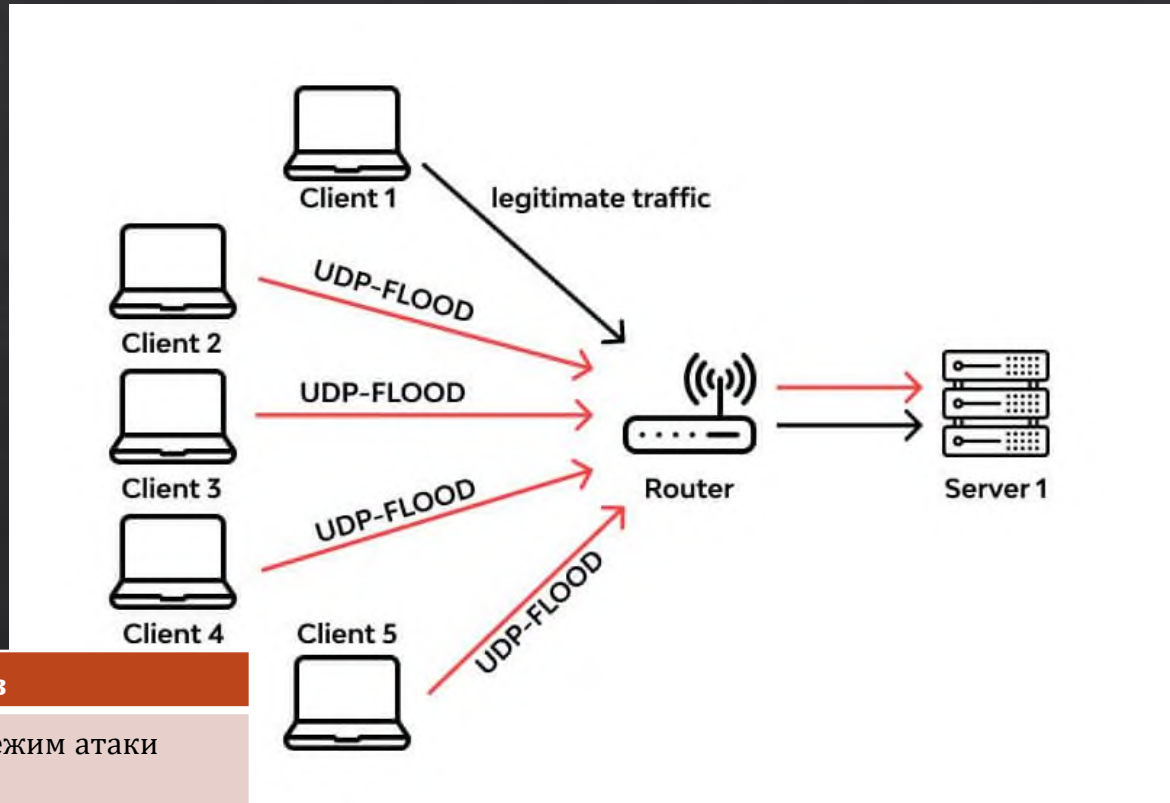
Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds
```

Команда: sudo nmap -sS scanme.nmap.org (сканування за допомогою SYN-пакетів).

Результат: список відкритих портів (SSH, HTTP, DNS), їхній статус та назви сервісів.

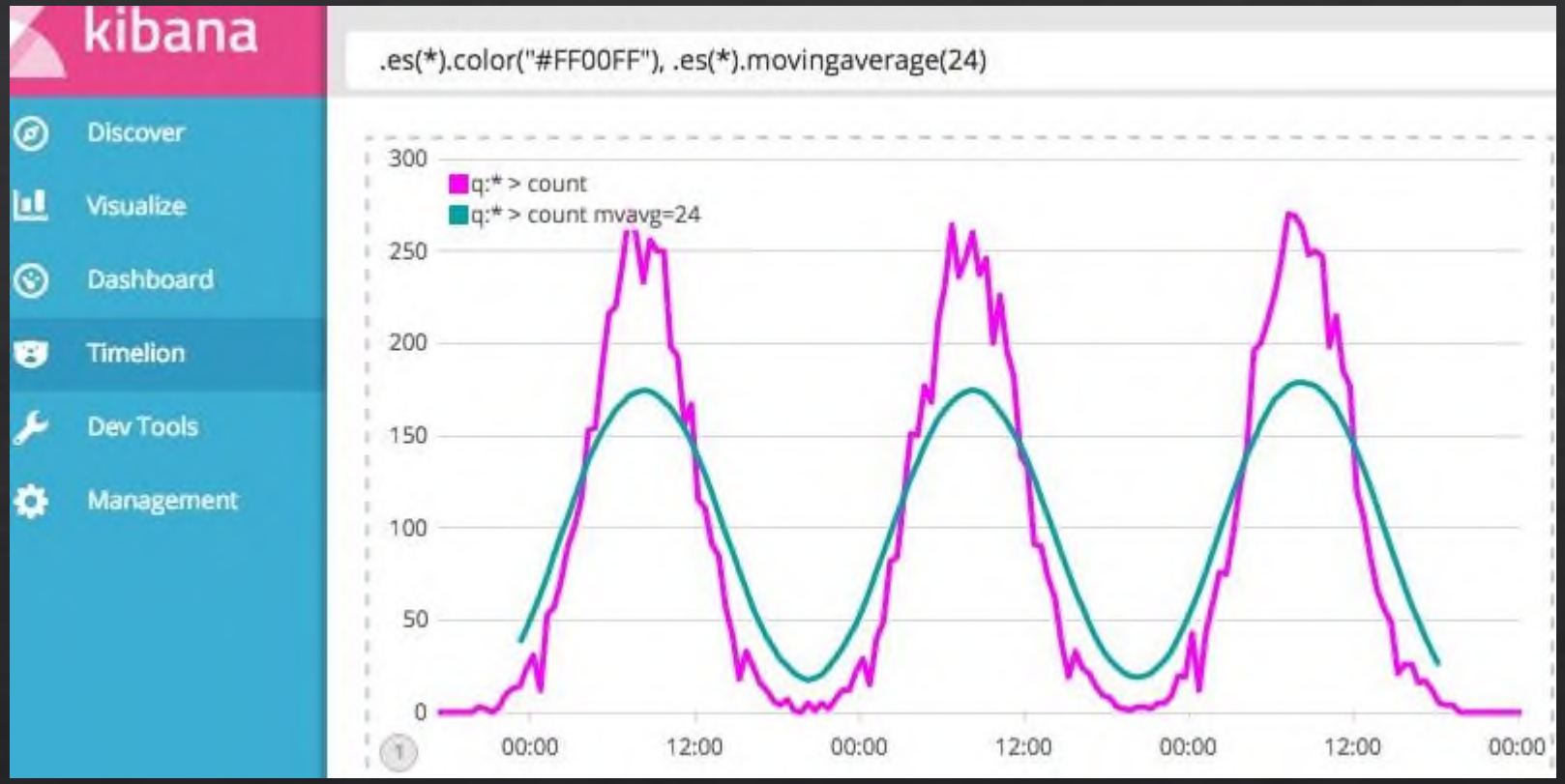
Тестування системи
Сценарій 2: DoS-атака

Імітація масової відправки пакетів (ICMP Flood)



№ послідовності	Розмір кількість пакетів	Час передачі пакетів, хв	
		Звичайний режим	Режим атаки
1	50000	15	20
2	100000	30	35
3	150000	60	65
4	200000	75	86
5	250000	84	98

DoS-атака



Різкий стрибок активності, вихід за порогові значення.

Результати та ефективність

Зниження відсотка хибних спрацювань на 15-20%

Здатність виявляти аномалії, які не мають чітких сигнатур (за обсягом та частотою)

Висновки

- Проаналізовано теоретичні засади моніторингу трафіку.
- Розроблено та протестовано прототип гібридної системи.
- Доведено доцільність використання комбінованих методів у телекомунікаційних системах.

Дякую за увагу!