Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод виявлення аномалій у транспортній комп'ютерній мережі

(тема)

Виконав:

студент II курсу, групи КСМм-21-1

Волошин І.А.
(прізвище, ініціали)

Спеціальність

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

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

Освітня програма

Комп’ютерні системи та мережі
(повна назва освітньої програми)

Керівник: проф. Кучук Н.Г.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

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

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

Освітня програма Комп’ютерні системи та мережі
(повна назва)

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

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Волошину Іллі Андрійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Метод виявлення аномалій у транспортній комп'ютерній мережі

затверджена наказом по університету від “ 07 ” листопада 2022 р. № 1453 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2022 р.

3. Вхідні дані до роботи 1) методи побудови систем виявлення аномалій;
2) системи машинного навчання; 3) стандартні набори навчальних даних.

4. Перелік питань, що потрібно опрацювати у роботі
1) аналіз предметної області та постановка завдання;
2) огляд систем виявлення аномалій;
3) розробка моделі системи;
4) проведення експериментальних досліджень;
5) висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Демонстраційні матеріали. Плакати – 12 арк. ф. А4

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень	08.11.22-14.11.22	
2	Розробка моделі виявлення аномалій	15.11.22-21.11.22	
3	Розробка процедур та наборів даних	22.11.22-25.11.22	
4	Проведення експериментів	26.11.22-02.12.22	
5	Оформлення матеріалів кваліфікаційної роботи	03.12.22-06.12.22	
6	Подання кваліфікаційної роботи керівникові та	07.12.22-08.12.22	
	її попередній захист		
7	Подання кваліфікаційної роботи на рецензу-	09.12.22-12.12.22	
	вання		

Дата видачі завдання 07 листопада 2022 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Кучук Н.Г.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 68 с., 17 рис., 5 табл., 2 дод., 39 джерел.

АТАКА, ВИЯВЛЕННЯ АНОМАЛІЙ, КЛАСТЕРИЗАЦІЯ, МАШИННЕ НАВЧАННЯ, ТРАНСПОРТНА КОМП’ЮТЕРНА МЕРЕЖА.

Метою кваліфікаційної роботи є розробка методу для виявлення аномалій транспортній комп’ютерній мережі на основі класифікації атак.

У ході виконання кваліфікаційної роботи запропоновано модель глибокого навчання для виявлення аномалії в транспортній комп’ютерній мережі. Представлено комплексну структуру для підготовки даних мережевого трафіку для розробки вказаної системи. Обгрунтовано метод вибору ознак усереднення з використанням кластеризації K-means для підвищення ефективності запропонованої системи і для виконання аналізу мережних атрибутів і атак з метою моніторингу мережі.

ABSTRACT

Master’s thesis: 68 pages, 17 figures, 5 tables, 2 appendices, 39 sources.

ANOMALY DETECTION, ATTACK, CLUSTERIZATION, MACHINE LEARNING, VEHICULAR COMPUTER NETWORK.

The major goal of this thesis is to develop a method for detecting anomalies in the vehicular computer network based on the classification of attacks.

During the qualification work, a deep learning model was proposed for anomaly detection in the vehicular computer network. A comprehensive framework for preparing network traffic data for the development of the specified system is presented. The method of selecting averaging features using K-means clustering is substantiated to increase the efficiency of the proposed system and to perform analysis of network attributes and attacks for the purpose of network monitoring.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ANN – штучна нейронна мережа (англ., Artificial Neural Network)

CICIDS – Канадський інститут систем виявлення невідомих вторгнень (англ., Canadian Institute for Obscurity Intrusion Detection System)

CNN – згорткова нейронна мережа (англ., Convolutional Neural Network)

DT – дерева рішень (англ., Decision Trees)

DFEL – метод машинного навчання (англ., Deep Feature Embedding Learning)

DL – глибоке навчання (англ., Deep Learning)

DeeRaI – глибокий радіальний інтелект (англ., Deep Radial Intelligence)

DoS – відмова в обслуговуванні (англ., Denial of Service)

DNS – система доменних імен (англ., Domain Name System)

GNB – гаусівський наївний байєс (англ., Gaussian Naive Bayes)

GBT – дерево посилення градієнта (англ., Gradient Boosting Tree)

IoT – інтернет речей (англ., Internet of Things)

IG – приріст інформації (англ., Information Gain)

ID – виявлення вторгнень (англ., Intrusion Detection)

IDS – система виявлення вторгнень (англ., Intrusion Detection System)

IVADE – автомат виявлення вторгень всередині транспортного засобу (англ, In-Vehicle Anomaly Detection Engine)

KNN – K-найближчі сусіди (англ., K-Nearest Neighbors)

LR – логістична регресія (англ., Logistic Regression)

LSTM – довга короткочасна пам'ять (англ., Long Short-Term Memory)

ML – машинне навчання (англ., Machine Learning)

MQTT – телеметричний транспорт черги повідомлень (англ., Message Queuing Telemetry Transport)

MADAMID – дані аудиту видобутку для автоматизованих моделей ідентифікації (англ., Mining Audit Data for ID Automated Models)

MLP – багатошаровий персептрон (англ., Multi-Layer Perceptron)

NB – наївний байєс (англ., Naive Bayes)

NIDS – система виявлення вторгнень у мережу (англ., Network Intrusion Detection System)

NIMS – група управління та безпеки мережевої інформації (англ., Network Information Management and Security Group)

PCA – аналіз головних компонент (англ., Principle Component Analysis)

RBF – радіальна базисна функція (англ., Radial Basis Function)

RF – випадковий ліс (англ., Random Forest)

RBM – обмежена машина Больцмана (англ., Restricted Boltzmann Machine)

RNN – рекурентна нейронна мережа (англ., Recurrent Neural Network)

RSU – придорожній блок (англ., Roadside Unit)

SOM – самоорганізуючі карти (англ., Self-Organizing Maps)

SNN – спільний найближчий сусід (англ., Shared Nearest Neighbor)

SVM – підтримуюча векторна машина (англ., Support Vector Machine)

UNSW – університет Нового Південного Уельсу (англ., University of New South Wales)

VANETS – автомобільні мережі типу «Ad hoc» (англ., Vehicular Ad Hoc Networks)

xNN – пояснювана нейронна мережа (англ., Explainable Neural Network)

ВСТУП

Проблема виявлення та ідентифікації складних кібератак в широкому діапазоні галузей зараз ускладнюється. Одним із прикладів таких галузей є транспортні мережі (англ., Internet of Vehicles, IoV). IoV – це мережа транспортних засобів, яка складається з датчиків, актуаторів (приводів), мережевих рівнів і систем зв'язку між транспортними засобами. Вагомою складовою IoV є комунікації. Транспортні засоби в мережі обмінюються інформацією на основі кількох протоколів. Через бездротовий зв'язок між транспортними засобами вся мережа стає чутливою до кібератак. Під час таких атак конфіденційна інформація може передаватися зловмисній мережі або фіктивному користувачу, що призведе до зловмисних атак на IoV.

Протягом останніх кількох років виявлення атак в IoV було складним завданням. Традиційним системам виявлення вторгнень (IDS) стає дедалі важче виявляти нові, складніші атаки, які використовують незвичайні схеми. Щоб уникнути виявлення, зловмисники маскуються під типових користувачів. Ці проблеми можна вирішити за допомогою глибокого навчання. Для виявлення зловмисних атак було реалізовано багато моделей машинного та глибокого навчання (DL), проте вибір функцій залишається основною проблемою. Завдяки використанню навчальних емпіричних даних DL самостійно визначає ознаки вторгнення.

В даній кваліфікаційній роботі пропонується модель вторгнення на основі DL, яка зосереджена на атаках типу «відмова в обслуговуванні» (DoS). При цьому використовується кластеризація K-means для оцінки та ранжирування ознак. Після виділення найкращих функцій для виявлення аномалій застосовується новий метод пояснюваної нейронної мережі (англ., Explainable Neural Network, xNN), який дозволяє окремо класифікувати атаки в наборах даних CICIDS2019 і UNSW-NB15. Метод показав хороші результати щодо точності, влучності, повноти, міри F1. Для порівняння

можна побачити, що запропонований метод xNN демонструє хороші результати після використання техніки підрахунку характеристик. У наборі даних 1 (UNSW-NB15) xNN показав найвищу точність 99,7%, тоді як CNN – 87%, LSTM – 90%, DNN – 92%. xNN досяг найвищої точності 99,3% під час класифікації атак у другому наборі даних (CICIDS2019), CNN – 87%, LSTM – 89%, DNN – 82%. Запропоноване рішення перевершує існуючі системи за точністю виявлення та класифікації.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Виявлення аномалій у транспортних мережах

Транспортна мережа (англ., Internet of Vehicles, IoV) – це відкрита конвергентна мережева система, яка заохочує взаємодію між людьми, транспортними засобами та навколишнім середовищем [1, 2]. Завдяки автомобільним мережам типу «Ad hoc» (англ., Vehicular Ad Hoc Networks, VANET), хмарним обчисленням і багатоагентним системам (англ., Multi-Agent Systems, MAS), ця гібридна парадигма відіграє вирішальну роль у розробці інтелектуальної транспортної системи, яка є одночасно кооперативною та ефективною [3]. Задля забезпечення достовірності та безпеки даних сучасному невизначеному світі важливою для IoV є наявність системи виявлення аномалій. Проте, якщо справа доходить до аналізу критичних даних безпеки, слід враховувати вартість виявлення аномалій у режимі реального часу всіх даних у пакеті даних [4].

Можна констатувати, що IoV складається з трьох рівнів:

- рівень збираних даних та керування;
- обчислювальний рівень;
- прикладний рівень.

На рівні збираних даних та керування здійснюється моніторинг та керування транспортним засобом відповідно до отриманих даних та інформації з навколишнього середовища. На обчислювальному рівні транспортні засоби спілкуються за допомогою WLAN, стільникового зв’язку (4G/5G) і бездротових мереж малого радіусу дії [5]. На прикладному рівні реалізуються закриті та відкриті моделі обслуговування, або різні моделі IoV. Ключові компоненти транспортної мережі показано на рисунку 1.1.

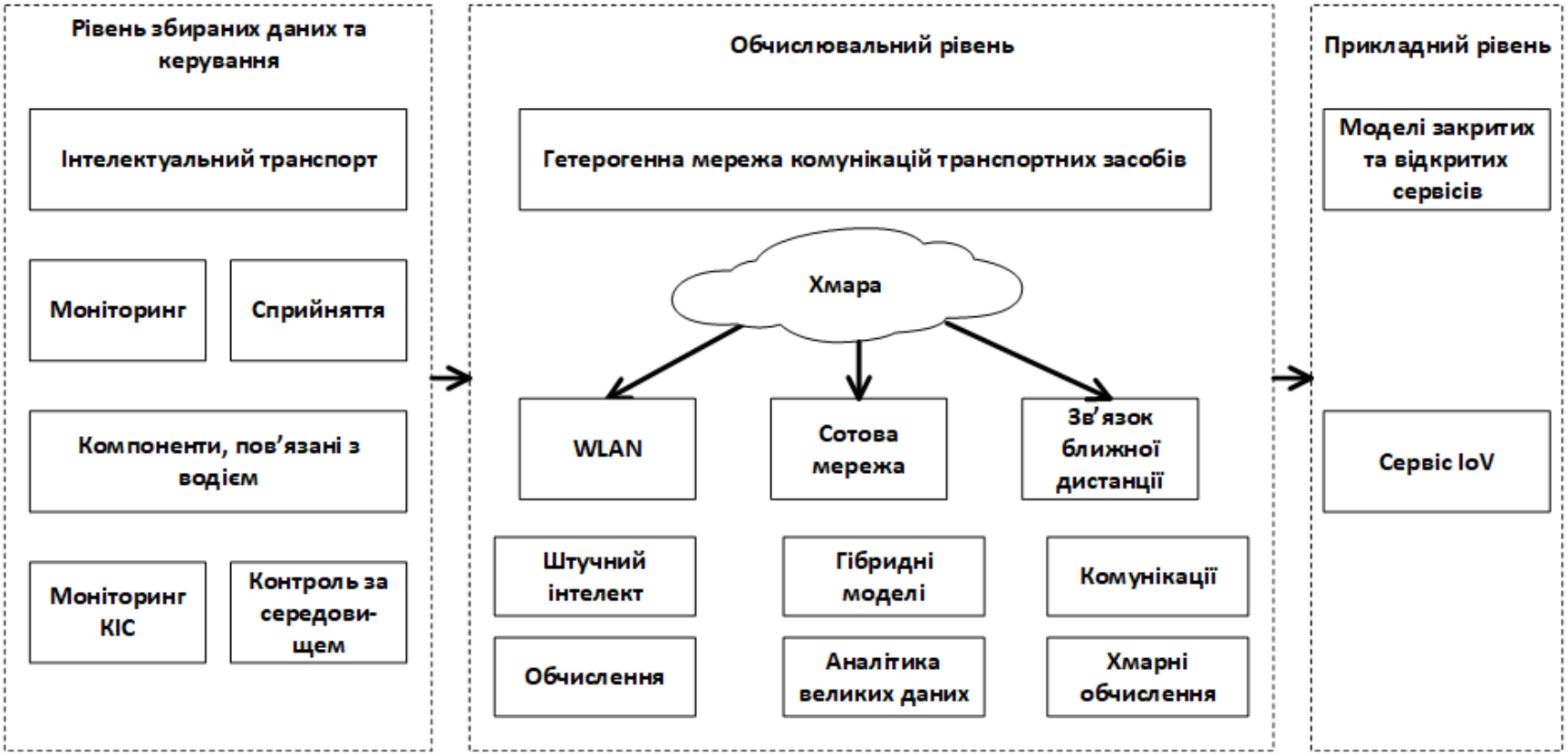

Рисунок 1.1 – Ключові компоненти та рівні транспортної мережі

На відміну від специфічних методів захисту даних в Інтернеті, проблеми безпеки даних IoV починаються з внутрішніх і зовнішніх факторів [6, 7]. Відсутність надійного механізму перевірки даних в автомобілях, наприклад протоколу CAN (англ., Controller Area Network), є однією з причин відображення внутрішніх проблем безпеки транспортних засобів на існуючі комунікаційні протоколи Інтернет. Захист даних від кібератак ускладнюється відкритою архітектурою IoV і широким використанням [8]. Предметом цієї кваліфікаційної роботи є автономна система виявлення аномалій у компонентах IoV. IoV стають безпрецедентними та вразливими, якщо їхня підтримка забезпечується динамічною та невизначеною мережею [9].

Безпека людей і майно можуть опинитися під загрозою через зловмисні напади та підробку даних, а також збої системи [10]. Рисунок 1.2 показує можливі ризики безпеки в системі IoV. Зв’язок між транспортними засобами (англ., Vehicle to Vehicle, V2V) є першим ризиком, де дані можуть бути атаковані зловмисником і можуть завдати шкоди водіям. У той саме час у сценарії зв’язку транспортного засобу з інфраструктурою (англ., Vehicle to Infrastructure, V2I) є можливим другий ризик безпеки.

Через численні моделі атак на інтелектуальні транспортні засоби виникають занепокоєння щодо конфіденційності та безпеки інтелектуальних транспортних засобів та інтелектуальних транспортних мереж [10]. Кіберзловмисники можуть глушити та підробляти сигнал комунікаційної мережі VANET, що створює серйозні проблеми з безпекою [11]. Це може призвести до того, що вся система V2x постраждає від спотворення інформації та затримки сигналів, що гарантує, що передане повідомлення пошкоджене та не відповідає потрібному призначенню [12].

Інтернет або фізичний доступ до пов’язаної інтелектуальної системи автомобіля є ще однією загрозою безпеці, з якою стикаються інтелектуальні автомобілі. У 2016 році професіонали з безпеки Чарлі Міллер і Кріс Валасек, наприклад, бездротовим способом зламали розвідувальну систему Jeep Cherokee [13]. Поки водій Jeep Cherokee все ще був за кермом, дослідники

Міллер і Валасек скомпрометували систему розваг, рульове управління та гальма, а також систему кондиціонування повітря, щоб показати, що інтелектуальна система Jeep має вразливість у безпеці. Кіберзлочинці зловживали супутньою програмою Nissan Leaf, використовуючи унікальний ідентифікаційний номер автомобіля, який зазвичай відображається на вікнах. Завдяки цьому недоліку хакерам вдалося отримати контроль над системою HVAC (англ., Heating, Ventilation & Air Conditioning – опалення, вентиляція й кондиціонування повітря) [14].

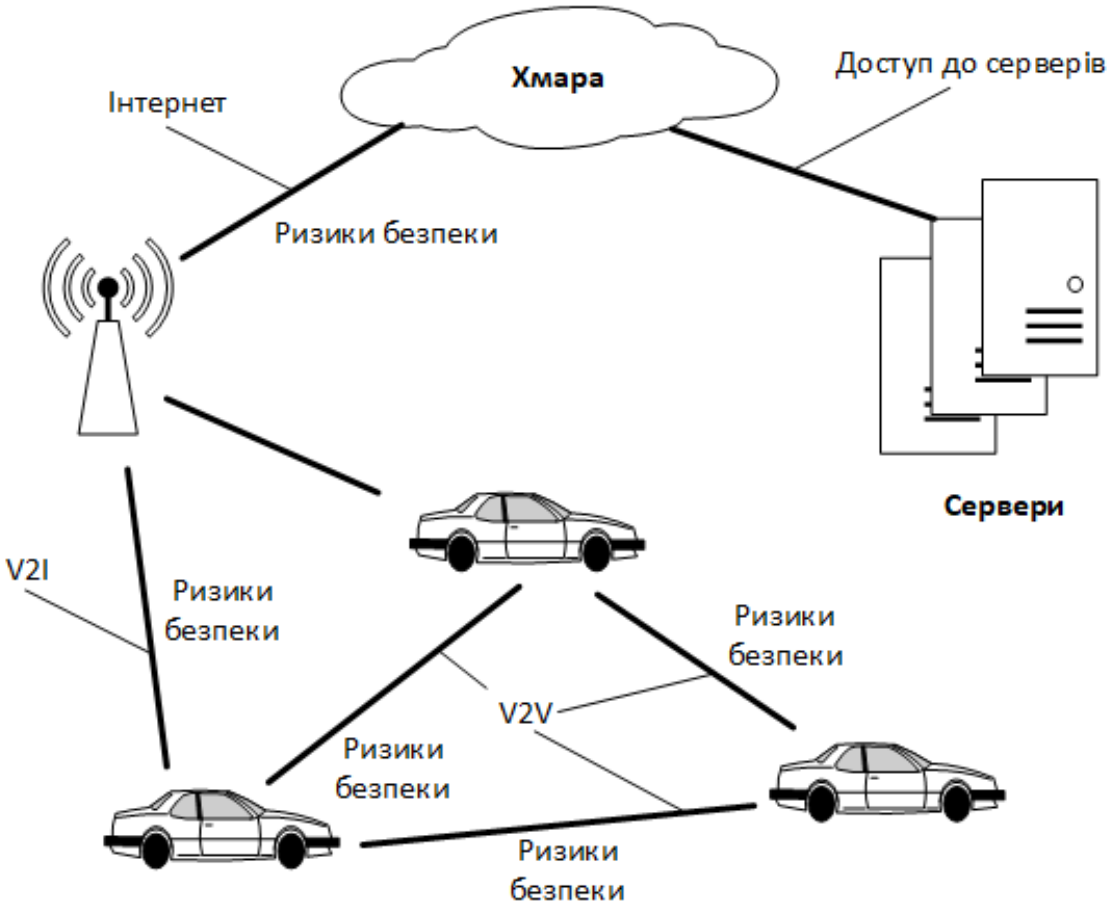

Рисунок 1.2 – Інформаційні ризики в транспортній мережі

Зростанню IoV сприяли вбудовані системи, вдосконалення апаратного та програмного забезпечення та мережеві пристрої. Однак в IoV все ще існує кілька проблемних напрямків, пов’язаних із загрозами: захищеність,

точність, продуктивність, мережна взаємодія, конфіденційність. Багато проблем із захищеністю та конфіденційністю виникли через зростання використання інтелектуальних служб, віддаленого доступу та частих модифікацій мережі. Як наслідок, серйозне занепокоєння викликають уразливості безпеки під час передачі даних IoV. Для вирішення проблем мережної взаємодії та захищеності, пов'язаних із IoV, можна використовувати кластеризацію [15, 16] та алгоритми і підходи глибокого навчання [17-19]. У рамках цього дослідження описано стандарти безпеки для застосунків IoV, які сприяють підвищенню ефективності мережі та надання послуг користувачу. Відмова в обслуговуванні (англ., Denial of Service, DoS) виявляється за допомогою нової моделі xNN. Мотиваціями цього дослідження є:

- запропонувати модель глибокого навчання для виявлення аномалії в транспортній мережі;
- представити комплексну структуру для підготовки даних мережевого трафіку для розробки IDS;
- запропонувати метод вибору ознак усереднення з використанням кластеризації K-means для підвищення ефективності запропонованої IDS і для виконання аналізу мережних атрибутів і атак з метою моніторингу мережі.

1.2 Системи виявлення аномалій

1.2.1 Загальні відомості

Безпека користувачів транспортних мереж є серйозною проблемою. У разі проникнення в систему IoV хакери можуть отримати прямий контроль над транспортними засобами, що призведе до дорожньо-транспортних пригод. До цього часу проведено багато досліджень щодо підвищення безпеки транспортних мереж. Для виявлення як відомих, так і невідомих атак

на автомобільні мережі Янг та ін. [1] представили багаторівневу гібридну систему, яка об’єднує IDS із сигнатурою та IDS з аномалією. Запропонована система може виявляти кілька відомих нападів з точністю 99,99% і 99,88% на наборі даних CICIDS2017, що представляє дані зовнішньої мережі транспортних засобів CAN-intrusion-dataset.

Запропонована система має високі оцінки F1 0,963 і 0,800 на обох наведених вище наборах даних при виявленні атак нульового дня. Мережі виявлення вторгнень, дизайн IDS, а також обмеження та характеристики мережі IOV були досліджені Ву та ін. [3]. Були детально обговорені конструкції IDS для мереж IOV, і в цій роботі було досліджено та ретельно проаналізовано широкий спектр цілей оптимізації. Автомобільні мережі VANET забезпечують бездротовий зв’язок між автомобілями та інфраструктурою, а підключені транспортні засоби можуть допомогти розумним містам і інтелектуальним транспортним системам (ITS). Основні цілі VANET – скоротити час у дорозі та підвищити безпеку водія, комфорт і продуктивність. VANET відрізняється від інших ad hoc-мереж своєю надзвичайною мобільністю. Однак відсутність централізованої інфраструктури наражає їх на кілька недоліків безпеки.

Вказане створює серйозну загрозу безпеці дорожнього руху. CAN – це протокол для надійного та ефективного зв’язку між бортовими частинами автомобіля. Шина CAN не містить інформації про джерело або призначення; отже, повідомлення не можна перевірити, коли вони передаються між вузлами. Зловмисник може легко вставити будь-яке повідомлення та спричинити проблеми з системою. Альшаммарі та ін. [4] представили методики KNN і SVM для групування та категоризації вторгнень VANET. Для виявлення вторгнень перевірялися коефіцієнт зміщення та часовий проміжок між запитом на повідомлення CAN і відповіддю.

1.2.2 Моделі на основі машинного навчання

IDS, керована даними, була розроблена шляхом оцінки поведінки завантаження зв’язку придорожнього блоку (англ., Roadside Unit, RSU) в Інтернеті речей (англ., Internet of Things, IoT) проти різних нападів, які спричиняють порушення потоку трафіку. Вторгнення, націлене на RSU, можна виявити за допомогою архітектури глибокого навчання на основі згорткової нейронної мережі (англ., Convolutional Neural Network, CNN). Пропонована архітектура [5] використовує стандартний варіант CNN і основний термін помилки на основі конвергенції алгоритму зворотного поширення. Водночас, запропоноване ймовірнісне представлення глибинної архітектури на основі CNN забезпечує теоретичний аналіз конвергенції.

Система IoV повинна ефективно керувати трафіком, переналаштовувати та захищати потокові дані. Програмно-визначені мережі (SDN) забезпечують гнучкість мережі та контроль. Однак це може залучити ворожих агентів. Методика автора використовує ймовірнісні структури даних для виявлення аномальної поведінки IoV. Для пошуку сугестивних вузлів використовується скетч Count-Min. Фаза 2 використовує контроль на основі фільтра Блума для перевірки підписів сумнівних вузлів. Фаза 3 використовує фільтр Quotient для швидкого зберігання ризикованих вузлів. Щоб виявити суперточки (зловмисні хости, які підключаються до кількох місць призначення), автор підрахував потоки через кожен комутатор на етапі 4. Було здійснено перевірку за допомогою комп’ютерного моделювання. Запропонований спосіб [7] перевершив поточний стандарт щодо коефіцієнтів виявлення та хибнопозитивних результатів.

У загальній моделі загроз зловмисник може отримати доступ до шини CAN, використовуючи загальні точки доступу. Сяо та ін. [8] представили систему виявлення аномалій транспортної мережі на основі симетрії SIMATT і SECCU. Для отримання найсучаснішої продуктивності виявлення аномалій було інтегровано SECCU та SIMATT. Автори мали за мету зменшити

витрати на обчислення на етапах навчання та виявлення. Моделі SECCU та SIMATT тепер мають лише один шар із 500 комірок кожен, що зменшує витрати на обчислення. Численні оцінки архітектур SIMATT-SECCU показали майже оптимальну точність і показники відкликання (з іншими традиційними алгоритмами, такими як LSTM, GRU, GIDS, RNN або їх похідними) [20, 21].

1.2.3 Виявлення аномалій на основі шаблонів водіння

Виявлення аномалій на основі алгоритму емоційного стану водія (англ., Driver’s Emotional State, EAD) було запропоновано Дінгом та ін. [9]. Завданням було досягти виявлення в режимі реального часу даних, пов’язаних із безпечним водінням у кооперативній мережі транспортних засобів. У цьому дослідженні була визначена кількісна модель емоційної оцінки водія, яка в першу чергу використовувалася для характеристики стилю водіння. По-друге, техніка виявлення аномалій даних була побудована з використанням змішаної моделі Гауса (англ., Gaussian Mixed Model, GMM) на основі моделі квантування емоцій та інформації про стан водіння автомобіля. Нарешті, автори провели масштабні експерименти на реальному наборі даних (NGSIM), щоб продемонструвати високу продуктивність алгоритму EAD у поєднанні зі сценаріями застосування кооперативних автомобільних мереж.

Оскільки хмара IoV надає невелику кількість позначених даних для нової атаки, Лі та ін. [10] запропонували два підходи до оновлення моделі. Хмарні оновлення від IoV можуть надати невелику кількість даних. Використання методу локального оновлення не дозволяє хмарі IoV швидко надсилати дані з мітками. Це дослідження показує, що попередньо позначені дані можна використовувати для отримання псевдомітки непозначених даних у нових атаках. Транспортний засіб може оновлюватися, не отримуючи позначені дані з хмари IoV. Запропоновані схеми покращили точність

виявлення на 23% у порівнянні зі звичайними методами.

Кібербезпека та безпека підключених транспортних засобів розглядаються за допомогою методів виявлення аномалій. Попередні дослідження в цій галузі класифікуються відповідно до запропонованої таксономії [11]. В цій таксономії існує дев’ять основних категорій і 38 підкатегорій. Дослідники виявили такі особливості:

- реальні дані використовуються рідко;
- більшість результатів отримують за допомогою моделювання;
- V2I та зв’язок у транспортному засобі не розглядаються разом;
- запропоновані методики рідко порівнюються з базовою лінією;
- безпеці транспортних засобів приділяється не так багато уваги, як кібербезпеці.

Підтримка безпечної інтелектуальної транспортної системи вимагає уникати маршрутів, схильних до аварій. Допомогти водіям уникати небезпечних умов водіння (наприклад, засніжених доріг і дощових ділянок дороги) можуть інтелектуальні навігаційні системи, завдяки краудсорсингу та історичним даним про аварії. Використовуючи отримані дані, такі як зображення, показання датчиків тощо, хмара автомобіля може обчислювати такі безпечні маршрути та реагувати швидше, ніж централізована служба. В інтелектуальній маршрутизації для кожного власника даних повинні бути забезпечені безпека та конфіденційність. Крім того, перед використанням даних, отриманих натовпом, їх потрібно перевірити в хмарі автомобіля. Джой та ін. [12] досліджували способи забезпечення безпеки, конфіденційності та захисту транспортних хмар від вторгнень.

Протягом останніх кількох років складність і з’єднуваність сучасних автомобілів постійно зростали. У контексті цього розвитку відбулося значне зростання ризиків безпеки для автомобільних мереж і їхніх компонентів. Крім ризику для водія та інших учасників дорожнього руху, ці атаки можуть поставити під загрозу критичні системи безпеки автомобіля. Виявлення аномалій в автомобільних мережах обговорюється різними авторами [13]. На

основі характеристик типових автомобільних мереж, таких як CAN, було представлено набір датчиків виявлення аномалій. Ці датчики дозволяють виявляти атаки під час роботи автомобіля, не викликаючи помилкових спрацьовувань. Також описано та обговорено систему виявлення атак на транспортні засоби з точки зору їхної конструкції та критеріїв застосування.

1.2.4 Розподілена система виявлення аномалій

Негі та ін. [14] запропонували структуру для розподіленої системи виявлення аномалій, яка включає новий онлайн-алгоритм вибору даних, який спрямовує перенавчання та змінює параметри моделі за потреби для самокерованих та підключених автомобілів. Офлайн-навчання моделі LSTM на багатьох машинах розподіленим способом з використанням усіх доступних даних є частиною реалізації фреймворку. Виявлення аномалії відбувається на рівні транспортного засобу за допомогою навчених параметрів, а потім надсилається до окремих транспортних засобів. Використовується більш складна модель виявлення аномалій LSTM – довга короткочасна пам'ять (англ., Long Short-Term Memory), а точність запропонованого розподіленого фреймворку у виявленні аномалій покращено за допомогою фреймворку MXnet, який використовується для тестування продуктивності фреймворку.

Сакіяма та ін. [22] запропонували банки фільтрів, що визначаються сумою синусоїдальних хвиль у спектральній області графа. Ці банки фільтрів мають низькі похибки апроксимації навіть при використанні апроксимації нижчого порядку полінома Чебишева. Їхні параметри можуть бути ефективно отримані з будь-яких лінійних фазових фільтрів із кінцевою імпульсною характеристикою на регулярній основі. Запропонована автором конструкція групи фільтрів у частотній області має ті ж характеристики, що й класична група фільтрів. Точність апроксимації визначає порядки апроксимації. Існує багато вейвлетів спектральних графів і банків фільтрів

для перевірки методів автора.

Для автономних і підключених автомобілів безпека транспортних засобів є головним пріоритетом у світлі інциденту з Jeep Cherokee 2015 року, коли транспортним засобом незаконно керували дистанційно шляхом підробки повідомлень, розміщених у публічній мобільній мережі. Рішення безпеки для кожної невідомої кібератаки передбачають своєчасну ідентифікацію атак, які відбуваються протягом усього терміну експлуатації транспортних засобів. Спокінгові зв'язки на центральному шлюзі можна виявити за допомогою IDS [23]. Використовуючи зв’язок із реальною автомобільною мережею, автор також повідомив про продуктивність системи виявлення.

1.2.5 Система виявлення вторгнень в ad hoc-мережу транспортних засобів

Мережі транспортних засобів типу ad hoc еволюціонують до Інтернету автомобілів, оскільки Інтернет речей опановує IoV. IoV може залучити велику кількість компаній і дослідників завдяки швидкому розвитку обчислювальних і комунікаційних технологій. Використовуючи абстрактну модель IoT, дослідниками [24] надано огляд технологій, необхідних для створення IoV, розглянуто багато програм, пов’язаних з IoV, і надано деякі відкриті дослідницькі завдання та опис необхідних майбутніх досліджень у сфері IoV.

Майбутні мережі CAV (англ., Automated and Connected Vehicles – автоматизовані та з’єднані транспортні засоби), або ITS, утворять мережу з високим ступенем взаємозв’язків. Якщо транспортні засоби підключені до «Інтернету транспортних засобів» (Інтернет CAV), стає можливим координувати міські транспортні потоки. Контролювати та регулювати CAV можна буде за допомогою анонімних даних про мобільність CAV. Для забезпечення безпечної та надійної роботи вирішальне значення має раннє

виявлення аномалій. В одній з дослідницьких робіт [25] запропоновано техніку неконтрольованого навчання на основі глибокого автокодувальника для виявлення аномалій розташування, про які повідомляють самі CAV. Кількісні дослідження змодельованих наборів даних показують, що запропонований підхід добре спрацював у виявленні аномалій розташування, про які повідомляють користувачі.

Оскільки виявлення аномалій у режимі реального часу на повних пакетах даних є дорогим, пропонується [26] зосереджуватися на аналізі важливих даних безпеки. У попередній обробці використовувалася модель стільникового автомата трафіку, що дозволяє досягти оптимального виявлення аномалій за мінімальні комп'ютерні ресурси. Алгоритм може виявляти порушення в даних, пов'язаних із безпечним водінням, у режимі реального часу та онлайн, моделюючи специфічний стиль водіння. Спочатку реалізується модель квантування стилю водіння, яка описує його як коефіцієнт водіння, потім – модель суміші Гауса (GMM), для виявлення аномалій даних на основі квантування стилю водіння та визначеного стану водіння автомобіля. Нарешті, це дослідження оцінювало продуктивність запропонованого алгоритму ADD у додатках IoV з використанням реальних і змодельованих даних.

У даній кваліфікаційній роботі підсумовано дослідження щодо виявлення аномалій. Існуючі методи можна класифікували у групи на основі використаного основного підходу. Для кожної категорії враховуються ключові припущення [27], що дозволяє відрізнити нормальну поведінку від девіантної. При використанні кількох припущень можна рекомендувати тестування ефективності методики в певній області. Використовуючи основну техніку виявлення аномалій, можна показати, що всі існуючі методи є варіаціями однієї методики. Цей шаблон полегшує класифікацію та запам'ятовування методики в кожній області. Переваги та недоліки кожної методики наведено окремо. Також розглядається обчислювальна складність методик, що є важливим для реальних додатків. Це дослідження має на меті

краще зрозуміти, як стратегії, розроблені для однієї сфери, можна застосувати до інших сфер. Можна сподіватися, що результати будуть корисними.

Ще одним прикладом є система IVADE (англ, In-Vehicle Anomaly Detection Engine – вбудований у транспортний засіб автомат виявлення вторгень) – технологія виявлення вторгнень на основі машинного навчання, [28]. Система відстежує дані про мобільність транспортного засобу за допомогою повідомлень про кооперативну обізнаність CAM (англ., Cooperative Awareness Messages), які передаються між автомобілями та інфраструктурою через мережі V2V і V2I (такі як положення, швидкість і напрямок). Система допомоги в утриманні у смузі IVADE використовує ECU для вимірювання сигналу та обчислень керування на шині CAN (LKAS). Для реалізації машинного навчання в IVADE потрібні поля повідомлень CAN, специфічні для автомобільної сфери знання про динамічну поведінку системи та дерева рішень. Результати моделювання свідчать про те, що IVADE може виявляти порушення в роботі транспортних засобів, таким чином підсилюючи функції безпеки.

1.2.6 Вбудовані у транспортний засіб системи виявлення мережевого вторгнення

Віддалена бездротова атака на автомобільну мережу можлива за допомогою 5G та Інтернету транспортних засобів. Системи виявлення аномалій можуть бути ефективними в якості першої лінії захисту від загроз безпеці. Прикладом може стати система виявлення аномалій [29], яка використовує ієрархічну часову пам’ять HTM (англ., Hierarchical Temporal Memory) для захисту мережевої шини контролера автомобіля. Модель HTM може передбачати дані потоку в реальному часі на основі попереднього навчання. Алгоритм оцінки аномальних показників прогнозу було вдосконалено за допомогою створених вручну модифікацій полів і атак

повтору. Результати показали, що розподілена система виявлення аномалій HTM перевершила рекурентні нейронні мережі та системи виявлення прихованої моделі Маркова щодо оцінки RCC, точності та повноти.

Також описано [30] онлайн-підхід при виявленні аномалій для роботів, який є легким і здатним враховувати велику кількість датчиків і внутрішніх вимірювань з високою точністю. Вибравши онлайн-корельовані дані, автори представили специфічну для робота версію добре відомої відстані Махаланобіса. Автори також продемонстрували, як це можна застосувати до великих розмірностей. Автори перевірили ці внески за допомогою комерційних безпілотних літальних апаратів (БПЛА), робота-пилососа та симулятора польоту високої точності. Згідно з їхніми висновками, дистанція Online Mahalanobis перевершила попередні методи.

Наприклад, автомобілі є CPS завдяки своїм унікальним датчикам, електронним блокам управління та приводам. Зовнішнє підключення збільшує поверхню атаки, впливаючи на тих, хто знаходиться всередині транспортних засобів, і тих, хто знаходиться поблизу. Поверхня атаки зросла через складні системи, побудовані на старих, менш безпечних фреймворках загальної шини, у яких відсутні базові методи автентифікації. Для того, щоб зробити такі системи безпечнішими, автори розглядають це як завдання аналізу даних. В роботі [31] застосовано приховану марковську модель для виявлення небезпечної поведінки та надсилання сповіщень, коли транспортний засіб рухається. Для демонстрації здатності методу виявляти аномалії в транспортних засобах, автори протестували його з одним і двома параметрами. Причому цей метод працював як на нових, так і на старих автомобілях.

1.2.7 Функціональна система виявлення вторгнень

Гарг та ін. [32] запропонували систему виявлення аномалій з трьома етапами: (а) вибір функції, (б) оптимізація параметрів SVM і (в) класифікація

трафіку. Перші два етапи виражаються за допомогою задачі багатоцільової оптимізації. Таке поєднання збільшує можливості оптимізатора та швидкість локального пошуку, який здійснюється ним. Останній етап класифікації даних використовує SVM з оновленими параметрами. Для широкого оцінювання запропонованої моделі використовувалися OMNET++ і SUMO. Швидкість виявлення, точність і частота помилкових позитивних результатів підтверджують ефективність.

Марчетті та ін. [33] розглянули теоретико-інформаційні методи виявлення аномалій для сучасних автомобільних мереж. Це дослідження було зосереджено на детекторах аномалій на основі ентропії. Автори змоделювали атаки на автомобільну мережу, вставивши фальшиві повідомлення CAN у реальних даних сучасного ліцензованого автомобіля. Експеримент показав, що виявлення ентропійної аномалії, застосоване до всіх повідомлень CAN, здатне виявити велику кількість помилкових сигналів CAN. Підробку сигналів CAN можна було виявити лише за допомогою виявлення аномалій на основі ентропії, що вимагає багатьох різних детекторів аномалій для кожного класу повідомлень CAN.

Для того, щоб точно визначити місцезнаходження та швидкість транспортного засобу, AEKF має додатково враховувати ситуацію навколо транспортного засобу. Модель стеження за автомобілем враховує фактор затримки зв’язку. Це надає можливість підвищити її придатність для реальних застосувань. Інший метод виявлення аномалії [34] припускає, що він є кращим за метод AEKF із типовим 2-детектором. Збільшення часу затримки негативно вплинуло на загальну ефективність виявлення.

1.2.8 З’єднані та автономні транспортні засоби

Очікується, що з’єднані та автономні транспортні засоби (CAV) зроблять революцію в автомобільній промисловості. Автономні системи прийняття рішень обробляють дані зовнішніх і бортових датчиків. При цьому

актуалізуються такі проблеми, як саботування сигналів, погіршення апаратного забезпечення, помилки програмного забезпечення, нестабільність живлення та кібератаки. Запобігти ці потенційно фатальні аномалії можна завдяки виявленню в реальному часі [35] та ідентифікації. Наприклад [36], запропоновано ієрархічну модель для надійної категоризації кожної сигнальної послідовності в режимі реального часу за допомогою автоматичного кодувальника LSTM.

Для трьох випадків досліджено вплив модифікації параметрів моделі на виявлення аномалії та переваги посилення каналу. Модель була точною на 95,5%. Таблиця 1.1 показує порівняльний аналіз попередніх досліджень, проведених для виявлення аномалій IoV. У наведеній нижче таблиці видно, що раніше використовувалися кілька методів, наприклад, гібридні моделі, випадкові ліси, моделі суміші Гауса, MXNet, моделі HTM, SVM та різні інші моделі машинного і глибокого навчання.

Таблиця 1.1 – Порівняльний аналіз попередніх досліджень

Посилання	Методика	Набір даних	Точність, %
Ян та ін. [1]	Гібридні моделі	CICIDS2017	96,3
Ву та ін. [3]	Випадкові ліси	CICIDS2017	95
Дінг та ін. [9]	Модель суміші Гауса	CICIDS2017	97
Негі та ін. [14]	MXNet	Офлайн-набір даних	98,5
Ванг та ін. [29]	Модель HTM	UNSW-NB15	97,45
Гарг та ін. [32]	SVM	CICIDS2019	91

1.2.9 Мета дослідження

Здатність систем виявлення аномалій виявляти несподівані атаки викликала великий інтерес, і це призвело до їхнього широкого використання в таких сферах, як штучне виявлення, розпізнавання образів і машинне

навчання. Традиційні методи машинного навчання, які зазвичай використовуються в IDS, покладаються на трудомісткі процеси вилучення та вибору функцій. Крім того, алгоритм класифікації, який зараз використовується, використовує неглибоке машинне навчання. У реальних мережевих програмах неглибокі методи машинного навчання можуть аналізувати вхідні дані великого розміру, що призводить до нижчого рівня виявлення.

Також дані, з якими мають працювати системи IDS, здебільшого складаються з мережевого трафіку або послідовностей викликів хостів, і між ними існують значні відмінності. Послідовності викликів хоста більше схожі на проблему послідовності, ніж дані мережевого трафіку. Хоча більш ранні методи, як правило, орієнтовані на конкретний випадок, алгоритми виявлення не є адаптивними, особливо для гібридних систем виявлення джерел даних або розширених систем виявлення. Отже, попередні алгоритми виявлення неефективні. З метою вибору функцій можна використовувати кластеризацію K-means задля того, щоб отримати та вибрати найкращі функції. Для класифікації атак можна запропонувати пояснювану нейронну мережу xNN (англ., Explainable Neural Network).

Основні проблеми, які потрібно вирішити:

- у випадку класифікації з кількома класами, для точної ідентифікації або виявлення всіх класів даних проблему становить можлива незбалансованість класів;
- іноді матимуть місце великовимірні дані, а функції можуть бути розріджені, тому ефективний вибір функцій є проблемою;
- виявлення та передбачення ефективніше в глибокому навчанні, ніж із застосуванням традиційних методів машинного навчання.

У цій кваліфікаційній роботі пропонується модель xNN для виявлення аномалій транспортній мережі на основі класифікації атак у двох різних наборах даних окремо.

2 ЗАПРОПОНОВАНА МОДЕЛЬ XNN ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ В ТРАНСПОРТНІЙ МЕРЕЖІ

2.1 Архітектура нейронної мережі

Класичним нейронним мережам важко працювати з послідовностями даних. У наборах даних UNSWNB і CICIDS за порядком системних викликів слідують виклики хостів [37, 38]. Незвичайна поведінка може містити послідовності викликів і підпослідовності, які є нормальними. Це означає, що під час виявлення вторгнення в транспортну мережу необхідно враховувати властивості послідовності системних викликів.

Сказане вище означає, що класифікація вхідних даних повинна враховувати поточні дані, а також попередні дані, їхні зміщені та масштабовані атрибути. Таким чином, для виявлення вторгнення, розробленого для отримання вхідних екземплярів із нормальною та ненормальною послідовностями, потрібно зміщувати та масштабувати функції кластеризованих даних K-means, що забезпечить відповідність вищезазначеним вимогам для xNN. xNN працює на моделі адитивного індексу як:

$$f(x) = g_1\beta_1^T x + g_2\beta_2^T x + [...] + g_K\beta_K^T x. \quad (2.1)$$

У (2.1) f(x) – функція класифікації вихідної змінної, тобто атак, g – вхідна функція. Усі функції впорядковано відповідно до значення у базисі K із кластеризації K-means, тоді як x є значенням кожного екземпляра з функції. T – коефіцієнт масштабування, який безпосередньо пов’язаний з β.

У рівнянні (2.1) додано параметри масштабування в нейронній мережі, тоді як у рівнянні (2.2) додано параметр зсуву γ з коефіцієнтом зсуву, тобто σ, а h – функція передачі гіперпараметрів для надмірної та недостатньої

підгонки моделі. Альтернативне формулювання для xNN:

$$f(x) = \sigma + \gamma_1 h_1 \beta_1^T x + \gamma_2 h_2 \beta_2^T x + [...] + \gamma_K h_K \beta_K^T x . \quad (2.2)$$

Коли дані надходять у мережу, вони множаться на вагові коефіцієнти, призначені кожному числу, перш ніж надсилаються на другий рівень нейронів, як показано на рисунку 2.1. Сигмовидна функція активації будується шляхом підсумовування зважених сум функцій активації кожного з нейронів. Тепер ваги зв'язків між другим і третім шарами поділені на ці значення. Далі процес повторюється до останнього шару.

Архітектуру xNN демонструє рисунок 2.1.

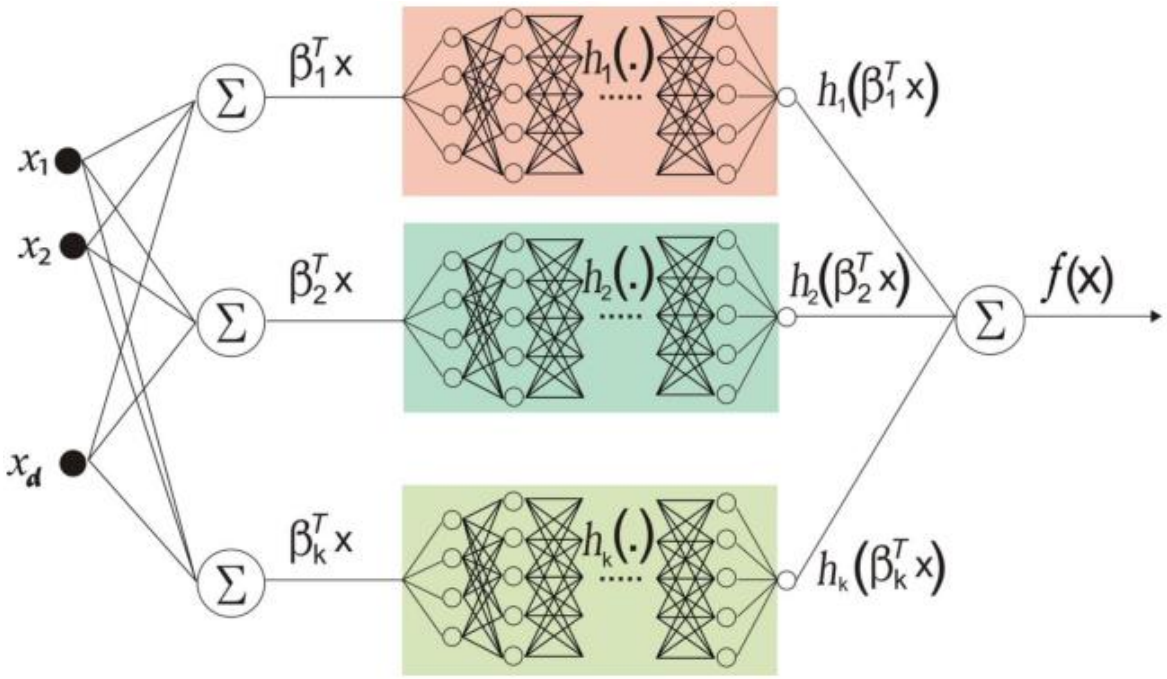

Рисунок 2.1 – Запропонована архітектура xNN

Введемо позначення:

a_j^l – активація j-го нейрона у шарі l;

$w_{j,k}^l$ – значення ваги з'єднання j-го нейрона у шарі l з k-м нейроном у

шарі l-1;

b_j^l – зміщення j-го нейрона у шарі l;

n_l – кількість нейронів у шарі l.

Тоді можна визначити універсальне рівняння, щоб знайти активацію будь-якого нейрона в нейронній мережі:

$$a_j^l = \sigma\left(\left[\sum_{k=1}^{n_{l-1}} w_{j,k}^l a_k^{l-1}\right] + b_j^l\right). \quad (2.3)$$

Зважений орієнтований граф можна використовувати для концептуалізації xNN, в якій нейрони є вузлами, а спрямовані ребра з вагами з'єднують вузли. Інформація, що надходить іззовні, кодується у вигляді векторів і приймається моделлю нейронної мережі. Для d входів, позначення x(d) використовується для позначення цих входів.

Ваги кожного входу перемножуються. Нейронна мережа налаштовується за допомогою ваг. Вага зазвичай використовується для представлення сили зв'язків між нейронами в нейронній мережі.

Обчислювальний блок підсумовує всі вхідні дані, які були зважені (штучний нейрон). У випадку, якщо зважений підсумок дорівнює нулю, додається зміщення, щоб зробити результат відмінним від нуля або збільшити швидкість реагування системи. Вага та вхід дорівнюють «1» у зміщенні.

До суми можна додати будь-яке число від 0 до нескінченності. Порогове значення використовується для обмеження відповіді бажаним значенням. Для зміщення суми вперед використовується функція активації f(x).

Для отримання бажаного результату функція активації встановлюється на функцію передачі. Функція активації може бути лінійною або нелінійною.

2.2 Метод навчання

У цьому підрозділі пояснюється детальний опис набору даних, методології та показників ефективності. Використано два набори даних автономних транспортних мереж, тобто UNSW-NB15 і CICIDS2019, які містять поєднання класичних і нових атак. Повний потік поточної методології показано на рисунку 2.2.

Вже тривалий час кілька дослідницьких спільнот цікавляться виявленням аномалій. У деяких випадках все ще потрібні передові підходи для вирішення складних проблем і перешкод. Останніми роками з'явився важливий новий шлях у виявленні аномалій – виявлення аномалій із підтримкою глибокого навчання (іноді відоме як «глибоке виявлення аномалій»). За допомогою цих двох останніх наборів даних перевіряється запропонований метод. Набори даних попередньо обробляються, щоб до них можна було застосувати методи глибокого навчання. Міра однорідності (кластеризація k-середніх) – це стратегія вибору релевантних ознак з обох наборів даних неконтрольованим способом для покращення продуктивності класифікаторів. Продуктивність моделей глибокого навчання можна оцінити та покращити за допомогою п'ятикратної перехресної перевірки. В роботі для класифікації атак використано Explainable Neural Network (xNN).

2.2.1 Набір даних UNSW-NB15

Мережеві вторгнення відстежуються в наборі даних UNSW-NB15. DoS, хробаки, бекдори та Fuzzers – це лише деякі з дев'яти різноманітних типів атак, включених до цього шкідливого програмного забезпечення. Пакети з мережі включені в набір даних. Є 175341 записів у навчальному наборі та 82332 запису в тестовому наборі атакуючих і звичайних записів. У наведеній таблиці 2.1 показано атрибути набору даних, тобто ідентифікатор, тривалість, протоколи, стан, прапорці, байти джерела та призначення та пакети. Атака –

це вихідна змінна з декількома класами, наприклад DDoS, бекдор-атаки, хробаки та інші. Опис набору даних UNSW-NB15 наведено в таблиці 2.1.

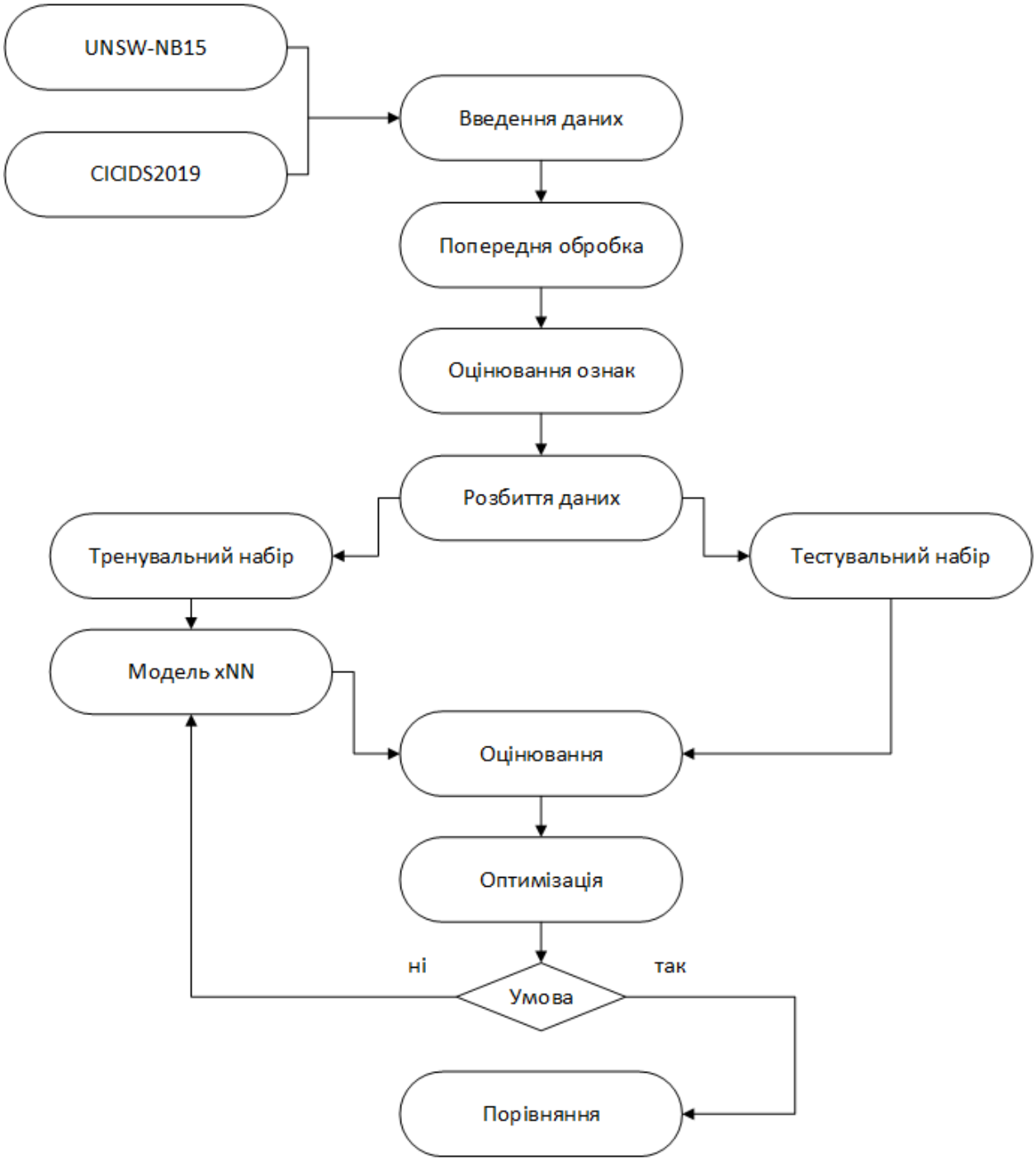

Рисунок 2.2 – Структура потоку даних при реалізації запропонованого методу

Таблиця 2.1 – Опис набору даних UNSW-NB15

Функція/атрибут	Опис	Значення	Тип змінної
ID	ID транспортного засобу	Будь-яке натуральне число	Вхідна змінна
Duration	Загальний час підключення транспортного засобу до мережі	Години/хвилини/секунди	Вхідна змінна
Proto	Основні механізми передачі даних, включені в комунікаційні протоколи	TCP/IP, HTTP	Вхідна змінна
State	Стан транспортного засобу (підключення)	0 (відключено) або 1 (підключено)	Вхідна змінна
Spkts	Пакети джерела (надіслані до пункту призначення)	Будь-яке натуральне число	Вхідна змінна
Dpkts	Пакети призначення (отримані в пункті призначення)	Будь-яке натуральне число	Вхідна змінна
Sbytes	Байти джерела (надіслано з джерела)	Будь-яке натуральне число	Вхідна змінна
Dbytes	Байти призначення (отримано з джерела)	Будь-яке натуральне число	Вхідна змінна
AttackCat	Категорія атаки	UNSW-NB15 визначає дев'ять атак (DDoS, Backdoors, Worms тощо)	Вихідна/цільова змінна з дев'ятьма класами

На рисунку 2.3 показано розподіл і загальну кількість протоколів, тобто HTTP, FTP, FTP Data, SMTP, POP3, DNS, SNMP, SSL, DHCP, IRC, Radius і SSH.

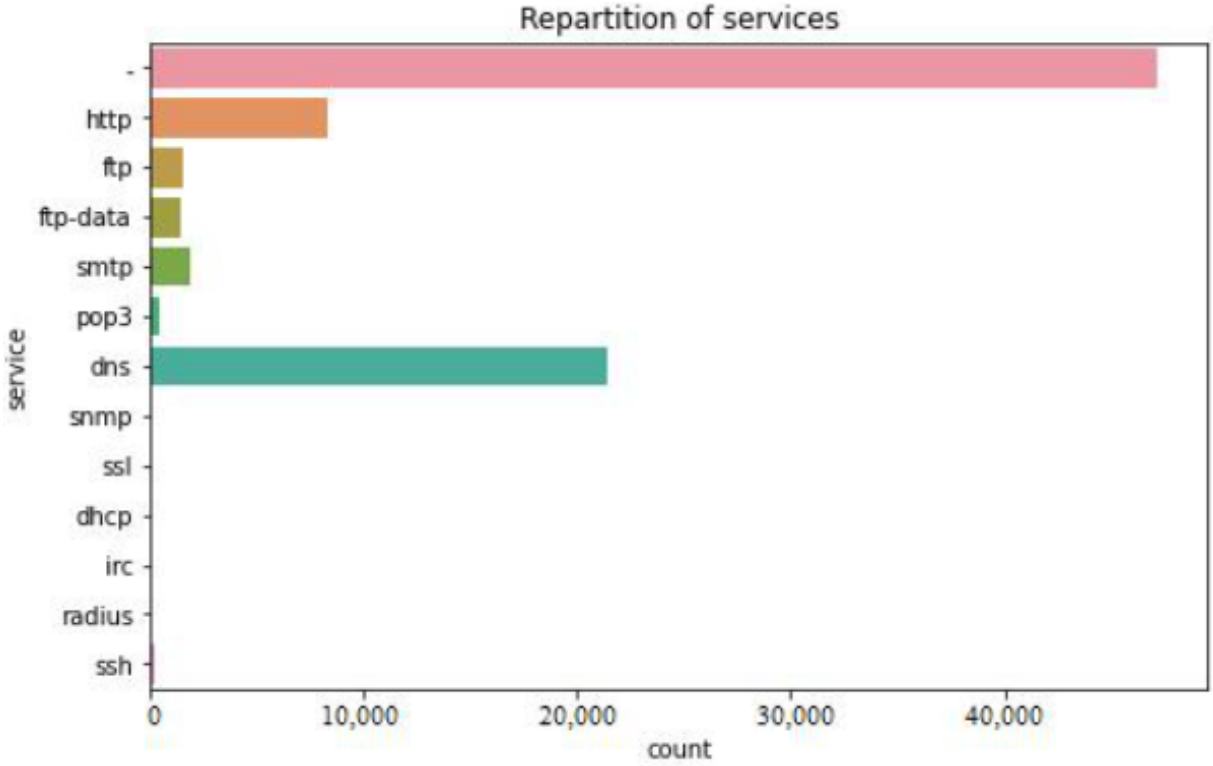

Рисунок 2.3 – Розподіл сервісів в UNSW-NB15

Рисунок 2.4 показує кількість загальних категорій атак, присутніх у наборі даних UNSW-NB15, тобто Generic, Shell Code, DOS, Reconnaissance, Backdoor, Exploits, Analysis, Fuzzers і Worms, тоді як загалом 3500 випадків вважалися звичайними.

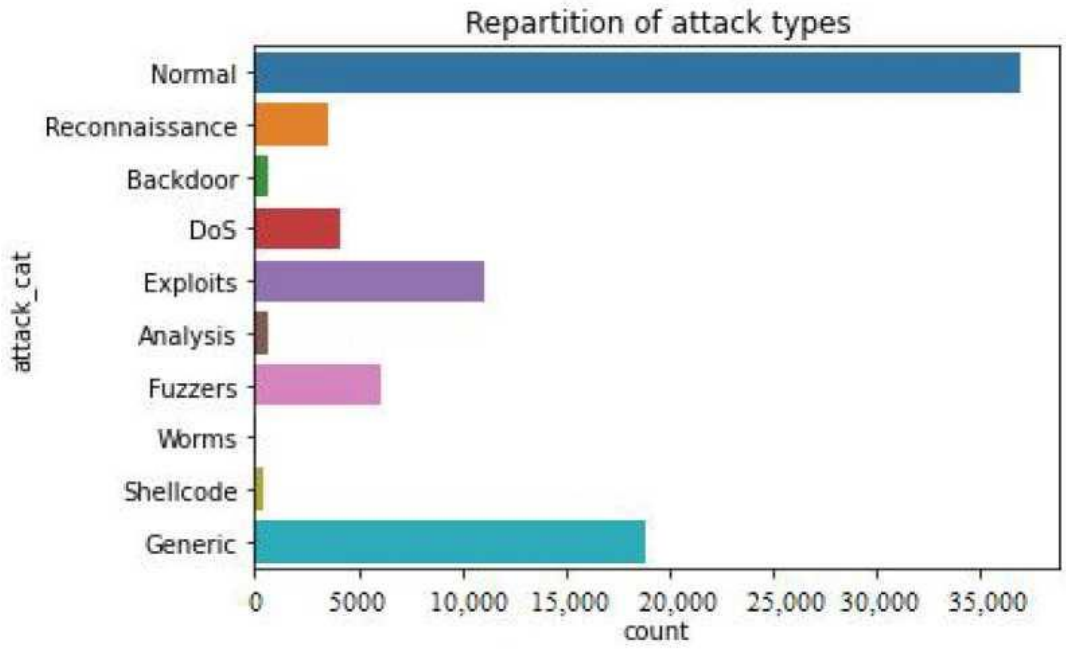

Рисунок 2.4 – Розподіл типів атак

2.2.1 Набір даних CICIDS2019

Таблиця 2.2 показує атрибути іншого набору даних, використаного в дослідженні, від CICIDS2019. У цьому наборі даних можна знайти низку зловмисних атак у мережах транспортних засобів, які пов’язані з аномаліями в реальному світі. Позначка часу, IP-адреси джерела та призначення, порти джерела та призначення, протоколи та атаки включаються в результати аналізу мережевого трафіку за допомогою Cyclometers. Витягнуте визначення функції також доступне. Період збору даних тривав 5 днів, з 9 ранку понеділка, 3 липня 2019 р., до 17:00 п’ятниці, 7 липня 2019 р. Понеділок був звичайним днем із невеликим трафіком. У вівторок, середу, четвер і п’ятницю вранці та вдень застосовувалися проникнення, ботнети та DDoS-атаки.

Рисунок 2.5 показує розподіл цільової змінної, тобто Атаки.

Таблиця 2.2 – Опис набору даних CICIDS2019

Функція/атрибут	Опис	Значення	Тип змінної
ID	ID транспортного засобу	Будь-яке натуральне число	Вхідна змінна
Flow Duration	Загальний час підключення транспортного засобу до мережі	Години/хвилини/секунди	Вхідна змінна
Destination Ports	Кількість портів передачі даних	2.0, 3.0	Вхідна змінна
Total Forwarded Packets	Пакети джерела (надіслані до місця призначення)	0 (відключено) або 1 (підключено)	Вхідна змінна
Total Backward Packets	Пакети призначення (отримані в пункті призначення)	Будь-яке натуральне число	Вхідна змінна
Length of Packets	Довжина пересланих і зворотних пакетів	Будь-яке натуральне число	Вхідна змінна
Sbytes	Байти джерела (надіслано з джерела)	Будь-яке натуральне число	Вхідна змінна
Dbytes	Байти призначення (отримано з джерела)	Будь-яке натуральне число	Вхідна змінна
Attacks	Категорія атаки	CICIDS2019 визначає дві загальні аномалії («доброякісні» та ботнети)	Вихідна/цільова змінна з 2 класами

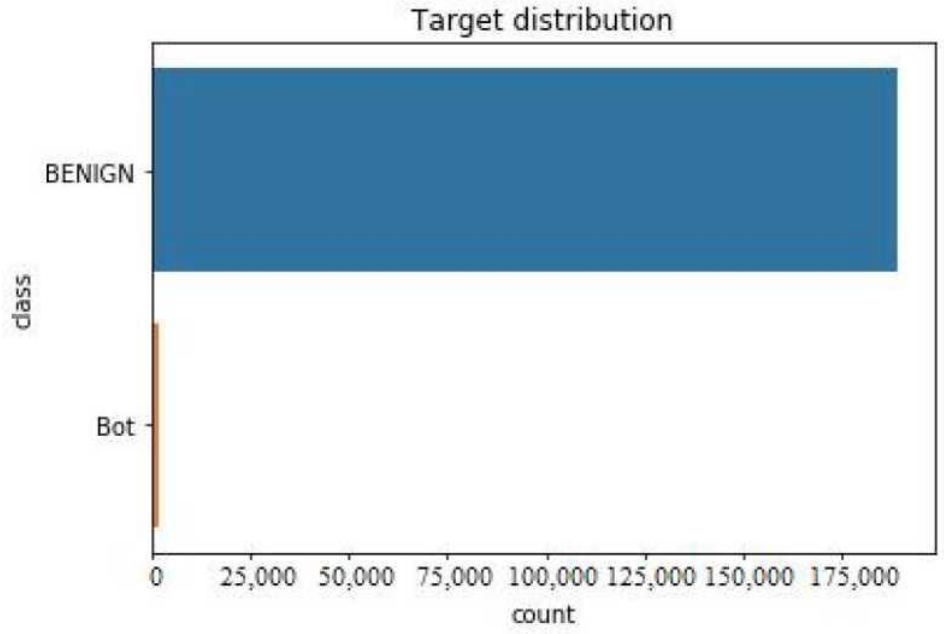

Рисунок 2.5 – Розподіл цільових змінних у CICIDS2019

2.3 Попередня обробка даних

Набір даних попередньо обробляється з метою зробити його більш відповідним для класифікатора нейронної мережі.

Крок 1. Видалення інформації про сокет.

Для неупередженої ідентифікації необхідно видалити IP-адресу вхідного та кінцевого хостів у мережі з вихідного набору даних, оскільки ця інформація може призвести до надмірного навчання щодо цієї інформації про сокет. Замість того, щоб покладатися на інформацію про сокет, класифікатор має бути навчений характеристиками пакета, щоб будь-який хост із подібною інформацією про пакет було виключено.

Крок 2. Видалення пробілів.

Під час створення багатокласових міток можуть додаватися пробіли. Оскільки фактичне значення відрізняється від міток інших кортежів у тому ж класі, ці пробіли створюють окремі класи.

Крок 3. Кодування міток.

Для позначення міток кількох класів у наборі даних, які включають

назви атак, використовуються дані типу рядків. Щоб навчити класифікатор, до якого класу належить кожен кортеж, необхідно закодувати ці значення чисельно. Для цієї операції використовуються багатокласові мітки, оскільки двійкові мітки вже знаходяться у формі нуль-один для цієї операції.

Крок 4. Нормалізація даних.

Набір даних містить широкий спектр числових значень, що створює труднощі для класифікатора під час навчання. Це означає, що мінімальне та максимальне значення для кожної характеристики повинні бути встановлені рівними нулю та одиниці відповідно. Це дає класифікатору більш уніфіковані значення, зберігаючи релевантність значень кожного атрибута.

Крок 5. Видалення нульових і відсутніх значень.

Набір даних CICIDS2019 містить 2867 кортежів як відсутні та нескінченні значення. Це вирішується двома способами, що призводить до двох наборів даних. У другому наборі даних нескінченні значення замінюються максимальними значеннями, а відсутні значення замінюються середніми. Запропонований метод був протестований на обох наборах даних. Для оцінки запропонованого підходу використовувалися лише пакети інформації про атаку, при цьому пакети даних, що представляють нормальний мережевий трафік з обох наборів, ігнорувалися.

Крок 6. Оцінювання ознак.

Попередньо оброблені набори даних вводяться в процедуру кластеризації K-means, яка використовує кожен атрибут окремо, щоб ранжувати їх за важливістю перед тим, як застосувати для кластеризації всього набору даних. Для багатокласової класифікації k дорівнює кількості атак у наборах даних, що означає, що точка даних об’єкта кластеризується на дві групи: нормальна та аномальна. Щоб класифікувати атрибути, обчислюється оцінка однорідності кластерів, причому вища однорідність означає вищу подібність класу між об’єктами всередині кожного кластера. Високий бал означає, що цей атрибут важливий у класифікації, тоді як низький бал означає, що цей атрибут неважливий. Для обчислення найвищої

оцінки подібності між функціями спочатку було обчислено відстань, а потім створено цільову функцію:

$$\mathrm{distance}(C_j, p) = \sqrt{\left(\sum_{i}^{d} = 1[(C_{(j_i)} - p_i)] \right)^2}. \qquad (2.4)$$

З рівняння (2.4) можна обчислити відстань j-го кластера від центроїда C, щоб перевірити подібність j-го елемента в екземплярі i з точкою даних p в екземплярі i. Після цього можна створити цільову функцію, щоб мінімізувати відстань між центроїдом кластера та перевірити однорідність між вибраними функціями.

$$\mathrm{Obj}(C_j) = \sum_{m}^{p} [\mathrm{distance}(C_j, p)]^2 . \qquad (2.5)$$

Для ранжування ознак отримано цільову функцію для j-х ознак у рівнянні (2.5). Це надає мінімальну відстань центру C від p, взявши m як початкову точку для ранжування найкращих характеристик.

3 ЕКСПЕРИМЕНТАЛЬНІ РЕЗУЛЬТАТИ

У цьому розділі показано впровадження моделі xNN та отримані результати на вибраних наборах даних. Модель xNN було застосовано до обох наборів даних окремо. Обидва набори даних є загальнодоступними [37, 38]. В експериментальному дослідженні використано Python в якості мови програмування та компілятор Jupyter на системі, що використовує графічний процесор з частотою 3,2 ГГц. Фактично, це є мінімальною вимогою моделювання для експериментальної установки. На першому етапі було оцінено модель на основі точності, влучності, повноти і міри F1 для класифікації дев’яти атак у наборі даних UNSW-NB15. Крім того, на другому етапі модель була оцінена на наборі даних CICIDS2019.

3.1 Дослідження моделі xNN на наборі даних UNSW-NB15

Рисунок 3.1 показує якість моделі xNN на UNSW-NB15 після застосування методу оцінки функцій на основі кластеризації K-Means. На рисунку вісь ординат показує відносну оцінку характеристики, а вісь x – точність, влучність, повноту та міру F1 xNN. Це показує, що модель показує точність 99,7% класифікації атак у наборі даних на основі IoV.

З рисунку 3.2 видно, що без оцінки ознак влучність xNN становить 91,5%, що менше, ніж влучність класифікації з оцінкою ознак. На рисунку 3.2 вісь ординат показує відносну оцінку характеристики, а вісь x – точність, влучність, повноту та міру F1 xNN.

Рисунок 3.3 показує матрицю помилок з оцінкою ознак, а рисунок 3.4 показує матрицю помилок без оцінки ознак. З рисунку 3.3 видно, що справжній позитивний показник із оцінкою ознак набагато вищий, ніж без матриці помилок оцінки ознак.

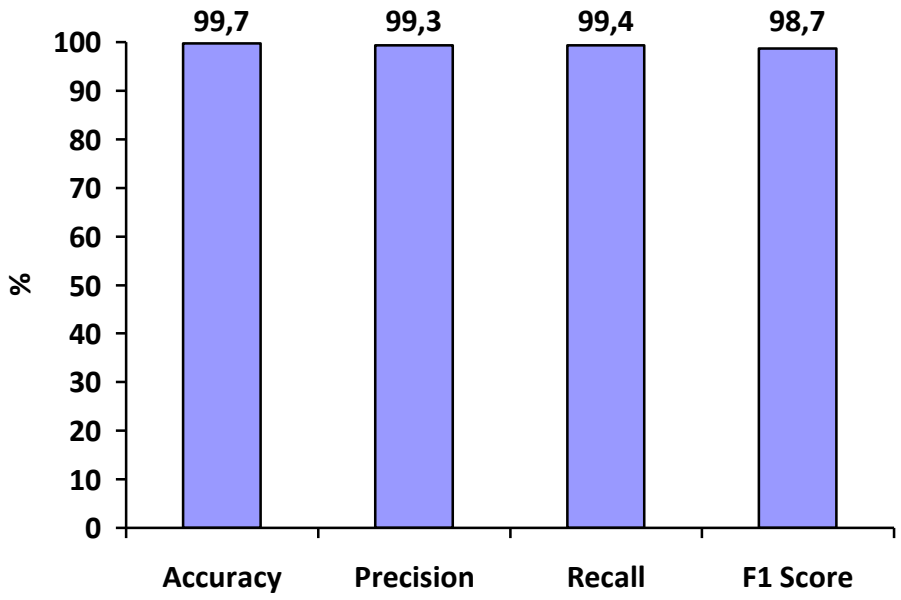

Рисунок 3.1 – Ефективність моделі xNN на UNSW-NB15

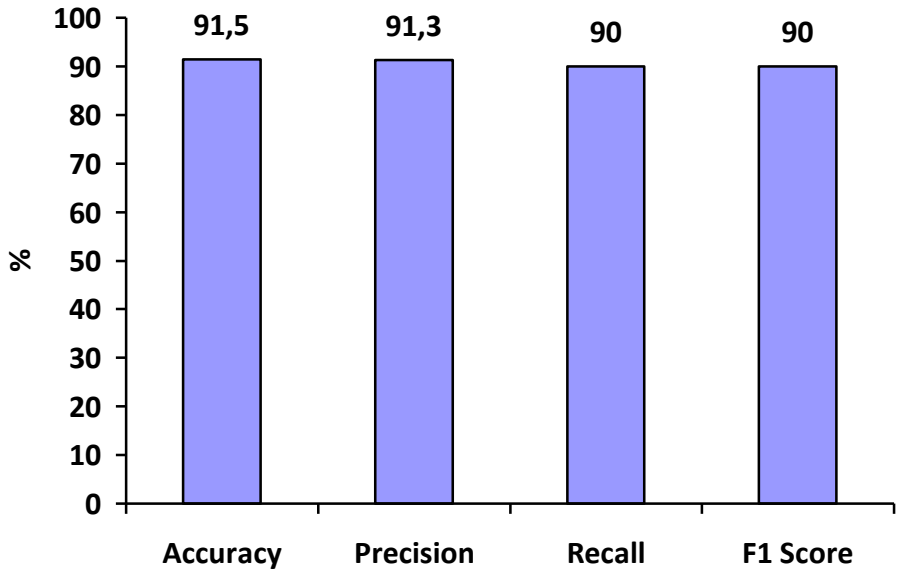

Рисунок 3.2 – Ефективність моделі xNN на UNSW-NB15 без оцінювання ознак

Також було застосовано згорткову нейронну мережу та довгу короткочасну пам’ять для класифікації атак, щоб порівняти запропоновану модель із попередніми сучасними моделями. xNN продемонструвала

багатообіцяючу точність і була найвищою серед інших моделей глибокого навчання. Порівняння моделей глибокого навчання для класифікації атак в UNSW-NB15 показано на рисунку 3.5. На рисунку вісь ординат показує відсоток точності, а вісь x – гістограму точності моделі.

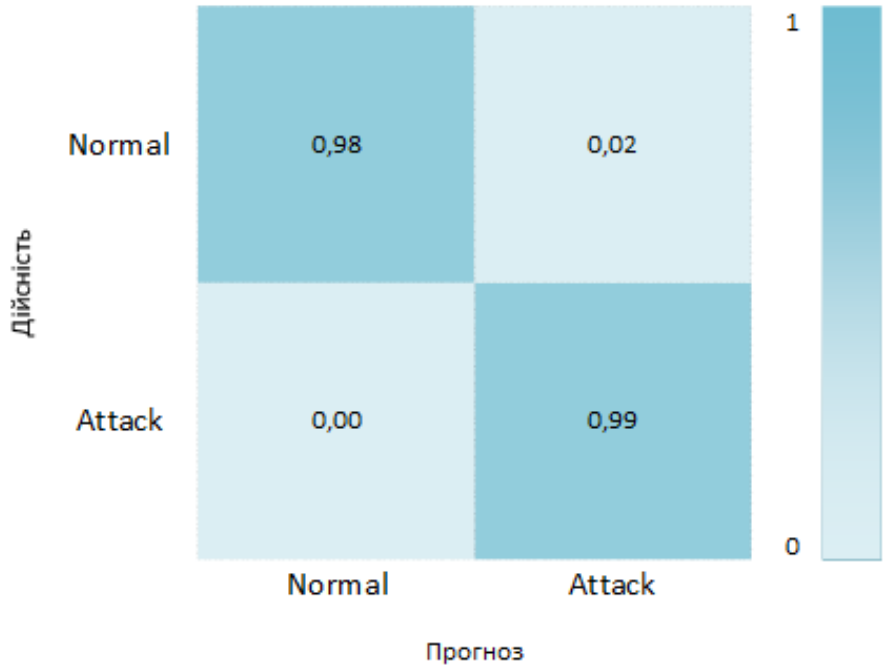

Рисунок 3.3 – Матриця помилок xNN для UNSW-NB15 із оцінюванням ознак

3.2 Дослідження моделі xNN на наборі даних CICIDS2019

Рисунок 3.6 показує якість моделі xNN на CICIDS2019 після застосування методу оцінки ознак на основі кластеризації K-means. Це показує, що модель була точною на 99,3% у класифікації атак у наборі даних на основі IoV. На рисунках 3.6 і 3.7, вісь y показує відсоток, а вісь x показує гістограму точності моделі.

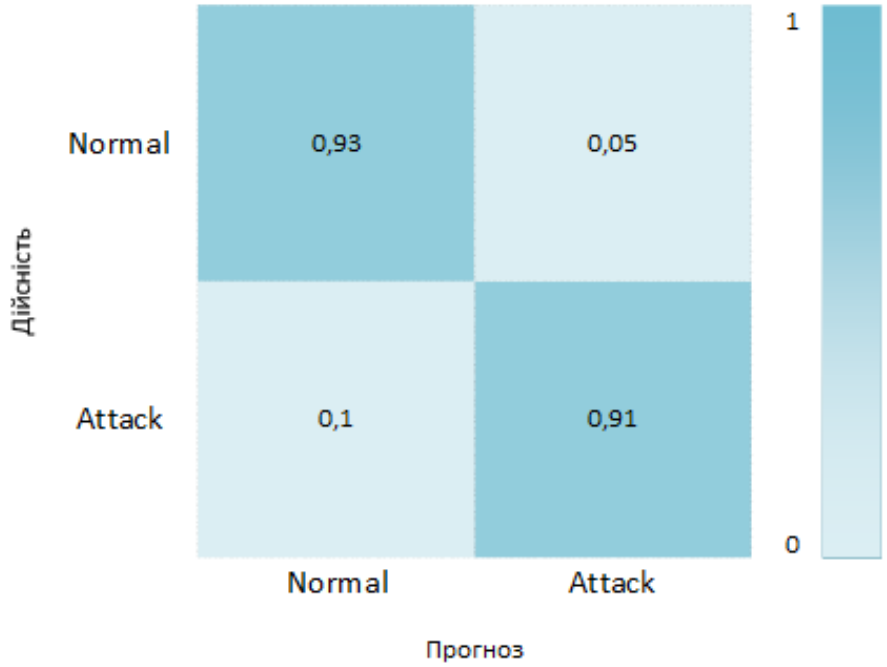

Рисунок 3.4 – Матриця помилок xNN для UNSW-NB15 без оцінювання ознак

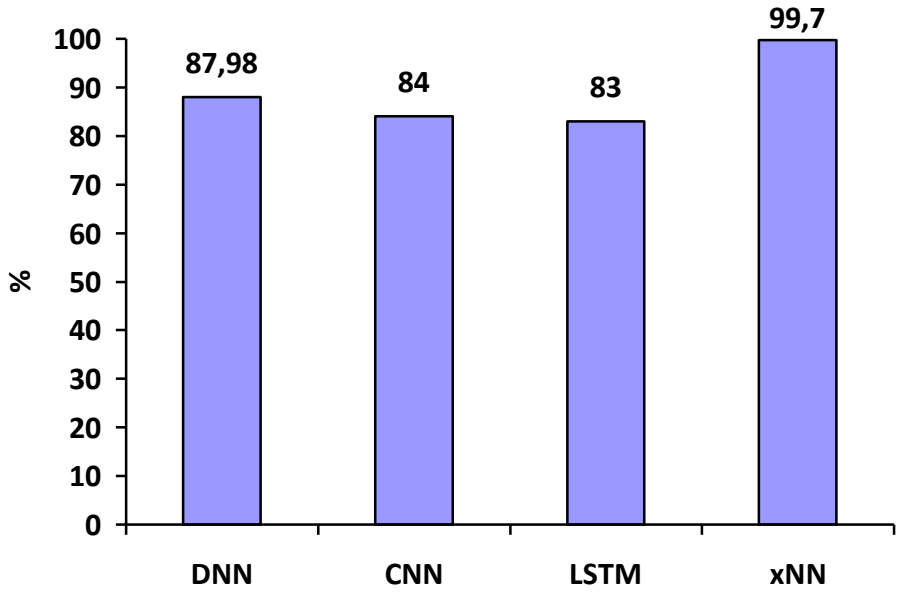

Рисунок 3.5 – Порівняння моделей глибокого навчання для класифікації атак в UNSW-NB15

З рисунку 3.7 видно, що без оцінки ознак точність xNN становить 87,3%, що менше, ніж точність з оцінкою ознак. Також було застосовано

згорткову нейронну мережу та довготривалу короткочасну пам’ять для класифікації атак, щоб порівняти запропоновану модель із попередніми сучасними моделями. xNN продемонструвала багатообіцяючу точність і була найвищою серед інших моделей глибокого навчання. Порівняння моделей глибокого навчання для класифікації атак у CICIDS2019 показано на рисунку 3.10. На рисунку вісь ординат показує відсоток точності, а вісь x – гістограму точності моделі.

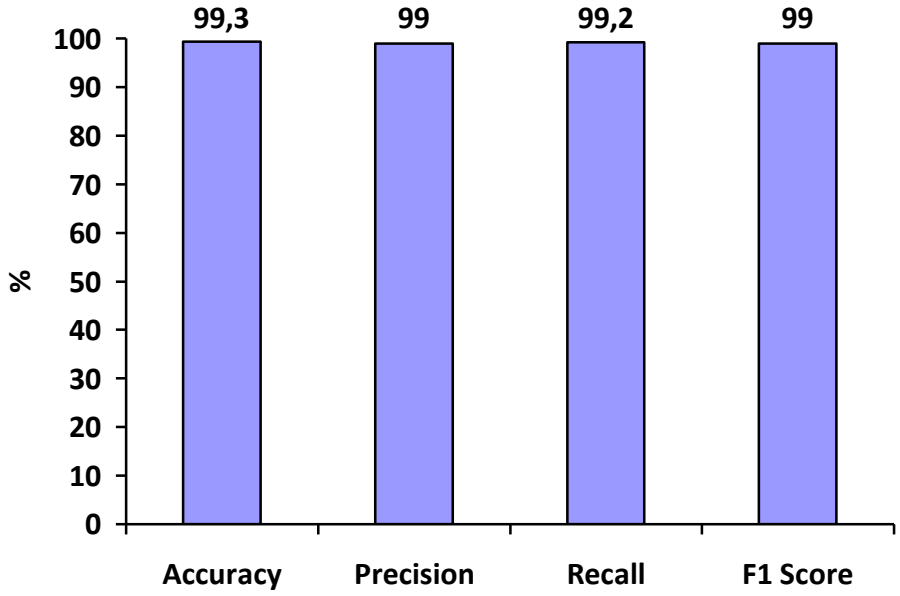

Рисунок 3.6 – Ефективність моделі xNN на CICIDS2019

Для порівняння можна побачити, що запропонована модель xNN показала хороші результати після використання техніки підрахунку характеристик. У першому наборі даних (UNSW-NB15) xNN показали хороші результати з найвищою точністю 99,7%, тоді як CNN набрав 87%, LSTM набрав 90%, а DNN набрав 92%. У класифікації атак у другому наборі даних (CICIDS2019) xNN отримав найвищу точність у 99,3%, CNN – 87%, LSTM – 89%, а DNN – 82%. Таблиці 3.1 і 3.2 демонструють порівняльний аналіз моделей глибокого навчання, запропонованих у цьому дослідженні, щоб підтвердити, що xNN має найвищу точність і є постійною моделлю для

виявлення вторгнень в обидва набори даних.

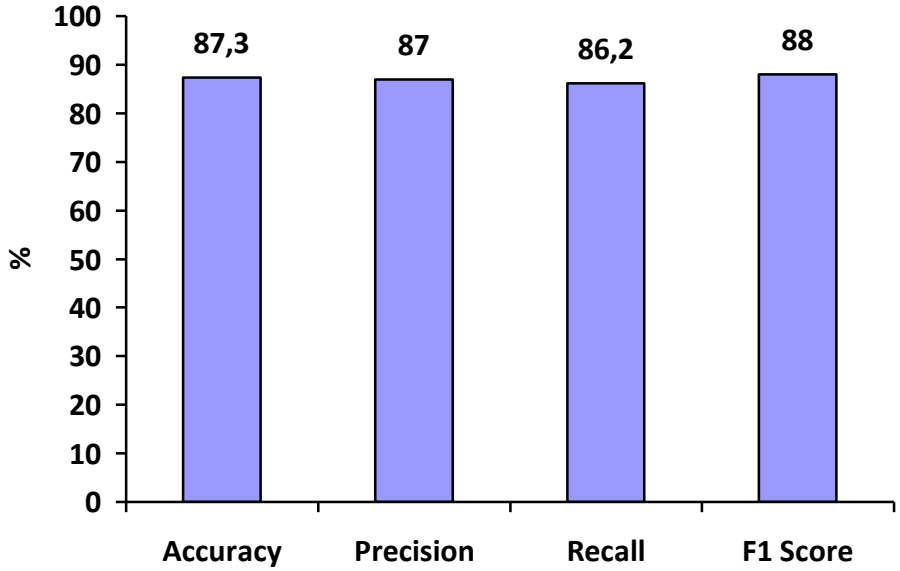

Рисунок 3.7 – Ефективність моделі xNN на CICIDS2019 без оцінювання ознак

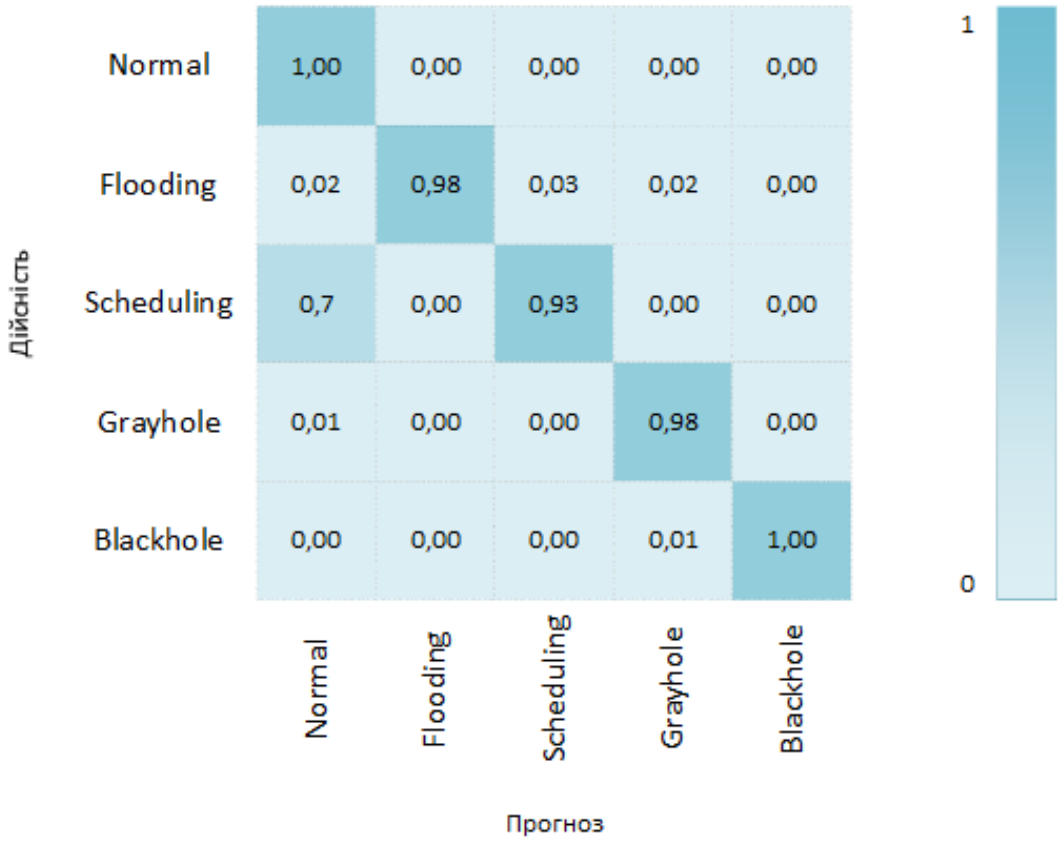

Рисунок 3.8 – Матриця помилок xNN для CICIDS2019 із оцінюванням ознак

Рисунки 3.8-3.9 демонструють матриці помилок xNN для CICIDS2019 з оцінкою ознак, матрицю помилок xNN для CICIDS2019 без оцінки ознак і порівняння моделі глибинного навчання на наборі даних CICIDS2019 відповідно.

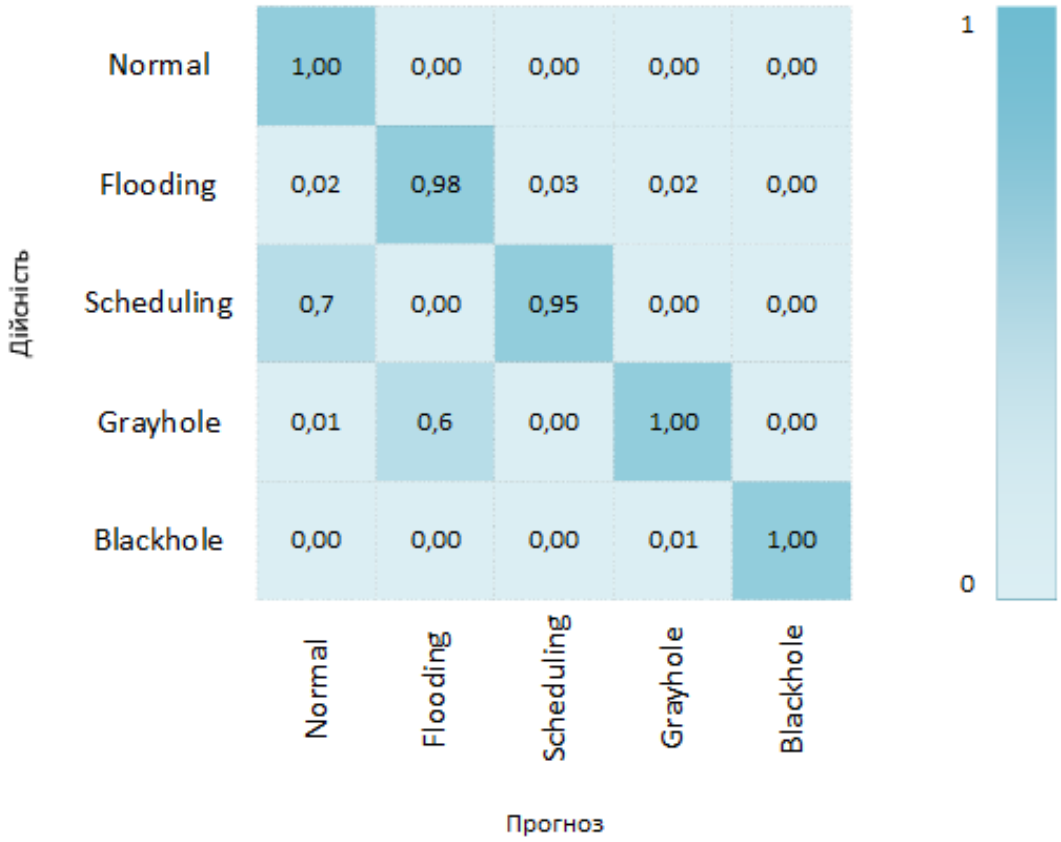

Рисунок 3.9 – Матриця помилок xNN для CICIDS2019 без оцінювання ознак

Запропоновану модель було порівняно з попередніми дослідженнями. Під час порівняльного аналізу було виявлено, що запропонована модель показала найвищу точність щодо деяких останніх попередніх методів дослідження.

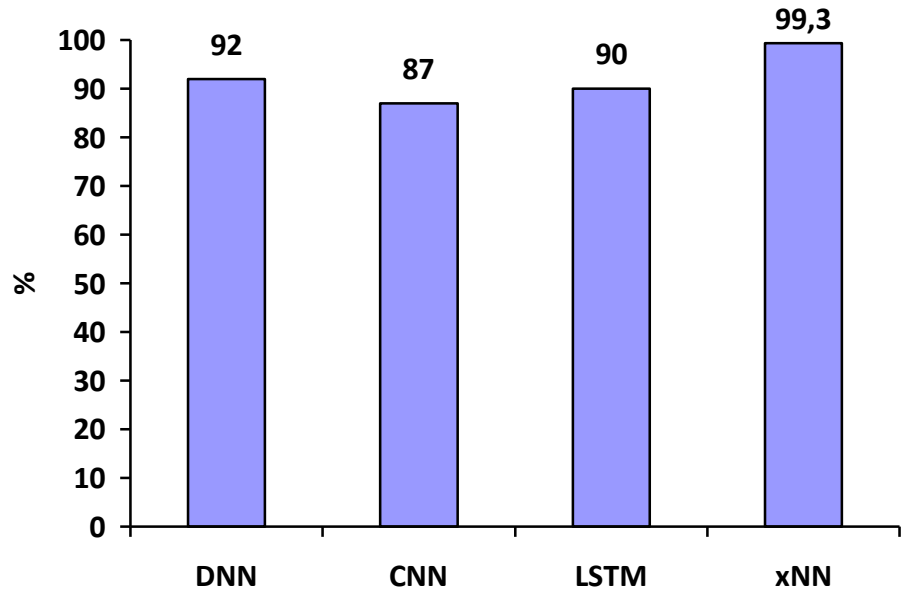

Рисунок 3.10 – Порівняння моделей глибокого навчання на наборі даних CICIDS2019

Таблиця 3.1 – Порівняльний аналіз моделей глибокого навчання

Модель	Набір даних	Оцінка ознак	Точність
xNN	CICIDS 2019	За замовчуванням	87,3 %
		K-means	99,3%
	UNSW-NB15	За замовчуванням	91,5%
		K-means	99,7%
LSTM	CICIDS 2019	За замовчуванням	89,7%
		K-means	90%
	UNSW-NB15	За замовчуванням	78,65%
		K-means	83%
CNN	CICIDS 2019	За замовчуванням	85,4%
		K-means	87%
	UNSW-NB15	За замовчуванням	79,67%
		K-means	84%

Продовження таблиці 3.1

Модель	Набір даних	Оцінка ознак	Точність
DNN	CICIDS 2019	За замовчуванням	83,2%
		K-means	92%
	UNSW-NB15	За замовчуванням	85%
		K-means	87,89%

Таблиця 3.2 – Порівняльний аналіз із попередніми дослідженнями

Посилання	Метод	Набір даних	Точність
Ян та ін.[1]	Гібридні моделі	CICIDS2017	96,3%
Ву та ін.[3]	Випадкові ліси	CICIDS2017	95%
Ding та ін.[9]	Модель суміші Гауса	CICIDS2017	97%
Негі та ін.[14]	MXNet	Офлайн-набір даних	98,5%
Wang та ін.[29]	Модель HTM	UNSW-NB15	97,45%
Гарг та ін.[32]	SVM	CICIDS2019	91%
Дана робота	Пояснювана нейронна мережа (xNN)	CICIDS2019	99,3% і 99,7%, відповідно
		UNSWNB15	

ВИСНОВКИ

Однією з найскладніших сучасних проблем є розробка систем, здатних якомога раніше виявляти атаки на повідомлення CAN. Мережі транспортних засобів можна захистити від кіберзагроз за допомогою технологій штучного інтелекту. Глибоке навчання захищає автономний транспортний засіб, коли зловмисник намагається проникнути до нього.

Для оцінки запропонованої системи безпеки використовувалися набори даних безпеки CICIDS2019 і UNSW-NB15. Попередня обробка – це процес перетворення даних категорії в числові дані. Задля визначення того, які характеристики є найважливішими, була використана кластеризація K-means.

Виявлення типів атак у цьому наборі даних було здійснено за допомогою пояснюваної нейронної мережі xNN. Точність, запам’ятовування, оцінка F1 і достовірність є високими для моделі, що стало обнадійливим результатом. Застосувавши методику підрахунку характеристик, можна побачити, що запропонована модель xNN перевершила конкурентів. У наборі даних 1 (UNSW-NB15) xNN перевершив конкурентів, набравши 99,7% точності, тоді як CNN набрав 87% точності, LSTM набрав 90% точності, а DNN набрав 92% точності. У класифікації атак у другому наборі даних (CICIDS2019) xNN досягла найвищої точності 99,3%, за нею йдуть CNN з точністю 87%, LSTM з точністю 89% і DNN з точністю 82%.

Що стосується точності виявлення та класифікації, а також безпеки шини CAN у реальному часі, запропонований підхід перевершив існуючі рішення в дослідженні.

Цю роботу можна поширити на реальні сценарії та керовані транспортні засоби в реальному часі, а також на автономні системи для захисту від зловмисних атак. Пакет даних у протоколі, проаналізований із максимальними значеннями за допомогою високопродуктивної моделі xNN, буде кращим для використання в майбутньому для зменшення та усунення

атак на безпеку, наприклад для IoV.

Внесок цього дослідження узагальнено таким чином.

1. Наскільки відомо, xNN ніколи не реалізовувався в IDS, особливо в транспортних комп’ютерних мережах.

2. Оцінка та ранжирування ознак на основі K-means також сприяли в цьому дослідженні найкращим методам вибору ознак і ранжирування на основі вагових коефіцієнтів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles. IEEE Internet Things J. 2021, 9, 616-632.

2. Irshad, M.; Liu, W.; Wang, L.; Khalil, M.U.R. Cogent Machine Learning Algorithm for Indoor and Underwater Localization Using Visible Light Spectrum. Wirel. Pers. Commun. 2021, 116, 993-1008.

3. Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A Survey of Intrusion Detection for In-Vehicle Networks. IEEE Trans. Intell. Transp. Syst. 2020, 21, 919-933.

4. Alshammari, A.; Zohdy, M.A.; Debnath, D.; Corser, G. Classification Approach for Intrusion Detection in Vehicle Systems. Wirel. Eng. Technol. 2018, 9, 79-94.

5. Raziq, Y.; Sadiq, A.; Ali, H.; Asar, A.A. AI and Blockchain Integrated Billing Architecture for Charging the Roaming Electric Vehicles. IoT 2020, 7, 382-397.

6. Li, Y.; Xue, W.; Wu, T.; Wang, H.; Zhou, B.; Aziz, S.; He, Y. Intrusion detection of cyber physical energy system based on multivariate ensemble classification. Energy 2021, 218, 119505.

7. Garg, S.; Singh, A.; Aujla, G.S.; Kaur, S.; Batra, S.; Kumar, N. A Probabilistic Data Structures-Based Anomaly Detection Scheme for Software-Defined Internet of Vehicles. IEEE Trans. Intell. Transp. Syst. 2021, 22, 3557-3566.

8. Xiao, J.; Wu, H.; Li, X. Internet of Things Meets Vehicles: Sheltering In-Vehicle Network through Lightweight Machine Learning. Symmetry 2019, 11, 1388.

9. Ding, N.; Ma, H.; Zhao, C.; Ma, Y.; Ge, H. Driver's Emotional State-Based Data Anomaly Detection for Vehicular Ad Hoc Networks. In Proceedings of

the 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, 9-11 August 2019; pp. 121-126.

10. Li, X.; Hu, Z.; Xu, M.; Wang, Y.; Ma, J. Transfer learning based intrusion detection scheme for Internet of vehicles. Inf. Sci. 2021, 547, 119-135.

11. Rajbahadur, G.K.; Malton, A.J.; Walenstein, A.; Hassan, A.E. A Survey of Anomaly Detection for Connected Vehicle Cybersecurity and Safety. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Suzhou, China, 26-30 June 2018; pp. 421-426.

12. Joy, J.; Rabsatt, V.; Gerla, M. Internet of Vehicles: Enabling safe, secure, and private vehicular crowdsourcing. Internet Technol. Lett. 2018, 1, e16.

13. Muter, M.; Groll, A.; Freiling, F.C. A structured approach to anomaly detection for in-vehicle networks. In Proceedings of the 2010 Sixth International Conference on Information Assurance and Security, Atlanta, GA, USA, 23-25 August 2010; pp. 92-98.

14. Negi, N.; Jelassi, O.; Chaouchi, H.; Clemencon, S. Distributed online Data Anomaly Detection for connected vehicles. In Proceed-ings of the 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 19-21 February 2020; pp. 494-500.

15. Wang, W.; Xia, F.; Nie, H.; Chen, Z.; Gong, Z.; Kong, X.; Wei, W. Vehicle Trajectory Clustering Based on Dynamic Representation Learning of Internet of Vehicles. IEEE Trans. Intell. Transp. Syst. 2021, 22, 3567-3576.

16. Jiang, Y.; Zhang, J. Interaction between company Manager’s and Driver’s decisions on expressway routes for truck transport. Transp. Policy 2019, 76, 1-12.

17. Zhang, R.; Aziz, S.; Farooq, M.; Hasan, K.; Mohammed, N.; Ahmad, S.; Ibadah, N. A Wind Energy Supplier Bidding Strategy Using Combined EGA-Inspired HPSOIFA Optimizer and Deep Learning Predictor. Energies 2021, 14, 3059.

18. Lydia, E.; Jovith, A.; Devaraj, A.; Seo, C.; Joshi, G. Green Energy Efficient Routing with Deep Learning Based Anomaly Detection for Internet of

Things (IoT) Communications. Mathematics 2021, 9, 500.

19. Nie, X.; Min, C.; Pan, Y.; Li, K.; Li, Z. Deep-Neural-Network-Based Modelling of Longitudinal-Lateral Dynamics to Predict the Vehicle States for Autonomous Driving. Sensors 2022, 22, 2013.

20. Ma, Z.; Guo, S.; Xu, G.; Aziz, S. Meta Learning-Based Hybrid Ensemble Approach for Short-Term Wind Speed Forecasting. IEEE Access 2020, 8, 172859-172868.

21. Irshad, M.; Liu, W.; Arshad, J.; Sohail, M.N.; Murthy, A.; Khokhar, M.; Uba, M.M. A Novel Localization Technique Using Luminous Flux. Appl. Sci. 2019, 9, 5027.

22. Sakiyama, A.; Watanabe, K.; Tanaka, Y. Spectral Graph Wavelets and Filter Banks With Low Approximation Error. IEEE Trans. Signal Inf. Process. Netw. 2016, 2, 230-245.

23. Hamada, Y.; Inoue, M.; Adachi, N.; Ueda, H.; Miyashita, Y.; Hata, Y. Intrusion detection system for in-vehicle networks. SEI Tech. Rev. 2019, 88, 76-81.

24. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of Internet of Vehicles. China Commun. 2014, 11, 1-15.

25. Wang, X.; Mavromatis, I.; Tassi, A.; Santos-Rodriguez, R.; Piechocki, R.J. Location Anomalies Detection for Connected and Autonomous Vehicles. In Proceedings of the 2019 IEEE 2nd Connected and Automated Vehicles Symposium (CAVS), Honolulu, HI, USA, 22-23 September 2019; pp. 1-5.

26. Ding, N.; Ma, H.; Zhao, C.; Ma, Y.; Ge, H. Data Anomaly Detection for Internet of Vehicles Based on Traffic Cellular Automata and Driving Style. Sensors 2019, 19, 4926. [PubMed]

27. Chandola, V.; Banerjee, A.; Kumar, V. Survey of Anomaly Detection. ACM Comput. Surv. 2009, 41, 1-72.

28. Araujo. Innovative Approaches to Quality Assurance in Healthcare. Bull. Roszdravnadzor 2017, 6, 5-9.

29. Wang, C.; Zhao, Z.; Gong, L.; Zhu, L.; Liu, Z.; Cheng, X. A Distributed

Anomaly Detection System for In-Vehicle Network Using HTM. IEEE Access 2018, 6, 9091-9098.

30. Khalastchi, E.; Kaminka, G.A.; Kalech, M.; Lin, R. Online anomaly detection in unmanned vehicles. In Proceedings of the 10th International Conference on Advanced Agent Technology, Taipei, Taiwan, 2-6 May 2011; Volume 1, pp. 105-112.

31. Narayanan, S.N.; Mittal, S.; Joshi, A. OBD SecureAlert: An Anomaly Detection System for Vehicles. IEEE Workshop Smart Serv. Syst. 1993. Available online: https://ebiquity.umbc.edu/_file_directory_/papers/792.pdf (accessed on 20 January 2022).

32. Garg, S.; Kaur, K.; Kaddoum, G.; Gagnon, F.; Kumar, N.; Han, Z. Sec-IoV. In Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era-PERSIST-IoT ’19, Catania, Italy, 2 July 2019; pp. 37-42.

33. Aziz, H.S.; Wang, Y.; Liu, J.P.; Fu, X. An Approach to Kinetic Energy Recovery System for Electric Vehicle Considering SC and Bi-directional Converters. In Proceedings of the IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), Singapore, 22-25 May 2018; pp. 1273-1277.

34. Yang, S.; Liu, Z.; Li, J.; Wang, S.; Yang, F. Anomaly Detection for Internet of Vehicles: A Trust Management Scheme with Affinity Propagation. Mob. Inf. Syst. 2016, 2016, 1-10.

35. Oucheikh, R.; Fri, M.; Fedouaki, F.; Hain, M. Deep Real-Time Anomaly Detection for Connected Autonomous Vehicles. Procedia Comput. Sci. 2020, 177, 456-461.

36. Wang, Y.; Masoud, N.; Khojandi, A. Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors. IEEE Trans. Intell. Transp. Syst. 2021, 22, 1411-1421.

37. IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. Available online: https://www.unb.ca/cic/ datasets/ids-2017.html (accessed on 29 January 2022).

38. Moustafa, N.; Slay, J. The evaluation of Network Anomaly Detection

Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Inf. Secur. J. A Glob. Perspect. 2016, 25, 18-31.

39. Росінський Д. М., Волошин І. А. Система виявлення аномалій у мережі IoV // Проблеми інформатизації. Тези доповідей десятої міжнародної науково-технічної конференції, 24-25 листопада 2022 р., Черкаси: ЧДТУ, 2022. – С. 74.