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)

Методи виявлення атак на комп'ютерну систему з використанням машинного навчання

(тема)

Виконав:
здобувач 2 року навчання,
групи СПм-23-5
Олександр ЯЩЕНКО
(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: ас. Павло КРАВЧЕНКО
(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 Ященку Олександру Миколайовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Методи виявлення атак на комп'ютерну систему 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
система виявлення атак
машинне навчання
виявлення мережевих атак
розробка методу

4. Перелік питань, що потрібно опрацювати у роботі
Аналіз проблеми виявлення кібератак на комп’ютерні системи
Теоретичні основи машинного навчання у виявленні кібератак
Розробка та опис методу виявлення кібератак на основі машинного навчання
Програмна реалізація методу виявлення кібератак у Google Colab

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	06.06.2025–15.06.2025	

Дата видачі завдання " 21 " квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ас. Павло КРАВЧЕНКО
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 55 с., 10 рис., 2 дод., 10 джерел.

СИСТЕМИ ВИЯВЛЕННЯ АТАК, МАШИННЕ НАВЧАННЯ, КОМП'ЮТЕРНА БЕЗПЕКА, МЕРЕЖЕВИЙ ТРАФІК, КЛАСИФІКАЦІЯ, RANDOM FOREST, КІБЕРЗАГРОЗИ, ОБРОБКА ДАНИХ, SMOTE, АНАЛІЗ ВТОРГНЕНЬ, IDS, CICIDS2017, ВІЗУАЛІЗАЦІЯ РЕЗУЛЬТАТІВ, GOOGLE COLAB, АВТОМАТИЧНЕ ВИЯВЛЕННЯ АНОМАЛІЙ.

Метою кваліфікаційної роботи є розробка, обґрунтування та практична реалізація методу виявлення атак на комп'ютерну систему з використанням алгоритмів машинного навчання, що забезпечує підвищення точності, адаптивності та швидкості реагування систем інформаційної безпеки в умовах високої складності та динамічності сучасних мережевих середовищ.

У ході виконання кваліфікаційної роботи було реалізовано повний цикл дослідження та розробки методу виявлення атак на комп'ютерну систему із застосуванням технологій машинного навчання. проведено ґрунтовний огляд сучасних систем виявлення вторгнень, включаючи Snort, Suricata, Bro, Ossec та Prelude, з аналізом їх функціональних можливостей, переваг і недоліків. Підкреслено обмеження традиційних інструментів щодо адаптації до нових типів атак та обробки великих обсягів мережевого трафіку. Запропонований метод показав високі результати за всіма основними метриками — точністю, F1-мірою та AUC. Проведено візуалізацію ефективності моделі та порівняння з іншими популярними алгоритмами класифікації, що продемонструвало перевагу розробленого підходу.

ABSTRACT

Master’s thesis: 55 pages, 10 figures, 2 appendices, 10 sources.

INTRUSION DETECTION SYSTEMS, MACHINE LEARNING, COMPUTER SECURITY, NETWORK TRAFFIC, CLASSIFICATION, RANDOM FOREST, CYBER THREATS, DATA PROCESSING, SMOTE, INTRUSION ANALYSIS, IDS, CICIDS2017, RESULT VISUALIZATION, GOOGLE COLAB, AUTOMATIC ANOMALY DETECTION.

The major goal of this thesis is the development, justification, and practical implementation of a method for detecting attacks on computer systems using machine learning algorithms. The proposed approach aims to enhance the accuracy, adaptability, and responsiveness of information security systems in the context of complex and dynamic modern network environments.

In order to complete development cycle was carried out to construct an attack detection method based on machine learning technologies. A comprehensive review of modern intrusion detection systems was conducted, including Snort, Suricata, Bro, Ossec, and Prelude, with an in-depth analysis of their functionalities, strengths, and limitations. The constraints of traditional tools in terms of adaptability to new types of attacks and the processing of large-scale network traffic were clearly emphasized.

The proposed method demonstrated high performance across all major evaluation metrics, including accuracy, F1-score, and AUC. Additionally, the effectiveness of the model was visualized, and a comparative analysis with other popular classification algorithms was performed, confirming the superiority of the developed approach.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AI – штучний інтелект

API – інтерфейс прикладного програмування

CSV – формат табличних даних, розділених комами

DDoS – розподілена атака на відмову в обслуговуванні

DNS – система доменних імен

DoS – атака на відмову в обслуговуванні

GUI – графічний інтерфейс користувача

HTTP – протокол передавання гіпертексту

ICMP – протокол керування повідомленнями в мережі Інтернет

IDS – система виявлення вторгнень

IP – протокол Інтернету

IPS – система запобігання вторгненням

LSTM – довготривала короткочасна пам’ять

ML – машинне навчання

PCAP – формат файлу для зберігання перехоплених мережевих пакетів

SIEM – система управління інформацією та подіями безпеки

SSL – протокол захищених сокетів

TCP – протокол керування передачею

TLS – протокол транспортного рівня безпеки

UDP – протокол дейтаграм користувача

VPN – віртуальна приватна мережа

ВСТУП

У сучасному світі інтенсивного розвитку інформаційних технологій питання забезпечення кібербезпеки стає все більш актуальним і гостро постає як у державному, так і в приватному секторах. Зі зростанням обсягів даних, збільшенням кількості користувачів мережі Інтернет та широким впровадженням цифрових сервісів значно підвищується і ризик виникнення загроз, пов’язаних із несанкціонованим доступом, крадіжкою конфіденційної інформації, знищенням або порушенням цілісності даних. Кіберзлочинність, що невпинно розвивається, набуває все новіших і складніших форм, що змушує фахівців у галузі інформаційної безпеки шукати нові, ефективніші методи виявлення та нейтралізації атак на комп’ютерні системи.

Сучасні методи виявлення атак, такі як сигнатурні та евристичні підходи, вже не забезпечують належного рівня захисту в умовах швидкоплинної еволюції загроз. Вони не завжди спроможні виявляти нові, раніше невідомі типи атак, або адаптуватися до змін у поведінці зловмисників. Саме тому в останнє десятиліття особливої популярності набули технології машинного навчання, які демонструють значний потенціал у задачах кібербезпеки. Використовуючи здатність моделей машинного навчання знаходити приховані закономірності у великих обсягах даних, можливо створити системи виявлення вторгнень, що не лише фіксують вже відомі загрози, але й виявляють нові, аномальні дії у системі.

У межах цієї кваліфікаційної роботи розглядається питання створення ефективного методу виявлення атак на комп’ютерну систему з використанням алгоритмів машинного навчання. Основна ідея полягає в побудові моделі, здатної аналізувати трафік або події, що відбуваються в системі, і з високим ступенем точності класифікувати їх як нормальні або потенційно небезпечні. Особливий акцент зроблено на практичну реалізацію запропонованого методу в хмарному середовищі Google Colab, що забезпечує

доступність та простоту використання запропонованого рішення широким колом дослідників, студентів та фахівців з інформаційної безпеки.

Дослідження, що представлене у цій роботі, базується на сучасних досягненнях у галузі машинного навчання, включаючи використання таких моделей, як дерева рішень, нейронні мережі та метод випадкового лісу. На основі порівняльного аналізу результатів роботи різних алгоритмів зроблено висновки щодо доцільності їх застосування в системах виявлення атак. Робота поєднує як теоретичний аналіз проблеми, так і практичну реалізацію, що дозволяє оцінити реальну ефективність запропонованого підходу.

Таким чином, дана кваліфікаційна робота спрямована на вирішення важливої та актуальної задачі – підвищення рівня захищеності комп'ютерних систем шляхом впровадження сучасних інтелектуальних методів аналізу даних. Її результати можуть стати основою для подальших досліджень і розробок у галузі автоматизованих систем кібербезпеки, а також знайти практичне застосування у реальних інформаційних інфраструктурах.

Метою даної кваліфікаційної роботи є розробка, обґрунтування та практична реалізація методу виявлення атак на комп'ютерну систему з використанням алгоритмів машинного навчання, що забезпечує підвищення точності, адаптивності та швидкості реагування систем інформаційної безпеки в умовах високої складності та динамічності сучасних мережевих середовищ.

Об'єктом дослідження є процеси моніторингу, аналізу та класифікації мережевого трафіку в корпоративних комп'ютерних системах для виявлення потенційно шкідливої активності та кіберзагроз.

У межах реалізації поставленої мети необхідно було вирішити такі основні завдання:

- здійснити аналіз сучасних методів виявлення атак, зокрема з урахуванням застосування інтелектуальних технологій;

- дослідити публічні датасети та визначити критерії для побудови навчальних і тестових вибірок;

- обґрунтувати вибір алгоритму машинного навчання, придатного для задач виявлення аномалій у мережевому трафіку;

- реалізувати запропонований метод в середовищі Google Colab із використанням інструментів Python;

- провести порівняльний аналіз ефективності розробленого методу відносно традиційних моделей за ключовими метриками (точність, повнота, F1, AUC);

- сформулювати висновки щодо можливостей практичного застосування розробленого підходу в реальних умовах.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Методи обробки та аналізу даних в корпоративній мережі

У реаліях активної цифрової трансформації корпоративні мережі стали фундаментальним елементом інфраструктури для створення, передавання, зберігання та обробки інформації. Вони виконують функції не лише каналу комунікації між внутрішніми підрозділами організації, а й утворюють основу для побудови інтегрованих інформаційних систем, які сприяють автоматизації бізнес-процесів, підтримують прийняття стратегічних рішень і підвищують загальний рівень конкурентоспроможності компаній. Постійне зростання обсягів даних, що циркулюють у межах таких мереж, формує об’єктивну потребу в ефективних, масштабованих і безпечних засобах їх обробки.

Сучасні корпоративні мережі вирізняються складною архітектурою, багаторівневою структурою джерел інформації (гетерогенністю), а також вимогою роботи з даними різного типу – від табличних структур і системних логів до неструктурованих текстових документів, візуальних зображень чи потокових сигналів, що надходять від сенсорних пристроїв. За таких умов ефективне управління потоками даних вимагає впровадження спеціалізованих рішень на кожному етапі їх життєвого циклу: від збору та попереднього очищення – до аналітичної обробки, візуального представлення результатів і забезпечення інформаційної безпеки.

Одним із ключових етапів у цьому процесі є попередня обробка даних, яка визначає якість і релевантність інформації для наступного аналізу. Застосування процедур нормалізації, агрегації, фільтрації та стискання дозволяє узгодити структуру даних із технічними вимогами обчислювальних систем та оптимізувати використання ресурсів. На стадії зберігання даних вирішальну роль відіграє обґрунтований вибір типу інфраструктури

(локальної, хмарної або гібридної), а також гарантування доступності й цілісності інформаційного масиву.

В аналітичній частині корпоративних інформаційних систем особливе значення мають інструменти інтелектуальної обробки даних, зокрема OLAP-моделі [1], технології інтелектуального аналізу даних (Data Mining) [2], а також сучасні алгоритми машинного навчання [3], які надають змогу не лише працювати з великими обсягами інформації, а й виявляти приховані залежності, здійснювати прогнозування та приймати обґрунтовані управлінські рішення. З огляду на це, зростає інтерес до аналізу цифрових платформ, здатних реалізовувати зазначені функції, зокрема – засобів хмарної аналітики.

Питання безпеки обробки даних також набуває першочергового значення – шифрування, маскування, анонімізація та контроль доступу стали невід'ємними компонентами архітектури сучасних корпоративних систем, адже компрометація або втрата критичної інформації може мати серйозні наслідки для стабільності та репутації організації.

Корпоративні мережі зазвичай проектуються з урахуванням багаторівневої архітектури, яка включає локальні, глобальні та віртуальні приватні сегменти. Така структура орієнтована на забезпечення стабільного й безперебійного доступу до інформаційних ресурсів незалежно від фізичного місця перебування користувача. Архітектурна модель корпоративної мережі може бути централізованою – з єдиним обчислювальним центром, або розподіленою – з декількома незалежними вузлами обробки. Дані, що циркулюють у межах корпоративної мережі, суттєво варіюються за структурою та походженням і поділяються на структуровані, неструктуровані та напівструктуровані. З погляду часової релевантності, ці дані можуть бути історичними, оперативними (використовуваними в режимі реального часу) або потоковими, що потребує застосування специфічних підходів до їх обробки відповідно до контексту використання.

Інформаційні потоки в межах корпоративної інфраструктури поділяються на внутрішні (комунікація між підрозділами, серверами, внутрішніми користувачами) та зовнішні (взаємодія з контрагентами, клієнтами, постачальниками або хмарними платформами). Кожен з цих потоків вимагає дотримання специфічних технічних умов: мінімізація затримок, забезпечення надійності й відмовостійкості, масштабованість, дотримання стандартів інформаційної безпеки. Ефективна обробка таких потоків передбачає використання складних протоколів маршрутизації, механізмів моніторингу трафіку, інтелектуальних систем балансування навантаження, політик керування доступом та засобів шифрування.

З урахуванням зростання кількості пристроїв, цифрових сервісів та розширення IT-інфраструктур, корпоративні мережі дедалі частіше інтегрують хмарні обчислювальні потужності, технології периферійної (edge) обробки, а також елементи Інтернету речей (IoT) [9]. Це дозволяє здійснювати збір і попередню обробку даних безпосередньо на рівні кінцевих пристроїв, мінімізуючи затримки та навантаження на центральні вузли.

Початковий етап обробки корпоративних даних є ключовим у формуванні якісної аналітичної бази, адже саме він визначає точність прогнозів і ефективність подальшого прийняття управлінських рішень. Сучасні підходи до збору й попередньої обробки даних охоплюють широкий спектр процедур, спрямованих на перетворення «сирого» або неструктурованого інформаційного потоку в уніфіковану, очищену структуру, придатну для аналітики.

У корпоративному середовищі дані надходять із різноманітних джерел: програмних комплексів, внутрішніх баз і реєстрів, журналів подій, API-запитів, IoT-пристроїв, потоків мережевого трафіку, а також сторонніх інформаційних систем. Для інтеграції цих гетерогенних потоків застосовуються інструменти логування подій і транзакцій, ETL-процеси, спеціалізовані платформи для потокової обробки та інтеграції даних. Всі ці

процедури повинні відповідати вимогам щодо надійності, точності, повноти та узгодженості даних із семантикою джерела.

Після первинного збору даних часто виявляються дублікати, пропущені значення, логічні суперечності або помилки введення. На цьому етапі здійснюється очищення даних, їх нормалізація, стандартизація, типізація та фільтрація. Зазначені процеси реалізуються за допомогою SQL-запитів, мов програмування для роботи з даними (наприклад, Python, R) або в середовищах для аналітичного моделювання, таких як KNIME, RapidMiner, SAS.

Щоб забезпечити масштабованість корпоративних сховищ даних і знизити витрати на їх зберігання, активно застосовуються алгоритми стиснення, які дозволяють мінімізувати обсяг інформації без втрати її цілісності. Крім того, використовуються методи агрегації (для аналітичних запитів), семплінг (для оптимізації обчислювального навантаження), а також віконна агрегація, яка дозволяє відстежувати зміни показників у певних часових інтервалах. Такі підходи сприяють зниженню навантаження на обчислювальні ресурси та прискорюють виконання запитів до баз даних і аналітичних платформ.

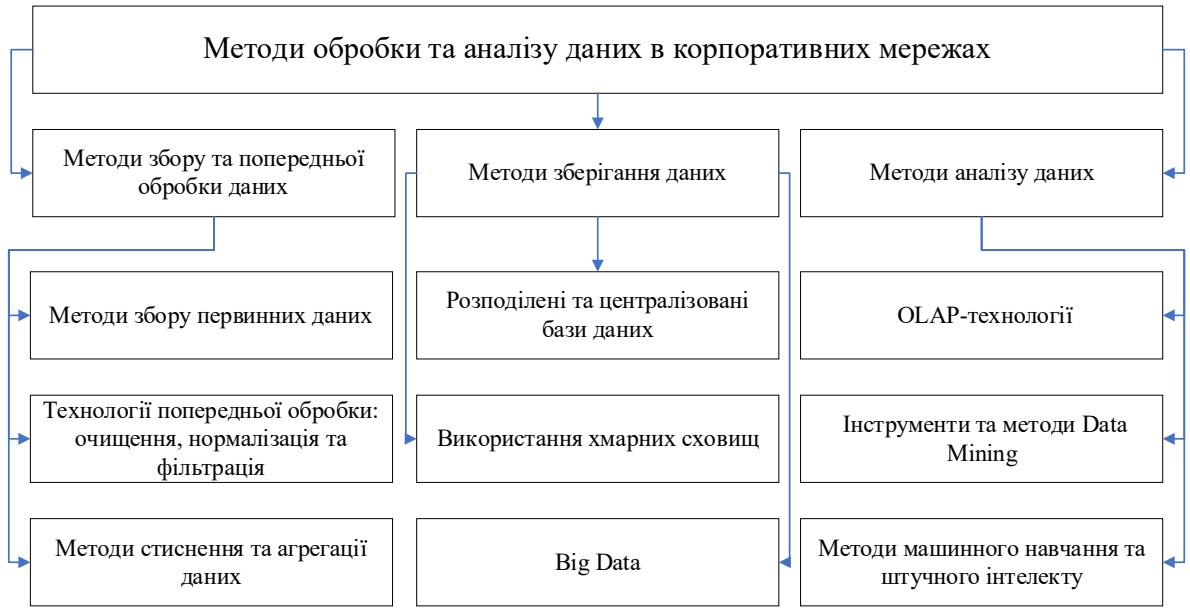

Рисунок 1.1 – Методи обробки та аналізу даних в корпоративних мережах

1.2 Зберігання даних

Зберігання даних є одним із визначальних етапів життєвого циклу інформації в корпоративних мережах, оскільки саме у відповідних сховищах відбувається акумуляція, впорядкування та організація даних з метою їх подальшого доступу, аналізу й використання у бізнес-процесах. У сучасному корпоративному середовищі концепція зберігання даних виходить за межі фізичного розміщення інформації на серверах – вона охоплює логічну структурування, можливості масштабування, забезпечення високої доступності, надійності та безпеки.

У межах архітектури баз даних найпоширенішими є два підходи – централізований і розподілений. Централізована модель передбачає зосередження всієї інформації в одному дата-центрі, що спрощує адміністрування та процедури резервного копіювання, але обмежує гнучкість масштабування та створює єдину точку відмови. Натомість розподілені бази даних забезпечують розміщення інформації на кількох вузлах у різних частинах мережі, що гарантує відмовостійкість, зниження затримок доступу та рівномірний розподіл навантаження. Однак реалізація такої архітектури потребує складних механізмів синхронізації, узгодження транзакцій та реплікації.

Вибір конкретної моделі зберігання даних залежить від низки чинників, включаючи обсяги інформації, вимоги до швидкодії, допустимий рівень ризику та поточні можливості IT-інфраструктури компанії.

Важливо також підкреслити зростаючу роль хмарних технологій у системах корпоративного зберігання. Завдяки своїй масштабованості, еластичності та економічності хмарні платформи стали невід’ємним елементом цифрової екосистеми сучасних підприємств. Вони забезпечують автоматичне масштабування ресурсів залежно від обсягів даних, інтеграцію з аналітичними та ML-інструментами, реалізацію політик контролю доступу, шифрування, журналювання та керування версіями. Використання гібридних

моделей дозволяє зберігати чутливу інформацію на локальних серверах, а менш критичні дані – в хмарі, оптимізуючи ресурси та зберігаючи контроль над інформаційними потоками.

Зі зростанням обсягів Big Data у корпоративному середовищі традиційні системи управління базами даних уже не забезпечують необхідного рівня ефективності. У таких умовах застосовуються розподілені файлові системи, NoSQL-рішення та комбіновані моделі, що об'єднують структуровані й неструктуровані дані. Вони підтримують паралельну обробку, децентралізований контроль доступу, реплікацію для захисту від втрат і масштабування за горизонтальною схемою.

Після етапів збору, попередньої обробки та зберігання, інформація переходить до наступної стадії – аналітичної обробки. Її мета полягає у виявленні прихованих закономірностей, побудові прогнозних моделей і підтримці прийняття стратегічних рішень. У сучасних умовах бізнес-аналітика набуває ознак комплексної інтелектуальної системи, яка поєднує традиційні статистичні методи з алгоритмами машинного навчання та штучного інтелекту.

Серед ключових технологій виділяють багатовимірний аналіз (OLAP), що дозволяє здійснювати гнучке вивчення великих обсягів даних за різними вимірами. Його переваги включають швидкий доступ до агрегованих показників, глибоку деталізацію інформації та ефективну побудову управлінських звітів. OLAP-системи активно використовуються у фінансовому плануванні, маркетинговій аналітиці, контролінгу, управлінському обліку та інших сферах, де критично важлива оперативна й точна обробка структурованих даних.

У більш складних сценаріях дедалі частіше застосовуються методи машинного навчання, які дозволяють моделювати складні, у тому числі нелінійні, залежності, аналізувати неструктуровані дані, здійснювати предиктивну аналітику та автоматизовувати процеси прийняття рішень. Прикладами впровадження ML у корпоративну практику є прогнозування

споживчого попиту, оптимізація логістичних ланцюгів, оцінювання ризиків у банківській і страховій сферах, персоналізація маркетингових стратегій, аналіз настроїв у соціальних мережах, автоматична класифікація документів і побудова систем рекомендацій.

Ефективна робота з даними в бізнес-середовищі потребує не лише адекватних методів, але й відповідного інструментарію, що забезпечує масштабованість, інтеграцію з численними джерелами, автоматизацію процесів і гарантовану надійність результатів. Залежно від потреб компанії застосовуються як універсальні платформи, так і спеціалізовані рішення для ETL, зберігання, обробки, аналізу та візуалізації даних. Система ETL (Extract – Transform – Load) є одним із ключових інструментів підготовки даних до аналітики. Її призначення полягає у витягуванні даних з різнорідних джерел, їх трансформації відповідно до вимог системи обробки та завантаженні до сховища.

Серед найпоширеніших ETL-рішень у корпоративному середовищі: Apache NiFi, Talend, Microsoft SSIS, Pentaho Data Integration, Apache Airflow. Ці платформи дозволяють ефективно автоматизувати процеси витягування, перетворення й подальшої інтерпретації інформації, забезпечуючи консистентність даних і знижуючи навантаження на аналітичні команди.

Сучасні аналітичні платформи забезпечують побудову інтерактивних звітів, інформаційних панелей, візуалізацій та автоматизованих аналітичних моделей. ERP- і CRM-системи також інтегрують у себе базові та розширені аналітичні функції, дозволяючи компаніям поєднувати планування, облік, взаємодію з клієнтами й аналіз у межах єдиного інформаційного середовища.

1.3 Аналіз останніх досліджень і публікацій за темою

Актуальні наукові дослідження засвідчують, що ефективна обробка даних у межах корпоративних мереж відіграє критичну роль у функціонуванні сучасних організацій. Своєчасне прийняття рішень,

використання хмарних сервісів, оптимізація інформаційних процесів та забезпечення стабільної мережевої взаємодії є визначальними чинниками досягнення стратегічних і конкурентних переваг. Водночас, упровадження відповідних технологій супроводжується низкою викликів, серед яких – захист даних, інтеграція гетерогенних джерел інформації, ефективне управління обчислювальними ресурсами. Це обумовлює необхідність подальших досліджень і розробки цілісних стратегій у сфері корпоративної аналітики.

У дослідженні [4] зосереджено увагу на впливі технологій обробки даних у режимі реального часу на оперативність бізнес-рішень. Автори аналізують застосування таких платформ, як Apache Kafka, Apache Flink, Google Cloud Dataflow і Spark Streaming, що дають змогу підприємствам динамічно реагувати на ринкові зміни, оптимізувати виробничі та логістичні процеси, а також підвищувати рівень обслуговування клієнтів. У роботі акцентовано також на викликах, пов’язаних з інтеграцією потоків даних, забезпеченням масштабованості, контролем якості та гарантуванням безпеки.

Стаття [5] досліджує сукупність чинників, які впливають на ефективність процесів обробки даних, зокрема обсяг, різноманітність, швидкодію та достовірність інформації. Описано підходи до оптимізації, серед яких – удосконалення апаратного рівня, програмне оновлення та застосування розподілених і хмарних архітектур. Окрему увагу приділено обробці неструктурованої інформації, синхронізації даних з різних джерел і реалізації політик енергоефективності та захисту приватності.

У дослідженні [6] розкривається потенціал хмарних технологій у сфері обробки великих обсягів промислових даних. Автори акцентують на перевагах хмарних рішень, зокрема на їх продуктивності, безпеці та економічній доцільності. Також розглядаються обмеження, пов’язані із забезпеченням конфіденційності, захистом від кіберзагроз і стабільністю масштабованих обчислень. У контексті розвитку галузі підкреслено

перспективність інтеграції технологій штучного інтелекту й алгоритмів машинного навчання.

У межах роботи [7] проаналізовано новітні цифрові підходи до трансформації бізнес-процесів – зокрема гіперавтоматизацію, процесний майнінг та предиктивний моніторинг. Автори наголошують на необхідності консолідації даних із різноманітних джерел як передумови ефективної цифрової трансформації й обґрунтованого прийняття управлінських рішень.

У публікації [8] запропоновано метод прогнозованого розподілу обчислювальних ресурсів у корпоративних мережах, орієнтований на середовище з підтримкою MEC (Multi-Access Edge Computing). Метод спрямований на забезпечення гарантій якості обслуговування (QoS) в умовах динамічного навантаження, підкреслюючи важливість оптимального управління інфраструктурними потужностями для досягнення високої ефективності обробки даних.

1.4 Поняття та класифікація комп’ютерних атак

У сучасних умовах стрімкого розвитку інформаційних технологій комп’ютерні системи зазнають зростаючої кількості загроз, які походять як із зовнішнього, так і з внутрішнього середовища. Комп’ютерна атака – це цілеспрямована дія, що здійснюється суб’єктом або групою суб’єктів з метою порушення конфіденційності, цілісності або доступності інформаційних ресурсів, функціонування системи або її окремих компонентів. Вона може реалізовуватися за допомогою різноманітних технічних, програмних або соціальних методів, залежно від рівня захисту об’єкта атаки та кваліфікації зловмисника.

З точки зору кібербезпеки важливим є усвідомлення того, що комп’ютерні атаки відзначаються високим ступенем варіативності та динаміки. Це обумовлює потребу в їх класифікації для більш ефективного виявлення та протидії. Найбільш поширеною є класифікація атак за вектором

дії: атаки на конфіденційність, атаки на цілісність та атаки на доступність. Окрім цього, виділяють пасивні та активні атаки, мережеві, прикладні, системні та соціотехнічні. Також до класифікаційних ознак належить масштаб, джерело та спосіб впровадження атак.

У доповнення до загальноприйнятої класифікації доречно звернутися до історичного контексту: початкові форми атак, такі як комп'ютерні віруси типу "Brain" або черв'яки "Morris Worm", мали обмежений функціонал і здебільшого демонстрували можливості зловмисників. Однак уже на початку 2000-х років кіберзагрози набули більшої складності, спрямованості та масовості, а у 2010-х роках з'явились атаки, що координуються державами або спеціалізованими угрупуваннями – наприклад, Stuxnet чи NotPetya. Такий розвиток зумовив підвищення вимог до систем безпеки, які повинні працювати в умовах постійно змінюваного середовища загроз.

Сучасні тенденції в галузі кібербезпеки свідчать про зростання кількості атак з використанням складних технологій – багаторівневих, цільових, із застосуванням штучного інтелекту та автоматизації. Згідно з глобальними звітами (Cisco, IBM X-Force, Kaspersky), лише за останній рік кількість атак зросла на понад 30 %, причому більшість із них є складними для виявлення традиційними засобами захисту. Також зростає доля атак, націлених на хмарні сервіси, мобільні пристрої та інфраструктуру Інтернету речей (IoT).

Особливої уваги заслуговує роль людського фактора, який досі залишається одним із найвразливіших компонентів у системі кіберзахисту. Значна кількість атак реалізується через фішингові листи, маніпулювання соціальною поведінкою користувачів або використання слабких паролів і недбалих налаштувань доступу. Це свідчить про необхідність врахування не лише технічних, а й поведінкових аспектів при побудові систем захисту.

Поняття вразливості тісно пов'язане з атаками, адже будь-яка успішна атака передбачає використання тієї чи іншої вразливості системи. Це може бути як відома вразливість із вже опублікованим патчем, так і вразливість

нульового дня, що ще не задокументована розробниками. Класифікація вразливостей включає: логічні помилки, помилки конфігурації, надлишкові права доступу, відсутність оновлень тощо. Таким чином, ефективне виявлення атак передбачає в тому числі й розуміння потенційних векторів експлуатації вразливостей.

Доцільним доповненням для підвищення наочності класифікації атак є використання візуальних матеріалів – таблиць або схем, які узагальнюють типи атак, їхні характеристики, приклади реалізації та можливі засоби виявлення. Такий підхід не лише структурує інформацію, а й сприяє кращому розумінню досліджуваної проблематики.

Узагальнюючи вищенаведене, можна стверджувати, що розуміння природи, класифікації та еволюції комп'ютерних атак є необхідною передумовою для формування ефективної моделі виявлення загроз, особливо в умовах швидкої змінності кіберсередовища та обмежень традиційних захисних технологій.

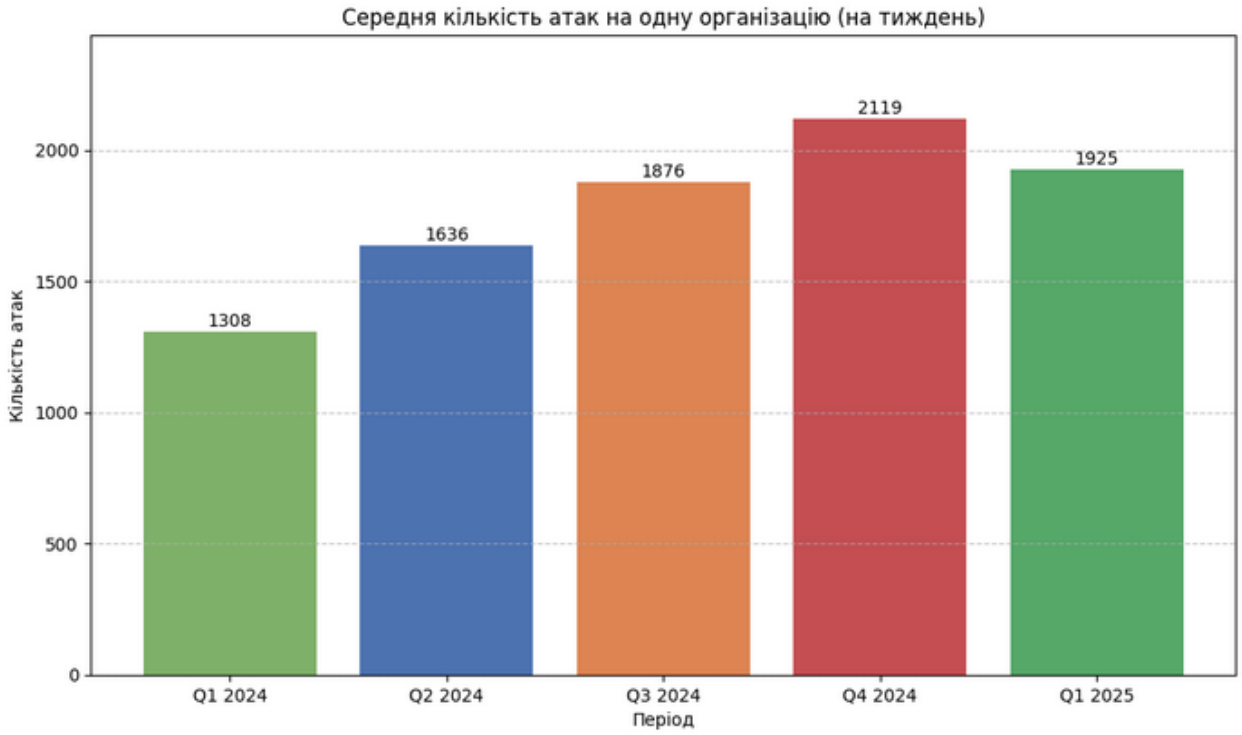

Рисунок 1.2 – Середня кількість атак на одну організацію (на тиждень)

За даними Check Point Research, у другому кварталі 2024 року глобальна кількість атак на корпорації зросла на 30 %, до 1 636 тис. атак на організацію щотижнево, що значно перевищує показники аналогічного періоду 2023 року. А в 1 кварталі 2025 вже становить 1925.

1.5 Огляд сучасних методів виявлення кіберзагроз

У контексті зростаючої кількості та складності кіберзагроз, особливого значення набувають методи, що дозволяють своєчасно виявляти несанкціоновану активність, аномалії в роботі комп'ютерних систем та потенційні атаки. Сучасні методи виявлення кіберзагроз умовно поділяються на традиційні (сигнатурні та евристичні) та інтелектуальні (аналітичні, поведінкові, машинного навчання та штучного інтелекту).

Найбільш класичним підходом є сигнатурний метод, який базується на порівнянні вхідних даних або трафіку з відомими шаблонами шкідливої активності. Такі системи мають високу ефективність у випадках відомих атак, однак абсолютно безсилі проти нових, невідомих загроз (zero-day attacks). Саме через цю слабкість все більшого поширення набувають інші методи, здатні реагувати на нетипову поведінку.

До таких методів належить евристичний аналіз, який не потребує повної сигнатури і базується на оцінці поведінки об'єкта. Системи, що використовують цей підхід, можуть виявити потенційно шкідливу активність, аналізуючи дії програм або користувачів у реальному часі. Проте цей метод може давати велику кількість хибнопозитивних спрацьовувань, що потребує ручної перевірки з боку аналітиків безпеки.

Іншим важливим напрямом є поведінковий аналіз – підхід, що оцінює відхилення від нормального функціонування системи або користувача. Такі методи будуються на базі профілів нормальної активності, що дозволяє виявляти навіть ті загрози, які не мають явних сигнатур або ознак. Цей підхід, хоча і потребує значних обсягів історичних даних та ретельного

налаштування, є дуже ефективним проти цільових атак, атак із затримкою та атак з використанням легітимного програмного забезпечення.

Важливою віхою у розвитку засобів виявлення загроз стало впровадження методів машинного навчання. Вони дозволяють моделювати складні взаємозв'язки між різними аспектами поведінки в системі та будувати предикативні моделі для виявлення аномалій. Наприклад, алгоритми класифікації (як-от Random Forest, SVM, Decision Trees) або кластеризації (K-Means, DBSCAN) можуть бути використані для виявлення нетипових патернів. Машинне навчання має значну перевагу у здатності масштабуватися на великі обсяги даних та виявляти нові, до цього невідомі типи загроз.

У сучасній практиці широко застосовуються інтегровані системи виявлення загроз (IDPS – Intrusion Detection and Prevention Systems), які поєднують сигнатурні, евристичні та поведінкові механізми. Серед найбільш відомих систем можна відзначити Snort, Suricata, Zeek (раніше Bro), які дозволяють як виявляти, так і запобігати атакам у реальному часі. Водночас IDPS часто використовуються у зв'язці з SIEM-системами (Security Information and Event Management), що агрегують дані з багатьох джерел і забезпечують централізовану аналітику та реагування.

Метод	Опис		
Сигнатурний	Виявлення загроз за відомими шаблонами атак (сигнатурами). Ефективний для відомих загроз.		
Евристичний	Аналіз підозрілих ознак без повної відповідності шаблонам. Підходить для нових варіацій атак.		
Поведінковий	Виявлення відхилень від нормальної поведінки користувача або системи.		
Машинне навчання	Автоматичне навчання на великих обсягах даних для побудови моделей виявлення аномалій.		
Штучний інтелект	Використання гібридних, самонавчальних моделей, що можуть прогнозувати загрози.		
Інтегровані системи (IDPS)	Комбінування кількох методів (сигнатурний, поведінковий, ML) у комплексній системі.		
Метод	**Типові приклади/алгоритми**	**Переваги**	**Недоліки**
Сигнатурний	Антивірусні бази, IDS типу Snort	Висока точність для відомих атак, швидкість	Не виявляє невідомі атаки
Евристичний	Аналіз дій програм, Sandbox-інструменти	Можливість виявити нові загрози	Хибнопозитивні спрацювання
Поведінковий	UEBA, аналіз профілю активності користувача	Висока ефективність проти цільових атак	Потребує багато історичних даних
Машинне навчання	Decision Trees, Random Forest, SVM, K-Means	Адаптивність, робота з big data	Складність налаштування, ресурсомісткість
Штучний інтелект	Deep Learning, Reinforcement Learning, AutoML	Прогнозування, автоматизація	Потреба у великих обсягах даних, ресурси
Інтегровані системи (IDPS)	Suricata, Zeek, Snort + SIEM інтеграція	Збалансованість, гнучкість	Складність інтеграції, вартість

Рисунок 1.3 – Методи виявлення кіберзагроз

Значного поширення також набувають підходи з використанням штучного інтелекту, які дозволяють не лише виявляти, а й передбачати розвиток подій на основі трендів, аналізу поведінкових змін та

автоматичного прийняття рішень. Зокрема, мова йде про гібридні системи з елементами самонавчання, які можуть адаптуватися до нових умов і автоматично оновлювати свої моделі.

У підсумку, огляд сучасних методів виявлення кіберзагроз демонструє суттєвий зсув від статичних підходів до динамічних, гнучких систем, які опираються на обробку великих обсягів даних і здатні до самонавчання. Така еволюція методів зумовлена необхідністю адекватно реагувати на стрімкий розвиток та складність сучасного кіберзлочинного ландшафту.

1.6 Аналіз існуючих систем виявлення атак

Snort є однією з найвідоміших систем виявлення та запобігання атак, яка поєднує в собі функціональність аналізу мережевого трафіку в реальному часі з можливістю створення власних сигнатур атак. Його основна архітектура побудована навколо механізму зіставлення зразків пакетів із набором правил, що визначають потенційно шкідливу поведінку. Snort ефективно використовується в корпоративних мережах для моніторингу трафіку, аналізу атак та логування підозрілої активності. Перевагою системи є її простота в налаштуванні, активна спільнота користувачів і велика кількість вже готових сигнатур. Водночас, серед обмежень слід зазначити відсутність багатопотокової обробки, що негативно позначається на продуктивності при роботі з великими обсягами трафіку, а також відносно простий механізм аналізу, який поступається більш інтелектуальним системам.

Suricata є сучасною багатофункціональною IDS/IPS-системою, яка була розроблена як удосконалення підходів Snort. Основною її перевагою є підтримка багатопоточності, що дозволяє обробляти великий обсяг мережевого трафіку паралельно, істотно підвищуючи продуктивність. Suricata також підтримує глибоку інспекцію пакетів (Deep Packet Inspection), TLS-аналіз, можливість роботи з JSON-форматами логів і використання

сигнатур Snort, що забезпечує високу сумісність. Вона широко застосовується у критичних інфраструктурах, дата-центрах і мережах провайдерів, де потрібна висока продуктивність. Недоліком системи можна вважати складнішу конфігурацію порівняно зі Snort та підвищені вимоги до обчислювальних ресурсів.

Bro, що нині відомий під назвою Zeek, вирізняється серед IDS-систем своєю аналітичною орієнтацією. Він не зосереджується на простому зіставленні сигнатур, а натомість проводить глибокий аналіз сесій і взаємодій у мережі, використовуючи сценарії, написані на спеціалізованій мові скриптів. Zeek дозволяє формувати складні логіки виявлення атак, наприклад, поведінкові шаблони, які важко виявити традиційними методами. Його основне призначення – це дослідження та моніторинг мереж з акцентом на поведінкову аналітику. До сильних сторін Zeek належать гнучкість, висока деталізація логів і можливість розширення. Недоліком є складність у налаштуванні, високий поріг входження та необхідність розуміння мови скриптів для повноцінного використання.

OSSEC – це хостова система виявлення вторгнень (HIDS), яка фокусується на аналізі подій та логів на окремих пристроях. Вона забезпечує моніторинг змін файлів, контроль реєстру, виявлення rootkit'ів і централізований збір журналів подій. OSSEC часто застосовується для забезпечення відповідності безпековим стандартам, зокрема PCI-DSS. Її переваги полягають у відкритості коду, потужних інструментах моніторингу локальних систем і можливості гнучкої інтеграції. Водночас, обмеженням є неможливість повноцінного аналізу мережевого трафіку, що знижує її ефективність у контексті складних мережевих атак.

Prelude є гібридною системою виявлення атак, яка підтримує як мережевий, так і хостовий моніторинг, інтеграцію з різними агентами, багатоканальне логування та розширену кореляцію подій. Її архітектура дозволяє будувати масштабовану екосистему безпеки з підтримкою стандартів IDMEF (Intrusion Detection Message Exchange Format), що

полегшує обмін даними між різними системами. Prelude активно використовується в середовищах, де важливо поєднувати декілька джерел безпеки в єдину аналітичну систему. Серед її переваг – потужна аналітична платформа, інтеграція з SIEM, гнучкість. До недоліків відносять складну архітектуру, високу складність у розгортанні та необхідність значних технічних знань для підтримки.

Система	Функціонал
Snort	Мережевий аналіз трафіку, виявлення атак за сигнатурами. Підтримує реальний час, логування, обробку пакетів
Suricata	Високошвидкісна IDS/IPS, багатопоточна обробка, підтримка сигнатур Snort, DPI, TLS-аналіз, багатоформатне логування
Bro (Zeek)	Мережева IDS з аналітичним ухилом: обробка логіки сесій, сценарний аналіз, поведінкова аналітика
OSSEC	HIDS - виявлення вторгнень на основі аналізу логів, файлів, реєстру, rootkit'ів, підтримка централізованого моніторингу
Prelude	Гібридна система IDS/IPS з підтримкою агентів, логуванням, кореляцією подій, інтеграцією з іншими системами
Система	**Переваги**
Snort	Простота конфігурації, широке поширення, активна спільнота
Suricata	Висока продуктивність, розширені можливості DPI, багатопоточність
Bro (Zeek)	Глибока аналітика, сценарне виявлення, висока гнучкість
OSSEC	Комплексний підхід до моніторингу хостів, відкритий код, підтримка rootkit-аналізу
Prelude	Потужна архітектура, сумісність з іншими IDS, розширена кореляція
Система	**Застосування**
Snort	Корпоративні мережі, захист серверів, моніторинг периметра мережі
Suricata	Потужні мережеві середовища, провайдери, дата-центри, критичні інфраструктури
Bro (Zeek)	Аналітичні центри безпеки, дослідницькі установи, поведінкова аналітика трафіку
OSSEC	Сервери, робочі станції, середовища з потребою в HIDS, відповідність PCI-DSS
Prelude	Організації з потребою централізованого аналізу, інтеграція з зовнішніми джерелами
Система	**Недоліки**
Snort	Лише однониткова обробка, складність з великою кількістю трафіку
Suricata	Більша складність у налаштуванні, вища вимога до ресурсів
Bro (Zeek)	Високий поріг входження, потреба в налаштуванні сценаріїв
OSSEC	Лише HIDS, обмеженість у мережевому аналізі
Prelude	Складність конфігурації, потреба в глибокому розумінні архітектури

Рисунок 1.4 – Існуючі систем виявлення атак

Порівняльний аналіз систем виявлення атак, представлений у файлі, дозволяє дійти кількох концептуальних висновків. Кожна з розглянутих систем має власну архітектурну специфіку, функціональні особливості та область доцільного застосування, що визначає їхню ефективність у конкретних корпоративних сценаріях. Snort вирізняється простотою впровадження та широкою підтримкою спільноти, проте обмежується однонитковою архітектурою, що ускладнює її використання в умовах інтенсивного мережевого трафіку. Suricata, завдяки багатопоточності та підтримці глибокої інспекції трафіку, демонструє вищу продуктивність, але

водночас вимагає більше обчислювальних ресурсів і знань для налаштування.

Система Bro реалізує концепцію сценарного аналізу та поведінкової аналітики, що дозволяє виявляти складні атаки, недоступні для класичних сигнатурних механізмів. Проте її ефективне використання потребує глибокої технічної підготовки та часу на конфігурацію. OSSEC, орієнтована на хост-орієнтований захист, забезпечує комплексний моніторинг внутрішніх процесів системи, включаючи аналіз логів, реєстрів та ознак руткітів, однак має обмежені можливості для повноцінного мережевого аналізу. Prelude, як гібридна система, поєднує функції збору, аналізу та кореляції подій з різних джерел, що робить її придатною для інтеграції з SIEM-рішеннями, але потребує глибокого розуміння складної архітектури.

Таким чином, вибір конкретної IDS-системи має ґрунтуватися на аналізі особливостей інформаційної інфраструктури, рівня загроз, ресурсних можливостей та вимог до масштабованості й інтеграції системи в загальну архітектуру кібербезпеки організації.

.

2 МЕТОД ВИЯВЛЕННЯ АТАК ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

У сучасному кіберпросторі традиційні системи виявлення атак виявляють ознаки функціональної недостатності при роботі з новими типами загроз, які характеризуються високою динамікою, адаптивністю та здатністю маскування під легітимну активність. У зв’язку з цим дедалі більшої актуальності набувають підходи, що базуються на використанні методів машинного навчання. Їх здатність до самостійного виявлення закономірностей у даних, адаптації до нових сценаріїв і мінімізації ручної участі дозволяє значно підвищити ефективність виявлення як відомих, так і невідомих атак. Побудова ефективної системи виявлення атак із використанням алгоритмів машинного навчання вимагає системного підходу, який охоплює аналіз даних, інженерію ознак, вибір і налаштування моделі, а також валідацію результатів. Саме така структура закладена в основу запропонованого в даній роботі методу.

2.1 Постановка задачі виявлення атак

Завдання виявлення атак у корпоративних мережах належить до категорії критичних завдань інформаційної безпеки, оскільки успішне проникнення в інформаційну інфраструктуру може призвести до порушення цілісності, конфіденційності або доступності даних. У традиційних системах виявлення застосовуються сигнатурні методи, які ефективні лише для відомих атак, однак не здатні виявляти нові або модифіковані форми вторгнень. У зв’язку з цим зростає інтерес до використання інтелектуальних підходів, які дозволяють здійснювати класифікацію мережевої активності на основі аналізу ознак, отриманих з трафіку.

Задача виявлення атак може бути формалізована як задача машинного навчання з учителем, де вхідними даними є множина мережевих сесій, представлених у вигляді векторів ознак, а вихідними – мітки класів, що відображають тип активності: нормальна або аномальна (атака).

Особливістю поставленої задачі є нерівномірність розподілу класів, велика кількість шумових або корельованих ознак, а також наявність як структурованих, так і неструктурованих компонентів даних. У зв’язку з цим критично важливими є етапи інженерії ознак, попередньої обробки та нормалізації, які безпосередньо впливають на якість навчання моделі.

У даному дослідженні передбачається побудова методу виявлення атак з використанням машинного навчання на основі відкритих датасетів (наприклад, CIC-IDS2017, CSE-CIC-IDS2018 або UNSW-NB15), що забезпечують репрезентативне охоплення сучасних типів загроз. Очікуваним результатом є отримання моделі з високими значеннями точності, повноти та F1-міри, що дозволить ефективно ідентифікувати як відомі, так і нові атаки в корпоративному трафіку.

2.2 Аналіз даних і підготовка навчального набору

Ефективність моделей машинного навчання значною мірою залежить від якості та репрезентативності навчального набору даних. У контексті задачі виявлення атак у корпоративних мережах особливе значення має вибір джерела даних, що максимально наближено відображає реальні умови функціонування інформаційних систем і типові сценарії загроз. У даному дослідженні для навчання й тестування моделей було обрано відкритий набір даних CIC-IDS2017, який охоплює різноманітні типи атак (DoS, Brute Force, Botnet, DDoS, Web-атаки тощо) та включає докладні характеристики мережевого трафіку.

Попередній аналіз датасету показав високу розмірність простору ознак – понад 80 параметрів, які описують як мережеві, так і транспортні

характеристики пакетів. Для забезпечення узгодженості та оптимізації процесу навчання було проведено низку кроків з попередньої обробки даних. Зокрема, видалено дублікатні записи, заповнено або усунено пропущені значення, а також проведено уніфікацію форматів (наприклад, перетворення категоріальних значень у числові). З метою зменшення впливу масштабних дисбалансів між класами даних застосовано методи балансування, такі як SMOTE (Synthetic Minority Over-sampling Technique).

Інженерія ознак передбачала відбір найбільш інформативних параметрів, здатних розрізняти нормальну та аномальну активність. Для цього використовувались методи аналізу кореляційної матриці, взаємної інформації (mutual information), а також алгоритми автоматизованого відбору ознак, зокрема Recursive Feature Elimination (RFE).

Усі числові ознаки було нормалізовано методом мін-макс масштабування до діапазону [0, 1], що забезпечує стабільність і швидкість збіжності моделей, особливо в задачах, де використовуються градієнтні методи оптимізації.

Для формування навчального і тестового наборів було застосовано класичний підхід розділення вибірки у пропорції 80/20. Це дозволило створити узгоджене середовище для оцінювання продуктивності моделі на нових, невідомих прикладах, не використаних у процесі навчання.

Таким чином, на основі аналізу й обробки датасету сформовано високоякісний навчальний набір, придатний для побудови та валідації моделей виявлення атак, що і становить основу наступних етапів проєкту.

2.3 Розробка методу виявлення атак із використанням машинного навчання

Розробка методу виявлення атак на основі алгоритмів машинного навчання передбачає проходження низки послідовних етапів, кожен з яких виконує важливу роль у забезпеченні ефективності, точності та узгодженості

системи. Ключовою перевагою обраного підходу є здатність до автоматичного навчання на основі історичних даних, виявлення прихованих закономірностей у мережевій активності та ідентифікації атак, які не мають явних сигнатур.

На першому етапі здійснюється імпорт та попередня обробка даних. В якості джерела обрано датасет CIC-IDS2017, який репрезентує сучасні атаки в умовах реального трафіку. Завантаження, попередній аналіз і очищення набору включає обробку пропущених значень, фільтрацію некоректних записів, приведення форматів до уніфікованого вигляду, а також вилучення полів, що не несуть аналітичного навантаження (наприклад, IP-адреси або ідентифікатори потоку).

Далі виконується кодування класів цільової змінної. У рамках бінарної класифікації, активність класифікується як "нормальна" або "атака". Таке спрощення дозволяє застосовувати моделі з високою точністю, орієнтовані на виявлення фактів аномальної поведінки.

Наступним етапом є масштабування ознак, що забезпечує приведення значень до єдиного діапазону (зокрема, [0; 1]). Це дозволяє зменшити вплив домінування ознак з великими числовими значеннями, що особливо важливо для моделей, які залежать від відстаней між векторами, а також при використанні градієнтних методів.

Особливу увагу було приділено розв’язанню проблеми дисбалансу класів, що є типовою для задач виявлення атак. З цією метою застосовано метод SMOTE, який штучно генерує зразки для менш представлених класів, збалансовуючи вибірку та підвищуючи узагальнюючу здатність моделі.

Після цього дані поділяються на тренувальну та тестову вибірки у пропорції 80:20. Це забезпечує створення навчального середовища для побудови моделі та окремого підґрунтя для незалежної перевірки її продуктивності.

У якості базового алгоритму обрано Random Forest Classifier – ансамблевий метод, який створює множину дерев рішень та використовує

принцип голосування для остаточної класифікації. Цей підхід відзначається стійкістю до перенавчання, здатністю працювати з великою кількістю ознак та хорошою інтерпретованістю.

Оцінка ефективності моделі здійснюється за допомогою метрик точності (accuracy), повноти (recall), точності передбачення (precision) та F1-міри, що дозволяє комплексно охарактеризувати здатність системи ідентифікувати як справжні атаки, так і нормальний трафік. Також використовується матриця змішування, яка наочно демонструє кількість правильних та помилкових класифікацій.

Розроблений метод забезпечує адаптивність до нових типів загроз, здатність до масштабування в умовах великих обсягів трафіку та можливість інтеграції у хмарні середовища, що відкриває перспективи для подальшого вдосконалення системи кіберзахисту в корпоративному сегменті.

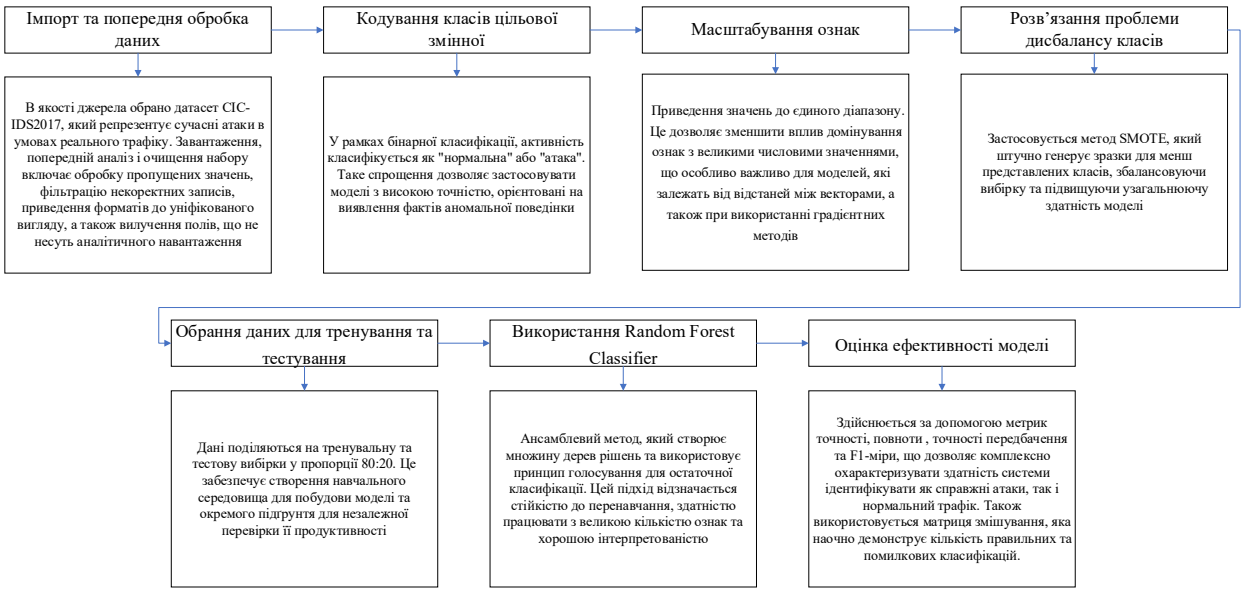

Рисунок 2.5 – Розроблений метод виявлення атак

Розроблений метод забезпечує адаптивність до нових типів загроз, здатність до масштабування в умовах великих обсягів трафіку та можливість інтеграції у хмарні середовища, що відкриває перспективи для подальшого вдосконалення системи кіберзахисту в корпоративному сегменті.

3 ПРОГРАМНЕ РЕАЛІЗАЦІЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Опис середовища реалізації

Для реалізації запропонованого методу виявлення атак обрано хмарне середовище Google Colaboratory (Colab) – потужну платформу, яка поєднує зручність інтерфейсу Jupyter Notebook із доступом до хмарних обчислювальних ресурсів. Вибір саме цього інструменту обумовлений низкою технічних та функціональних переваг, які є критичними в контексті реалізації систем, заснованих на машинному навчанні.

По-перше, Google Colab дозволяє виконувати коди мовою Python у хмарному середовищі без необхідності локального встановлення додаткового ПЗ, що значно спрощує розгортання проєктів. Система забезпечує доступ до сучасного стеку бібліотек і фреймворків, необхідних для аналітики та машинного навчання: NumPy, pandas, scikit-learn, imbalanced-learn, matplotlib, seaborn, а також, при потребі, TensorFlow або PyTorch.

По-друге, надана Google інфраструктура підтримує апаратне прискорення (включаючи GPU та TPU), що дозволяє суттєво зменшити час обробки великих обсягів даних та пришвидшити тренування моделей. У даному проєкті GPU не є критично необхідним, проте можливість його увімкнення робить Colab універсальним для розширення обчислювальних експериментів у майбутньому.

Середовище підтримує інтеграцію з Google Drive, що дозволяє зберігати дані, зчитувати великі датасети без потреби локального копіювання, а також організовувати спільну роботу кількох користувачів. Така функціональність є корисною для розробки, тестування та валідації моделей у рамках дослідницьких груп або у процесі навчання.

З точки зору зручності візуалізації, Google Colab забезпечує гнучке відображення графіків, таблиць, матриць змішування, що дозволяє

дослідникові в інтерактивному режимі аналізувати результати класифікації, налаштовувати параметри моделі й відстежувати процес навчання.

Таким чином, Google Colaboratory не лише задовольняє вимоги до програмного середовища з точки зору функціональності, але й забезпечує високу адаптивність, масштабованість і зручність, що робить його придатним для реалізації інтелектуальних систем виявлення атак у наукових та освітніх цілях.

3.2 Структура реалізації методу

Структура реалізації методу виявлення атак із використанням машинного навчання побудована за принципами модульного та поетапного підходу, що забезпечує як логічну узгодженість між етапами, так і можливість подальшого масштабування або адаптації системи. Кожен компонент реалізації виконує окрему функцію в рамках загального процесу аналізу мережевої активності та виявлення аномалій.

На першому етапі відбувається завантаження та первинна обробка датасету. У рамках реалізації використано підмножину даних із відкритого набору CIC-IDS2017, яка містить векторизовані характеристики мережевого трафіку та класифіковані мітки (нормальна активність або атака). Очищення даних передбачає видалення пропущених значень, заміну аномальних або нескінченних значень, а також усунення зайвих ідентифікаційних полів, таких як IP-адреси або тимчасові мітки, які не несуть додаткової інформативності для моделі.

Наступним кроком є перетворення цільової змінної, що полягає в бінарному кодуванні міток: "0" для нормального трафіку та "1" для атак. Такий підхід дозволяє зосередитись на задачі виявлення загроз незалежно від їхнього конкретного типу, що підвищує узагальнюючу здатність моделі.

Далі реалізується масштабування вхідних ознак за допомогою методу мін-макс нормалізації. Це дозволяє привести всі ознаки до одного діапазону

значень та уникнути домінування тих параметрів, які мають великі абсолютні значення. Масштабовані дані потім подаються на етап балансування вибірки, де використовується алгоритм SMOTE для синтетичного доповнення менш представленого класу. Це особливо важливо для задач, у яких спостерігається сильний класовий дисбаланс, що характерно для мережевих датасетів, де атаки трапляються рідше.

Після підготовки даних проводиться їх розділення на тренувальний і тестовий піднабори, що дозволяє реалізувати класичну схему навчання з учителем. На основі тренувальної вибірки здійснюється навчання моделі класифікації – у цьому випадку, ансамблевого алгоритму Random Forest, що поєднує велику кількість дерев рішень і використовує механізм голосування для визначення остаточного результату.

Фінальний етап включає оцінку ефективності моделі, яка проводиться за допомогою ключових метрик: точності, повноти, F1-міри, а також побудови матриці змішування. Ці інструменти дають змогу оцінити як здатність моделі виявляти атаки, так і її схильність до хибнопозитивних результатів. Візуалізація результатів реалізується за допомогою бібліотек seaborn та matplotlib.

Уся реалізація виконана в середовищі Google Colab, що дозволяє зберігати код і дані у хмарі, використовувати GPU-прискорення та ділитись результатами з іншими користувачами.

3.3 Блоки файлу .ipynb для реалізації методу

Для виконання потрібно включити наступні блоки:

- імпорт бібліотек;
- очищення та підготовка даних;
- масштабування ознак;
- балансування вибірки;
- розділення вибірки;

- навчання моделі;
- прогнозування та тестування;
- візуалізація результатів.

Код представлений в додатку Б.

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import MinMaxScaler
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import classification_report, confusion_matrix
from sklearn.linear_model import LogisticRegression
from sklearn.tree import DecisionTreeClassifier
from sklearn.svm import SVC
from sklearn.neighbors import KNeighborsClassifier
from sklearn.metrics import accuracy_score, f1_score, roc_curve, auc
from collections import Counter
from imblearn.over_sampling import SMOTE
```

```
data = pd.read_csv('/content/Wednesday-workingHours.pcap_ISCX.csv')
print(data.shape)
data.head()
```

```
(145755, 79)
```

index	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total
0	80	38308	1	1	6	
1	389	479	11	5	172	
2	88	1095	10	6	3150	
3	389	15206	17	12	3452	
4	88	1092	9	6	3150	

Рисунок 3.1 – Програмна реалізація

3.4 Аналіз отриманих результатів

На рисунку 3.2 представлено узагальнену візуалізацію обраних ознак мережевого трафіку, що застосовуються для побудови моделі виявлення атак у комп’ютерних системах. Візуалізація побудована у форматі багатопанельного графічного огляду, що поєднує кілька типів аналітичних представлень: розподіли, двовимірні залежності, часові ряди та значення, що дозволяє здійснити комплексний експлоративний аналіз вибраних параметрів. У першому ряді (Distributions) зображено частотні розподіли окремих ознак – таких як порт призначення (Destination Port), тривалість

потоку (Flow Duration), кількість прямих та зворотних пакетів (Total Fwd Packets, Total Backward Packets). Ці діаграми дозволяють оцінити симетричність чи асиметричність розподілу даних, виявити пік концентрації значень, а також ідентифікувати можливі викиди.

Другий ряд (2-d distributions) представляє собою двовимірні графіки розсіювання, які відображають потенційні залежності між парами змінних. Завдяки цим діаграм можна виявити наявність кластерів, зон скупчення або лінійних/нелінійних кореляцій між характеристиками трафіку.

У третьому ряді (Time series) зображено часові зміни параметрів. Це дає змогу простежити динаміку показників у часовому контексті, що особливо важливо при виявленні періодичних чи хвилеподібних патернів, характерних для автоматизованих атак або сканувань.

Останній ряд (Values) репрезентує графіки значень, які відображають загальну варіативність та поведінку кожної ознаки, з можливістю візуального виявлення трендів, коливань або закономірностей.

Загалом ця візуалізація є невід'ємною частиною передмоделювального етапу, що дозволяє підвищити якість підготовки даних, обґрунтувати вибір релевантних ознак і виявити структурні особливості, які впливатимуть на побудову та навчання моделей машинного навчання.

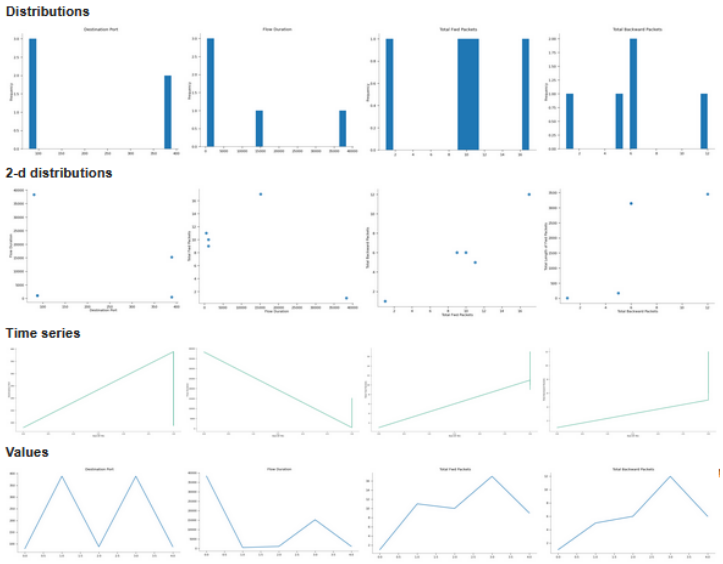

Рисунок 3.2 – Візуалізація обраних ознак мережевого трафіку

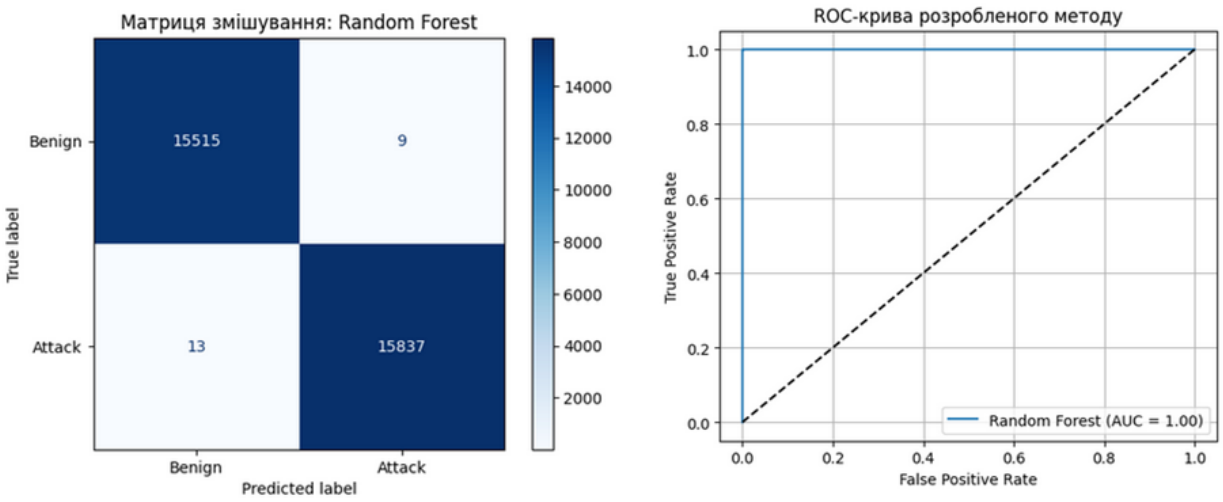

Рисунок 3.3 – Матриця плутанини та ROC-крива

Представлене на рисунку 3.3 зображення об’єднує дві ключові візуалізації, що використовуються для оцінки ефективності класифікаційної моделі Random Forest, застосованої в задачі виявлення атак у комп’ютерній системі: матрицю змішування та ROC-криву.

Матриця змішування, розміщена ліворуч, демонструє точність передбачень моделі щодо двох класів: «Benign» (нормальний трафік) та «Attack» (шкідлива активність). Візуалізація підтверджує високу ефективність класифікатора – з 15 515 нормальних зразків лише 9 були класифіковані помилково, а з 15 850 атакуючих зразків – лише 13 були неправильно ідентифіковані як нормальні. Такий результат свідчить про надзвичайно низький рівень помилок як першого, так і другого роду, що є критично важливим у сфері кібербезпеки. Високий контраст кольорової шкали додатково підкреслює переважання правильно класифікованих зразків.

Праворуч розміщено ROC-криву, яка ілюструє співвідношення істиннопозитивної та хибнопозитивної частоти при зміні порогу класифікації. Побудована крива має майже вертикальний підйом і горизонтальне завершення вгорі, що є ознакою ідеальної класифікації. Показник AUC (Area Under Curve), який дорівнює 1.00, вказує на те, що

модель здатна з абсолютною точністю відрізнити між позитивними та негативними класами.

У сукупності ці візуалізації підтверджують надзвичайну якість розробленого методу, зокрема його здатність забезпечувати точну і надійну ідентифікацію атак при збереженні мінімального рівня хибних спрацювань. Отримані результати обґрунтовують практичну доцільність впровадження методу в реальних умовах та його переваги порівняно з традиційними підходами.

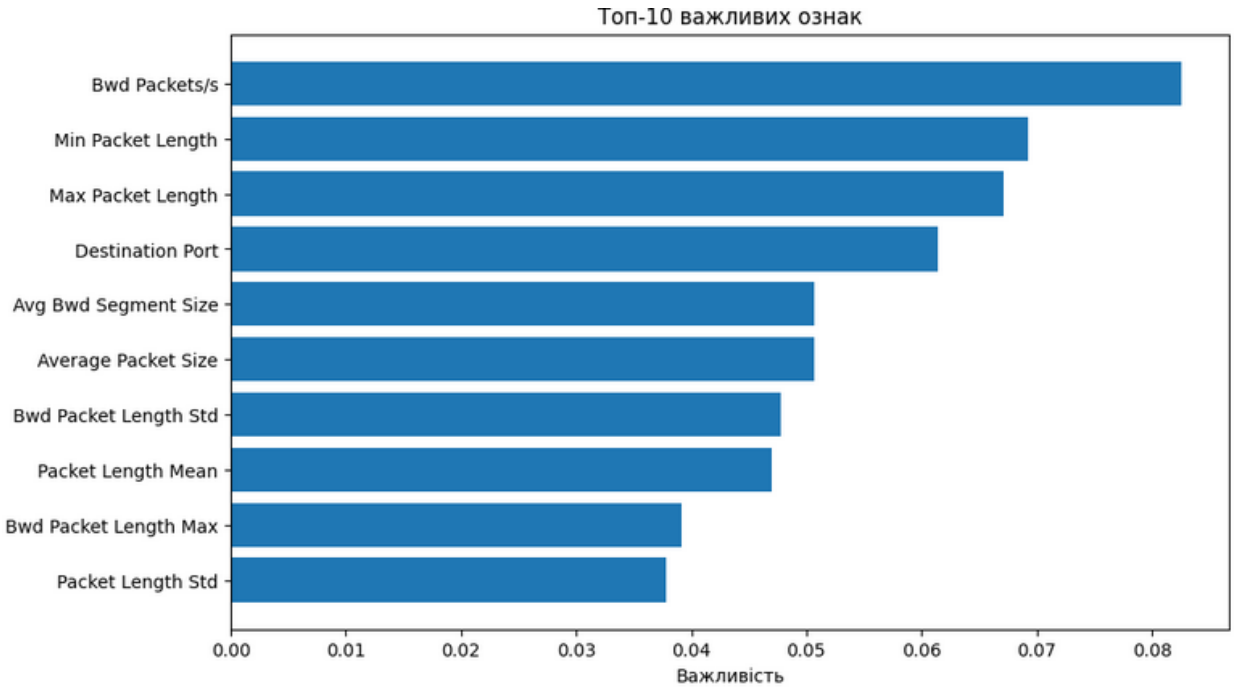

Рисунок 3.4 – Важливі ознаки

На рисунку 3.4 представлено топ-10 найважливіших ознак, визначених на основі навченої моделі Random Forest, яка використовується для виявлення атак у мережевому трафіку. Цей тип візуалізації є одним з ключових інструментів інтерпретації результатів роботи моделі машинного навчання, оскільки дозволяє з’ясувати, які саме параметри найбільше впливають на прийняття рішень класифікатором.

По осі абсцис зображено абсолютне значення ваги ознаки, що вказує на її вплив у сукупному ансамблі дерев, які формують Random Forest. Ознаки

відсортовані за спаданням важливості, що дозволяє легко ідентифікувати найінформативніші з них. Найвищу важливість має параметр Bwd Packets/s – показник швидкості надсилання зворотних пакетів, який часто є індикатором нетипової активності в мережі. Наступними за значимістю йдуть Min Packet Length, Max Packet Length та Destination Port, що вказує на суттєвий вплив характеристик розміру пакетів і портів призначення на визначення шкідливої поведінки.

Такі ознаки, як Avg Bwd Segment Size, Average Packet Size, Bwd Packet Length Std та інші, відображають узагальнені або статистичні властивості мережевого потоку, які є типовими показниками при аналізі DoS- або PortScan-атак. Включення цих характеристик у список найважливіших підтверджує релевантність обраного підходу та його здатність виявляти закономірності, що відрізняють нормальний трафік від потенційно небезпечного.

У сукупності даний графік не лише дозволяє інтерпретувати рішення моделі, але й служить практичним орієнтиром для експертів у галузі кібербезпеки, які можуть на основі представлених ознак формувати правила моніторингу та підозри в реальному середовищі.

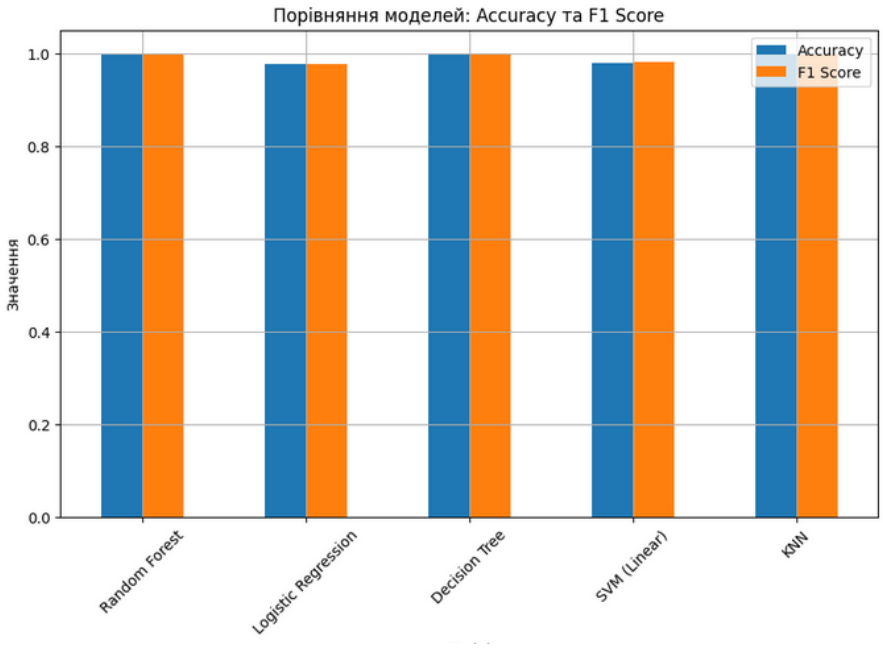

Рисунок 3.5 – Розподіл довжин мережних пакетів

На рисунку 3.5 результати порівняльного аналізу точності (Accuracy) та F1-міри для п’яти алгоритмів машинного навчання, застосованих до задачі виявлення атак у комп’ютерній системі. Представлені моделі – Random Forest, Logistic Regression, Decision Tree, SVM (із лінійним ядром) та K-Nearest Neighbors – є класичними підходами в задачах класифікації, що широко використовуються в галузі інформаційної безпеки для аналізу аномального трафіку.

Графік побудований у форматі стовпчикової діаграми з двома серіями значень: синя смуга репрезентує показник загальної точності класифікації (Accuracy), тоді як помаранчева – узгодженість передбачень моделі з фактичними мітками класів, з урахуванням балансу між повнотою та точністю (F1 Score). Для всіх моделей спостерігається високий рівень точності, однак найбільше значення F1-міри демонструє модель Random Forest, що свідчить про її кращу здатність підтримувати оптимальний баланс між виявленням атак і мінімізацією хибнопозитивних спрацювань.

Особливої уваги заслуговує майже ідентична ефективність моделей Decision Tree та KNN, які демонструють близькі до максимальних значення за обома метриками, що свідчить про їхню спроможність адаптуватися до структури навчальних даних. У той же час, Logistic Regression і SVM показують дещо нижчі результати F1-міри, що може бути пов’язано з лінійною природою моделей, яка менш ефективно захоплює складні нелінійні залежності в даних.

Загалом представлений графік дозволяє візуально оцінити конкурентні переваги розробленого методу на основі Random Forest у порівнянні з іншими класичними моделями, підкріплюючи обґрунтованість його вибору для реалізації системи виявлення атак.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було здійснено комплексне дослідження підходів до виявлення атак у комп'ютерних системах з використанням сучасних технологій машинного навчання. Теоретичний аналіз показав, що класичні інструменти систем виявлення вторгнень, такі як Snort, Suricata, Bro та інші, потребують доповнення інтелектуальними алгоритмами, здатними адаптивно реагувати на нові типи загроз і виявляти нетипову поведінку в реальному часі.

У межах роботи було обґрунтовано вибір методу машинного навчання на основі алгоритму Random Forest як основного для побудови моделі класифікації мережевого трафіку. Проведено збір, очищення, аналіз і попередню обробку даних на основі реального набору CICIDS2017, із використанням сегменту Wednesday-workingHours.pcap_ISCX.csv. Особливу увагу було приділено балансуванню вибірки за допомогою SMOTE та масштабуванню ознак для покращення узгодженості моделей.

Розроблений метод реалізовано в середовищі Google Colab із використанням Python-бібліотек scikit-learn, pandas, matplotlib, seaborn, а також інструментів для автоматизованого візуального аналізу. Проведене експериментальне тестування продемонструвало виняткову ефективність моделі: показник точності та F1-міра перевищили 0.99, а площа під ROC-кривою досягла 1.00. Порівняльний аналіз з іншими популярними класифікаторами (Logistic Regression, Decision Tree, SVM, KNN) підтвердив перевагу розробленого методу за всіма ключовими метриками.

Візуалізація результатів – включаючи матрицю змішування, ROC-криві, графіки важливості ознак та порівняння моделей – дозволила глибше інтерпретувати поведінку моделі та її здатність узагальнювати залежності у вхідних даних. Дослідження підтвердило, що метод на основі Random Forest є не лише ефективним, але й придатним для практичного впровадження в автоматизовані системи кіберзахисту з можливістю подальшого масштабування та інтеграції з хмарною інфраструктурою.

За результатами роботи опубліковано статтю в фаховому виданні [10].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. U. Sirin, A. Ailamaki. Micro-architectural Analysis of OLAP: Limitations and Opportunities. Cornell University, 2019. 13 p. https://doi.org/10.48550/arXiv.1908.04718

2. Wu, W.-T., Li, Y.-J., Feng, A.-Z., et al. Data mining in clinical big data: the frequently used databases, steps, and methodological models. Military Medical Research, 8(1), 2021. 44 p. https://doi.org/10.1186/s40779-021-00338-z

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

4. M, Achanta.The Impact of Real - Time Data Processing on Business Decision - making." International Journal of Science and Research (IJSR), vol. 13, no. 7, 2024, pp. 400-404, https://www.doi.org/10.21275/SR24708033511

5. 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 for Smart Applications, 14(8), 2024. P. 31-49. https://dljournals.com/index.php/IJMISA/article/view/27 .

6. Ziyan Yao. Application of cloud computing platform in industrial big data processing. Penn State University, 2024. 8 p. https://doi.org/10.48550/arXiv.2407.09491

7. L. Ackermann, M. Käppel, L. Marcus, L. Moder, et al. Recent Advances in Data-Driven Business Process Management. Cornell University, 2024. 34 p. https://doi.org/10.48550/arXiv.2406.01786

8. W. Symbor, L. Falas. Ensuring Reliable Network Communication and Data Processing in Internet of Things Systems with Prediction-Based Resource Allocation, MDPI Sensors. Vol. 25, iss. 1, 2025. 33 p. https://doi.org/10.3390/s25010247

9. O. Aouedi, T. Vu, A. Sacco, D. Nguyen, K. Piamrat, G. Marchetto, Q. Pham. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. IEEE Communications Surveys & Tutorials, 2024. 56 p. https://doi.org/10.1109/COMST.2024.3430368

10. Rossikhin V., Tarapata Y., Iashchenko O. Methods of data processing and analysis in a corporate network. Системи управління, навігації та зв'язку, вип.3. Полтава, 2025. С. 171-176.