Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

# КВАЛІФІКАЦІЙНА РОБОТА

Мандрицького Богдана Олександровича

на здобуття ступеня вищої освіти Бакалавра

Система виявлення прихованих атак у приватній мережі

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ. 2102157.21.02.19 ПЗ

Виконав студент 4 курсу група КБ-21-2 Богдан МАНДРИЦЬКИЙ
Керівник докт. тех. наук, професор Михайло КАСЯНЧУК
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

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

Мандрицькому Богдану Олександровичу

1 Тема роботи Система виявлення прихованих атак у приватній мережі

Керівник роботи Михайло Касянчук

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 12.06.2025

3 Вихідні дані до роботи Актуальні дані про мережевий трафік у приватних мережах, інструменти аналізу трафіку (Scapy, Wireshark, PyShark), система виявлення аномалій, дані текстових атак, статистичні методи, Python-скрипти, візуалізаційні бібліотеки (Matplotlib, Seaborn).

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Огляд типів приватних мереж і методів атак, Аналіз сучасних систем виявлення вторгнень, Побудова моделі виявлення прихованих атак, Реалізація аналізу трафіку та виявлення аномалій, Візуалізація результатів і оцінка ефективності систем

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) «Схема моделі виявлення прихованих атак у приватній мережі», «Архітектура приватної мережі», «Схема логіки візуалізації результатів аналізу трафіку»

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

| Назва етапів (розділів) кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|
| Вибір і затвердження теми кваліфікаційної роботи | Лютий | |
| Ознайомлення з предметною областю | Лютий | |
| Дослідження існуючих рішень | Лютий | |
| Постановка задачі | Березень | |
| Визначення загальних принципів реалізації системи виявлення атак | Березень | |
| Деталізація технічного підходу (вибір інструментів, аналіз Scapy, PyShark) | Квітень | |
| Розробка програмного прототипу системи | Квітень | |
| Апробація проєктних рішень (тестування, виявлення аномалій, візуалізація) | Травень | |
| Оформлення пояснювальної записки згідно вимог | Травень | |
| Оформлення графічної частини | Червень | |
| Захист КР | Червень | |

Студент _____ Богдан МАНДРИЦЬКИЙ

Керівник кваліфікаційної роботи _____ Михайло КАСЯНЧУК

# АНОТАЦІЯ

Тема кваліфікаційної роботи: Система виявлення прихованих атак у приватній мережі.

Автор роботи: Мандрицький Богдан Олександрович.

Керівник роботи: Касянчук Михайло Миколайович.

Пояснювальна записка: 62 с., 2 додатки, 9 рисунків,1 таблиця,40 джерел.

Графічна частина: 3 плакати.

КІБЕРБЕЗПЕКА, ВИЯВЛЕННЯ АТАК, АНАЛІЗ ТРАФІКУ, ПРИВАТНІ МЕРЕЖІ, АНАЛІЗ ВРАЗЛИВОСТЕЙ, МОНІТОРИНГ, ТЕСТУВАННЯ.

Кваліфікаційна робота присвячена розробці системи виявлення прихованих атак у приватній мережі. У роботі проаналізовано основні типи атак, що загрожують приватним мережам, розглянуто сучасні методи їх виявлення та проаналізовано існуючі рішення у сфері кібербезпеки.

У результаті дослідження було розроблено модель системи виявлення атак, що ґрунтується на автоматизованому моніторингу трафіку мережі. Запропонований метод передбачає аналіз трафіку, виявлення аномалій та оцінку загроз. Проведено тестування та оцінку достовірності системи в реальному середовищі, що підтвердило її працездатність і здатність ефективно ідентифікувати потенційні.

10 .06 .2025 _____

# ABSTRACT

Bachelor's Thesis Topic: Hidden Attack Detection System in a Private Network.

Author: Bohdan Mandrytskyi Oleksandrovych.

Head of work: Kasianchuk Mykhailo Mykolayovych.

Explanatory note:62 p., 2 appendices,9 figures,1 table, 40 sources

Graphic part: posters, presentation slides.

CYBERSECURITY, ATTACK DETECTION, TRAFFIC ANALYSIS, PRIVATE NETWORKS, VULNERABILITY ANALYSIS, MONITORING, TESTING.

The bachelor's thesis is dedicated to the development of a system for detecting hidden attacks in a private network. The study analyzes the main types of attacks threatening private networks, examines modern methods of detection, and evaluates existing solutions in the field of cybersecurity.

As a result of the research, a model of an attack detection system based on automated network traffic monitoring was developed. The proposed methodology includes traffic analysis, anomaly detection, and threat assessment. Testing and evaluation of the system's effectiveness in a real environment confirmed its functionality and ability to efficiently identify potential attacks.

10.06.2025 _____

ЗМІСТ

# ВСТУП

Однією з проблем інформаційної безпеки в мережах є виявлення прихованих атак, які не мають чітких сигнатур і не проявляють себе явно. Зловмисники дедалі частіше застосовують методи обходу традиційних механізмів захисту, наприклад, використовують шифрування, обфускацію, приховані канали комунікації або малі обсяги фрагментованого трафіку, які складно виявити за допомогою звичайних фаєрволів чи антивірусів. Тому значного значення набувають системи, здатні виявляти аномалії в поведінці мережі, тобто відхилення від звичного функціонування, які можуть свідчити про потенційне вторгнення.

У цьому контексті актуальним є використання статистичних методів аналізу трафіку, які дозволяють без попередньо визначених сигнатур виявляти відхилення на основі поведінкових шаблонів. На відміну від сигнатурних систем, що орієнтовані на вже відомі загрози, системи на основі аномалій аналізують характер трафіку в часі, будують базові моделі нормальної активності й визначають потенційно підозрілі ситуації на основі статистичних змін, наприклад, збільшення кількості пакетів, нетипова частота запитів або неочікувані з'єднання з зовнішніми вузлами.

Ця кваліфікаційна робота присвячена розробці системи виявлення прихованих атак у приватній мережі. Вона спрямована на створення інструменту, здатного в реальному часі аналізувати мережевий трафік, будувати статистичну модель поведінки мережі та виявляти підозрілу активність. Однією з головних переваг запропонованого підходу є використання відкритих технологій, що дозволяє адаптувати рішення до конкретного середовища та інтегрувати його у вже наявну інфраструктуру з мінімальними витратами.

Практична цінність роботи полягає в тому, що розроблена система може бути використана у невеликих локальних мережах організацій або окремих сегментах більшої інфраструктури для базового контролю безпеки. Вона може слугувати інструментом першого рівня моніторингу, який не потребує значних

обчислювальних ресурсів, але дозволяє швидко виявляти потенційні загрози.

Структурно кваліфікаційна робота складається з трьох основних розділів. У першому розділі наведено теоретичні основи виявлення атак і класифікацію методів аналізу трафіку. У другому розділі подано опис побудови моделі виявлення аномалій, архітектури системи, її схеми роботи, принципів функціонування та візуалізації результатів. У третьому розділі розглянуто питання впровадження системи в тестове середовище, продемонстровано приклади виявлення аномальної активності, оцінено ефективність реалізованого рішення та окреслено перспективи розвитку.

Кваліфікаційна робота спрямована на вирішення актуальної проблеми інформаційної безпеки через створення практичного інструменту для виявлення аномалій у локальних мережах, що може бути застосований як окремо, так і в складі більш комплексних систем захисту.

У процесі реалізації було обрано підхід, який не потребує складної інфраструктури та може бути розгорнутий навіть на окремому хості в умовах обмежених ресурсів. Це забезпечує гнучкість і доступність системи для малого бізнесу, навчальних закладів або дослідницьких лабораторій. Запропоноване рішення дозволяє протестувати ключові концепції виявлення аномалій без необхідності у дорогому обладнанні, використовуючи лише програмні засоби на базі Python та бібліотеку Scapy. Такий підхід дає змогу оцінити практичну доцільність виявлення прихованих атак у контрольованому середовищі з перспективою подальшої масштабованості.

# 1 АНАЛІЗ НАЯВНИХ РІШЕНЬ

## 1.1 Приватні мережі

У сучасних умовах розвитку цифрових технологій приватні мережі стали основним елементом інфраструктури для забезпечення безпечного обміну даними, ефективної організації інформаційних потоків та захисту критичних ресурсів підприємств, організацій і приватних осіб. Приватні мережі дозволяють побудувати ізольоване інформаційне середовище, яке контролюється адміністратором і має обмежений доступ із зовнішнього середовища. Тут розглянуте поняття, класифікацію, архітектурні особливості, переваги, недоліки, а також потенційні загрози, притаманні приватним мережам, що є базові для теми виявлення прихованих атак.

Приватна мережа (англ. Private Network) - це комп’ютерна мережа, яка використовує приватні діапазони IP-адрес (згідно з RFC 1918) і призначена для обмеженого доступу, зазвичай всередині однієї організації. Така мережа ізольована від глобальної мережі Інтернет або підключається до неї через NAT (Network Address Translation), що забезпечує додатковий рівень захисту [1-3].

Перш за все це локальні обчислювальні мережі (LAN**)**. Базовий тип таких приватних мереж охоплює невелику географічну зону, зазвичай офіс, лабораторію, навчальний заклад або будівлю. LAN дозволяє ефективно об'єднати робочі станції, сервери, принтери та інші пристрої в єдину інфраструктуру, що забезпечує високу пропускну здатність, швидкий обмін файлами, спільний доступ до ресурсів і централізоване управління. LAN реалізується на основі дротових або бездротових технологій, має просту топологію і високий рівень внутрішньої безпеки за рахунок фізичної ізоляції [4].

Ще одним типом є корпоративні мережі (Enterprise Networks). Великомасштабні, складні та ієрархічно побудовані мережі, які з'єднують офіси, філії, виробничі об'єкти, дата-центри та хмарні платформи в єдину інформаційну систему. Такі мережі підтримують різноманітні рівні доступу, забезпечують балансування навантаження, відмовостійкість, контроль політик безпеки та

централізоване логування. У корпоративних мережах активно використовуються MPLS, VLAN, VPN, фаєрволи, системи моніторингу та інші засоби, що дозволяють досягати високого рівня керованості та масштабованості [5-6].

Також прикладом віртуальних мереж є віртуальні приватні мережі (VPN). Ці логічні мережі створюють захищені канали (тунелі) через публічні мережі, переважно Інтернет, для забезпечення безпечного віддаленого з'єднання користувачів або філій з основною приватною мережею. VPN використовують криптографічні протоколи, такі як IPSec, SSL/TLS, OpenVPN для шифрування трафіку, аутентифікації та цілісності даних. Основна перевага VPN - це можливість розширення приватної мережі на географічно віддалені вузли без значного збільшення вартості інфраструктури. Застосовується як для індивідуальних користувачів, так і для міжмережевого з'єднання корпоративного рівня. На рисунку 1.1 зображено класифікацію приватних мереж.

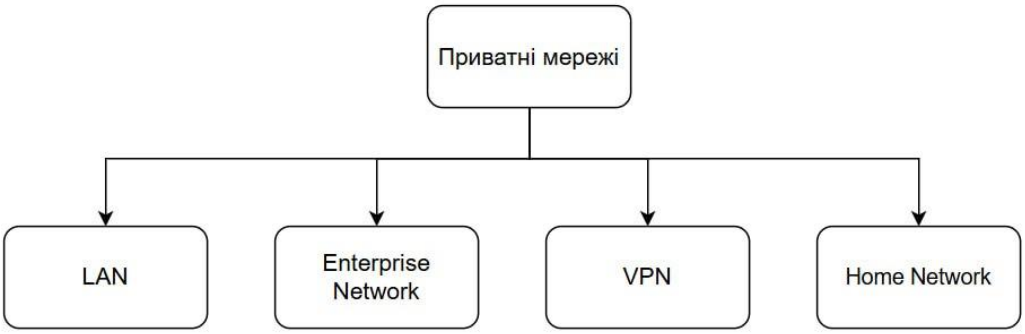



Рисунок 1.1 – Класифікація приватних мереж

Домашні мережі - це невеликі приватні мережі, призначені для побутового використання в межах житлового приміщення. Типово включають маршрутизатор, до якого підключені персональні комп'ютери, ноутбуки, смартфони, телевізори, IoT-пристрої та принтери. Домашні мережі реалізуються переважно через Wi-Fi та Ethernet, використовують приватні IP-адреси та NAT, а також прості механізми шифрування WPA2/WPA3. Попри обмеженість у масштабах, ці мережі також є вразливими до атак, через слабке налаштування безпеки користувачем або вразливості IoT-пристроїв [7].

Архітектура приватних мереж визначається масштабом, призначенням та рівнем безпеки конкретної системи. Як правило, до складу такої мережі входять клієнтські пристрої (робочі станції, смартфони, принтери), інфраструктура передачі даних (комутатори, маршрутизатори, точки доступу), серверні ресурси (бази даних, файлові сервери, контролери домену), а також засоби безпеки (фаєрволи, IDS/IPS-системи, проксі-сервери). Взаємодія всіх цих компонентів відбувається відповідно до моделі OSI або TCP/IP, де на фізичному та канальному рівнях реалізується передача даних, на мережевому рівні здійснюється маршрутизація, на транспортному забезпечується контроль цілісності даних, а на прикладному надається доступ до сервісів. На рисунку 1.2 зображено архітектуру приватної мережі.

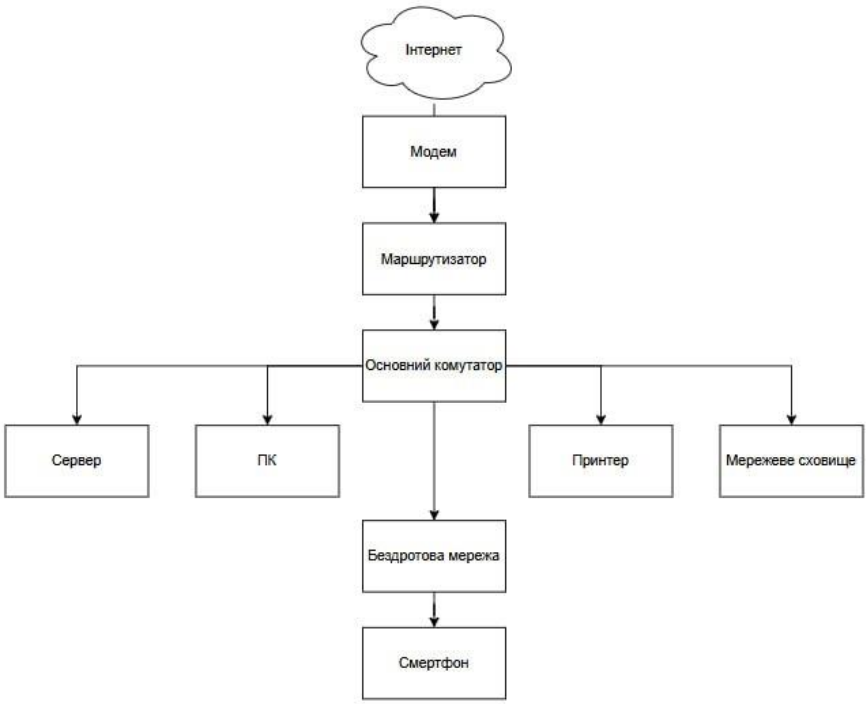



Рисунок 1.2 – Архітектура приватної мережі

Серед основних переваг приватних мереж можна виділити високий рівень безпеки, оскільки відсутність прямого доступу з Інтернету значно знижує ризик зовнішніх атак. Також важливою перевагою є повний контроль з боку

адміністратора над усіма вузлами та політиками безпеки. Передача даних у межах локальної інфраструктури відбувається значно швидше, ніж у публічних мережах, що позитивно впливає на продуктивність. Крім того, приватні мережі дозволяють реалізувати кастомізовану конфігурацію та гнучке управління доступом відповідно до потреб організації.

Разом із тим, приватні мережі мають і певні недоліки. Їхня ізольованість ускладнює інтеграцію з хмарними сервісами та реалізацію віддаленого доступу. Підтримка та обслуговування такої інфраструктури потребують наявності кваліфікованого IT-персоналу, що призводить до збільшення витрат. Внутрішня безпека також не є абсолютною можливі загрози зсередини, зокрема інсайдерські атаки або підключення заражених пристроїв. Крім того, у випадку розширення приватної мережі виникають труднощі з масштабуванням, що вимагає додаткових ресурсів і ретельного планування.

Загрози у приватних мережах залишаються актуальними навіть попри їхню ізольованість від загальнодоступного Інтернету. Обмежений доступ не гарантує повної безпеки, оскільки загрози можуть виникати як ззовні, так і зсередини самої мережі. Однією з найсерйозніших є інсайдерські атаки, коли зловмисні дії здійснюють особи, які мають легітимний доступ до системи - це можуть бути співробітники, підрядники чи інші користувачі з правами доступу. Вони можуть свідомо чи несвідомо викрасти конфіденційну інформацію, внести шкідливі зміни або передати доступ третім особам.

Ще однією поширеною загрозою є міжмережеве сканування, яке передбачає виявлення відкритих портів, служб або активних вузлів у мережі з метою ідентифікації вразливих точок для подальшого проникнення. Така активність зазвичай передує цілеспрямованим атакам і використовується для збору розвідувальної інформації про мережеву інфраструктуру.

ARP-спуфінг становить небезпеку на канальному рівні. Цей тип атаки полягає в підміні MAC-адрес, унаслідок чого зловмисник отримує можливість перехоплювати, змінювати або перенаправляти трафік між вузлами мережі. Це дозволяє проводити атаки типу "людина посередині" (MITM), які є вкрай

небезпечними в середовищі внутрішньої мережі [8-9].

Не менш критичною є загроза DNS-спуфінгу, яка полягає в підміні відповідей DNS-сервера. Зловмисник надсилає фальшиві відповіді на DNS-запити, спрямовуючи користувача на фальшиві або шкідливі ресурси. Це може призвести до компрометації облікових даних, встановлення шкідливого програмного забезпечення або викрадення конфіденційної інформації [10].

Ще однією формою загроз є зловмисне програмне забезпечення, включаючи віруси, трояни, руткіти та інші шкідливі компоненти, які можуть проникати у приватну мережу через вразливості в програмному забезпеченні, несанкціоноване підключення пристроїв або через соціальну інженерію. Таке ПЗ може залишатися непоміченим тривалий час, збираючи інформацію, змінюючи конфігурації або виконуючи шкідливі інструкції.

Окрему загрозу становить фішинг через локальні сервіси, коли зловмисники створюють підроблені внутрішні веб-сайти, служби чи інтерфейси доступу, що візуально імітують справжні ресурси. Метою таких дій є викрадення облікових даних користувачів або введення їх в оману для отримання критично важливої інформації.

Відповідно, приватні мережі, хоча й менш уразливі до зовнішніх атак, потребують не менш ретельного захисту. Внутрішні загрози, складність виявлення аномальної поведінки та високий рівень довіри до внутрішніх вузлів роблять ці мережі потенційно небезпечним середовищем при відсутності належного моніторингу та заходів безпеки.

Проблематика виявлення атак у приватних мережах полягає в тому, що більшість загроз у такому середовищі складно ідентифікувати через їхню схожість із легітимною мережею активністю. Це актуально у випадках, коли атаки здійснюють інсайдери або скомпрометовані пристрої, які вже мають дозволений доступ до системи та не викликають підозри з боку традиційних механізмів безпеки. Системи виявлення та запобігання вторгненням (IDS/IPS), як правило, орієнтовані на аналіз зовнішнього трафіку, і тому можуть мати обмежену ефективність у межах внутрішнього сегмента, де події відбуваються

поза їхньою основною зоною контролю [11].

Серед основних труднощів, що ускладнюють виявлення атак у приватних мережах, варто виокремити кілька специфічних чинників. По-перше, велика кількість подій, що генерується численними сервісами, пристроями та додатками, створює значний обсяг мережевого «шуму». У такому потоці даних стає надзвичайно складно вирізнити справжні аномалії або підозрілу активність, без використання систем аналізу поведінки або машинного навчання.

Другою важливою проблемою є шифрування трафіку, яке стало стандартною практикою для забезпечення конфіденційності. Проте це також значно ускладнює глибокий аналіз вмісту переданих пакетів, оскільки IDS/IPS більше не мають доступу до «начинки» трафіку і можуть виявляти лише метадані або шаблони з’єднань, що знижує точність виявлення.

Ще одна складність динамічна топологія приватних мереж. Постійна поява нових пристроїв, зміна IP-адрес, переміщення користувачів між сегментами або точками доступу вимагають постійного оновлення політик, правил безпеки та сигнатур. Відсутність своєчасного реагування може призвести до появи «сліпих зон» у мережі, які легко використовуються зловмисниками.

Також серйозною перешкодою є відсутність централізованого логування у багатьох приватних мережах. Коли події фіксуються лише локально на окремих пристроях, стає надзвичайно важко здійснити кореляцію подій, простежити ланцюжок атаки або вчасно виявити координовані дії зловмисника. Це критично для великих або розподілених мереж, де без систем централізованого моніторингу (SIEM) або журналювання можна пропустити ключові індикатори компрометації [12].

У сукупності всі ці фактори свідчать про те, що для ефективного захисту приватних мереж потрібен комплексний підхід: від впровадження сучасних систем моніторингу до регулярного оновлення політик безпеки, розширеного аналізу поведінки користувачів та автоматизації реагування на інциденти.

Приватні мережі відіграють фундаментальну роль у побудові стратегії захисту інформаційних систем. Вони забезпечують першу лінію оборони

шляхом фізичної або логічної ізоляції критичних ресурсів, створюють можливості для впровадження політик доступу, сегментації, обмеження трафіку та контролю взаємодії між елементами мережі.

У рамках виявлення прихованих атак приватні мережі потребують спеціалізованих засобів моніторингу, які враховують специфіку внутрішніх процесів, дозволяють аналізувати поведінку користувачів і пристроїв, а також виявляти нетипові або аномальні дії. Саме це обґрунтовує актуальність розробки спеціалізованих рішень, які будуть розглянуті у наступних підрозділах.

Розуміння особливостей приватних мереж, їхньої архітектури, вразливостей і типових загроз є основою для створення ефективної системи виявлення прихованих атак, що є темою цієї кваліфікаційної роботи.

## 1.2 Поширені типи атак

Із розвитком інформаційних технологій та зростанням обсягів переданої інформації через приватні мережі, зловмисники дедалі активніше розробляють і застосовують різноманітні типи атак, спрямованих на порушення цілісності, доступності та конфіденційності даних. Хоча приватні мережі ізольовані від публічного Інтернету або мають обмежений доступ до нього, це не робить їх повністю безпечними. Існує безліч сценаріїв, за яких приватна мережа може стати об’єктом цілеспрямованої або випадкової атаки.

Атаки на приватні мережі мають різноманітну природу та можуть реалізовуватись через широкий спектр векторів. Залежно від джерела, методів реалізації та цільового рівня мережевої інфраструктури, їх можна систематизувати за кількома базовими критеріями. Така класифікація є важливою для розуміння специфіки загроз та розробки ефективних механізмів їх виявлення і протидії.

Одним із фундаментальних підходів до класифікації є розмежування атак за їхнім походженням: зовнішні атаки здійснюються з поза меж внутрішньої

мережі. Здебільшого вони надходять із Інтернету або через інші відкриті комунікаційні інтерфейси. Такі атаки мають на меті прорвати периметр безпеки, експлуатуючи вразливості в маршрутизаторах, фаєрволах, сервісах віддаленого доступу або веб-додатках, відкритих ззовні. Прикладами є DoS-атаки, сканування портів, експлуатація веб-вразливостей.

Внутрішні атаки ініційовані з середини мережі, тобто з боку користувачів, які мають легітимний або тимчасовий доступ до ресурсів. Це можуть бути співробітники, технічний персонал, або пристрої, що вже були заражені шкідливим програмним забезпеченням. Внутрішні атаки є небезпечними через високу ймовірність обходу звичайних засобів контролю, оскільки дії зловмисника часто маскуються під типову активність. Залежно від характеру втручання, атаки можуть бути активними або пасивними. Активні атаки передбачають активне втручання в роботу системи. Зловмисник намагається змінити, знищити або підробити інформацію, вплинути на поведінку мережі, ініціювати перехоплення чи підміну сеансу зв’язку, або впровадити зловмисний код. Такі дії зазвичай мають явний вплив на цілісність чи доступність системи. Наприклад, це може бути атака типу ARP-спуфінг, DoS, SQL-ін’єкція або викрадення сесій [14].

Пасивні атаки здійснюються без безпосереднього втручання у трафік або системні ресурси. Їх метою є збір інформації для подальших атак або викрадення конфіденційних даних. При цьому мережа не зазнає змін, і тому такі атаки складніше виявити. Прикладами є прослуховування трафіку (sniffing), аналіз метаданих, визначення топології мережі, збирання даних про MAC-адреси, IP-структуру тощо.

Інформаційні атаки можуть реалізовуватися на різних рівнях моделі OSI (Open Systems Interconnection), яка поділяє мережеву взаємодію на сім функціональних рівнів. Кожен з них має власні типи вразливостей і відповідно - типові атаки. На фізичному рівні (Physical Layer), що охоплює апаратні засоби (кабелі, порти, мережеві інтерфейси), атаки включають фізичне відключення пристроїв, підключення несанкціонованих засобів перехоплення, створення

електромагнітних перешкод або блокування каналів передачі. На канальному рівні (Data Link Layer), відповідальному за передачу даних у межах одного сегменту мережі, поширеними є маніпуляції з MAC-адресами, ARP-спуфінг, MAC-flooding (переповнення таблиць комутаторів), VLAN hopping (несанкціоноване переміщення між сегментами мережі). Ці дії дозволяють зловмиснику перехоплювати або перенаправляти трафік. [15-16]

На мережевому рівні (Network Layer), який відповідає за маршрутизацію пакетів між вузлами, актуальні загрози включають IP-спуфінг, ICMP-атаки, DoS-атаки, а також зловживання протоколами маршрутизації з метою впливу на напрямок трафіку або виведення з ладу вузлів. На транспортному рівні (Transport Layer), що забезпечує надійну передачу даних, поширеними є TCP-сесійні атаки, сканування портів, маніпуляції з номерами послідовності, надсилання фрагментованих пакетів. На сеансовому рівні (Session Layer), відповідальному за встановлення і підтримку сеансів, можуть здійснюватись атаки на викрадення сесій, підміну токенів чи повторне використання активних з'єднань без повторної автентифікації. Представницький рівень (Presentation Layer), який забезпечує форматування та шифрування даних, також піддається атакам через експлуатацію вразливостей у бібліотеках обробки файлів чи обхід механізмів шифрування. Нарешті, на прикладному рівні (Application Layer), де працюють основні сервіси (веб-додатки, пошта, бази даних), реалізується найбільша кількість атак від SQL-ін'єкцій, XSS та CSRF до фішингу, крадіжки токенів автентифікації, викрадення куків тощо [18].

Класифікація атак дозволяє краще зрозуміти природу загроз, які виникають у приватних мережах, та вибудовувати захисну стратегію з урахуванням багаторівневої моделі. У рамках безпеки критично важливо не лише виявляти окремі атаки, а й передбачати можливість їх комбінованого використання у межах складних, багатоступеневих сценаріїв. Саме тому системи моніторингу та виявлення загроз повинні охоплювати всі рівні моделі OSI та взаємодіяти з іншими компонентами інфраструктури безпеки.

Одними з найнебезпечніших залишаються інсайдерські атаки, коли

зловмисник уже має легітимний доступ до внутрішньої мережі. Це може бути співробітник компанії, підрядник або навіть гість, який тимчасово під'єднується до мережі. Основна небезпека таких атак полягає у тому, що вони часто залишаються непомітними для звичайних засобів безпеки, оскільки дії інсайдера виглядають законними. Типові дії інсайдерів включають: збір конфіденційної інформації; крадіжку облікових даних або токенів доступу; встановлення бекдорів або шпигунського ПЗ; навмисне знищення або зміна даних; перенаправлення трафіку на зовнішні сервери [13].

Зловмисники часто використовують методи соціальної інженерії для отримання початкового доступу до системи. Це можуть бути фішингові листи, телефонні дзвінки під виглядом служби підтримки, або підроблені сайти.

У приватних мережах соціальна інженерія часто спрямована на: отримання логінів і паролів для внутрішніх сервісів; переконання співробітників виконати певні дії (наприклад, підключити заражений флеш-накопичувач); отримання конфіденційної інформації шляхом обману.

ARP-спуфінг - атака на канальному рівні, коли зловмисник підміняє MAC-адресу у таблиці ARP жертви, змушуючи її відправляти трафік на пристрій атакуючого. Це дозволяє перехоплювати, змінювати або переспрямовувати трафік між пристроями в межах приватної мережі. Такий тип атаки є небезпечним у локальних мережах (LAN), де ARP-запити використовуються для маршрутизації всередині сегмента [17].

DNS-спуфінг це атака на рівні системи доменних імен, під час якої зловмисник підробляє відповіді DNS-серверів. Унаслідок цього запити на легітимні адреси (наприклад, внутрішній ресурс компанії) можуть бути перенаправлені на фальшиві сайти, які збирають облікові дані або розповсюджують шкідливе ПЗ.

У цій атаці зловмисник надсилає пакети, які мають підроблену IP-адресу відправника, щоб обійти механізми фільтрації або маскувати своє реальне місцезнаходження. IP-спуфінг часто є підготовчим етапом до більш складних атак, таких як DoS або TCP-сесійні викрадення.

Sniffing - пасивна атака, під час якої зловмисник зчитує трафік, що передається мережею. У незашифрованих приватних мережах це дозволяє отримати паролі, особисту інформацію, фінансові дані тощо. вразливими є мережі Wi-Fi без належного захисту [19].

MITM-атаки передбачають перехоплення трафіку між двома сторонами без їхнього відома. Зловмисник може не тільки слухати трафік, а й змінювати його в реальному часі. Це дозволяє реалізовувати фішинг, перехоплення сесій, зміну транзакцій, тощо. У приватних мережах MITM часто здійснюється через ARP- або DNS-спуфінг.

Навіть у відносно закритих мережах DoS-атаки можуть бути серйозною загрозою. Їх мета вивести з ладу певні сервіси шляхом перевантаження мережевими запитами або некоректними пакетами. У великих корпоративних мережах DDoS-атаки можуть бути здійснені через ботнети, до яких вже підключені заражені пристрої з внутрішньої інфраструктури [20].

Ці атаки полягають у багаторазовому підборі пароля до облікового запису. Навіть у внутрішній мережі, де ресурси здаються захищеними, слабкі паролі дозволяють швидко отримати доступ до критичних елементів. Наприклад, адмін-консолі, веб-інтерфейси NAS-серверів чи роутерів [21].

Мережі можуть бути заражені шкідливими програмами через флешки, підключення до зовнішніх пристроїв або через компрометовані програми. Найпоширеніші типи:

- трояни (дають віддалений доступ до системи);
- кейлогери (записують натискання клавіш);
- руткіти (приховують свою присутність);
- шифрувальники (блокують доступ до файлів, вимагаючи викуп).

Часто пристрої в приватних мережах використовують застаріле програмне забезпечення або прошивки. Зловмисники можуть скористатися відомими вразливостями (наприклад, EternalBlue у Windows) для проникнення в систему або підвищення своїх привілеїв [22-23].

У приватних мережах використовуються різноманітні протоколи

автентифікації Kerberos, NTLM, LDAP тощо. У разі їхньої неправильної конфігурації зловмисник може: захопити хеші паролів; реалізувати атаки Pass-the-Hash або Pass-the-Ticket; підробити токени доступу [24].

Зі зростанням популярності «розумних» пристроїв у корпоративних і домашніх мережах з'являються нові вектори атак. IoT-пристрої часто мають: відкриті порти; типові логіни/паролі; відсутність шифрування [25].

## 1.3 Аналіз наявних рішень

У сучасних умовах стрімкого розвитку інформаційних технологій та зростання кіберзагроз, питання захисту інформаційної інфраструктури приватних мереж набуває критичного значення. Система виявлення прихованих атак є важливою складовою комплексної безпеки організацій, оскільки забезпечує можливість своєчасного реагування на інциденти, які можуть залишатися непоміченими тривалий час.

Серед найбільш розповсюджених рішень, що використовуються для виявлення атак, виділяють системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), засоби аналізу поведінки користувачів і пристроїв (UEBA), платформи централізованого журналювання та кореляції подій (SIEM), а також рішення на основі штучного інтелекту (AI/ML). Кожна з цих категорій має власні принципи роботи, що визначають їхню ефективність у конкретних контекстах [26].

IDS-системи (Intrusion Detection Systems) є основою традиційного моніторингу мережевої безпеки. Вони здійснюють аналіз трафіку або подій на предмет наявності сигнатур відомих атак або відхилень від очікуваної поведінки. Найбільш відомими прикладами таких систем є Snort, Suricata, Zeek та OSSEC. Snort, як одна з перших відкритих IDS-платформ, застосовує сигнатурний підхід порівнює вхідні пакети з базою відомих шаблонів атак. Цей метод дозволяє ефективно виявляти вже відомі загрози, однак є вразливим до нових або

модифікованих атак, які не відповідають наявним сигнатурам. Suricata доповнює сигнатурний підхід можливістю аналізу потоків та багатопотоковою обробкою, що дозволяє підвищити продуктивність у великих мережах. Zeek, на відміну від класичних IDS, орієнтується на аналіз протоколів і моделювання подій, що дозволяє глибше розуміти контекст подій у мережі, але потребує високої кваліфікації для налаштування та підтримки. Загальною слабкою стороною IDS є обмежена ефективність у виявленні прихованих, зокрема інсайдерських атак, оскільки останні часто не супроводжуються характерними шаблонами [27-28].

IPS-системи (Intrusion Prevention Systems) - це логічне розширення IDS із додатковою функціональністю блокування загроз у реальному часі. Приклади включають Cisco Firepower, Fortinet FortiGate, Palo Alto Networks NGFW. Ці рішення зазвичай інтегруються з фаєрволами і працюють на основі сигнатур, евристик або статистичного аналізу. Основна перевага IPS - можливість автоматичного реагування, що забезпечує проактивний захист. Проте у випадку з прихованими атаками, зокрема у внутрішньому сегменті мережі, IPS можуть демонструвати нижчу ефективність через недоступність повного трафіку або відсутність контексту щодо поведінки внутрішніх користувачів [29].

Більш гнучким і сучасним підходом є використання систем типу UEBA (User and Entity Behavior Analytics). Ці системи орієнтовані не на фіксацію технічних ознак атак, а на моделювання та виявлення відхилень у поведінці користувачів і пристроїв. UEBA-інструменти, такі як Exabeam, Varonis, Splunk UEBA, Microsoft Defender for Identity, використовують машинне навчання для створення профілів нормальної активності та виявлення аномалій. Наприклад, якщо користувач, який зазвичай працює в офісі з 9 до 18, раптово починає масово завантажувати файли опівночі, система позначить це як потенційно шкідливу активність. UEBA ефективна для виявлення інсайдерських загроз, атак типу "живлення зсередини" (living off the land), та атак без використання шкідливого ПЗ (fileless). Основним недоліком UEBA є висока вартість впровадження, складність навчання моделей і ймовірність хибнопозитивних спрацювань на початкових етапах [30-31].

Комплексним рішенням є впровадження SIEM-платформ (Security Information and Event Management), таких як Splunk, IBM QRadar, ArcSight, LogRhythm. Вони здійснюють централізоване збирання, зберігання, нормалізацію та аналіз логів з різноманітних джерел: серверів, мережевого обладнання, прикладного ПЗ, кінцевих точок.

SIEM дозволяють корелювати події за часовими мітками, джерелами, активними обліковими записами тощо, і виявляти складні атаки, які проходять через кілька етапів. Вони часто використовуються у поєднанні з SOAR-системами (Security Orchestration, Automation and Response) для автоматизації реагування. Проте ефективність SIEM залежить від якості вхідних даних, своєчасного оновлення правил кореляції та здатності персоналу інтерпретувати результати. У випадку з прихованими атаками, SIEM може виявити інцидент лише тоді, коли вже наявна достатня кількість ознак компрометації.

Новітнім напрямом є застосування рішень, заснованих на штучному інтелекті, зокрема методів машинного навчання, глибокого навчання та нейромереж. Такі системи здатні навчатися на реальних даних, виділяти латентні закономірності у поведінці трафіку, моделювати статистичні відхилення без потреби в ручному конфігуруванні сигнатур або правил. Наприклад, Darktrace використовує власну платформу на основі AI, яка моделює "імунну систему" організації і адаптивно реагує на аномалії.

Подібні рішення демонструють хороші результати у виявленні zero-day атак, складних APT-кампаній, активностей ботнетів і повільних розвідок. Але вони потребують потужних обчислювальних ресурсів, великих обсягів історичних даних, а також спеціалістів для обслуговування моделі. У внутрішніх мережах із великою кількістю змінних факторів існує ризик як пропущених загроз, так і хибних тривог.

Також заслуговують уваги рішення на рівні кінцевих точок (EDR - Endpoint Detection and Response), такі як CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint. Вони забезпечують детальний моніторинг активності на комп’ютерах користувачів і серверах: зміни в реєстрі, запуск процесів,

з’єднання, запис файлів, підозрілі сценарії тощо. В умовах приватної мережі EDR може бути головним засобом для виявлення внутрішніх атак, тих, які не генерують нетиповий мережевий трафік. Проте, ефективність EDR напряму залежить від повного покриття інфраструктури, а також здатності централізовано керувати та корелювати дані з інших джерел.

Варто зазначити, що більшість сучасних платформ безпеки прагнуть до інтеграції в єдину екосистему - наприклад, Microsoft пропонує пов’язану архітектуру між Defender, Azure Sentinel, Intune, що дозволяє забезпечити наскрізну видимість усіх рівнів від мережі до кінцевих точок. Такий підхід дозволяє підвищити ефективність виявлення прихованих атак за рахунок об'єднання контексту з різних джерел, проте водночас створює залежність від одного постачальника технологій.

У загальному, жодне з існуючих рішень не забезпечує абсолютного виявлення всіх можливих загроз, тих, що мають складну, багатоступеневу структуру, або здійснюються інсайдерами. Це зумовлює необхідність поєднання кількох підходів у межах гібридної архітектури безпеки. Сучасна тенденція полягає в інтеграції SIEM, UEBA, IDS/IPS і EDR з компонентами машинного навчання, оркестрації реакцій (SOAR), а також побудові моделей загроз на основі TTP (Tactics, Techniques and Procedures), описаних у фреймворку MITRE ATT&CK.

Аналіз наявних рішень свідчить про наявність значного арсеналу інструментів для виявлення атак у приватних мережах. Проте їх застосування потребує ретельного налаштування, контекстуалізації та координації між різними рівнями інфраструктури.

Виявлення прихованих атак є складною задачею, що вимагає поєднання технічних засобів, аналітичних моделей та висококваліфікованого персоналу. Саме тому в рамках цієї кваліфікаційної роботи пропонується розробка власної системи виявлення, орієнтованої на специфіку внутрішніх мереж і здатної враховувати їхню динаміку, особливості трафіку та поведінку користувачів.

Таблиця 1.1 - Порівняльна характеристика сучасних систем виявлення атак

| Тип системи | Метод виявлення | Опис функціонування | Приклади рішень | Переваги | Недоліки | Актуальність для виявлення прихованих атак |
|---|---|---|---|---|---|---|
| IDS | Сигнатурний та евристичний аналіз мережевого трафіку | Аналіз мережевих пакетів для виявлення шаблонів, що відповідають відомим атакам. Працює у пасивному режимі - не блокує трафік, лише повідомляє. | Snort, Zeek (Bro), Suricata | Легкість впровадження, відкритість, підтримка спільноти, простота налаштування | Не виявляє нові або нестандартні атаки | Низька |
| IPS | Сигнатурний + політики блокування | Аналогічно до IDS, але з можливістю блокування шкідливого трафіку в реальному часі. Інтегрується з фаєрволом. | Cisco Firepower, Palo Alto NGFW, Fortinet FortiGate | Активне реагування, зручна інтеграція у периметр | Обмежена ефективність проти внутрішніх загроз, складність масштабування | Середня |
| UEBA | Поведінкове моделювання на основі ML | Створює профілі поведінки користувачів і пристроїв, виявляє аномалії в активності | Exabeam, Splunk UEBA, Microsoft Defender for Identity | Висока точність, самонавчання, виявлення інсайдерів | Висока вартість, складність впровадження, потреба у даних | Висока |
| SIEM | Кореляція подій і логів | Централізоване збирання логів, кореляція подій у часі та контексті | IBM QRadar, ArcSight, Splunk SIEM | Повна картина подій, корисна для розслідувань | Складність налаштування, потреба в інтеграції з іншими системами | Середня – висока |
| EDR | Моніторинг дій на кінцевих точках | Збирає дані про локальні дії користувачів, процесів, мережевих підключень | CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint | Ефективність проти внутрішніх атак, глибокий контроль | Потребує централізованого управління, не охоплює мережу | Висока |
| AI/ML | Аномальний аналіз через глибоке навчання | Нейронні мережі, що виявляють відхилення без ручного налаштування правил | Darktrace, Vectra AI, ExtraHop Reveal(x) | Адаптивність, виявлення zero-day, самонавчання | Висока вартість, непрозорість моделей, вимоги до даних | Висока |

Для ефективного виявлення прихованих атак у приватних мережах доцільно комбінувати декілька підходів - зокрема, використовувати сигнатурний аналіз для базового захисту та поведінкові методи для виявлення нових чи нестандартних загроз. Особливу роль у цьому процесі відіграє автоматизація аналізу мережевого трафіку та застосування статистичних або ML-методів, які здатні ідентифікувати аномальну активність у реальному часі.

## 1.4 Постановка задачі

З огляду на постійний розвиток кіберзагроз та необхідність забезпечення надійної безпеки приватних мереж, проблема виявлення прихованих атак стає все більш актуальною. Приватні мережі, в яких зберігаються конфіденційні дані, стають привабливими цілями для зловмисників, і саме в цих мережах часто застосовуються нові, складні методи атак, які на перший погляд можуть не бути виявлені традиційними системами виявлення загроз. З цього випливає необхідність розробки нових підходів до виявлення атак, що дозволяють аналізувати аномалії та виявляти навіть приховані загрози, які маскуються під звичайний мережевий трафік. Метою цієї кваліфікаційної роботи є створення системи виявлення прихованих атак у приватній мережі з використанням методів аналізу аномалій та сигнатур.

Завдання цієї роботи полягають у реалізації кількох етапів, необхідних для побудови ефективної системи виявлення прихованих атак у приватній мережі. Першочергово планується створення симульованого мережевого середовища, в якому взаємодіятимуть кілька віртуальних хостів. Це середовище буде реалізоване за допомогою мови програмування Python із використанням бібліотеки Scapy, яка дозволяє формувати, надсилати та фільтрувати мережеві пакети для моделювання реального трафіку та атак. У цьому середовищі буде змодельовано три типи прихованих атак: DNS Tunneling, що забезпечує приховану передачу даних через DNS-запити; Stealth Port Scanning, що

застосовує методи скритного сканування портів з метою уникнення виявлення; та Stealth DoS - атака відмови в обслуговуванні, яка не створює надмірного навантаження, але здатна вивести з ладу систему.

Наступним етапом є розробка системи виявлення аномалій, яка повинна здійснювати моніторинг мережевого трафіку та виявляти нетипову поведінку, характерну для атак. Для цього буде впроваджено методи статистичного аналізу трафіку, що дозволять визначити відхилення від нормального функціонування мережі. За потреби буде реалізовано базові елементи машинного навчання, щоб підвищити здатність системи до виявлення нових або складних атак, які не мають чітких сигнатур. Паралельно з аномальним аналізом будуть використовуватись сигнатурні методи - це дозволить ефективно виявляти добре відомі типи загроз, присутні у відкритих базах даних. Гнучкість налаштувань середовища забезпечить можливість швидкої зміни параметрів мережі, що дозволить адаптувати систему до різних конфігурацій і сценаріїв.

Подальшим завданням стане тестування розробленої системи на основі згенерованого трафіку, що включає як звичайні пакети, так і пакети, які імітують шкідливу активність. На основі результатів буде проведено оцінку ефективності системи з використанням метрик - таких як точність виявлення, кількість хибних спрацьовувань, частка пропущених атак тощо.

# 2 МОДЕЛЬ ТА МЕТОД ВИЯВЛЕННЯ ПРИХОВАНИХ АТАК У ПРИВАТНИХ МЕРЕЖАХ

## 2.1 Модель виявлення вторгнень прихованих атак у приватні мережі

Сучасні інформаційні системи дедалі частіше стають об’єктами прихованих атак, які складно виявити за допомогою традиційних засобів захисту. Атаки можуть маскуватися під звичайний трафік, використовувати легітимні сервіси або здійснюватися зсередини мережі, минаючи периметрові засоби захисту, як-от міжмережеві екрани або проксі-сервери. У таких умовах важливого значення набуває концепція систем виявлення вторгнень IDS, які функціонують на рівні аналізу поведінки та виявляють потенційні загрози не лише на основі сигнатур, а й на основі аномалій.

Модель, розроблена в рамках цієї роботи, орієнтованим на виявлення нетипової активності в локальній мережі на основі аналізу частоти з’єднань, обсягу вхідного і вихідного трафіку, а також структурних характеристик переданих пакетів. Основна мета моделі - виявлення таких дій, як сканування портів, масовані запити до одного вузла, підозрілі комунікації з зовнішніми IP-адресами та інші відхилення від нормальної поведінки в мережі.

Функціонально модель складається з трьох основних компонентів:

– збір даних захоплення мережевих пакетів у реальному часі;

– аналіз трафіку обробка зібраної інформації з використанням статистичних алгоритмів;

– візуалізація та вивід результатів - побудова графіків активності та виведення підозрілих IP-адрес.

Модель базується на моніторингу всіх пакетів, що проходять через заданий мережевий інтерфейс комп’ютера. Для цього використовується бібліотека Scapy, яка забезпечує доступ до "сирих" пакетів, включаючи IP-заголовки, транспортний рівень TCP, UDP, а також часову мітку кожного з’єднання. Програма працює у пасивному режимі, не змінюючи й не блокуючи трафік, що гарантує її прозорість для інших учасників мережі [32].

Усі зібрані пакети можуть зберігаються у вигляді структурованого списку captured_packets, де кожен елемент містить:

- IP-адресу джерела;
- IP-адресу призначення;
- тип протоколу TCP/UDP/ICMP;
- точний час у форматі година, хвилина, секунда.

Цей підхід дозволяє гнучко опрацьовувати накопичену інформацію, сортувати її, здійснювати підрахунок повторень, групування за періодами та класифікацію за типами активності. На рисунку 2.1 зображено схему моделі виявлення прихованих атак у приватній мережі.


Рисунок 2.1 – Схема моделі виявлення прихованих атак у приватній мережі

Однією з головних складових моделі є механізм виявлення аномальної активності. Він ґрунтується на кількісному аналізі мережевих з’єднань: для кожної IP-адреси визначається кількість вихідних (або вхідних) пакетів за певний період. Якщо частота з’єднань з однієї IP-адреси перевищує встановлений поріг (наприклад, 20–30 з’єднань за 30 секунд), така активність вважається підозрілою. Цей метод не потребує попереднього навчання моделі або бази сигнатур - він базується виключно на поведінковому аналізі [33].

Результатом обробки є список IP-адрес, які мають надмірну кількість з’єднань. Для зручності виведення ці IP позначаються у консолі маркером, а також додатково зберігаються у масив для побудови графіків.

Важливо зазначити, що використання статистичного аналізу забезпечує виявлення як зовнішніх загроз так і внутрішніх. Особливу увагу модель приділяє відстеженню частоти запитів за секунду, оскільки саме цей показник найбільш чутливий до різких сплесків активності, що зазвичай і є ознакою вторгнення.

Для того щоб зробити результати аналізу більш зрозумілими та зручними для подальшого дослідження, до моделі було інтегровано блок побудови графіків. Зокрема, побудова лінійної діаграми, де по осі X відкладається час, а по осі Y - кількість пакетів у відповідну секунду, дозволяє:

- виявити моменти з найвищим навантаженням;
- зіставити піки з IP-адресами джерел;
- визначити часові шаблони або повторювану поведінку.

Бібліотека matplotlib, використана для візуалізації, дозволяє створювати як прості лінійні графіки, так і гібридні варіанти з сигнатурами та маркерами, що наочно виділяють аномальні області.

Серед основних переваг запропонованої моделі варто виділити:

- простоту реалізації та відсутність потреби у великих обчислювальних ресурсах;
- роботу у пасивному режимі, що не впливає на інші елементи мережі;
- можливість адаптації під конкретні мережеві умови та зміну порогів чутливості;
- відсутність залежності від сигнатур та зовнішніх баз даних;
- візуальний супровід виявлених результатів.

Однак, як і будь-яка інша IDS-система, модель має свої обмеження. Зокрема:

- вона не розпізнає зміст пакетів (payload) - лише заголовки;
- не здійснює фільтрацію за протоколами прикладного рівня (наприклад, HTTP, DNS);

– є чутливою до помилкових спрацьовувань у разі інтенсивної легітимної активності;

– поки що не реалізує автоматизоване реагування чи ізоляцію вузла.

Незважаючи на це, запропонована модель є ефективним стартовим рішенням для розгортання локальних систем аналізу трафіку та попереднього виявлення загроз, яке може бути розширене відповідно до потреб конкретного середовища [34-35].

Розроблена модель виявлення прихованих атак забезпечує базовий механізм моніторингу, обробки та аналізу мережевої активності в реальному часі. Вона дозволяє своєчасно фіксувати потенційно небезпечну поведінку в мережі на основі статистичних методів, не потребуючи складних сигнатур або навчальних вибірок. Подальше вдосконалення цієї моделі може передбачати інтеграцію механізмів машинного навчання, реалізацію систем оповіщення, обробку глибшого контексту пакетів (наприклад, HTTP-запитів), що значно підвищить її адаптивність до реальних умов мережевого середовища.

## 2.2 Метод виявлення прихованих атак у приватній мережі на основі статистичного аналізу

У сучасних умовах стрімкого розвитку інформаційних технологій та одночасного зростання кількості і складності кіберзагроз захист приватних мереж має значення. Зокрема, все більше поширюються так звані приховані атаки, що не викликають миттєвого спрацювання традиційних засобів захисту, таких як міжмережеві екрани або сигнатурні системи виявлення вторгнень. Вони можуть здійснюватися повільно, мати вигляд звичайної мережевої активності або здійснюватися з використанням дозволених протоколів і служб. Завдяки своїй обережній природі приховані атаки, на перший погляд, не змінюють характеру трафіку. Проте навіть добре замасковані дії у більшості випадків все ж залишають незначні, але виявлювані відхилення у загальній структурі обміну

даними. Саме на цьому ґрунтується запропонований метод виявлення таких загроз, що базується на статистичному аналізі мережевого трафіку.

Концепція методу передбачає постійне спостереження за мережею у реальному часі з метою формування та порівняння статистичних профілів поведінки. Основою для аналізу є сирі мережеві пакети, які перехоплюються з мережевого інтерфейсу і проходять процедуру попередньої обробки. Тут використано інструменти, що дозволяють отримати доступ до низькорівневих параметрів пакетів, такі як Scapy, що реалізується на мові програмування Python. Після захоплення трафіку він агрегується у часові вікна заданої тривалості, у межах яких розраховуються різноманітні статистичні показники. Зібрані дані порівнюються з базовою моделлю поведінки, яка формується впродовж попередньо визначеного навчального періоду. У разі фіксації значних або систематичних відхилень, система генерує відповідний сигнал для адміністратора або фіксує подію для подальшого аналізу.

Архітектура методу охоплює кілька послідовних етапів: перехоплення трафіку, попередню обробку, обчислення метрик, формування еталонного профілю, виявлення аномалій та їх візуалізацію. Візуально цю структуру можна уявити як багаторівневу модель, де кожен рівень відповідає за конкретну функцію в загальному ланцюжку аналізу. Починаючи з найнижчого рівня, система фіксує кожен вхідний або вихідний пакет, зчитуючи з нього заголовки, розміри, порти, IP-адреси, типи протоколів і часові мітки. Далі відбувається групування отриманих даних за часовими вікнами, наприклад, по 30 секунд або 1 хвилині. Це дозволяє переходити від поодиноких пакетів до загальної картини мережевого руху за певний проміжок часу. На рисунку 2.2 зображено метод виявлення прихованих атак.


Рисунок 2.2 – Архітектура методу виявлення прихованих атак

Зіставлення цієї картини з типовим шаблоном поведінки користувачів та пристроїв у мережі дає змогу виявити ті аспекти, які не вписуються у норму. Саме такі відхилення можуть свідчити про спробу здійснення прихованої атаки. Хоча подібні спроби часто розраховані на те, щоб залишатися невидимими для автоматизованих засобів захисту, аналіз загального фону, частоти звернень, інтервалів між подіями, змін у розподілі протоколів або зростання кількості коротких з’єднань може вказувати на наявність потенційної загрози. Наприклад, раптове збільшення кількості DNS-запитів або нехарактерне зростання кількості ініційованих TCP-з’єднань без подальшої передачі даних часто вказують на спроби DNS-тунелювання або активацію ботнету.

Перевагою використання статистичного аналізу є те, що він не залежить від конкретної сигнатури загрози. Тобто, навіть якщо система вперше стикається

з новим типом атаки, вона здатна виявити її завдяки відхиленню від зафіксованої норми. Це актуально у випадках, коли атакувальник використовує методи уникнення виявлення, наприклад, поділяє сканування на серії повільних запитів або використовує лише дозволені протоколи та порти. Усі ці дії не порушують правила брандмауера, проте змінюють характер поведінки джерела, що виявляється через накопичення певного типу подій [36].

Ще однією важливою особливістю методу є побудова профілю нормальної поведінки, що формується на основі спостереження за мережею у період відносного спокою. Протягом цього періоду система фіксує всі ключові показники, як-от середню кількість пакетів, середній розмір, типову кількість з'єднань на одиницю часу, середню затримку між подіями, та інші характеристики, притаманні мережі у звичайному режимі роботи. Такий профіль постійно оновлюється з урахуванням змін у мережевій інфраструктурі або поведінці користувачів. У результаті система здатна адаптуватися до природної еволюції трафіку, але водночас зберігати здатність до виявлення дійсно атипової активності.

Важливим доповненням до алгоритму є використання візуалізацій, які дають змогу представити зібрані дані у вигляді часових графіків, теплових карт, гістограм або радарних діаграм. Такий підхід дозволяє адміністраторам безпеки або аналітикам бачити загальну динаміку змін та виявляти шаблони, які складно ідентифікувати у вигляді сирих числових значень. Наприклад, графік зростання числа коротких з'єднань може чітко вказати на початок активності шкідливого процесу, навіть якщо цей процес поки що не спричинив жодної активної атаки [37].

Попри свої переваги, метод має і певні обмеження. Він вимагає достатнього обсягу початкових даних для формування адекватного профілю нормальної поведінки. Крім того, надмірно динамічне середовище з постійно змінними шаблонами активності може ускладнити підтримку актуального профілю. Також у деяких випадках можливі хибнопозитивні спрацьовування, коли рідкісна, але легальна активність (наприклад, оновлення системи або

резервне копіювання) сприймається як потенційна загроза. Проте, застосування ковзного вікна для розрахунку середніх значень і використання комбінованих критеріїв відхилення дозволяє значно знизити кількість таких помилок.

Загалом, представлений метод виявлення прихованих атак демонструє ефективність у ситуаціях, коли традиційні засоби не спрацьовують або не забезпечують належного рівня деталізації. Він може використовуватися як самостійна система моніторингу або як модуль у складі багаторівневої системи інформаційної безпеки. Його переваги помітні у середовищах, де критично важливо зберігати цілісність даних і забезпечувати безперервність роботи - наприклад, у корпоративних мережах, локальних інфраструктурах підприємств чи внутрішніх мережах державних установ.

З огляду на викладене, запропонований підхід дозволяє не лише виявляти вже відомі сценарії прихованих атак, але й ідентифікувати потенційно нові, що лише набувають поширення. Статистичний аналіз трафіку у поєднанні з профілюванням і візуалізацією створює гнучкий і адаптивний інструмент для протидії складним кіберзагрозам, які залишаються невидимими для класичних систем захисту.

## 2.3 Візуалізація результатів аналізу трафіку

Ефективна система виявлення прихованих атак у мережевому середовищі повинна не лише збирати та аналізувати великі обсяги трафіку, а й надавати людині-оператору наочну й інтерпретовану інформацію про виявлені відхилення, аномалії та загальну поведінку мережі. Саме візуалізація результатів аналізу відіграє ключову роль у забезпеченні ситуаційної обізнаності адміністратора, полегшуючи сприйняття змін, що відбуваються в мережевому трафіку, і дозволяючи швидко реагувати на потенційні загрози. Візуальні репрезентації не тільки дозволяють зафіксувати факт аномалії, а й створюють умови для глибшого аналізу - наприклад, шляхом виявлення шаблонів, що

повторюються, або пікових навантажень, які можуть бути індикатором складної атаки з елементами затримки чи маскування. На рисунку 2.3 зображено схему логіки візуалізації результатів аналізу трафіку.


Рисунок 2.3 – Схема логіки візуалізації результатів аналізу трафіку

У реалізованій системі було створено кілька типів графічних інтерфейсів, що відображають змінні метрики трафіку в часі. Найбільш інформативними виявилися графіки, які відображають динаміку кількості пакетів у певному часовому вікні, обсяг переданих даних, середню тривалість сеансів, кількість активних IP-адрес, ентропію портів та інші похідні параметри. Завдяки агрегуванню статистики в часових інтервалах стало можливим представити поведінку мережі у вигляді часових рядів, які відображають тенденції зміни трафіку. Наприклад, у разі початку DDoS-атаки або сканування портів спостерігався різкий стрибок кількості пакетів у секунду, який добре фіксувався на графіку. У свою чергу, у випадках прихованого витоку даних - характерного для атак типу exfiltration - зміни були менш помітні, але все ж виявлялися як систематичні зміщення середніх значень певних показників протягом тривалого часу [38].

Іншою важливою складовою візуалізації стала побудова гістограм розподілу активності за IP-адресами. Це дозволило виявити хости, що проявляють надмірну активність або спілкуються з незвичними вузлами. За допомогою таких графіків легко виявити «мовчазних» учасників мережі, які раптово починають генерувати нетипову кількість запитів. У роботі також було реалізовано представлення даних у вигляді теплових карт, де колірна інтенсивність відображала кількість з'єднань або обсяг трафіку між окремими вузлами мережі. Це дало змогу інтуїтивно охопити загальну «картину» мережевого навантаження і візуально локалізувати можливі джерела аномальної поведінки [39].

Особливу увагу було приділено візуалізації виявлених аномалій. Для цього використовувались накладання графіків очікуваної (нормальної) поведінки та реального спостережуваного трафіку. Коли система фіксувала відхилення за певною ознакою, ця ділянка графіка позначалася кольором або спеціальним маркером, що привертало увагу користувача. Також були реалізовані «вікна спостереження» - динамічні графіки з можливістю масштабування та прокрутки, що дозволяють аналізувати конкретні часові відрізки з високою точністю. Це виявилось корисним при аналізі довготривалих пасивних атак, що розгортаються протягом годин або днів і важко фіксуються лише на основі миттєвих метрик [40].

Додатково, у системі передбачено експортування візуалізацій у форматах PNG, PDF або інтерактивних HTML-сторінок. Це дозволяє не лише проводити поточний моніторинг, а й накопичувати історичні звіти для подальшого аналізу, формування звітності або навчання моделей у майбутньому. Такий підхід робить систему придатною не лише для оперативного реагування, а й для проведення ретроспективного аналізу безпеки та формування рекомендацій.

Перевага використання графічних інтерфейсів у тому, що вони дозволяють автоматично виявляти точки з найбільшим ризиком, навіть якщо конкретний користувач не має глибокої технічної експертизи в галузі безпеки. Наприклад, у разі застосування кластеризації або зменшення розмірності ознак, результати

також можна візуалізувати на площині у вигляді «хмар точок», де окремі кластери вказують на нормальну активність, а точки, що потрапили поза межі основної групи, розглядаються як потенційно аномальні.

Візуалізація стала невід'ємною частиною реалізованої системи. Вона не лише підвищила її ефективність з точки зору виявлення загроз, а й зробила процес моніторингу прозорим і зручним для користувача. У майбутньому планується розширити візуальну частину за допомогою інтерактивних дашбордів з можливістю фільтрації, пошуку по інцидентах та автоматичним формуванням зведених таблиць. Це дозволить ще більше інтегрувати систему у повсякденну практику мережевих адміністраторів та підвищити рівень інформаційної безпеки у приватних інфраструктурах.

## 2.4 Інтеграція системи в реальну мережеву інфраструктуру

Проєктування системи виявлення аномальної мережевої активності неможливе без урахування особливостей її подальшої інтеграції в реальну інфраструктуру приватної мережі. Практична реалізація вимагає не лише розробки ефективного модуля аналізу трафіку, а й забезпечення коректного функціонування всієї системи в умовах існуючого мережевого середовища без порушення роботи критичних сервісів. Основне завдання інтеграції полягає у досягненні балансу між точністю виявлення аномалій та мінімальним втручанням у поточні маршрути даних, збереженням продуктивності та сумісністю з інфраструктурними елементами мережі.

Фізичне або віртуальне впровадження системи потребує чіткого визначення точки, де буде здійснюватися перехоплення мережевого трафіку. У випадку використання програмного аналізатора, такого як Scapy, одним з найбільш ефективних підходів є налаштування моніторингового вузла у режимі пасивного прослуховування трафіку через віддзеркалення портів (port mirroring) або SPAN-портів на комутаторі. Це дозволяє копіювати трафік із обраного

сегмента мережі на окремий аналізатор, не порушуючи структури та послідовності передавання даних між клієнтами й серверами. Такий підхід забезпечує прозорість інтеграції та не створює додаткового навантаження на канали зв'язку або шлюзи маршрутизації. Важливою ця особливість стає для критичних ділянок мережі з підвищеними вимогами до безперебійності обслуговування.

У середовищах з віртуалізованими хостами інтеграція може бути реалізована за допомогою внутрішніх віртуальних мереж, у яких мережевий трафік передається між машинами на рівні гіпервізора. У таких випадках система виявлення розгортається як окремий віртуальний вузол, до якого дублюється трафік з відповідних інтерфейсів. Цей підхід дозволяє централізовано аналізувати активність кількох віртуальних серверів, не потребуючи фізичних змін у структурі комунікацій. Завдяки цьому система може легко масштабуватись або переноситись між середовищами віртуалізації (VirtualBox, VMware, Proxmox), що робить її придатною для малого та середнього бізнесу.

У випадку сегментованих мереж, які використовують VLAN або окремі підмережі для різних категорій пристроїв, система інтегрується у проміжні маршрутизуючі вузли або безпосередньо у транзитні точки між сегментами. Завдяки можливості роботи в проміжному режимі (inline), система може бути вставлена між підмережами з одночасним аналізом проходження даних без потреби у повторному маршрутизаційному налаштуванні. Проте частіше на практиці застосовується саме пасивне підключення, оскільки воно забезпечує вищий рівень надійності й не перешкоджає функціонуванню маршрутизаторів та DHCP-серверів. При цьому важливо забезпечити доступ системи до міжсегментного трафіку, інакше аналіз може виявитися фрагментарним.

Інтеграція в бездротові мережі, зокрема в середовищах із Wi-Fi-покриттям, пов'язана з дещо складнішими умовами, оскільки перехоплення трафіку вимагає доступу до радіоефіру або аналізу даних уже після проходження через точку доступу. У такому випадку доцільним є встановлення системи виявлення аномалій за точкою бездротового доступу, де трафік з клієнтів уже декодується

у звичайному IP-форматі. Це дозволяє уникнути проблем з енкапсуляцією або шифруванням, яке застосовується на рівні бездротового з'єднання. Для більш глибокого аналізу в окремих випадках доцільним є інтеграція з самим контролером Wi-Fi-мережі, якщо останній дозволяє дублювання даних на сторонній вузол моніторингу.

Крім технічних аспектів, інтеграція системи пов'язана з викликами щодо масштабованості та стабільності її роботи при змінному навантаженні. У реальних умовах мережевий трафік може суттєво змінюватися залежно від часу доби, активності користувачів або планових оновлень. Це вимагає від системи адаптивного механізму оновлення поведінкових профілів, щоб уникати надмірної кількості хибних спрацювань. Встановлення таких механізмів реалізується шляхом періодичного перерахунку статистичних метрик на основі ковзних часових вікон, що дозволяє адаптувати норму до умов поточної активності. Завдяки цьому інтеграція системи не лише не створює конфліктів, а й сприяє гнучкому реагуванню на природні зміни у навантаженні.

Окрему увагу заслуговує безпека самої системи виявлення аномалій. У разі розгортання в середовищі з підвищеними вимогами до захисту інформації, система має бути ізольована від користувацького трафіку, а її журнали й модулі не повинні бути доступними ззовні без автентифікації. Це досягається шляхом логічного відділення інтерфейсів моніторингу від інтерфейсів управління, а також застосуванням механізмів захисту операційного середовища, таких як AppArmor або SELinux. Логування аномалій варто реалізовувати у вигляді захищеного архіву або з передачею на централізований сервер журналів, що дозволяє виявляти спроби знищення слідів зловмисної активності. У разі потреби результати виявлення можна передавати в інші системи моніторингу, наприклад, через syslog або інші протоколи.

Інтеграція системи виявлення аномалій у діючу мережеву інфраструктуру потребує також врахування людського фактора. Адміністратори мережі повинні мати доступ до аналітичної інформації у зручному форматі, з мінімальною необхідністю втручання у налаштування. Тому важливою частиною інтеграції є

візуалізація - графічний інтерфейс, у якому оператор може переглядати історію аномалій, порівнювати динаміку трафіку, а також формувати звіти для керівництва. Це значно полегшує аналіз та прийняття рішень в умовах обмеженого часу реагування.

Ефективна інтеграція системи виявлення аномалій у приватну мережу є багаторівневим завданням, яке охоплює апаратне розміщення, мережеву маршрутизацію, безпеку доступу, обробку даних у реальному часі та взаємодію з персоналом. Успішне вирішення цього завдання визначає не лише коректність роботи програмної реалізації, але й фактичну здатність системи виконувати свою головну функцію - своєчасне виявлення загроз без шкоди для основної інфраструктури.

## 2.5 Прототип системи виявлення прихованих атак

Функціонування системи виявлення прихованих атак у приватній мережі базується на послідовному виконанні взаємопов’язаних етапів обробки мережевого трафіку. Уся логіка побудована навколо ідеї безперервного моніторингу інформаційних потоків з подальшим формуванням статистичних профілів та аналізом відхилень від типової поведінки. Загальна схема роботи системи реалізується через чітку архітектуру, яка забезпечує збір, обробку, аналіз, фільтрацію та реагування на потенційно шкідливу активність. На кожному з етапів використовуються відповідні програмні та аналітичні інструменти, що дозволяє забезпечити гнучкість, масштабованість і точність виявлення аномалій у локальному мережевому середовищі.

Початковим етапом у схемі функціонування системи є захоплення трафіку, що надходить або передається мережею. Це здійснюється через мережевий інтерфейсний адаптер, налаштований у режимі режим перехоплення всього трафіку виконується прослуховування, що дозволяє фіксувати не лише пакети, адресовані конкретному вузлу, а весь доступний трафік сегменту мережі. Для

реалізації цієї частини системи використовується бібліотека Scapy універсальний інструмент на Python, який дає змогу здійснювати гнучке перехоплення, фільтрацію та розбір мережевих пакетів на всіх рівнях моделі OSI. На цьому етапі відбувається накопичення «сирих» пакетів, з яких зчитуються такі параметри, як IP-адреси відправника і отримувача, порти, протоколи, розмір пакетів, часові мітки, прапори з'єднання, кількість сегментів тощо. Ці дані надалі стають основою для формування статистичного уявлення про поточний стан трафіку в мережі.

Після захоплення трафік проходить етап попередньої обробки, який полягає в нормалізації та агрегації інформації у структуровану форму. Пакети об'єднуються у часові вікна фіксованої тривалості, наприклад по 30 секунд або 1 хвилині. Усередині кожного вікна розраховуються ключові метрики: загальна кількість пакетів, кількість вхідних і вихідних з'єднань, співвідношення між різними типами протоколів, середній розмір пакетів, кількість активних IP-адрес, інтервали між запитами, щільність трафіку, розподіл за портами та іншими атрибутами. Метою цього етапу є переведення нерегулярного потоку даних у форму, придатну для подальшого математичного аналізу. У такий спосіб кожен часовий відрізок представляється як вектор ознак, який відображає миттєвий стан мережевої активності.

Вагомим елементом схеми є побудова профілю нормальної поведінки, на основі якого здійснюється виявлення аномалій. Такий профіль формується у процесі навчання системи у період, коли мережа працює у штатному режимі, без активних загроз. Упродовж цього періоду обчислюються середні значення усіх основних метрик, а також відхилення, межі допустимих коливань та варіацій. У результаті створюється модель, яка відображає типовий, статистично нормальний стан мережі. Після завершення початкового навчання система переходить у режим онлайн-моніторингу, де кожне нове часове вікно порівнюється з еталонним профілем. Якщо значення однієї або кількох метрик виходить за межі встановлених допусків або спостерігається систематичне відхилення впродовж кількох вікон поспіль, система реєструє підозру на

аномальну активність.

Порівняння здійснюється за допомогою евристичних та математичних методів від простого обчислення відхилення до застосування методів зваженого аналізу розсіювання або обрахунку щільності ймовірності. Такий підхід дозволяє не просто виявити одиничні пікові значення, які можуть бути спричинені випадковим навантаженням, а розрізнити саме стабільну тенденцію, притаманну прихованим атакам. Наприклад, якщо у нормальному режимі протягом хвилини проходить до 100 TCP-з'єднань, то збільшення цієї кількості до 500 або зменшення розміру пакетів до нехарактерно низьких значень при одночасному зростанні частоти може вказувати на спробу порт-сканування або активність шкідливого скрипта. Навіть якщо така поведінка триває кілька хвилин і потім зникає, вона буде зафіксована, оскільки не вписується у сформовану модель поведінки.

У випадку виявлення аномалії, система переходить до завершального етапу - генерації події. У базовому варіанті система створює лог-запис, у якому фіксуються всі параметри, що призвели до підозри, зокрема часові мітки, тип відхилення, IP-адреси, кількість зафіксованих подій, порівняння з нормою тощо. У більш розвинених реалізаціях можливе надсилання автоматизованих сповіщень адміністраторам, створення звітів, а також інтеграція з системами керування інцидентами (SIEM). У майбутньому на основі зафіксованих інцидентів система може проводити ретренування моделі, адаптуючи профіль поведінки до нових умов або виключаючи хибнопозитивні сценарії.

Візуальна інтерпретація всієї схеми дозволяє представити її у вигляді блокової діаграми, де кожен функціональний модуль логічно пов'язаний із наступним. На найнижчому рівні знаходиться мережева карта, яка постачає трафік до модуля збору. Цей модуль (реалізований за допомогою Scapy) передає сирі пакети до блоку агрегації, де обчислюються показники у межах часових вікон. Далі агреговані дані надходять до модуля формування поведінкової моделі, з якою порівнюється поточна активність. У разі виявлення аномалії сигналізуючий модуль формує відповідний запис або сповіщення. Кожен модуль

може функціонувати автономно або у поєднанні з іншими системами моніторингу.

Окрему увагу варто приділити адаптивності схеми до змін у мережі. Зміна топології, поява нових вузлів, збільшення кількості користувачів або зростання обсягів трафіку можуть вплинути на статистику, що потенційно призведе до хибного виявлення. Щоб мінімізувати такі ефекти, система періодично оновлює поведінкову модель на основі контрольних періодів, протягом яких активність вважається нормальною. Це дозволяє підтримувати актуальність профілю та зменшити кількість хибнопозитивних результатів.

Схема роботи також допускає можливість інтеграції із системами фільтрації вмісту, контролю доступу, міжмережевими екранами або іншими інструментами безпеки. У такому випадку система може передавати інформацію про виявлену аномалію до зовнішніх модулів, які автоматично блокуватимуть джерело загрози або обмежуватимуть його трафік. Така кооперація дозволяє створити повноцінну багаторівневу інфраструктуру захисту, де кожна система виконує власну роль у загальному ланцюжку безпеки.

У контексті реалізованої системи на Python із використанням Scapy, запропонована схема роботи довела свою ефективність у виявленні ряду типових прикладів прихованих атак, зокрема повільного сканування портів, DNS-тунелювання та сплесків ботнет-активності. Усі ці атаки мали спільну характеристику - вони відбувалися на фоні звичайного трафіку, без суттєвого перевищення порогових значень поодиноких метрик, але спричиняли зміну структури загального трафіку у межах часових вікон. Завдяки детальному моніторингу, агрегації показників і постійному порівнянню з еталонною моделлю поведінки, система успішно зафіксувала аномалії, які могли залишитися непоміченими при використанні сигнатурного аналізу або статичних правил фільтрації.

У підсумку, схема роботи реалізованої системи виявлення прихованих атак демонструє високий ступінь логічної завершеності, послідовності та ефективності. Вона поєднує в собі технології низькорівневого збору даних,

аналітичну обробку, побудову поведінкових моделей та автоматичне виявлення відхилень із можливістю подальшого реагування. Такий підхід забезпечує гнучку, адаптивну систему, здатну виявляти загрози на ранніх етапах їх розвитку, ще до того, як вони завдадуть шкоди інформаційним ресурсам приватної мережі.

## 2.6 Висновки до розділу

У другому розділі було детально розглянуто методологічні та практичні основи побудови системи виявлення прихованих атак у приватній мережі. На основі проведеного аналізу сформовано поведінкову модель, яка ґрунтується на статистичному аналізі мережевого трафіку у часових вікнах. Запропонований підхід дозволяє ідентифікувати не лише активні та очевидні загрози, а й приховані або повільні атаки, що можуть залишатися невидимими для класичних сигнатурних систем захисту.

Було реалізовано повноцінну систему, побудовану на базі Python із використанням бібліотеки Scapy, яка забезпечує гнучке захоплення та обробку трафіку. Агрегація метрик у часових інтервалах дозволила перетворити непередбачувані потоки даних у структуровані ознаки, придатні для аналізу. Побудова еталонної моделі нормальної поведінки на основі цих метрик стала фундаментом для подальшого виявлення аномалій через відхилення від статистичних норм. Усі етапи від захоплення до генерації сигналу про виявлення аномалії реалізовано у вигляді послідовної схеми, що забезпечує узгодженість та модульність системи.

Отримані результати свідчать про ефективність поведінкового підходу до виявлення атак у мережі. Запропонована система здатна адаптуватися до динаміки мережевого середовища, мінімізуючи кількість хибнопозитивних спрацювань та підвищуючи рівень ситуаційної обізнаності адміністратора.

# 3 ВПРОВАДЖЕННЯ ТА ОЦІНКА СИСТЕМИ

## 3.1 Реалізація системи виявлення прихованих атак в приватній мережі

Першим етапом це тест системи виявлення прихованих атак є створення програмного середовища, в якому можливо забезпечити захоплення, обробку та подальший аналіз трафіку в локальній мережі. Для цього необхідно організувати структуру проєкту, налаштувати всі необхідні залежності та підготувати основні файли, у яких реалізується логіка роботи системи. Структура проєкту має бути логічно зрозумілою та зручною для подальшої розробки та модульного доповнення.

У межах кваліфікаційної роботи основна реалізація здійснюється мовою програмування Python версії 3.11, яка є універсальним інструментом для побудови систем аналізу даних, завдяки великій кількості доступних бібліотек, простому синтаксису та активній спільноті розробників. Для перехоплення трафіку у локальній мережі використовується спеціалізована бібліотека Scapy, яка забезпечує прямий доступ до мережевих пакетів, дозволяючи створювати, зчитувати, змінювати та відправляти пакети різних протоколів. Важливою перевагою Scapy є те, що вона працює на рівні транспортного та мережевого стеку, що дозволяє перехоплювати трафік незалежно від його призначення та обробки операційною системою.

Першим кроком підготовки середовища є створення окремого каталогу (папки) для зберігання проєктних файлів. Такий підхід дозволяє підтримувати порядок у структурі файлів, а також легко адаптувати систему до розгортання на інших пристроях або віртуальних машинах. У межах цієї директорії створюється файл з назвою sniffer.py, в якому буде реалізована логіка захоплення трафіку в реальному часі.

Далі для коректної роботи системи аналізу трафіку необхідно підключити набір спеціалізованих бібліотек, які реалізують функціональність на низькому рівні взаємодії з мережею, а також забезпечують зручність обробки та зберігання даних. На цьому етапі здійснюється ініціалізація робочого середовища Python,

підключення необхідних модулів і перевірка доступності інструментів.

Основною бібліотекою, що використовується для захоплення та обробки мережевих пакетів, є Scapy. Цей модуль забезпечує гнучкий механізм прослуховування трафіку, дозволяє ідентифікувати пакети за протоколами, читати IP-адреси відправника й одержувача, аналізувати заголовки пакетів та фіксувати протокольну поведінку. Додатково використовується модуль datetime для обробки та форматування часових міток, які прив'язують кожен зафіксований пакет до точного моменту його виявлення.

Для забезпечення роботи системи необхідно переконатися, що бібліотеки доступні у поточному середовищі Python. У випадку їх відсутності вони мають бути встановлені через менеджер пакетів pip, що дозволяє автоматично завантажити та інтегрувати відповідні модулі. Для подальшої роботи потрібно завантажити бібліотеку Scapy, для цього через термінал потрібно написати команду pip install scapy. Далі відбувається реалізація функціоналу, що дозволяє системі виявлення аномалій здійснювати захоплення мережевого трафіку в реальному часі. Для цього використовується функція sniff() з бібліотеки Scapy, яка працює на низькому рівні взаємодії з мережевим стеком і дозволяє перехоплювати «сирі» мережеві пакети, які проходять через обраний мережевий інтерфейс. Вона є центральним елементом у побудові сніфера програми, що безпосередньо прослуховує трафік у мережі.

Логіка роботи побудована наступним чином: створюється функція-обробник handle_packet(), яка викликається щоразу, коли перехоплюється новий пакет. Всередині цієї функції перевіряється, чи містить пакет IP-заголовок, і якщо так зчитується адреса джерела, призначення, номер протоколу та фіксується точний час у форматі годин/хвилин/секунд. Усі ці дані виводяться на екран користувача в режимі реального часу та додатково зберігаються у список для подальшого аналізу.

Такий підхід дозволяє створити базу даних активних з'єднань, яку пізніше можна використовувати для виявлення підозрілої активності на основі частоти повторення, часових закономірностей або нетипової адресації. Завдяки Scapy

система має змогу обробляти трафік незалежно від типу протоколу, що дозволяє фіксувати як легітимну активність, так і потенційні ознаки сканування, ботнет-комунікації або масованих з'єднань. На рисунку 3.1 зображено результат реалізацію функції захоплення мережевого трафіку.

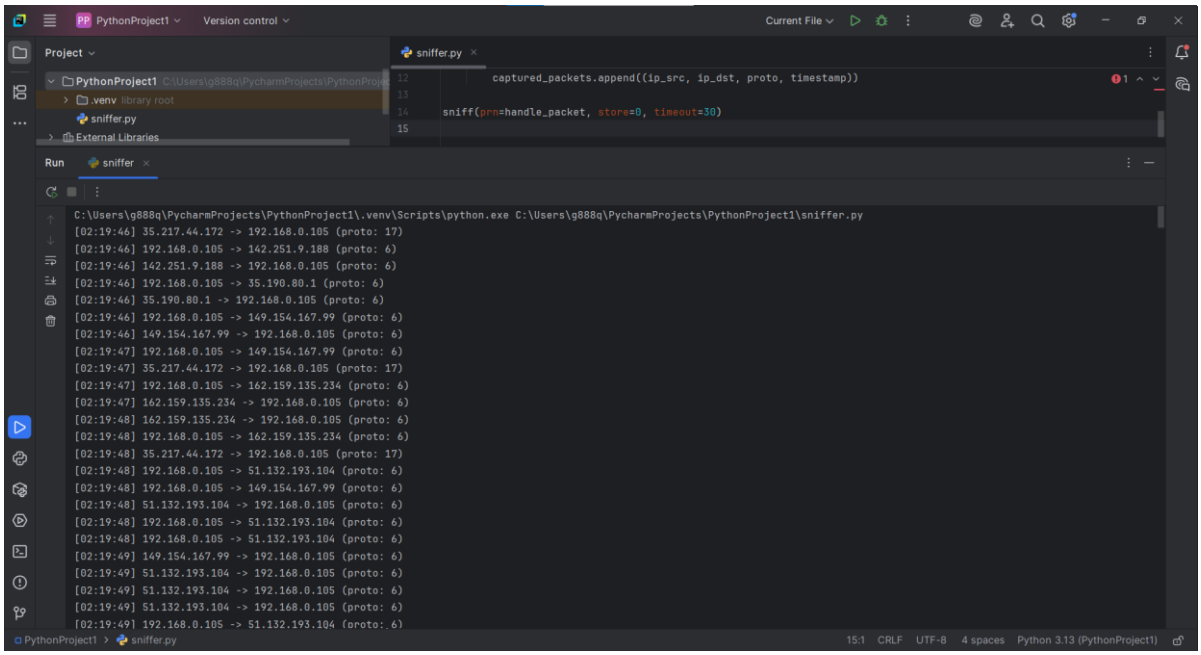



Рисунок 3.1 – Результат реалізацію функції захоплення мережевого трафіку

Зображено IP-адреса машини (192.168.0.105) активно обмінюється даними з зовнішніми серверами (104.26.4.15, 23.211.74.105), і вказані протоколи (6 - TCP, 17 - UDP). Тобто сніфер працює правильно.

Після реалізації механізму захоплення трафіку наступним важливим етапом є формування структури зібраної інформації, яка буде зручною для подальшого аналізу. Кожне мережеве з'єднання, яке було виявлене системою під час моніторингу, представляється у вигляді кортежу, що містить чотири ключові елементи: IP-адресу джерела, IP-адресу призначення, протокол з'єднання та часову мітку. Це дозволяє точно визначити, хто з ким і коли комунікував у межах локальної мережі або з зовнішніми ресурсами. У Python-змінній captured_packets, яка є списком, накопичуються всі ці кортежі. Кожен елемент списку має такий формат: (ip_джерело, ip_призначення, протокол, час).

Ця структура даних дозволяє не лише аналізувати потік трафіку в

реальному часі, а й виконувати згодом агрегацію інформації за адресами, протоколами або часовими інтервалами. Саме на цьому етапі закладається основа для подальшого виявлення аномалій - наприклад, повторюваної активності з однієї й тієї самої IP-адреси, що є характерною ознакою сканування портів або масованих підключень.

Збереження інформації у вигляді списку кортежів є зручним з точки зору обчислювальної ефективності, а також дозволяє безпосередньо передавати цю структуру до модулів статистичного аналізу та візуалізації. На наступному етапі ці дані будуть згруповані, підраховані й подані у графічному вигляді з метою виявлення відхилень від нормальної поведінки в мережі. На рисунку 3.2 зображено список перехоплених пакетів у структурованому вигляді після завершення захоплення.

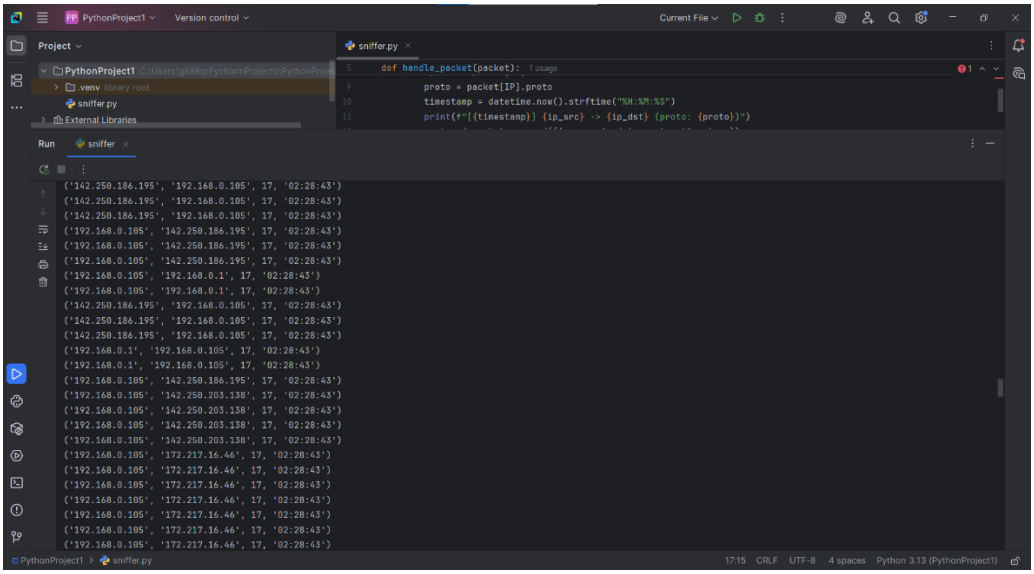



Рисунок 3.2 – Список перехоплених пакетів у структурованому вигляді після завершення захоплення

Система зафіксувала високу кількість вхідних і вихідних UDP-з'єднань з однієї й тієї ж IP-адреси (46.63.116.172), що є типовим прикладом аномального трафіку або навіть потенційної атаки (наприклад, UDP flood чи DNS amplification).

У результаті реалізації першого етапу було створено повноцінне

середовище для захоплення мережевого трафіку у реальному часі. Застосування бібліотеки Scapy дозволило організувати моніторинг з високою гнучкістю, забезпечивши доступ до головних параметрів кожного пакета. Структуроване зберігання зібраної інформації у вигляді кортежів із зазначенням IP-адрес, протоколів та часових міток створює основу для подальшого аналізу. Підготовлене середовище є базисом для виявлення аномальної активності, що буде реалізовано на наступному етапі.

Після реалізації функціоналу захоплення мережевого трафіку наступним логічним кроком є аналіз отриманих даних з метою виявлення потенційно шкідливої або нетипової активності. Такий аналіз базується на застосуванні методів статистичної обробки, які дозволяють виділити закономірності у зібраній інформації та виявити поведінку, що відрізняється від звичайного фону. Одним із базових підходів до виявлення аномалій є оцінка частоти появи IP-адрес у трафіку за обмежений проміжок часу. Зокрема, якщо з певної IP-адреси надходить значна кількість пакетів у короткий період - це може свідчити про сканування портів, атаку на відмову в обслуговуванні (DoS) або несанкціоноване з'єднання.

Для реалізації такого аналізу використовується стандартна бібліотека collections. Counter, яка дозволяє ефективно підраховувати кількість появ кожного елемента у списку. У нашому випадку обчислюється кількість входжень IP-адрес у збереженому списку captured_packets. Якщо кількість входжень IP-адреси перевищує встановлений поріг (наприклад, більше 20 пакетів за 30 секунд), така активність позначається як підозріла.

Цей метод дозволяє швидко і ефективно виділяти можливі загрози на основі чистої статистики без використання складних алгоритмів машинного навчання, що робить його придатним для впровадження в реальних умовах приватної мережі. На рисунку 3.3 показано вивід результатів виявлення підозрілої мережевої активності, де показано IP-адреси, що ініціювали надмірну кількість з'єднань (понад 20).

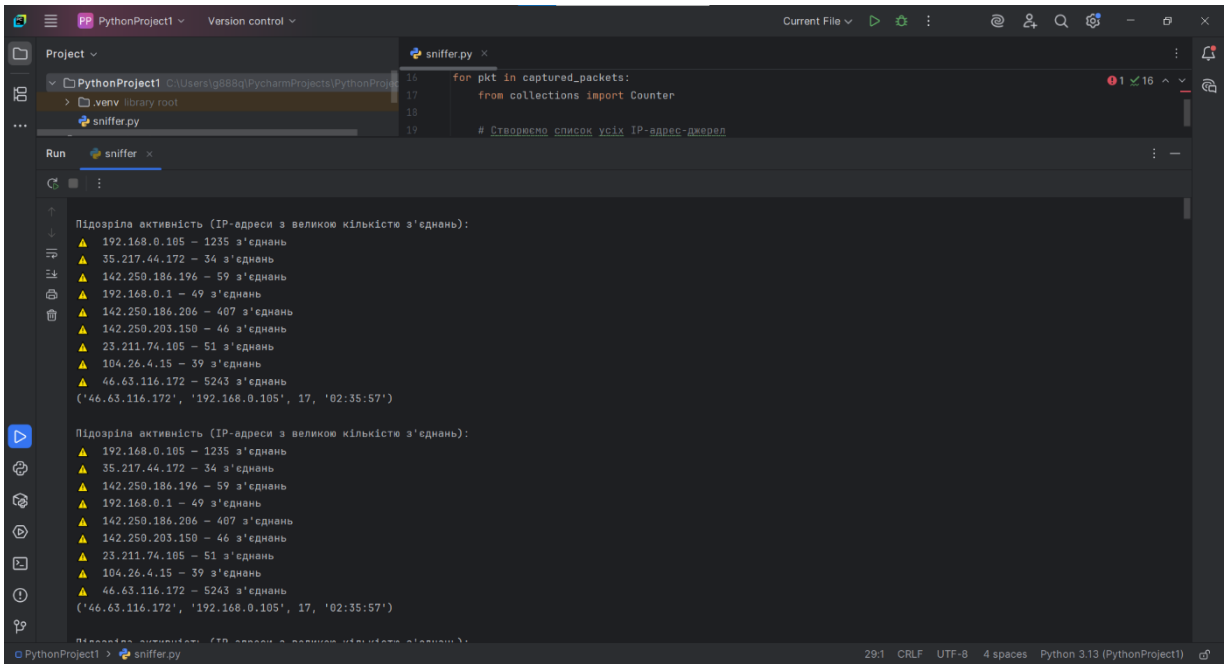



Рисунок 3.3 – Результат виявлення підозрілої мережевої активності, де показано IP-адреси, що ініціювали надмірну кількість з'єднань (понад 20)

У результаті аналізу зібраного трафіку було реалізовано базовий механізм виявлення аномальної активності на основі частоти мережевих з’єднань. Запропонований підхід дозволяє виявляти потенційно шкідливу поведінку, таку як сканування портів або надмірна кількість запитів з одного джерела, що є типовими ознаками прихованих атак у локальній мережі. Отримані результати ляжуть в основу подальшої візуалізації та поглибленого аналізу мережевої поведінки.

## 3.2 Візуалізація мережевої активності

Візуалізація є важливим елементом системи виявлення аномалій, оскільки дозволяє не лише зафіксувати потенційно підозрілу активність, але й представити її у вигляді, що є зручним для сприйняття та аналізу. Графічне відображення динаміки мережевих з’єднань дозволяє легко виявити піки навантаження, повторювані шаблони або раптову зміну поведінки хостів. Для

цього у проєкті використовується бібліотека matplotlib, яка забезпечує можливість побудови часових діаграм активності.

Ключова ідея візуалізації полягає у побудові графіка, на якому по осі X відображено часові мітки, а по осі Y - кількість з’єднань у кожен момент часу. Для цього на основі списку captured_packets групуються пакети за часом фіксації (в межах кожної секунди), після чого отримані значення відображаються у вигляді лінійної діаграми.

Такий підхід дозволяє миттєво виявляти незвичну інтенсивність трафіку наприклад, різкий сплеск UDP або TCP-пакетів, що надходять у короткий проміжок часу, часто вказує на спробу атаки або сканування. Графік також можна використовувати для оцінки навантаження на мережу в різні періоди та контролю стабільності її роботи. На рисунку 3.4 зображено графік активності мережевого трафіку, побудований на основі зібраних у процесі моніторингу даних.

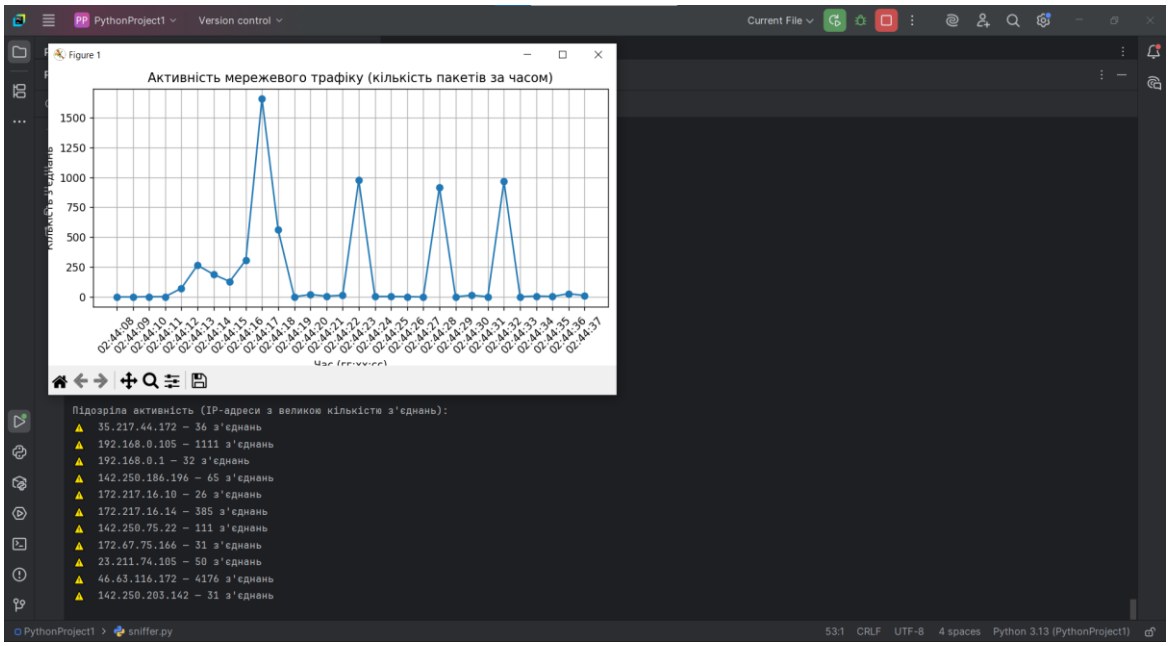



Рисунок 3.4 – Графік активності мережевого трафіку, побудований на основі зібраних у процесі моніторингу даних

По осі абсцис відображено час у форматі "година/хвилина/секунда", по осі ординат - кількість зафіксованих з’єднань (мережевих пакетів) у відповідну

секунду. Завдяки цьому графіку вдалося чітко ідентифікувати різкі піки навантаження, що можуть свідчити про наявність аномальної активності в мережі.

На діаграмі спостерігається кілька характерних сплесків, де кількість з'єднань перевищує 1500 пакетів за одну секунду. Такі значення є нетиповими для звичайного користувацького трафіку і можуть вказувати на фонову атаку типу UDP flood або масове сканування портів з боку зовнішнього або внутрішнього вузла.

Крім того, у підсумковій статистиці було виявлено низку IP-адрес з аномально високою кількістю з'єднань:

- IP 46.63.116.172 - 4176 з'єднань;
- IP 192.168.0.105 - 1111 з'єднань;
- IP 172.217.16.14 - 385 з'єднань;
- IP 142.250.75.22 - 111 з'єднань;
- IP 23.211.74.105, 142.250.186.196 - понад 50 з'єднань.

Зокрема, IP-адреса 46.63.116.172 продемонструвала надзвичайно високу інтенсивність взаємодії, що значно перевищує типовий поріг у 20 - 30 з'єднань. Також власна IP-адреса вузла (192.168.0.105) вказує на можливу надмірну вихідну активність, що може бути спричинено запуском декількох потоків або дією локального сервісу.

Побудований графік дозволяє зробити висновок про наявність вираженої пікової активності в окремі моменти часу, що потребує подальшої перевірки. Така візуалізація є ефективним інструментом як для ручного, так і автоматизованого виявлення аномалій.

Отже, візуалізація трафіку дозволила чітко виявити піки активності та зіставити їх із джерелами підозрілих з'єднань. Графічне представлення динаміки трафіку значно полегшує аналіз мережевої поведінки та є ефективним доповненням до статистичних методів виявлення аномалій. Отримані результати підтверджують доцільність використання візуальних інструментів для оперативного виявлення потенційних загроз у приватній мережі.

## 3.3 Оцінка достовірності роботи системи виявлення аномалій

Після завершення етапу реалізації системи виявлення аномалій у мережевому трафіку постає необхідність об'єктивної оцінки її ефективності, що є пріорітетним кроком у процесі перевірки придатності розробленого рішення до використання в умовах реального інформаційного середовища. Така оцінка передбачає не лише перевірку працездатності окремих модулів системи, але й аналіз загальної якості детектування відхилень, здатності до виявлення прихованих атак, рівня точності реакцій, чутливості до навмисного обфускування або шифрування трафіку, а також стабільності функціонування при змінному мережевому навантаженні. Підґрунтям для оцінювання є низка експериментів, які було проведено в тестовому середовищі, що моделює роботу невеликої приватної мережі з типовими вузлами та симульованими аномальними подіями.

Методика оцінювання базується на застосуванні основних метрик якості, таких як точність, повнота, рівень хибних спрацювань, затримка детектування, а також якість логування та візуального відображення інцидентів. Для формування контрольного трафіку використовувався як нормальний мережевий обмін без зловмисної активності, так і трафік з ін'єкцією типових аномалій: мережеве сканування, підміна ARP-таблиць, аномальні DNS-запити, надмірна кількість підключень за короткий проміжок часу, а також тунелювання даних через дозволені порти. Усі тести були спрямовані на створення навантаження, яке могло б імітувати активність реального порушника або автоматизованого скрипта вторгнення. На основі цих сценаріїв оцінювалася реакція системи, насамперед модулів агрегації метрик, поведінкової моделі та модуля виявлення аномалій. Було зафіксовано частоту виявлення атак, випадки відсутності реакції, а також випадки помилкового спрацювання на нормальну активність, з метою глибокого аналізу меж чутливості та стабільності системи.

Однією з головних переваг реалізованої системи виявилося те, що в основі алгоритмів прийняття рішень закладено статистичний підхід з фіксацією

нормальної поведінки на основі зібраного профілю трафіку за «чистий» період. Це дозволило знизити рівень хибнопозитивних спрацювань при стандартній роботі користувачів мережі. Система не реагувала на звичайні піки трафіку або масові однотипні запити в межах допустимих параметрів. У той же час, виявлення різких змін у частоті або структурі пакетів викликало стабільну реакцію виявлення. Наприклад, при імітації швидкісного сканування з одного хосту система сигналізувала про зміну інтенсивності запитів за лічені секунди. Подібні результати були отримані також для ARP-спуфінгу та активності з підміною MAC-адрес, що підтверджує придатність системи для фіксації низькорівневих атак на інфраструктуру.

Значною перевагою також виявилась гнучкість побудови поведінкових профілів для окремих IP-адрес або вузлів, що дозволяє фіксувати не лише глобальні зміни в мережі, але й локальні відхилення у роботі окремих пристроїв. Наприклад, при запуску на клієнтському хості процесу, який генерує значний обсяг DNS-запитів до невідомих доменів, система коректно зафіксувала аномалію, не сплутавши її з типовою активністю інших клієнтів. Таким чином, ефективність виявлення не обмежується глобальним трафіком, а адаптується до мікроповедінкових змін на рівні хостів. Проте варто зазначити, що для виявлення складних, повільно протікаючих атак або довготривалого тунелювання через легальні канали, система потребує більш тривалого спостереження або поглибленого аналізу часу життя підключень, що вказує на межу поточної реалізації.

Ще одним аспектом оцінки ефективності є чутливість до шифрованого або заздалегідь маскованого трафіку. Після проведення тестів із запуском SSL-тунелів та VPN-з’єднань через стандартні порти, виявилося, що хоча система не аналізує вміст пакетів, вона здатна фіксувати зростання ентропії заголовків та тривалість стабільних з’єднань, що дозволяє в деяких випадках інтерпретувати такий трафік як потенційно аномальний. Водночас, точність виявлення в таких сценаріях знижується, що є типовою особливістю всіх систем, що базуються виключно на статистичному аналізі без глибокої інспекції вмісту. Це не є

недоліком системи як такої, а радше вказує на область подальшого вдосконалення шляхом інтеграції методів машинного навчання або семантичного аналізу трафіку.

Також у рамках оцінки ефективності тестувалася продуктивність і стабільність системи при навантаженні. Під час надсилання великої кількості запитів за короткий період або підключення десятків одночасних хостів система не втрачала продуктивності і продовжувала обробляти трафік у режимі реального часу. Час виявлення критичних відхилень зазвичай становив до 2 секунд після початку аномальної поведінки, що підтверджує відповідність критерію оперативності. Окрім цього, система вела журнал подій із фіксацією базових параметрів виявлених інцидентів, включаючи час, джерело, тип аномалії та супровідні метрики. Такий підхід дозволяє не лише виявляти події в момент їхнього виникнення, але й забезпечує базу для ретроспективного аналізу та побудови звітності.

У візуалізаційному модулі також закладено потенціал для оцінки ефективності. Графічне представлення трафіку до та після виявленої аномалії дозволяє верифікувати поведінку системи шляхом порівняння з відображеною структурою даних. Завдяки наявності гістограм частоти пакетів, графів з’єднань та температурних карт активності, користувач може переконатися в доцільності спрацювання системи або, навпаки, виявити приклади хибних реакцій. Це підвищує прозорість механізмів ухвалення рішень і сприяє довірі до результатів аналізу.

Проведене експериментальне оцінювання підтверджує, що реалізована система здатна ефективно виконувати функції виявлення аномальної активності у мережевому трафіку. Результати тестування вказують на високу точність виявлення атак низького рівня, прийнятний рівень хибних спрацювань, стабільність роботи під навантаженням та наявність інтуїтивних засобів верифікації рішень. Водночас спостерігаються обмеження щодо обробки зашифрованого трафіку та складних атак з обфускованими патернами, що створює підґрунтя для подальшого розвитку системи з використанням гібридних

або інтелектуальних підходів до аналізу. У сукупності ці характеристики дозволяють зробити висновок про практичну придатність системи до впровадження в середовищах з обмеженими ресурсами та потребою у швидкому, автономному виявленні загроз.

## 3.4 Висновки до розділу

У третьому розділі було розглянуто процес впровадження та тестування локальної системи виявлення прихованих атак у приватній мережі. Реалізована система є прототипом механізму захисту, здатного фіксувати мережеву активність, виявляти аномальні з'єднання та візуалізувати отримані результати для подальшого аналізу.

Першим кроком у межах реалізації стало створення експериментального середовища, у якому імітується робота звичайного користувача, потенційного атакувального вузла та вузла-монітору. Середовище побудоване у вигляді окремого Python-проєкту з використанням бібліотеки Scapy, яка забезпечила можливість прямого доступу до мережевого інтерфейсу та захоплення "сирих" мережевих пакетів. Було реалізовано функціонал перехоплення трафіку у реальному часі з фіксацією центральних параметрів кожного з'єднання: IP-адрес джерела і призначення, протоколу та часу передачі. Така структура дозволила створити повну картину мережевої активності протягом визначеного періоду.

На другому етапі було реалізовано статистичний аналіз зібраних даних, зокрема, підрахунок частоти повторення IP-адрес серед усіх перехоплених з’єднань. Виявлено, що надмірна кількість пакетів, які надходять від одного джерела за короткий проміжок часу, є надійним індикатором потенційної загрози зокрема, сканування портів, підготовки до атаки або самої атаки на відмову в обслуговуванні (DoS). Застосований підхід базується на бібліотеці collections.Counter, яка забезпечила ефективну агрегацію та фільтрацію IP-адрес за частотою появи. Після запуску системи в тестовому середовищі було виявлено

кілька IP-адрес, з яких надходило понад 1000 з’єднань за короткий час - що чітко вказує на аномальну поведінку. Водночас у звичайному легітимному трафіку такі показники практично не зустрічаються.

Третій етап передбачав візуалізацію мережевої активності за допомогою бібліотеки matplotlib. Графік, побудований на основі часових міток, дозволив наочно представити динаміку трафіку протягом усього періоду моніторингу. Були зафіксовані характерні сплески трафіку, де кількість пакетів у межах однієї секунди перевищувала 1000–1500, що ще раз підтвердило виявлення аномальної активності. Графічна інтерпретація даних доповнила статистичний аналіз, дозволивши зробити візуальний висновок про інтенсивність навантаження в окремі моменти часу. Отримані діаграми можуть бути використані як елемент звітності, або як інструмент для подальшого розширення системи у напрямку автоматичного реагування.

Загалом, у межах розділу 3 було повністю реалізовано та перевірено базову модель системи виявлення вторгнень, яка здатна:

- здійснювати пасивний моніторинг трафіку в локальній мережі;
- збирати, фільтрувати та аналізувати IP-з'єднання;
- виявляти джерела аномальної активності на основі частоти звернень;
- виводити результати у текстовому та графічному форматах для подальшого аналізу.

Одержані результати підтверджують практичну ефективність використаних методів, а також демонструють доцільність впровадження подібних систем на локальному рівні - наприклад, у рамках корпоративної мережі, малого офісу або домашнього середовища. Побудована система легко модифікується та масштабуються, що відкриває можливість її подальшого вдосконалення.

# ВИСНОВКИ

У межах цієї кваліфікаційної роботи було досліджено, спроєктовано та реалізовано систему виявлення прихованих атак у приватній мережі з використанням методів аналізу мережевого трафіку. Актуальність теми обумовлена зростаючою складністю і прихованістю сучасних кіберзагроз, які часто залишаються непоміченими традиційними засобами захисту. Особливу увагу було приділено виявленню аномальної активності за допомогою статистичного аналізу, побудові поведінкових моделей, а також ефективній візуалізації результатів для подальшого прийняття рішень.

У теоретичній частині роботи було розглянуто сучасні підходи до виявлення атак у комп'ютерних мережах, типологію аномалій, методи побудови моделей поведінки та специфіку роботи інструментів збору й обробки трафіку. Проведений аналіз дозволив визначити оптимальні підходи для створення системи, орієнтованої на приватне середовище, де важлива не тільки точність, але й швидкодія, масштабованість та низький рівень хибнопозитивних спрацювань.

У практичній частині було реалізовано систему на базі Python з використанням бібліотеки Scapy для перехоплення й аналізу трафіку. Було розроблено модулі для агрегування даних у часових вікнах, виявлення аномалій через відхилення від базової поведінкової моделі, а також модуль візуалізації результатів. Створена система дозволяє в реальному часі виявляти підозрілу активність, наприклад різкі зміни частоти пакетів, підозріло високу інтенсивність з'єднань або незвичну поведінку окремих хостів.

В ході впровадження у тестове середовище було перевірено ефективність системи на прикладах типових атак, зокрема сканування портів, фрагментованого трафіку та симуляцій прихованого тунелювання. Система продемонструвала здатність виявляти відхилення на ранніх етапах, що підтверджує її прикладну цінність для захисту локальних мереж

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ


1. Address Allocation for Private Internets Datatracker URL: https://datatracker.ietf.org/doc/html/rfc1918 (дата звернення 19.01.2025)

2. Using 31-Bit Prefixes on IPv4 Point-to-Point Links Datatracker URL: https://datatracker.ietf.org/doc/html/rfc3021 (дата звернення 19.01.2025)

3. Network Address Translation (NAT) Terminology and Considerations Datatracke URL: https://datatracker.ietf.org/doc/html/rfc2663 (дата звернення 19.01.2025)

4. Understanding Local Area Networks (LANs) Cisco URL: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-lan.html (дата звернення 20.01.2025)

5. What is an Enterprise Network?, Fortinet URL: https://www.fortinet.com/resources/cyberglossary/enterprise-network (дата звернення 20.01.2025)

6. VPN Overview, Cloudflare Learning Center URL: https://www.cloudflare.com/learning/network-layer/what-is-a-vpn/ (дата звернення 21.01.2025)

7. Wi-Fi Security: WPA2 and WPA3, Wi-Fi Alliance URL: https://www.wi-fi.org/discover-wi-fi/security (дата звернення 24.01.2025)

8. Understanding ARP Spoofing: Techniques & Countermeasures, Imperva URL: https://www.imperva.com/learn/ddos/arp-spoofing/ (дата звернення 27.01.2025)

9. MITM (Man-In-The-Middle) Attacks, IBM Security URL: https://www.ibm.com/topics/mitm (дата звернення 30.01.2025)

10. DNS Spoofing: Як Захистити Систему? Cyberset URL: https://cyberset.com.ua/network/dns-spoofing-yak-zahistiti-systemu/ (дата звернення 02.02.2025)

11. What is IDS and IPS? Juniper URL: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html (дата звернення

03.02.2025)

12. SIEM (Security Information and Event Management) Explained, CrowdStrike
URL: https://www.crowdstrike.com/cybersecurity-101/siem/ (дата звернення 05.02.2025)

13. Insider Threats: Detect, Respond, Mitigate MITRE URL: https://www.mitre.org/publications/technical-papers/insider-threats-detect-respond-mitigate (дата звернення 06.02.2025)

14. Active vs Passive Attacks TechTarget URL: https://www.techtarget.com/searchsecurity/definition/passive-attack (дата звернення 06.02.2025)

15. OSI Model Security Threats Fortinet URL: https://www.fortinet.com/resources/cyberglossary/osi-model (дата звернення 08.02.2025)

16. MAC Flooding & VLAN Hopping Explained Cisco Press URL: https://www.ciscopress.com/articles/article.asp?p=2202410 (дата звернення 10.02.2025)

17. Understanding ARP Spoofing RedHat URL: https://www.redhat.com/sysadmin/understanding-arp-spoofing (дата звернення 11.02.2025)

18. TCP Session Hijacking OWASP Foundation URL: https://owasp.org/www-community/attacks/Session_hijacking_attack (дата звернення 13.02.2025)

19. Network Sniffing Tools and Defense IBM Security URL: https://www.ibm.com/topics/packet-sniffing

20. Types of DoS and DDoS Attacks Radware URL: https://www.radware.com/security/ddos-chronicles/types-of-ddos-attacks/ (дата звернення 15.02.2025)

21. Brute Force Attacks: Techniques & Defenses SANS Institute URL: https://www.sans.org/blog/brute-force-attacks-techniques-defenses/ (дата звернення 16.02.2025)

22. Malware Types and Threats US-CERT (CISA) URL: https://www.cisa.gov/news-events/news/malware-brief-overview (дата звернення 17.02.2025)

23. EternalBlue Vulnerability Analysis Rapid7 URL: https://www.rapid7.com/blog/post/2017/05/15/eternalblue-exploit-analysis/ (дата звернення 18.02.2025)

24. Attacking and Defending NTLM and Kerberos FireEye URL: https://www.fireeye.com/blog/threat-research/2019/10/kerberos-attack-techniques.html (дата звернення 20.02.2025)

25. IoT Attack Surface Expansion Forescout Research URL: https://www.forescout.com/company/resources/the-rise-of-iot-attacks/ (дата звернення 22.02.2025)

26. What UEBA Stands For Exabeam URL:https://www.exabeam.com/explainers/ueba/what-ueba-stands-for-and-a-5-minute-ueba-primer/ (дата звернення 23.02.2025)

27. Suricata IDS/IPS/NSM engine Open Information Security Foundation URL: https://suricata.io (дата звернення 25.02.2025)

28. Introduction to Zeek Zeek.org URL: https://zeek.org/what-is-zeek (дата звернення 01.03.2025)

29. What is an Intrusion Prevention System (IPS)? Palo Alto Networks URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips 04.03.2025

30. What is UEBA (User and Entity Behavior Analytics)? IBM URL: https://www.ibm.com/topics/ueba (дата звернення 08.03.2025)

31. Microsoft Defender for Identity documentation Microsoft URL: https://learn.microsoft.com/en-us/defender-for-identity/what-is (дата звернення 11.03.2025)

32. About Scapy Scapy URL: https://scapy.readthedocs.io/en/latest/introduction.html (дата звернення 14.03.2025)

33. Adaptive Adapters: An Efficient Way to Incorporate BERT Into Neural Machine Translation Researchgate URL: https://www.researchgate.net/publication/351299456_A_Statistical_Approach_for_Network_Anomaly_Detection (дата звернення 20.03.2025)

34. Understanding Application Layer Attacks Akamai URL: https://www.akamai.com/blog/security/application-layer-attacks (дата звернення 26.03.2025)

35. Simple Line Plot Example Matplotlib URL: https://matplotlib.org/stable/gallery/lines_bars_and_markers/simple_plot.html (дата звернення 01.04.2025)

36. Deep Packet Inspection (DPI), Cloudflare URL: https://www.cloudflare.com/learning/ddos/glossary/deep-packet-inspection/ (дата звернення 09.04.2025)

37. Real-Time Network Traffic Visualization Techniques, Ieeexplore URL: https://ieeexplore.ieee.org/document/9387330 (дата звернення 20.04.2025)

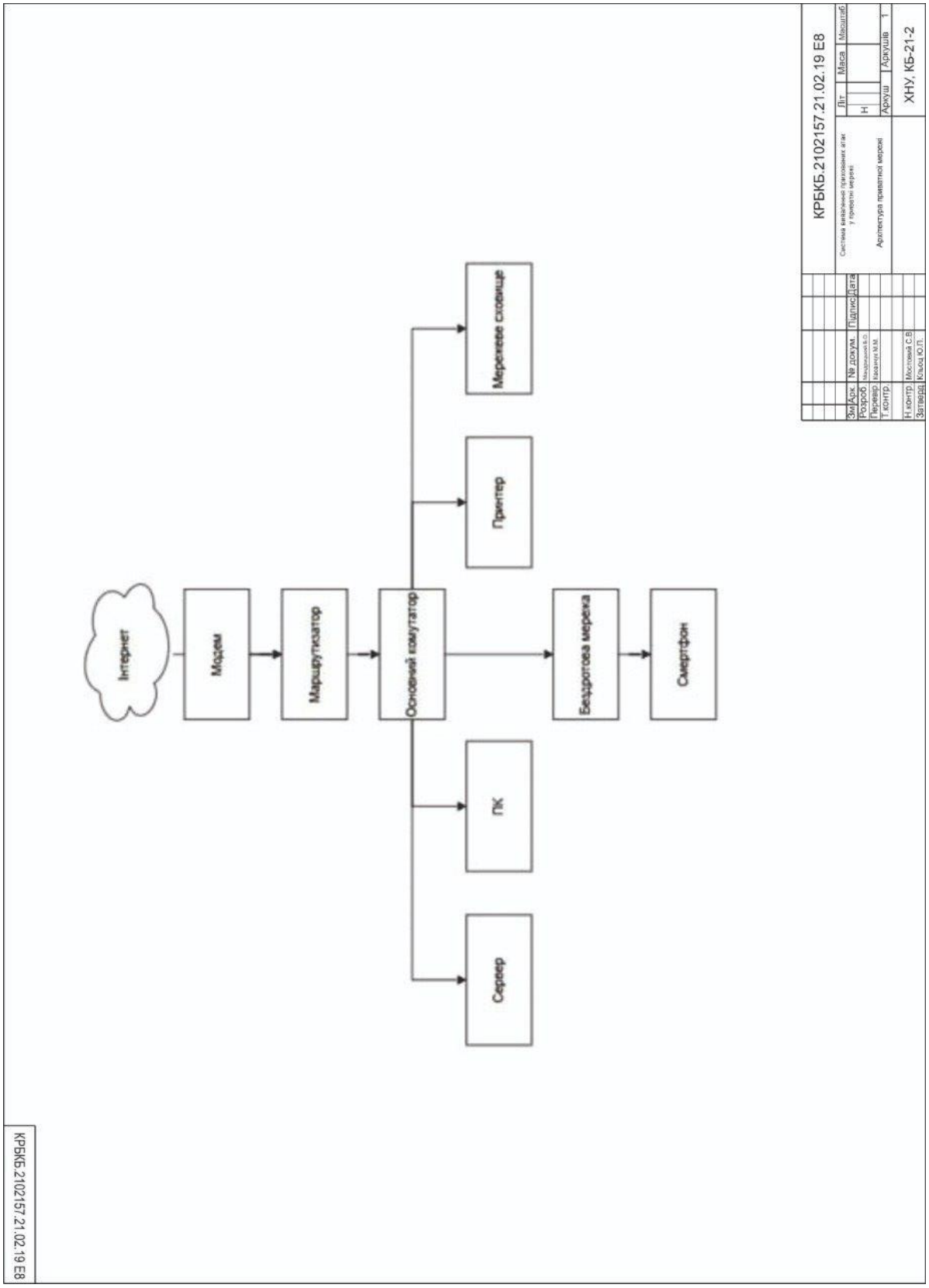
38. Statistical Data Visualization Seaborn URL: https://seaborn.pydata.org (дата звернення 22.04.2025)

39. Interactive Graphing Library Ploty URL: https://plotly.com/python (дата звернення 02.05.2025)

40. Open Observability Platform Grafana URL: https://grafana.com (дата звернення 09.05.2025)

Додаток А

Копія графічної частини



КРБКБ.2102157.21.02.19 Е8


| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102157.21.02.19 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | Система виявлення прихованих атак у приватні мережі | Літ | Маса / Масштаб |
| Розроб. | | Мандрицький В.О. | | | Схема логіки візуалізації результатів аналізу трафіку | Н | |
| Перевір. | | Кравчук М.М. | | | | Аркуш | Аркушів 1 |
| Т.контр. | | | | | | | |
| Н.контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | |
| Затверд. | | Кльоц Ю.П. | | | | | |


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | КРБКБ.2102157.21.02.19 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | Система виявлення прихованих атак у приватній мережі | Літ | Маса | Масштаб |
| Розроб. | | Макдецький К.О. | | | Схема моделі експлоїтів прихованих атак у приватній мережі | Н | | |
| Перевір. | | Кваснук М.М. | | | | Аркуш | Аркушів 1 | |
| Т.контр. | | | | | | | | |
| Н.контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | | |
| Затвердив | | Кольод Ю.П. | | | | | | |

Додаток Б

Аналізатор та візуалізатор мережевого трафіку

```
from scapy.all import sniff, IP
from datetime import datetime
captured_packets = []
def handle_packet(packet):
if IP in packet:
ip_src = packet[IP].src
ip_dst = packet[IP].dst
proto = packet[IP].proto
timestamp = datetime.now().strftime("%H:%M:%S")
print(f"[{timestamp}] {ip_src} -> {ip_dst} (proto: {proto})")
captured_packets.append((ip_src, ip_dst, proto, timestamp))
sniff(prn=handle_packet, store=0, timeout=30)
print("\nCaptured packets:")
for pkt in captured_packets:
from collections import Counter
ip_sources = [pkt[0] for pkt in captured_packets]
counter = Counter(ip_sources)
print("\nПідозріла активність (IP-адреси з великою кількістю з'єднань):")
for ip, count in counter.items():
if count > 20:
print(f"⚠ {ip} -{count} з'єднань")
import matplotlib.pyplot as plt
from collections import defaultdict
time_counts = defaultdict(int)
for pkt in captured_packets:
time_counts[pkt[3]] += 1 # pkt[3] - це час
sorted_times = sorted(time_counts.items())
times = [t[0] for t in sorted_times]
counts = [t[1] for t in sorted_times]
plt.figure(figsize=(10, 5))
plt.plot(times, counts, marker='o')
plt.title('Активність мережевого трафіку (кількість пакетів за часом)')
plt.xlabel('Час (гг:хх:сс)')
plt.ylabel('Кількість з’єднань')
plt.xticks(rotation=45)
plt.grid(True)
plt.tight_layout()
plt.show()
print(pkt)
```

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Мандрицького Богдана Олександровича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-2

# ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

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

10.06.25
дата

підпис

# Anti-Plagiarism (UA) v-15.281 Educational

**The maximum coincidence with one document 1.0%**

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

| | Document | | Sum coincidence on the DB | |
|---|---|---|---|---|
| | Symbols | Lexemes | Symbols | Lexemes |
| ID: 245268<br>Title: Система виявлення прихованих атак у приватній мережі<br>Added in a DB: 2025-06-12<br>Authors: Мандрицький Богдан Олександрович<br>Heads: Касянчук М.М.<br>Consultants:<br>Opponents: | 92046 | 617 | 505 (1%) | 5 (1%) |

Plagiarism sources

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

**Протокол аналізу звіту подібності науковим керівником**

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

**Автор:** Мандрицький Богдан Олександрович

**Співавтор:**

**Назва:** Система виявлення прихованих атак у приватній мережі

**Науковий керівник:**

**Підрозділ:** Кафедра кібербезпеки

**Коефіцієнт подібності 1:**0.9%

**Коефіцієнт подібності 2:**0.2%

**Мікропробіли:** 0

**Заміна букв:** 0

**Інтервали:** 0

**Білі знаки:** 0

**Дата створення звіту:** 2025-06-12 09:34:36.0

**Після аналізу Звіту подібності констатую наступне:**

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

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

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

Обгрунтування:

12.06.2025р.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система виявлення прихованих атак у приватній мережі

Автор: Мандрицький Богдан Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Науковий керівник: Михайло КАСЯНЧУК, докт. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

| № | Висновок | Позначка про відповідність |
|---|---|---|
| 1 | Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту. | відповідає |
| 2 | Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи. | |
| 3 | Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат. | |
| 4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту. | |
| 5 | Інше: | |

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 99,1%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Михайло КАСЯНЧУК

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Мандрицький Богдан Олександрович

Тема Система виявлення прихованих атак у приватній мережі.

Спеціальність 125 – Кібербезпека

**Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:**

кількість листів креслень 3; кількість сторінок записки 62.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено систему виявлення прихованих атак у приватній мережі з використанням методів статистичного аналізу трафіку. Реалізовано підхід до виявлення аномалій без використання сигнатур, на основі поведінкових характеристик мережевої активності. Практична частина включає обробку трафіку за допомогою бібліотеки Scapy (Python), побудову моделей нормальної активності, автоматичне виявлення відхилень та візуалізацію результатів. Рішення адаптовано до умов невеликих локальних мереж, з можливістю масштабування в більші середовища..

2. Висновок про відповідність кваліфікаційної роботи завданню. Робота повністю відповідає затвердженій темі, програмі підготовки та завданню. Усі поставлені задачі реалізовано повною мірою: виконано теоретичний огляд, побудовано модель, здійснено програмну реалізацію, виконано тестування та оцінку ефективності. Практична частина логічно продовжує теоретичний аналіз, забезпечуючи зв'язок між концепцією і реалізацією.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У роботі систематизовано підходи до виявлення атак, наведено класифікацію загроз на основі моделі OSI. Проаналізовано сучасні засоби виявлення атак (IDS, IPS, SIEM, UEBA, AI/ML), наведено порівняльну характеристику. У другому розділі обґрунтовано метод статистичного виявлення аномалій, побудовано архітектурну схему, описано функціональну логіку системи. У третьому розділі реалізовано систему на мові Python із використанням Scapy, PyShark, Matplotlib, Seaborn. Результати тестування свідчать про здатність системи виявляти сканування, зміни частоти запитів і підозрілі шаблони.

4. Позитивні сторони роботи Робота вирізняється логічною структурою, практичною спрямованістю та актуальністю. Запропонований підхід не потребує спеціалізованого обладнання, а отже придатний до впровадження у ресурсно обмежених умовах. Окремо слід відзначити якісне застосування відкритих технологій, а також адаптивність реалізованої системи до різних мережевих сценаріїв. Візуалізація результатів дозволяє легко ідентифікувати аномалії.

5. Негативні сторони роботи У системі відсутній графічний інтерфейс для керування системою, що ускладнює її використання некваліфікованими користувачами.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічна частина містить інформативні схеми: архітектура системи, логіка обробки, схема візуалізації. Пояснювальна записка відповідає вимогам університету, оформлення виконано охайно, стиль викладу технічно коректний, без значних граматичних помилок.

7. Відгук про роботу в цілому Робота є самостійним інженерним проєктом, який вирішує актуальне завдання з кібербезпеки. Всі етапи - від постановки задачі до тестування системи виконані на високому рівні. Робота демонструє здатність автора до системного аналізу, використання сучасних засобів програмування та критичного мислення.

8. Інші зауваження Рекомендується у подальшій роботі реалізувати графічний інтерфейс користувача та модулі автоматизованого реагування на інциденти, а також розглянути інтеграцію з SIEM-платформами.

9. Оцінка кваліфікаційної роботи Враховуючи всебічний аналіз, застосування сучасних технологій і якісну реалізацію, робота заслуговує оцінки «задовільно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Нічепорук Андрій Олександрович кандидат технічних наук, доцент кафедри комп'ютерної інженерії та інформаційних систем

« 12 » 06 2025. (підпис)