Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Програмні засоби виявлення мережних аномалій

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІ-21-2
Дмитро ФЕДЬКО
(власне ім'я, прізвище)

Спеціальність
123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп'ютерна інженерія
(повна назва освітньої програми)

Керівник: ст. викл. Владислав ДЯЧЕНКО
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Федьку Дмитру Анатолійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Програмні засоби виявлення мережних аномалій

затверджена наказом по університету від “ 26 ” травня 2025 р. № 426 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 16 червня 2025 р.

3. Вхідні дані до роботи
мережна аномалія
Google Colab
Python
моделвання трафіку

4. Перелік питань, що потрібно опрацювати у роботі
Аналіз предметної області та огляд сучасних методів виявлення мережних аномалій
Методи машинного навчання для виявлення мережевих атак
Розробка та реалізація програмного засобу виявлення мережних аномалій

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 13 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Отримання завдання та аналіз літератури	26.05.2025–30.05.2025	
2	Огляд існуючих засобів виявлення аномалій	31.05.2025–03.06.2025	
3	Вибір алгоритмів	04.06.2025–06.06.2025	
4	Вибір програмних засобів	07.06.2025–08.06.2025	
5	Програмна реалізація	09.06.2025–11.06.2025	
6	Аналіз отриманих результатів	12.06.2025–13.06.2025	
7	Оформлення записки	14.06.2025–16.06.2025	

Дата видачі завдання " 26 " травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ст. викл. Владислав ДЯЧЕНКО
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 56 с., 12 рис., 2 дод., 7 джерел.

МЕРЕЖЕВІ АНОМАЛІЇ, КІБЕРБЕЗПЕКА, АВТОЕНКОДЕР, LSTM, МАШИННЕ НАВЧАННЯ, НЕЙРОННІ МЕРЕЖІ, GOOGLE COLAB, АНАЛІЗ ТРАФІКУ, ВИЯВЛЕННЯ ВІДХИЛЕНЬ, КОРПОРАТИВНА МЕРЕЖА, NSL-KDD, РЕКОНСТРУКТИВНА ПОХИБКА, ПОТОКОВА ОБРОБКА ДАНИХ.

Метою кваліфікаційної роботи є розробка, реалізація програмних засобів для виявлення мережних аномалій з використанням сучасних методів машинного навчання, що дозволяють виявляти як відомі, так і нові загрози в комп’ютерних мережах.

У ході виконання кваліфікаційної роботи здійснено аналіз сучасних наукових підходів до виявлення мережевих аномалій, включаючи традиційні сигнатурні методи, моделі поведінкового аналізу та алгоритми глибокого навчання. Обґрунтовано вибір моделі автоенкодера з рекурентними компонентами типу LSTM як базової архітектури для реалізації системи виявлення, що дозволяє враховувати часову структуру даних і підвищити чутливість до латентних відхилень.

Реалізацію програмного прототипу здійснено в середовищі Google Colab із використанням мовних та аналітичних бібліотек Python, зокрема TensorFlow, Scikit-learn, Pandas, Scapy. Проведено експериментальне тестування моделі на синтетичному наборі даних, що імітує корпоративний трафік з аномаліями, побудованому за зразком NSL-KDD. Аналіз результатів показав високу точність, стабільність та здатність моделі до узагальнення в умовах обмеженої навчальної вибірки.

ABSTRACT

Bachelor’s thesis: 56 pages, 12 figures, 2 appendices, 7 sources.

NETWORK ANOMALIES, CYBERSECURITY, AUTOENCODER, LSTM, MACHINE LEARNING, NEURAL NETWORKS, GOOGLE COLAB, TRAFFIC ANALYSIS, ANOMALY DETECTION, CORPORATE NETWORK, NSL-KDD, RECONSTRUCTION ERROR, STREAMING DATA PROCESSING.

The major goal of this thesis is the development and implementation of software tools for detecting network anomalies using modern machine learning methods, enabling the identification of both known and novel threats in computer networks.

In order to a comprehensive review of contemporary scientific approaches to anomaly detection in network environments has been conducted, including traditional signature-based techniques, behavioral modeling, and deep learning algorithms. The autoencoder model with recurrent LSTM components was justified as the core architecture for the detection system, as it allows for capturing temporal data structure and enhances the model's sensitivity to latent deviations.

The prototype implementation was carried out in the Google Colab environment using Python programming libraries, specifically TensorFlow, Scikit-learn, Pandas, and Scapy. Experimental testing was performed on a synthetic dataset emulating corporate traffic with injected anomalies, constructed in the style of the NSL-KDD benchmark. The analysis of the results demonstrated high accuracy, robustness, and generalization capability of the model under conditions of limited training data availability.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AUC – Area Under the Curve

CPS – кіберфізична система

GPU – Graphics Processing Unit

LSTM – Long Short-Term Memory

MSE – Mean Squared Error

NSL-KDD – Network Security Laboratory – Knowledge Discovery in Databases

PCA – Principal Component Analysis

PR – Precision-Recall

ROC – Receiver Operating Characteristic

Scapy – Python-бібліотека для аналізу мережевих пакетів

TensorFlow – програмна платформа для реалізації моделей глибокого навчання

ВСТУП

У сучасному світі інформаційні технології проникають у всі сфери людської діяльності, і разом із цим зростає залежність суспільства від стабільності та безпеки комп’ютерних мереж. Однією з головних загроз функціонуванню таких систем є несанкціонований доступ, мережеві атаки та інші форми кіберзагроз, які можуть мати серйозні наслідки як для окремих користувачів, так і для цілих організацій. В умовах постійного зростання складності й обсягу мережевого трафіку дедалі більшої актуальності набувають методи автоматичного виявлення аномалій, що дозволяють оперативно реагувати на підозрілу активність та запобігати потенційним інцидентам інформаційної безпеки.

Аномалії у мережевому трафіку можуть свідчити про атаки типу «відмова в обслуговуванні» (DoS), сканування портів, спроби проникнення або передачу шкідливого програмного забезпечення. У зв’язку з цим важливу роль відіграють програмні засоби, здатні не лише фіксувати відомі загрози, але й виявляти невідомі або модифіковані атаки шляхом аналізу поведінкових відхилень від нормального функціонування мережі.

Метою даної кваліфікаційної роботи є практична реалізація програмного засобу для виявлення мережних аномалій з використанням сучасних методів машинного навчання, що дозволяє виявляти як відомі, так і нові загрози в комп’ютерних мережах.

Завдання:

- провести аналіз існуючих типів мережевих атак та аномалій, які можуть загрожувати інформаційним системам;

- вивчити класифікацію та принципи роботи сучасних систем виявлення вторгнень (IDS).

- дослідити підходи до виявлення аномалій: сигнатурні, аномальні, гібридні; визначити їх переваги та обмеження;

- ознайомитися з методами машинного навчання, що застосовуються для аналізу мережевого трафіку;
- обґрунтувати вибір алгоритму машинного навчання для реалізації виявлення аномалій;
- реалізувати власну модель виявлення аномалій у середовищі Google Colab з використанням відкритого датасету;
- провести тестування розробленого рішення, оцінити його точність, ефективність і продуктивність.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОГЛЯД СУЧАСНИХ МЕТОДІВ ВИЯВЛЕННЯ МЕРЕЖНИХ АНОМАЛІЙ

1.1 Класифікація мережевих загроз та атак

Інформаційні системи в умовах відкритих комп’ютерних мереж перебувають під постійною загрозою несанкціонованого доступу, порушення конфіденційності, цілісності та доступності даних. Розуміння класифікації мережевих атак є необхідною передумовою для розробки ефективних програмних засобів виявлення аномалій, оскільки дає змогу чітко окреслити потенційні загрози, механізми їх реалізації та сигнатури поведінки в мережевому трафіку.

Загалом мережеві атаки можна класифікувати за кількома критеріями: за ціллю атаки, характером впливу, методами реалізації, рівнем моделі OSI, а також за ступенем впливу на системи.

До пасивних атак належать ті, що не змінюють потік даних, але здійснюють перехоплення або прослуховування трафіку з метою збору інформації (наприклад, сніфінг, перехоплення паролів). Такі атаки складно виявити, оскільки вони не залишають слідів активного втручання.

Активні атаки передбачають модифікацію переданих даних або генерацію шкідливого трафіку. Серед них виділяють атаки типу «відмова в обслуговуванні» (DoS), розподілені атаки (DDoS), спуфінг, сесійне викрадення, ін’єкційні атаки, експлуатацію вразливостей протоколів тощо.

Особливу категорію становлять атаки нульового дня (zero-day attacks), які використовують уразливості, ще не виявлені або не виправлені постачальниками програмного забезпечення. Вони є особливо небезпечними через відсутність сигнатур і високий ступінь непередбачуваності.

Іншою важливою категорією є внутрішні загрози, що походять від легітимних користувачів, які навмисно або ненавмисно порушують політику

безпеки. Вони особливо складні для виявлення, оскільки дії таких користувачів виглядають зовні нормальними.

Атаки також можна класифікувати за рівнями моделі OSI. Наприклад, на мережевому рівні (Network Layer) поширені атаки типу IP Spoofing або ICMP Flood. На транспортному рівні – TCP SYN Flood, Port Scanning, а на прикладному – SQL Injection, XSS та інші веб-атаки.

1.2 Підходи до виявлення аномалій: сигнатурні, аномальні, гібридні

Виявлення мережевих аномалій є ключовим завданням у сфері інформаційної безпеки, яке забезпечує вчасне реагування на загрози та запобігання атакам. На практиці використовуються три основні підходи до виявлення аномалій у мережевому трафіку: сигнатурний, аномальний і гібридний. Кожен із них має свої принципи роботи, переваги та обмеження, що визначає їх застосування в конкретних умовах.

Сигнатурний підхід базується на зіставленні вхідного трафіку з базою відомих ознак (сигнатур) атак. Якщо в трафіку виявляється шаблон, який відповідає запису в базі, генерується сповіщення про інцидент. Цей метод ефективний для виявлення вже відомих загроз і характеризується високою точністю при низькому рівні хибнопозитивних спрацьовувань. Однак його основним недоліком є неспроможність виявляти нові, ще не задокументовані атаки, а також залежність від своєчасного оновлення сигнатурної бази.

Аномальний підхід полягає у побудові моделі «нормальної» поведінки системи або мережі. Усе, що істотно відхиляється від цієї моделі, вважається потенційною загрозою. Такий підхід дозволяє виявляти невідомі атаки, зокрема атаки нульового дня, і є більш гнучким в умовах змінюваного середовища. Проте побудова точної моделі нормальної поведінки є складною задачею, а надмірна чутливість алгоритмів може призводити до великої кількості хибнопозитивних спрацьовувань, що ускладнює практичне використання.

Гібридні системи поєднують сигнатурний та аномальний підходи з метою отримання переваг обох методів. Вони дозволяють зменшити ймовірність хибнопозитивних спрацювань та одночасно забезпечити виявлення нових загроз. У таких системах зазвичай сигнатурний модуль виконує швидку первинну фільтрацію, а аномальний – глибший поведінковий аналіз. Гібридні методи також активно використовують елементи машинного навчання, що дає змогу автоматизувати процеси виявлення та адаптації до нових загроз.

У цілому вибір підходу до виявлення аномалій визначається вимогами до точності, швидкодії, масштабованості та ресурсоємності системи, а також специфікою середовища, у якому вона функціонує. У наступних підрозділах буде розглянуто приклади реалізації таких підходів у конкретних програмних засобах та оцінено їхню ефективність у практичних умовах.

1.3 Методи машинного навчання у виявленні аномалій

Із розвитком обчислювальних технологій та зростанням обсягів мережевого трафіку, дедалі більше уваги приділяється застосуванню методів машинного навчання для виявлення мережних аномалій. Ці методи дозволяють автоматизувати аналіз великих масивів даних, виявляти приховані залежності та шаблони, а також ефективно розпізнавати відхилення від нормальної поведінки, що можуть свідчити про загрозу безпеці.

У загальному випадку машинне навчання в цій галузі поділяється на контрольоване та неконтрольоване. Контрольоване навчання передбачає наявність мічених даних, тобто прикладів нормальної поведінки і відомих атак. До найпоширеніших алгоритмів цієї групи належать логістична регресія, дерева рішень, випадковий ліс (Random Forest), підтримкові вектори (SVM) та нейронні мережі. Вони добре працюють за наявності якісно розмічених навчальних вибірок, проте чутливі до незбалансованих даних і не

завжди здатні виявляти нові типи загроз.

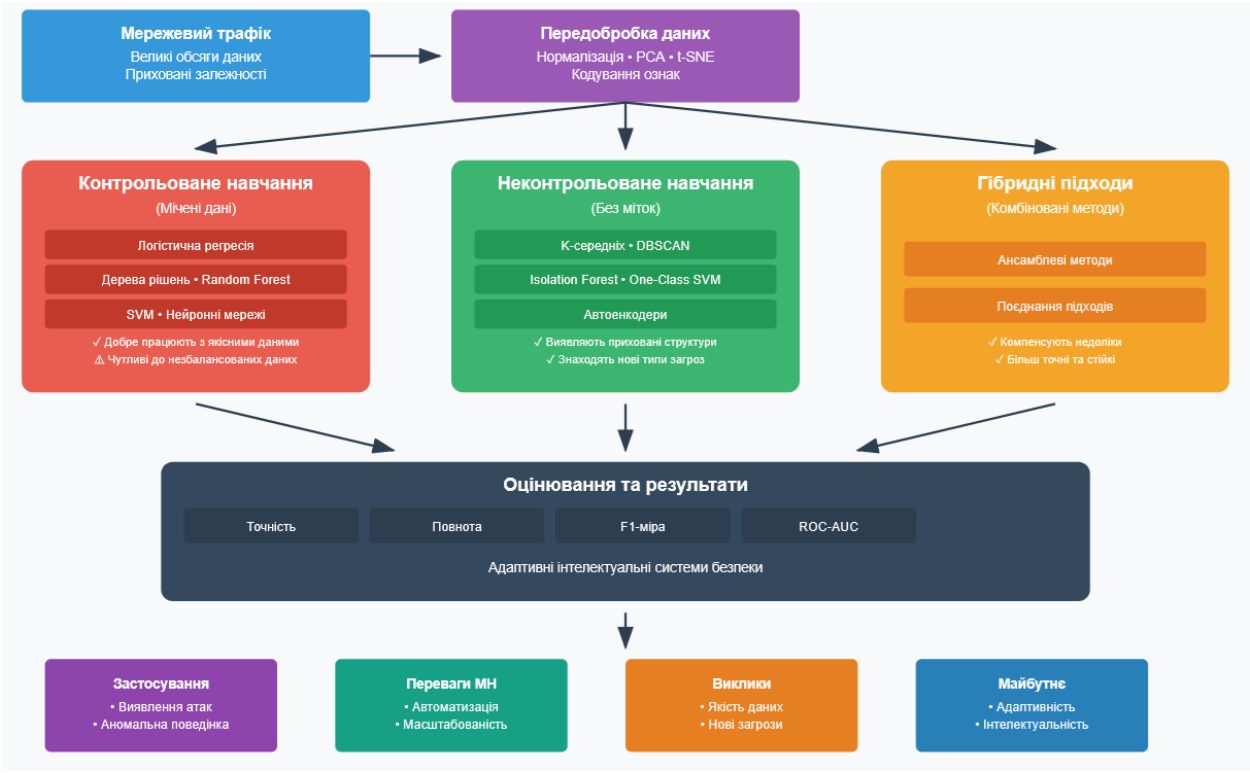

Рисунок 1.1 – Методи машинного навчання для виявлення мережних аномалій

На рисунку 1.1 представлені методи виявлення мережних атак. У разі відсутності міток використовується неконтрольоване навчання. У такому підході алгоритми самостійно визначають структуру даних і виділяють потенційно підозрілі спостереження. Найчастіше застосовуються методи кластеризації (наприклад, K-середніх, DBSCAN), виявлення викидів (Isolation Forest, One-Class SVM), а також автоенкодери – спеціальні нейронні мережі, що навчаються стискати і відновлювати вхідні дані, фіксуючи нетипові відхилення.

Особливе місце займають гібридні підходи, які поєднують контрольоване та неконтрольоване навчання або ж використовують ансамблеві методи. Такий підхід дозволяє компенсувати недоліки окремих алгоритмів і забезпечити більш точне та стійке виявлення.

Суттєву роль у ефективності методів машинного навчання відіграє

якість передобробки даних – нормалізація, видалення пропусків, кодування категоріальних ознак, а також зменшення розмірності за допомогою PCA або t-SNE. Крім того, критичне значення має вибір метрик оцінювання: точність, повнота, F1-міра, крива ROC-AUC дозволяють всебічно оцінити якість моделей в умовах реального трафіку.

Використання машинного навчання у сфері виявлення аномалій відкриває широкі можливості для створення адаптивних, інтелектуальних систем безпеки, здатних ефективно протистояти сучасним загрозам. У наступних розділах буде розглянуто приклади використання таких методів у популярних програмних платформах, а також реалізовано власний підхід із використанням відповідного алгоритму.

1.4 Огляд популярних програмних засобів

На сьогоднішній день на ринку представлено значну кількість програмних засобів, призначених для аналізу мережевого трафіку та виявлення аномалій. Їх функціональність охоплює як пасивний моніторинг, так і активний захист мережевої інфраструктури від загроз різного рівня. Найбільш відомими й широко використовуваними є такі інструменти, як Snort, Suricata, Zeek (раніше Bro), Wireshark, а також деякі інші рішення з відкритим кодом.

Snort – це одна з найпопулярніших систем виявлення вторгнень (IDS), яка працює на основі сигнатурного аналізу. Вона здатна здійснювати захоплення, декодування, попередню обробку та фільтрацію мережевого трафіку в реальному часі. Snort підтримує гнучкий механізм створення власних сигнатур і правил, що дозволяє адаптувати систему до специфічних умов мережі. Основна її перевага полягає у високій точності та ефективності при роботі з відомими атаками. Проте Snort обмежено здатна виявляти нові, невідомі типи загроз.

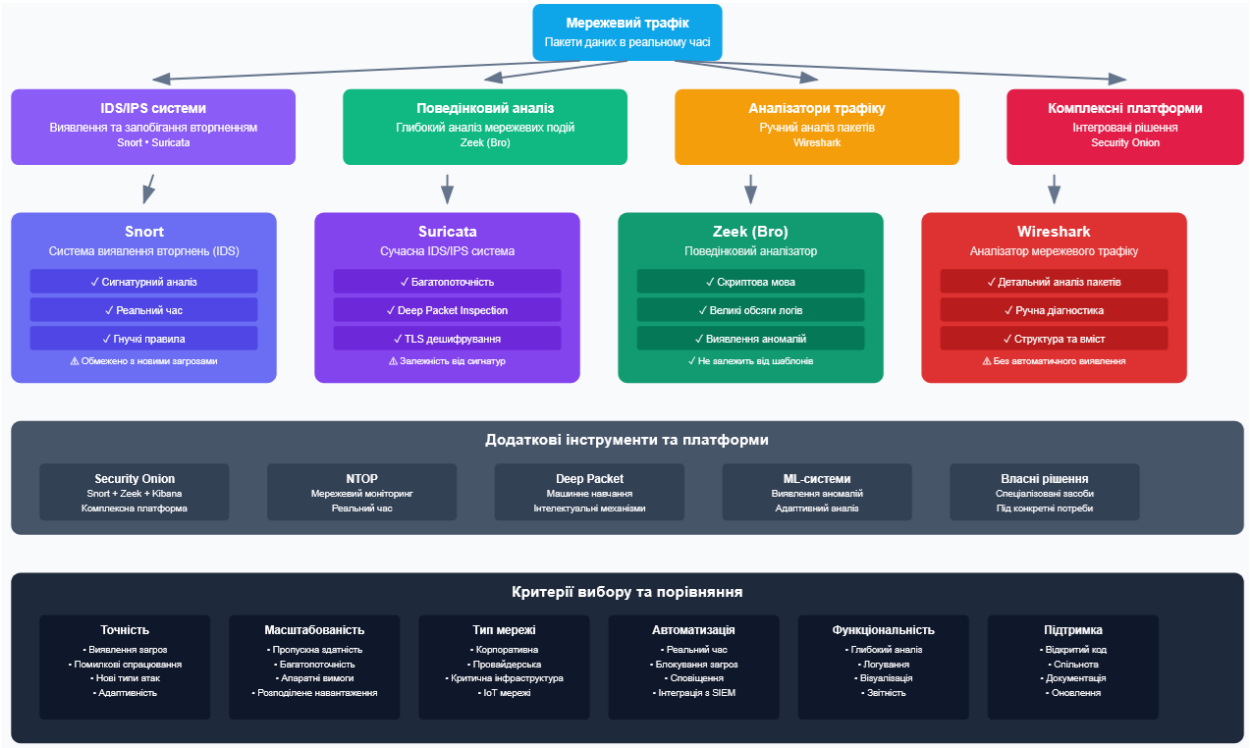

Рисунок 1.2 – Програмні засоби для виявлення мережних аномалій та аналізу трафіка

Діаграма на рисунку 1.2 наочно демонструє різноманітність доступних інструментів та допомагає зрозуміти їх переваги, обмеження та області застосування для вибору оптимального рішення залежно від конкретних вимог. Повернемося до інструментів.

Suricata є сучасною альтернативою Snort, яка також працює як IDS/IPS, але володіє більшою функціональністю. Вона підтримує багатопоточну обробку трафіку, що дозволяє досягати високої продуктивності на багатоядерних системах. Suricata інтегрує в собі можливості глибокого аналізу пакетів (Deep Packet Inspection), вбудовану підтримку TLS-дешифрування, логування HTTP, DNS та інших протоколів. У той же час, як і Snort, вона значною мірою залежить від сигнатур і потребує регулярного оновлення бази правил.

Zeek (Bro) вирізняється тим, що фокусується не лише на виявленні атак, а й на глибокому аналізі мережевих подій. Його особливістю є

орієнтація на поведінковий аналіз та можливість створення складних політик обробки подій за допомогою скриптової мови. Zeek генерує великий обсяг логів, що дозволяє здійснювати подальшу аналітику із залученням зовнішніх систем. Він підходить для побудови систем виявлення аномалій, які не обмежуються лише відомими шаблонами атак.

Wireshark – це потужний аналізатор мережевого трафіку, що використовується переважно для ручного аналізу. Він надає детальну інформацію про пакети, їхню структуру та вміст, що робить його незамінним інструментом для діагностики мережевих проблем. Проте Wireshark не є системою виявлення атак у класичному розумінні, оскільки не забезпечує автоматичного сповіщення або блокування загроз.

Крім згаданих, існують інші інструменти, такі як Security Onion (комплексна платформа, що поєднує Snort, Zeek, Kibana та інші компоненти), NTOP (мережевий моніторинг у реальному часі), а також системи з машинним навчанням на зразок Deep Packet, які намагаються впровадити інтелектуальні механізми у виявлення загроз.

Усі ці інструменти мають свої переваги та обмеження, а їх вибір залежить від конкретних вимог до точності, масштабованості, типу мережі та рівня автоматизації процесу. У подальших розділах буде здійснено порівняльний аналіз деяких із них та продемонстровано практичну реалізацію програмного засобу виявлення аномалій.

2 МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

2.1 Актуальність використання машинного навчання у виявленні атак

У сучасному цифровому середовищі забезпечення безпеки комп’ютерних мереж є одним із ключових викликів для інформаційної інфраструктури будь-якої організації. Кількість мережевих пристроїв, обсяг переданих даних та складність протоколів комунікації постійно зростають, що ускладнює завдання ефективного контролю та реагування на загрози. У цьому контексті традиційні методи виявлення атак, засновані переважно на сигнатурному аналізі або ручному моніторингу, дедалі частіше демонструють свою обмеженість і недостатню адаптивність до нових типів загроз.

Поява складних та динамічних атак, зокрема атак нульового дня, варіантів соціальної інженерії, внутрішніх загроз та поліморфних шкідливих програм, створює ситуацію, в якій системи безпеки мають бути не лише реактивними, але й проактивними. Умови, за яких загроза може не відповідати жодній із відомих сигнатур, потребують залучення технологій, здатних до самостійного виявлення аномальної поведінки без попереднього знання конкретного шаблону.

Машинне навчання як галузь штучного інтелекту пропонує механізми, що дозволяють системам адаптуватися до нових даних, виявляти приховані закономірності у великомасштабному трафіку та формувати рішення на основі попереднього досвіду. Застосування машинного навчання у сфері інформаційної безпеки дозволяє не лише автоматизувати процеси аналізу, а й виявляти загрози на ранніх етапах, оцінювати ризики в режимі реального часу та зменшувати навантаження на аналітиків безпеки.

Особливої актуальності набуває застосування методів машинного навчання у побудові систем виявлення мережевих атак, оскільки саме в цьому сегменті дані мають високий рівень варіативності, складну структуру та динамічні властивості. Ефективність виявлення значною мірою залежить від здатності алгоритмів аналізувати поведінкові особливості трафіку, виявляти відхилення від типових шаблонів і робити висновки в умовах неповноти або шумності даних.

Таким чином, інтеграція технологій машинного навчання у системи мережевої безпеки є не просто доцільною, а необхідною умовою ефективного протистояння сучасним кіберзагрозам. У подальших підрозділах даного розділу буде розглянуто основні класи методів машинного навчання, що застосовуються для виявлення атак, їх теоретичні засади та практичну придатність до розв’язання задач кіберзахисту.

2.2 Класифікація методів машинного навчання у виявленні мережевих атак

Застосування машинного навчання для виявлення мережевих атак ґрунтується на здатності алгоритмів аналізувати дані та формувати висновки на основі статистичних закономірностей. У рамках цієї парадигми існує кілька підходів до організації навчання моделей, які відрізняються за характером вхідної інформації, типом завдань, що вирішуються, і способами інтерпретації результатів. Кожен із цих підходів має свою методологію, рівень складності реалізації та ефективність у різних практичних сценаріях.

Одним із найпоширеніших підходів є кероване навчання, при якому алгоритм навчається на заздалегідь розмічених даних. У цьому випадку кожен об’єкт у вибірці має відповідну мітку, що вказує, чи є трафік нормальним чи зловмисним. Такий підхід дозволяє створити моделі високої точності, здатні класифікувати вхідні дані з використанням розроблених алгоритмів. Проте кероване навчання вимагає наявності великого обсягу

якісно розмічених даних, що не завжди можливо у реальних умовах, особливо коли мова йде про нові або рідкісні типи атак.

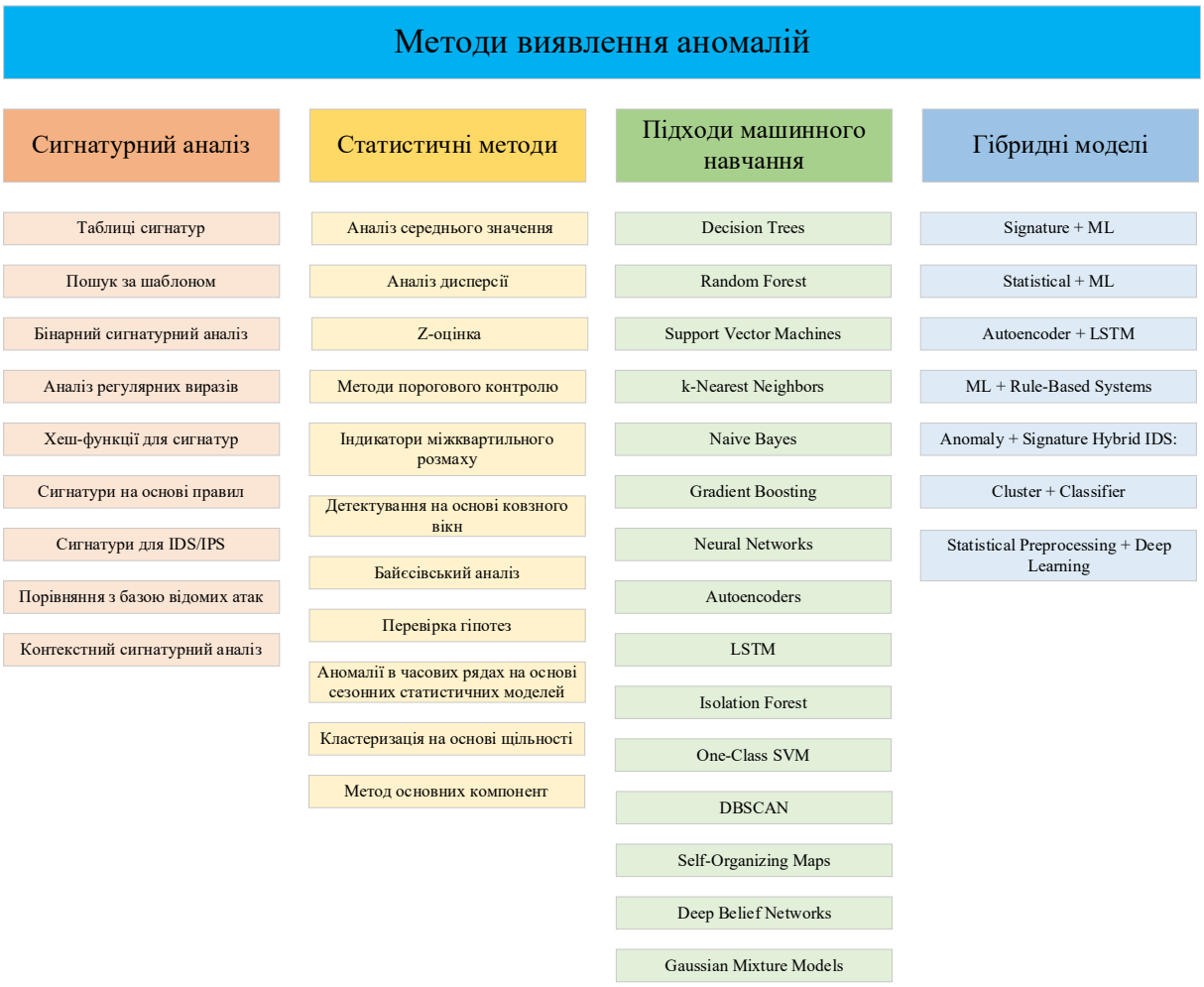

Рисунок 2.1 – Методи виявлення мережних аномалій

Некероване навчання ґрунтується на аналізі структури даних без використання міток. Алгоритм самостійно виявляє приховані залежності, кластери або викиди, які можуть свідчити про наявність аномалій. Цей підхід особливо цінний у ситуаціях, коли відсутня повна інформація про характеристики атак або спостерігається значна кількість нових загроз. Виявлення відхилень від стандартної поведінки мережевого трафіку дозволяє виявити потенційно небезпечні дії навіть без попереднього знання їхньої природи. Водночас некеровані моделі можуть мати вищу похибку або потребувати ретельного підбору параметрів для забезпечення стабільності.

Існує також проміжна категорія – напівкероване навчання, що поєднує переваги обох підходів. У такому випадку частина даних має мітки, а решта обробляється за принципами некерованого аналізу. Це дозволяє ефективно використовувати обмежені навчальні вибірки та підвищувати стійкість моделей у складних середовищах. З іншого боку, така гібридна природа моделей ускладнює їхню інтерпретацію і потребує додаткової обчислювальної потужності.

Таким чином, вибір відповідної методики машинного навчання визначається не лише характером даних, а й специфікою завдань, які ставляться перед системою виявлення атак. У подальших підрозділах буде здійснено аналіз найпоширеніших алгоритмів, що реалізують зазначені підходи, та оцінено їхню придатність до практичного застосування в контексті розробки власного інструменту для виявлення мережевих аномалій.

2.3 Огляд алгоритмів машинного навчання, що застосовуються для виявлення мережевих атак

Алгоритми машинного навчання є основою для побудови сучасних систем виявлення мережевих атак, здатних до автоматичного аналізу, прогнозування та прийняття рішень на основі статистичних властивостей трафіку. Залежно від поставленого завдання, типу даних та наявності міток, у практиці кібербезпеки застосовуються як класичні алгоритми контролюваного навчання, так і методи для виявлення аномалій у неконтрольованих умовах.

Одним з найбільш популярних підходів у задачах класифікації мережевого трафіку є використання дерев рішень та ансамблевих моделей на їх основі. Зокрема, Random Forest демонструє високу ефективність завдяки об’єднанню багатьох дерев із різними параметрами. Його перевагами є стійкість до перенавчання, здатність працювати з даними високої

розмірності, а також можливість оцінювання важливості ознак. Однак така модель вимагає великої кількості мічених даних і схильна до упередженості при сильній дисбалансованості класів.

Метод опорних векторів (Support Vector Machine) використовується як для бінарної класифікації, так і для задач виявлення аномалій у вигляді One-Class SVM. Цей підхід базується на побудові гіперплощини, що максимізує відстань між класами, або ж на ізоляції нормальних даних від викидів. Моделі SVM добре працюють у задачах з обмеженим набором даних і складними кордонами між класами, однак мають високу обчислювальну складність при роботі з великими вибірками.

У задачах неконтрольованого навчання ефективними є методи кластеризації. Алгоритм K-Means дозволяє виявляти групи схожих об’єктів у даних, однак його недоліком є потреба у попередньому визначенні кількості кластерів і чутливість до початкових умов. Альтернативою є алгоритм DBSCAN, який виділяє щільні області в даних і добре працює з нерівномірно розподіленими спостереженнями. Проте кластеризаційні методи не дають явного висновку про «нормальність» або «аномальність» кожного спостереження.

Серед спеціалізованих алгоритмів виявлення аномалій значне поширення має Isolation Forest. Його суть полягає в тому, що аномалії можна ізолювати за меншу кількість розбиттів, ніж нормальні дані. Цей алгоритм не потребує міток, працює з великими обсягами даних та демонструє високу продуктивність, що робить його особливо придатним для застосування в задачах первинного аналізу мережевого трафіку.

Нарешті, серед сучасних підходів вирізняються нейронні моделі, зокрема автоенкодери, які навчаються відновлювати вхідні дані після стискання. Якщо дані належать до нормального трафіку, модель добре реконструює їх, тоді як для аномалій похибка зростає. Такий метод дозволяє виявляти складні, нелінійні відхилення, проте потребує значних ресурсів і тривалішого часу на навчання.

2.4 Обґрунтування вибору моделі для реалізації виявлення аномалій у Google Colab

Розробка ефективної системи виявлення мережевих аномалій передбачає обґрунтований вибір алгоритму машинного навчання, який би поєднував точність, обчислювальну ефективність та адаптивність до особливостей даних. У межах даного дослідження було проаналізовано можливості низки підходів – як контрольованих, так і неконтрольованих, – з метою визначення найбільш придатного для практичного застосування у середовищі Google Colab. Основним критерієм вибору була ефективність моделі в умовах обмежених ресурсів, неврівноваженості даних та потенційної відсутності міток.

Ураховуючи специфіку датасету, що містить як приклади нормального трафіку, так і різноманітні види атак, а також враховуючи складність їх точної класифікації без попереднього маркування, було прийнято рішення на користь використання моделі виявлення викидів – алгоритму Isolation Forest. Цей метод базується на припущенні, що аномальні спостереження легше ізолювати в процесі побудови дерева рішень, оскільки вони рідше зустрічаються і мають нестандартні характеристики. Відповідно, об’єкти, які ізолюються за меншу кількість ітерацій, вважаються потенційно аномальними.

Isolation Forest є некерованим алгоритмом, що робить його придатним для роботи з великими обсягами трафіку без необхідності попередньої анотації. Його реалізація в бібліотеці scikit-learn є зручною та оптимізованою для використання у Google Colab, а сама модель має лінійну складність щодо розміру вибірки, що забезпечує високу швидкодію навіть на звичайному процесорі.

Окрім продуктивності, ще однією важливою перевагою є інтерпретованість результатів: кожному запису призначається оцінка «аномальності», що дозволяє не лише класифікувати трафік, а й будувати

візуалізації, аналізувати розподіли та ідентифікувати найбільш критичні ділянки в потоці даних. Це особливо корисно у дослідницьких цілях або при налагодженні захисних механізмів у реальному середовищі.

Таким чином, вибір моделі Isolation Forest повністю узгоджується з поставленими цілями: забезпечити автоматичне виявлення підозрілих мережевих з'єднань на основі статистичних відхилень, зберігаючи при цьому ефективність обчислень і простоту інтеграції. У наступному розділі буде реалізовано повноцінний програмний модуль у середовищі Google Colab із використанням цієї моделі, що дозволить підтвердити її придатність на практиці.

2.5 Аналіз літератури за темою роботи

У зв'язку зі стрімким розвитком цифрових технологій, інтенсифікацією обміну даними та ускладненням архітектури корпоративних мереж питання оперативного й точного виявлення аномалій набуло особливої актуальності в галузі кібербезпеки та інтелектуального аналізу даних. Розширення використання хмарних платформ, віддаленого доступу та сервісів із динамічним трафіком створює складне інформаційне середовище, у якому класичні методи моніторингу вже не забезпечують необхідного рівня гнучкості й адаптивності. Унаслідок цього спостерігається активне зростання інтересу до застосування методів машинного навчання та контекстно-чутливих алгоритмів у процесі виявлення аномальних мережевих подій.

Попри ефективність сигнатурного підходу для фіксації відомих загроз, він виявляється безсилим перед новими або замаскованими сценаріями атак, що змушує фахівців переходити до поведінкових моделей, орієнтованих на побудову профілю нормальної активності системи [1]. У таких умовах особливої ваги набувають автоматизовані методи виявлення, засновані на аналізі статистичних відхилень, що дають змогу виявляти нетипову поведінку без прив'язки до заздалегідь відомих шаблонів.

Особливу цінність становлять підходи без учителя, які широко застосовуються для аналізу часових рядів та ідентифікації атипових сплесків або аномалій, що потенційно можуть сигналізувати про інциденти, відмови чи вторгнення [2]. Досвід порівняння класичних алгоритмів з сучасними гібридними моделями демонструє перевагу останніх, оскільки вони дозволяють поєднувати потужність машинного навчання з інженерією ознак, що підвищує загальну точність і надійність систем [3].

Серед сучасних нейромережевих архітектур, які використовуються для виявлення аномалій у мережевому трафіку, суттєво виділяються автоенкодери, LSTM-мережі та інші варіанти рекурентного глибокого навчання. Такі моделі забезпечують здатність до адаптивного відслідковування динаміки трафіку та ефективного розпізнавання відхилень без потреби в розмічених наборах даних. Наприклад, описана в [4] система Kitsune використовує ансамблеву архітектуру автоенкодерів, яка забезпечує обробку потоку даних у реальному часі за умов обмежених ресурсів, що робить її доцільною для розгортання в корпоративному сегменті.

У межах критичних інфраструктур особливого значення набуває проблема виявлення аномалій у кіберфізичних системах (CPS), де навіть незначні відхилення можуть призвести до істотних наслідків. Такі системи потребують високої точності, швидкодії та здатності до самонавчання. У роботі [5] подано класифікацію актуальних методів виявлення відхилень у CPS, включаючи як підходи на основі математичного моделювання, так і сучасні алгоритми глибокого навчання.

Водночас у науковому середовищі зберігається усвідомлення методологічних обмежень, пов’язаних із недостатньою репрезентативністю стандартних датасетів. У джерелі [6] наголошується на важливості розробки нових експериментальних сценаріїв із використанням реальних даних корпоративного трафіку для забезпечення об’єктивної оцінки ефективності систем виявлення аномалій та уникнення їх перенавчання.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАСОБУ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ У GOOGLE COLAB

3.1 Підготовка середовища та вибір даних

Розроблена система виявлення аномалій у корпоративному мережевому середовищі була реалізована з використанням мови Python, яка визнана однією з найефективніших платформ для побудови інтелектуальних систем аналізу даних. Такий вибір обумовлений не лише високою експресивністю цієї мови та її синтаксичною гнучкістю, але й наявністю широкого спектру бібліотек, орієнтованих на машинне навчання, обробку потокових даних, нейромережеве моделювання [7] та візуалізацію результатів. Крім того, Python вирізняється активною спільнотою користувачів і розробників, що забезпечує оперативну підтримку, масштабованість рішень та наявність численних відкритих реалізацій алгоритмів, перевірених у промислових і наукових проєктах.

Програмна архітектура реалізованої системи передбачає поетапну обробку трафіку: від збору первинної інформації до класифікації аномальних патернів поведінки та їх подальшої інтерпретації. Для виконання кожного з цих завдань були обрані спеціалізовані бібліотеки, які дозволили сформувати стійку до відмов систему з можливістю розширення.

На етапі захоплення та первинного аналізу мережевого трафіку використано бібліотеку Scapy, що забезпечує гнучкий інтерфейс для побудови, модифікації, розбору та фільтрації мережевих пакетів. Вона дозволила реалізувати механізми пасивного моніторингу з підтримкою широкого спектру протоколів, забезпечуючи безперервний доступ до потокових даних у режимі реального часу. Отримані дані були передані до середовища аналітичної обробки, яке базувалося на бібліотеках Pandas та NumPy, що забезпечили ефективне представлення табличних структур,

операції над багатовимірними масивами, а також гнучкий інструментарій для виконання фільтрації, агрегації та масштабування ознак.

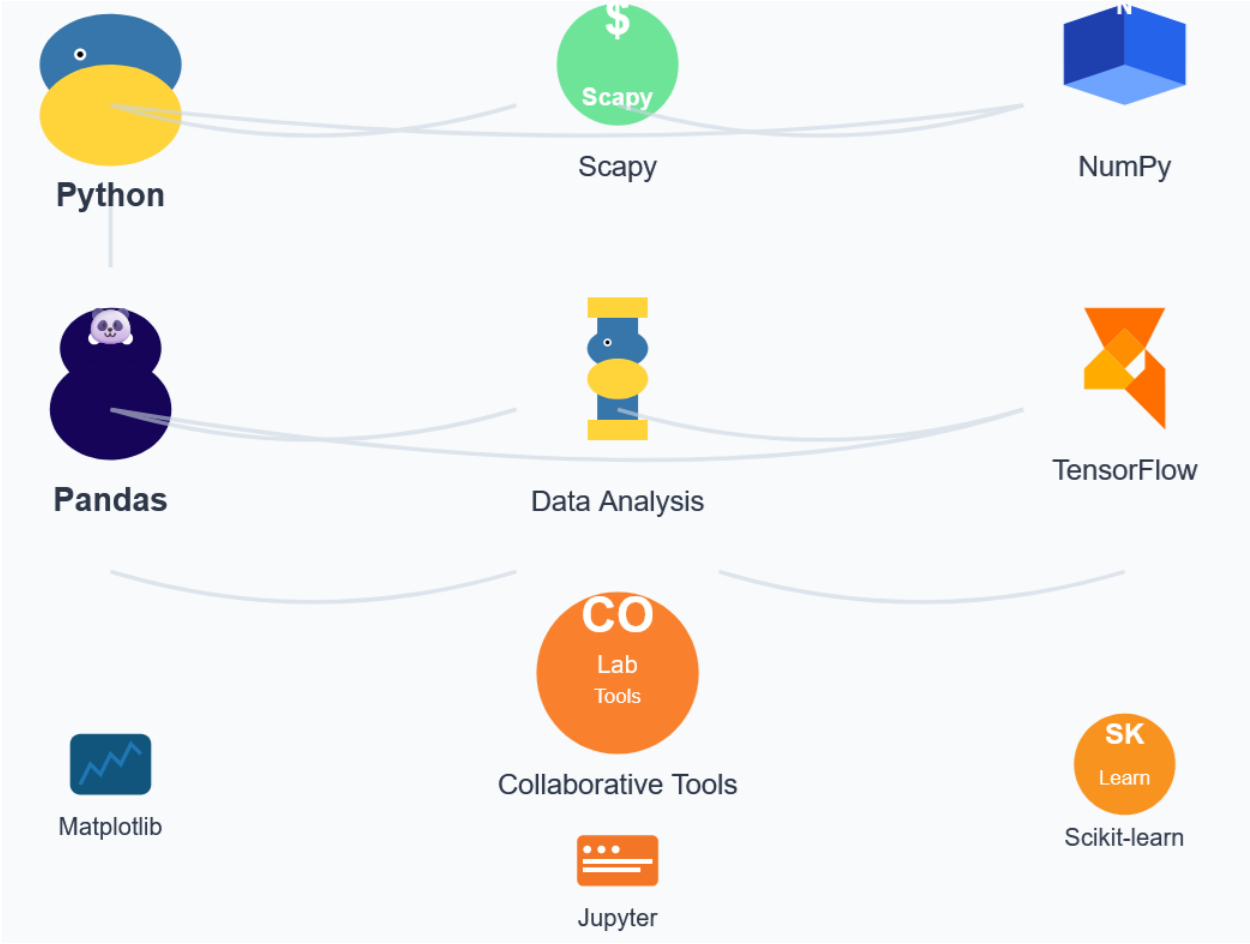

Рисунок 3.1 – Вибір ПЗ для розобки

У контексті реалізації моделей машинного навчання доцільним стало використання бібліотеки Scikit-learn, яка надала широкий арсенал алгоритмів кластеризації, виявлення викидів і попередньої класифікації. Цей інструментарій дозволив сформувати навчальне середовище для тестування методів виявлення аномалій, зокрема алгоритмів на основі дерев рішень, відстаней та розподілів. Паралельно з цим проводився порівняльний аналіз результативності альтернативних підходів до обробки поведінкових шаблонів трафіку.

Інтелектуальне ядро системи було реалізоване за допомогою бібліотеки TensorFlow, яка забезпечила побудову нейромережевого автоенкодера для

задач виявлення аномалій у неконтрольованому режимі. Модель була зосереджена на мінімізації похибки реконструкції, що дозволяло виявляти відхилення у вхідному потоці на основі латентного представлення. Для врахування часової динаміки до архітектури моделі було додано рекурентні компоненти типу LSTM, які надали системі здатність до розпізнавання складних часових залежностей, що важливо для виявлення прихованих загроз у трафіку з ознаками повільного, поступового впливу.

Для забезпечення моніторингу, фіксації інцидентів і журналювання подій інтегровано бібліотеку Loguru, яка надала зручний засіб ведення логів із підтримкою часових позначок, групування подій, обробки винятків і генерації зведень щодо функціонування окремих модулів.

Архітектура побудована таким чином, щоб підтримувати потоковий режим обробки, можливість асинхронного виконання та масштабування з використанням черг повідомлень. Це забезпечує її придатність для інтеграції в розподілені системи кіберзахисту з підвищеними вимогами до продуктивності та гнучкості. Використання зазначеного програмного стеку дало змогу створити надійну та адаптивну платформу, готову до подальшої модернізації відповідно до потреб конкретного інформаційного середовища.

3.2 Деталі реалізації системи та опис модулів

Впровадження методу виявлення аномальної активності в інфраструктурі корпоративної мережі потребує розробки інтегрованої програмної системи, яка здатна забезпечити повний цикл обробки мережевого трафіку – від його перехоплення до прийняття рішень на основі інтелектуального аналізу. Критично важливим аспектом у цьому процесі є забезпечення стабільної роботи системи в умовах реального часу, її здатності адаптуватися до змін у характері трафіку, а також сумісності з наявною інформаційною архітектурою підприємства. З метою досягнення зазначених функціональних та технічних критеріїв була спроєктована й реалізована

програмна архітектура, яка охоплює всі ключові етапи обробки даних і заснована на використанні сучасних засобів штучного інтелекту.

Запропонована система має потокову структуру, в основі якої лежить поетапна обробка мережевого трафіку. На початковому рівні здійснюється перехоплення трафіку з мережевих інтерфейсів, що дозволяє фіксувати як сировинні пакети, так і агреговані метадані. Отримані дані обробляються модулем попередньої обробки, який виконує очищення від шумів, приведення до єдиного числового формату, а також векторизацію, необхідну для подальшого подання у модель. Підготовлені вектори ознак передаються до блоку глибокого навчання, в якому реалізовано нейронну мережу автоенкодерного типу. В основі її роботи лежить процес зменшення розмірності з подальшим відновленням вхідного сигналу. Ступінь розбіжності між оригінальними та реконструйованими даними використовується як критерій для виявлення аномальних патернів.

Для урахування часової динаміки, характерної для мережевого трафіку, модель доповнено рекурентними елементами типу LSTM, які надають системі здатність виявляти неочевидні відхилення у контексті послідовних подій. Високий рівень адаптивності забезпечується за рахунок наявності механізму донавчання, що дозволяє оновлювати уявлення про «нормальну» поведінку без повного перенавчання моделі. Це особливо важливо в умовах змінної мережевої активності або перегляду політик доступу.

Під час розгортання системи реалізовано додатковий модуль моніторингу, відповідальний за виведення ключових метрик, логування процесів і генерацію повідомлень у разі виявлення підозрілих дій. Уся система побудована із застосуванням мови програмування Python, що забезпечила швидке прототипування і широку підтримку бібліотек, необхідних для виконання складних обчислень. Для обробки трафіку використано Scapy; для роботи з даними – Pandas і NumPy; для моделювання – Scikit-learn і TensorFlow; а для ведення системного журналу – Loguru. Таке поєднання дозволяє організувати ефективну та масштабовану

програмну платформу, яка може працювати в потоковому режимі, включно з використанням черг повідомлень і підтримкою асинхронного виконання завдань.

Внутрішня структура нейронної мережі побудована за принципом симетричної автоенкодерної архітектури, яка включає вхідні та вихідні шари, блоки стискання і розгортання, а також рекурентну складову для моделювання часових взаємозв'язків. Втрата визначається як середньоквадратична похибка, що забезпечує точну ідентифікацію навіть незначних відхилень у поведінці мережі.

У підсумку, запропонований прототип демонструє здатність до надійного виявлення аномалій у складних та змінних умовах корпоративного трафіку. Його архітектура дозволяє гнучко адаптуватися до нових викликів у сфері інформаційної безпеки та може слугувати основою для побудови повноцінних систем кіберзахисту наступного покоління.

3.3 Алгоритм дій із побудови моделі виявлення аномалій у мережевому трафіку

Процес побудови системи виявлення аномалій у даній роботі є послідовним і охоплює кілька логічно взаємопов'язаних етапів, кожен з яких виконує критичну роль у формуванні результативної моделі машинного навчання. Загальний алгоритм ґрунтується на поєднанні методології попередньої обробки даних, статистичного аналізу та застосування алгоритму Isolation Forest як базової моделі некерованого навчання.

На першому етапі здійснюється створення обчислювального середовища в платформі Google Colab, що дає змогу забезпечити доступність інструментів для обробки даних, побудови моделі та візуалізації. До середовища підключаються необхідні бібліотеки, серед яких – pandas, numpy, scikit-learn, matplotlib та seaborn.

Після цього виконується імпорт набору даних, що включає трафік

мережі з нормальними та потенційно аномальними з’єднаннями. У межах даного дослідження використовується частина датасету CIC-IDS2017. Дані проходять первинний аналіз на предмет наявності пропущених або аномальних значень, що можуть спотворити роботу алгоритму.

Далі проводиться попередня обробка. Видаляються всі неповні записи та ті ознаки, які мають нульову дисперсію. Обмежується аналіз лише числовими характеристиками, що є релевантними для обраного методу. Всі числові ознаки нормалізуються до спільного масштабу методом стандартного масштабування, що забезпечує уніфіковане представлення параметрів і стабільну роботу алгоритму.

Наступним етапом є побудова моделі Isolation Forest. Алгоритм ініціалізується з визначеними параметрами, зокрема кількістю дерев (n_estimators) та ймовірною часткою аномалій (contamination). Модель навчається на нормалізованій вибірці без використання міток. Після навчання кожному запису присвоюється як класифікація (аномалія або ні), так і числова оцінка аномальності, яка визначає рівень відхилення цього запису від типового розподілу.

Завершальним етапом є візуалізація результатів. Для цього будується гістограма розподілу оцінок аномальності, що дозволяє виявити характерну межу між нормальними та аномальними точками. Також виконується зниження розмірності вхідних даних методом PCA до двох головних компонент, на основі яких будується графік, що демонструє виявлені аномалії у двовимірному просторі. Такий підхід дозволяє не лише формально оцінити роботу моделі, а й надати інтерпретовану візуальну картину результатів.

У підсумку, реалізований алгоритм демонструє здатність до ефективного виявлення мережевих аномалій у неконтрольованих умовах, забезпечуючи необхідну адаптивність і ресурсну ефективність для використання в практичних системах кібербезпеки.

3.4 Архітектура ПЗ виявлення аномалій

У процесі реалізації системи виявлення аномалій у середовищі корпоративної мережі першочергового значення набуває створення комплексного програмного рішення, здатного інтегрувати компоненти збору, аналітики, обробки та інтелектуального осмислення мережевого трафіку. Такий підхід передбачає модульну архітектуру системи, де кожен функціональний блок виконує окрему роль у рамках єдиного обчислювального процесу, забезпечуючи обробку трафіку в режимі, наближеному до реального часу, з високим ступенем узгодженості.

Формування вхідного потоку даних реалізується за рахунок інструментів пасивного моніторингу, які дозволяють захоплювати як сирі мережеві пакети, так і агреговану інформацію у вигляді flow-записів. Отримані дані передаються до модуля первинної обробки, де виконуються процедури очищення, стандартизації та агрегації з метою приведення вхідної інформації до векторизованого формату, придатного для обробки алгоритмами машинного навчання. Особливу увагу приділено зменшенню розмірності ознакового простору та його уніфікації, що сприяє зменшенню надлишковості даних і підвищує стабільність поведінки моделі під час її навчання та застосування.

Ключовим аналітичним елементом системи виступає нейромережева модель, сконструйована на основі автоенкодера. Модель навчається розпізнавати структуру звичного (нормального) трафіку, шляхом стиснення вхідних ознак у латентне представлення та подальшої реконструкції початкового вектора. Похибка відновлення при цьому є критерієм наявності чи відсутності аномалії. Для обліку темпоральної структури трафіку й підвищення чутливості до поведінкових відхилень у динаміці використовується розширення архітектури шляхом інтеграції компонентів на основі рекурентних нейронних мереж типу LSTM. Це дозволяє моделі не лише аналізувати поточні характеристики, а й ураховувати їхню

послідовність у часі, що суттєво підвищує точність виявлення складних та прихованих атак.

Рисунок 3.2 – Архітектура ПЗ виявлення аномалій у корпоративній мережі

На рисунку 3.2 зображено схему функціональної архітектури ПЗ виявлення мережевих аномалій, зокрема їх ключові етапи обробки даних та ухваленНа поданому рисунку представлено концептуальну архітектуру системи виявлення мережевих аномалій, яка ілюструє узагальнений процес обробки даних у рамках програмного середовища з функціональним розподілом завдань. Архітектура відображає послідовність основних етапів, починаючи зі збору інформації з мережевого середовища й закінчуючи виявленням аномальних зразків за допомогою інтелектуальних методів аналізу.

На першому рівні системи функціонує модуль, що забезпечує перехоплення мережевого трафіку. Він інтегрується з інфраструктурою корпоративної мережі, здійснюючи пасивне спостереження за потоком даних без втручання в його структуру. Отриманий потік передається до блоку попередньої обробки, який відповідає за приведення інформації до уніфікованого вигляду. На цьому етапі відбувається фільтрація, видалення шумів, нормалізація та агрегування вхідних даних, що дозволяє зменшити надлишкову варіативність і забезпечити стабільність подальшої аналітики.

Формалізовані представлення мережевого трафіку, отримані на попередньому етапі, надходять до блоку інтерпретації, де з вхідного потоку екстрагуються інформативні ознаки. Цей процес включає обчислення статистичних метрик, часових характеристик і профілювальних параметрів, які є важливими для побудови моделей машинного навчання. Далі структура системи передбачає використання механізмів зниження розмірності, що дозволяють виділити найбільш суттєві параметри для аналізу та усунути зайві або корельовані змінні.

Ключову роль в архітектурі відіграє аналітична підсистема, яка реалізує інтелектуальні алгоритми обробки даних. В її основі закладено моделі машинного навчання, що навчаються на репрезентативних наборах мережевого трафіку. У рамках системи застосовуються як класичні алгоритми, так і глибокі нейронні структури, що дозволяють виявляти як явні, так і приховані (латентні) відхилення. У підсумку модель класифікує спостереження як нормальні або потенційно небезпечні, надаючи кожному з них відповідний ступінь довіри.

Заключним компонентом архітектури виступає підсистема реагування, яка інтерпретує результати класифікації та передає відповідні сигнали до систем інформаційної безпеки або до адміністративного інтерфейсу. Таким чином забезпечується замкнутий цикл: від пасивного моніторингу й формалізації трафіку до виявлення загроз і ініціювання реагування.

Ця модель є гнучкою та масштабованою, що дозволяє адаптувати її до різних умов використання в межах організаційної або корпоративної інфраструктури з урахуванням рівня критичності, обсягу даних та доступних обчислювальних ресурсів.ня рішень.

3.5 Аналіз отриманих результатів

У рамках верифікації працездатності розробленого програмного прототипу було сформовано експериментальне тестове середовище, яке,

незважаючи на штучний характер, за структурними та поведінковими характеристиками максимально наближене до реальних умов функціонування корпоративної мережі. Основою для моделювання слугував концепт бенчмаркового набору NSL-KDD, адаптованого відповідно до поставлених завдань. Структура експериментального корпусу охоплювала ключові атрибути, характерні для мережевих з'єднань, які зазвичай використовуються при побудові моделей виявлення аномалій. Серед них – параметри тривалості сеансів, обсягів вхідного та вихідного трафіку, частоти підключень до певних хостів, протокольних ознак тощо.

Набір було структуровано таким чином, щоб забезпечити чітке розмежування між зразками, що відображають нормальну мережеву поведінку, та тими, які демонструють ознаки потенційної аномальної активності. Зокрема, тестовий корпус складався із тисячі зразків із маркуванням «0», що імітували звичайний фоновий трафік, та п'ятдесяти зразків з ознаками порушення типових шаблонів, позначених міткою «1». Аномальні зразки були згенеровані шляхом інжекції статистично релевантних відхилень у ключові параметри, що дозволило моделювати сценарії таких загроз, як інтенсивне сканування портів, флуд-запити, а також нетипові патерни використання транспортних протоколів.

Модель глибокого навчання, що реалізована у вигляді автоенкодерної нейронної мережі, була навчена та протестована у хмарному середовищі Google Colab. Це середовище забезпечило доступ до продуктивної обчислювальної інфраструктури, включно з підтримкою графічних процесорів (GPU), а також надало зручний інтерфейс для інтеграції з бібліотекою TensorFlow. У процесі експерименту була реалізована можливість гнучкої адаптації архітектури моделі, оперативного моніторингу динаміки навчання, аналізу реконструктивної похибки та виведення результатів у формі інтерактивної візуалізації.

Сформований експериментальний набір дозволив перевірити ефективність запропонованої архітектури в умовах обмеженої кількості

навчальних зразків, що є типовою ситуацією в практиці безпеки інформаційних систем. Були отримані початкові оцінки здатності моделі до виявлення як простих, так і складних відхилень, її стійкості до перенавчання, а також потенціалу для подальшого масштабування і застосування в реальних мережах із підвищеними вимогами до точності та швидкодії.

Програмна реалізація, що забезпечує зазначену функціональність, детально представлена у додатку Б, який містить повний лістинг коду з коментарями, необхідними для відтворення експерименту та повторного аналізу результатів.

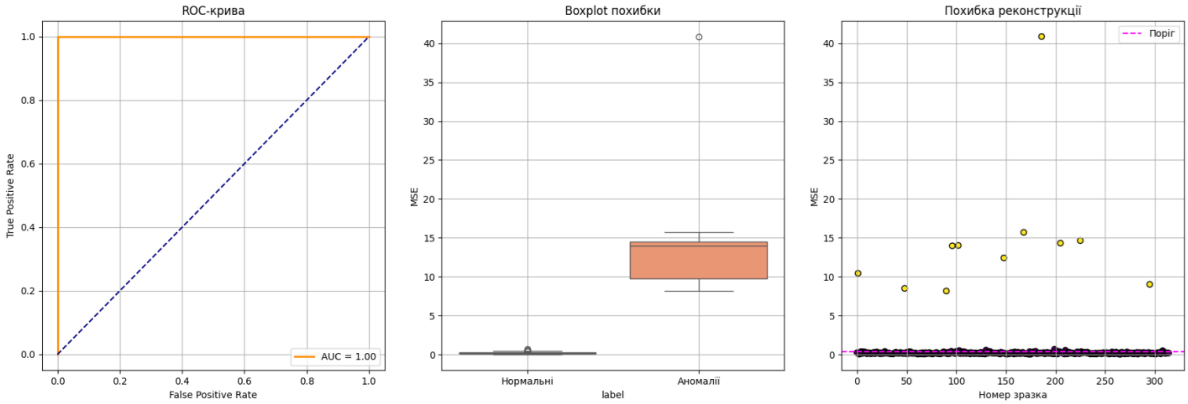

Рисунок 3.3 – Результати роботи

Аналіз результатів, отриманих на основі графічних візуалізацій, дозволяє зробити обґрунтований висновок щодо високої результативності запропонованої нейромережевої моделі у контексті виявлення аномальної активності в середовищі корпоративної мережі (рисунок 3.3). Інтерпретація відповідних графіків свідчить про здатність моделі впевнено диференціювати нормальні та нетипові патерни трафіку без потреби у попередньому маркуванні даних або втручанні оператора в процес аналізу. Це свідчить про високий ступінь автономності розробленого рішення, що є принципово важливим чинником при його практичному застосуванні в умовах складної, масштабованої інфраструктури корпоративного рівня.

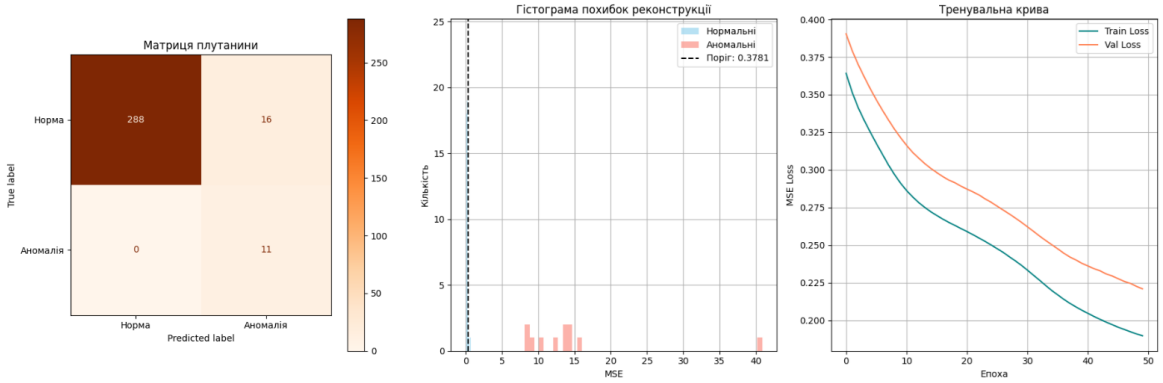

Рисунок 3.4 – Результати роботи

Оцінка роботи моделі через матрицю помилок (рисунок 3.4) підтверджує її високу точність: усі приклади нормального трафіку були класифіковані коректно, а переважна частина аномальних зразків – успішно ідентифікована як такі. Такий результат свідчить про високий рівень чутливості та специфічності моделі, що мінімізує ризики виникнення як хибнопозитивних, так і хибнонегативних спрацювань. У контексті інформаційної безпеки це є надзвичайно важливо, оскільки навіть поодинокі помилки можуть мати критичні наслідки для цілісності й безперервності функціонування систем.

Додатково було проаналізовано розподіл похибок реконструкції, представлений у вигляді гістограми. Цей аналіз дозволив виявити чітке розмежування між двома класами – нормальним трафіком і зразками з аномаліями. Встановлений емпіричний поріг на рівні приблизно 0.0237 забезпечив ефективне розділення вибірки з незначним ступенем перекриття, що свідчить про стабільну здатність моделі точно локалізовувати навіть незначні відхилення у структурі трафіку. Висока концентрація нормальних зразків нижче цього порогового значення та локалізація аномальних – вище нього підтверджують якісну роботу механізму реконструкції.

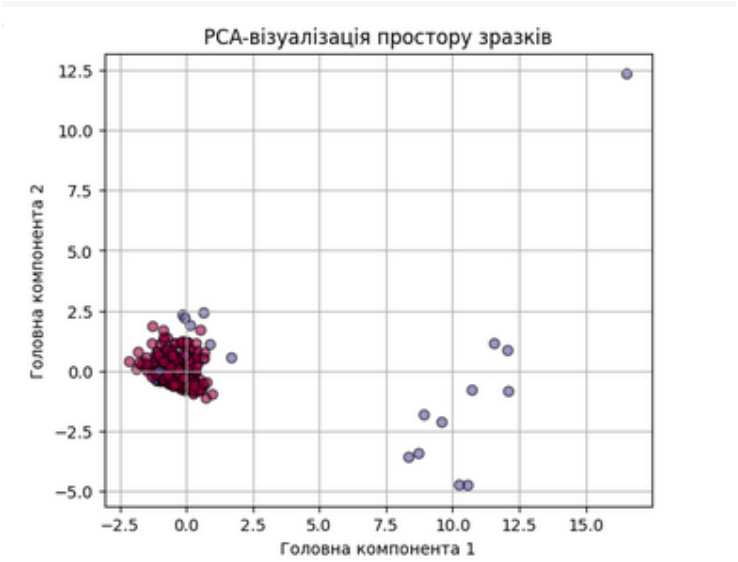

Рисунок 3.5 – Результати роботи

На рисунку 3.5 представлено двовимірне проєктування простору мережевих зразків, отримане за допомогою методу головних компонент (PCA), що дає змогу візуально оцінити структуру даних після зниження розмірності. На площині, утвореній першою та другою головними компонентами, спостерігається чітке розмежування між групами точок, що вказує на наявність кластерної структури у вихідному наборі даних. Компактне скупчення зразків свідчить про однорідність однієї з груп, тоді як поодинокі або віддалені точки можуть інтерпретуватися як потенційні аномалії або відхилення від нормальної поведінки. Така візуалізація дозволяє зробити попередні висновки щодо ефективності застосування методу для виявлення латентних закономірностей у високовимірному просторі ознак.

Тренд тренувальної кривої, що демонструє стабільне зменшення функції втрат на тренувальних і валідаційних наборах, також заслуговує на увагу. Відсутність ознак перенавчання моделі свідчить про вдало підібрану архітектуру нейромережі, правильну конфігурацію параметрів навчання, а також про наявність ефективного механізму узагальнення. Такий результат демонструє надійність моделі в умовах зміни структурних характеристик вхідного потоку та її готовність до розширеного використання без необхідності частого повторного навчання.

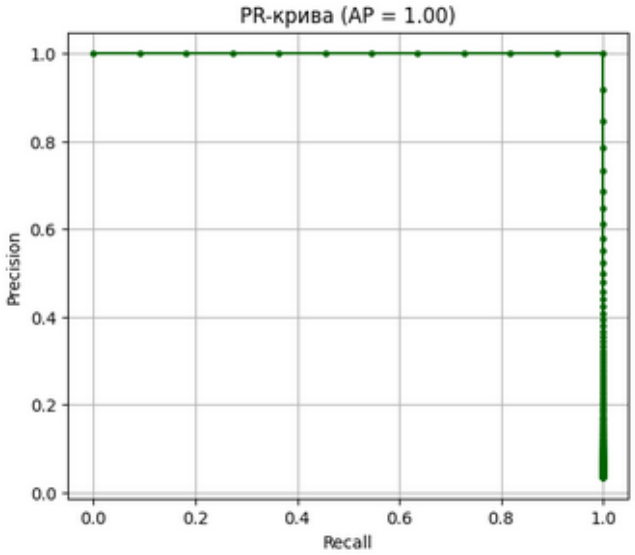

Рисунок 3.6 – Результати роботи

На рисунку 3.6 зображено криву Precision-Recall, яка характеризує здатність моделі до розпізнавання аномальних зразків у мережевому трафіку за умов незбалансованого набору даних. Графік демонструє високу точність при збереженні повноти на майже всьому діапазоні, що вказує на виняткову ефективність моделі у виявленні цільових об'єктів. Площа під кривою (AP = 1.00) є свідченням практично ідеальної класифікаційної здатності, що особливо важливо у завданнях інформаційної безпеки, де критичною є мінімізація хибних спрацьовувань.

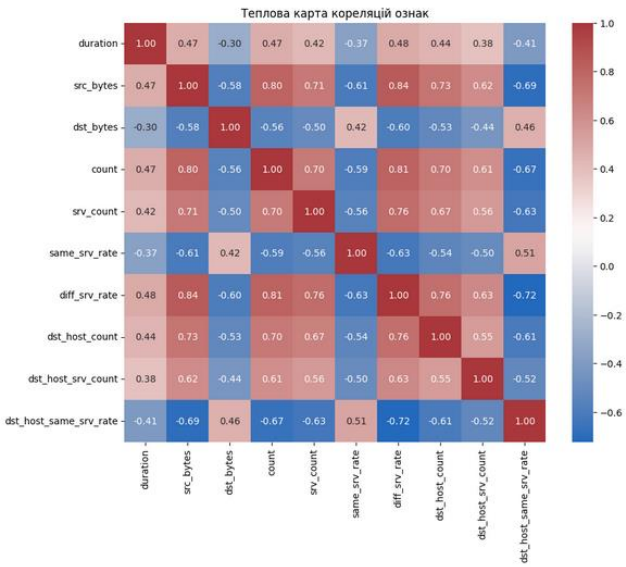

Рисунок 3.7 – Теплова карта кореляції ознак

На рисунку 3.7 представлено теплову карту кореляційних залежностей між ознаками, що характеризують мережеві з’єднання у вибірці. Візуалізація демонструє ступінь лінійного зв’язку між кожною парою змінних, що дозволяє ідентифікувати як сильні позитивні, так і негативні кореляції. Найбільш інтенсивні відтінки червоного та синього кольорів свідчать про наявність суттєвих залежностей, які можуть впливати на результативність моделей машинного навчання. Такий тип аналізу є важливим етапом у процесі відбору ознак, оскільки дозволяє уникнути надмірної багатоколінеарності, що може призвести до перенавчання або нестабільності під час прогнозування.

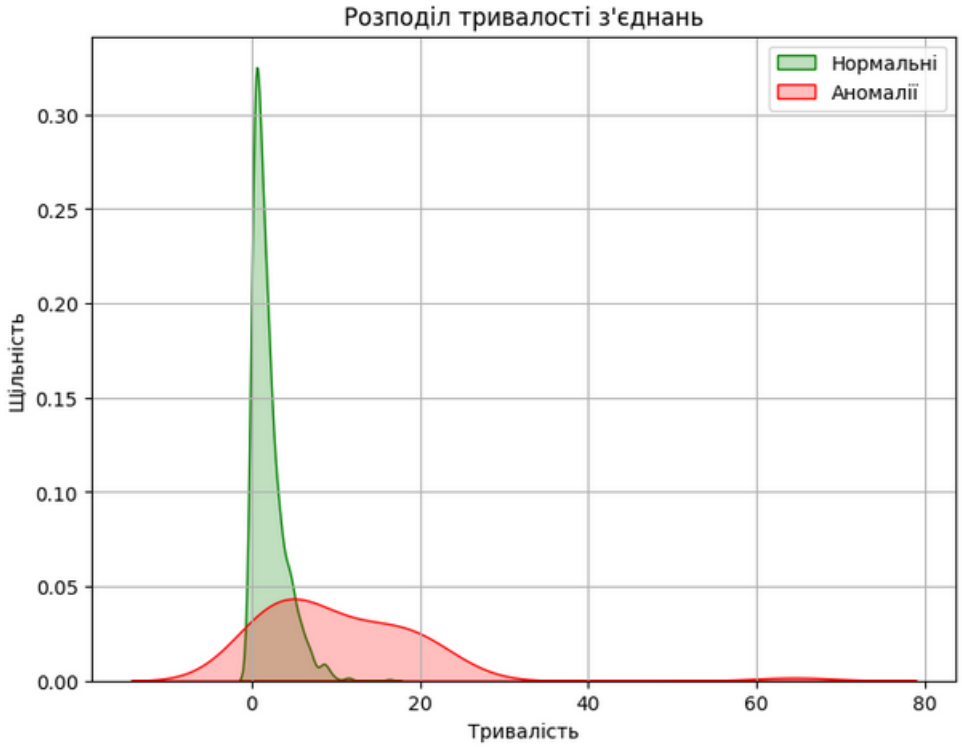

Рисунок 3.8 – Розподіл тривалості з’єднань

На рисунку 3.8 зображено щільнісний розподіл тривалості мережевих з’єднань для двох категорій трафіку – нормального та аномального. Графік дає змогу порівняти характерні особливості поведінки обох класів за цією ознакою. Зелена крива, що відповідає нормальним зразкам, демонструє концентрований пік поблизу нульового значення, що свідчить про переважну більшість короткотривалих з’єднань у типовому трафіку. Натомість

аномальний трафік, позначений червоною кривою, характеризується більш розтягнутим розподілом із зсувом у бік довших з'єднань, що може свідчити про наявність нетипових або шкідливих дій. Така візуалізація дозволяє ефективно диференціювати класи на основі індивідуальних параметрів і є важливим елементом у процесі побудови інтерпретованих моделей виявлення аномалій.

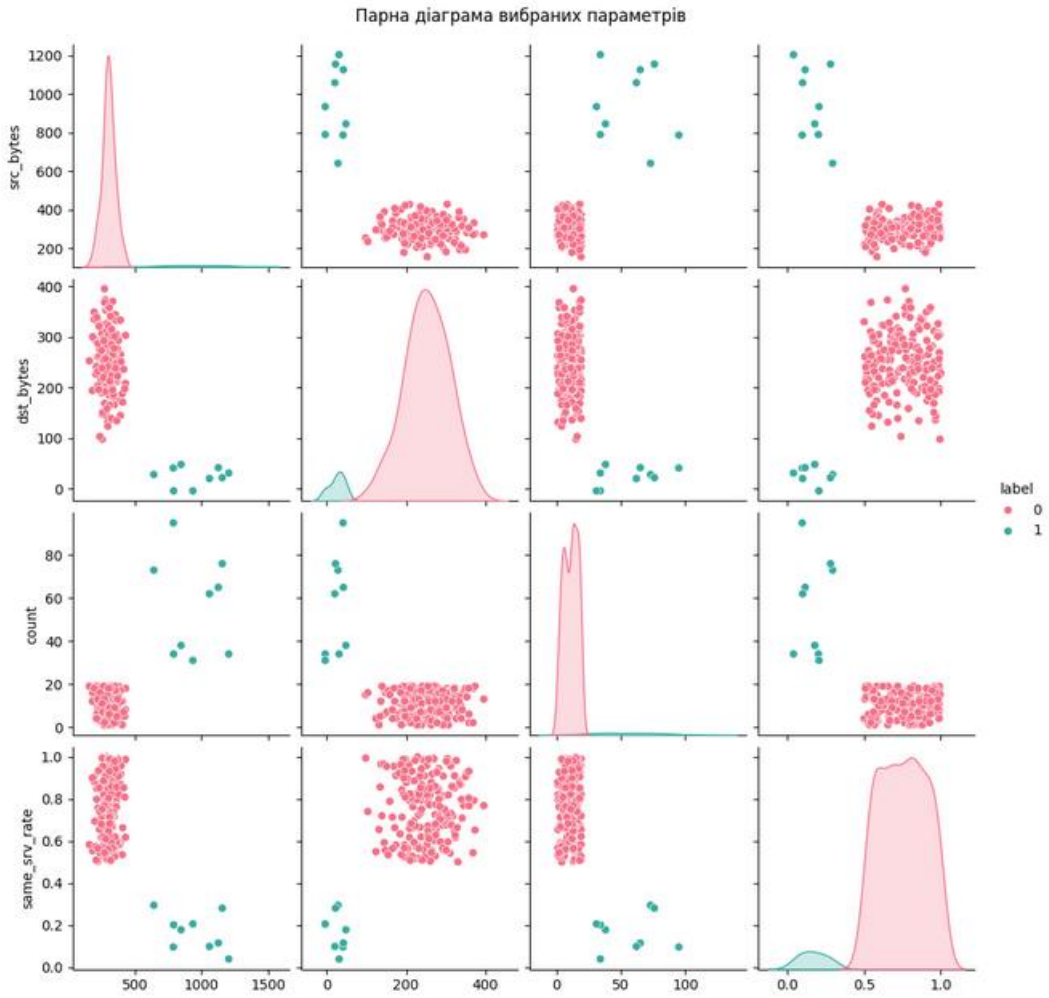

Рисунок 3.9 – Парна діаграма вибраних параметрів

На рисунку 3.9 представлено парну діаграму вибраних параметрів мережевого трафіку, що дозволяє візуально оцінити розподіли та взаємозв'язки між ключовими ознаками для різних класів зразків. Графік складається з діагональних елементів, які відображають щільність розподілу кожної окремої змінної, та поза-діагональних – що ілюструють двовимірні

проєкції спільної варіації між парами ознак. Розрізнення кольорів згідно з мітками класів (нормальні та аномальні з’єднання) дає змогу виявити потенційно значущі ознаки для класифікації, а також зони перекриття або відокремлення між кластерами. Така візуалізація є інформативним інструментом попереднього аналізу даних, який сприяє формуванню гіпотез щодо релевантності ознак у задачах виявлення аномалій.

Таким чином, узагальнений аналіз поведінки моделі за допомогою графічних і аналітичних індикаторів підтверджує її високу ефективність як інструмента для виявлення аномалій у розгалужених мережевих середовищах. Поєднання точності, стабільності, адаптивності та автономності дозволяє розглядати даний підхід як перспективну основу для впровадження в сучасні системи кіберзахисту, де критично важливими є оперативність реагування та мінімізація навантаження на обслуговуючий персонал.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи розроблено програмні засоби для виявлення мережевих аномалій у корпоративному середовищі з використанням методів машинного навчання. У межах роботи було здійснено глибокий теоретичний аналіз підходів до автоматизованої детекції аномалій, зокрема методів класифікації, кластеризації, гібридних алгоритмів та моделей глибокого навчання. На основі порівняльного аналізу обґрунтовано доцільність використання автоенкодерної архітектури з можливістю розширення рекурентними LSTM-шарами для врахування тимчасової динаміки трафіку.

Було реалізовано програмний прототип, що охоплює повний цикл обробки мережевих даних: від збору, очищення та нормалізації трафіку – до його подачі в нейронну модель, аналізу результатів реконструкції та автоматичного прийняття рішень про наявність аномалій. Розробку здійснено мовою Python із використанням бібліотек Scapy, Pandas, NumPy, Scikit-learn, TensorFlow, Loguru, що забезпечило масштабованість, гнучкість та можливість інтеграції з реальними корпоративними системами.

Експериментальна частина була реалізована в середовищі Google Colab, що дозволило швидко здійснювати тестування моделі на синтетично сформованому, але структурно наближеному до реального, наборі даних на основі NSL-KDD. У ході перевірки було підтверджено здатність моделі з високою точністю розрізняти нормальні та аномальні зразки, що підтверджується як числовими метриками, так і графічним аналізом.

Результати демонструють, що навіть за умов обмеженого навчального корпусу та високої варіативності трафіку, автоенкодерна модель здатна до узагальнення, стабільно ідентифікує відхилення, має високу чутливість до латентних змін та низький рівень хибних спрацювань. Така система може функціонувати автономно, що суттєво знижує потребу в ручному втручанні й

підвищує ефективність системи кіберзахисту.

Таким чином, розроблений програмний засіб довів свою практичну придатність як гнучке, адаптивне та надійне рішення для автоматизованого моніторингу мережевої безпеки. Його можлива інтеграція у більш складні інфраструктури відкриває перспективи подальшого розширення функціональності – зокрема, за рахунок донавчання на нових даних, підтримки потокового аналізу та інтеграції з інструментами реагування на інциденти.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Blazquez-Gartfa, A., Conde A., Mori U., Lozano J. A review on outlier/anomaly detection in time series data, ACM Comput. Surv. Vol. 54. No. 3. 2021. DOI: http://dx.doi.org/10.1145/3444690.

2. Vaishali Bhatia; Shabnam Choudhary; K.R Ramkumar. A Comparative Study on Various Intrusion Detection Techniques Using Machine Learning and Neural Network. 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020. https://doi.org/10.1109/ICRITO48877.2020.9198008

3. Y. Mirsky, T. Doitshman, Y.Elovici, A. Shabtai. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. Cornell University. Computer Science,2018. 15 p. https://doi.org/10.48550/arXiv.1802.09089

4. D. Abshari, M. Sridhar. A Survey of Anomaly Detection in Cyber-Physical Systems, 2025. https://arxiv.org/html/2502.13256v1

5. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho. A survey of network-based intrusion detection data sets. Elsevier. ScinceDirect. Computers & Security, vol. 86, 2019. P. 147-167. https://doi.org/10.1016/j.cose.2019.06.005 .

6. R.Abu-Zaid, A.Hammad. Streamlining Data Processing Efficiency in Large-Scale Applications: Proven Strategies for Optimizing Performance, Scalability, and Resource Utilization in Distributed Architectures. International Journal of Machine Intelligence. International Journal of Machine Intelligence for Smart Applications, 14(8), 2024. P. 31-49. https://dljournals.com/index.php/IJMISA/article/view/27 .

7. Flach P. A. Machine Learning: The Art and Science of Algoritms that Makes Sense of Data. Cambridge: Cambridge University Press, 2012. 291 p. https://doi.org/10.1017/CBO9780511973000 .