Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Дослідження шляхів підвищення точності виявлення аномалій для застосування в IDS системах"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Липянчик Ростислав Сергійович
підпис (прізвище та ініціали)

Керівник Скарга-Бандурова І.С.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Липянчику Ростиславу Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи "Дослідження шляхів підвищення точності виявлення аномалій для застосування в IDS системах

Керівник роботи Скарга-Бандурова Інна Сергіївна, д.т.н., професор кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «22» 11 2024 року № 4/7-1119

2. Термін подання студентом завершеної роботи 20.12.2024

3. Вихідні дані до роботи
Літературні джерела, набір даних CICIDS 2017

4. Зміст роботи (перелік питань, які потрібно розробити)
Методи та засоби захисту комп'ютерних мереж
Теоретичні основи побудови систем виявлення вторгнень на основі аномалій
Шляхи вдосконалення виявлення аномалій мережевого трафіку

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
CIA тріада, Засоби мережевого захисту від загроз, IDS vs IPS
Класифікація систем виявлення вторгнень (IDS) за місцем встановлення
Класифікація систем виявлення вторгнень (IDS) за способом виявлення атак
Основні групи методів виявлення аномалій
Алгоритм запропонованого підходу до виявлення мережевих атак, як аномалій
Інструменти збору ознак мережевого трафіку, Метод головних компонент (PCA)
Метрики класифікації, Вплив кількості головних компонент на точність
Результати тестування, Порівняльний аналіз впливу програмних інструментів збору ознак з трафіку на точність класифікації Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 23.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	23.09 – 25.09	*Виконано*
2.	Підбір наукових джерел про способи і засоби виявлення вторгнень	26.09-13.10	*Виконано*
3.	Переклад та опрацювання наукових джерел про теоретичні підходи виявлення аномалій	14.10-25.10	*Виконано*
4.	Виконання дослідження щодо пошуку шляхів підвищення ефективності виявлення аномалій	26.10-10.11	*Виконано*
5.	Виконання експериментальних досліджень	11.11-20.11	*Виконано*
6.	Оформлення розділу «Методи та засоби захисту комп'ютерних мереж»	21.11-25.11	*Виконано*
7.	Оформлення розділу «Теоретичні основи побудови систем виявлення вторгнень на основі аномалій»	26.11-30.11	*Виконано*
8.	Оформлення розділу «Шляхи вдосконалення виявлення аномалій мережевого трафіку»	01.12-05.12	*Виконано*
9.	Виконання завдання до підрозділу «Охорона праці»	04.12-08.12	*Виконано*
10.	Виконання завдання до підрозділу «Безпека в надзвичай них ситуаціях»	04.12-08.12	*Виконано*
11.	Оформлення кваліфікаційної роботи	01.12-08.12	*Виконано*
12.	Нормоконтроль	09.12 – 11.12	*Виконано*
13.	Перевірка на плагіат	12.12 – 15.12	*Виконано*
14.	Попередній захист кваліфікаційної роботи	16.12 – 20.12	*Виконано*
15.	Захист кваліфікаційної роботи	28.12.2024	

Студент _____ Липянчик Р.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Скарга-Бандурова І.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження шляхів підвищення точності виявлення аномалій для застосування в IDS системах// ОР «Магістр» // Липянчик Ростислав Сергійович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2024 // С. 73, рис. – 14, табл. – - 8, кресл. – __, додат. – 2.

Ключові слова: ВТОРНЕННЯ, МАШИННЕ НАВЧАННЯ, АНОМАЛІЇ, IDS.

Кваліфікаційна робота присвячена дослідженню шляхам підвищення ефективності виявлення вторгнень, як пошуку аномалій мережевого трафіку, для подальшого вдосконалення систем виявлення вторгень (IDS)

В першому розділі здійснено огляд основних загроз при передачі даних в мережів та основних засобів захисту комп'ютерних мереж. Більш детально проаналізовано системи виявлення вторгнень, їх види та принципи роботи.

В другому розділі кваліфікаційної роботи наведено основні теоретичні підходи до визначення аномалій.

В третьому розділі запропоновано підхід ансамблювання результатів різних моделей та коротко описано основні етапи підходу. Також проведено аналіз впливу на якість визначення вторгнень різних інструментів вилучення ознак з мережевого трафіку та впливу розміру простору ознак на кінцеву якість класифікаційної моделі.

ABSTRACT

Research on Improving Anomaly Detection Accuracy for Use in IDS Systems // Thesis of educational level "Master"// Rostyslav Lypianchyk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБмз-61 // Ternopil, 2024// P. 73, figs. 14, tables 8, drawings __ added. – 2.

Keywords: INTRUSION, MACHINE LEARNING, ANOMALY, IDS

The qualification thesis is devoted to the study of ways to increase the efficiency of intrusion detection, as network traffic anomalies identification, for further improvement of intrusion detection systems (IDS)

The first section provides an overview of the main threats to network data transmission and the main means of protecting computer networks. Intrusion detection systems, their types and principles of operation are analyzed in more detail.

The second section of the thesis presents the main theoretical approaches to anomaly detection.

The third section proposes an approach to ensemble the results of different models and briefly describes the main stages of the approach. The paper also analyzes the impact on the quality of intrusion detection of various tools for extracting features from network traffic and the impact of the size of the feature space on the final quality of the classification model.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DoS	—	Denial of Service
IDS	—	Intrusion Detection System
DNS	—	Domain Name System
APT	—	Advanced Persistent Threat
IT	—	Information Technologies
SIEM	—	Security Information and Event Management
SOC	—	Security Operation Center
NAC	—	Network Access Control
DM	—	Data Mining
ML	—	Machine Learning
kNN	—	k Nearest Neighbors
SVM	—	Support Vector Machine
PCA	—	Principal Component Analysis
API	—	Application Programming Interface

ВСТУП

Актуальність теми. Сучасний світ стрімко розвивається завдяки цифровим технологіям, які проникають у всі сфери життя: від бізнесу та фінансів до охорони здоров'я та державного управління. Разом із цим зростає і складність кіберзагроз, які стають все більш численними, витонченими та масштабними. Атаки на інформаційні системи стають серйозною загрозою для безпеки даних, конфіденційності користувачів, а також стабільності критично важливих інфраструктур.

За даними світових аналітичних компаній, кількість кібератак щороку збільшується [1]. Це включає не лише традиційні атаки (наприклад, DDoS, фішинг), але й нові складні загрози, такі як атаки на основі штучного інтелекту або шкідливе програмне забезпечення, яке адаптується в реальному часі. Про це свідчать дані IBM® X-Force® Threat Intelligence Index 2024, що ґрунтується на висновках і спостереженнях, отриманих в результаті моніторингу понад 150 мільярдів подій безпеки на день у більш ніж 130 країнах світу [2].

Системи виявлення вторгнень (IDS) є ключовим компонентом сучасних рішень у сфері кібербезпеки. Вони забезпечують моніторинг мережі, виявлення шкідливих дій і реагування на потенційні загрози. Проте розвиток кіберзагроз і збільшення складності сучасних IT-інфраструктур створюють нові виклики, які вимагають вдосконалення IDS. Зокрема, сучасні загрози, такі як атаки нульового дня, складні цільові атаки (APT) та шкідливе програмне забезпечення, що постійно адаптується, значно ускладнюють виявлення. Традиційні IDS, засновані на сигнатурних методах, не можуть ефективно протидіяти таким загрозам. Поява нових видів атак, які важко виявити за допомогою стандартних методів, ставить під загрозу традиційні системи виявлення вторгнень.

Крім того, у сучасних мережах генерується величезна кількість даних, які необхідно обробляти в реальному часі. Це ставить виклик перед IDS-системами, які повинні залишатися ефективними навіть у масштабованих середовищах.

Виявлення аномалій є ефективним підходом до створення систем виявлення вторгнень (IDS) через здатність таких систем ідентифікувати незвичну

поведінку, яка може сигналізувати про нові чи раніше невідомі загрози. Крім того, використання аномалій забезпечує гнучкість і адаптивність IDS у динамічному кіберсередовищі, що робить цей напрям критично важливим для сучасної кібербезпеки.

Метою дослідження є пошук шляхів підвищенні ефективності виявлення аномального трафіку для класифікації вторгнень при побудові нових або удосконаленні існуючих IDS систем.

Досягнення мети передбачало виконання наступних *завдань*:

- зробити огляд літературних джерел способів і засобів виявлення вторгнень;
- розглянути теоретичні підходи виявлення аномалій;
- провести дослідження шляхів удосконалення систем виявлення вторгнень на основі штучного інтелекту;
- оцінити точність різних підходів з використанням відкритих датасетів;
- сформувати рекомендації щодо удосконалення IDS.

Об'єкт дослідження: системи виявлення вторгнень

Предмет дослідження: методи виявлення аномалій

Наукова новизна одержаних результатів кваліфікаційної роботи полягає в дослідженні шляхів підвищення точності знаходження та ідентифікації аномалій для виявлення вторгнень в мережі. Зокрема було досліджено вплив інструментів вилучення ознак з мережевого трафіку, кількості використаних ознак та різних налаштувань моделі на якість визначення атак з використанням даних відкритого набору даних CICIDS 2017. Також запропоновано метод ансамблювання , що дозволило підвищити точність результатів виявлення мережевих атак

Практичне значення одержаних результатів. Результати дослідження можуть бути використані при побудові нових або вдосконаленні існуючих систем виявлення вторгнень, що працюють на основі виявлення аномалій.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: XIII Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» (м.Тернопіль, Україна).

Публікації. Окремі результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

У сучасному світі комп'ютерні мережі проникли у всі сфери життя, включаючи енергетику, транспорт, роботу та повсякденну діяльність, стаючи невід'ємною частиною людського існування. Вони забезпечують взаємодію та обмін інформацією, що істотно підвищує ефективність багатьох процесів. Однак з розширенням мереж збільшуються і ризики, пов'язані з атакою зловмисників, що створює серйозні виклики для забезпечення їхньої безпеки.

Мета захисту комп'ютерних мереж полягає у забезпеченні безперебійної роботи систем, а також збереженні доступності, цілісності та конфіденційності даних. Важливо гарантувати, що інформація під час передачі чи обміну через мережу не буде змінена, втрачена чи викрадена. Це досягається шляхом впровадження різноманітних технічних і управлінських заходів, які дозволяють створити надійний та безпечний інформаційний простір.

Забезпечення безпеки комп'ютерних мереж вимагає застосування широкого спектра технологій. До ключових підходів належать шифрування даних, аутентифікація користувачів, виявлення та запобігання вторгненням, антивірусний захист та використання віртуальних приватних мереж (VPN) [3]. Деякі з цих методів є активними заходами захисту, інші — пасивними, а частина з них забезпечує платформу для дослідження нових підходів до безпеки.

1.1 Основні загрози комп'ютерних мереж

Мережева безпека знаходиться під великою загрозою через наявність різноманітних загроз та атак, які можуть призвести до розголошення чутливої та конфіденційної інформації. Основна відмінність між загрозою та атакою полягає в тому, що загроза - це наявність постійної небезпеки для цілісності, конфіденційності та доступності інформації, атака - це фактичний акт порушення безпеки мережі.

Для того, щоб забезпечити заходи безпеки в мережі даних, атаки повинні бути чітко визначені. Атака – це небезпечна або безпечна спроба змінити або

використати ресурс, доступний через мережу, у спосіб, який не був не було запланований. Відповідно до [4] всі кібератаки можна віднести до однієї з трьох категорій, визначених триадою безпеки інформації (CIA):

1- Конфіденційність: порушується при несанкціонованому доступі неавторизованих осіб до інформації в мережі.

2- Цілісність: порушується при несанкціонованій зміні або знищенні інформації.

3- Доступність: порушується при атаках, які призводять до відмови в обслуговуванні (DoS/DDoS)

Ключовим словом у перших двох категоріях є вчинення дій незаконно. Визначення того, які дії користувача вважаються дозволеними, а які ні, є визначальним фактором політики безпеки мережі. Будь-яка спроба отримати доступ до інформації або ресурсів, які не дозволені політикою, вважається несанкціонованою. Такий вид атаки є одним з найпоширеніших у кіберпросторі. Зловмисники використовують різноманітні методи, такі як підбір паролів, створення нових шляхів доступу, реєстрація фальшивих облікових записів та застосування шкідливого програмного забезпечення, щоб проникнути в обмежені зони мережі та отримати доступ до конфіденційних даних.

Одна з найбільш руйнівних форм кібератак полягає у навмисному знищенні інформації. Зловмисники, виконуючи шкідливі команди, можуть стерти великі обсяги даних за лічені секунди, завдаючи серйозних збитків організації. Такі дії можуть призвести до повного колапсу системи та втрати доступу до необхідних даних. Крім того, атаки, що перешкоджають нормальному функціонуванню мережі, також є серйозною загрозою.

Загрози мережевій безпеці поділяються на одну або дві загальні категорії: логічні атаки та атаки з використанням ресурсів. Раціональні атаки, як випливає з назви, використовують будь-яку слабкість в системі. Слабкими місцями можуть бути вразливості в програмному забезпеченні, такі як бекдори та помилки безпеки в коді. Кібератаки можуть мати різні цілі, але пошкодження або отримання несанкціонованого доступу до системи спрямовані на порушення її нормального функціонування. Ресурсні атаки спрямовані на виснаження

ресурсів мережі шляхом створення великої кількості запитів до сервера, , які він не може контролювати. Такий тип атаки, відомий як DDoS (Distributed Denial of Service), може зробити систему недоступною для легітимних користувачів. Крім того, зловмисники можуть використовувати шкідливе програмне забезпечення для зниження продуктивності системи або крадіжки даних. спрямовані на знищення ресурсів мереж.

Існує також інша класифікація різних атак на захищені мережі:

- Пасивні атаки - це тип кібератак, які спрямовані на збір інформації без прямого втручання в систему. Оскільки зловмисник лише приховано спостерігає та збирає розвід дані, то виявити його дуже складно. Шляхами захисту від пасивних атак є використання шифрування в мережевій інфраструктурі, віртуальні приватні мережі, системи виявлення вторгнень [5].
- Активні атаки це прямі дії, спрямовані на зміну системи або даних. Зловмисник може спробувати проникнути в систему, модифікувати дані, видалити файли або навіть повністю вивести систему з ладу. Шляхами захисту від активних атак є налаштування брандмауерів (програмних і апаратних), а також використання систем IPS та IDS [6].
- Внутрішні атаки. В цьому типі атак зловмисники отримують фізичний доступ до систем. Фізичний доступ до систем відкриває перед зловмисниками необмежені можливості для здійснення шкідливих дій. Це може призвести до викрадення даних, руйнування обладнання, а також до інших серйозних наслідків. Саме тому фізична безпека є невід'ємною частиною загальної стратегії захисту інформації.
- Інсайдерські атаки - це серйозна загроза для будь-якої організації, оскільки вони здійснюються співробітниками компанії. Співробітники, володіючи знаннями про внутрішні системи, можуть обійти стандартні засоби захисту. Тому крім технічних заходів необхідно приділяти особливу увагу фізичній безпеці та проведенню навчання персоналу.

В таблиці 1.1 мережеві атаки, які завдають шкоди компаніям по всьому світу [7]

Таблиця 1.1 – Розподіл мережевих атак за 2016 [8,9]

Назва атаки	Відсо-ток	Опис атаки
Browser	36%	Під час таких атак хакери додають скрипти, не змінюючи зовнішній вигляд веб-сайту, які можуть перенаправити користувача на інший веб-сайт і призвести до завантаження в систему шкідливих програм. Після цього зловмисник може дистанційно керувати системою користувача, отримуючи особисту інформацію, таку як дані кредитної картки та банківські реквізити, для крадіжки особистих даних.
Brute Force	19%	Це метод вгадування, який полягає у розшифровці пароля та пін-коду за допомогою методу проб і помилок. Зловмисники використовують автоматизоване програмне забезпечення, щоб вгадати тисячі комбінацій паролів. Блокування акаунту після невдалих спроб входу - один із способів запобігти подібним атакам.
Denial of service	16%	Ці види атак блокують доступ користувача до певної мережі, щоб щоб запобігти отриманню інформації та сервісів. Зловмисник створює перевантаження трафіку через шкідливого бота на цільову IP-адресу і заливає мережу більшою кількістю запитів, ніж може обробити сервер.
SSL	11%	Це різновид атаки, при якій зловмисник перериває дані перед їх шифруванням і таким чином отримує доступ до конфіденційної інформації системи
Scan	3%	Різновид прикладного програмного забезпечення, яке намагається отримати інформацію про відкриті порти на сервері або хості. Вони являють собою комбінацію ворожих пошукових запитів, які зловмисник використовує для отримання доступу до комп'ютера.
DNS	3%	Атака, яка перенаправляє мережевий трафік на іншу систему, яка контролюється зловмисником. Ця атака пошкоджує DNS-сервер шляхом внесення даних в кеш системи доменних імен для повернення неправильної IP-адреси.
Backdoor	3%	Такі атаки обходять системи виявлення вторгнень і дозволяють хакерам отримати віддалений доступ до інформації. У бекдор-атаках може бути застосовано багато стратегій бекдор-атаки
Others	9%	Інші атаки складають близько 9% від загальної кількості атак і можуть включають в себе всі атаки, які можуть бути невеликими за своєю природою, але мають значний вплив на безпеку мережевих систем.

Окрім вище зазначених є ще багато видів атак, які можуть задати серйозної шкоди організації. До таких атак належать: фішингові атаки, атаки соціальної інженерії, віруси та трояни. Проте в даній кваліфікаційній роботі ми зосередимось на захисті від атак на мережеві ресурси.

1.2 Засоби захисту комп’ютерних мереж

Засоби захисту мережі включають широкий спектр рішень для забезпечення її безпеки. З розумінням проблем безпеки, потенційних зловмисників, необхідного рівня безпеки та факторів, які роблять мережу вразливою до атак, розробляється ефективний план мережевої безпеки розробляється ефективний план мережевої безпеки [10]. Для того, щоб зробити комп'ютер менш вразливим до мережевих атака, існує багато продуктів, основними з яких є:

- Міжмережеві екрани (Firewall): блокують несанкціонований доступ і фільтрують трафік.
- Системи виявлення та запобігання вторгнень (IDS/IPS): виявляють аномалії та реагують на підозрілу активність.
- SIEM системи.
- VPN (Virtual Private Network): забезпечує шифрування з'єднань.
- Антивірусні програми: запобігають проникненню шкідливого ПЗ.
- Системи контролю доступу (NAC): обмежують доступ до ресурсів мережі.
- Рішення для сегментації мережі: розділяють мережу на ізольовані сегменти для обмеження впливу загроз.

Кожен із цих засобів виконує специфічні функції та є частиною комплексної стратегії кіберзахисту . Розглянемо детальніше окремі з цих засобів.

1.2.1 Міжмережеві екрани (Firewall)

Міжмережевий екран або брандмауер - це пристрій керування двома різними мережами для реалізації взаємного доступу, і є важливим пристроєм мережевої безпеки для реалізації контролю доступу до приватної та публічної

мережі відповідно до сформульованої політики контролю [10]. Основна роль брандмауера полягає в тому, щоб захистити внутрішню інформацію, структуру та роботу захищеної мережі, а також контролювати і обмежувати потік даних через мережу. Технологія брандмауера - це прикладна технологія безпеки, що базується на сучасних комунікаційних мережевих технологіях комунікаційних мереж і технологіях захисту інформації, яка найбільш визнаною і широко використовуваною в сучасній сфері мережевої сфері мережевої безпеки. Діаграма розміщення фаєрволу в мережі показано на рисунку 1.1

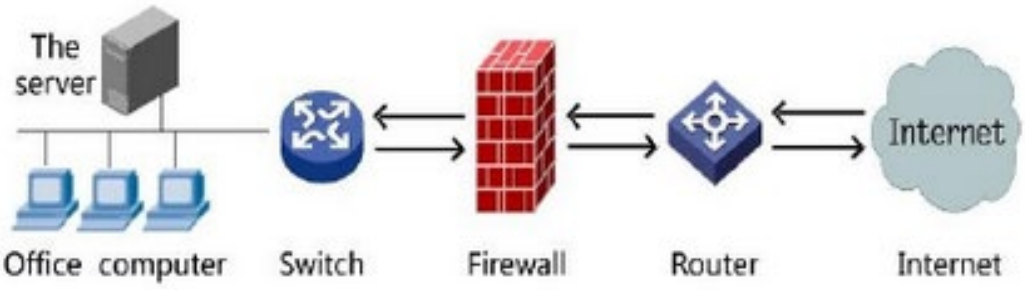

Рисунок 1.1 – Діаграма розміщення фаєрволу в мережі

Основними функціями брандмауера є:

- моніторинг і обмеження доступу;
- контроль протоколів і сервісів;
- захист внутрішньої мережі;
- конвертація мережевих адрес;
- функції VPN;
- логування та аудит.

1.2.2 Системи виявлення та запобігання вторгнень (IDS/IPS)

Комерційні компанії широко використовують IDS (системи виявлення вторгнень) та IPS (системи запобігання вторгненням) для забезпечення безпеки своїх інформаційних систем і захисту від руйнівних кібератак. Ці технології працюють разом, але мають різні функції та завдання [11]. Системи виявлення вторгнень (Intrusion Detection System IDS) допомагають аналізувати мережевий трафік і генерувати сповіщення в разі виявлення зловмисної активності. Система

запобігання вторгненням (Intrusion Prevention System IPS) активно реагує на потенційні загрози, не лише виявляючи їх, але й блокуючи або припиняючи атакуючі дії в реальному часі.

На рисунку 1.2 узагальнено відмінні та спільні риси IDS/IPS систем

Рисунок 1.2 – IDS vs IPS

Деякі організації використовують брандмауери, а також маршрутизатори разом з IPS/IDS. Основна різниця між ними полягає в тому, що брандмауер перевіряє лише IP-адресу та номер порту. Використовуючи номер порту та IP-адресу, він блокує трафік. Брандмауер - це перша лінія, яка може захистити мережу від зловмисників. Він може виявити лише обмежену кількість атак. Тому рекомендують додатково використовувати IDS/IPS, щоб забезпечити додатковий рівень захисту трафіку від атак з боку веб-серверів, доступних з Інтернету [12].

Відповідно до [13], IDS є одним з широко розповсюджених інструментів, що дозволяє здійснювати моніторинг цілого ряду мережевих систем, хмарних обчислень, а також інформаційної системи. За місцем встановлення систем виявлення вторгнень (IDS), їх поділяють на:

- Мережеві IDS (NIDS - Network IDS). Ці системи розташовані на рівні мережі і аналізують весь трафік, що проходить через мережу. Вони допомагають

виявити атаки, спрямовані на мережу або що використовують мережеві вразливості.

- Хостові IDS (HIDS - Host IDS). Ці системи встановлюються на окремих пристроях (наприклад, серверах, комп'ютерах) і контролюють їх активність, включаючи доступ до файлів, журнали подій, використання процесора тощо.

NIDS сканує мережевий трафік з сегмента локальної мережі. Він також може відстежувати більше мережевих цілей, намагаючись виявити загрози, які можуть бути пропущені HIDS, оскільки HIDS не може читати заголовки пакетів і не може виявити певні типи атак. Проте мережеві дані генеруються з великою швидкістю та у значній кількості. Тому є дуже важливою задача правильної репрезентації характеристик мережевого трафіку, виділяють пакетний, потоковий та аналіз на рівні прикладного шару. Пакетний аналіз розглядає характеристики мережевих пакетів. Потоковий аналіз оперує групами пакетів із однієї сесії та їх агрегованими характеристиками. Аналіз на рівні прикладного шару використовує мережеві дані додатків.

На рисунку 1.3 наведено приклад розміщення мережевих та хостових систем виявлення вторгнень.

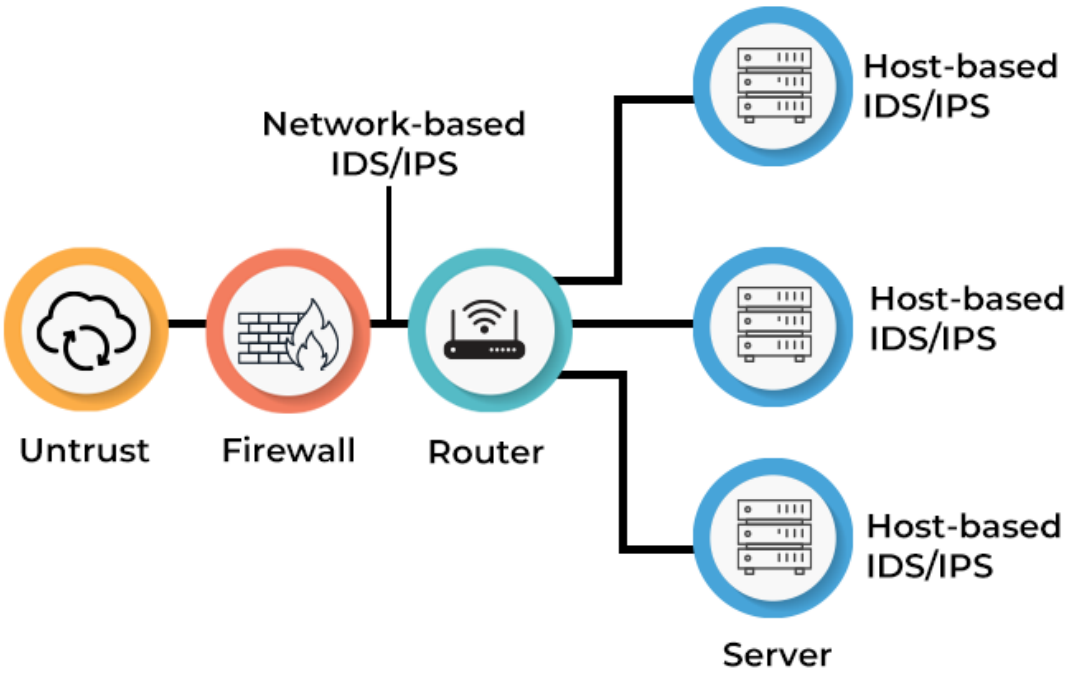

Рисунок 1.3 – Розміщення різних видів IDS/IPS систем в структурі мережі організації

За способом виявлення атак IDS поділяють на:

- Сигнатурні IDS (Signature-Based IDS). Ці системи працюють за принципом порівняння з відомими шаблонами атак (сигнатурами). Якщо виявлено дії, які відповідають відомим атакам, система сигналізує про загрозу.
- Аномалійні IDS (Anomaly-Based IDS). Ці системи вивчають нормальну поведінку системи або мережі і сигналізують, коли відбувається відхилення від цієї норми. Це може бути ознакою нової атаки
- Гібридні IDS (Hybrid IDS). Поєднують методи сигнатурного та аномалійного виявлення, щоб забезпечити більш точне та ефективне виявлення атак.

На рисунку 1.4 наведено робочий процес (Workflow) IDS на основі підписів та аномалій.

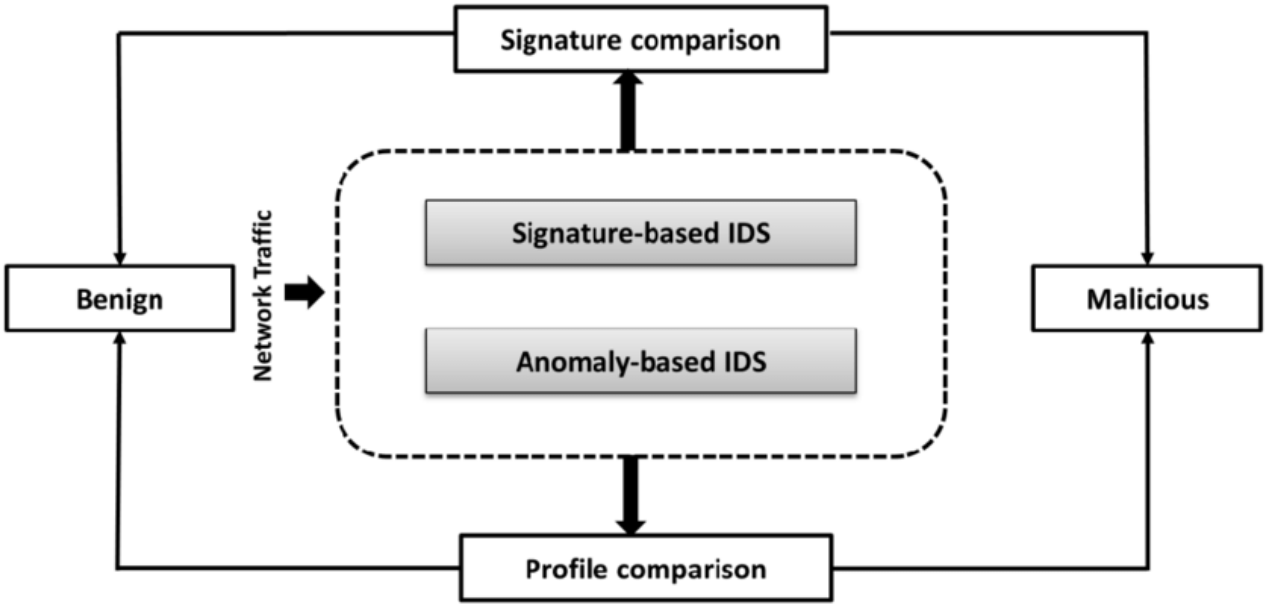

Рисунок 1.4 – Робочий процес IDS на основі підписів та аномалій

До переваг аномалійних IDS відносять здатність виявляти нові або невідомі атаки [14]. Аномалійні IDS можуть використовувати різні методи для виявлення відхилень:

- Статистичний аналіз: порівнює поточну активність з відомими статистичними моделями нормального використання.
- Методи машинного навчання (ML): деякі аномалійні IDS використовують алгоритми машинного навчання для розпізнавання шаблонів і

виявлення аномальних поведінкових патернів. Це дозволяє системі адаптуватися до нових умов і загроз.

- Нейронні мережі: складніші моделі, які допомагають покращити точність виявлення, оскільки вони можуть аналізувати більше параметрів і взаємозв'язків у даних.

Однак варто зазначити, що Anomaly-Based IDS також мають певні недоліки, такі як високі вимоги до обчислювальних ресурсів та складність налаштування. Тому їх найкраще використовувати в комплексі з іншими методами захисту, такими як сигнатурні системи та поведінкові системи виявлення вторгнень.

1.2.3 SIEM (Security information and event management) системи

SIEM, що розшифровується як Security Information and Event Management, - це рішення для кібербезпеки, яке співвідносить дані журналів і подій з систем у всьому IT-середовищі. SIEM поєднує в собі дві важливі функції: Управління інформацією про безпеку (SIM) та Управління подіями безпеки (SEM), надаючи організаціям наступні переваги:

- покращене виявлення загроз і реагування на них;
- покращене розслідування інцидентів завдяки детальним даним журналів;
- спрощена відповідність нормативним вимогам;
- централізована видимість мережевої безпеки.

Реалізовані у вигляді програмного, апаратного забезпечення або керованих послуг, SIEM-системи відіграють центральну роль в операційних центрах безпеки (SOC), які виявляють, розслідують і реагують на інциденти безпеки.

Системи управління інформацією та подіями безпеки (SIEM) були розроблені, щоб допомогти адміністраторам розробляти політики безпеки та керувати подіями з різних джерел.

Як правило, проста SIEM складається з окремих блоків (наприклад, пристрій-джерело, збір логів, нормалізація синтаксичного аналізу, механізм правил, зберігання логів, моніторинг подій), які можуть працювати незалежно один від одного, але без їх спільної роботи SIEM не буде функціонувати

належним чином. На рисунку 1.5 зображені основні компоненти звичайного рішення SIEM.

Рисунок 1.5 – Базові компоненти SIEM системи

Платформи SIEM забезпечують аналіз подій безпеки, що генеруються мережевими пристроями та додатками, в режимі реального часу. Крім того, навіть незважаючи на те, що нове покоління SIEM надає можливості реагування, вони дозволяють автоматизувати процес вибору та розгортання контрзаходів, поточні системи реагування вибирають і розгортають заходи безпеки без проведення комплексного аналізу впливу атак і сценаріїв реагування.

Основні відмінності між IDS, IPS та SIEM наведені на рисунку 1.6.

Рисунок 1.6 – Основні відмінності між IDS, IPS та SIEM

SIEM не може замінити IDS та IPS. Вона збирає інформацію з IDS, IPS, Firewall, логів, щоб побудувати повну картину безпеки мережі та вжити відповідні заходи.

1.2.4 NAC системи

Контроль доступу до мережі (NAC), також відомий як контроль доступу до мережі, - це процес обмеження доступу неавторизованих користувачів і пристроїв до корпоративної або приватної мережі. NAC гарантує, що тільки авторизовані користувачі та пристрої, які відповідають політикам безпеки, можуть увійти в мережу.

Контроль доступу до мережі має ряд переваг для організацій:

- Контроль користувачів, що входять в корпоративну мережу.
- Контроль доступу до додатків і ресурсів, до яких користувачі хочуть отримати доступ.
- Дозволи підрядникам, партнерам і гостям входити в мережу за необхідності, але обмежувати їх доступ.
- Сегментація співробітників на групи відповідно до їхніх посадових обов'язків і створюйте політики доступу на основі ролей.
- Захист від кібератак, впровадивши системи та засоби контролю, які виявляють незвичну або підозрілу активність.
- Автоматизація реагування на інциденти.

РОЗДІЛ 2 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ АНОМАЛІЙ

Системи виявлення вторгнень на основі аномалій (Anomaly-Based IDS) пропонують низку переваг, що роблять їх цінним інструментом у сучасному ландшафті кібербезпеки:

1. Виявлення невідомих загроз:

- Здатність виявляти невідомі та невідомі загрози, які не мають чітко визначених сигнатур.

- Моніторинг мережевого трафіку та виявлення відхилень від нормальної поведінки.

2. Проактивний захист:

- Можливість виявляти нові та емерджентні атаки, на які традиційні сигнатурні системи можуть не реагувати.

- Забезпечення проактивного захисту від нових загроз, що з'являються.

3. Адаптивність до змін:

- Здатність адаптуватися до змін у мережевому трафіку та поведінці користувачів.

- Постійне навчання та оновлення моделей для виявлення нових аномалій.

4. Зниження кількості помилкових спрацьовувань:

- Використання статистичних методів для визначення меж нормальної поведінки.

- Зменшення кількості помилкових спрацьовувань, що призводять до зайвих тривог.

5. Гнучкість у налаштуванні:

- Можливість налаштування чутливості та порогових значень для виявлення аномалій.

- Адаптація системи до конкретних потреб організації та мережевого середовища.

6. Інтеграція з іншими системами безпеки:

- Можливість інтеграції з іншими системами безпеки, такими як системи SIEM та SOAR.
- Забезпечення комплексного підходу до кібербезпеки та автоматизації процесів реагування на інциденти.

Розглянемо в цьому розділі основні підходи до побудови систем виявлення вторгнень на основі аномалій. На рисунку 2.1 наведено основні групи методів, які можуть використовуватись при побудові такого роду систем.

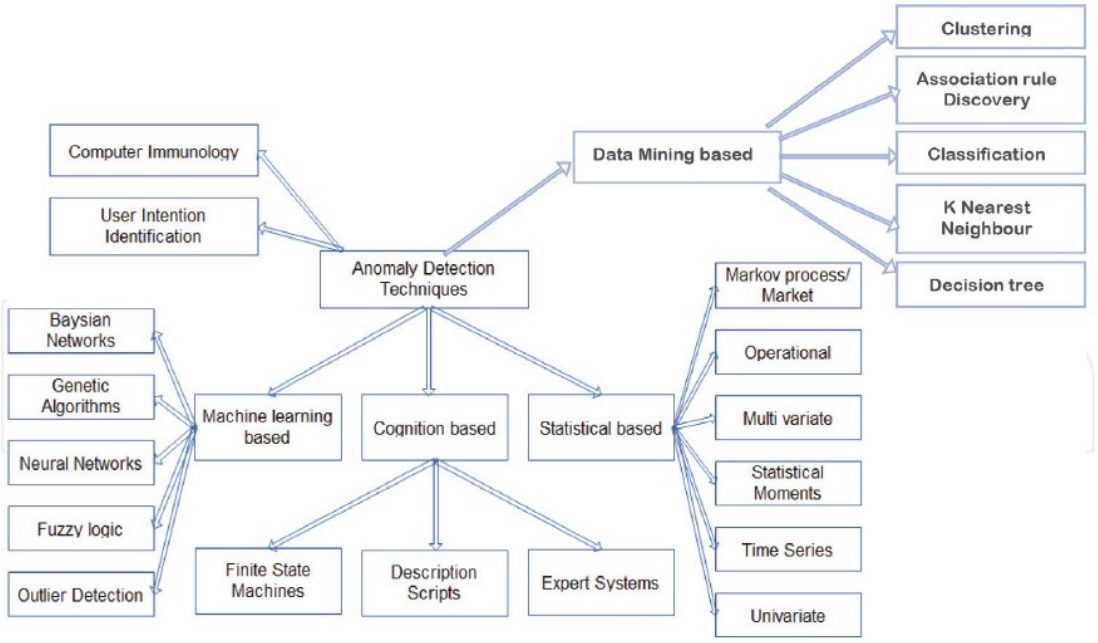

Рисунок 2.1 – Основні групи методів виявлення вторгнень, як аномалій [15]

Як видно з рисунку до таких методів належать: статистичні методи, когнітивні методи, методи машинного навчання, методи інтелектуального аналізу даних, методи глибокого навчання на інші. Розглянемо детальніше найбільш групи методів виявлення аномалій

2.1 Статистичні методи виявлення аномалій

Статистичні методи використовують статистичні властивості, такі як середнє значення та дисперсія, нормальних транзакцій для побудови профілю нормальної поведінки [16]. Статистичні тести використовуються для визначення того, чи відхиляється спостережувана транзакція від нормального профілю.

Система виявлення вторгнень (IDS) присвоює бал транзакціям, чий профіль відхиляється від нормального. Якщо бал досягає порогу, піднімається тривога.

2.1.1 Методи на основі статистичних моментів

Ця група методів використовує статистичні показники, такі як математичне сподівання та стандартне відхилення, для визначення довірчого інтервалу значень. Будь-яка подія, яка виходить за межі цього діапазону, вважається аномальною. Крім того існує група методів, заснованих на щільності розподілу та застосуванні так званого z-тесту. Перевагою цих методів є те, що вони не вимагають попереднього знання нормальної поведінки. Крім того, дані методи можуть адаптуватися до змін у поведінці користувача шляхом присвоєння більшої ваги останнім діям. Гнучкість, адаптивність, здатність виявляти нові типи атак є додатковими бонусами застосування цих методів. Натомість до недоліків можна віднести досить велику кількість хибних спрацювань.

2.1.2 Порогові методи

Цей метод виявляє аномалії шляхом підрахунку подій протягом певного періоду часу. Якщо кількість подій перевищує верхню межу або менша за нижню, то система спрацьовує. Наприклад, якщо користувач кілька разів не може увійти в систему (більше ніж "n" спроб), або якщо розмір завантаженого файлу перевищує встановлений ліміт (більше ніж "n" мегабайт). Головна складність цього методу полягає у визначенні оптимальних значень для цих порогів.

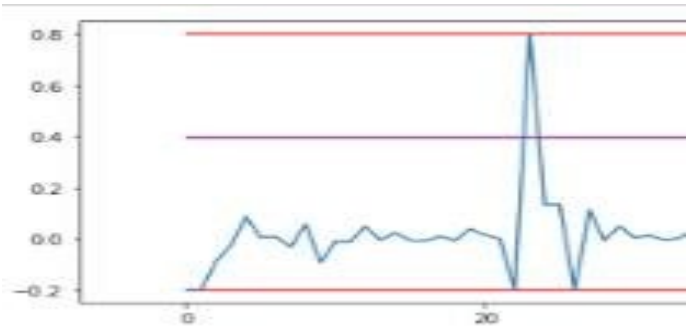

Рисунок 2.2 – Візуалізація порогових методів

На графіку рисунку 2.2 показана кількість подій з часом. Сині лінії - це встановлені пороги. Якщо значення виходить за межі цих ліній, то фіксується аномалія. Правильне визначення порогу тривоги є критичним для балансування між чутливістю та специфічністю системи.

2.1.3 Модель Марківського процесу або модель Маркова

Марківські ланцюги - це стохастичні процеси, в яких ймовірність переходу в наступний стан залежить лише від поточного стану. Матриця переходів описує ймовірності переходів між станами:

$$P(s\_t + 1 \mid s\_t) = P(s\_t + 1 \mid s\_t, s\_t - 1, \ldots) \quad (2.1)$$

де $P(s\_t + 1 \mid s\_t)$ - ймовірність переходу в стан s_t+1 з стану s_t,

s_t - стан системи в момент часу t

Алгоритм виявлення аномалій заснований на моделі Маркова може виглядати наступним чином:

1. Визначення станів: Спочатку визначаються можливі стани системи, які можуть бути релевантними для виявлення аномалій. Наприклад, для мережевого трафіку це можуть бути типи пакетів, джерела та призначення.
2. Побудова матриці переходів: На основі історичних даних будується матриця переходів, яка відображає ймовірності переходів між різними станами.
3. Моніторинг поточного стану**:** В реальному часі відстежується поточний стан системи.
4. Розрахунок ймовірності наступного стану: Використовуючи матрицю переходів, розраховується ймовірність того, що система перейде в наступний стан.
5. Виявлення аномалій: Якщо розрахована ймовірність дуже низька, то це може свідчити про те, що відбувається незвичайна подія, тобто аномалія.

Підсумовуючи, можна сказати, що цей метод відстежує стан системи через певні інтервали часу і розраховує ймовірність переходу системи з одного стану в інший. Стани можуть представляти різні типи пакетів (наприклад, HTTP, FTP,

SMTP). Переходи між станами відображають ймовірність того, що після одного типу пакету піде інший. Якщо спостерігається послідовність переходів, яка має дуже низьку ймовірність, то це може свідчити про атаку або іншу аномалію.

Цей метод особливо ефективний для виявлення аномалій у послідовності подій, наприклад, у серії команд, виконаних користувачем.

Переваги моделі Маркова

- Проста реалізація: Модель Маркова відносно проста в розумінні та реалізації.
- Ефективність: Модель може обробляти великі обсяги даних в реальному часі.
- Гнучкість: Модель може бути адаптована до різних типів даних і сценаріїв.

Обмеження моделі Маркова:

- Припущення про стаціонарність: Модель припускає, що ймовірності переходів є стаціонарними, тобто не змінюються з часом.
- Проблема "холодного старту": Для побудови точної моделі потрібна достатня кількість історичних даних.
- Складність для складних систем: Для систем з великою кількістю станів і складними залежностями побудова моделі Маркова може бути складною.

Модель Маркова є потужним інструментом для виявлення аномалій, але її ефективність залежить від правильності вибору станів і побудови матриці переходів.

2.1.4 Інші статистичні підходи

До інших статистичних методів відносять:

- Модель часових рядів: Аналізує послідовність даних у часі для виявлення аномалій.
- Параметричні підходи: Припускають, що дані походять з відомого розподілу ймовірностей (наприклад, нормального розподілу).
- Мультиваріатна модель: Аналізує кілька змінних одночасно для виявлення аномалій.

Статистичні методи є потужним інструментом для виявлення аномалій у мережевому трафіку. Вони особливо корисні для виявлення невідомих атак, але вимагають точного налаштування та обробки даних, зокрема вимагають знань характеристик статистичних розподілів. Вибір правильного статистичного тесту залежить від типу даних і припущень про розподіл даних. В той самий час, статистичні методи можуть бути чутливими до шуму та помилок у даних.

Комбінація статистичних методів з іншими методами, такими як машинне навчання та поведінкові методи, може значно підвищити ефективність систем виявлення вторгнень.

2.2 Інтелектуальні методи виявлення аномалій

Інтелектуальні методи виявлення аномалій базуються на техніках Data Mining (DM) та Machine Learning (ML). Data mining та machine learning – це дві тісно пов'язані дисципліни, які часто використовуються разом для виявлення аномалій. Однак, вони мають свої особливості та підходи.

Data mining націлений на видобування прихованих знань та закономірностей з великих даних [17]. Він використовує статистичні та математичні методи для аналізу даних та виявлення асоціацій, кластерів та інших патернів. DM визначає аномалії як точки даних, які значно відрізняються від загальної маси даних.

Machine learning націлений на створення моделей, які можуть навчатися на даних та робити прогнози або приймати рішення. Використовує алгоритми, які дозволяють комп'ютерам навчатися на даних без явного програмування. Визначає аномалії як точки даних, які не відповідають моделі, навченій на нормальних даних. Визначає аномалії як точки даних, які не відповідають моделі, навченій на нормальних даних.

Основні відмінності між Data Mining і Machine Learning узагальнено в таблиці 2.1

Таблиця 2.1 - Основні відмінності між Data Mining і Machine Learning

	Data Mining	Machine Learning
Мета	Видобування знань	Побудова моделей
Методи	Статистичні, математичні	Алгоритми навчання
Аномалії	Відхилення від загальної маси	Відхилення від моделі
Фокус	Описання даних	Прогнозування та прийняття рішень

На рисунку 2.3 наведено візуалізацію роботи системи виявлення вторгнень на основі аномалій, що базується на інтелектуальних методах.

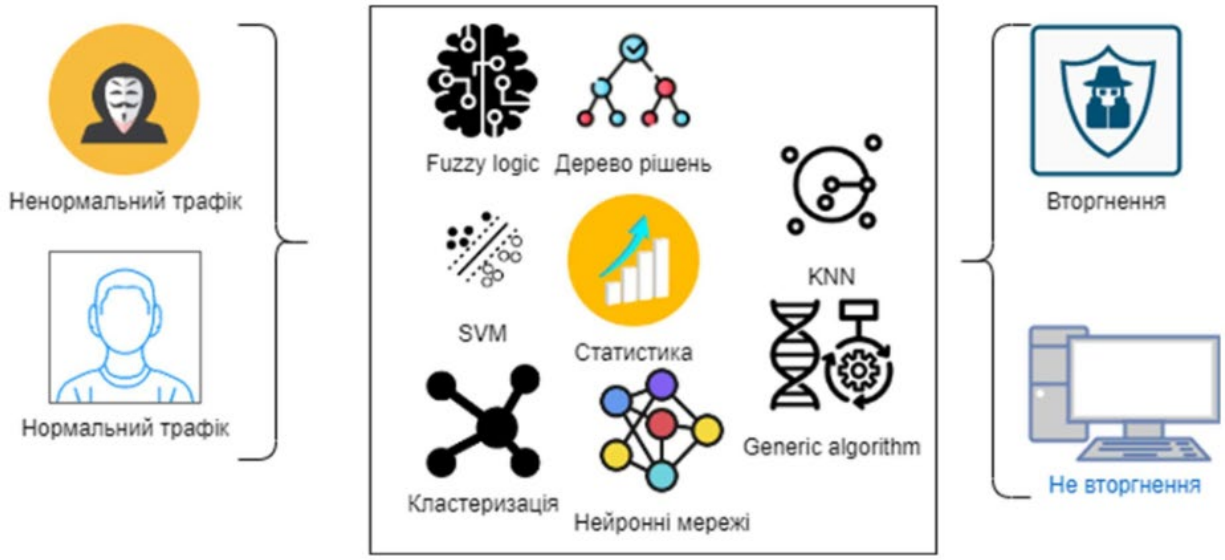

Рисунок 2.3 – Візуалізація роботи системи виявлення вторгнень на основі аномалій, що базується на інтелектуальних методах

Загалом методи машинного навчання поділяються на керовані та некеровані. У керованому машинному навчанні алгоритми навчаються на наборі даних, який містить як вхідні дані, так і відповідні їм мітки класів (цілі). Мета навчання – побудувати модель, яка зможе правильно класифікувати нові, раніше не бачені дані. У некерованому машинному навчанні алгоритми навчаються на наборі даних, який не містить міток класів. Мета навчання – знайти приховані структури та закономірності в даних.

2.2.1 Керовані методи машинного навчання

Основними видами керованого навчання є:

- Класифікація: Передбачення, до якого класу належить новий об'єкт (наприклад, спам/не спам, кіт/собака).
- Регресія: Передбачення числового значення (наприклад, ціна будинку, температура).

В таблиці 2.2 резюмовано основні характеристики класифікації та регресії

Таблиця 2.2 - Основні характеристики класифікації та регресії

Класифікація	**Регресія**
Прогнозування дискретної мітки класу	Прогнозування неперервної величини
Алгоритм класифікації може передбачити неперервне значення у формі ймовірності для мітки класу	Алгоритм регресії може передбачити дискретне значення у формі цілого числа
Оцінка якості: точність, влучність, повнота	Оцінка якості: MAE, MSE, RMSE

Найпростішим для розуміння методом керованого навчання є k-найближчих сусідів. kNN (k-Nearest Neighbors) — це один з найпростіших, але ефективних алгоритмів машинного навчання, який використовується для класифікації та регресії. Основна ідея полягає в тому, що об'єкт належить до того ж класу, що й більшість його k найближчих сусідів.

Алгоритм kNN для задачі класифікації:

- Вибір значення k. Визначається кількість найближчих сусідів (k), які будуть враховуватися при класифікації нового об'єкта.
- Обчислення відстані. Для нового об'єкта обчислюється відстань до всіх об'єктів у навчальному наборі.
- Вибір k найближчих сусідів. Вибирається k об'єктів з найменшою відстанню до нового об'єкта.

- Голосування. Клас нового об'єкта визначається шляхом "голосування" серед k найближчих сусідів. Найчастіше зустрічається клас і буде присвоєний новому об'єкту.

Не зважаючи на простоту методу, він не є однозначним. В залежності від вибору параметру k результат може відрізнятися, що продемонстровано на рисунку 2.4.

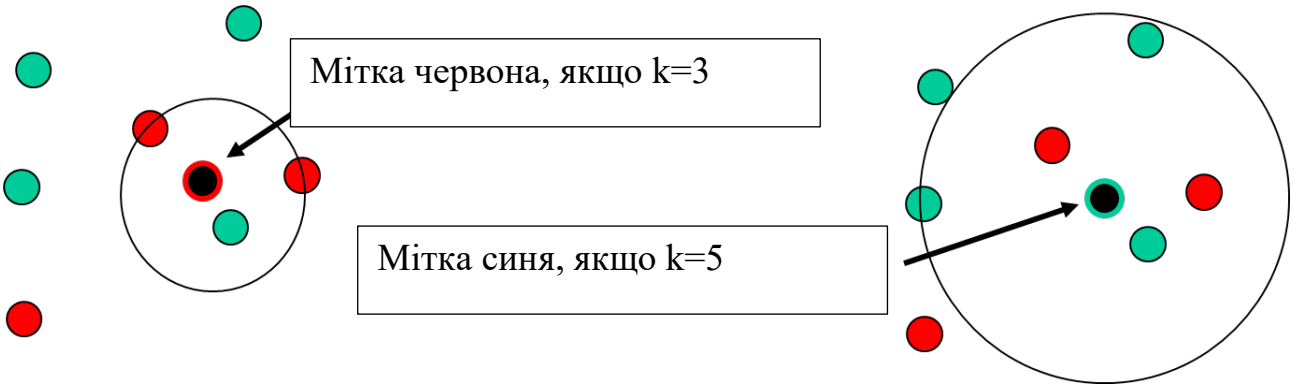

Рисунок 2.4 – Вплив параметру k – кількості сусідів на результат

Також на результат впливає вибір метрики, який здійснюється в залеежності від типу даних. Найчастіше використовують:

- Евклідова відстань - для числових даних;
- Манхеттенська відстань - для категоріальних даних;
- косинусна міра - для векторних даних.

Не зважаючи на простоту та універсальність метод має ряд обмежень у використанні, зумовлених наступними факторами:

- Швидкодія. Алгоритм може працювати повільно на великих наборах даних через необхідність обчислення відстаней до кожного з найближчих сусідів.
- Чутливість до шуму. Наявність шумних даних може негативно вплинути на точність класифікації, оскільки алгоритм враховує найближчі сусідів, включаючи потенційні виключення.
- Вибір гіперпараметра. Оптимальне значення параметра k значно впливає на результати, але його вибір може бути складним завданням.

- Проблема розмірності. Зі збільшенням кількості ознак ефективність алгоритму може знижуватися, оскільки відстані між об'єктами стають менш інформативними.

Іншими словами, k-NN може бути чутливим до якості даних, обчислювально складним для великих наборів даних і вимагає ретельного налаштування параметрів.

Ще одним відомим методом керованого навчання є метод опорних векторів (Support Vector Machines, SVM). Це потужний алгоритм машинного навчання, який використовується для класифікації та регресії. Його основна ідея полягає у знаходженні оптимальної гіперплощини, яка максимально відділяє дані різних класів. SVM знаходить найкращу пряму (або гіперплощину у багатовимірному просторі), яка максимально чітко відокремлює точки різних категорій одна від одної.

Ця пряма (гіперплощина) проходить так, щоб відстань до найближчих точок даних була максимальною. Саме ці найближчі точки і називаються опорними векторами. Вони визначають розташування розділяючої прямої (рисунок 2.5).

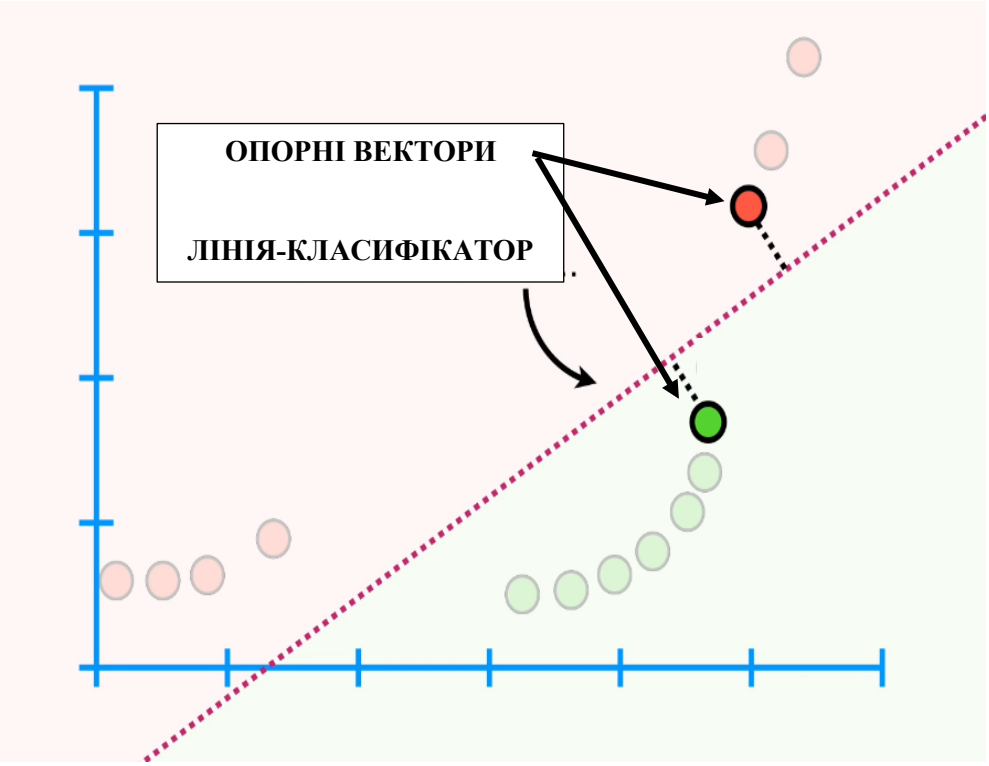

Рисунок 2.5 – Ілюстрація основних понять методу опорних векторів

Одна з ключових особливостей SVM полягає в тому, що він може працювати не тільки з лінійно роздільними даними. За допомогою спеціальних функцій, які називаються ядрами, дані можуть бути перетворені в більш високовимірний простір, де їх легше розділити лінійною гіперплощиною.

Переваги SVM:

- Ефективність у багатовимірних просторах. SVM добре справляється з даними, які мають багато характеристик.
- Стійкість до перенавчання. Метод менш схильний до запам'ятовування випадкових особливостей даних.
- Універсальність. Може використовуватися для розв'язання різних завдань, від класифікації зображень до аналізу текстів.

Недоліки SVM:

- Обчислювальна складність. Для великих наборів даних навчання моделі може бути тривалим.
- Чутливість до параметрів. Вибір правильних параметрів моделі може вплинути на її точність.
- Складність інтерпретації. Іноді буває складно зрозуміти, як саме модель приймає рішення.

Крім того відомими моделями є дерева рішень та випадкові ліси.

Дерево рішень є одним з популярних методів машинного навчання, який використовується для класифікації та регресії. Це структура, яка моделює процес прийняття рішень у вигляді дерева, де кожен вузол представляє перевірку на певну умову, а гілки ведуть до різних варіантів результатів. Кожен кінцевий вузол дерева (лист) містить відповідь на запитання, що ставиться до вхідних даних.

Основною ідеєю дерева рішень є поділ набору даних на підмножини за допомогою певних умов, щоб у кінцевому підсумку отримати рішення, яке оптимально розділяє дані. Кожен розподіл здійснюється таким чином, щоб зменшити невизначеність або нерівномірність даних, застосовуючи певний критерій, як-от інформаційний приріст чи показник Джині.

Під час побудови дерева рішень алгоритм починає з кореневого вузла і розглядає всі можливі умови, щоб вирішити, яку умову слід застосувати для поділу даних на два підмножини. Цей процес триває до тих пір, поки не буде досягнуто певного критерію зупинки, такого як максимальна глибина дерева або мінімальна кількість прикладів у листі.

Алгоритм дерева рішень активно застосовується завдяки своїй простоті в розумінні та здатності працювати як з числовими, так і з категоріальними даними. Однак є і певні обмеження, такі як схильність до перенавчання при надмірній глибині дерева, тому часто застосовуються різні методи регуляризації та усічення дерева.

Переваги дерев рішень:

- Простота інтерпретації. Дерева рішень легко візуалізувати і зрозуміти, навіть для людей без глибоких знань в області машинного навчання.
- Здатність обробляти як числові, так і категоріальні дані.
- Не вимагає нормалізації даних.
- Може використовуватися для задач класифікації та регресії.

Недоліки дерев рішень:

- Схильність до перенавчання. Дерева рішень можуть бути занадто складними і точно підлаштовуватися під навчальні дані, що призводить до поганої узагальнюючої здатності на нових даних.
- Нестабільність. Невеликі зміни в даних можуть призвести до суттєвих змін у структурі дерева.
- Проблеми з неперервними даними. Дерева рішень можуть погано працювати з даними, що мають велику кількість можливих значень.

Випадкові ліси - це спосіб усунути недолік, пов’язаний з низькою точністю і чутливістю до даних дерев рішень. Ліч формується на основі таблиць, де об’єкти вибираються випадковим чином з головної таблиці.

2.2.2 Некеровані методи машинного навчання

Основними видами завдань некерованого навчання є наступні:

- Кластеризація: Розбиття даних на групи (кластери) таким чином, щоб об'єкти в одному кластері були більш схожими між собою, ніж з об'єктами з інших кластерів.
- Зменшення розмірності: Перетворення даних з високою розмірністю в простір з меншою розмірністю, зберігаючи при цьому максимальну інформацію.
- Асоціативний аналіз: Виявлення правил асоціації між змінними.

Загалом методи кластеризації поділяють на ієрархічні та неієрархічні. Розглянемо для прикладу метод неієрархічної кластеризації k-means.

Метод кластеризації k-means — це популярний алгоритм без вчителя, який використовується для поділу набору даних на кілька груп (кластерів) на основі схожості між елементами. Ключова ідея методу полягає в тому, що дані розподіляються так, щоб кожен елемент належав до одного з k кластерів, де k — це кількість груп, яку визначає користувач.

Алгоритм починається з того, що випадковим чином вибираються k початкових центрів кластерів. Далі для кожного елемента в даних визначається, до якого з цих центрів найближчий за допомогою певної метрики, зазвичай Евклідової відстані. Таким чином, кожен елемент отримує свою кластерну приналежність.

Після цього алгоритм оновлює центри кластерів, обчислюючи середнє значення всіх точок, які належать до кожного з кластерів. Центри кластерів переміщуються в нові позиції, і цей процес повторюється до тих пір, поки зміщення центрів кластерів не стане мінімальним або не досягне певної межі за кількістю ітерацій.

Метод k-means має низку переваг, таких як простота реалізації та ефективність на великих наборах даних, але й певні недоліки. Одним із основних є те, що k потрібно задавати заздалегідь, і вибір цього числа може впливати на результати кластеризації. Крім того, метод чутливий до початкових умов (вибір початкових центрів), тому може призвести до різних результатів при різних початкових розподілах. Тому для досягнення стабільних результатів часто використовуються методи, які оптимізують вибір початкових центрів.

Загалом підходи Data mining та Machine learning часто використовуються разом для досягнення кращих результатів. Data mining використовують для підготовки даних. Перед застосуванням методів машинного навчання дані зазвичай піддаються попередній обробці за допомогою методів Data mining (очищення, трансформація, відбір ознак). Machine learning використовують для побудови моделей прийняття рішень. На підготовлених даних будуються моделі машинного навчання для виявлення аномалій. Методи Data mining використовуються для аналізу та інтерпретації результатів роботи моделей машинного навчання та отримання більш глибокого розуміння даних.

2.3 Методи глибокого навчання

Штучні нейронні мережі (ШНМ) – це потужний інструмент машинного навчання, натхненний біологічними нейронними мережами. Вони здатні виявляти складні закономірності в даних, які можуть бути недоступні для традиційних методів аналізу. Багатошаровий персептрон (MLP) – одна з найвідоміших архітектур ШНМ. Він складається з кількох шарів нейронів, пов'язаних між собою. Кожен нейрон обчислює зважену суму своїх входів, додаючи до неї зміщення, а потім застосовує нелінійну функцію активації. MLP здатний навчатися на великих обсягах даних і виявляти нелінійні залежності. Однак, MLP має свої обмеження: він може бути неефективним при роботі з новими даними, особливо якщо вони значно відрізняються від тренувальних.

Для вирішення цієї проблеми було розроблено інші типи нейронних мереж. Одна з таких мереж – це радіально-базисна нейронна мережа (RBFN). На відміну від MLP, RBFN використовує радіальні базисні функції для обчислення виходу. Кожна нейрон в RBFN відповідає за певний кластер даних. Коли на вхід подається новий вектор, мережа визначає, до якого кластера він належить, і видає відповідний вихід.

Модифікована імовірнісна нейронна мережа (PNN) – це ще одна цікава архітектура, яка є розширенням RBFN. PNN використовує статистичні методи

для оцінки ймовірності того, що новий вхідний вектор належить до певного класу.

Переваги RBFN та PNN:

- Швидке навчання. Навчання цих мереж зазвичай займає менше часу, ніж навчання MLP.
- Хороша узагальнююча здатність. RBFN та PNN зазвичай краще узагальнюють на нові дані, ніж MLP.
- Інтерпретованість. Структура цих мереж може бути більш інтуїтивно зрозумілою, ніж структура MLP.

Штучні нейронні мережі є потужним інструментом для вирішення широкого кола завдань. Вибір конкретної архітектури залежить від особливостей задачі, обсягу даних та вимог до швидкості навчання та точності. RBFN та PNN можуть бути хорошим вибором для задач, де важлива швидкість навчання та узагальнююча здатність.

Можливими напрямками майбутнього дослідження є:

- Згорткові нейронні мережі (CNN): спеціалізовані мережі для обробки зображень.
- Рекурентні нейронні мережі (RNN): мережі для роботи з послідовними даними (тексти, часові ряди).
- Генеративні змагальні мережі (GAN): мережі для генерації нових даних.
- Трансформери: сучасна архітектура, що використовується в моделях обробки природної мови (NLP).

2.4 Когнітивні методи, що базуються на знаннях

Такі методи отримують знання з конкретних атак та вразливостей системи. Ці знання можуть бути використані для ідентифікації вторгнень або атак, що відбуваються в мережі або системі. Вони генерують тривогу, як тільки виявляється атака. Вони можуть бути використані як для виявлення зловмисного трафіку, так і для виявлення аномалій [18]

Методи, що базуються на знаннях, поділяються на наступні основні три групи:

- Аналіз переходів між станами. Скінченний автомат (finite state machine FSM) або скінченний автомат - це модель поведінки, зафіксованої у станах, переходах та діях. Стан містить інформацію про минуле, тобто будь-які зміни у на вході фіксуються, і на основі цього відбувається перехід. Дія це опис діяльності, яка має бути виконана в даний момент часу. Існує декілька типів дій: дія на вході, дія на виході дія та дія переходу.
- Експертні системи. Людський досвід у вирішенні проблем використовується в інтелектуальних системах. Один або декілька експертів встановлюють правила для функціонування системи на основі свого досвіду. Ці системи ефективні в певних проблемних областях, а також розглядаються як клас задач штучного інтелекту (ШІ)
- Аналіз сигнатур. Така модель будується на основі правил, що використовуються для опису нормального трафіку чи атаки.
- Методи, засновані на знаннях, мають високу точність і дуже низький рівень помилкових спрацювань.

Методи, засновані на знаннях, підтримують знання про кожну атаку на основі ретельного і детального аналізу; але це трудомістке завдання. Актуалізація попередніх знань про кожну атаку є надскладним завданням.

2.5 Інші методи виявлення аномалій

Ще одним напрямом виявлення аномалій може бути ідентифікація намірів користувача.

Система виявлення вторгнень може бути побудована на основі ознак, які класифікують користувача або використання системи, щоб відрізнити аномальну діяльність від нормальної. Під час раннього дослідження виявлення аномалій основний акцент робився на профілюванні поведінки системи або користувача на основі даних системного журналу або журналу бухгалтерського обліку, що контролюється. Дані журналу або системного журналу можуть містити команди

оболонки UNIX, системні виклики, натискання клавіш, події аудиту та використані мережеві пакети.

Ще одним підходом є комп'ютерна імунологія - галузь науки, яка включає в себе високопродуктивні геномні та біоінформатичні підходи до імунології. Основною метою є перетворення імунологічних даних в обчислювальні задачі, розв'язання цих задач за допомогою статистичних та обчислювальних підходів, а потім перетворення результатів в імунологічно значущі інтерпретації.

Однак, слід зазначити, що не зважаючи на велику кількість переваг, зазначену в цьому розділі, Anomaly-Based IDS також мають певні недоліки, такі як високі вимоги до обчислювальних ресурсів та складність налаштування. Тому їх найкраще використовувати в комплексі з іншими методами захисту, такими як сигнатурні системи та поведінкові системи виявлення вторгнень.

РОЗДІЛ 3 ШЛЯХИ ВДОСКОНАЛЕННЯ ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ

3.1 Огляд підходів до систем виявлення вторгнень на основі аномалій

Системи ідентифікації на основі аномалій або системи ідентифікації на основі поведінки аналізують мережевий трафік на основі поведінки мережі.

Вони визначають нормальну поведінку мережі, і якщо виявлено будь-яку аномальну поведінку або мережа відхиляється від нормальної поведінки мережі, з'являється попередження. Однак ці системи не є не дуже точні, коли йдеться про ідентифікацію, оскільки профілювання мережі є складним процесом і часто призводить до високого рівня помилкових тривог [19]. Більшість підходів, які зараз використовуються в системах ідентифікації не можуть належним чином впоратися зі складною та динамічною природою зловмисних загроз. Тому шукають різні методи машинного навчання, щоб досягти кращого рівня виявлення (Detection Rate - DR), рівня хибних тривог та обчислювальних витрат [20]. Традиційні методи ідентифікації мають кілька обмежень у захисті системи; особливо це стосується випадків, коли системи стикаються з великою обсягом зловмисних атак (DoS/DDoS); системи можуть отримати високі значення хибнонегативних спрацьовувань [21]

Останнім часом багато дослідників використовують методи машинного навчання для систем ідентифікації, щоб покращити показники ідентифікації. Було проведено кілька досліджень, спрямованих на вдосконалення та застосування цього методу до систем ідентифікації [22]. Було виявлено, що моделі машинного навчання мають багато проблем, які уповільнюють процес навчання; ці проблеми включають в себе розмір набору даних та пошук найбільш оптимальних параметрів моделі. Такі проблеми спонукали дослідників шукати найефективнішу методологію. Однак прості підходи до машинного навчання обмежені [23], в той час як методи вторгнення розширюються і стають все більш складнішими. Займались вивченням цього питання і вчені нашого університету [24]

Тому метою нашого дослідження є пошук шляхів вдосконалення виявлення аномалій в мережевому трафіку.

3.2 Існуючі набори даних, що можуть бути використані для тестування нових підходів для створення систем виявлення вторгнень

CICIDS 2017 та CICIDS 2018 — це два важливі датасети, створені Канадським інститутом кібербезпеки для досліджень у галузі виявлення аномалій та кіберзагроз в мережах. Ці датасети мають велике значення для розробки та оцінки алгоритмів машинного навчання, які застосовуються в системах кібербезпеки, особливо в контексті виявлення вторгнень і атак на комп'ютерні мережі. Вони містять реальні мережеві дані, що дозволяють тестувати методи виявлення атак, таких як DDoS, SQL-ін’єкції, спроби зламування паролів, та інші види зловмисної діяльності.

Для збору даних, агрегованих в датасеті CICIDS 2017 на основі реального мережевого трафіку була спеціально розроблена тестова інфраструктура. В межах цієї системи було розроблено та імплементовано кілька видів атак, зокрема DDoS, Botnet, DoS. Також були накопичені дані нормального трафіку. Датасет складається з майже 3 мільйонів записів даних з окремими характеристиками мережевих пакетів, до яких належать IP-адреси, порти, час відгуку, обсяг трафіку та інші важливі параметри, що допомагають виявляти аномалії.

Із записаного трафіку було добуто 80 характеристик, набір даних записано у файл з розширенням .csv. Кожен запис містить свої ознаки і характеризується міткою нормального трафіку або певної атаки. Набір даних CICIDS 2017 містить дані, які нагадують файли реальних даних PCAP. Крім цього, в даному наборі також є результати аналізу мережевого трафіку за допомогою CICFlowMeter (файли CSV).

Головним пріоритетом у створенні цього набору даних була симуляція трафіку максимально схожого до реальних умов. Для цього набору даних було

симульовано поведінку 25 користувачів на основі протоколів HTTP, HTTPS, FTP, SSH і електронної пошти.

CICIDS 2018 побудований на основі попереднього датасету, але містить нові, вдосконалені дані, що дозволяють досліджувати ще ширший спектр атак і методів їх виявлення. Цей датасет містить більш складні атаки, такі як атаки з використанням криптовалют, а також різні типи атак на рівні додатків та мереж. Він також включає дані про типи атак на веб-додатки, що відображає розвиток кіберзагроз у сучасному світі. Датасет також зібраний з реального мережевого трафіку, з урахуванням різноманітних мережевих топологій і типів комунікацій, що дозволяє створювати більш реалістичні моделі виявлення атак.

Однією з особливостей CICIDS 2017 і CICIDS 2018 є те, що вони містять мітки для кожного типу мережевого трафіку, що дозволяє автоматизувати процес навчання алгоритмів машинного навчання. Ці датасети використовуються для тренування та тестування моделей класифікації, таких як дерева рішень, методи опорних векторів (SVM), нейронні мережі та інші алгоритми. Дані містять не тільки сиру мережеву інформацію, а й відповідні мітки, які вказують на нормальний або аномальний характер трафіку, що значно полегшує завдання класифікації.

Використання CICIDS 2017 і CICIDS 2018 у наукових дослідженнях і практиці допомагає вдосконалювати технології виявлення вторгнень, розробляти системи попередження та реагування на кіберзагрози, а також покращувати безпеку в мережах. Вони стали важливим ресурсом для дослідників у галузі кібербезпеки, а також для фахівців, які працюють з технологіями захисту даних і виявлення аномалій. Ці датасети активно використовуються для порівняння ефективності різних підходів до класифікації та виявлення атак у реальному часі.

В таблиці 3.1 наведено порівняння двох датасетів CICIDS 2017 і CICIDS 2018

Таблиця 3.1 – Порівняння датасетів CICIDS 2017 і CICIDS 2018

Dataset	CICIDS 2017	CICIDS 2018
Capture duration	5 days	10 Days
Number of Classes	15	18
Number of features	80	83
Number of records/instances	28,30,743	162,33,022
Number of attacks	5,57,646 (19%)	27,59,364 (17%)
Number of Benign	22,73,097 (81%)	134,73,658 ((83%)
Data size (csv)	885Mb	7Gb
Types of attacks	DoS DDoS Brute Force Botnet Infiltration Web Attack	DoS DDoS Brute Force Botnet Infiltration Web Attack

Набір даних CICIDS 2017 складається з 8 файлів CSV, що містять потік мережевого трафіку за 5 днів. Як видно з таблиці 3.1 ці CSV-файли були об'єднані, утворивши єдиний CSV-файл, що складається з 2830743 записів.

Автори дослідження [25] стверджують, що використання усіх 83 ознак є ресурсо- і обчилювально затратним. Тому формування та вибір ознак є важливим початковим етапом для майбутньої моделі, що може, як і підвищити точність класифікації, і так і зменшити ресурсоємність методу.

В наступному підрозділі здійснимо огляд інструментів, які впливають вибір інформативних ознак з мережевого трафіку.

3.3 Процес вилучення ознак з даних мережевого трафіку

3.3.1 Отримання характеристик з даних мережевого трафіку

Для отримання характеристик з мережевого з'єднання можна використовувати різні методи. Найчастіше використовуються такі методи:

- Захоплення та аналіз пакетів: передбачає захоплення пакетів мережевого трафіку та їх аналіз для вилучення таких характеристик, як розмір пакета, протокол, IP-адреси джерела та призначення, номери портів і прапорів.

- Аналіз потоків: полягає в групуванні пакетів у потоки, які є послідовностями пакетів одного сеансу зв'язку. Розмір, тривалість і протокол потоку - це характеристики потоку, які можна виділити з потоку мережевого трафіку.

- Моніторинг прикладного рівня: передбачає моніторинг мережевого трафіку на прикладному рівні для вилучення таких характеристик, як тип прикладного трафіку, URL-адреси, до яких здійснюється доступ, і обсяг переданих даних.

Характеристики часто витягуються із PCAP файлів. Це формат файлів, який використовується для зберігання мережевого трафіку, захопленого сніферами пакетів або інструментами мережевого моніторингу. Ці інструменти захоплюють пакети даних, коли вони проходять через мережу, включаючи таку інформацію, як IP-адреси джерела та призначення, порти, протоколи та вміст самих пакетів. PCAP - це широко використовувані файли для мережевого аналізу, усунення несправностей і забезпечення безпеки, які дозволяють дослідникам кібербезпеки перевіряти мережевий трафік на наявність аномалій, зловмисної активності або проблем з продуктивністю.

Конкретні ознаки, які витягуються, залежать від конкретної програми і впливають на ефективність алгоритму. Наприклад, програма для виявлення шкідливого трафіку може вилучати інші ознаки, ніж програма для моніторингу продуктивності мережі.

3.3.2 Основні підходи до вилучення ознак в системах виявлення вторгнень

Ознаки на основі пакетів та на основі потоку є двома основними підходами до збору та аналізу мережевого трафіку в системах виявлення вторгнень (IDS). Кожен з цих підходів має свої переваги та недоліки, що робить їх більш або менш придатними для різних типів атак і ситуацій. Розглянемо їх детальніше.

Ознаки на основі пакетів (Packet level features) та на основі потоку (Flow level features) є двома основними підходами до збору та аналізу мережевого трафіку в системах виявлення вторгнень (IDS). Кожен з цих підходів має свої

переваги та недоліки, що робить їх більш або менш придатними для різних типів атак і ситуацій. Розглянемо їх детальніше.

Ознаки на основі пакетів.

Ознаки на основі пакетів зібрані безпосередньо з окремих мережевих пакетів, що передаються через мережу. Цей підхід зосереджений на детальному аналізі кожного пакету, його заголовків та вмісту, що дозволяє отримати точнішу інформацію про мережеві з'єднання. Системи виявлення вторгнень на основі пакетів (IDS) високо цінуються за їхню гнучкість у моделях виявлення вторгнень завдяки великому обсягу даних, які вони збирають, включаючи всі заголовки аж до прикладного рівня (рівень 7 OSI) і повне корисне навантаження. Це дозволяє точно визначити правила для будь-якої частини трафіку, що призводить до зменшення кількості помилкових спрацьовувань і підвищення надійності оповіщення. Пакетний аналіз включає перевірку таких характеристик, як IP-адреси, порти, протоколи, прапорці TCP, розмір пакету, час між пакетами та інші параметри.

Переваги цього підходу включають здатність точно виявляти конкретні аномалії, такі як неправильні або підроблені заголовки, зловмисні дані, несанкціоновані порти або спроби спілкування з відомими небезпечними IP-адресами. Однак, цей підхід має і недоліки. Враховуючи велику кількість пакетів, що можуть бути передані в мережі, аналіз кожного окремого пакету може вимагати значних обчислювальних ресурсів і часу. Крім того, пакетні IDS обробляють весь трафік, що надходить до них, що може призвести ще до більшого використання ресурсів.

Такий підхід не може забезпечити чіткої картини поведінки зловмисника, оскільки часто важливо аналізувати послідовність пакетів (тобто як вони взаємодіють між собою), а не лише окремі пакети.

Впровадження простих пакетних IDS є порівняно простим, оскільки немає необхідності попередньо декодувати протоколи. У деяких сценаріях, коли повні дані доступні в режимі реального часу, пакетні IDS відмінно справляються з максимальною роздільною здатністю в часі. Однак зашифроване корисне

навантаження створює проблему для таких систем, оскільки зіставлення підписів стає непрактичним і знижує ефективність виявлення.

Ознаки на основі потоку

Вилучення ознак на основі потоку часто покладається на протокол NetFlow. Записи NetFlow зазвичай містять агреговані дані аж до мережевого рівня (рівень OSI 3) і, в залежності від конфігурації, можуть містити специфічну транспортну інформацію (рівень OSI 4), наприклад, прапори TCP. Через обмеженість даних, доступних в IDS на основі потоку, визначення точних правил виявлення не завжди може бути здійсненним, що потенційно може призвести до зниження достовірності попереджень і збільшення кількості хибних спрацьовувань.

Генерація потокових записів призводить до затримки між встановленням з'єднання та передачею записів до IDS. Залежно від конфігурації, записи можуть надсилатися тільки після закриття з'єднання або таймауту, що потенційно може вплинути на завдання виявлення вторгнень.

Потоки можуть не мати достатньої часової роздільної здатності для деяких завдань виявлення вторгнень, наприклад, для визначення таймінгів передачі байтів.

Ознаки на основі потоку зосереджуються на аналізі більш крупних одиниць передачі даних, таких як потоки — сукупності пакетів, що належать до одного з'єднання або сесії між двома кінцевими точками (наприклад, клієнтом і сервером). Потоки можна визначати за допомогою певних атрибутів, таких як IP-адреси джерела та призначення, порти, а також інші параметри, що дозволяють відстежувати сесію між двома точками.

Аналіз потоку має значну перевагу в тому, що дозволяє виявляти аномалії, пов'язані з поведінкою на рівні з'єднання або сесії. Це може включати виявлення атак типу "brute force", спроб виведення сервісів з ладу (DoS), або тривалих підозрілих з'єднань, які можуть вказувати на віруси або ботнети. Потоковий аналіз більш ефективний у випадках, коли атакувальник намагається здійснити множинні запити через одну сесію або провести тривалі несанкціоновані з'єднання. Однак, з іншого боку, він менш детально вивчає індивідуальні пакети,

що може призвести до пропуску малих, але критичних аномалій, які виявляються лише на рівні окремих пакетів.

3.4 Огляд інструментів для вилучення ознак з мережевого трафіку

3.4.1 CICFlowMeter

CICFlowMeter — це потужний інструмент, створений для генерації мережевих потоків з мережевого трафіку, який дозволяє зібрати та структурувати дані для подальшого аналізу в системах виявлення вторгнень (IDS) та дослідженнях кібербезпеки [26]. Інструмент обробляє інформацію, що міститься в пакетах, і формує потоки, що представляють собою сукупності пакетів, які належать до одного сеансу між двома кінцевими точками (наприклад, між клієнтом і сервером). Цей підхід дозволяє зберігати важливі характеристики сесії, такі як час її початку та завершення, обсяг переданих даних і кількість пакетів, що передаються.

CICFlowMeter підтримує різні мережеві протоколи, включаючи TCP, UDP та ICMP, що дає змогу використовувати його для широкого спектра застосувань, від аналізу звичайного мережевого трафіку до виявлення аномалій або зловмисних дій, таких як DDoS-атаки, сканування портів, спроби злому та інші. Завдяки здатності генерувати числові ознаки для кожного потоку, інструмент дозволяє здійснювати глибший аналіз і застосовувати методи машинного навчання для виявлення відхилень у поведінці мережевих з'єднань.

Один з основних аспектів використання CICFlowMeter — це його здатність працювати з великими обсягами даних, що важливо для аналізу реального часу в умовах високої пропускної здатності мережі. Програма забезпечує створення зручних для обробки даних у вигляді CSV або JSON файлів, що дозволяє інтегрувати отримані дані в різні системи аналізу та виявлення загроз. Крім того, CICFlowMeter активно використовується для підготовки датасетів для тренування алгоритмів машинного навчання, зокрема в дослідженнях щодо класифікації атак.

CICFlowMeter є важливим інструментом в дослідженнях з кібербезпеки завдяки своїй здатності швидко та ефективно обробляти великі обсяги мережевого трафіку та генерувати відповідні ознаки, що дають змогу виявляти як нормальні, так і аномальні мережеві з'єднання. Він активно використовується в рамках датасетів CICIDS 2017 і CICIDS 2018, які є стандартними наборами даних для розробки та тестування алгоритмів виявлення вторгнень. Цей інструмент став важливим ресурсом для дослідників у галузі кібербезпеки, оскільки він забезпечує гнучкість і точність для виявлення різних типів атак і допомагає покращити існуючі методи захисту мереж.

3.4.2 Wireshark

Wireshark — це популярний і потужний інструмент для аналізу мережевого трафіку, який дозволяє перехоплювати, відображати та детально вивчати пакети, що передаються через комп'ютерні мережі. Він є відкритим програмним забезпеченням і підтримує численні мережеві протоколи, що дозволяє здійснювати глибокий аналіз з'єднань на різних рівнях. Wireshark здобув велику популярність серед фахівців з кібербезпеки, адміністраторів мереж, а також у сфері тестування програмного забезпечення, оскільки дає змогу досліджувати та усувати проблеми в мережах, а також виявляти аномалії або зловмисні дії.

Wireshark працює шляхом "прослуховування" мережі, де він перехоплює пакети, що проходять через мережеві інтерфейси. Інтерфейс Wireshark дозволяє детально відображати інформацію про кожен пакет: його заголовки, вміст, тип протоколу, IP-адреси джерела та призначення, порти і багато інших параметрів. Завдяки широким можливостям фільтрації, користувач може зосередитись лише на цікавих або підозрілих пакетах, що значно полегшує аналіз. Wireshark підтримує графічний інтерфейс, що робить його доступним для новачків, а також має потужні інструменти для досвідчених користувачів, зокрема можливість написання власних фільтрів і скриптів для автоматизації процесу.

Однією з основних переваг Wireshark є його здатність підтримувати величезну кількість мережевих протоколів, таких як TCP, UDP, HTTP, DNS, FTP, а також більше 1000 інших протоколів [27]. Це робить Wireshark універсальним

інструментом для аналізу як локальних, так і великих корпоративних мереж. Крім того, Wireshark має можливість декодувати зашифровані дані, якщо є відповідні ключі для дешифрування, що дозволяє досліджувати з'єднання, що використовують захищені протоколи, такі як SSL/TLS.

Wireshark активно використовують у багатьох сферах: від навчальних лабораторій і тестування мережевих пристроїв до виявлення проблем з безпекою та діагностики мережевих інцидентів. Оскільки він дає змогу не тільки перехоплювати пакети, але й аналізувати їх для виявлення аномалій або помилок в мережевих протоколах, Wireshark є незамінним інструментом для фахівців, які займаються забезпеченням безпеки, адмініструванням мереж або дослідженням мережевого трафіку.

3.4.3 Argus

Argus (Audit Record Generation and Utilization System) — це потужний інструмент для моніторингу та аналізу мережевого трафіку, який використовується для збору і аналізу інформації про потоки в мережі. Він забезпечує детальне відображення активності на рівні мережевих потоків, що дозволяє фахівцям з кібербезпеки та мережевих адміністраторів отримувати точні дані про всі з'єднання між пристроями в мережі. Argus підтримує великий набір протоколів і дозволяє збирати дані про різноманітні характеристики мережевого трафіку, такі як час, обсяг переданих даних, IP-адреси джерела і призначення, порти, типи протоколів та інші важливі параметри [28].

Однією з головних особливостей Argus є його здатність працювати з великими обсягами даних у реальному часі, що робить його ідеальним для моніторингу великих корпоративних мереж або інфраструктур з високою пропускною здатністю. Він забезпечує не лише моніторинг потоку трафіку, але й дозволяє зберігати статистику для подальшого аналізу, виявлення аномалій і проведення ретроспективного аналізу інцидентів безпеки. Argus здатний ефективно працювати в умовах активних атак на мережу, таких як DDoS-атаки або спроби зламів, надаючи важливу інформацію для виявлення зловмисних дій.

Argus збирає дані в формі потоків, що дозволяє здійснювати їх подальшу обробку та аналіз. Він генерує різноманітні метрики, що використовуються для класифікації трафіку, виявлення аномалій, а також для побудови моделей виявлення вторгнень. Завдяки своєму гнучкому інтерфейсу і можливості інтеграції з іншими системами, Argus активно застосовується у різних сферах: від наукових досліджень до практичних рішень для моніторингу великих мереж. Інструмент дозволяє розробникам створювати власні інтерфейси для роботи з даними і легко інтегрувати його в наявні інфраструктури для покращення безпеки.

Однією з переваг Argus є його висока масштабованість та ефективність. Завдяки продуманій архітектурі, Argus може працювати навіть з найбільшими мережами без значних втрат у продуктивності, що дозволяє йому обробляти величезні обсяги інформації про трафік в реальному часі. Цей інструмент є важливим компонентом для тих, хто займається забезпеченням безпеки мереж, аналізом мережевих даних і виявленням потенційних загроз.

3.4.4 Zeek

Zeek (раніше відомий як Bro) — це потужна система моніторингу мережевого трафіку та виявлення вторгнень, яка використовується для аналізу мережевих потоків та виявлення аномалій у реальному часі. Zeek працює на основі сценаріїв (scripts), що дозволяють налаштовувати систему під конкретні вимоги та специфічні потреби організації. Цей інструмент дозволяє детально аналізувати мережеві з'єднання, протоколи, а також виявляти складні атаки, такі як DDoS, сканування портів, спроби зламів і багато інших типів зловмисної діяльності. Однією з основних переваг Zeek є його гнучкість і можливість розширення для аналізу не лише базових мережевих даних, але й більш складних загроз.

Zeek збирає і обробляє дані про мережевий трафік, зокрема про потоки, які є основними одиницями для аналізу в системі. Інструмент працює з даними з різних протоколів, таких як HTTP, DNS, FTP, SSL/TLS, SMTP та багатьох інших. Zeek не лише збирає статистику про мережеві з'єднання, але й забезпечує

детальну інформацію про події, що відбуваються в мережі. Завдяки використанню сценаріїв, система може автоматично реагувати на конкретні події, що допомагає виявляти несанкціоновані дії або аномалії в реальному часі.

Однією з особливостей Zeek є його здатність проводити глибокий аналіз на рівні додатків, що дозволяє йому виявляти складні атаки, які можуть залишатися непоміченими для традиційних систем IDS. Наприклад, Zeek може здійснювати аналіз трафіку SSL/TLS і виявляти потенційні спроби компрометації або зловмисні з'єднання, навіть якщо дані зашифровані. Крім того, система здатна інтегруватися з іншими інструментами для подальшого аналізу, такими як Elastic Stack або інші системи для візуалізації та збереження даних.

Zeek активно використовується у великих організаціях, які потребують надійного моніторингу мережевого трафіку, а також у сфері академічних досліджень, де проводяться дослідження новітніх загроз та методів захисту. Завдяки своїй гнучкості, розширюваності та широким можливостям для налаштування, Zeek став одним із стандартів у галузі безпеки мереж, що дозволяє проводити ефективний аналіз та виявлення складних загроз на різних етапах атаки.

В таблиці 3.1 наведено узагальнена інформація про інструменти збору ознак

Таблиця 3.1 – Узагальнена інформація про інструменти збору ознак

Інструмент	Рівень
CICFlowmeter	Flow
Wireshark	Packet
Argus	Flow
Zeek	Packet, flow, application

Для подальшого дослідження було обрано CICFlowmeter та Zeek.

CICFlowmeter є потоковим аналізатором трафіку і використовувався при формуванні обраного відкритого датасету.

Натомість Zeek робить акцент на зборі всебічної інформації про трафік, іноді інтегруючи спеціальні аналізатори протоколів, пристосовані до протоколів середовища. Незважаючи на те, що ці інструменти функціонально перетинаються, їхні основні цілі та сценарії використання відрізняються.

3.5 Попередня обробка даних

Як було зазначено вище, набір даних CICIDS 2017 складається з 2830743 записів. Під час експерименту було виявлено декілька неповних записів у наборі даних, які було вилучено з файлу з допомогою команди `dropna()`. Було помічено, що атрибут «Fwd Header Length» набору даних існував двічі, що було виправлено шляхом видалення однієї копії атрибуту. «Flow Bytes/s» та “Flow Packets/s” містили значення infinity та NaN (відсутні значення), які було перетворено на цілі числа -1 та 0 відповідно. Також було визначено, що декілька атрибутів, включаючи стовпчик Label, були типу string. В результаті попередньої обробки всі мітки нормального трафіку були перетворені в ціле число 0, а мітки записів, що відповідали атакам, були перетворені в число 1.

Для оцінки ефективності навчання, виконаного моделлю, набір даних CICIDS 2017 розбивавали на дві частини: навчальну та тестову. Річ в тому, що якщо тренувати модель на всіх даних, вона може запам'ятати конкретні особливості даних (шум, випадкові коливання), а не навчитися узагальнювати на нові, невідомі дані. Це означає, що модель добре працюватиме лише на навчальному наборі, але її точність на нових даних може суттєво погіршитися. Тестова частина дозволяє оцінити, як добре модель працює на даних, яких вона не бачила під час тренування. Це важливо для перевірки здатності моделі до узагальнення і її реальної продуктивності.

Тому, як правило, алгоритми машинного навчання тренуються на навчальному наборі і перевіряються на тестовому наборі. Крім того, таке розбиття даних допомагає провести налаштування моделі оптимальним чином та знайти оптимальні параметри. В такому випадку навчальна частина використовується для тренування, а тестова – для оцінки того, які параметри працюють найкраще в реальних умовах.

Набір даних CICIDS 2017 був цілісним і не містив попередньо визначених навчальної та тестової частини, тому дані були розділені на дві частини за допомогою бібліотек python. Було використано функцію `train_test_split`

бібліотеки Sklearn, щоб випадковим чином розділити набір даних на 80% навчальних даних та на 20% тестових даних.

Крім того, було проведено нормалізацію для масштабування даних до діапазону [0,1], зі збереженням їх поведінки. Цей крок допомагає статистичним моделям і методам машинного навчання краще навчатись, при цьому вирівнюється вага всіх критеріїв. Нормалізація була виконана з допомогою Min-Max підходу.

3.6 Вилучення ознак

Як вже згадувалось раніше, обраний набір даних містив 83 ознаки, одна з яких була задубльована. Проте така кількість ознак значно сповільнює час навчання та тестування моделі. В цьому дослідженні ми вирішили застосувати метод головних компонент (Principal component analysis – PCA), щоб дослідити вплив кількості ознак на точність прогнозу.

Метод головних компонент (PCA) – це потужний статистичний метод, який використовується для зниження розмірності даних. Іншими словами, PCA дозволяє нам представити великі набори даних з багатьма змінними у вигляді меншої кількості нових змінних, які називаються головними компонентами. Ці компоненти впорядковані за спаданням їхньої здатності пояснювати варіацію в даних.

Якщо уявити собі багатовимірний набір даних як хмару точок у просторі, PCA знаходить нову систему координат, де осі відповідають напрямкам найбільшої дисперсії даних. Перша головна компонента вказує на напрямок, вздовж якого дані розкидані найбільше, друга – на наступний за величиною напрямок і так далі. Таким чином, PCA проектує дані на меншу кількість осей, зберігаючи при цьому максимальну інформацію.

Алгоритм методу в спрощеному вигляді може виглядати наступним чином:

Нехай X - матриця даних, де кожен рядок відповідає одному зразку, а кожен стовпець - одній змінній. Тоді:

1. Центрування даних: Спочатку дані центруються, щоб середнє значення кожної змінної було рівне нулю.
2. Обчислення коваріаційної матриці: Обчислюється коваріаційна матриця C.
3. Обчислення власних векторів V і власних значень Λ матриці C.
4. Вибір головних компонент: власні вектори V є головними компонентами.
5. Проєктування даних: нові дані Y обчислюються як $Y = X \cdot V$.

Зазвичай вибирають таку кількість головних компонент, яка пояснює достатню частку загальної дисперсії даних (наприклад, 95%). Або ж залишають тільки компоненти з власними значеннями, більшими за середнє арифметичне всіх власних значень

3.7 Ансамблювання

Ансамблювання – це потужна техніка в машинному навчанні, яка полягає в об'єднанні декількох моделей для отримання кращих результатів, ніж кожна модель окремо. Можна собі уявити собі групу експертів, кожен з яких має свої знання та досвід. Якщо об'єднати їхні думки, можна отримати більш точне рішення, ніж від кожного експерта окремо. Аналогічно, в машинному навчанні, об'єднання декількох моделей може значно підвищити точність прогнозів та стійкість до перенавчання.

Існує кілька методів ансамблювання, таких як беггінг, бустинг та стекинг. Беггінг полягає в навчанні декількох моделей на різних підмножинах даних, а потім усередненні їхніх прогнозів. Бустинг навчає моделі послідовно, причому кожна наступна модель намагається виправити помилки попередньої. Стекинг же використовує мета-модель для об'єднання прогнозів базових моделей. Вибір конкретного методу залежить від задачі та характеристик даних. В даній роботі ми вирішили застосувати найпростіший підхід, який обирає мітку як результат голосування більшості моделей. На рисунку 3.1 наведено загальний алгоритм запропонованого підходу.

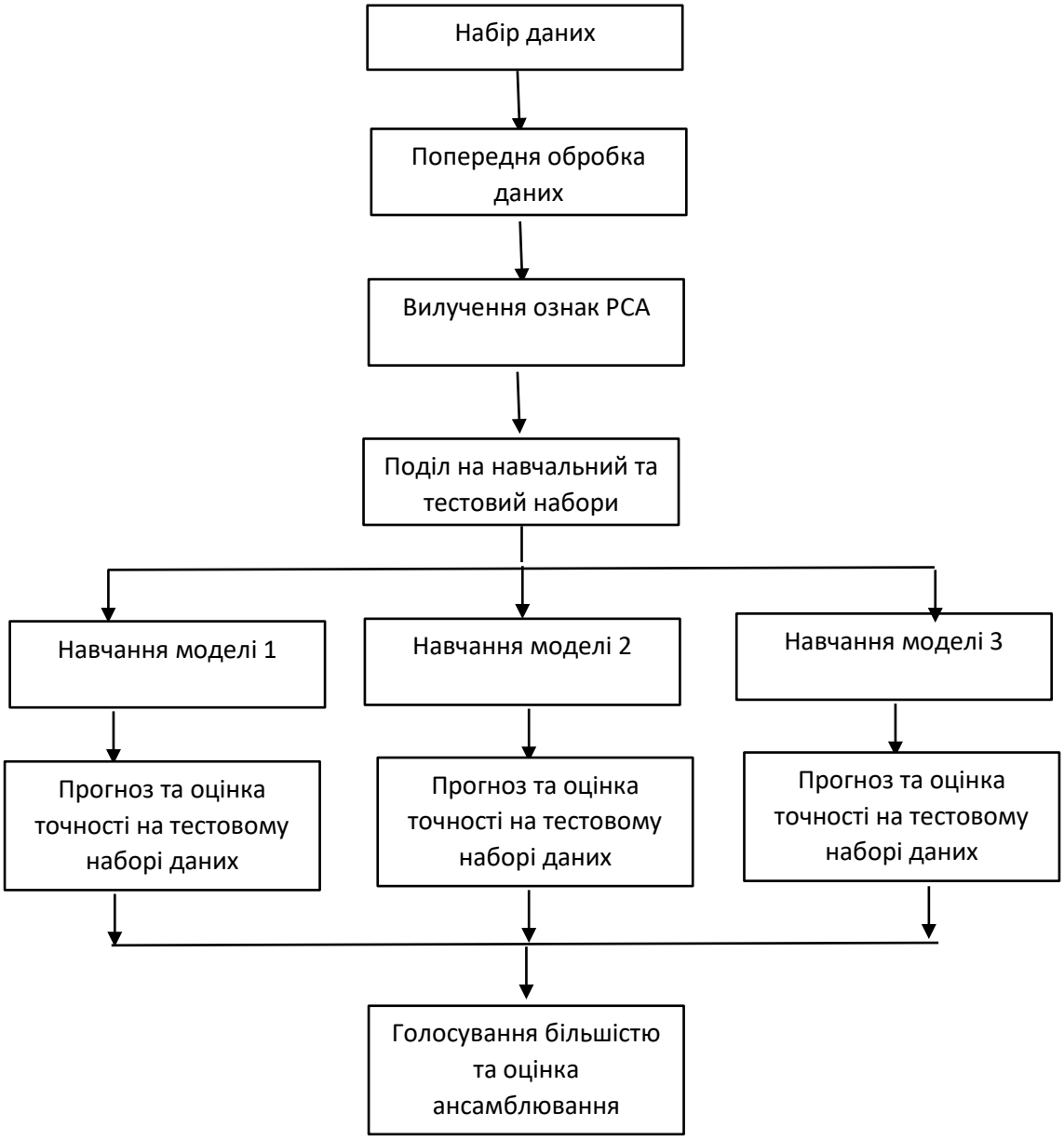

Рисунок 3.1 – Алгоритм запропонованого підходу

В рамках цього підходу ми спробуємо дослідити вплив кількості ознак на результати тестування

3.8 Результати тестування моделі

Для реалізації запропонованого підходу було обрано три моделі: модель Наївного Баєса, метод опорних векторів та випадков ліси. Імлементація вибраних моделей відбувалась у програмному середовищі Python 3, який став стандартом

де-факто для машинного навчання завдяки своїй простоті, гнучкості, великій екосистемі бібліотек та великій кількості ресурсів.

Основними бібліотеками Python, які використовуються при імплементації мооделей машинного навчання є:

- NumPy: для ефективних обчислень з багатовимірними масивами.
- Pandas: для маніпуляції та аналізу даних.
- Matplotlib та Seaborn: для візуалізації даних.
- Scikit-learn: для широкого спектру алгоритмів машинного навчання.
- TensorFlow та PyTorch: для глибокого навчання.
- Keras: високорівневий API для TensorFlow та інших фреймворків глибокого навчання.

Для вибору найкращих параметрів кожноїмоделі ми скористались функціоналом RandomizedSearchCV та GridSearchCV. RandomizedSearchCV вибирає випадкові діапазони значень гіперпараметрів з заданого розподілута дозволяє звузити діапазон гіперпараметрів для наступної функції. GridSearchCV систематично перебирає всі можливі комбінації значень гіперпараметрівзі знайденого діапазону. Це гарантує, що буде знайдена найкраща модель. Такий підхід буде оптимальним для великої кількості гіперпараметрів.

Для оцінки ефективності моделей машинного навчання використовують наступні метрики, що базуються на матриці помилок (confusion matrix), ідея якої зображена на рисунку 3.2

Actually Negative	**True Negative (TN)**	**False Positive (FP)**
Actual Positive	False Negative (FN)	True Positive (TP)
	Predicted Negative	**Predicted Positive**

Рисунок 3.2 - Confusion Matrix

Загальноприйнятими метриками класифікації є наступні:

- точність (Accuracy)

$$\text{Accuracy} = \frac{TN + TP}{TN + TP + FN + FP} \tag{3.1}$$

- влучність (Precision)

$$\text{Precision} = \frac{TP}{TP + FP} \tag{3.2}$$

- повнота (Recall)

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3.3}$$

- F1 score

$$\text{F1} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \tag{3.3}$$

Отже спочатку дослідимо влив кількості ознак, виділених за PCA методом на точність побудованої моделі.

На рисунку 3.3 наведено залежність характеристики F1 від кількості вибраних головних компонент.

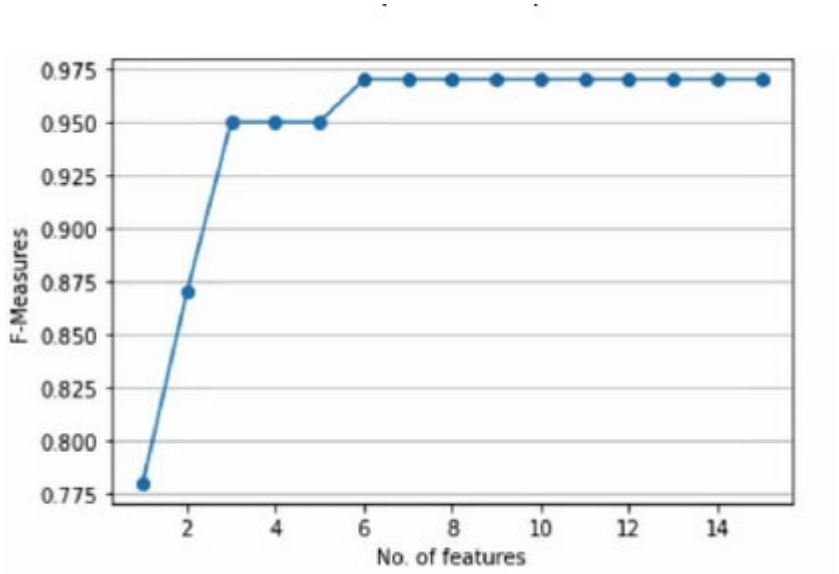

Рисунок 3.3 - Вплив кількості головних компонент на точність

Отже для оцінки ефективності вибраного підходу було обрано 7 та 8 компонент для порівняння.

Матриці похибок для двох варіантів кількостей головних компонент відображені в таблицях 3.2 та 3.3

Таблиця 3.2 – Матриця похибок для кількості головних компонент рівній 7

		Predicted	
		False	True
Actual	False	109070	2459
	True	7364	447256

Таблиця 3.3 – Матриця похибок для кількості головних компонент рівній 8

		Predicted	
		False	True
Actual	False	109087	2442
	True	7330	447290

Як бачимо зміна кількості компонент мінімальним чином вплинула на точність моделі.

В таблиці 3.4 наведено порівняння ефективності обраних моделей та запропонованого методу ансамблювання:

Таблиця 3.4 – Оцінка класифікації:

Кількість головних компонент	Моделі	Точність /Accuracy	Влучність/ Precision	Повнота/ Recall	F1
7	Ансамблювання	0,98	0,97	0,98	0,97
	Модель Байєса	0,85	0,74	0,7	0,72
	SVM	0,87	0,79	0,75	0,77
	Випадковий ліс	0,96	0,97	0,93	0,94
8	Ансамблювання	0,98	0,97	0,98	0,97
	Модель Байєса	0,84	0,73	0,7	0,72
	SVM	0,87	0,78	0,75	0,77
	Випадковий ліс	0,96	0,97	0,94	0,94

З таблиці 3.4 можемо зробити висновок, що ансамблювання моделей призводить до кращого результату. А вибір меншої кількості ознак хоч і в незначній мірі впливає на точність, проте значно економить обчислювальні та часові ресурси, необхідні на обробку даних.

Крім того, ми провели невелике дослідження впливу інструментів вилучення ознак з трафіку на прикладі CICFlowmeter та Zeek (таблиця 3.5).

Таблиця 3.5 – Порівняльний аналіз впливу програмних інструментів збору ознак з трафіку на точність класифікації

Інструмент	Моделі	F1
CICFlowmeter	Ансамблювання	0,97
	Модель Байєса	0,72
	SVM	0,77
	Випадковий ліс	0,94
Zeek	Ансамблювання	0,97
	Модель Байєса	0,73
	SVM	0,77
	Випадковий ліс	0,95

В даному випадку бачимо, що використання різних інструментів в даному випадку не значно вплинула на кінцеву якість моделі.

Для майбутніх досліджень варто було б спробувати різні техніки балансування датасету, а також розширити перелік інструментів вилучення ознак з трафіку з метою дослідження їх впливу на датасет, а також спробувати інші методи зменшення кількості ознак датасету.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою кваліфікаційної роботи магістра є дослідження шляхів підвищення ефективності виявлення аномалій для вдосконалення систем виявлення вторгнень. Оскільки, проведення робіт з розробки та використання системи передбачає використання комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників, в тому числі і фахівців з підвищення ефективності контролю доступу в приміщення, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом мінрегіону України від 13.11.2014 N 312 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких

розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп'ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п'ять комп'ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп'ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання

при відключенні має бути зворотним. Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп’ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп’ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

4.2 Безпека в надзвичайних ситуаціях

4.2.1 Міжнародний тероризм

Терор (лат. terror – страх, жах) – має ознаку «усувати», «закривати». Ця обставина і визначає терор як особливу форму політичного насильства, що

характеризується жорстокістю, цілеспрямованістю й уявленою ефективністю. Ці особливості визначили широке використання терору упродовж людської історії як засобу політичної боротьби в інтересах держави, організацій чи окремих угруповань. Безпосередньо сам факт привселюдної страти кримінальних чи політичних злодіїв, чи процес «аутодафе» в період середньовікової інквізиції, є класичною формою терору в інтересах держави чи католицької церкви.

Правовою основою боротьби з міжнародним тероризмом є «Декларація про заходи для ліквідації міжнародного тероризму», що затверджена на 49-й сесії Генеральної асамблеї ООН (резолюція 49/60 від 9 грудня 1994 р.)

Цей документ встановлює принципи відносин світової спільноти і програму заходів з метою ліквідації такого огидного суспільного явища, як міжнародний тероризм, а також встановлює подальше співробітництво між державами для невідкладної ліквідації будь-яких форм і проявів терористичної діяльності. Характерним для розвитку світової спільноти є те, що наявність лідера (провідної країни чи провідної сили) народжує відповідну реакцію – формування нижчого за рангом (рівнем) іншого лідера (іншої країни чи іншої провідної сили). Має місце формування біполярності, виникають реалії антагонізму на різних рівнях світового суспільства На другому етапі формування ці політичні, злочинні та інші сили (групи) шукають собі відповідні «ніші» існування; економічну, політичну, наукову та інші види підтримок; формують свої озброєні сили, відповідні професійні кадри, джерела озброєння, територію знаходження тощо. При цьому використовуються всі «блага» цивілізації особистого розвитку і поширення впливу на світову спільноту.

Міжнародний тероризм, створюючи свій плацдарм, може викликати кризи (системні) в світовій, моральній, політичній, економічній системі відносин і зруйнувати та усунути всі передумови розвитку світової спільноти.

В Україні, за даними служби безпеки, за останні два роки скоєно понад 560 злочинів терористичного характеру, внаслідок цього 90 осіб (із них 15 представників владних структур) загинуло. В Україні зростає активність міжнародних терористичних організацій, насамперед із країн Ближнього Сходу («Хезбола», «Абу Ніджаль», «Хамас», «Брати мусульмани»), які прагнуть

використати територію України для транзиту своїх бойовиків до країн західної Європи, підготовки терористичних акцій.

Головними принципами попередження та боротьби з міжнародним тероризмом має стати постійне удосконалення відповідної законодавчої бази, співробітництво з правоохоронними організаціями, консолідація з іншими країнами й організація напрямів запобігань поширенню будь-яких терористичних організацій і угруповань.

Терористичний акт не має безпосередніх можливостей досягнення оголошеної кінцевої мети і звичайно складається з таких елементів: насильницька дія у різноманітних її формах, політичний мотив в основі здійснення самого терористичного акту; сам акт спрямовано проти осіб, організацій, націй, національностей і меншин, державних інститутів чи їх представників з метою їх залякування чи виконання окремих вимог. Терор щодо націй, етнічної, расової чи релігійної групи, що здійснюється для її повного чи часткового усунення, розглядається світовою спільнотою вже як акт геноциду.

Варіанти комбінацій за спрямованістю суб'єкт—об'єкт здійснення терористичного акту багатоспрямовані, тому важко дати універсальне визначення «терору». Проте деякі критерії певної класифікації можна встановити:

- індивідуальний, організований терор і терор як політика держави;
- терор як метод внутрішньополітичної боротьби і терористичні акти міжнародного характеру.

4.2.2 Структура системи БЖД

Поняття «життєдіяльність» стосується тільки людини. Людина живе і працює в безпосередньому зв’язку з навколишнім середовищем.

Життєдіяльність (ЖД) – це складна фізіологічна система, яка має назву «система ЖД».

Системою називають сукупність взаємозв’язаних елементів, функціонування яких спрямоване на досягнення певної загальної мети.

Система ЖД складається із взаємопов’язаних елементів: життя, діяльності людини, навколишнього середовища, – і має підтримувати комфортне та безпечне існування людини, забезпечити сталий розвиток людства.

Розглянемо характеристики елементів системи ЖД.

Життя – це форма існування матерії, яка характеризується обміном речовин, здатністю до розмноження і розвитку, вмінням пристосовуватись до навколишнього середовища.

Людина – вища форма розвитку живої матерії, і її існування – дуже складний процес, що не тільки підтримує її фізіологічний стан, але й задовольняє духовні потреби. Крім того, на життя людини суттєво впливають умови проживання та праці, медичний догляд і багато інших факторів, що виникають завдяки діяльності самих людей.

Діяльність – це специфічна форма ставлення людей до навколишнього середовища та одне до одного, яка має задовольняти потреби та інтереси людини. Це соціальна категорія, нерозривно зв’язана із суспільством. Тільки завдяки діяльності людини створено всі блага, які має людство.

Основні види діяльності такі:

- виробнича;
- наукова;
- мистецька;
- освітня.

Однією із специфічних форм діяльності людини є праця – перша й основна умова існування людини (людства).

Праця – цілеспрямована діяльність людини, у процесі якої вона впливає на природу і використовує її з метою виробництва матеріальних та інших благ, необхідних для задоволення своїх потреб.

Потреби – це необхідність для людини того, що забезпечує її існування і самозабезпечення (фізіологічне, матеріальне, соціальне, духовне та ін.).

Навколишнє середовище (довкілля) або середовище існування – це все, що оточує людину впродовж її життя. Навколишнє середовище, у свою чергу, поділяють на такі види:

- природне середовище;
- штучне середовище.

Природне середовище (біосфера) – це частина Землі і простору навколо неї, де зосереджено все живе. Біосфера включає:

- атмосферу (газоподібна частина);
- гідросферу (рідка водна частина);
- літосферу (тверда частина).

На ЖД людей найбільше впливає частина біосфери від поверхні Землі вглиб на 15–20 км і до висоти 20–22 км, де починається озоновий шар. Природне середовище є джерелом природних ресурсів для існування людини: повітря, води, деревини, корисних копалин, ґрунту та ін.

Штучне середовище – це складова довкілля, створена людством за тривалий час його існування. Штучне середовище умовно можна поділити на два види:

- виробниче середовище;
- побутове середовище.

Виробничим називають середовище, в якому людина реалізує свою трудову діяльність (підприємства, установи, навчальні заклади тощо).

Побутовим є середовище, де люди мешкають або проводять вільний час. Воно охоплює сукупність житлових будинків, комунально-побутових об’єктів, місця відпочинку та ін.

Організм людини може нормально функціонувати тільки тоді, коли умови (параметри) зовнішнього середовища відповідають оптимальним. Якщо умови середовища змінюються, стають несприятливими, то на протидію їм організм людини включає спеціальні механізми, які зберігають постійність параметрів внутрішнього середовища (всередині організму) чи змінюють їх у межах допустимого.

Можливість функціонування організму в середовищі, параметри якого постійно змінюються, забезпечується завдяки механізму, який називають адаптацією.

Адаптація (лат. adapto – пристосування) – динамічний процес пристосування організму до мінливих умов зовнішнього середовища, який

спостерігається в будь-якому виді діяльності щоразу, коли виникають значні зміни в системі «людина – середовище». Адаптація може бути фізіологічною, психологічною, соціальною.

Отже, для функціонування системи ЖД середовище має обов'язково відповідати природним параметрам. Відхилення можливі в межах допустимого, коли організм людини здатний адаптуватися, захистити себе, підтримувати існування. Усе, що існує за цими межами, становить загрозу життю, тому виникає потреба захисту ЖД людей. Отже, безпека – важлива складова системи ЖД.

Розглядаючи систему ЖД як взаємодію людей з навколишнім середовищем, слід зауважити, що вона завжди підпорядкована певним принципам, правилам, умовам життя, природним умовам, традиціям тощо.

Система ЖД має такі характерні ознаки:

- її функціонування підпорядковане об'єктивним законам природи;
- це динамічна система, яка розвивається, удосконалюється, пристосовується до змін умов існування;
- тяжіє до сталого розвитку, вживаючи заходів захисту від упливу негативних факторів.

Основні принципи забезпечення ЖД такі:

- своєчасність, достатність, якість забезпечення людей необхідними для життя засобами високої якості і заходами в потрібний час у належній кількості;
- безпека ЖД (захист ЖД від упливу негативних факторів, що виникають унаслідок як природних явищ, так і діяльності людей).

Рівень реалізації цих принципів значною мірою залежить від способів забезпечення ЖД. Виходячи із сказаного, можна визначити такі головні способи забезпечення ЖД:

1. Організація ефективної трудової діяльності людей в суспільстві з максимальним залученням усіх ресурсів (створення робочих місць, упровадження високопродуктивного виробництва і технологій, нормування праці тощо).

2. Організація та удосконалення освіти і підготовка кадрів, розвиток науки відповідно до вимог часу.

3. Розвиток сфери послуг (комунальних, транспортних, торговельних, побутових і т. ін.).

4. Розширення мережі культурних, спортивних, розважальних установ.

5. Проведення заходів щодо збереження здоров'я людей (диспансеризація, оздоровлення, кваліфіковане медичне обслуговування і лікування, санітарно-епідеміологічний стан).

6. Розроблення законодавчих і нормативно-правових актів із забезпечення прав, свобод і захисту людей і суспільства в цілому.

Залежно від того, якою мірою реалізуються принципи та способи забезпечення ЖД, визначається рівень життя людей окремих країн і загальний розвиток людства.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи освітнього рівня «Магістр» було досліджено вплив інструментів вибору ознак з мережевого трафіку та розмірності простору ознак на точність класифікації атак в мережевому трафіку. Для дослідження використано відкритий набір даних CICIDS у форматі CSV файлів

Було досягнуто виконання наступних завдань:

- проведено аналіз загроз мережевій безпеці;
- здійснено огляд літератури стосовно способів і засобів виявлення вторгнень;
- проаналізовано теоретичні підходи для виявлення аномалій;
- проведено аналіз інструментів отримання ознак з мережевого трафіку;
- проведено дослідження впливу на точність виявлення вторгнень кількості ознак та інструменту їх отримання;
- проведено оцінку якості різних класифікаційних моделей з використанням відкритих датасетів;
- запропоновано підхід ансамблювання результатів кількох класифікаційних моделей, що дозволило підвищити точність виявлення атак;
- розглянуто окремі питання з охорони праці і безпеки в надзвичайних ситуаціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Top Cybersecurity Statistics for 2024. [Електронний ресурс]. URL: https://www.cobalt.io/blog/cybersecurity-statistics-2024
2. IBM X-Force Threat Intelligence Index 2024. [Електронний ресурс]. URL: https://www.ibm.com/reports/threat-intelligence
3. Jian He; The research of computer network security and protection strategy. AIP Conference. Proceedings. 8 May 2017; Volume 1839, Issue 1: 020173. https://doi.org/10.1063/1.4982538
4. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.
5. A. Simmonds, P. Sandilands, and L. Van Ekert “An ontology for network security attacks,“ In: Asian Applied Computing Conference. Springer, pp. 317-323, 2004.
6. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.
7. Hasan, Mohammad & Khan, Ruzaina. (2017). NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW. International Journal of Advanced Computer Research. 9. 10.26483/ijarcs.v8i9.4641.
8. Kharchenko, O., Raichev, I., Bodnarchuk, I., & Zagorodna, N. (2018, February). Optimization of software architecture selection for the system under design and reengineering. In 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) (pp. 1245-1248). IEEE.
9. c. Manimegalai and A. Sumithra, “An Overview of Attacks in the Network Security System,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 10, pp. 816–819, 2015.

10. Priyank Sanghavi, Kreena Mehta, Shikha Soni. Network Security. International Journal of Scientific and Research Publications, Volume 3, Issue 8, August 2013 URL: https://www.ijsrp.org/research-paper-0813/ijsrp-p20131.pdf
11. Kharchenko, A., Halay, I., Zagorodna, N., & Bodnarchuk, I. (2015, September). Trade-off optimal decision of the problem of software system architecture choice. In 2015 Xth International Scientific and Technical Conference" Computer Sciences and Information Technologies"(CSIT) (pp. 198-205). IEEE.
12. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.
13. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081
14. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.
15. Veeramreddy, Jyothsna & Prasad, Koneti. (2019). Anomaly-Based Intrusion Detection System. Computer and Network Security DOI:10.5772/intechopen.82287
16. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.
17. Caulkins LTCBD, Lee J, Wang M. dynamic data mining technique for intrusion detection systems. In: Proceedings of the 43rd Annual Southeast Regional Conference (ACM-SE 43). Vol. 2. 2005. pp. 148-153

18. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.
19. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
20. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
21. Ashfaq Khan, Muhammad & Kim, Yangwoo. (2021). Deep Learning-Based Hybrid Intelligent Intrusion Detection System. Computers, Materials & Continua. 68. 10.32604/cmc.2021.015647.
22. Fryz, M., Mlynko, B., Mul, O., & Zagorodna, N. (2010). Conditional Linear Periodical Random Process as a Mathematical Model of Photoplethysmographic Signal. Rigas Tehniskas Universitates Zinatniskie Raksti, 45, 82.
23. Mahesh, B. (2020) Machine Learning Algorithms—A Review. International Journal of Science and Research, 9, 381-386.
24. N Zagorodna, M Stadnyk, B Lypa, M Gavrylov, R Kozak. 2022. Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, No 1, P. 55-61
25. Lalduhsaka, R. & Bora, Nilutpol & Khan, Ajoy. (2022). Anomaly-Based Intrusion Detection Using Machine Learning: An Ensemble Approach. International Journal of Information Security and Privacy. 16. 1-15. 10.4018/IJISP.311466.
26. Derkach, M., Skarga-Bandurova, I., Matiuk, D., & Zagorodna, N. (2022, December). Autonomous quadrotor flight stabilisation based on a complementary filter and a PID controller. In 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-7). IEEE.

27. Wireshark.URL: https://www.wireshark.org/
28. Argus. URL: https://openargus.org/
29. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання «БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ» / В.С. Стручок – Тернопіль: ФОП Паляниця В.А., – 156 с. Отримано з https://elartu.tntu.edu.ua/handle/lib/39196.

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XIII Міжнародної науково-практичної конференції молодих учених та студентів
11-12 грудня 2024 року

УКРАЇНА
ТЕРНОПІЛЬ – 2024

Матеріали XIII Міжнародної науково-практичної конференції молодих учених та студентів
«АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 11-12 грудня 2024 року

УДК 004.056

Р.С.Липянчик, Б.М. Липа, О.В.Мардинавка
(Тернопільський національний технічний університет імені Івана Пулюя)

ШЛЯХИ УДОСКОНАЛЕННЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖЕВИХ IDS СИСТЕМАХ

UDC 004.056

R. Lypianchyk, B. Lypa, O. Mardynavka

WAYS TO IMPROVE INTRUSION DETECTION IN NETWORK IDS SYSTEMS

Використання комп'ютерних систем та Інтернету останнім часом призвело до серйозних проблем безпеки, приватності та конфіденційності. Кількість кібератак постійно зростає, і з кожним роком вони стають більш складними та витонченими. Злочинці використовують новітні методи, такі як атаки нульових днів, фішинг, складні типи DoS-атак і шкідливі програми.

Комерційні компанії широко використовують IDS (системи виявлення вторгнень) та IPS (системи запобігання вторгненням) для забезпечення безпеки своїх інформаційних систем і захисту від руйнівних кібератак. Ці технології працюють разом, але мають різні функції та завдання [1]. Системи виявлення вторгнень (Intrusion Detection System IDS) допомагають аналізувати мережевий трафік і генерувати сповіщення в разі виявлення зловмисної активності. Система запобігання вторгненням (Intrusion Prevention System IPS) активно реагує на потенційні загрози, не лише виявляючи їх, але й блокуючи або припиняючи атакуючі дії в реальному часі.

Деякі організації використовують брандмауери, а також маршрутизатори разом з IPS/IDS. Основна різниця між ними полягає в тому, що брандмауер перевіряє лише IP-адресу та номер порту. Використовуючи номер порту та IP-адресу, він блокує трафік. Брандмауер - це перша лінія, яка може захистити мережу від зловмисників. Він може виявити лише обмежену кількість атак. Тому рекомендують додатково використовувати IDS/IPS, щоб забезпечити додатковий рівень захисту трафіку від атак з боку веб-серверів, доступних з Інтернету [2].

Відповідно до [3], IDS є одним з широко розповсюджених інструментів, що дозволяє здійснювати моніторинг цілого ряду мережевих систем, хмарних обчислень, а також інформаційної системи. За місцем встановлення систем виявлення вторгнень (IDS), їх поділяють на:

- Мережеві IDS (NIDS - Network IDS). Ці системи розташовані на рівні мережі і аналізують весь трафік, що проходить через мережу. Вони допомагають виявити атаки, спрямовані на мережу або що використовують мережеві вразливості.
- Хостові IDS (HIDS - Host IDS). Ці системи встановлюються на окремих пристроях (наприклад, серверах, комп'ютерах) і контролюють їх активність, включаючи доступ до файлів, журнали подій, використання процесора тощо.

NIDS сканує мережевий трафік з сегмента локальної мережі. Він також може відстежувати більше мережевих цілей, намагаючись виявити загрози, які можуть бути пропущені HIDS, оскільки HIDS не може читати заголовки пакетів і не може виявити певні

Додаток А Лістинг програми

```
import pandas as pd
import numpy as np
from sklearn.model_selection import train_test_split, RandomizedSearchCV, GridSearchCV
from sklearn.preprocessing import MinMaxScaler
from sklearn.decomposition import PCA
from sklearn.naive_bayes import GaussianNB
from sklearn.svm import SVC
from sklearn.ensemble import RandomForestClassifier, VotingClassifier
from sklearn.metrics import accuracy_score

# Завантаження набору даних
data = pd.read_csv('CICIDS2017.csv')

# Видалення пропущених даних
data = data.dropna()

# Обробка "Flow Bytes/s" та "Flow Packets/s"
data['Flow Bytes/s'] = data['Flow Bytes/s'].replace([np.inf, -np.inf], -1).fillna(0).astype(int)
data['Flow Packets/s'] = data['Flow Packets/s'].replace([np.inf, -np.inf], -1).fillna(0).astype(int)

# Перетворення міток (Label)
data['Label'] = data['Label'].apply(lambda x: 0 if 'BENIGN' in x else 1)

# Відокремлення ознак і міток
X = data.drop('Label', axis=1)
```

```
y = data['Label']

# Масштабування даних
scaler = MinMaxScaler()
X_scaled = scaler.fit_transform(X)

# PCA для зменшення кількості ознак до 8
pca = PCA(n_components=8)
X_pca = pca.fit_transform(X_scaled)

# Розділення даних на навчальні та тестові
X_train, X_test, y_train, y_test = train_test_split(X_pca, y, test_size=0.2,
random_state=42)

# Модель Байєса
nb = GaussianNB()
nb.fit(X_train, y_train)
y_pred_nb = nb.predict(X_test)
nb_accuracy = accuracy_score(y_test, y_pred_nb)

# Модель SVC з RandomizedSearchCV
svc = SVC()
svc_params = {
    'C': [0.1, 1, 10, 100],
    'gamma': [1, 0.1, 0.01, 0.001],
    'kernel': ['linear', 'rbf']
}
random_search_svc = RandomizedSearchCV(svc, svc_params, n_iter=10, cv=3,
random_state=42)
random_search_svc.fit(X_train, y_train)
```

```
y_pred_svc = random_search_svc.predict(X_test)
svc_accuracy = accuracy_score(y_test, y_pred_svc)

# Модель Random Forest з GridSearchCV
rf = RandomForestClassifier(random_state=42)
rf_params = {
    'n_estimators': [50, 100, 200],
    'max_depth': [10, 20, None],
    'min_samples_split': [2, 5, 10]
}
grid_search_rf = GridSearchCV(rf, rf_params, cv=3)
grid_search_rf.fit(X_train, y_train)
y_pred_rf = grid_search_rf.predict(X_test)
rf_accuracy = accuracy_score(y_test, y_pred_rf)

# Ансамблювання за принципом голосування більшістю
voting_clf = VotingClassifier(
    estimators=[('nb', nb), ('svc', random_search_svc.best_estimator_), ('rf',
grid_search_rf.best_estimator_)],
    voting='hard'
)
voting_clf.fit(X_train, y_train)
y_pred_voting = voting_clf.predict(X_test)
voting_accuracy = accuracy_score(y_test, y_pred_voting)

# Виведення результатів
print(f"GaussianNB Accuracy: {nb_accuracy:.2f}")
print(f"SVC Accuracy: {svc_accuracy:.2f}")
print(f"Random Forest Accuracy: {rf_accuracy:.2f}")
print(f"Voting Classifier Accuracy: {voting_accuracy:.2f}")
```