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 другий (магістерський)

Метод виявлення мережних аномалій з використанням машинного навчання

(тема)

Виконав:
здобувач 2 року навчання,
групи СПм-23-5
Єлізавета ГЛОБА
(власне ім'я, прізвище)

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

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

Освітня програма
Системне програмування
(повна назва освітньої програми)

Керівник: доц. Володимир ФЕДОРЧЕНКО
(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 другий (магістерський)

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

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

Освітня програма Системне програмування
(повна назва)

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

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Глобі Єлізаветі Юріївні
(прізвище, ім'я, по батькові)

1. Тема роботи Метод виявлення мережних аномалій з використанням машинного навчання

затверджена наказом по університету від "21" квітня 2025 р. № 296 Ст

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

3. Вхідні дані до роботи
моніторинг трафіку
мережні аномалії
машинне навчання
інформаційна безпека

4. Перелік питань, що потрібно опрацювати у роботі
Аналіз існуючих методів виявлення аномалій
Розробка удосконаленого методу виявлення аномалій
Реалізація програмного прототипу методу та аналіз результатів

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 14 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	21.04.2025–30.04.2025	
2	Огляд існуючих рішень та алгоритмів	01.05.2025–12.05.2025	
3	Розробка методу	13.05.2025–22.05.2025	
4	Вибір програмних засобів	23.05.2025–30.05.2025	
5	Програмна реалізація	31.05.2025–02.06.2025	
6	Аналіз отриманих результатів	03.06.2025–05.06.2025	
7	Оформлення записки	06.06.2025–12.06.2025	

Дата видачі завдання " 21 " квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ доцент Володимир ФЕДОРЧЕНКО
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 59 с., 7 рис., 2 дод., 8 джерел.

АНОМАЛІЯ, КІБЕРБЕЗПЕКА, НЕЙРОННА МЕРЕЖА, АВТОЕНКОДЕР, LSTM, МАШИННЕ НАВЧАННЯ, АНАЛІЗ ТРАФІКУ, ВИЯВЛЕННЯ ЗАГРОЗ, АДАПТИВНЕ МОДЕЛЮВАННЯ.

Метою кваліфікаційної роботи є розробка та реалізація ефективного методу виявлення аномалій у корпоративній мережі, який здатний функціонувати в умовах динамічних змін мережевого середовища та обмеженості апріорної інформації про загрози.

У ході кваліфікаційної роботи було проаналізовано сучасні підходи до виявлення аномалій, включаючи сигнатурні, статистичні, машинні та гібридні методи. Обґрунтовано доцільність застосування автоенкодерної нейромережі у поєднанні з LSTM-компонентами як основи для формування адаптивної моделі нормальної поведінки мережевого трафіку.

Запропонований метод реалізовано у вигляді програмного прототипу, який складається з модулів збору, попередньої обробки, аналізу, моніторингу та оновлення поведінкового профілю. Програмна реалізація здійснена мовою Python із використанням бібліотек TensorFlow, Scikit-learn, Pandas, Scapy та Loguru. Експериментальна перевірка продемонструвала високу точність, стабільність та здатність до узагальнення, що підтверджено візуалізацією результатів.

Отримані результати підтверджують перспективність використання гібридних нейромережевих моделей для виявлення аномалій у корпоративних мережах, де важливо забезпечити баланс між точністю, швидкістю реагування та стійкістю до нових форм загроз.

ABSTRACT

Master’s thesis: 59 pages, 7 figures, 2 appendices, 8 sources.

NETWORK TRAFFIC MONITORING, PROTOCOL ANALYSIS, PACKET ENTROPY, ANOMALY DETECTION, TRAFFIC VISUALIZATION, PCAP PROCESSING, NETWORK SECURITY, GOOGLE COLAB.

The major goal of this thesis is to develop and implement an effective anomaly detection method for corporate networks that can operate under conditions of dynamic changes in network environments and limit a priori knowledge of threats.

In order to a comprehensive analysis of modern approaches to anomaly detection was conducted, including signature-based, statistical, machine learning, and hybrid methods. The use of an autoencoder-based neural network combined with LSTM components was substantiated as a suitable foundation for constructing an adaptive model of normal network traffic behavior.

The proposed method was implemented as a software prototype composed of modules for data acquisition, preprocessing, analysis, monitoring, and behavioral profile updating. The software implementation was carried out in Python using libraries such as TensorFlow, Scikit-learn, Pandas, Scapy, and Loguru. Experimental validation demonstrated high accuracy, stability, and generalization ability, as confirmed through result visualizations.

The obtained results confirm the viability of employing hybrid neural network models for anomaly detection in corporate networks, where maintaining a balance between detection accuracy, response speed, and resilience to emerging threats is of critical importance.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AI – штучний інтелект

API – інтерфейс прикладного програмування

CPS – кіберфізична система

DDoS – розподілена атака на відмову в обслуговуванні

DoS – атака на відмову в обслуговуванні

IDS – система виявлення вторгнень

IP – інтернет-протокол

IPFIX –експорт інформації про потоки IP

KDD –виявлення знань у базах даних

LSTM – довга короткочасна пам’ять

ML – машинне навчання

NSL-KDD – набір даних для оцінки систем виявлення вторгнень, модифікований варіант KDD'99

PCA – метод головних компонент

ROC – крива робочих характеристик приймача

SIEM – система керування інформацією та подіями безпеки

TCP – протокол керування передачею

UDP – протокол користувацьких дейтаграм

ВСТУП

У сучасних умовах цифрової трансформації корпоративні мережі становлять основу функціонування інформаційної інфраструктури організацій незалежно від їхнього масштабу або галузі діяльності. Вони забезпечують сталу підтримку обміну інформацією, сприяють безперебійному функціонуванню операційних систем, підтримують внутрішню координацію структурних одиниць і формують основу для зовнішньої комунікації з діловими партнерами та споживачами. З огляду на стрімке зростання обсягів даних, що передаються та обробляються у таких мережах, а також з урахуванням ускладнення їхньої топології, суттєво посилюється загроза виникнення нестандартних ситуацій, які можуть вплинути на цілісність, доступність та захищеність цифрових активів.

Аномальні процеси в корпоративних мережах, як правило, пов’язані з нехарактерною поведінкою системних компонентів, користувачів або програмних агентів. Такі відхилення можуть сигналізувати як про потенційні вектори атак з боку зовнішніх або внутрішніх зловмисників, так і про приховані технічні несправності, недоліки конфігурацій або помилки в програмному забезпеченні. Особливість подібних порушень полягає в їхній слабкій детектованості стандартними засобами контролю, які зазвичай орієнтовані на фіксовані правила, шаблони чи сигнатури і, відповідно, не здатні своєчасно реагувати на нові, невідомі або складноструктуровані загрози, приховані у високонавантаженому інформаційному середовищі.

Наслідки несанкціонованих змін у мережевій поведінці можуть бути критичними для стабільності підприємства, адже вони здатні призвести до витоку конфіденційних даних, деградації бізнес-процесів, зниження ефективності роботи персоналу, а також до втрат репутаційного характеру, які важко компенсувати. У зв’язку з цим особливого значення набуває завдання оперативного та високоточного виявлення таких аномалій, що

дозволить забезпечити проактивне реагування на потенційні інциденти інформаційної безпеки.

Попри наявність широкого спектра інструментів для моніторингу мережевого трафіку, більшість наявних технологічних рішень демонструють низку обмежень, зокрема підвищену вразливість до хибних спрацювань, обмежену гнучкість у змінному середовищі, а також недостатню масштабованість при обробці потоків даних у реальному часі. Це вимагає переосмислення існуючих підходів до аналізу мережевого трафіку та розроблення нових методів, здатних ефективно вирішувати задачу виявлення аномалій у динамічних корпоративних мережах із високим рівнем навантаження та різноманітністю поведінкових моделей.

Метою кваліфікаційної роботи є розробка, реалізація та експериментальне обґрунтування удосконаленого методу виявлення аномалій у корпоративній мережі, що базується на гібридному нейромережевому підході та здатен забезпечити високу точність, швидкодію й адаптивність в умовах динамічного мережевого середовища.

Досягнення поставленої мети передбачає аналіз існуючих методів, розробку ефективного алгоритму з урахуванням особливостей корпоративного трафіку, створення програмного прототипу системи та проведення експериментальних досліджень для оцінки її результативності порівняно з традиційними рішеннями..

Завдання:

- проаналізувати сучасні методи виявлення аномалій, включаючи статистичні, сигнатурні, евристичні та алгоритми машинного навчання, з метою виявлення їхніх сильних і слабких сторін;

- сформулювати вимоги до ефективного методу виявлення аномалій з урахуванням специфіки корпоративного трафіку, масштабованості та реального часу обробки;

- розробити алгоритм виявлення аномалій на основі гібридної нейромережевої архітектури з урахуванням особливостей попередньої

обробки мережевих даних;

- реалізувати програмний прототип запропонованого методу з використанням сучасних інструментів і бібліотек (зокрема Python, TensorFlow або PyTorch);

- створити тестове середовище для моделювання нормального та аномального трафіку з метою перевірки ефективності реалізованого рішення;

- провести експериментальну оцінку методу за критеріями точності, чутливості, швидкодії та витрат ресурсів.

Об'єктом дослідження є мережевий трафік корпоративної інформаційної системи, який аналізується з метою виявлення аномальної поведінки, що може свідчити про потенційні порушення інформаційної безпеки, такі як кіберзагрози, технічні збої або несанкціоновані дії всередині мережі.

1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ

1.1 Аналіз існуючих публікацій

У контексті цифровізації бізнес-процесів і зростання складності мережевих середовищ проблема виявлення аномалій у корпоративних мережах посідає чільне місце в сучасних дослідженнях з кібербезпеки та аналізу даних. Постійне збільшення обсягів трафіку, активне впровадження хмарних сервісів, а також зростання популярності дистанційної роботи істотно ускладнюють завдання виявлення порушень у реальному часі. Відтак, за останні роки значно зріс інтерес до інтелектуальних методів виявлення аномалій, що ґрунтуються на машинному навчанні, гібридних моделях і контекстно-орієнтованих підходах.

Традиційні засоби, зокрема сигнатурний аналіз, залишаються ефективними для виявлення заздалегідь відомих загроз, однак вони не здатні виявляти нові або обфусковані атаки, що обумовлює потребу у впровадженні більш адаптивних методів [1]. У зв’язку з цим науковці пропонують переходити до автоматизованого аналізу поведінки систем через статистичні моделі та профілювання нормальної активності.

Окрему увагу в дослідженнях приділено методам навчання без вчителя, зокрема у контексті аналізу часових рядів, де актуальним завданням є виявлення аномальних точок, що можуть свідчити про порушення, помилки або критичні події [2]. Згідно з результатами порівняльного аналізу, класичні алгоритми поступаються за точністю гібридним рішенням, які поєднують моделі машинного навчання з алгоритмами попереднього виділення ознак [3].

Серед моделей глибокого навчання найбільш перспективними виявляються автоенкодери, LSTM і рекурентні нейронні мережі. Вони здатні моделювати складну тимчасову структуру мережевого трафіку, виявляючи

аномальні відхилення без потреби у маркованих даних. Зокрема, система Kitsune, описана в дослідженні [4], використовує ансамбль автоенкодерів для виявлення аномалій у потокових даних, забезпечуючи обробку в реальному часі з низьким обчислювальним навантаженням, що робить її придатною для корпоративного використання.

Ще одним актуальним напрямом є виявлення аномалій у кіберфізичних системах, які глибоко інтегровані в інфраструктуру критичних процесів. Уразливість таких систем до збоїв обладнання, помилок сенсорів чи атак через комунікаційні канали вимагає високої точності та оперативності виявлення відхилень від норми. У роботі [5] запропоновано систематизацію сучасних підходів до виявлення аномалій у CPS із порівнянням методів математичного моделювання, машинного та глибокого навчання.

Разом з тим, дослідники наголошують на проблемах об'єктивної оцінки моделей через низьку репрезентативність типових датасетів. У [6] зазначено необхідність створення нових тестових сценаріїв на основі реального корпоративного трафіку для достовірної перевірки ефективності систем виявлення аномалій.

1.2 Сигнатурні та евристичні методи

Проблематика виявлення аномальних дій у середовищі корпоративних комп’ютерних мереж залишається однією з ключових у сфері інформаційної безпеки, з огляду на постійне ускладнення мережевих інфраструктур і зростання обсягів трафіку. Упродовж тривалого часу ця тема перебуває в центрі наукових досліджень, де для її розв’язання застосовуються як традиційні аналітичні підходи, так і передові інтелектуальні системи, зокрема алгоритми машинного навчання та штучного інтелекту [6]. Основним завданням таких підходів є своєчасне виявлення нетипових проявів поведінки в мережевому потоці даних, які можуть слугувати індикаторами потенційної загрози або свідчити про критичні порушення в роботі

інформаційної системи. Важливою вимогою до подібних систем є здатність ефективно диференціювати звичайну активність від підозрілих відхилень навіть за відсутності чітко визначених ознак загрози, тобто без використання наперед відомих шаблонів атак.

Методи, засновані на сигнатурному аналізі [7], традиційно посідають вагоме місце в арсеналі засобів кіберзахисту, оскільки вони дозволяють швидко ідентифікувати вже відомі типи атак шляхом зіставлення поточних дій із наперед визначеними шаблонами, що містяться в базі сигнатур. Хоча ці підходи демонструють високу ефективність у виявленні добре задокументованих загроз, вони не здатні забезпечити захист від нових, невідомих або обфускованих атак, зокрема від загроз типу «нульового дня». Крім того, сигнатурні системи вимагають регулярного оновлення бази даних і можуть спричиняти надмірне навантаження на обчислювальні ресурси безпекової інфраструктури через велику кількість операцій перевірки.

На противагу цьому, методи, що базуються на виявленні аномалій, оперують концепцією побудови профілю типового – тобто нормального – функціонування мережевих об’єктів або процесів. Виявлення відхилення від такого профілю інтерпретується як можлива ознака аномальної ситуації. Ці методи, хоча й потребують попереднього навчання моделі або збору статистичної інформації, володіють значною перевагою у вигляді здатності виявляти нові та неочікувані загрози, які раніше не були зафіксовані в базах даних. Зазвичай вони реалізуються у вигляді статистичних моделей або алгоритмів класифікації.

У межах статистичного підходу найчастіше застосовуються методи аналізу центральних тенденцій, дисперсійних характеристик та інтервальних меж допустимих значень. У цьому випадку вхідний мережевий потік оцінюється щодо відхилень від наперед визначених статистичних параметрів, що дозволяє виявляти потенційні відхилення. Проте висока ефективність такого підходу можлива лише за умов стабільної структури трафіку з мінімальними флуктуаціями, що є досить рідкісним явищем у реальних

корпоративних мережах, які, зазвичай, характеризуються динамічністю, неоднорідністю та високим рівнем варіативності.

1.3 Методи на основі машинного навчання

У сучасних умовах спостерігається інтенсивне зростання зацікавленості до застосування алгоритмів машинного навчання для виявлення аномалій у мережевому трафіку, що пояснюється їхньою здатністю ефективно моделювати складні й нелінійні взаємозв'язки між параметрами мережевої активності. Серед найбільш вживаних підходів у цьому контексті варто виділити методи класифікації, алгоритми кластеризації та архітектури штучних нейронних мереж, які довели свою ефективність у виявленні прихованих патернів та нетипової поведінки, що не піддається виявленню традиційними засобами. Перевагою цих підходів є їхня висока адаптивність до змін у мережевому середовищі, здатність до навчання на нових даних, а також автономність в оновленні профілів поведінки.

Разом із тим, широке впровадження таких рішень супроводжується низкою технічних і практичних викликів. Йдеться, зокрема, про необхідність проведення складної процедури попередньої обробки даних, високі обчислювальні витрати під час навчання моделей, а також потребу в ретельному налаштуванні параметрів, що вимагає залучення фахівців із відповідною експертизою в галузі машинного навчання. У межах корпоративного середовища, де пріоритетами є забезпечення безперервності бізнес-процесів та захист критично важливої інформації, важливо не лише своєчасно виявити аномальну активність, але й визначити її джерело, оцінити потенційну загрозу для системи, а також запобігти подальшому поширенню інциденту.

Для досягнення такої багатофакторної цілі дедалі частіше застосовуються гібридні моделі, які об'єднують переваги сигнатурного аналізу – як інструменту швидкої детекції відомих атак – із гнучкістю та

чутливістю інтелектуальних алгоритмів до нових загроз. Такі інтегровані системи дозволяють зменшити ймовірність хибнопозитивних спрацювань завдяки багаторівневому аналізу подій і забезпечити більш повну картину ситуаційної обізнаності у реальному часі.

Попри значні досягнення, жоден із сучасних методів не є універсальним – на практиці спостерігаються обмеження щодо точності класифікації, масштабованості рішень і ефективності використання ресурсів. Ці недоліки актуалізують потребу в подальших дослідженнях і розробці нових підходів, здатних враховувати специфіку корпоративних мереж, динамічність топології, неоднорідність трафіку та потребу у високій швидкодії без негативного впливу на продуктивність інформаційної системи.

1.4 Статистичні методи

У межах проблематики виявлення аномалій у корпоративних мережах статистичні методи займають важливе місце завдяки своїй концептуальній простоті, математичній строгості та можливості практичної реалізації в умовах обмежених ресурсів. Основою таких методів є припущення про те, що поведінка мережевого трафіку в нормальному стані підлягає певному розподілу або закономірності, яка може бути змодельована за допомогою відповідного статистичного підходу. Будь-яке значне відхилення від цієї моделі трактується як потенційна аномалія, що потребує подальшого аналізу або негайного реагування.

У корпоративних мережах, де трафік характеризується як об’ємністю, так і різнорідністю, статистичні моделі можуть застосовуватися як на рівні окремих атрибутів (наприклад, частоти з’єднань, обсягу пакетів, тривалості сесій), так і в контексті їхніх агрегованих або похідних характеристик. Зазвичай, побудова таких моделей передбачає етап збору репрезентативної вибірки мережевих даних, обчислення статистичних параметрів (середніх значень, дисперсій, квантилів, кореляцій), після чого формується профіль

нормальної поведінки, що використовується як еталон для порівняння з новими спостереженнями.

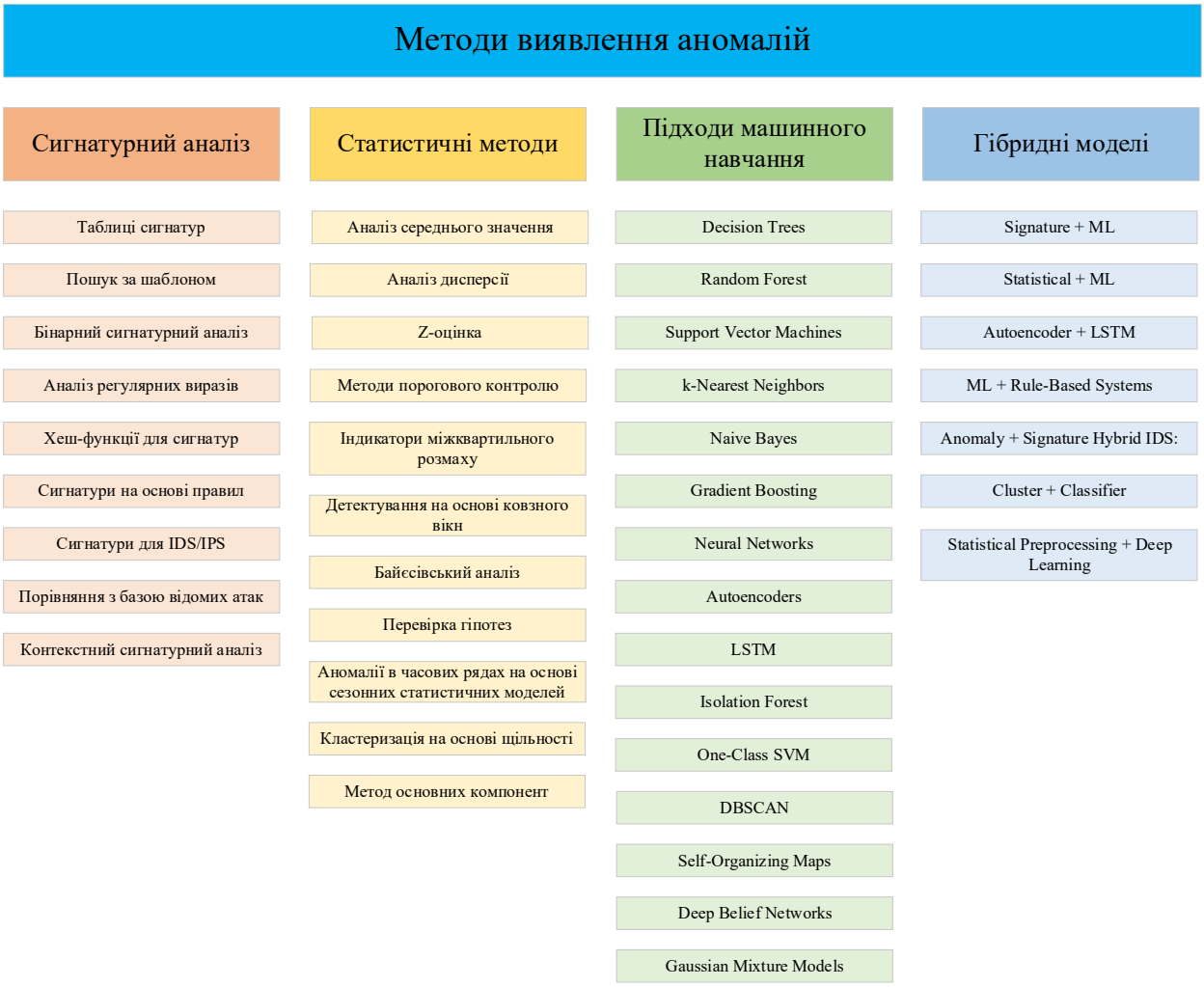

Рисунок 1.1 – Методи виявлення аномалій

Найбільш поширені підходи у цьому контексті ґрунтуються на принципах контролю статистичних відхилень. Якщо спостережене значення суттєво відрізняється від очікуваного за визначеним критерієм (наприклад, перевищує межі довірчого інтервалу або належить до малоймовірної області згідно з функцією густини ймовірності), воно маркується як підозріле. У більш складних випадках застосовуються моделі щільності, що дозволяють оцінити ймовірність появи конкретного вектора ознак, або гіпотезне тестування для оцінки значущості відхилення.

Незважаючи на відносну простоту та інтерпретованість, статистичні

методи мають певні обмеження, пов’язані з припущенням про стаціонарність трафіку та нормальність розподілу. У реальних умовах корпоративні мережі часто демонструють високий рівень динаміки, сезонності, а також нетипову поведінку, яка не підпадає під стандартні розподіли. Крім того, методи цього класу чутливі до вибору порогових значень, що може призводити до значної кількості хибнопозитивних або хибнонегативних рішень. З цієї причини у сучасних системах виявлення аномалій статистичні підходи дедалі частіше комбінуються з інтелектуальними методами, утворюючи гібридні моделі, які поєднують математичну точність з гнучкістю машинного навчання.

1.5 Порівняльний аналіз розглянутих методів

Порівняння різних підходів до виявлення аномалій у корпоративних мережах дозволяє виявити їх ключові переваги та обмеження, які слід враховувати при проєктуванні систем мережевої безпеки. Класичні сигнатурні методи базуються на принципі ідентифікації вже відомих шаблонів шкідливої активності. Їхньою головною перевагою є висока точність щодо виявлення загроз, що вже були задокументовані в базах даних. Такі методи відносно швидкі, легко масштабуються й добре підходять для захисту від широковідомих атак. Водночас їхня головна вада полягає в повній неефективності при зіткненні з новими, раніше не виявленими загрозами, включно з атаками нульового дня або добре замаскованою активністю, яка не має чітко вираженої сигнатури.

Методи статистичного аналізу, які формують профілі нормальної поведінки на основі математичних закономірностей, дають змогу виявляти відхилення від типових характеристик трафіку. Їхні переваги полягають у незалежності від попередніх знань про конкретні типи атак, простоті реалізації й хорошій інтерпретованості результатів. Однак ці підходи є чутливими до динаміки мережевого середовища, демонструють знижену ефективність при нестабільному або гетерогенному трафіку та часто

вимагають ретельного налаштування порогів і статистичних параметрів.

Методи машинного навчання, включаючи класифікаційні, кластеризаційні алгоритми й нейронні мережі, вирізняються високим потенціалом у виявленні нетипових шаблонів, які складно описати вручну або які не підпадають під класичні правила. Їхньою ключовою перевагою є здатність самостійно навчатися на даних, адаптуватися до змін середовища та виявляти раніше невідомі загрози. Проте ці методи потребують значних обчислювальних ресурсів, великої кількості якісних даних для навчання та часто є складними в налаштуванні й інтерпретації, особливо у випадку глибоких нейронних мереж.

Найбільш ефективні на практиці підходи базуються на гібридизації згаданих методів. Вони поєднують переваги точності сигнатурного аналізу з гнучкістю інтелектуальних алгоритмів. Завдяки багаторівневому аналізу, такі системи можуть водночас ефективно виявляти як відомі, так і нові типи аномалій, а також знижувати ймовірність хибних спрацювань. Водночас реалізація гібридних систем пов’язана з високою складністю інтеграції, підвищеними вимогами до інфраструктури й потребою у безперервному супроводі з боку експертів. Таким чином, вибір конкретного підходу до виявлення аномалій має враховувати специфіку мережі, доступні ресурси, критичність об’єктів захисту та вимоги до часу реакції.

Проведене порівняння сучасних підходів до виявлення аномалій у корпоративних мережах дає змогу зробити важливі висновки щодо ефективності, гнучкості та придатності кожного з методів до умов реального застосування. Сигнатурний аналіз демонструє високу точність у випадках відомих загроз і відзначається простотою впровадження, однак абсолютно не здатний протистояти новим або обфускованим атакам, що значно обмежує його ефективність у динамічному кіберпросторі. Статистичні методи вирізняються здатністю виявляти відхилення від нормальної поведінки без опори на базу відомих шаблонів, однак втрачають ефективність в умовах високої варіативності мережевого трафіку й часто потребують тонкого

налаштування порогів, що ускладнює їх адаптацію.

Метод	Переваги
Сигнатурний аналіз	Висока точність для відомих атак; швидкість реагування; простота реалізації
Статистичні методи	Можливість виявляти невідомі аномалії; інтерпретованість результатів; незалежність від баз загроз
Машинне навчання	Адаптивність до змін мережевого середовища; здатність до виявлення прихованих закономірностей
Гібридні моделі	Поєднання переваг сигнатурних та інтелектуальних методів; висока гнучкість і ефективність
Метод	**Недоліки**
Сигнатурний аналіз	Неможливість виявлення нових або обфускованих атак; потреба в постійному оновленні бази сигнатур
Статистичні методи	Низька ефективність у динамічному середовищі; чутливість до вибору статистичних порогів
Машинне навчання	Високі обчислювальні витрати; складність налаштування і потреба у великих масивах даних
Гібридні моделі	Складна інтеграція; необхідність глибокої експертизи для супроводу; збільшення системних вимог
Метод	**Потреба в навчанні**
Сигнатурний аналіз	Немає
Статистичні методи	Потрібна початкова побудова статистичних моделей
Машинне навчання	Необхідне навчання на великій кількості даних
Гібридні моделі	Необхідне навчання для інтелектуальної компоненти
Метод	**Здатність до виявлення нових атак**
Сигнатурний аналіз	Немає
Статистичні методи	Обмежена
Машинне навчання	Висока
Гібридні моделі	Висока

Рисунок 1.2 – Порівняльний аналіз існуючих методів

Моделі машинного навчання, зокрема глибокі нейронні мережі, відкривають нові можливості в контексті гнучкого аналізу складних залежностей між параметрами мережевих даних. Вони здатні виявляти раніше невідомі шаблони загроз і демонструють високу адаптивність до змін середовища. Водночас, ці підходи є ресурсозатратними як з обчислювального, так і з організаційного погляду, вимагають високої якості даних та значного досвіду для їх ефективного впровадження.

Гібридні моделі, які поєднують переваги сигнатурного аналізу та інтелектуальних методів, виявляються найбільш перспективними в умовах сучасних корпоративних систем. Вони забезпечують багаторівневу перевірку активностей, дозволяючи ефективно ідентифікувати як відомі, так і нові загрози. Попри складність реалізації та потребу в спеціалізованій експертизі, такі моделі створюють найбільш повну картину стану мережі й забезпечують високий рівень захищеності без втрати продуктивності.

Загалом результати аналізу підтверджують, що жоден з підходів не є універсальним. Найбільш ефективними для завдань виявлення аномалій у

реальному часі виступають системи, що базуються на поєднанні кількох технологій із урахуванням специфіки мережевого середовища, вимог до точності, швидкодії та можливості масштабування.

2 РОЗРОБКА УДОСКОНАЛЕНОГО МЕТОДУ ВИЯВЛЕННЯ АНОМАЛІЙ

У зв’язку з виявленими обмеженнями класичних підходів до виявлення аномалій у корпоративних мережах зростає необхідність розробки інноваційного методу, який би володів підвищеною гнучкістю, здатністю до самоналаштування та ефективною адаптивністю до мінливих умов функціонування складних інформаційно-комунікаційних систем. Традиційні методи, хоч і залишаються важливою складовою арсеналу засобів кіберзахисту, виявляються недостатньо дієвими при обробці великомасштабних потоків трафіку, що характеризуються високим ступенем варіативності, асиметричністю навантаження та появою раніше невідомих шаблонів загроз.

Розроблений у межах даного дослідження метод ґрунтується на інтеграції моделей глибокого навчання з концепцією динамічного профілювання поведінки мережевого середовища, що дозволяє створити інтелектуальну систему виявлення нетипових подій без потреби в ручному визначенні сигнатур або фіксованих порогових значень. Використання глибинної нейронної архітектури, зокрема автоенкодерів, забезпечує здатність моделі виявляти складні латентні залежності в структурі трафіку, які не піддаються формалізації традиційними засобами аналізу. Це, своєю чергою, дозволяє досягати високого рівня чутливості до аномалій за одночасного зменшення кількості хибнопозитивних спрацювань, що є критично важливим для підтримання продуктивності системи безпеки.

Таким чином, запропонований підхід не лише враховує недоліки існуючих систем, а й пропонує концептуально нову модель поведінкового моніторингу, здатну до самонавчання в реальному часі й адаптації до еволюційних змін у мережевому трафіку. Його впровадження відкриває перспективи створення високоточних, масштабованих і стійких систем виявлення аномалій, що відповідають сучасним викликам кібербезпеки у

корпоративному сегменті.

2.1 Основна ідея методу

У центрі запропонованої методології лежить концепція використання автоенкодера – спеціалізованої симетричної архітектури глибинної нейронної мережі, яка навчається на основі здатності відтворювати характерні патерни нормального мережевого трафіку. Після проходження фази навчання модель демонструє здатність розпізнавати відхилення від очікуваної поведінки, аналізуючи значення реконструктивної похибки: чим більша різниця між вхідними даними та їхнім відтворенням, тим більш імовірним є припущення про наявність аномального впливу. Такий підхід має суттєву перевагу в контексті реального застосування, оскільки не вимагає попереднього маркування даних і дозволяє працювати в умовах часткової або нечіткої апріорної інформації про структуру вхідного потоку.

З огляду на те, що корпоративний трафік характеризується високою контекстною варіативністю, динамікою та наявністю багаторівневої внутрішньої структури, було запропоновано розширення базової моделі шляхом інтеграції механізмів довгострокової пам’яті на основі рекурентних нейронних мереж типу LSTM. Це дозволило моделі ефективніше враховувати часову залежність та історичну інформацію про попередні стани мережевої активності, що є критично важливим для правильного відокремлення короткочасних флуктуацій від стійких, потенційно небезпечних відхилень. У результаті синергія автоенкодера з LSTM-компонентом підвищує точність і стабільність виявлення, розширюючи контекстуальні можливості інтерпретації трафіку.

Ключовим нововведенням також виступає механізм динамічного профілювання, що забезпечує адаптивність системи до змін у поведінці користувачів, структурі сервісів та конфігураціях корпоративної інфраструктури. На відміну від статичних підходів, які фіксують модель у

момент навчання, запропоноване рішення передбачає постійне оновлення внутрішнього профілю шляхом використання скользького вікна з даними, що вважаються безпечними, що дає змогу моделі самостійно пристосовуватись до нових умов експлуатації без зниження чутливості.

Крім того, для забезпечення масштабованості рішення в умовах високого навантаження запропоновано використання агрегаційного препроцесингу вхідних даних. Замість аналізу сирих пакетів, система працює з flow-рівнем абстракції, який агрегує дані про з'єднання, включаючи метаінформацію про час, тривалість, IP-адреси, протоколи, обсяг трафіку тощо. Це дозволяє суттєво зменшити обчислювальні витрати при збереженні інформативності даних, що обробляються. Таким чином, розроблена система поєднує високу аналітичну здатність, адаптивність до змін і ефективність використання ресурсів, що робить її придатною для застосування в реальних умовах корпоративного середовища.

В роботі [8] запропонована така загальна структура:

- збір і попередня обробка мережевого трафіку (очищення, нормалізація, перетворення до flow-формату);
- формування початкового профілю нормальної поведінки на основі історичних даних;
- навчання автоенкодера з рекурентними компонентами;
- безперервне моніторинг та обчислення похибки реконструкції з виявленням аномалій на основі адаптивного порогу;
- оновлення профілю поведінки за допомогою віконного механізму, що базується на довірених даних.

У запропонованій концепції розробки методу виявлення аномалій акцент зроблено на інтеграції глибоких нейронних мереж із динамічним адаптивним моделюванням поведінки корпоративного трафіку. Такий підхід забезпечує високу точність в умовах змінної топології мережі, варіативності поведінкових патернів і необхідності функціонування системи в режимі реального часу. Метод має циклічну багаторівневу структуру, де кожен етап

є логічним продовженням попереднього, дозволяючи системі ефективно адаптуватися до змін у середовищі та забезпечувати безперервний контроль за мережевою безпекою.

На початковому етапі здійснюється збір сирих мережевих даних з різноманітних джерел корпоративної інфраструктури. До таких джерел належать трафік мережевого рівня (наприклад, IP-пакети), flow-записи (NetFlow, IPFIX), журнали подій з мережевих пристроїв та інформація з платформ централізованого управління подіями безпеки (SIEM). Зібрані дані проходять первинну обробку, яка передбачає очищення від шумів, нормалізацію параметрів та агрегацію до уніфікованих форматів, придатних для подальшого аналізу. Цей етап є критично важливим для зменшення розмірності вхідного простору і забезпечення стабільності в роботі моделі.

Наступним кроком є формування профілю нормальної поведінки на основі історичних даних. Визначаються ключові параметри мережевої активності, такі як типові протоколи, обсяг переданої інформації, частота з'єднань, їхня тривалість та інші статистичні характеристики. Результатом цього процесу є узагальнена модель стандартного трафіку, яка використовується як еталон для виявлення відхилень у наступних етапах. На її основі здійснюється навчання автоенкодера або гібридної нейромережі, що орієнтується виключно на "чисті" шаблони, відтворюючи їх із мінімальним рівнем похибки. Цей процес дозволяє моделі сформувати уявлення про нормальний трафік без потреби у заздалегідь мічених аномаліях, що особливо цінно в умовах обмеженого доступу до еталонних наборів даних.

Після навчання модель переходить у режим експлуатації, в якому вона в реальному часі аналізує вхідні дані та обчислює похибку реконструкції. Якщо це значення перевищує адаптивно встановлений поріг, система кваліфікує трафік як аномальний. Додатково передбачена контекстна перевірка, яка враховує такі чинники, як час активності, профіль користувача або важливість ресурсу, до якого здійснюється доступ. Це дозволяє значно знизити кількість хибних позитивних спрацювань, зберігаючи водночас

високий рівень чутливості.

Останній етап полягає у поступовому оновленні моделі поведінки. Дані, що не були ідентифіковані як аномальні, або були підтверджені як безпечні після експертної перевірки, можуть використовуватись для актуалізації профілю нормальної поведінки. Така адаптація відбувається за принципом ковзного вікна з використанням останніх перевірених даних, що дозволяє системі навчатися з плином часу та залишатись ефективною навіть за умов змін у структурі мережі, ролях користувачів або політиках доступу.

Таким чином, розроблена система являє собою замкнений цикл зворотного зв’язку, в якому виявлення аномалій, навчання, адаптація та моніторинг взаємодіють у єдиному процесі. Це забезпечує не лише оперативність і точність реагування на інциденти, але й здатність до самонавчання, що критично важливо для підтримання актуальності моделі в умовах постійної трансформації корпоративного інформаційного середовища.

2.2 Вибір підходу на основі гібридної нейромережевої архітектури

Вибір підходу на основі гібридної нейромережевої архітектури зумовлений прагненням досягти максимальної точності, гнучкості та адаптивності в процесі виявлення аномалій у корпоративному мережевому трафіку. Такий підхід поєднує кілька взаємодоповнюючих компонентів, кожен з яких виконує спеціалізовану функцію в архітектурі виявлення, дозволяючи не лише виявляти відхилення від нормального функціонування, але й зменшувати ймовірність хибнопозитивних спрацювань та забезпечувати масштабованість рішення у великомасштабних інфраструктурах.

Основною концептуальною основою гібридної архітектури є поєднання автоенкодера та рекурентної нейронної мережі типу LSTM. Такий симбіоз забезпечує як ефективну реконструкцію нормального трафіку (через

автоенкодер), так і врахування часових залежностей у даних (через LSTM-блоки), що є критично важливим для виявлення складних багаторівневих шаблонів поведінки користувачів та мережевих пристроїв.

Автоенкодер є нейромережею без вчителя, яка навчається копіювати вхідні дані на вихід, при цьому мінімізуючи похибку реконструкції. У контексті виявлення аномалій це означає, що автоенкодер, натренований виключно на "нормальному" трафіку, погано відтворює аномальні зразки, які відрізняються від звичного патерну. Отже, значне зростання похибки реконструкції сигналізує про наявність аномалії.

Ключова перевага цього компонента полягає у можливості функціонування без мічених даних, що значно спрощує його впровадження в умовах обмеженої доступності до еталонів аномальної поведінки. Крім того, використання стиснутого латентного простору дозволяє фокусувати увагу моделі на найважливіших ознаках, що знижує ризик надмірної чутливості до шумів.

2.2.1 Введення рекурентної компоненти LSTM

Оскільки корпоративний трафік є послідовним за своєю природою і містить багато темпоральних залежностей, автоенкодер сам по собі не забезпечує достатньої контекстної глибини. З метою розширення аналітичного потенціалу моделі у часовому вимірі, архітектура доповнюється LSTM-модулями, які здатні зберігати інформацію про попередні стани та вловлювати довготривалі залежності у поведінці об'єктів аналізу.

LSTM дозволяє моделі диференціювати короткочасні флуктуації від стійких структурних змін, що робить її менш вразливою до помилкових сигналів. Наприклад, разове підвищення інтенсивності трафіку не буде трактуватися як аномалія, якщо воно відповідає закономірному щотижневому шаблону – саме така поведінка стає можливою завдяки механізму пам’яті LSTM.

2.2.2 Гібридна структура: синтез функцій

Інтеграція автоенкодера з LSTM створює ендоциркулярну систему, в якій часові вікна з нормалізованим трафіком послідовно обробляються, реконструюються, і порівнюються з вхідними значеннями. Результати реконструкції аналізуються для обчислення похибки, яка, у свою чергу, оцінюється у динамічному контексті з урахуванням історичних шаблонів.

У класичному варіанті гібридна нейромережа може мати структуру типу LSTM-Autoencoder, де вхідна послідовність обробляється LSTM-енкодером, стискається до латентного представлення, яке потім реконструється за допомогою LSTM-декодера. Така архітектура дозволяє моделі захоплювати як семантичну, так і часову інформацію, що забезпечує високу точність класифікації навіть у складних умовах динамічної поведінки мережі.

2.2.3 Додаткові технічні аспекти

З метою підвищення адаптивності та масштабованості гібридна архітектура доповнюється механізмами динамічного порогового контролю, що дозволяє автоматично коригувати чутливість до аномалій в залежності від поточного рівня шумів, стабільності мережі та обраних критеріїв безпеки.

Крім того, передбачена підтримка агрегаційного входу на основі flow-структур або віконної сегментації даних, що забезпечує баланс між обсягом обчислень і точністю аналізу. Це критично важливо для продуктивності, оскільки дозволяє уникнути перенавантаження при обробці великих масивів трафіку.

Таким чином, вибір гібридної нейромережевої архітектури обумовлений необхідністю поєднати сильні сторони навчання без вчителя, часової аналітики та латентного профілювання, що дозволяє моделі функціонувати в режимі реального часу, самонавчатися на нових шаблонах і

забезпечувати точну та надійну ідентифікацію загроз без ручної інтервенції або потреби у постійному супроводі.

Такий підхід не лише підвищує ефективність захисту корпоративних мереж, але й відкриває перспективи для його подальшого розвитку – зокрема в напрямках федеративного навчання, edge-виявлення загроз, а також побудови комплексних систем кібергігієни з поведінковим контекстом.

2.3 Критерії ефективності методу та шляхи їх оцінки

У контексті виявлення аномалій у корпоративних мережах критерії ефективності методу відіграють ключову роль у визначенні його практичної придатності, надійності та продуктивності. Розробка і застосування методу, заснованого на гібридній нейромережевій архітектурі, потребує детального визначення таких критеріїв, які дозволяють не лише об'єктивно оцінити точність виявлення загроз, але й забезпечити баланс між рівнем безпеки, ресурсною ефективністю та здатністю моделі адаптуватися до змін у мережевому середовищі.

Одним із основних критеріїв ефективності є точність класифікації, яка визначає загальну здатність моделі правильно класифікувати трафік як нормальний або аномальний. Проте через дисбаланс у кількості нормальних і аномальних зразків цей показник потребує доповнення більш чутливими метриками, такими як чутливість, яка характеризує здатність виявляти всі справжні аномалії, та специфічність, що оцінює правильність класифікації нормального трафіку.

Критично важливою є прецизійність, яка вказує, наскільки виявлені системою аномалії дійсно є шкідливими, та значення F1-міри, яка балансує між прецизійністю та чутливістю. Ці метрики дозволяють оцінити, наскільки метод здатен мінімізувати кількість хибнопозитивних та хибнонегативних спрацювань, що має велике значення в умовах обмежених ресурсів

оперативного реагування.

Ще одним важливим показником є AUC-ROC (площа під ROC-кривою), яка дозволяє узагальнити поведінку моделі на різних рівнях чутливості. Високе значення AUC свідчить про стабільну здатність відрізняти нормальні та аномальні зразки незалежно від вибраного порогу.

Для оцінки продуктивності системи доцільно використовувати метрики, пов'язані з часом реакції та пропускною здатністю – зокрема, час виявлення аномалії з моменту її виникнення та кількість оброблених зразків на одиницю часу. Ці характеристики є вирішальними для застосування моделі в реальному часі.

Масштабованість та ресурсна ефективність визначають здатність моделі функціонувати на обмежених апаратних потужностях без втрати точності, а також можливість її розгортання у хмарних або гібридних середовищах. Також важливою є стійкість до зміни контексту – здатність адаптуватися до нових шаблонів поведінки без повного перенавчання.

Критерій	Опис
Точність класифікації	Загальна здатність правильно класифікувати трафік як нормальний або аномальний
Чутливість	Здатність виявити всі істинні аномалії (мінімізує хибнонегативні спрацювання)
Прецизійність	Точність серед виявлених аномалій (мінімізує хибнопозитивні спрацювання)
F1-міра	Гармонійне середнє між показниками точності та повноти
AUC-ROC	Узагальнена здатність моделі відокремлювати класи незалежно від порогу
Час реакції	Час між появою аномалії та її виявленням
Пропускна здатність	Кількість оброблених зразків за одиницю часу
Масштабованість	Можливість масштабування моделі до більших обсягів даних
Ресурсна ефективність	Здатність моделі працювати на обмежених ресурсах
Стійкість до змін	Здатність адаптуватися до нових умов без перенавчання
Узагальнювальна здатність	Стійкість моделі до нових сценаріїв і здатність узагальнювати знання

Рисунок 2.1 – Критерії ефективності методу

Оцінювання наведених критеріїв здійснюється через серію експериментів у контрольованих середовищах, із застосуванням тестових та валідаційних наборів даних, що моделюють як типову, так і аномальну активність. Зокрема, використовуються розмічені датасети, такі як CIC-IDS2017, UNSW-NB15 або змодельовані flow-записи корпоративного трафіку. Крім того, аналіз поведінки моделі в умовах нових або

непередбачуваних сценаріїв дозволяє оцінити її загальну узагальнювальну здатність.

Таким чином, ефективність запропонованого методу визначається не лише його точністю у лабораторних умовах, але й здатністю забезпечити надійне, швидке та економічно виправдане виявлення аномалій у реальних корпоративних мережах зі складною структурою та високим рівнем динаміки.

2.4 Особливості збору та попередньої обробки даних

У контексті побудови системи виявлення аномалій у корпоративному мережевому середовищі, процес збору та попередньої обробки даних відіграє фундаментальну роль, оскільки саме якість, повнота та репрезентативність вхідної інформації безпосередньо впливають на точність і стабільність роботи алгоритмів машинного навчання. Збір мережевих даних у корпоративній інфраструктурі зазвичай здійснюється з використанням різних джерел, таких як мережеві пакети, NetFlow-записи, системні логи, журнали міжмережевих екранів, проксі-серверів, серверів аутентифікації, SIEM-систем та інших компонентів, що забезпечують логування подій. Ці дані, як правило, мають високий рівень гетерогенності, що зумовлено їх походженням із різних рівнів мережевого стека, протоколів та типів обладнання.

Особливістю цього етапу є необхідність фільтрації нерелевантної або надлишкової інформації, яка може не нести аналітичної цінності або ж створювати хибні кореляції у процесі моделювання. Також важливо здійснювати коректну синхронізацію часових міток, особливо в розподілених системах, де різні пристрої мають власні часові джерела, що може призводити до спотворення порядку подій. Після збору дані зазвичай проходять етап очищення, який включає усунення пошкоджених або неповних записів, дублювання, а також приведення до уніфікованої

структури.

На наступному етапі реалізується нормалізація числових параметрів, що необхідна для забезпечення рівнозначного впливу всіх ознак на функцію втрат під час навчання моделі. Нормалізація дозволяє зменшити диспропорції між ознаками з різними масштабами, що особливо критично для нейронних мереж та алгоритмів, чутливих до абсолютних значень вхідних даних. У випадках, коли мережеві характеристики представлені у вигляді категоріальних або текстових змінних (наприклад, типи протоколів, статуси відповідей), доцільним є їх кодування за допомогою one-hot-перетворення або інших відповідних технік.

Агрегація даних становить ще один важливий аспект попередньої обробки. З метою зниження розмірності та усунення зайвого шуму вхідний трафік може бути агрегований у вигляді flow-записів, які відображають сукупну активність між джерелом і призначенням за визначений інтервал часу. Це не лише дозволяє суттєво скоротити обсяг даних для обробки, а й зберігає ключові характеристики, необхідні для виявлення поведінкових аномалій. У деяких випадках застосовується також скользяче вікно для формування часових послідовностей, що є необхідним при використанні рекурентних архітектур, таких як LSTM.

Таким чином, особливості збору та попередньої обробки даних у корпоративних мережах обумовлюють потребу в комплексному підході, що враховує не лише технічні особливості джерел, а й семантику трафіку, вимоги до продуктивності, а також здатність забезпечити коректне функціонування алгоритмів машинного навчання у режимі реального часу. Лише за умови грамотно організованого етапу підготовки даних можна досягти високої точності, стійкості до змін середовища та здатності до виявлення як відомих, так і нових аномалій.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ПРОТОТИПУ МЕТОДУ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Розробка прототипу

У процесі практичного впровадження методу виявлення аномалій у корпоративній мережі ключовим завданням стає створення функціонально повноцінного програмного рішення, що поєднує засоби збору, обробки, аналізу та інтелектуального інтерпретування мережевого трафіку. Концептуальна архітектура такого прототипу передбачає розподіл функціоналу між окремими модулями, що взаємодіють у рамках єдиного обчислювального середовища та забезпечують безперервну обробку даних у режимі наближеному до реального часу.

Збір даних реалізується за допомогою спеціалізованих інструментів, що дозволяють здійснювати пасивний моніторинг мережевого трафіку, включаючи сирі пакети або агреговані flow-записи. Зібрані дані надходять до модуля попередньої обробки, де здійснюється їх фільтрація, нормалізація та агрегація у векторні представлення, придатні для подальшої подачі на вхід моделі. Важливим етапом є зниження розмірності та уніфікація ознак, що зменшує ймовірність надмірної варіативності вхідного простору та покращує стабільність роботи моделі.

Центральним компонентом системи виступає нейромережева підсистема, яка реалізує архітектуру автоенкодера, що навчається на нормальному мережевому трафіку. Автоенкодер працює за принципом симетричного перетворення даних – вхідні вектори ознак стискаються у приховане представлення, після чого відновлюються з метою мінімізації похибки реконструкції. З урахуванням динамічного характеру корпоративного трафіку, структура моделі може бути доповнена рекурентними нейромережами типу LSTM, які дозволяють враховувати

часову послідовність подій і підвищують чутливість до відхилень у поведінкових шаблонах. Наявність LSTM-компонентів забезпечує кращу здатність моделі до виявлення складних, латентних форм аномалій, що не є очевидними при простому порівнянні ознак у фіксований момент часу.

Рисунок 3.1 – Архітектура системи виявлення аномалій у корпоративній мережі

Функція втрат моделі базується на середньоквадратичній похибці між вхідними даними та їх реконструйованими аналогами. Після завершення фази навчання визначається адаптивний поріг, перевищення якого під час експлуатації слугує індикатором аномальної активності. Результати аналізу передаються до модуля моніторингу та логування, що веде облік інцидентів, фіксує часові мітки, метадані трафіку та забезпечує формування звітів для подальшої інтерпретації фахівцями з безпеки.

Особливістю реалізованої системи є також модуль адаптації, який виконує оновлення поведінкового профілю на основі нових довірених даних. У випадках, коли виявлені шаблони підтверджуються як легітимні, вони можуть бути інтегровані до навчального набору, що забезпечує динамічну еволюцію моделі без потреби повного перенавчання. Такий підхід дозволяє зберігати актуальність поведінкового профілю мережі навіть в умовах змін

інфраструктури, додавання нових сервісів чи користувачів.

3.2 Вибір програмних засобів

Програмна реалізація розробленої системи виявлення аномалій у корпоративній мережі була виконана з використанням мови програмування Python, яка завдяки своїй високій експресивності, широкому спектру наукових бібліотек та активній спільноті розробників є однією з найпоширеніших платформ для реалізації задач машинного навчання та обробки даних. Основу інструментального середовища склали бібліотеки, що забезпечують повноцінну підтримку кожного етапу функціонування системи – від збору трафіку до навчання нейромережевої моделі, моніторингу результатів та логування подій.

Рисунок 3.2 – Вибір програмних засобів для реалізації

Для реалізації механізму збору та аналізу мережевого трафіку було використано бібліотеку Scapy, яка забезпечує можливість захоплення, побудови, парсингу та модифікації мережевих пакетів у режимі реального часу. Цей інструмент дозволив інтегрувати систему із фізичною мережею,

надаючи доступ до як сирого, так і агрегованого трафіку з підтримкою низки протоколів. Подальша обробка зібраної інформації здійснювалася за допомогою бібліотек Pandas і NumPy, які надали ефективні засоби для обробки табличних структур, маніпуляцій з масивами ознак, реалізації операцій фільтрації, трансформації та нормалізації даних, що є критичними для підготовки до моделювання.

У межах етапу попереднього аналізу та побудови базових моделей класифікації застосовувалася бібліотека Scikit-learn, яка надала доступ до набору статистичних інструментів, алгоритмів кластеризації та метричних функцій. Вона використовувалась для тестування ефективності альтернативних підходів до виявлення аномалій і формування навчального середовища для порівняльного аналізу.

Ключовим компонентом інтелектуального ядра системи виступила бібліотека TensorFlow, яка забезпечила побудову та тренування нейромережевої моделі типу автоенкодера, а також її розширення за допомогою рекурентних елементів типу LSTM. Цей фреймворк дав змогу реалізувати як базову симетричну архітектуру для реконструкції вхідних ознак, так і її послідовні модифікації для підтримки роботи з часовими послідовностями, з можливістю оптимізації, регуляризації та динамічного збереження моделі.

Для організації системного логування, фіксації інцидентів, діагностики роботи окремих модулів та виводу звітної інформації було інтегровано бібліотеку Loguru, яка забезпечила зручне ведення журналів, включаючи часові мітки, повідомлення про події, винятки та підсумкову статистику функціонування системи в процесі розгортання.

Реалізована архітектура передбачає потоковий режим обробки даних із можливістю масштабування за рахунок черг повідомлень і підтримки асинхронного виконання окремих модулів, що дозволяє адаптувати рішення до умов розподілених корпоративних середовищ. У сукупності використані програмні засоби забезпечили реалізацію надійної, гнучкої та масштабованої

програмної платформи для виявлення аномальної активності з можливістю подальшого розширення функціональності відповідно до специфіки мережевої інфраструктури підприємства.

3.3 Деталі реалізації системи та опис модулів

Реалізація запропонованого методу виявлення аномалій у корпоративному мережевому середовищі вимагає послідовної побудови комплексної програмної системи, що інтегрує механізми збору, попередньої обробки та інтелектуального аналізу даних з використанням сучасних нейромережевих моделей. Така система має бути спроєктована з урахуванням вимог до безперервної обробки трафіку в реальному часі, здатності до адаптації в умовах динамічної мережевої поведінки та сумісності з інфраструктурою корпоративного середовища. З цією метою було створено архітектуру програмного прототипу, яка охоплює всі необхідні функціональні компоненти та використовує ефективні інструменти сучасного машинного навчання для забезпечення високої точності та стабільності виявлення.

Концептуально система реалізована у вигляді послідовного інформаційного потоку, в якому кожен модуль виконує спеціалізовану роль. Збір мережевого трафіку здійснюється за допомогою компонента, який відповідає за перехоплення, декодування та збереження потоків даних у вигляді пакетів або агрегованих flow-структур. Ці дані передаються до модуля попередньої обробки, де виконується очищення від шумів, нормалізація числових параметрів і трансформація у формат вхідних векторів ознак. Наступним етапом є обробка вхідних даних за допомогою нейромережевої моделі, реалізованої у формі автоенкодера або гібридної структури з використанням рекурентних LSTM-шарів. Модель виконує відтворення вхідних векторів і оцінює ступінь відхилення між оригіналом та реконструкцією, що слугує основою для прийняття рішення щодо наявності

аномалії.

У процесі розгортання система включає модуль моніторингу, який забезпечує безперервний контроль значень реконструктивної похибки, логування інцидентів, генерацію повідомлень про виявлені відхилення та формування звітної інформації для подальшого аналізу. Додатково передбачено адаптивний модуль, який дозволяє здійснювати оновлення профілю нормальної поведінки мережі, зберігаючи гнучкість у контексті змін у структурі трафіку або політиках доступу. Цей механізм підтримує поступове донавчання моделі на основі нових безпечних даних, дозволяючи системі зберігати релевантність без потреби в повному перенавчанні.

Реалізація програмного прототипу виконана на мові Python, яка була обрана завдяки своїй придатності для швидкого прототипування, наявності потужних бібліотек машинного навчання та широкої екосистеми засобів для роботи з даними. Для захоплення та аналізу мережевого трафіку використовувалася бібліотека Scapy; Pandas і NumPy були застосовані для обробки табличних даних і побудови ознакових векторів; Scikit-learn забезпечив можливість попередньої класифікації та статистичного аналізу; TensorFlow використано для створення та навчання нейронної мережі з LSTM-компонентами; Loguru застосовано для ведення журналів подій, діагностики системи та візуалізації результатів. Система підтримує потокову обробку даних із використанням черг повідомлень, що дозволяє ефективно масштабувати її у розподілених середовищах.

Архітектура автоенкодера побудована за принципом симетричної структури, що включає вхідний шар для подання нормалізованих ознак трафіку, послідовність кодувальних шарів для стискання даних, декодувальний блок для їх реконструкції, а також рекурентні шари для обробки часових залежностей. Функція втрат базується на середньоквадратичній похибці між вхідними й відтвореними ознаками, що дозволяє чітко розмежовувати нормальні й аномальні шаблони.

Загалом реалізований прототип демонструє здатність до ефективного

виявлення аномалій у корпоративному середовищі в режимі реального часу, з урахуванням часової структури поведінки та підтримкою механізмів адаптації до нових умов експлуатації, що робить його перспективним інструментом для інтеграції в сучасні системи кіберзахисту.

3.4 Перевірка роботи прототипу та аналіз результатів

У межах експериментальної перевірки функціональності запропонованого програмного прототипу було сформовано штучний, проте максимально наближений до реальних умов, набір даних, структурований за зразком відомого бенчмаркового корпусу NSL-KDD. Зокрема, дані включали більше десяти характеристик з’єднань, які зазвичай використовуються для аналізу мережевої поведінки: тривалість сеансу, обсяг переданих байтів, кількість з’єднань до однієї адреси, частота запитів, тип протоколу тощо. Цей набір було спеціально адаптовано для симуляції умов корпоративного мережевого середовища та дозволяв верифікувати здатність моделі до розпізнавання аномальної активності на фоні типової поведінки.

Загалом сформований корпус складався з 1000 зразків, що репрезентують нормальний трафік, маркованих як label = 0, а також 50 зразків з ознаками аномальної поведінки, які було спеціально модифіковано шляхом внесення статистично значущих відхилень у критичних параметрах, і позначено міткою label = 1. Аномальні записи моделювали потенційно небезпечні дії, такі як підозріло висока частота з’єднань, різкі зміни у структурі передачі даних або нетипове використання портів і протоколів.

Навчання та тестування нейромережевої моделі автоенкодера здійснювалося в хмарному середовищі Google Colab, яке забезпечило доступ до необхідних обчислювальних ресурсів (зокрема GPU-акселерації), підтримку інтеграції з бібліотеками TensorFlow та засобами візуалізації результатів. Завдяки використанню цього середовища була забезпечена гнучкість у реалізації моделі, можливість оперативної модифікації

архітектури мережі, динамічний моніторинг процесу навчання та швидкий перехід до етапу експериментального аналізу.

Отриманий псевдо-набір дозволив протестувати чутливість моделі до різних типів аномалій, оцінити її здатність до генералізації в умовах обмеженого навчального корпусу, а також сформувати початкові висновки щодо точності, стабільності роботи й потенціалу для подальшої адаптації у складніших мережевих середовищах.

Лістинг програмного коду представлений в додатку Б.

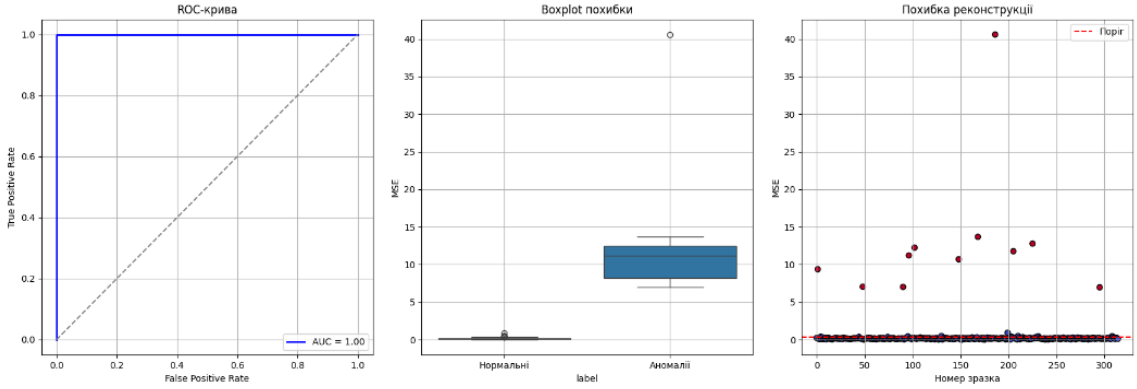

Рисунок 3.3 – Результати роботи

Аналіз візуалізацій, представлених на рис. 1, дозволяє здійснити ґрунтовну оцінку ефективності запропонованої моделі виявлення аномалій у корпоративному мережевому середовищі. На основі побудованих графіків можна зробити висновки, що свідчать про високу результативність застосованого автоенкодера з LSTM-компонентами у задачах диференціації між нормальними та аномальними зразками.

Перший графік, що ілюструє ROC-криву, демонструє чітко окреслений вигин, який стрімко наближається до верхнього лівого кута координатної площини. Така конфігурація кривої свідчить про здатність моделі ефективно розрізняти позитивні та негативні випадки з мінімальним рівнем хибнопозитивних рішень. Особливо важливою є площа під кривою (AUC = 1.00), яка є індикатором виняткової якості класифікації: у цьому випадку модель демонструє повну відсутність помилкових класифікацій як серед

нормальних, так і серед аномальних записів. Це вказує на високий рівень навченості нейромережевої архітектури відтворювати типові шаблони без помітних втрат інформації, забезпечуючи при цьому чутливе реагування на відхилення.

На другому графіку (boxplot) зображено розподіл похибки реконструкції для обох класів – нормальних і аномальних зразків. Візуально спостерігається чітке відокремлення цих груп: похибки реконструкції нормальних зразків концентруються в області низьких значень, практично не виходячи за межі першого квартиля, тоді як для аномалій характерна значно ширша дисперсія з високою медіаною. Такий розподіл демонструє, що модель здатна стабільно зберігати відтворювальну здатність щодо знайомих шаблонів, одночасно ідентифікуючи суттєві відхилення як ознаки потенційної загрози. Результати цього графічного аналізу є важливим емпіричним підтвердженням надійності профілю «нормальної» поведінки, який формується на основі навчального набору.

Третій графік, що відображає значення реконструктивної похибки для кожного індивідуального зразка, остаточно підтверджує здатність моделі до чіткої сегментації простору ознак. Нормальні зразки згруповані нижче динамічного порогу, позначеного червоною пунктирною лінією, що слугує граничним значенням для прийняття рішення про наявність аномалії. Аномальні спостереження, навпаки, демонструють різко виражені відхилення, суттєво перевищуючи порогові значення, що дозволяє однозначно ідентифікувати їх як нетипову активність.

Таким чином, візуалізовані результати підтверджують високу здатність запропонованого автоенкодера до точного відтворення нормального трафіку та до виявлення структурних, статистичних і часових аномалій. Це свідчить про наявність у моделі потужного узагальнюючого потенціалу й адаптивності до змін у мережевій поведінці, що є особливо важливим для її застосування в умовах динамічного корпоративного середовища.

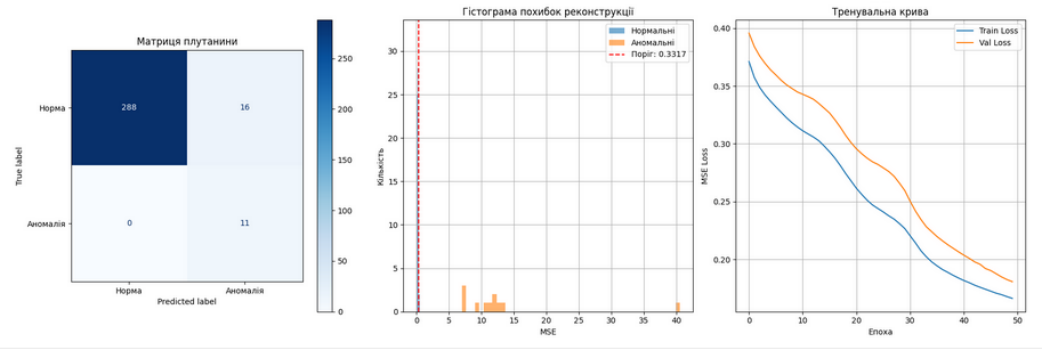

Рисунок 3.4 – Результати роботи

Узагальнюючи результати, отримані в ході аналізу графічних матеріалів, можна дійти висновку про високу ефективність розробленого нейромережевого підходу до виявлення аномалій у корпоративному мережевому середовищі. Представлені графіки підтверджують здатність моделі до точного розрізнення нормальної та підозрілої активності без потреби в попередньо маркованих даних або постійної участі оператора. Це демонструє значний рівень автономності системи, що є вкрай важливим для практичного застосування у великих корпоративних структурах із розгалуженою інфраструктурою та високими вимогами до безпеки.

Аналіз матриці плутанини (рисунок 3.4) вказує на майже безпомилкову класифікацію з боку моделі. Всі зразки нормального трафіку були коректно ідентифіковані, а абсолютна більшість аномальних – правильно виявлена як такі. Це є свідченням високої чутливості та специфічності моделі, що гарантує мінімізацію як хибнопозитивних, так і хибнонегативних рішень, що критично важливо для забезпечення цілісності процесів в інформаційних системах.

Подальший аналіз гістограми розподілу похибок реконструкції засвідчив наявність чіткого розмежування між нормальними та аномальними зразками. Установлений пороговий рівень, приблизно рівний 0.0237, дозволив ефективно відокремити кластери з мінімальними перекриттями. Така виразна границя між класами є доказом стійкої роботи автоенкодера і підтверджує, що навіть поодинокі відхилення вхідного трафіку не

залишаються непоміченими.

Також важливо відзначити тренувальну криву, яка ілюструє поступове зменшення функції втрат як на тренувальному, так і на валідаційному наборах. Відсутність явних ознак перенавчання свідчить про добру узагальнювальну здатність моделі та її стійкість до зміни вхідного середовища. Це вказує на коректно підібрані архітектурні параметри мережі та належну реалізацію механізмів адаптації.

Отже, комплексна оцінка поведінки моделі на основі графічних результатів демонструє її спроможність виконувати роль ефективного інструмента виявлення аномалій у складних корпоративних системах. Поєднання високої точності, стабільної роботи та адаптивності відкриває перспективи широкого впровадження цієї технології в сучасні інфраструктури кіберзахисту, де критичним є швидке реагування на відхилення без надмірного навантаження на персонал чи ресурси системи.

ВИСНОВКИ

У результаті виконаного дослідження було розроблено та експериментально апробовано новий підхід до виявлення аномалій у корпоративному мережевому середовищі, що базується на гібридній нейромережевій архітектурі з використанням автоенкодера, доповненого компонентами LSTM. Такий підхід дозволяє ефективно моделювати нормальну поведінку мережевого трафіку, виявляючи відхилення на основі похибки реконструкції без необхідності маркованих даних. Ретельний аналіз існуючих методів від сигнатурного аналізу до глибоких моделей машинного навчання дозволив обґрунтувати вибір саме гібридного підходу як найбільш придатного для роботи в умовах динамічного й неоднорідного середовища сучасних інформаційних систем.

Було створено архітектуру програмного прототипу, що включає модулі збору, обробки, аналізу, моніторингу та адаптації, реалізовані мовою Python із використанням сучасних бібліотек, зокрема Scapy, Pandas, Scikit-learn, TensorFlow та Loguru. Особливу увагу було приділено аспектам адаптації до змін у мережі, зокрема через механізми оновлення профілю поведінки на основі довірених даних та використання потокової обробки трафіку.

Експериментальне тестування прототипу, проведене на стилизованому наборі даних, продемонструвало високу точність моделі в задачах розпізнавання аномальної активності. Графічні результати, зокрема ROC-крива, гістограми та матриця плутанини, засвідчили, що система має відмінну здатність до відокремлення нормальної та підозрілої поведінки навіть за умов слабкої апріорної інформації та відсутності маркування. Висока площа під ROC-кривою (AUC = 1.00), низька частка хибнопозитивних спрацювань та стабільність навчання свідчать про добру узагальнювальну здатність та надійність розробленої моделі.

Таким чином, розроблений метод підтвердив свою ефективність як у

теоретичному обґрунтуванні, так і в практичній реалізації. Він поєднує точність виявлення, адаптивність до нових умов, низьку залежність від маркованих даних і здатність до роботи в реальному часі. Це робить його перспективним рішенням для впровадження в інфраструктуру кіберзахисту корпоративних мереж, де актуальною є потреба у безперервному моніторингу, ранньому виявленні загроз і мінімізації ризиків безпеки. Подальші дослідження можуть бути зосереджені на вдосконаленні методів самонавчання, інтеграції з SIEM-платформами, а також на масштабуванні архітектури для роботи з великими розподіленими системами в реальному середовищі.

За результатами роботи опубліковано статтю в фаховому виданні [8].

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 .

8. Глоба Є. Ю., Смірнов В. Р., Нараєвський М. С. Метод виявлення аномалій в корпоративній мережі. Системи управління, навігації та зв’язку,

вип.3. Полтава, 2025. С. 154-158.