Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Шлапак Олександри Сергіївни

на здобуття ступеня вищої освіти Бакалавра

Система аналізу поведінки користувачів у мережах приватних підприємств

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

Шифр КРБКБ.2101135.21.01.15 ПЗ

Виконала студентка 4 курсу група КБ-21-1 Олександра ШЛАПАК
Керівник канд. техн. наук, доцент Віра ТІТОВА
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
09 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 Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шлапак Олександрі Сергіївні

1 Тема роботи Система аналізу поведінки користувачів у мережах приватних підприємств

Керівник роботи канд. техн. наук, доцент, Тітова Віра Юріївна

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи Створити систему аналізу поведінки користувачів в корпоративній мережі

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Загальна характеристика систем аналізу поведінки користувачів. Аналіз нетипової поведінки користувачів та джерела загроз. Розробка систем аналізу поведінки користувачів в корпоративних мережах

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Модель загроз. Система виявлення та ідентифікації пристроїв. Блок - схема алгоритму системи. Графічні елементи програми розробленої для дипломної роботи

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	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студентка _____ Олександра ШЛАПАК

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система аналізу поведінки користувачів у мережах приватних підприємств

Автор роботи: Шлапак Олександра Сергіївна

Керівник роботи: Тітова Віра Юріївна

Пояснювальна записка: 64 с., 3 додатки, 14 рисунків, 2 таблиці, 41 джерело.

Графічна частина: 3 плакати.

СИСТЕМА АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ В КОРПОРАТИВНІЙ МЕРЕЖІ

Кваліфікаційна робота присвячена розробці системи аналізу поведінки користувачів у мережах приватних підприємств. Вона досліджує методи та алгоритми для виявлення аномалій та загроз безпеці, що виникають внаслідок дій 0користувачів.

Робота включає аналіз існуючих підходів до аналізу поведінки користувачів, розробку моделі поведінки користувачів, яка враховує специфіку приватних підприємств, створення алгоритмів для виявлення аномалій та загроз безпеці, розробку програмного забезпечення для реалізації системи аналізу поведінки користувачів.

01.06.2025 _____

ABSTRACT

Topic of the qualification work: User behavior analysis system in private enterprise networks

Author of the work: Shlapak Oleksandra Sergiyevna

Supervisor: Titova Vira Yuriyevna

Explanatory note: 64 p., 3 appendices, 14 figures, 2 tables, 41 sources.

Graphic part: 3 posters.

USER BEHAVIOR ANALYSIS SYSTEM IN A CORPORATE NETWORK.

The qualification work is dedicated to the development of a system for analyzing user behavior in private enterprise networks. It explores methods and algorithms for detecting anomalies and security threats arising from user actions.

The work includes an analysis of existing approaches to user behavior analysis, development of a user behavior model that takes into account the specifics of private enterprises, creation of algorithms for detecting anomalies and security threats, and development of software for implementing a user behavior analysis system.

01.06.2025 _____

ЗМІСТ

ВСТУП

В епоху цифрової трансформації, де інформація є одним із найцінніших активів приватних підприємств, забезпечення її безпеки стає першочерговим завданням. Зростання кількості та складності кібератак, а також ризики, пов'язані з внутрішніми загрозами, вимагають від організацій постійного вдосконалення своїх систем захисту. У цьому контексті особливу увагу привертають системи аналізу поведінки користувачів (САПК), які здатні виявляти потенційно небезпечну активність на основі аналізу дій співробітників у корпоративній мережі.

Актуальність даної кваліфікаційної роботи зумовлена кількома ключовими факторами. По - перше, традиційні методи захисту, такі як міжмережеві екрани та антивірусне програмне забезпечення, часто виявляються недостатньо ефективними проти складних атак та інсайдерських загроз. САПК пропонують проактивний підхід до виявлення аномалій, що дозволяє запобігти інцидентам інформаційної безпеки на ранніх стадіях. По - друге, зростання обсягів даних, що генеруються користувачами в корпоративних мережах, робить ручний аналіз практично неможливим. Автоматизовані системи аналізу поведінки користувачів здатні обробляти великі масиви даних у реальному часі, виявляючи закономірності та відхилення, які можуть вказувати на загрозу. По - третє, специфіка приватних підприємств, які часто мають унікальні бізнес - процеси та вимоги до безпеки, зумовлює необхідність адаптованих та ефективних рішень у сфері аналізу поведінки користувачів.

Метою даної кваліфікаційної роботи є дослідження та розробка системи аналізу поведінки користувачів, яка б враховувала особливості мереж приватних підприємств та забезпечувала своєчасне виявлення потенційних загроз інформаційній безпеці. Для досягнення поставленої мети передбачається вирішення ряду завдань. Насамперед, буде розглянуто загальні характеристики систем аналізу поведінки користувачів, включаючи їхні основи, методи збору та обробки даних про активність користувачів, а також роль моніторингу мережевого

трафіку та аналізу пакетів у забезпеченні безпеки. Окрему увагу буде приділено огляду існуючих систем аналізу поведінки користувачів та аналізу наслідків нетипової поведінки для інформаційної безпеки підприємства. Далі буде проаналізовано нетипову поведінку користувачів та визначено основні джерела загроз у мережах приватних підприємств. Це включає класифікацію нетипової поведінки, розгляд моделей внутрішніх та зовнішніх загроз безпеки мережі, а також дослідження методів виявлення аномальної активності користувачів та аналіз їхніх наслідків для інформаційної безпеки. На завершення буде проведено розробку системи аналізу поведінки користувачів в корпоративних мережах, включаючи обґрунтування необхідності створення системи аналізу поведінки користувачів, опис структури пропонованої системи, а також демонстрацію роботи системи аналізу поведінки користувачів.

Предметом дослідження є процеси аналізу поведінки користувачів у мережах приватних підприємств. Об'єктом дослідження є система аналізу поведінки користувачів як інструмент підвищення рівня інформаційної безпеки приватного підприємства.

Практичне значення отриманих результатів полягає у можливості використання розробленої системи або рекомендацій щодо її побудови для підвищення рівня інформаційної безпеки приватних підприємств, зменшення ризиків витоку інформації та запобігання кіберінцидентам.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА СИСТЕМ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ

1.1 Основи аналізу поведінки користувачів у корпоративних мережах

Корпоративна мережа - це зв'язок між комп'ютерами одного підприємства навіть в тому випадку, якщо офіси компанії географічно віддалені один від одного. Користувачами корпоративної мережі є тільки співробітники даного підприємства [1]. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям або користувачам (рисунок 1.1)

Рисунок 1.1 - Побудова корпоративних мереж

Корпоративною мережею вважається будь - яка мережа, що працює по протоколу TCP/IP і використовує комунікаційні стандарти Інтернету, а також сервісні застосування, що забезпечують доставку даних користувачам мережі. Корпоративні мережі дозволяють забезпечити колективну обробку даних користувачами підключених в мережу комп'ютерів і обмін даними між цими

користувачами, сумісне використання програм, сумісне використання принтерів, модемів та інших пристроїв.

Використання обчислювальних мереж дає підприємству наступні можливості:

- розподіл ресурсів;
- вдосконалення комунікацій;
- поліпшення доступу до інформації;
- швидке і якісне ухвалення рішень;
- свобода в територіальному розміщенні комп'ютерів.

Аналіз поведінки базується на збору та обробці даних про дії користувачів, таких як вхід у систему, використання корпоративних ресурсів, звернення до бази даних, робота з файлами та мережевими з'єднаннями. Одним із ключових підходів є моніторинг мережевого трафіку, який дає змогу фіксувати всі вхідні та вихідні з’єднання, аналізувати вміст переданих даних і виявляти позитивні дії. Наприклад, різке збільшення обсягу вихідного трафіку може свідчити про спробу витоку конфіденційної інформації [2].

Корпоративна мережа складається з різних компонентів, таких як сервери, комп’ютери співробітників, маршрутизатори, бази даних та інші ресурси. Користувачі взаємодіють із нею через різні пристрої та програмне забезпечення, залишаючи цифрові сліди, які можуть бути використані для аналізу їхньої поведінки. Основним принципом аналізу є збір і обробка даних про активність користувачів, включаючи ідентифікацію їхніх облікових записів, моніторинг спроб входу в систему, аналіз використання ресурсів та оцінку мережевих з'єднань.

Корпоративну мережу корисно розглядати як складну систему, що складається з декількох взаємодіючих шарів. У основі лежить шар комп’ютерних центрів зберігання і обробки інформації, і транспортна підсистема, що забезпечує надійну передачу інформаційних пакетів між комп'ютерами.

- над транспортною системою працює шар мережевих операційних систем, який організовує роботу додатків в комп'ютерах і надає через транспортну систему ресурси свого комп'ютера в загальне користування;

- над операційною системою працюють різні застосування, але за особливої ролі систем управління базами даних, що зберігають у впорядкованому виді основну корпоративну інформацію і що виробляють над нею базові операції пошуку, цей клас системних застосувань зазвичай виділяють в окремий шар корпоративної мережі;

- на наступному рівні працюють системні сервіси, які, користуючись СУБД, як інструментом для пошуку потрібної інформації, надають кінцевим користувачам цю інформацію в зручній для ухвалення рішення формі. А також ці системи виконують деякі загальні для підприємств усіх типів процедури обробки інформації. До цих сервісів відноситься служба World Wide Web, система електронної пошти, системи колективної роботи і багато інших;

- верхній рівень корпоративної мережі представляють спеціальні програмні системи, які виконують завдання, специфічні для цього підприємства або підприємств цього типу. Прикладами таких систем можуть служити системи автоматизації банку, організації бухгалтерського обліку, автоматизованого проєктування, управління технологічними процесами і тому подібне.

Кінцева мета корпоративної мережі втілена в застосовних програмах верхнього рівня, але для їх успішної роботи абсолютно необхідно, щоб підсистеми інших шарів чітко виконували свої функції [3].

Основна проблема, яку доводиться вирішувати при створенні корпоративної мережі - організація каналів зв'язку. Канали зв'язку створюються по лініях зв'язку за допомогою складної електронної апаратури і кабелів зв'язку. При цьому канали за характером переданих сигналів можуть бути аналоговими або цифровими, тобто на одній лінії зв'язку одночасно можна створити як аналогові, так і цифрові канали, що функціонують окремо. Для цього застосовують апаратуру формування каналів. Типи каналів зв’язку та їх особливості показано в табличці 1.1.

Таблиця 1.1 - Типи каналів зв’язку та їх особливості

Тип каналу	Характеристика	Приклад використання
Аналоговий	Передає сигнали у вигляді безперервної електромагнітної хвилі. Має більшу чутливість до перешкод, але може передавати голосові та відеосигнали без складного кодування.	Телефонні лінії, аналогове радіо.
Цифровий	Передає дані у вигляді дискретних сигналів (0 та 1). Відрізняється високою завадостійкістю та можливістю передавання великих обсягів даних.	Інтернет - з’єднання, комп’ютерні мережі.

Аналогові канали використовують безперервну електромагнітну хвилю, що забезпечує передачу голосових або відеосигналів, але водночас вони є більш чутливими до перешкод. Цифрові канали, які працюють на основі двійкових сигналів (0 та 1), мають кращу завадостійкість, дозволяють передавати значні обсяги даних і широко застосовуються у комп’ютерних мережах. В сучасних умовах на одній лінії зв’язку можуть одночасно працювати як аналогові, так і цифрові канали, що стало можливим завдяки спеціальному обладнанню, яке дозволяє розподіляти ресурси мережі відповідно до потреб компанії.

Однією з ключових технологій, які забезпечують ефективне використання каналів зв’язку, є мультиплексування. Це метод, що дозволяє передавати кілька потоків даних через один фізичний канал шляхом їхнього поділу за певними параметрами. Частотне мультиплексування використовується в аналогових системах, де кожен канал передає інформацію на окремій частоті, що дозволяє уникнути взаємних перешкод. Часове мультиплексування застосовується у

цифрових мережах і ґрунтується на розподілі смуги пропускання між каналами в різні часові інтервали.

Організація каналів зв’язку в корпоративних мережах вимагає використання спеціального обладнання, такого як маршрутизатори, комутатори, мультиплексори та модеми. Маршрутизатори та комутатори забезпечують передачу цифрових даних між сегментами мережі та оптимізують потоки інформації, запобігаючи перевантаженню. Мультиплексори дозволяють ефективно поєднувати кілька потоків даних в один канал, що особливо важливо при передачі інформації між віддаленими підрозділами компанії. Модеми перетворюють цифрові сигнали в аналогові та навпаки, що дає змогу підключатися до традиційних телефонних ліній або використовувати інші види комунікацій.

Таким чином, організація каналів зв’язку є одним із ключових завдань при створенні корпоративної мережі. Вона вимагає врахування не лише поточних потреб компанії, а й можливості масштабування мережі в майбутньому. Використання сучасних технологій дозволяє не тільки забезпечити якісний зв’язок між підрозділами, а й підвищити загальну ефективність роботи корпоративної інфраструктури, мінімізуючи ризики втрати даних та збоїв у системі.

Системи аналізу поведінки користувачів відіграють важливу роль у забезпеченні інформаційної безпеки компаній. Вони дозволяють своєчасно виявляти як внутрішні, так і зовнішні загрози, запобігати несанкціонованому доступу, оптимізувати політику контролю доступу та автоматизувати процес виявлення підозрілих дій. Завдяки традиційним правилам поведінкової аналітики сучасні компанії можуть ефективно захищати свої мережі та дані від потенційних загроз.

1.2 Методи збору та обробки даних про активність користувачів

Аналіз поведінки користувачів у корпоративних мережах базується на зборі та обробці великих обсягів даних, що відображають взаємодію співробітників із цифровими ресурсами компанії. Це необхідно для виявлення аномальної активності, запобігання витоку конфіденційної інформації, виявлення внутрішніх і зовнішніх загроз, а також оптимізації мережевих процесів. Ефективність систем аналізу залежить від точності та повноти зібраних даних, а також від методів їх обробки.

Для збору інформації використовуються різні джерела, серед яких найбільш важливими є журнали подій та лог-файли, аналіз мережевого трафіку, контроль файлової активності, моніторинг систем аутентифікації та управління доступом.

Файли журналу - це текстові файли, які використовуються для запису того, що відбувається на сервері. Їх можна використовувати для діагностики проблем та з'ясування того, що пішло не так. Файл журналу є найважливішим джерелом інформації для усунення несправностей. Це також корисно для аналізу кількості відвідувачів вашого сайту, звідки вони приходять і чи отримують вони помилки при відвідуванні вашого сайту [4].

Лог-файли також стають безцінним інструментом під час виявлення й аналізу проблем безпеки та збоїв у системі. Записи про помилки і незвичайні події можуть слугувати сигналом про потенційні загрози або несправності. Моніторинг подібних подій дає змогу оперативно реагувати на проблеми та забезпечувати безпечніше й надійніше функціонування застосунку. Крім того, лог-файли важливі і для аудиту, забезпечення відповідності стандартам безпеки. Записи про операції з даними, аутентифікацію та інші події можна використовувати для створення звітів, аналізу дій користувачів і забезпечення відповідності правилам і регулювання. Лог-файли можуть містити конфіденційну інформацію, таку як імена користувачів, паролі та інші дані. Тому важливо забезпечити захист і конфіденційність даних у лог-файлах [5].

Аналіз мережевого трафіку (Network Traffic Analyzer, NTA) - це метод моніторингу доступності та активності мережі для виявлення аномалій, зокрема проблем безпеки та роботи. Одним з основних завдань NTA є виявлення аномального трафіку, який може свідчити про кібератаку або іншу шкідливу дію. Наприклад, якщо велика кількість даних передається з одного джерела до багатьох призначень, це може свідчити про атаку DDoS. NTA дозволяє виявляти ці аномальні ситуації та сповіщати про них відповідних фахівців.

Аналіз мережевого трафіку є надзвичайно важливим для забезпечення стабільності, ефективності та безпеки мережі. Основні причини, чому аналіз мережевого трафіку є важливим:

- виявлення кіберзагроз та злочинної діяльності - аналіз мережевого трафіку дозволяє виявляти кіберзагрози та злочинну діяльність, такі як вторгнення, спам, фішинг та інші. Це допомагає запобігти можливим кібератакам та захистити мережу від шкідливих дій;
- підвищення ефективності мережі - аналіз мережевого трафіку дозволяє знайти проблеми з пропускною здатністю, визначити трафік, який споживає більше ресурсів мережі, та забезпечити оптимальне використання ресурсів мережі;
- відновлення роботи мережі - аналіз мережевого трафіку може допомогти відновити роботу мережі після виникнення проблем, таких як відмова обладнання чи програмного забезпечення;
- покращення безпеки мережі - аналіз мережевого трафіку може допомогти виявити вразливості в мережі та допомогти виправити їх, щоб уникнути можливих кібератак;
- підтримка рішень - аналіз мережевого трафіку може допомогти приймати обґрунтовані рішення щодо конфігурації мережі, вибору обладнання та відповідності вимогам безпеки.

Аналіз мережевого трафіку є важливим інструментом для забезпечення безпеки та ефективності мережі, а також для виявлення проблем та підтримки рішень [6].

Контроль файлової активності - це один із ключових методів забезпечення інформаційної безпеки в корпоративних мережах. Він дозволяє відстежувати всі дії користувачів із файлами та документами, що зберігаються на серверах, локальних пристроях або у хмарних середовищах. Такий моніторинг необхідний для запобігання витоку конфіденційної інформації, виявлення несанкціонованого доступу та аналізу підозрілих змін у файлах.

Система контролю файлової активності фіксує такі події, як створення, відкриття, редагування, копіювання, переміщення та видалення файлів. Крім того, вона може аналізувати метадані, зокрема, хто, коли та з якого пристрою здійснив операцію. Наприклад, якщо співробітник раптово починає масово копіювати файли з корпоративної мережі на зовнішні носії або завантажувати їх у хмарні сервіси, система може автоматично заблокувати такі дії або сповістити службу безпеки про потенційну загрозу [7].

Методи контролю файлової активності поділяються на кілька категорій. Найпростішим є ведення логів операцій, коли система записує всі зміни у файлах, створюючи історію взаємодії користувачів із документами.

Контроль файлової активності відіграє важливу роль у розслідуванні інцидентів безпеки. Якщо в компанії стався витік інформації, журнали файлової активності можуть допомогти встановити, хто отримував доступ до конфіденційних даних, коли це сталося і які дії були виконані. Це дозволяє оперативно реагувати на загрози, визначати винних та запобігати подібним випадкам у майбутньому.

Моніторинг систем аутентифікації та управління доступом є важливою складовою корпоративних мереж, оскільки дозволяє контролювати процес входу користувачів у систему, їхню взаємодію з ресурсами компанії та виявляти потенційні загрози. Аутентифікація забезпечує перевірку особи користувача перед наданням доступу до корпоративних сервісів, тоді як управління доступом регулює, які саме дії дозволені в межах його повноважень [8].

Основним завданням моніторингу є виявлення підозрілих або аномальних дій, які можуть свідчити про несанкціоновані спроби доступу, компрометацію облікових записів або порушення внутрішніх політик безпеки. Наприклад, якщо користувач входить у систему з незвичного місцезнаходження або використовує невідомий пристрій, система може автоматично заблокувати доступ або вимагати додаткову перевірку особи, наприклад, через двофакторну аутентифікацію.

Після збору інформації важливим етапом є її обробка та аналіз, що дозволяє виявити підозрілі дії та аномалії. Отримані дані проходять через серію фільтрів і алгоритмів, які дозволяють визначити закономірності поведінки користувачів, а також ідентифікувати можливі загрози.

Одним із ключових методів аналізу є правило - орієнтований підхід, коли система порівнює отримані дані з попередньо визначеними правилами. Наприклад, якщо користувач виконує спробу входу в систему з кількох географічно віддалених місць у короткий проміжок часу, система може розцінити це як потенційну компрометацію облікового запису.

Більш складним і гнучким є аналіз поведінкових відхилень, який ґрунтується на машинному навчанні та штучному інтелекті. Такий підхід передбачає створення моделей нормальної поведінки кожного користувача на основі історичних даних. Якщо система виявляє, що дії користувача значно відрізняються від його звичного шаблону роботи, вона може позначити таку активність як підозрілу. Наприклад, якщо працівник зазвичай отримує доступ до певного набору файлів, а раптом починає завантажувати великі обсяги інформації з нових ресурсів, це може сигналізувати про внутрішню загрозу або підготовку до витоку даних [9].

Також використовуються методи аналізу мережевого трафіку, які дозволяють оцінити характер переданих даних, визначити нетипові з’єднання та виявити потенційні атаки. Великий обсяг вихідного трафіку, часті запити до зовнішніх серверів або використання невідомих портів можуть свідчити про витік даних або дії шкідливого програмного забезпечення. Аналіз мережевого трафіку має

вирішальне значення для вирішення проблем із мережею, виявлення загроз безпеці та оптимізації продуктивності мережі.

Таким чином, якісний аналіз даних є основою ефективної системи кібербезпеки, яка не тільки фіксує порушення, але й допомагає запобігати потенційним загрозам. Використання сучасних алгоритмів та автоматизованих рішень дозволяє компаніям швидко адаптуватися до змінюваних загроз і забезпечувати стабільний рівень захисту корпоративних ресурсів.

1.3 Моніторинг мережевого трафіку, аналіз пакетів та їх роль у безпеці

Моніторинг - це систематичний збір і обробка інформації, яка може бути використана для поліпшення процесу ухвалення рішення, а також побічно для інформування громадськості або прямо як інструмент зворотного зв’язку в цілях здійснення проектів, оцінки програм або вироблення політики [10].

Моніторинг мережевого трафіку передбачає безперервне спостереження та запис мережевої активності, включаючи фіксацію інформації про передані дані, час передачі, джерела та призначення трафіку. Для цього використовуються різні методи та інструменти, такі як портове дзеркалювання, яке копіює трафік з портів комутатора, мережеві TAP, що пасивно копіюють трафік на фізичному рівні, а також програмні засоби моніторингу, що встановлюються на серверах або окремих системах для збору та аналізу мережевих даних. Детально про ці засоби показано в таблиці 1.2.

Також більш комплексні системи для моніторингу всієї мережі. Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) також постійно аналізують мережевий трафік на предмет підозрілої активності та можуть автоматично блокувати загрози.

Таблиця 1.2 – Поширені інструменти для аналізу пакетів та їх можливості

Інструмент	Операційна система	Основні можливості
Wireshark	Windows, macOS, Linux	Графічний інтерфейс, детальний розбір пакетів, фільтрація, аналіз протоколів, статистика
tcpdump	Linux, macOS, BSD	Командний рядок, потужні можливості фільтрації, низьке споживання ресурсів
Kismet	NIX, Windows, Cygwin, macOS	Захоплення пакетів, підтримка багатьох стандартів, одночасний моніторинг кількох каналів.

Під час моніторингу збираються різноманітні дані, включаючи IP-адреси джерела та призначення, номери портів, використовувані протоколи (TCP, UDP, ICMP, HTTP, DNS тощо), часові мітки подій, обсяг переданих даних та прапори TCP [11].

Постійний контроль за роботою локальної мережі, що становить основу будь-якої корпоративної мережі, необхідний для підтримки її в працездатному стані. Контроль - це необхідний перший етап, який повинен виконуватися при управлінні мережею. Зважаючи на важливість цієї функції її часто відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Такий поділ функцій контролю і власне управління корисно для невеликих і середніх мереж, які обов'язково потрібно інтегрованої системи управління економічно недоцільна. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки й пристрої мережі, а їх відключення або реконфігурацію він може виконувати в цьому випадку вручну.

Процес контролю роботи мережі зазвичай ділять на два етапи -моніторинг і аналіз. На етапі моніторингу виконується більш проста процедура - процедура збору первинних даних про роботу мережі: статистики про кількість циркулюючих

в мережі кадрів та пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів.

Далі виконується етап аналізу, під яким розуміється більш складний та інтелектуальний процес осмислення зібраної на етапі моніторингу інформації, зіставлення її з даними, отриманими раніше, і вироблення припущень про можливі причини повільної або ненадійної роботи мережі [12].

Аналіз пакетів є критично важливим для безпеки мережі, оскільки дозволяє виявляти різноманітні кібератаки в реальному часі або після інциденту, такі як сканування портів, атаки типу "відмова в обслуговуванні", вторгнення, витік даних та комунікації шкідливого програмного забезпечення з командними серверами. Крім того, він допомагає в розслідуванні інцидентів безпеки, виявленні внутрішніх загроз, моніторингу відповідності політикам безпеки та навіть в оптимізації продуктивності мережі. Для моніторингу та аналізу пакетів існує безліч інструментів, як безкоштовних (наприклад, Wireshark, tcpdump), так і комерційних (наприклад, SolarWinds Network Performance Monitor, Splunk).

Wireshark - це широко поширений аналізатор пакетів з відкритим вихідним кодом, який дозволяє перехоплювати та аналізувати мережевий трафік у режимі реального часу. Він може допомогти виявити та усунути неполадки в мережі та є цінним інструментом для аналітиків безпеки [13].

На рисунку 1.2 показано вікно програми Wireshark.

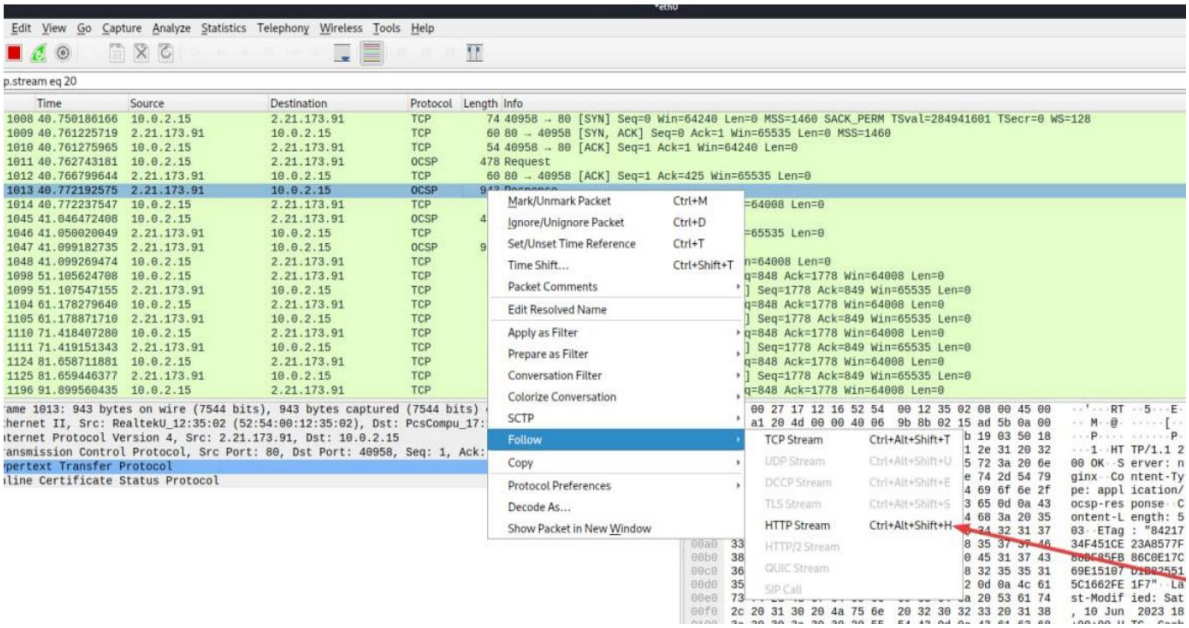


Рисунок 1.2 - Моніторинг трафіку за допомогою Wireshark і фільтрація за протоколом HTTP

TCPdump - це найуживаніша утиліта для усунення несправностей мережі адміністраторами мережі. Це сніффер/аналізатор пакетів командного рядка з відкритим вихідним кодом, який перехоплює TCP/IP - пакети, що передаються та одержуються через мережу через вказаний інтерфейс. Інструмент є вбудованим у дистрибутиви Linux з універсальними можливостями, включаючи різні фільтри та прапори [14].

Процес моніторингу мережевого трафіку зазвичай здійснюється за допомогою спеціалізованих інструментів, відомих як мережеві аналізатори або сніфери. Ці інструменти здатні перехоплювати мережевий трафік, що проходить через певний сегмент мережі або конкретний мережевий інтерфейс. Після перехоплення трафіку відбувається його аналіз пакетів, який включає декодування протоколів для розуміння використовуваних протоколів, вивчення вмісту пакетів для виявлення підозрілих патернів або шкідливого коду, статистичний аналіз трафіку для виявлення аномальних змін, пошук відомих сигнатур загроз та аналіз

поведінки трафіку для виявлення нетипових комунікаційних патернів. Приклад моніторингу мережевого трафіку показано на рисунку 1.2.

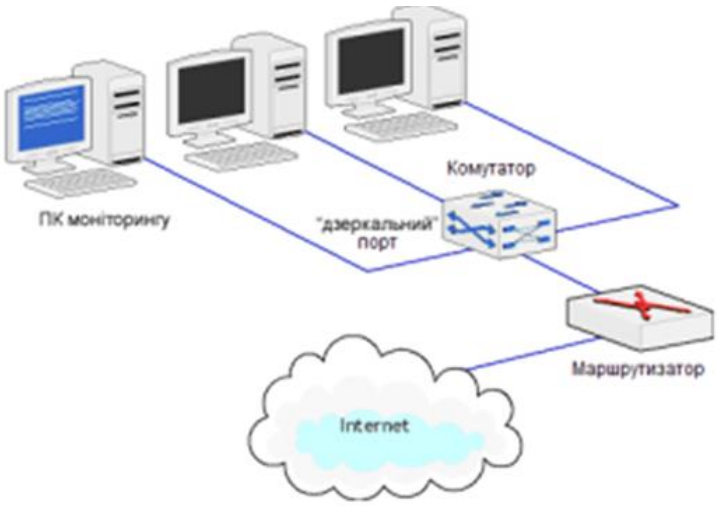


Рисунок 1.3 - Схема моніторингу мережевого трафіку

На даному рисунку зображено, як працює портове дзеркалювання на комутаторі, передаючи копію трафіку на окремий комп'ютер для моніторингу [15].

1.4 Наслідки нетипової поведінки для інформаційної безпеки підприємства

Нетипова поведінка користувачів та сутностей, таких як пристрої, додатки та мережеві вузли, у корпоративній мережі може мати серйозні та різноманітні наслідки для інформаційної безпеки підприємства. Виявлення таких аномалій є критично важливим, оскільки вони часто є ранніми індикаторами потенційних загроз, порушень політик безпеки або вже здійснених кіберінцидентів. Ігнорування або несвоєчасне реагування на нетипову поведінку може призвести до значних фінансових втрат, репутаційних ризиків, юридичних наслідків та порушення операційної діяльності.

Одним з основних наслідків є компрометація облікових записів, що передбачає несанкціонований доступ або контроль над онлайн - акаунтами людини, такими як електронна пошта, профілі в соціальних мережах, фінансові рахунки тощо. Це вторгнення не лише порушує приватність, але також створює значні загрози, дозволяючи зловмисникам неправомірно використовувати особисту інформацію, здійснювати шахрайські дії та потенційно ініціювати подальші кібербезпекові атаки, включно з кампаніями вимагання або фішингом [16]. Методики, які використовують кіберзлочинці для компрометації акаунтів, різноманітні та постійно еволюціонують, експлуатуючи цифрові сліди, які користувачі залишають в інтернеті. Звичайні методи включають [17]:

- крадіжка облікових даних - переважає через такі тактики, як фішингові електронні листи, соціальна інженерія, шпигунське ПЗ або кейлогери, крадіжка облікових даних передбачає пряме отримання логінів користувача;
- атаки Брут Форс - в цьому підході хакери використовують автоматизовані скрипти для невпинного підбору паролів користувача через систематичний метод проб і помилок, використовуючи слабкі або загальні паролі;
- витоки даних - це коли бази даних компрометованих вебсайтів, що містять імена користувачів, паролі або іншу персональну інформацію, зливаються, ці облікові дані можуть використовуватися для доступу до акаунтів, особливо коли паролі повторно використовуються;
- крадіжки токенів - представляють цифрові ключі, що тримають користувача залогіненим в сервісі, дозволяючи зловмисникам обійти необхідність пароля взагалі.

Іншим серйозним наслідком є інсайдерські загрози, що включають крадіжку інтелектуальної власності, саботаж, навмисне пошкодження даних або ненавмисні витоки чутливої інформації через нетипові дії співробітників. Інсайдерська загроза - це загроза безпеки з боку співробітника, колишнього співробітника або ділового партнера. Традиційні заходи забезпечують реальну безпеку на зовнішні атаки й не здатні запобігти внутрішній загрозі.

Інсайдери можуть діяти усвідомлено та неусвідомлено. Зазвичай їх поділяють на три категорії:

- зловмисні інсайдери - ті, хто навмисно зловживає обліковими даними для крадіжки інформації у фінансових чи особистих цілях. Наприклад, це може бути людина, яка незадоволена попереднім роботодавцем і тому дає секретну інформацію конкуренту. Інсайдери мають перевагу перед іншими зловмисниками, тому що вони знайомі з політикою та процедурою організації та їх вразливістю;
- інсайдери «з необережності» - невинні жертви, які ненавмисно наражають компанію на ризик. Це найпоширеніші типи внутрішніх загроз. Наприклад, співробітник може перейти за незабезпеченими посиланнями та заразити системними шкідливими програмними забезпеченнями;
- "кріт" - шахраї, які отримали інсайдерський доступ до привілейованої мережі. Це людина, яка вдає співробітника або партнера [18].

Крім того, нетипова поведінка може бути пов'язана з впровадженням та розповсюдженням шкідливого програмного забезпечення, такого як віруси, черв'яки, трояни або програми - вимагачі, що може призвести до зараження мережі, блокування даних або їхнього шифрування. Атаки на ланцюжок постачання також можуть проявлятися через нетипову активність облікових записів постачальників, які використовуються як плацдарм для атаки на підприємство.

Нетипова мережева активність, така як сканування мережі або портів, може бути ознакою розвідувальної діяльності зловмисників, які готуються до більш масштабної атаки. Крім того, нетипова поведінка може свідчити про порушення політик безпеки та нормативних вимог, наприклад, несанкціонований доступ до заборонених ресурсів або використання незатвердженого програмного забезпечення. Нарешті, надмірне споживання ресурсів внаслідок нетипової активності може призвести до зниження продуктивності та доступності критично важливих систем [19].

Ефективне виявлення та реагування на нетипову поведінку є ключем до мінімізації цих негативних наслідків. Впровадження систем аналізу поведінки

користувачів та сутностей (UEBA), які використовують машинне навчання для встановлення базових ліній поведінки та виявлення аномалій, є важливим кроком у підвищенні рівня інформаційної безпеки підприємства. Своєчасний аналіз нетипової поведінки дозволяє службам безпеки оперативно реагувати на потенційні загрози, запобігати їхньому розвитку та мінімізувати можливі збитки [20].

Для ефективного управління ризиками, пов'язаними з нетиповою поведінкою, організації повинні впроваджувати комплексні системи моніторингу та аналізу активності користувачів, систем і мережевого трафіку. Це передбачає визначення чітких базових рівнів нормальної поведінки для різних суб'єктів та процесів, що дозволить своєчасно виявляти будь-які відхилення. Важливим кроком є налаштування ефективної системи оповіщень про виявлення аномалій, яка дозволить оперативно реагувати на потенційні загрози. Крім того, необхідно розробити та впровадити чіткі процедури реагування на інциденти, пов'язані з нетиповою поведінкою, щоб мінімізувати потенційні збитки. Впровадження цих заходів дозволить організації значно підвищити свою стійкість до інформаційних загроз, пов'язаних з нетиповою поведінкою.

2 АНАЛІЗ НЕТИПОВОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ ТА ДЖЕРЕЛА ЗАГРОЗ

2.1 Класифікація нетипової поведінки в мережах приватних підприємств

Класифікація нетипової поведінки в мережах приватних підприємств є важливим етапом для розуміння спектру потенційних загроз та аномалій, що можуть виникати в корпоративному середовищі. Ця класифікація допомагає розробляти ефективні системи виявлення, реагування та запобігання інцидентам інформаційної безпеки. Нетипова поведінка може бути результатом як зловмисних дій, зовнішніх чи внутрішніх, так і випадкових помилок користувачів або технічних несправностей. За суб'єктом поведінки можна виділити кілька категорій.

Поведінка користувачів включає аномалії аутентифікації, такі як невдалі спроби входу з незвичних місць або у неробочий час, нетиповий доступ до ресурсів, наприклад, спроби відкрити файли, не пов'язані з посадовими обов'язками, незвичну активність з облікового запису, що проявляється у великому обсязі переданих даних або запуску невідомих процесів, порушення політик безпеки, включаючи спроби обходу обмежень, та реакцію на соціальну інженерію, наприклад, переходи за фішинговими посиланнями [21].

Поведінка пристроїв (кінцевих точок) характеризується незвичайним мережевим трафіком, нетиповим використанням системних ресурсів, змінами у системних файлах або конфігурації, встановленням неавторизованого програмного забезпечення та аномальною активністю периферійних пристроїв. Безпека кінцевої точки майже завжди живе або вмирає залежно від того, як вона захищає пристрої від доступу, зазвичай через зловмисне програмне забезпечення, крадіжку або помилку користувача. Таким чином, компоненти безпеки кінцевих точок часто нагадують стандартну безпеку домашнього користувача з додатковими міркуваннями про те, що користувач повинен і не повинен мати можливість робити на пристрої, підключеному до мережі. Критичні компоненти безпеки кінцевої точки включають [22]:

- антивірусне та антишкідливе ПЗ - антивірусні рішення є основними для виявлення та видалення шкідливого програмного забезпечення;

- брандмауери - вони відстежують вхідний і вихідний мережевий трафік і вирішують, дозволяти чи блокувати певний трафік на основі визначеного набору правил безпеки;

- системи запобігання вторгненням (IPS) - вони мають вирішальне значення для виявлення потенційних загроз і швидкого реагування на них;

- шифрування даних - шифрування даних на кінцевих точках гарантує, що вони залишаються нечитабельними та безпечними, навіть якщо дані перехоплюються або до них здійснюється неавторизований доступ;

- виявлення кінцевої точки та відповідь (EDR) - інструменти EDR постійно відстежують кіберзагрози та реагують на них.

Поведінка мережевих пристроїв (маршрутизаторів, комутаторів, брандмауерів) проявляється у незвичних журналах, неавторизованих змінах конфігурації, аномальному трафіку та атаках на інфраструктуру. Аномалії в їхній роботі можуть бути тривожним сигналом про кібератаки, технічні проблеми або помилкову конфігурацію, що потенційно призводить до збоїв у зв'язку, витоку важливих даних або повної відмови в обслуговуванні. Одним із ключових аспектів є аналіз незвичайних журналів. Раптове збільшення кількості помилок може свідчити про проблеми з обладнанням, некоректні налаштування або спроби зловмисників скористатися вразливостями. Іншим важливим аспектом є зміни конфігурації. Неавторизовані модифікації правил брандмауера, налаштувань маршрутизації або списків контролю доступу можуть відкрити шлях для атак або надати зловмисникам доступ до внутрішніх ресурсів. Слід звертати увагу на атаки на інфраструктуру, такі як спроби DoS/DDoS атак, сканування портів з внутрішньої мережі на критичні сервери, ARP - спуфінг та атаки на протоколи маршрутизації, які можуть серйозно порушити роботу мережі [23].

Поведінка серверів може включати нетипове використання ресурсів, аномальну активність додатків, зміни у файловій системі, нетипові мережеві

з'єднання та компрометацію облікових записів служб. Сервери є серцем інформаційної інфраструктури приватного підприємства, зберігаючи та обробляючи найважливіші дані та забезпечуючи функціонування ключових сервісів. Тому будь - яка нетипова поведінка серверів може бути ознакою серйозної загрози, проблем з продуктивністю або помилкових налаштувань. Одним з перших індикаторів є нетипове використання ресурсів. Раптове та значне зростання навантаження на центральний процесор, використання оперативної пам'яті або дискової підсистеми без видимих причин, а також неочікуване збільшення мережевого трафіку можуть свідчити про запуск шкідливого програмного забезпечення, криптомайнінг, DoS - атаки або витік даних. Зміни у файловій системі також є важливим індикатором. Несанкціоноване створення, модифікація або видалення файлів, зміна прав доступу до них, а особливо поява зашифрованих файлів або вимог викупу, є серйозними ознаками компрометації. Аналіз нетипових мережевих з'єднань також є критичним. Встановлення з'єднань з невідомими або підозрілими зовнішніми ресурсами, прослуховування незвичайних портів або велика кількість вихідних з'єднань можуть свідчити про зараження шкідливим програмним забезпеченням або участь сервера в атаках [24].

Потенційна мета нетипової поведінки в мережі приватного підприємства є ключовим для ефективного реагування на інциденти інформаційної безпеки. Різні типи аномалій можуть вказувати на різні етапи кібератаки або відображати зловмисні наміри.

Однією з потенційних цілей є розвідка та сканування мережі, коли зловмисники намагаються зібрати інформацію про цільову інфраструктуру для виявлення вразливостей та планування подальших дій. Це може проявлятися у скануванні портів, ping - sweep, визначенні версій сервісів, розвідці DNS, скануванні веб - додатків або розвідці SNMP. Виявлення такої активності є раннім попереджувальним сигналом про можливу атаку [25].

Іншою метою може бути несанкціонований доступ до ресурсів, коли зловмисники намагаються отримати доступ до захищених даних, облікових

записів, серверів або мережевого обладнання без належних прав. Це може проявлятися у невдалих спробах аутентифікації, спробах використання слабких паролів, експлуатації вразливостей аутентифікації, використанні скомпрометованих облікових даних або атаках типу "людина посередині".

Ще однією потенційною метою є розповсюдження шкідливого програмного забезпечення (вірусів, черв'яків, троянів, програм - вимагачів, шпигунського ПЗ) для виконання зловмисних дій, таких як крадіжка даних, шифрування файлів або віддалене керування системами. Шкідливе ПЗ може потрапити на улаштування, коли користувач переглядає зламані зловмисниками веб - сайти, відкриває демонстраційні версії ігор, завантажує заражені музичні файли, встановлює нові панелі інструментів від невідомого виробника, завантажує програми з неперевірених джерел, відкриває вкладення шкідливих повідомлень електронної пошти. Словом, це може статися в будь - якій ситуації, коли користувач завантажує будь - який контент з всесвітньої павутини на улаштування, на якому немає досить сильного захисту [26].

Витік даних є ще однією серйозною загрозою, коли зловмисники намагаються несанкціоновано скопіювати або передати конфіденційну інформацію за межі мережі підприємства. Більшість витоків даних спричинено людською помилкою. Працівник може зберігати дані в незахищеному розташуванні, випадково поділитися даними із стороною або стати жертвою фішингової атаки. Витік даних може завдати значної шкоди репутації, вплинути на здатність організації залучати нових клієнтів, майбутніх інвесторів та потенційних працівників. Наслідки витоку даних можуть мати далекосяжні наслідки, впливаючи не лише на безпосередню фінансову ситуацію, але й на довгострокову життєздатність організації [27].

Внутрішні загрози виникають, коли зловмисні дії здійснюються особами, які мають легітимний доступ до ресурсів підприємства. Це може включати несанкціонований доступ до інформації, копіювання або передачу конфіденційних

даних, модифікацію або видалення даних, зловживання привілеями або обхід контролів безпеки.

За рівнем складності нетипова поведінка може бути простою, легко виявлятися на основі простих правил, складною, що вимагає глибокого аналізу та кореляції подій, та прихованою, спрямованою на непомітність та імітацію легітимної поведінки [28].

Розуміння цієї класифікації є критично важливим для ефективного захисту мереж приватних підприємств. Застосування різноманітних інструментів та методів, таких як системи виявлення вторгнень, системи управління інформацією та подіями безпеки, а також аналіз поведінки користувачів та сутностей, дозволяє виявляти та реагувати на різні види нетипової поведінки, мінімізуючи ризики для інформаційної безпеки організації. Ефективна стратегія безпеки передбачає постійний моніторинг та аналіз для своєчасного виявлення та нейтралізації потенційних загроз.

2.2 Моделі внутрішніх та зовнішніх загроз безпеки мережі

Безпека комп'ютерних мереж є критично важливою для належного функціонування будь-якої організації чи особистих систем у сучасному взаємопов'язаному світі. Загрози безпеці мережі постійно еволюціонують, стають більш складними та різноманітними. Для ефективного захисту ресурсів необхідно розуміти природу цих загроз та розробляти відповідні моделі для їх ідентифікації, аналізу та мінімізації. Загалом, джерела загроз безпеці мережі можна розділити на дві основні категорії: внутрішні та зовнішні. Розуміння відмінностей між цими категоріями є фундаментальним для побудови ефективної стратегії кібербезпеки. При цьому персонал забезпечення, який виділений в окрему складову системи захисту, може бути і джерелом загроз. Так, результати аналізу джерел порушень

безпеки в інформаційних системах свідчать, що близько 70 відсотків порушень відбуваються через персонал забезпечення, рис. 1.4 [29].

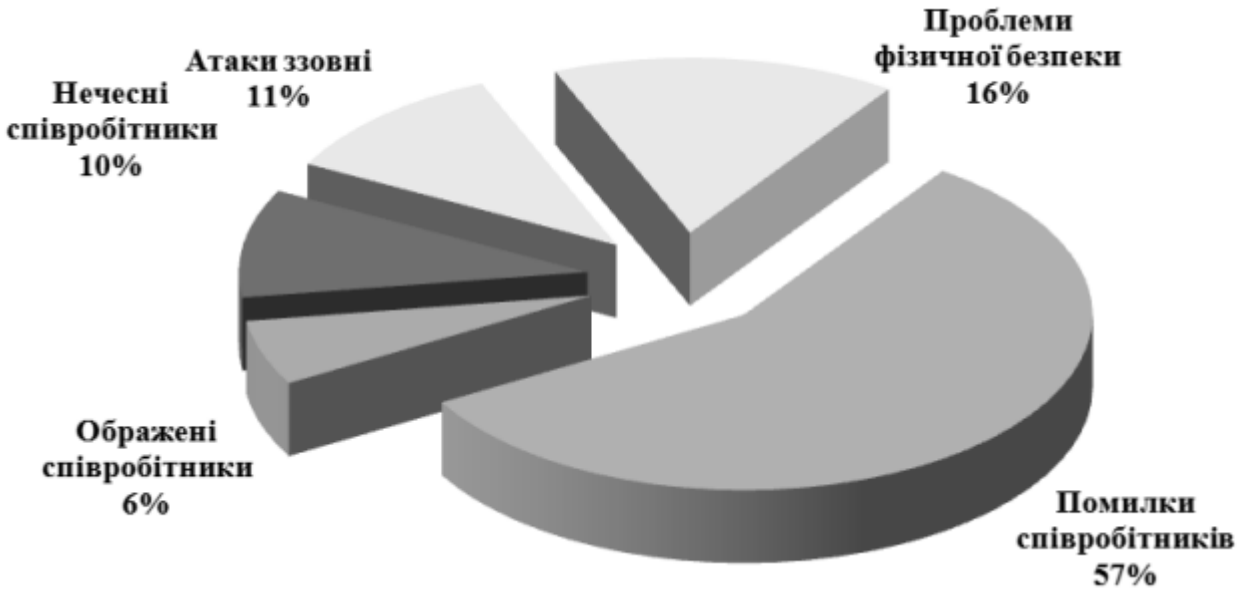


Рисунок 1.4 - Джерела порушень безпеки

Найбільший сектор на цій діаграмі, і, відповідно, найбільша проблема, це "Помилки співробітників". Цей сектор займає аж 57% діаграми. Це означає, що більше половини всіх проблем з безпекою виникають через звичайні людські помилки. Це можуть бути, наприклад, випадкове видалення важливих файлів, перехід за посиланнями у шахрайських електронних листах, або неправильне налаштування прав доступу. Крім помилок співробітників, є й інші джерела проблем з безпекою, хоча вони зустрічаються значно рідше. "Проблеми фізичної безпеки" становлять 16%. Це може включати в себе, наприклад, крадіжку обладнання, несанкціонований доступ до приміщень, або недостатній захист серверних кімнат. "Атаки ззовні" становлять 11%. Це різноманітні кібератаки, такі як хакерські атаки, віруси, або спроби злому мережі з метою викрадення даних або порушення роботи систем. Ще меншу частку займають проблеми, пов'язані з самими працівниками: "Нечесні співробітники" (10%) та "Ображені співробітники"

(6%). Це вже не випадкові помилки, а навмисні дії, коли працівники зловживають своїм доступом або намагаються нашкодити компанії.

Внутрішні загрози ініціюються суб'єктами, які мають легітимний або опосередкований доступ до внутрішньої мережі чи систем. Це можуть бути поточні або колишні співробітники, підрядники або ділові партнери. Мотивація таких дій варіюється від злого умислу, спричиненого, наприклад, помстою чи бажанням отримати фінансову вигоду, до звичайної недбалості, незнання правил безпеки або піддатливості на прийоми соціальної інженерії. Оскільки внутрішні зловмисники вже знаходяться всередині периметра і часто обізнані з внутрішньою структурою та процесами, їхні дії можуть бути складнішими для виявлення порівняно із зовнішніми атаками. До типових методів внутрішніх загроз належать зловживання наданими правами доступу, випадковий або навмисний витік конфіденційної інформації, інсайдерські змови, помилки у конфігурації систем, які створюють вразливості, або використання вже відомих внутрішніх слабкостей [30].

На противагу цьому, зовнішні загрози надходять з-за меж мережевого захисту організації. Їхніми джерелами є хакери, організовані кіберзлочинні угруповання, вороже налаштовані державні актори, недобросовісні конкуренти або будь - які сторонні особи без належних повноважень. Мотивація зовнішніх зловмисників часто включає фінансову наживу, корпоративне або державне шпигунство, саботаж, ідеологічні мотиви, кібертероризм або просто бажання завдати шкоди. Зовнішні атаки передбачають спроби подолати зовнішні засоби захисту, такі як фаєрволи та системи виявлення вторгнень. Серед поширених методів зовнішніх загроз - фішингові кампанії, розповсюдження шкідливого програмного забезпечення (вірусів, троянів, мережевих хробаків), розподілені атаки на відмову в обслуговуванні (DDoS), використання експлойтів нульового дня (невідомих раніше вразливостей), сканування портів для пошуку відкритих сервісів та атаки методом перебору паролів (брутфорс). Виявлення зовнішніх загроз, як правило, покладається на роботу систем моніторингу периметра, антивірусного програмного забезпечення та систем запобігання вторгненням [31].

Безпека комп'ютерних мереж та інформаційних систем є життєво важливою у сучасному цифровому ландшафті, де загрози постійно змінюються та вдосконалюються. Для ефективного захисту ресурсів необхідно не лише розпізнавати ці загрози, але й розуміти їхню природу та фактори, що сприяють їхній реалізації. Тому, я зробила модель загроз, їх джерела та вразливості для підприємства, яка показана на рисунку 1.5.

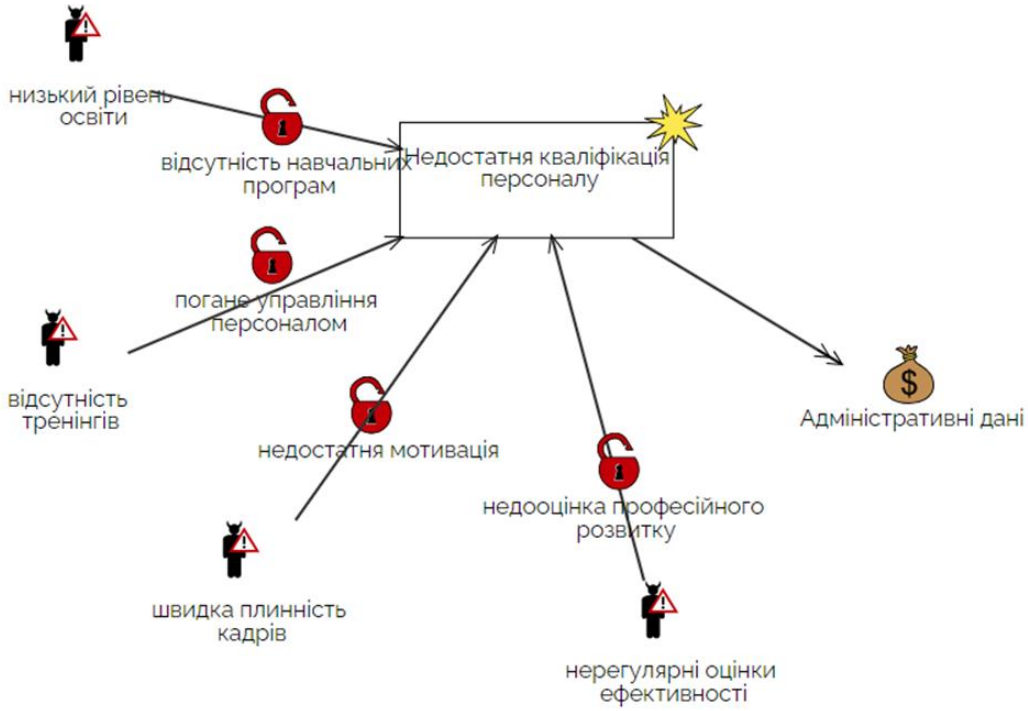


Рисунок 1.5 - Модель загроз «Недостатня кваліфікація персоналу»

Ця проблема є центральним фактором ризику, що може призвести до численних інцидентів безпеки. Низький рівень освіти співробітників, відсутність цілеспрямованих навчальних програм з питань безпеки, неефективне управління персоналом, ігнорування регулярних тренінгів та недостатня мотивація працівників до підвищення своїх знань і навичок - усі ці аспекти створюють середовище, де ризик помилок та неправильних дій значно зростає. Додатковим обтяжуючим фактором є висока плинність кадрів, яка ускладнює процес підтримки належного рівня обізнаності з питаннями безпеки серед нових співробітників.

Наслідком недостатньої кваліфікації персоналу є прямий вплив на адміністративні дані, що може проявитися у їх випадковому пошкодженні, несанкціонованому доступі через помилки конфігурації, спричинені незнанням, або навіть ненавмисному витоку чутливої інформації [32].

Друга модель деталізує загрозу, пов'язану з відмовою IT - систем, зокрема серверів. Ця загроза є критичною, оскільки сервери є основою більшості мережевих сервісів та сховищ даних. Фактори, що сприяють відмові, включають фізичні аварії обладнання, які можуть статися несподівано та призвести до виходу систем з ладу. Ненадійна фізична інфраструктура, що забезпечує роботу серверів, така як нестабільне електропостачання або неефективні системи охолодження, також значно підвищує ризик збоїв. Відсутність належної стратегії резервного копіювання даних та конфігурацій унеможливлює швидке та повне відновлення працездатності систем після відмови. Всі ці фактори, включно з безпосередніми технічними несправностями самих серверних пристроїв, створюють високу ймовірність порушення доступності сервісів та, що особливо важливо, ставлять під загрозу дані серверів та конфіденційну інформацію, що на них зберігається, аж до їх повної втрати або недоступності. Модель показано на рисунку 1.6.

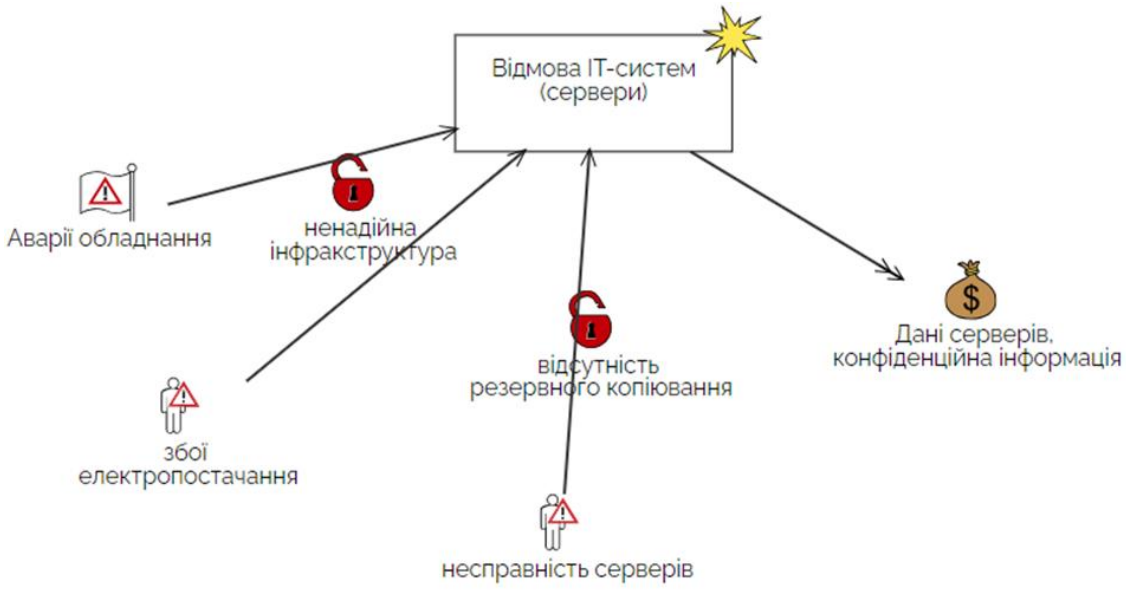


Рисунок 1.6 - Модель загроз «Відмова IT - систем»

Третя модель присвячена загрозі, яку несуть віруси та інше шкідливе програмне забезпечення. Це одна з найпоширеніших та постійно мутуючих категорій кіберзагроз. Джерелом поширення шкідливого ПЗ є кіберзлочинці, які цілеспрямовано розробляють та поширюють віруси, трояни, хробаки та інші види шкідливого коду. Заражені файли, що потрапляють у мережу через електронну пошту, змінні носії або завантаження з ненадійних джерел, є основним вектором розповсюдження. Відсутність комплексного антивірусного захисту на всіх рівнях мережі - від кінцевих пристроїв до серверів - відкриває двері для проникнення шкідливого ПЗ. Недостатня або повна відсутність фільтрації мережевого трафіку дозволяє шкідливому коду вільно переміщатися мережею та інфікувати системи. Використання несертифікованих або піратських програм також значно підвищує ризик зараження, оскільки таке програмне забезпечення може містити приховані шкідливі функції. Вплив вірусів та шкідливого ПЗ переважно спрямований на операційні дані, що може призвести до їх знищення, пошкодження, несанкціонованого шифрування (як у випадку програм - вимагачів) або викрадення, тим самим порушуючи нормальну роботу організації [33]. Модель показано на рисунку 1.7.

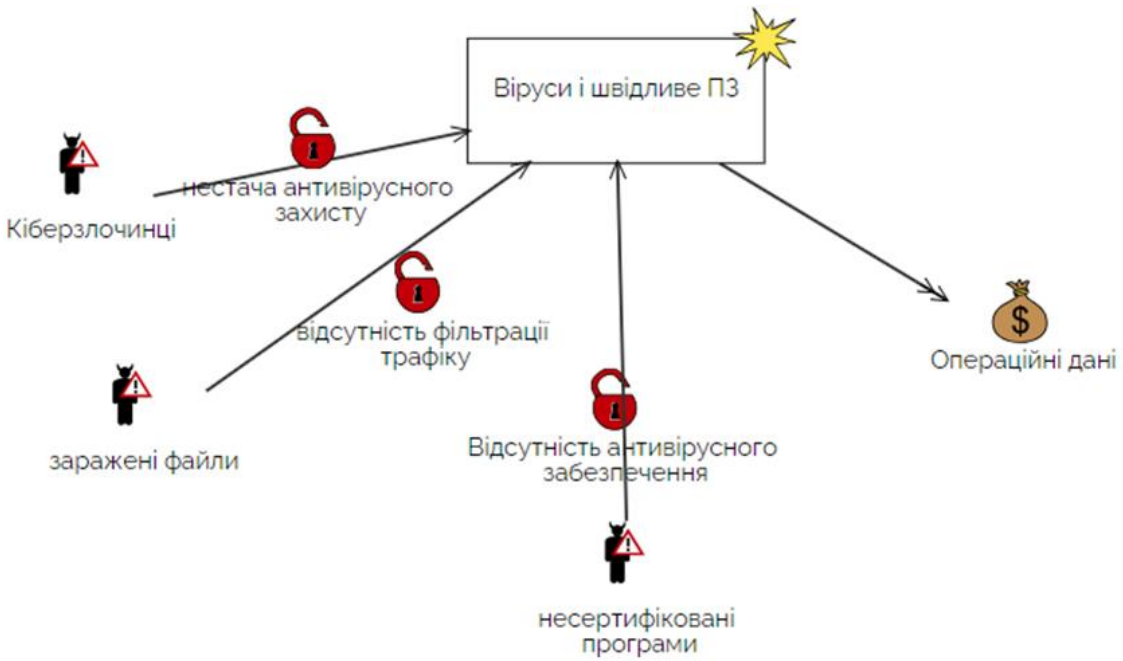


Рисунок 1.7 - Модель загроз «Віруси і шкідливе ПЗ»

Таким чином, представлені моделі загроз наочно демонструють різноманітність факторів ризику - від людських помилок та недостатньої підготовки до технічних збоїв та цілеспрямованих шкідливих програм. Ефективне забезпечення безпеки мережі вимагає не просто реагування на інциденти, а побудови комплексного підходу, що включає постійне підвищення кваліфікації персоналу, забезпечення надійності та стійкості технічної інфраструктури, а також впровадження багатошарових систем захисту від шкідливого програмного забезпечення. Розуміння цих моделей загроз є першим кроком до розробки ефективної стратегії кібербезпеки.

2.3 Метод виявлення аномальної активності користувачів

Аномалії - це відхилення від норми або очікуваної поведінки, які можуть виникати в різних контекстах, включаючи науку та технології. У контексті кібербезпеки аномалії - це відхилення від очікуваної поведінки системи, які можуть свідчити про порушення безпеки. Це може бути викликано різними факторами, як-от зловмисне програмне забезпечення, хакерство або внутрішні загрози [34].

Аномалії в контексті аналізу поведінки користувачів можуть проявлятися в різних аспектах діяльності. Це можуть бути:

- аномалії доступу, що включають незвичайні спроби входу в систему з невідомих локацій або в неробочий час, доступ до нетипових ресурсів чи підвищення привілеїв;

- аномалії в роботі з даними, такі як нехарактерно великий обсяг завантажень або передач, копіювання значної кількості файлів або доступ до невластивої інформації;

- мережеві аномалії включають незвичайний трафік або підключення до підозрілих IP - адрес. Аномалії у використанні пристроїв можуть проявлятися як вхід з невідомих пристроїв або незвичайні зміни в їхній конфігурації;

- темпоральні аномалії фіксують нетипову активність у неробочий час або нехарактерну частоту дій [35].

Необхідність використання методів виявлення аномальної активності зумовлена тим, що традиційні засоби захисту периметра не завжди ефективні проти загроз, які походять зсередини або реалізуються через легітимні облікові записи. Співробітники мають авторизований доступ до певних ресурсів, і їхні зловмисні дії або помилки можуть виглядати як частина звичайної робочої активності, якщо не аналізувати контекст та патерни поведінки. Процес виявлення аномальної активності користувачів зазвичай складається з кількох ключових етапів. Перш за все, відбувається збір даних. Це можуть бути різноманітні логи з різних джерел інформаційної інфраструктури: системні логи операційних систем, логи доступу до файлових ресурсів та баз даних, записи про використання додатків, мережеві логи, які фіксують трафік та з'єднання, а також спеціалізовані логи подій безпеки. Чим повнішими та детальнішими будуть зібрані дані, тим точнішим буде аналіз.

Система виявлення аномалій та ідентифікації пристроїв розміщується у внутрішній мережі розумного будинку та складається з наступних модулів: моніторингу мережевого трафіку, виявлення аномалій у мережевій поведінці, ідентифікації та прийняття рішення, модуля перетворення в PDML, модуля отримання ознак, класифікації. Інформація про виявленні пристрої зберігається в білому списку профілів функціонування розумних пристроїв. Передбачається, що розумні будинки поєднані у соціальну мережу. Модуль ідентифікації та прийняття рішення організовує роботу системи в трьох режимах: моніторинг мережевого трафіку та виявлення аномалій; пошук профілю пристроїв у кластері; пошук профілю в інших кластерах (рисунок. 1.8) [36].

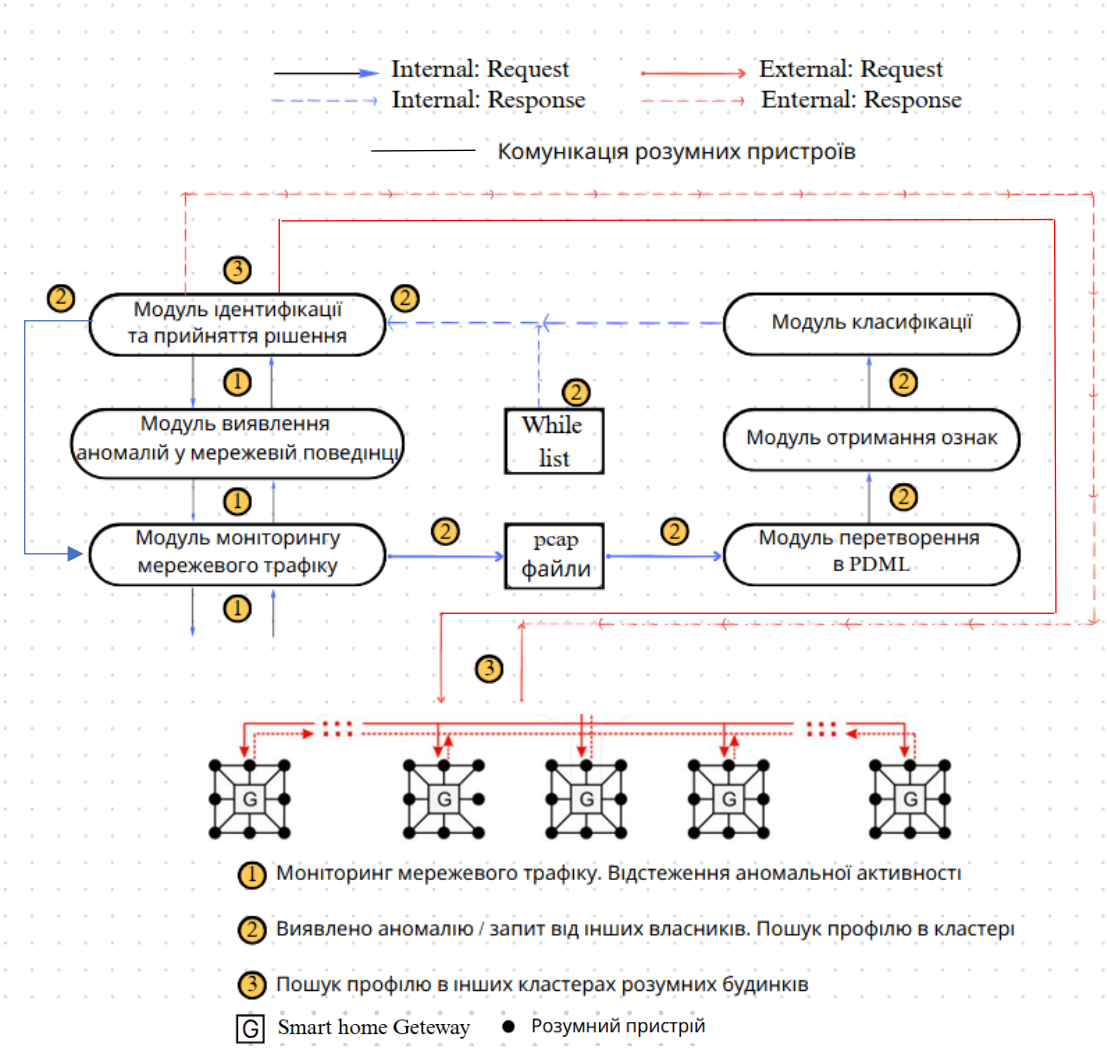


Рисунок 1.8 - Система виявлення аномалій та ідентифікації пристроїв розумних будинків на основі колективної комунікації

Сучасні системи виявлення аномалій активно використовують методи машинного навчання. Ці моделі здатні виявляти неочевидні закономірності та r5t4складні комбінації дій, що можуть свідчити про аномальну активність. До використовуваних методів можуть належати:

- кластеризація - групування схожих моделей поведінки та виявлення користувачів, чия поведінка значно відрізняється від будь - якого сформованого кластера;

- класифікація - навчання моделі для розрізнення нормальної та аномальної поведінки на основі розмічених даних;

- виявлення викидів (Anomaly Detection) - алгоритми, спеціально розроблені для ідентифікації рідкісних та нетипових спостережень [37].

Це можуть бути як методи навчання з учителем (потребують попередньо розмічених даних про нормальну та аномальну активність, що є складним завданням), так і методи навчання без учителя, які здатні виявляти нові, невідомі типи аномалій без попереднього визначення їхніх характеристик. Останнім часом набувають поширення системи аналізу поведінки користувачів та об'єктів (UEBA - User and Entity Behavior Analytics), які застосовують просунуту аналітику та корелюють дані з багатьох джерел для побудови складних моделей поведінки та виявлення витончених, комплексних загроз. Аналіз поведінки користувачів і сутностей (UEBA) - це передова технологія, призначена для виявлення, прогнозування та запобігання потенційним ризикам у режимі реального часу, покращуючи рівень безпеки будь - якої організації. На відміну від традиційних інструментів безпеки, які зосереджені на попередньо визначених сигнатурах загроз, UEBA постійно навчається та адаптується, забезпечуючи проактивний захист від внутрішніх загроз, зловживання привілеями та вдосконалених постійних загроз [38].

У разі виявлення активності, що вважається аномальною на основі застосованих методів, система генерує сповіщення або звіт. Ці сповіщення мають містити достатньо контекстної інформації (хто, коли, що робив, ступінь аномальності) для того, щоб служба безпеки могла провести розслідування. На етапі розслідування визначається, чи є виявлена аномалія реальною загрозою (справжнє спрацювання) або нешкідливим відхиленням від норми (хибне спрацювання). Залежно від результатів розслідування вживаються відповідні заходи реагування, такі як блокування облікового запису, додатковий моніторинг, примусове скидання пароля або дисциплінарні заходи.

Незважаючи на значні переваги, впровадження та ефективне використання методів виявлення аномальної активності стикається з певними викликами. До них належать складність точного визначення "нормальної" поведінки для всіх

користувачів та сценаріїв, необхідність обробки величезних обсягів даних, високий рівень хибних спрацювань на початкових етапах, що вимагає значних ресурсів для розслідування, а також постійна еволюція поведінки користувачів та методів зловмисників, що вимагає безперервного оновлення базових профілів та моделей аналізу.

Проте, незважаючи на ці труднощі, переваги використання методів виявлення аномальної активності є значними. Вони дозволяють своєчасно ідентифікувати внутрішні загрози, виявляти компрометацію облікових записів на ранніх стадіях, отримувати ранні попередження про спроби несанкціонованого доступу, витоку даних або саботажу, а також підвищують загальну видимість активності користувачів у мережі, що сприяє більш ефективному реагуванню на інциденти безпеки. Таким чином, метод виявлення аномальної активності користувачів є критично важливим елементом сучасної багаторівневої системи захисту інформації.

2.4 Висновки

Було розглянуто різні типи аномалій, які можуть виникати в мережевому трафіку та діях користувачів. Було встановлено, що нетипова поведінка може бути індикатором як випадкових помилок, так і навмисних зловмисних дій. Систематизація таких аномалій за різними критеріями (наприклад, за джерелом, типом впливу, часовими характеристиками) є важливим кроком для подальшого розроблення ефективних механізмів їх ідентифікації та реагування. Підрозділ 2.2 "Моделі внутрішніх та зовнішніх загроз безпеки мережі" надав комплексний огляд потенційних загроз, що походять як з внутрішнього, так і з зовнішнього середовища організації. Було підкреслено, що внутрішні загрози, часто недооцінені, можуть становити значний ризик, оскільки внутрішні зловмисники зазвичай мають легітимний доступ до мережевих ресурсів. Зовнішні загрози, своєю чергою,

характеризуються різноманітністю векторів атак та постійною еволюцією. Розуміння моделей цих загроз, їхніх мотивацій та потенційних наслідків є ключовим для побудови надійної системи безпеки. У підрозділі 2.3 "Метод виявлення аномальної активності користувачів" було представлено загальний підхід до ідентифікації підозрілої поведінки користувачів у мережі. Цей метод базується на аналізі поведінкових профілів користувачів та виявленні відхилень від цих профілів. Ефективність такого підходу залежить від точності побудови базових профілів та чутливості алгоритмів виявлення аномалій.

Узагальнюючи, другий розділ заклав теоретичну основу для подальшого дослідження в області виявлення та запобігання загрозам безпеці в мережах приватних підприємств. Визначення класифікації нетипової поведінки, аналіз моделей внутрішніх та зовнішніх загроз, а також розуміння принципів методу виявлення аномальної активності користувачів є необхідними передумовами для розробки практичних рішень у наступних розділах.

3 РОЗРОБКА СИСТЕМИ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1 Обґрунтування необхідності створення системи аналізу поведінки користувачів

Створення системи аналізу поведінки користувачів є наріжним каменем для сучасного приватного підприємства, що прагне до сталого розвитку та лідерства на ринку. В умовах жорсткої конкуренції та постійно зростаючих очікувань клієнтів, глибоке розуміння їхніх дій, вподобань та потреб стає не просто перевагою, а життєвою необхідністю. Така система дозволяє підприємству отримати всебічну картину взаємодії клієнтів з його продуктами, послугами, веб - сайтами та мобільними додатками, відкриваючи шлях до прийняття обґрунтованих стратегічних та тактичних рішень.

Однією з ключових переваг впровадження системи аналізу поведінки користувачів є можливість досягти безпрецедентного рівня розуміння клієнтської бази. Відстежуючи такі метрики, як переглянуті сторінки чи товари, час, проведений на них, здійснені кліки, пошукові запити та історію покупок, підприємство отримує цінну інформацію про інтереси та потреби різних сегментів аудиторії. Це дозволяє перейти від загальних маркетингових кампаній до персоналізованих комунікацій та пропозицій, які максимально відповідають очікуванням кожного клієнта. У результаті підвищується лояльність клієнтів, зростає рівень задоволеності та збільшується ймовірність повторних покупок.

Крім того, аналіз поведінки користувачів відіграє вирішальну роль в оптимізації користувацького досвіду. Виявляючи проблемні зони в інтерфейсі або процесах, підприємство може оперативно вносити необхідні поліпшення. Наприклад, високий відсоток відмов на певній сторінці може свідчити про незрозумілий контент або технічні помилки, а низька конверсія на етапі оформлення замовлення може вказувати на складний або незручний процес оплати. Усуваючи ці "вузькі місця", підприємство не лише підвищує зручність

використання своїх продуктів та послуг, але й значно збільшує конверсію та зменшує відтік клієнтів.

У сфері маркетингу система аналізу поведінки користувачів є незамінним інструментом для підвищення ефективності рекламних кампаній та оптимізації маркетингових витрат. Розуміючи, які канали комунікації є найбільш ефективними для залучення різних сегментів аудиторії, які типи контенту викликають найбільший інтерес та як користувачі взаємодіють з рекламними матеріалами після переходу, підприємство може більш точно націлювати свої маркетингові зусилля та інвестувати в найбільш перспективні канали. Це дозволяє значно підвищити ROI маркетингових інвестицій та залучати більш якісних лідів.

Не менш важливим є використання даних про поведінку користувачів для вдосконалення продуктів та послуг. Аналізуючи, які функції використовуються найчастіше, а які ігноруються, які розділи сайту чи додатка є найбільш популярними, а які викликають труднощі, підприємство отримує цінний зворотний зв'язок, що є основою для прийняття обґрунтованих рішень щодо подальшого розвитку продуктів та послуг. Це дозволяє створювати більш релевантні та затребувані пропозиції, які максимально відповідають потребам ринку.

Нарешті, система аналізу поведінки користувачів може відігравати важливу роль у забезпеченні безпеки та виявленні шахрайських дій. Аналізуючи нетипову активність користувачів, підозрілі спроби доступу або нехарактерні патерни поведінки, підприємство може своєчасно виявляти потенційні загрози та вживати необхідних заходів для їх запобігання, захищаючи таким чином свої фінансові активи та репутацію.

Таким чином, створення потужної системи аналізу поведінки користувачів є стратегічною інвестицією для будь - якого приватного підприємства, яке прагне до глибокого розуміння своїх клієнтів, оптимізації своєї діяльності, підвищення конкурентоздатності та досягнення довгострокового успіху. Вона забезпечує цінну інформацію, яка є основою для прийняття обґрунтованих рішень у всіх ключових

аспектах бізнесу, від розробки продуктів та маркетингу до покращення користувацького досвіду та забезпечення безпеки.

Розглянемо попередній алгоритм роботи системи моніторингу та аналізу активності користувачів в корпоративній мережі (рисунок 1.9).

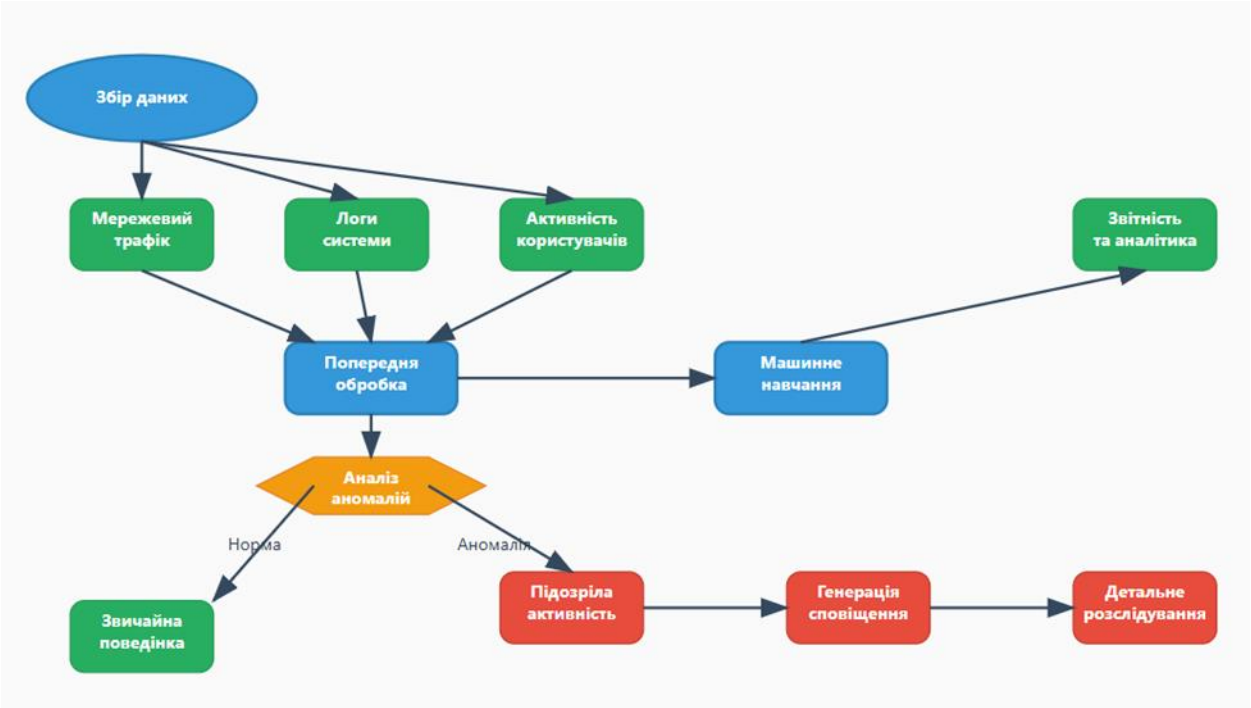


Рисунок 1.9 - Алгоритм роботи системи моніторингу та аналізу активності в корпоративній мережі

Тут ми можемо бачити, як на прикладі алгоритму описується робота системи моніторингу та аналізу активності в корпоративній мережі, спрямована на виявлення аномалій та потенційних загроз безпеці. Процес розпочинається зі збору даних, який є першим і критично важливим етапом. Система збирає інформацію з різних джерел, що відображають активність у корпоративній мережі. До цих джерел належать:

- мережевий трафік - аналізуються пакети даних, що передаються мережею, включаючи інформацію про джерела та призначення трафіку, протоколи, обсяги

переданих даних тощо. Це дозволяє відстежувати комунікації між різними вузлами мережі;

- логи системи - збираються журнали подій з операційних систем, серверів, мережевого обладнання та інших компонентів інфраструктури. Ці логи містять записи про дії користувачів, системні помилки, спроби доступу та інші важливі події;

- активність користувачів - відстежуються дії користувачів у мережі, включаючи їхні логіни та виходи з системи, запущені програми, відвідані веб - сайти, використані файли та інші дії, що фіксуються в системі [39].

Зібрані дані надходять на етап попередньої обробки. На цьому етапі дані очищаються від зайвої інформації, форматуються для подальшого аналізу, нормалізуються та можуть бути об'єднані з різних джерел для створення цілісної картини активності. Після попередньої обробки дані можуть бути використані для машинного навчання. На цьому етапі будується модель, яка навчається на основі історичних даних про нормальну активність у мережі. Метою є навчити систему розрізняти типову поведінку від аномальної.

Далі відбувається аналіз аномалій. На цьому етапі система використовує навчену модель (або інші методи аналізу) для порівняння поточної активності з визначеною нормою. Результатом аналізу є виявлення відхилень, які можуть бути класифіковані як норма або аномалія. Якщо поведінка відповідає встановленій нормі, система реєструє її як звичайну поведінку і продовжує моніторинг. У випадку виявлення аномалії, система ідентифікує її як підозрілу активність. Це може бути ознакою потенційної загрози безпеці, неправомірних дій користувачів або технічних проблем. Виявлення підозрілої активності призводить до генерації сповіщення. Система автоматично інформує відповідальних осіб (наприклад, адміністраторів безпеки) про виявлену аномалію, надаючи їм необхідну інформацію для реагування. Після отримання сповіщення розпочинається етап детального розслідування. На цьому етапі аналітики безпеки вивчають виявлену

підозрілу активність, намагаючись з'ясувати її причини, оцінити потенційний ризик та вжити необхідних заходів для усунення загрози або запобігання її повторенню.

Паралельно або після завершення основних етапів здійснюється звітність та аналітика. Це включає в себе узагальнення даних про виявлені аномалії, формування звітів про стан безпеки мережі, аналіз тенденцій та оцінку ефективності роботи системи моніторингу [40].

Таким чином, описаний алгоритм являє собою багаторівневу систему, призначену для безперервного моніторингу активності в корпоративній мережі, виявлення відхилень від норми, своєчасного сповіщення про потенційні загрози та надання можливості для їхнього детального аналізу та усунення.

3.2 Опис структури системи

Алгоритми відіграють ключову роль у світі програмування. Це фундаментальні інструменти для вирішення завдань та створення програм. Незалежно від вашого досвіду, уміння створювати ефективні алгоритми - невід'ємна навичка для програміста. Крім програмування, алгоритми застосовуються в багатьох областях, починаючи від управління бізнес - процесами до побудови маркетингових стратегій. Без ефективних алгоритмів складно уявити сучасний світ технологій.

Алгоритми дозволяють програмістам вирішувати завдання ефективніше та оптимізувати процеси. Вони допомагають покращити продуктивність програм, знизити навантаження на системи та скоротити час виконання завдань [41].

Тому я розробила алгоритм роботи системи аналізу поведінки користувачів у корпоративній мережі у вигляді блок - схеми, як показано на рисунку 1.10.

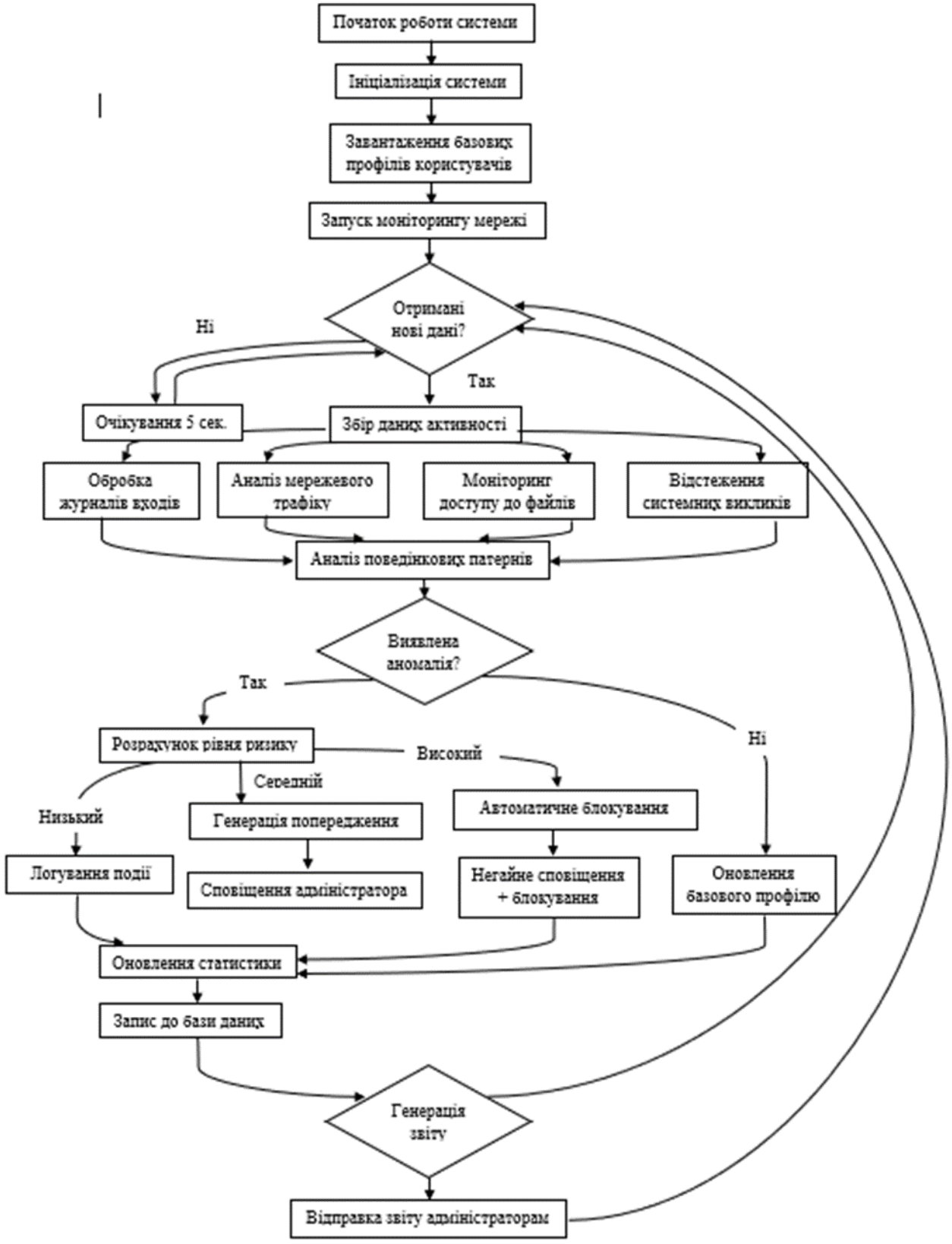


Рисунок 1.10 - Блок - схема алгоритму системи аналізу поведінки користувачів у корпоративній мережі

Алгоритм роботи показує повний цикл обробки від збору даних до програми роботи мережі, що дозволяє ефективно виявляти та реагувати на активність у корпоративній системі.

Розроблений мною алгоритм детально описує роботу системи аналізу поведінки користувачів у корпоративних мережах, починаючи з моменту запуску і завершуючи періодичною генерацією звітів для адміністраторів. Спочатку система ініціалізується, готуючи всі необхідні компоненти до функціонування, після чого завантажуються базові профілі поведінки для кожного користувача або їхніх груп. Ці профілі є еталоном звичайної активності та слугують для подальшого виявлення відхилень. Після ініціалізації система запускає безперервний моніторинг активності в корпоративній мережі, постійно очікуючи надходження нових даних.

При отриманні нових даних про активність, система здійснює їхній збір, який включає обробку журналів входів та виходів користувачів, аналіз мережевого трафіку, моніторинг доступу до файлів та відстеження системних викликів. Зібрані дані потім піддаються аналізу поведінкових патернів, де вони порівнюються з завантаженими базовими профілями та існуючими моделями поведінки з метою виявлення будь - яких відхилень, що можуть свідчити про аномальну активність.

Якщо в результаті аналізу аномалій не виявлено, система може використовувати отримані дані про звичайну активність для оновлення базових профілів користувачів, що дозволяє їй з часом ставати більш точною у визначенні норми. Після цього система повертається до очікування нових даних для продовження моніторингу.

У випадку виявлення аномальної активності, система переходить до розрахунку рівня ризику, пов'язаного з цією аномалією. Залежно від визначеного рівня ризику (низький, середній або високий), вживаються різні заходи реагування. При низькому рівні ризику інформація про подію просто логується, оновлюється статистика аномалій та записується до бази даних. При середньому рівні ризику генерується попередження, яке надсилається адміністратору безпеки, а також оновлюється статистика та робиться запис до бази даних. У випадку високого рівня

ризику система може автоматично блокувати підозрілу активність або обліковий запис користувача, негайно сповіщаючи про це адміністратора, а також оновлюючи статистику та зберігаючи інформацію про інцидент. Після вжиття відповідних заходів система також повертається до очікування нових даних для продовження моніторингу.

Крім безперервного моніторингу та реагування на аномалії, система періодично або за запитом здійснює генерацію звітів, які містять узагальнену інформацію про виявлену активність, аномалії, статистику та вжиті заходи. Згенеровані звіти потім надсилаються адміністраторам для ознайомлення та прийняття подальших рішень щодо безпеки корпоративної мережі.

Таким чином, система забезпечує безперервний цикл моніторингу, аналізу, реагування та звітності для підтримки безпечного середовища в корпоративній мережі.

Ефективність описаного алгоритму системи аналізу поведінки користувачів у корпоративних мережах є багатогранним поняттям, яке визначається його здатністю точно і своєчасно виявляти загрози безпеці, мінімізуючи при цьому кількість помилкових спрацювань та забезпечуючи адекватне реагування на інциденти. Однією з ключових переваг такого підходу є можливість проактивного виявлення загроз, оскільки аналіз відхилень від встановлених профілів поведінки дозволяє ідентифікувати потенційні внутрішні загрози, скомпрометовані облікові записи або неправомірні дії на ранніх етапах їхнього розвитку, ще до того, як вони можуть завдати значної шкоди корпоративній інфраструктурі. Крім того, поведінковий аналіз має потенціал для виявлення складних та раніше невідомих атак, які не мають чітких сигнатур і тому можуть бути пропущені традиційними сигнатурними системами безпеки. Особливо цінним є здатність системи виявляти інсайдерські загрози, оскільки вона безпосередньо спрямована на аналіз поведінки легітимних користувачів, що є критично важливим у боротьбі з внутрішніми порушеннями безпеки.

Дієвість алгоритму також підтримується його здатністю до адаптації через оновлення базових профілів поведінки, що дозволяє системі враховувати зміни у звичайній активності користувачів та знижувати кількість хибних спрацювань з плином часу. Своєчасне виявлення підозрілої активності та генерація попереджень надають адміністраторам безпеки необхідний час для аналізу ситуації та вжиття превентивних заходів, а можливість автоматичного блокування активності, що становить високий ризик, може значно обмежити потенційний збиток від атаки. Додатково, детальна звітність та аналітика, що генеруються системою, є цінним джерелом інформації для розуміння загальних тенденцій у сфері безпеки мережі, оцінки ефективності застосованих методів аналізу та планування подальших заходів з її зміцнення.

Однак його ефективність залежить від якості вхідних даних, точності налаштувань, здатності системи до адаптації, а також від кваліфікації персоналу, який її використовує та підтримує. Для досягнення максимальної ефективності потрібен постійний моніторинг, налаштування та оновлення системи з урахуванням специфіки корпоративної мережі та актуальних загроз.

3.3 Демонстрація роботи системи аналізу поведінки користувачів

При запуску системи нам потрібно здійснити авторизацію (рисунок 1.11). Алгоритм роботи даного вікна полягає в тому, щоб користувач ввів логін та пароль у спеціально відведені віконця. Нижче заголовка подано короткий, але чіткий опис призначення системи: "Моніторинг поведінки користувачів у корпоративній мережі". Цей текст одразу інформує про функціонал системи, вказуючи, що вона призначена для відстеження та аналізу дій працівників або інших користувачів у межах корпоративної мережі.

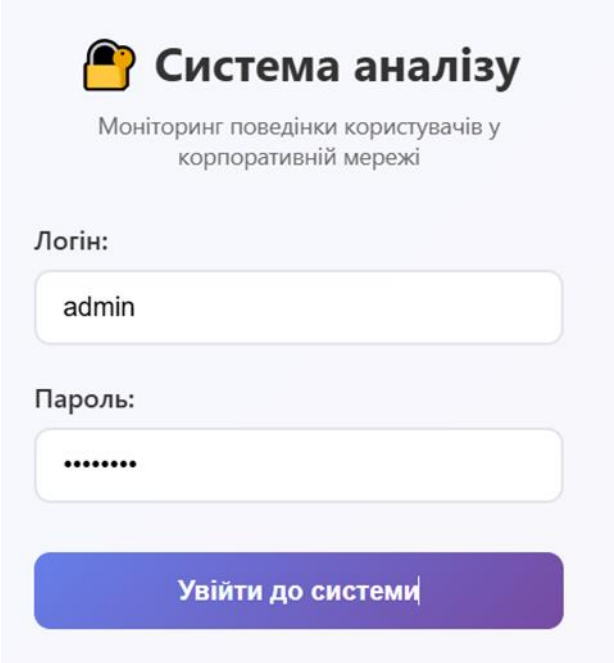


Рисунок 1.11 - Авторизація

Після успішного входу нас зустрічає меню у вигляді панелі управління (рисунок 1.12). Тут адміністратор може обирати опцію, необхідну для роботи.

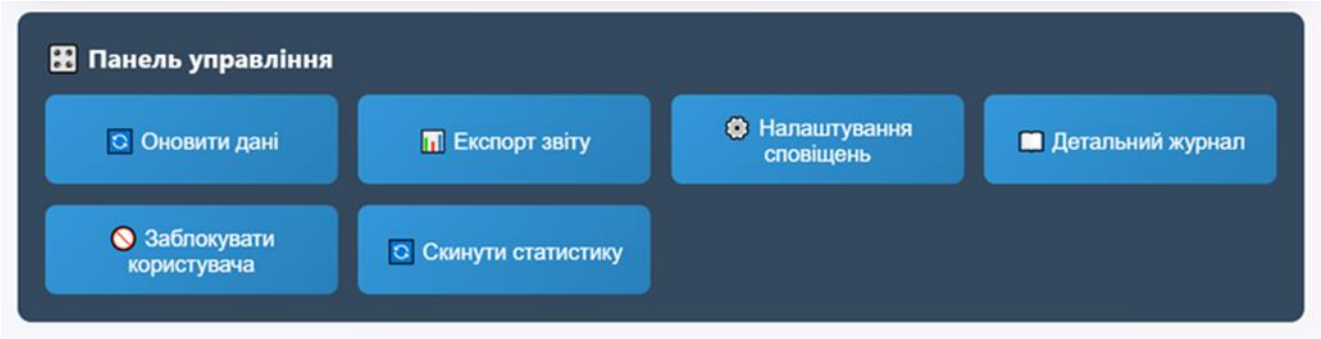


Рисунок 1.12 - Панель управління

Дана панель управління є частиною інтерфейсу системи аналізу поведінки користувачів у корпоративній мережі та надає швидкий доступ до ключових функцій системи. Вона розташована у верхній частині інтерфейсу та надає швидкий доступ до ключових функцій системи. Основні опції панелі управління:

- оновити дані - ця кнопка, ініціює процес оновлення відображуваних даних. Це корисно для отримання найактуальнішої інформації про поведінку користувачів та виявлені аномалії;

- експорт звіту - дана опція дозволяє експортувати згенеровані звіти про аналіз поведінки користувачів у різних форматах (наприклад, PDF, CSV);

- налаштування сповіщень - ця кнопка відкриває розділ налаштувань сповіщень системи. Тут адміністратор може конфігурувати, які події повинні викликати сповіщення, яким чином ці сповіщення повинні надходити (наприклад, електронна пошта, системні повідомлення) та для яких користувачів;

- детальний журнал - ця кнопка, відкриває доступ до детального журналу подій системи аналізу поведінки користувачів. У цьому журналі фіксуються всі дії системи, виявлені аномалії, спрацьовування правил та інша технічна інформація;

- заблокувати користувача - ця опція дозволяє адміністратору заблокувати обліковий запис певного користувача в корпоративній мережі. Ця функція може використовуватися у випадку виявлення підозрілої або зловмисної активності;

- скинути статистику - ця кнопка, дозволяє адміністратору скинути зібрану статистику аналізу поведінки користувачів. Це може бути необхідно для початку нового циклу аналізу або після внесення значних змін до налаштувань системи.

Таким чином, ця панель інструментів надає адміністратору системи аналізу поведінки користувачів швидкий доступ до основних функцій, включаючи оновлення даних, експорт звітів, налаштування сповіщень, перегляд детальних журналів, блокування користувачів та скидання статистики. Це забезпечує зручне керування та моніторинг активності в корпоративній мережі з метою виявлення та запобігання потенційним загрозам безпеці.

Далі якщо ми натиснемо на кнопку «експорт звіту» у нас з’явиться детальний звіт моніторингу, де інтерфейс розподілено на кілька логічних секцій, кожна з яких надає важливу інформацію про стан і активність у мережі (рис. 1.13).

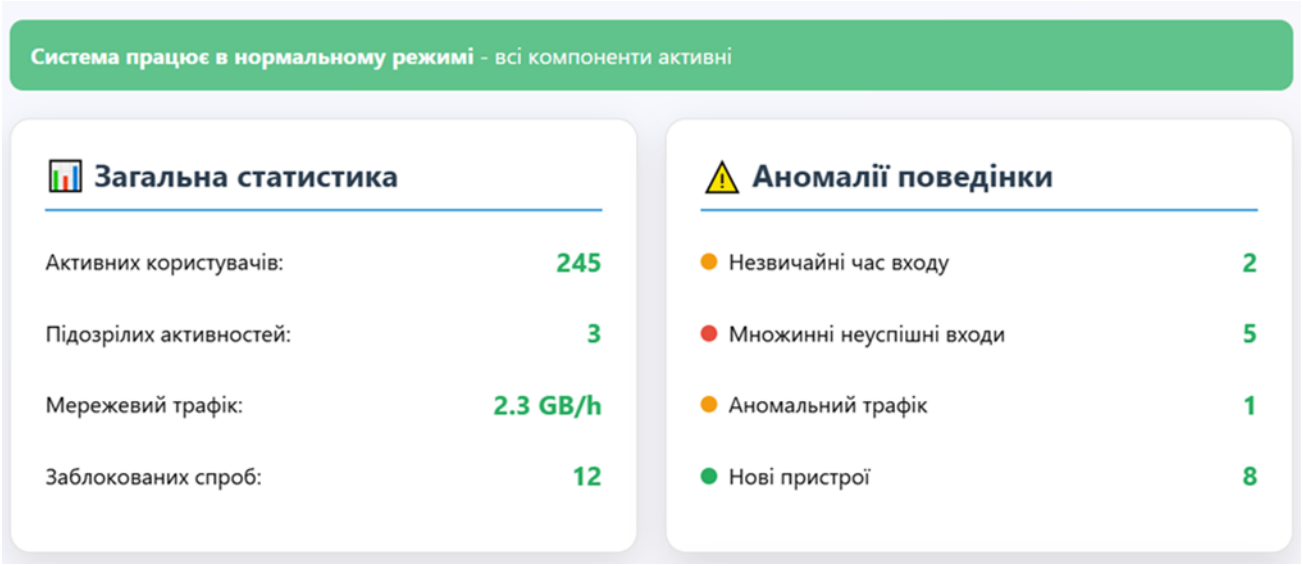


Рисунок 1.13 - Експорт звіту

Я структурувала інтерфейс таким чином, щоб надати адміністратору швидкий огляд ключових показників та виявлених відхилень. У найвищій частині вікна розташоване системне повідомлення на зеленому тлі, що підтверджує стабільну роботу системи. Цей індикатор є критично важливим, оскільки він запевняє, що моніторинговий функціонал працює коректно і надає актуальні дані. Нижче цього статусного повідомлення знаходяться дві основні інформаційні панелі, розташовані поруч, що дозволяє одночасно бачити як загальні метрики, так і деталі аномалій. Панель "Загальна статистика", надає сумарні дані про діяльність у мережі. Вона показує поточну кількість активних користувачів - 245, що є важливим показником завантаженості. Окрім того, система показує, що виявила 3 підозрілих активності, що свідчить про наявність потенційних загроз або нетипових подій, які потребують подальшого аналізу. Обсяг мережевого трафіку в реальному часі становить 2.3 ГБ/год, що дозволяє оцінювати пропускну здатність та можливі піки навантаження. Також відображається кількість заблокованих спроб - 12, що вказує на спрацювання захисних механізмів системи проти небажаних дій, таких як спроби несанкціонованого доступу.

Панель, що має назву "Аномалії поведінки", зосереджена на конкретних відхиленнях від норми, які були виявлені системою аналізу. Ці аномалії згруповані за типом, і для кожного типу вказано кількість випадків. Зафіксовано 2 випадки незвичайного часу входу, що може сигналізувати про спроби доступу поза робочими годинами або з нетипових часових поясів. Множинні неуспішні входи нараховують 5 випадків, що є яскравим індикатором можливих спроб підбору паролів або атаки перебором. Виявлено 1 випадок аномального трафіку, що може вказувати на незвичні обсяги даних, що передаються, або на нетипові шаблони мережевої активності. І система зареєструвала 8 нових пристроїв, які підключилися до корпоративної мережі, що вимагає перевірки для забезпечення відповідності політикам безпеки та виявлення потенційно неавторизованих пристроїв.

Щоб побачити журнал подій нам потрібно натиснути на кнопку «детальний журнал» (рисунок 1.14).

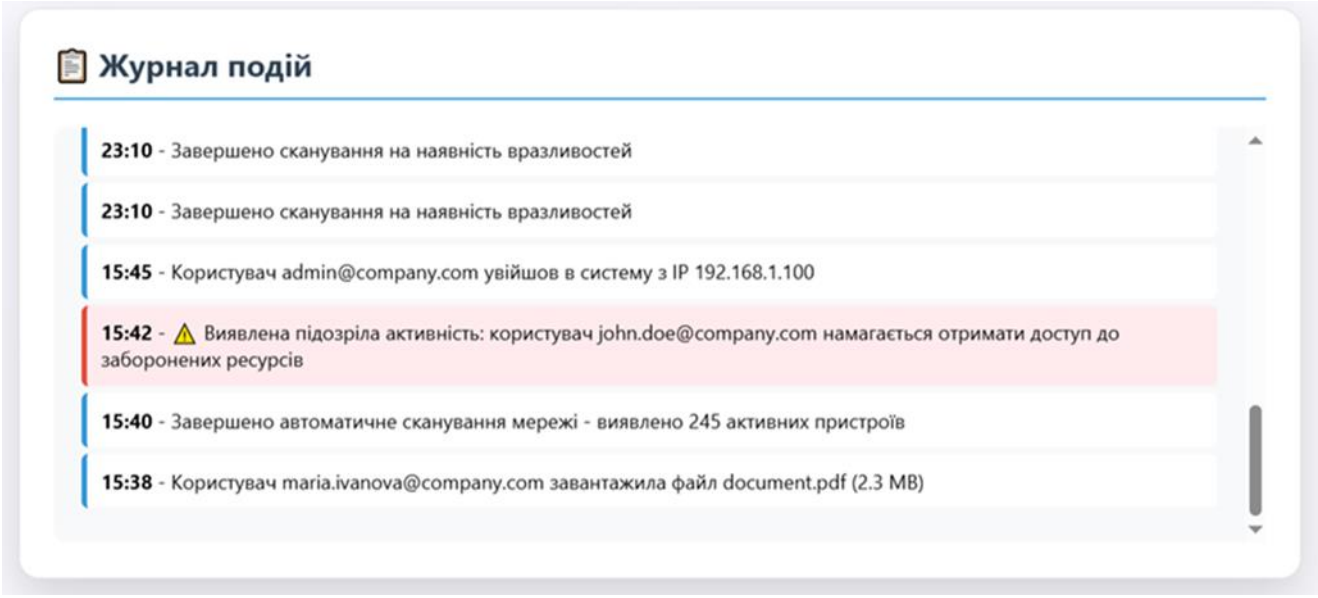


Рисунок 1.14 - Журнал подій

Цей журнал є хронологічним переліком подій, кожна з яких має точну часову мітку (години та хвилини). Кожен запис супроводжується кольоровою вертикальною смугою зліва, яка, індикує тип або критичність події. Більшість подій

позначені синьою смугою, що, можливо, означає стандартні або успішно завершені операції. Наприклад, сині смуги позначають стандартні операції або успішні події: двічі зафіксовано завершено сканування на наявність вразливостей (о 23:10), успішний вхід користувача admin@company.com з IP-адреси 192.168.1.100 (о 15:45), завершення автоматичного сканування мережі з виявленням 245 активних пристроїв (о 15:40) та завантаження файлу "document.pdf (2.3 MB)" користувачем maria.ivanova@company.com (о 15:38). Особливу увагу привертає запис, виділений червоним фоном та значком попередження: о 15:42 було виявлена підозріла активність: користувач john.doe@company.com намагається отримати доступ до заборонених ресурсів. Це є критично важливим повідомленням, що вказує на можливе порушення політики безпеки або спробу несанкціонованого доступу, що потребує негайної реакції.

3.4 Висновки до розділу

У третьому розділі цього дослідження описано процес розробки та впровадження системи аналізу поведінки користувачів в корпоративних мережах. Основна мета полягала в тому, щоб створити систему, яка буде надійно захищати користувачів, виявляти аномалії та потенційні загрози, одночасно забезпечуючи простоту використання та зручний інтерфейс.

У цьому розділі було обґрунтовано нагальну необхідність створення такої системи, підкреслюючи зростаючу складність внутрішніх загроз, потреба у відповідності регуляторним вимогам та обмеженість традиційних методів захисту. Було детально описано загальну структуру системи, яка включає модулі для безпечної авторизації, збору та агрегації даних про активність користувачів, а також потужний аналітичний блок, що відповідає за ідентифікацію аномалій. Особливу

увагу було приділено принципам її роботи, які базуються на безперервному моніторингу та зіставленні поточної поведінки з визначеними базовими лініями.

Процес демонстрації роботи системи наочно ілюстрував її ключові можливості. Візуалізація сторінки авторизації показала простоту та надійність входу, підтверджуючи захищений доступ до конфіденційних даних. Панель загальної статистики продемонструвала здатність системи надавати моментальний огляд стану мережі, включаючи кількість активних користувачів, обсяги трафіку та загальну кількість заблокованих спроб. Особливо цінною виявилася демонстрація панелі "Аномалії поведінки", яка чітко категоризує виявлені відхилення, такі як незвичайний час входу, множинні невдалі спроби авторизації, аномальний трафік та підключення нових пристроїв. Це підкреслює проактивний характер системи у виявленні потенційних інцидентів.

Загалом, результат впровадження системи аналізу поведінки користувачів полягає в тому, що вона задовільно відповідає встановленим вимогам щодо моніторингу та безпеки. Створений інструмент значно підвищує здатність організації оперативно виявляти та реагувати на внутрішні та зовнішні загрози, які проявляються через нетипову поведінку користувачів, тим самим посилюючи загальну інформаційну безпеку корпоративної мережі.

ВИСНОВКИ

На завершення проведеного дослідження, присвяченого розробці та аналізу системи аналізу поведінки користувачів у мережах приватних підприємств, можна зробити наступні висновки. У ході роботи було розглянуто теоретичні основи та практичні аспекти застосування систем для підвищення рівня інформаційної безпеки.

У першому розділі було визначено загальні характеристики систем аналізу поведінки користувачів, їхнє значення для корпоративних мереж, основні методи збору та обробки даних, а також роль моніторингу мережевого трафіку. Проведений огляд існуючих систем дозволив виявити їхні переваги та недоліки, а також підкреслити важливість своєчасного виявлення наслідків нетипової поведінки для запобігання потенційним загрозам.

Другий розділ був присвячений детальному аналізу нетипової поведінки користувачів та джерел загроз у контексті приватних підприємств. Було класифіковано різні види аномальної активності, розглянуто моделі внутрішніх та зовнішніх загроз, а також досліджено методи виявлення такої активності. Отримані результати підкреслюють критичну важливість своєчасного реагування на нетипову поведінку для мінімізації ризиків інформаційної безпеки.

У третьому розділі було описано необхідність створення даної системи, процес розробки та впровадження системи аналізу поведінки користувачів в корпоративній мережі. Основна мета полягала в тому, щоб створити систему, яка буде надійно захищати користувачів, виявляти аномалії та потенційні загрози, одночасно забезпечуючи простоту використання та зручний інтерфейс. Було представлено алгоритм, який детально описує роботу системи аналізу поведінки користувачів у корпоративних мережах, починаючи з моменту запуску і завершуючи періодичною генерацією звітів для адміністраторів.

Таким чином, це дослідження підтвердило актуальність та важливість розробки та впровадження систем аналізу поведінки користувачів у мережах приватних підприємств. Проведені дослідження та впровадження програмних

продуктів підтвердили потенціал подальшого впровадження та вдосконалення цих технологій для забезпечення кібербезпеки в сучасних умовах. Розроблена система аналізу поведінки користувачів у корпоративній мережі пропонує високий рівень захисту та виявлення аномалій завдяки сучасним процедурам моніторингу, що робить його цінним інструментом у боротьбі з кіберзлочинністю.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Корпоративні локальні мережі. 2020. Mediana. URL: https://mediana.net.ua/%20korporativni-lokalni-merezhi/ (дата звернення 06.03.25).

2. Особливості побудови і використання сучасних корпоративних комп'ютерних мереж. 2017. С. 1-2. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17175/1935.pdf?sequence=3&isAllowed=y (дата звернення 5.03.25).

3. Багатошарове представлення корпоративної мережі. 2016. С. 1. StudFiles. URL: https://studfile.net/preview/5470625/page:4/ (дата звернення 06.03.25).

4. «Що таке лог-файли, як ними керувати і для чого потрібні лог-файли»: стаття. 2024. Hostkoss blog. URL: https://hostkoss.com/b/uk/log/ (дата звернення 07.03.25).

5. Лог-файли як невід'ємна частина процесу розробки. 2023. Foxminded. URL: https: //foxminded.ua/shcho-take-loh-faily/ (дата звернення 07.03.25).

6. Аналіз мережевого трафіку. 2023. Intelligent IT Distribution. URL: https://iitd.ua/analiz-merezhevogo-trafiku-nta/ (дата звернення 08.03.25).

7. Конспект лекцій з дисципліни «Захист інформації у комп'ютерних системах» для студентів денної та заочної форми навчання спеціальності 123 "Комп'ютерна інженерія". Тернопіль. 2019. URL: https://elartu.tntu.edu.ua/bitstream/lib/29278/1/!!_Lek_print_zahust_123.pdf (дата звернення 08.03.25).

8. Рекомендації щодо моніторингу та виявлення загроз. Стаття. 2024. URL: https://learn.microsoft.com/uk-ua/power-platform/well-architected/security/monitor-threats (дата звернення 09.03.25).

9. Аналіз мережевого трафіку: інструменти та методи. 2024.ProxyRating. URL: https://proxys-rating.com/analiz-merezhevogo-trafiku-instrumenty-ta-metody/ (дата звернення 09.03.25).

10. Аналіз мережевого трафіку: Інструменти та методи для оптимізації 2024 Автор pro_ira. URL: https://proxys-rating.com/analiz-merezhevogo-trafiku-instrumenty-ta-metody-dlya-optymizacziyi/ (дата звернення 10.03.25).

11. Програми для моніторингу мережі. 2025. SoftinventiveJab. URL: https://www.softinventive.com.ua/best-network-monitoring-tools (дата звернення 10.03.25).

12. Засоби моніторингу та аналізу мережі. EDUKATION. Media wiki. Творімо освіту разом. 2014. URL: https://wiki.cusu.edu.ua/index.php/%D0%97%D0%B0%D1%81%D0%BE%D0%B1%D0%B8_%D0%BC%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%D1%83_%D1%82%D0%B0_%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D1%83_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96 (дата звернення 11.03.25).

13. Інструменти моніторингу. 2024. Oberig. URL: https://oberig-it.com/statti/9-najkrashhyh-instrumentiv-monitoryngu-merezhevoyi-bezpeky-dlya-vyyavlennya-potenczijnyh-zagroz/ (дата звернення 11.03.25).

14. Інструменти командного рядка. 2022. LinuxTheBest. URL: https://linuxthebest.net/6-instrumentov-komandnoj-stroki-dlya-monitoringa-proizvoditelnosti/ (дата звернення 12.03.2025).

15. Моніторинг та аналіз комп'ютерних мереж. 2019. С. 1.StudFile. URL: https:// studfile.net/preview/9239701/ (дата звернення 12.03.25).

16. Довгань О., Литвинова Л., Дорогих С.. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест. – К., 2023.– №12 (грудень) . – 354 с. URL: https://ippi.org.ua/sites/default/files/2023-12.pdf (дата звернення 13.03.25).

17. Компрометація акаунту. 2024. VPN Unlimited. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/account-compromise(дата звернення 14.03.25).

18. Інсайдерські загрози. 2020. Eska. URL: https://eska.global/blog/4-prikladi-insajderskih-zagroz-ta-yak-yih-zapobigti (дата звернення 15.03.25).

19. Смірнов О.А., Конопліцька - Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. С 50 Інформаційна безпека в комп'ютерних мережах : навч. посіб. — Кропивницький, 2020. — 295 с. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/73209786-0b68-4fc2-8338-a86137bf992c/content (дата звернення 16.03.25).

20. Інформаційна безпека та інформаційні технології: збірник наукових праць V Міжнародної науково-практичної конференціїю. ІБІТ 2024. м. Львів, 2024, 636 с. URL: https://indico.ldubgd.edu.ua/event/55/attachments/662/975/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%20%D0%BD%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%B8%D1%85%20%D0%BF%D1%80%D0%B0%D1%86%D1%8C%20%D0%BA%D0%BE%D0%BD%D1%84.%20%D0%86%D0%91%D0%86%D0%A2_2024%20%E2%80%93%20%D0%B7%20%D0%BE%D0%B1%D0%BA%D0%BB%D0%B0%D0%B4%D0%B8%D0%BD%D0%BA%D0%BE%D1%8E.pdf (дата звернення 17.03.25).

21. Антифішинг - як захиститися від фішингу у сучасних реаліях. ESKA. Fishing Protection. 2021. URL: https://eska.global/blog/antifishing-kak-zashititsya-v-sovremennyh-realiyah (дата звернення 18.03.25).

22. Безпека кінцевих точок. 2024. LazarusAlliance. URL: https://lazarusalliance.com/uk/endpoint-security-and-modern-compliance/(дата звернення 19.03.25).

23. Олещенко Л.М. Організація комп'ютерних мереж: конспект лекцій: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення», спеціалізації «Програмне забезпечення комп'ютерних та інформаційно – пошукових систем». – Київ, 2018. – 225 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/245d8d52-1715-4f2e-9e6a-e4bd17db7d4d/content (дата звернення 19.03.25).

24. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с. URL:

https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf (дата звернення 20.03.25).

25. Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. В. А. Романюка. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2023. № 3. 186 с. URL: https://journal.viti.edu.ua/downloads/MITIT_3_2023.pdf (дата звернення 21.03.25).

26. Шкідливе програмне забезпечення. 2023. Wikis.Fandom. URL: https://wikis.fandom.com/uk/wiki/%D0%9F%D0%BE%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8F_%D1%88%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D0%BE%D0%B3%D0%BE_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F (дата звернення 22.03.25).

27. Витік даних. 2023. Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-data-leak (дата звернення 23.03.25).

28. Пірог О.В. Безпека вебдодатків : навч. посібн. / О.В. Пірог. – Електронні дані. – Житомир : Житомирська політехніка, 2025. – 290 с. URL: https://eztuir.ztu.edu.ua/bitstream/handle/123456789/8813/%D0%9F%D1%96%D1%80%D0%BE%D0%B3%20%D0%9E.%D0%92.%20%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B2%D0%B5%D0%B1%D0%B4%D0%BE%D0%B4%D0%B0%D1%82%D0%BA%D1%96%D0%B2.%20%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA-2025.pdf?sequence=1&isAllowed=y (дата звернення 24.03.25).

29. Джерело загроз. 2015. ELAKPI. URL: https://ela.kpi.ua/server/api/core/bitstreams/1166b582-60dd-482e-a580-ac864b3468a4/content (дата звернення 25.03.25).

30. Найпоширеніші внутрішні загрози безпеці даних та способи боротьби з ними. 2022. COREWIN. URL: https://corewin.ua/blog/internal-data-security-threats/ (дата звернення 26.03.25).

31. Кіструга Ю.В. Економіка. Фінанси. Право. Внутрішні та зовнішні загрози безпеки підприємства: сутність та їх діагностика. Випуск: № 1, 2024. URL: http://efp.in.ua/uk/journal-article/1252 (дата звернення 27.03.25).

32. Франчук В. І. Теорія безпеки соціальних систем: підручник / В.І.Франчук. – Львів: ЛьвДУВС, 2016. – 216 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/476/1/%D1%82%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC.pdf (дата звернення 01.04.25).

33. Що таке шкідливе програмне забезпечення? Захисний комплекс Micro soft. 2025. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware (дата звернення 02.04.25).

34. Таксономія аномалій. 2023. URL: https://ela.kpi.ua/server/api/core/bitstreams/ecdf61dd-487e-46e2-817a c80f2198eff7/content (дата звернення 03.04.25).

35. Шушура О., Мороз Є., Сегеда І., Асєєва Л./ Інформаційна система виявлення аномалій в даних на основі методів машинного навчання. Вісник КрНУ ім. М.Остроградського. Випуск 5/2024 (148). URL: https://visnikkrnu.kdu.edu.ua/statti/2024_5_55.pdf (дата звернення 04.04.25).

36. Виявлення аномалій. 2021. Електротехнічні та комп'ютерні науки. Документ. URL: file:///C:/Users/77777/Downloads/3196-Article%20Text-2350-1-10-20210904.pdf (дата звернення 05.04.25).

37. Колодчак О.М. Сучасні методи виявлення аномалій в системах виявлення вторгнень. Львівська політехніка, 2012. URL:

https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6726/16-98-104.pdf (дата звернення 06.04.25).

38. Аналіз поведінки користувачів. 2024. Eska. URL: https://eska.global/solutions/ueba (дата звернення 07.04.25).

39. Хоменко В.Г., Павленко М.П. Х 76 Комп'ютерні мережі : Навчальний посібник / В. Г. Хоменко, М. П. Павленко. – Донецьк : ЛАНДОН-ХХІ, 2011. – 316 с. URL: https://vasylkiv-litsei.com.ua/media/library/book/1614070458.978003.pdf (дата звернення 08.04.25).

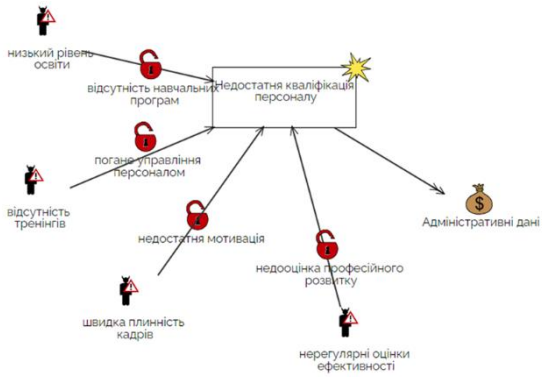
40. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. К 63 Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // - К.: Компрінт, 2017.- 821с. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_-_kompyuterni_merezhi.pdf (дата звернення 09.04.25).

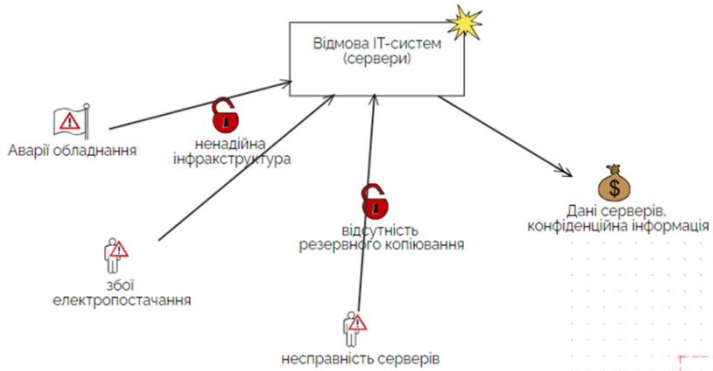
41. Алгоритм. 2023. ITSTEP. URL: https://cloud.itstep.org/blog/building-and-understanding-algorithms-a-step-by-step-guide-for-beginners (дата звернення 10.04.25).

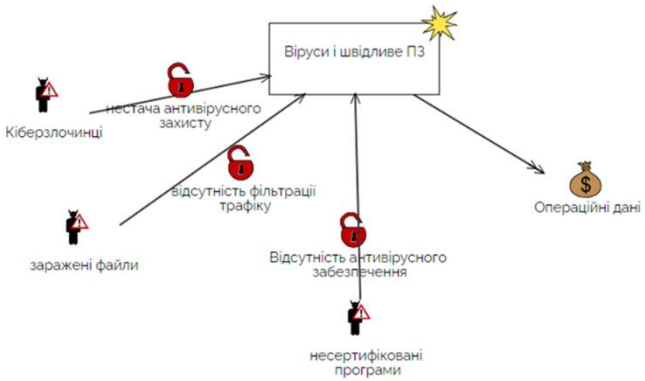
ДОДАТОК А

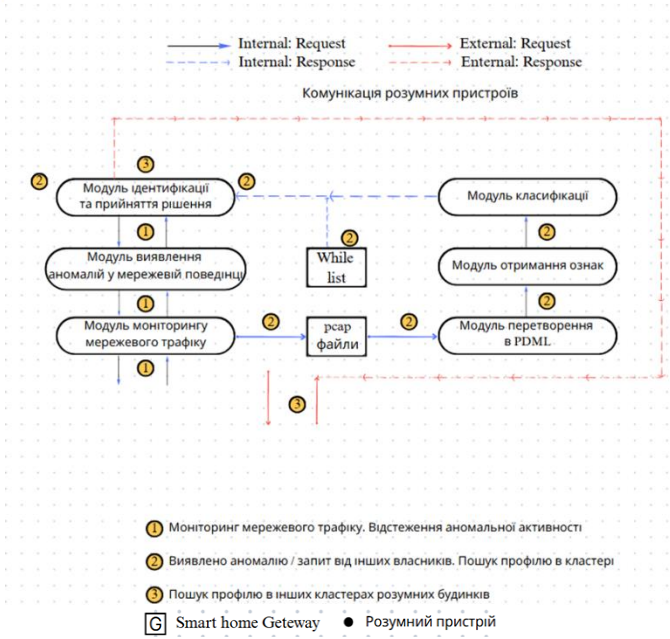
Копії графічної частини

КРБКБ.2101135.21.01.15.Е8



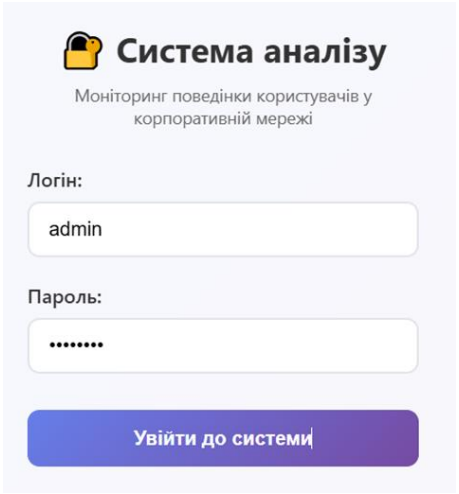


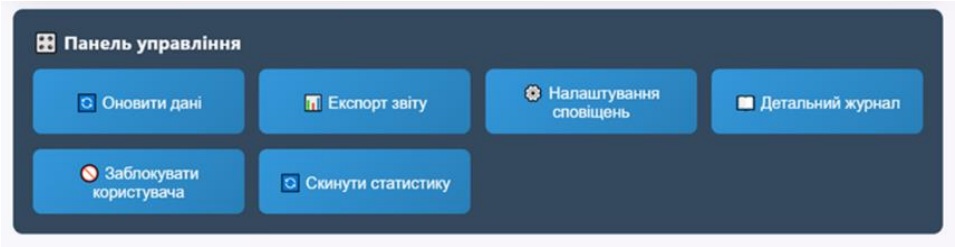


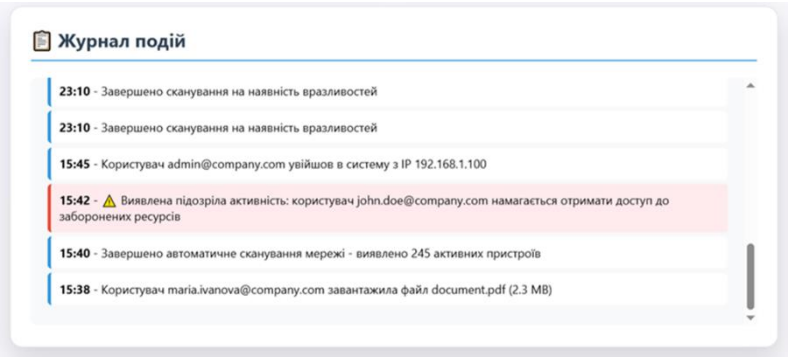


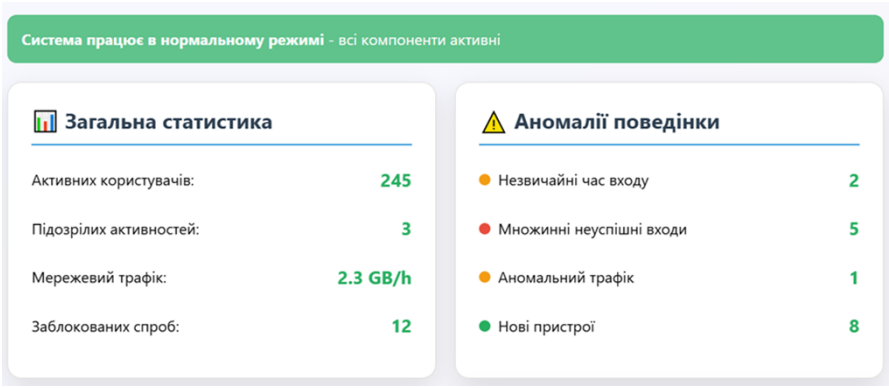
					КРБКБ.2101135.21.01.15 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система аналізу поведінки користувачів у мережах приватних підприємствах	Лит. / Маса / Масштаб
Розроб.		Шлапак О. С.				У
Перевір.		Тітова В.Ю.			Графічний вигляд програми	Аркуш 1 / Аркушів 3
Т. контр.						
Н.контр.		Мостовий С.				ХНУ, КБ-21-1
Затверд.		Ключ Ю.П.				

						КРБКБ.2101135.21.01.15 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система аналізу поведінки користувачів у мережах приватних підприємствах	Літ	Маса / Масштаб
Розроб.		Шлапак О. С.				У	
Перевір.		Тітова В.Ю.			Графічний вигляд програми	Аркуш 2	Аркушів 3
Т. контр.							
Н.контр.		Мостовий С.				ХНУ, КБ-21-1	
Затверд.		Кльоц Ю.П.					









					КРБКБ.2101135.21.01.15 Е8		
Зм	Арк	№ докум	Підпис	Дата	Система аналізу поведінки користувачів у мережах приватних підприємствах	Літ	Маса	Масштаб
Розроб.		Шлапак О. С.				У		
Перевір.		Тітова В.Ю.			Графічний вигляд програми	Аркуш 3	Аркушів 3	
Т. контр.								
Н.контр.		Мостовий С.				ХНУ, КБ-21-1		
Затверд.		Кльоц Ю.П.						

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 10.0%

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

	Document		Sum coincidence on the DB	
ID: 243441 Title: Система аналізу поведінки користувачів у мережах приватних підприємств Added in a DB: 2025-06-04 Authors: Шлапак Олександра Сергіївна Heads: Тітова В.Ю. Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	91213	640	14595 (16%)	115 (18%)

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: Шлапак Олександра Сергіївна

Співавтор:

Назва: Система аналізу поведінки користувачів у мережах приватних підприємств

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:2.8%

Коефіцієнт подібності 2:0.6%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-04 23:17:38.0

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:

06.06.2025р.

РІШЕННЯ ЕКСПЕРТНОЇ 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 аналізу поведінки користувачів у мережах приватних підприємств

Автор: Шлапак Олександра Сергіївна

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, канд. 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. 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 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.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою виявлення і запобігання плагіату StrikePlagiarism складає 97,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 90%.

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

Керівник роботи _____ Віра ТІТОВА

Гарант ОПП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Шлапак Олександра Сергіївна
Тема: «Система аналізу поведінки користувачів у мережах приватних підприємств»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 64;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці системи аналізу поведінки користувачів у мережах приватних підприємств. Вона досліджує методи та алгоритми для виявлення аномалій та загроз безпеці, що виникають внаслідок дій користувачів.

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

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі наведено методи збору та обробки даних про активність користувачів, методи моніторингу мережевого трафіку, аналіз пакетів та їх роль у безпеці, наслідки нетипової поведінки для інформаційної безпеки підприємства. У другому розділі проведено класифікацію нетипової поведінки в мережах приватних підприємств, розроблено моделі внутрішніх та зовнішніх загроз безпеки мережі, запропоновано метод виявлення аномальної активності користувачів. У третьому розділі наведено реалізацію системи захисту та продемонстровано її роботу.

4. Позитивні сторони кваліфікаційної роботи полягають у аналізі існуючих підходів до аналізу поведінки користувачів, розробці моделі поведінки користувачів, яка враховує специфіку приватних підприємств, створення алгоритмів для виявлення аномалій та загроз безпеці, розробку програмного забезпечення для реалізації системи аналізу поведінки користувачів.

5. Негативні сторони кваліфікаційної роботи: у роботі не проведено розрахунок помилок першого та другого роду, точності, акуратності, F-міри тощо.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) ___ завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 09 » червня 2025. _____ (підпис)

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.

Шлапак Олександри Сергіївної
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-1

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, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена 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 (StrikePlagiarism 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.

01.06.25
дата

підпис