Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Метод виявлення порушника в мережі на основі аналізу вихідних DNS-запитів нейронною мережею

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.220184.22.01.11 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Підпис Ємець М.О.

Керівник доц., к.т.н, доцент _____ Підпис Орленко В.С.

Нормоконтролер старший викладач _____ Підпис Мостовий С.В.

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Підпис Кльоц Ю.П.

8 12 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма КІБЕРБЕЗПЕКА

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ємцю Максиму Олександровичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод виявлення порушника в мережі на основі аналізу вихідних DNS-запитів нейронною мережею

Керівник роботи Орленко Вікторія Сергіївна

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 01.12.2023

3. Вихідні дані до проекту (роботи) Розрахунок ефективності LSTM мережі для виявлення зловмисного трафіку; розрахунок ефективності CNN мережі для виявлення зловмисного трафіку, розробка методу аналізу нейронною мережею вихідних DNS-запитів, що буде забезпечувати кращу ефективність у порівнянні із вищевказаними.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз атак із використанням DNS-трафіку та наявних методів виявлення. Модель DNS-запиту. Модель мережі. Метод виявлення порушника. Реалізація CNN-LSTM мережі. Доведення ефективності. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – загрози у комп'ютерних мережах; аналіз наявних методів виявлення порушника; постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі; вибір нейронних мереж для подальшої роботи	02.10.2023	
5	Робота над розділом 3 – реалізація тестового середовища; метод виявлення порушника	16.10.2023	
6	Робота над розділом 4 – реалізація розробленого методу; оцінка ефективності	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент _____ М.О. Ємець
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.С. Орленко
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод виявлення порушника в мережі на основі аналізу вихідних DNS-запитів нейронною мережею

Автор роботи: Ємець Максим Олександрович

Керівник роботи: к.т.н., доц. Орленко Вікторія Сергіївна

Загальний обсяг роботи: 82 сторінки, 31 рисунок, 12 таблиць, 1 додаток, 60 посилань.

Ключові слова: нейронна мережа, CNN мережа, LSTM мережа, порушник, DNS-запити.

Цифровізація суспільства призводить до збільшення відкритих сегментів мережі чи розгортання Wi-Fi мереж. Недоліком даних мереж є відсутність систем захисту, оскільки наявні рішення доцільно використовувати для приватних мереж. Зловмисники користуються цим та реалізовують атаки за допомогою публічних мереж. Тому для забезпечення роботоздатності мережі без наявності зловмисників доцільно розробити метод виявлення порушників, який можна буде легко впровадити у публічному сегменті.

В роботі представлено аналіз загроз у комп'ютерній мережі із використанням DNS-трафіку та проведено дослідження застосування нейронних мереж для виявлення порушника в мережі. Розроблено метод виявлення порушника на основі аналізу вихідних DNS-запитів; проведено дослідження ефективності CNN та LSTM нейронних мереж для пошуку порушників. Реалізовано CNN-LSTM нейронну мережу, яка під час доведення ефективності продемонструвала кращий результат у порівнянні з вищевказаними.

8.12.2023

ANNOTATION

Theme of qualification work: The method of detecting a violator in the network based on the analysis of outgoing DNS requests by a neural network

Author of the work: Yemets Maksym Oleksandrovych

Mentor: Ph.D., Assoc. Viktoriya Serhiyivna Orlenko

Total volume of work: 82 pages, 31 figures, 12 tables, 1 appendix, 60 references.

Keywords: neural network, CNN network, LSTM network, intruder, DNS queries.

Digitization of society leads to an increase in open network segments or deployment of Wi-Fi networks. The disadvantage of these networks is the lack of protection systems since the existing solutions should be used for private networks. Criminals take advantage of this and implement attacks using public networks. Therefore, to ensure the network's operation without intruders, it is advisable to develop a method of detecting violators, which can be easily implemented in the public segment.

The paper presents the analysis of threats in the computer network using DNS traffic and research on using neural networks to detect intruders in the network. A method of detecting the violator based on the analysis of outgoing DNS requests has been developed; a study of the effectiveness of CNN and LSTM neural networks for the search of violators was carried out. A CNN-LSTM neural network was implemented, demonstrating a better result than the above when proving its effectiveness.

8.12.2023

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

CNN –згорткова нейронна мережа (convolutional neural network)

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

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

IPS – система запобігання вторгненням (англ. Intrusion Prevention System)

LSTM – довга короткочасна пам’ять (long short-term memory)

НМ – нейронна мережа

ШНМ – штучна нейронна мережа

ВСТУП

Розвиток інформаційних технологій став невід'ємною частиною життя сучасного суспільства, а оскільки інформація є одним із найцінніших і найважливіших ресурсів будь-якого бізнес-процесу, інформаційна безпека стала найважливішим аспектом грамотного ведення бізнесу. Інформаційна безпека включає комплекс заходів, спрямованих на запобігання та усунення несанкціонованого доступу, обробки, спотворення, форматування, аналізу, неузгодженого оновлення, виправлення та знищення даних. Простіше кажучи, це набір заходів, стандартів та технологій, необхідних для захисту конфіденційних даних.

Проблема захисту інформації від несанкціонованого доступу та небажаних впливів існує давно, з розвитком людського суспільства, появою приватної власності, державного устрою, подальшим розширенням людської діяльності інформація набуває все більшого значення. Інформація стає цінною, а володіння нею дозволить нинішнім та потенційним власникам отримувати певні виграші.

Сьогодні питання важливості захисту інформації стоїть на першому місці. Проблема захисту стає все більш серйозною у зв'язку з обставинами, головними з яких є: масове розширення засобів електронної обчислювальної техніки; ускладнення шифрувальних технологій; потреба захисту не тільки державної та військової таємниці, а й промислової, комерційної та фінансової таємниць; розгортання можливості несанкціонованих дій над інформацією. Питання захисту інформації вимагають уваги, їх вирішення залежить від об'єктивних та суб'єктивних факторів. Таким чином, проблема забезпечення технічної захисту інформації є надзвичайно актуальною на сьогоднішній день.

Об’єкт дослідження - вихідний DNS-трафік.

Предмет дослідження – методи аналізу та виявлення зловмисного трафіку.

Мета дослідження полягає у визначенні методів виявлення зловмисного трафіку із застосуванням нейронних мереж.

Завдання дослідження наступні:

1. Проаналізувати наявні методи виявлення та ідентифікації порушників в інформаційно-комунікаційних системах, визначивши їх переваги та недоліки, особливості реалізації.

2. Дослідити наявні системи запобігання та виявлення вразливостей та вторгнень з метою порівняння їх функціональних можливостей та сфери застосування.

3. Дослідити особливості навчання, тестування та організації функціонування згорткової нейронної мережі для виявлення зловмисного DNS-трафіку, охарактеризувати переваги та недоліки даної мережі.

4. Дослідити особливості навчання, тестування та організації функціонування нейронної мережі довгої короткостроковій пам'яті для виявлення зловмисного DNS-трафіку, оцінити переваги та недоліки, запропонувати шляхи покращення.

5. Розробити метод виявлення зловмисного вихідного DNS-трафіку шляхом аналізу запитів у публічному сегменті мережі нейронною мережею.

Методи дослідження. Задля дослідження предметної області застосовувався метод узагальненнята метод порівняння, загальнонаукові методи аналізу і синтезу. Для вирішення поставлених задач використовуються основні положення методів аналізу даних й теорії множин та машинного навчання, математичної статистики.

Практична цінність роботи полягає у розширенні знань про застосування нейронних мереж в кібербезпеці, а саме реалізація методу виявлення порушника в публічній мережі на основі аналізу вихідних DNS-запитів.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Класифікація загроз у комп’ютерних мережах

Комп'ютерна мережа - це сукупність взаємопов'язаних комп'ютерів та інших пристроїв, які можуть обмінюватися даними і ресурсами через комунікаційні канали, такі як кабелі, бездротові з'єднання або інші технології передачі даних. Комп'ютерні мережі використовуються для спільного доступу до інформації, друку, забезпечення комунікації між користувачами та пристроями, а також для забезпечення інтернет-з'єднання. Слід зазначити, що у багатьох мережах існують спеціалізовані сервери, які забезпечують ресурси та послуги, і клієнти, які звертаються до серверів для доступу до цих ресурсів. Комп'ютерні мережі грають ключову роль в сучасному інформаційному суспільстві, забезпечуючи спосіб обміну даними і спілкування між користувачами та пристроями, що розташовані на різних відстанях один від одного.

Загрози в комп’ютерних мережах стосуються потенційних ризиків або вразливостей, що ставлять під загрозу безпеку мережі, цілісність даних мережі та користувачів. Ці загрози можуть надходити з різноманітних джерел, включаючи зловмисників, уразливості програмного забезпечення та ненавмисні дії.

Зловмисні дії в комп'ютерній мережі можуть призвести до різних наслідків, які можуть нанести значну шкоду як користувачам, так і організаціям. Ось деякі загальні наслідки зловмисних дій в комп'ютерній мережі:

- знищенням даних, які можуть призвести до втрати важливих і конфіденційних даних;
- доступ до особистих або конфіденційних даних користувачів або організацій і використовувати цю інформацію для незаконних цілей, таких як шахрайство або ідентичність;
- зміна або внесення незаконних змін в документи, програми або веб-сайти може призвести до впливу на інформаційні ресурси;

- атаки на відмову в обслуговуванні, що можуть переповнювати ресурси мережі, що призводить до відмови у доступі для легітимних користувачів, а також втрати часу і грошей;
- використання комп'ютерів та інші пристрої для створення ботнетів для виконання злочинних дій, таких як розсилка спаму, атаки на інші мережв або крадіжка інформації;
- зловмисники можуть використовувати мережу для поширення вірусів, червів та іншого шкідливого програмного забезпечення, що може заражати інші системи.

1.1.1 Шкідливе програмне забезпечення

Шкідливе програмне забезпечення – зловмисний код, що спеціально розроблений для руйнування, викрадення даних чи інших зловмисних дій у мережі. До найпоширеніших типів шкідливого програмного забезпечення відносять віруси, троянських коней, хробаків, програми-вимагачі [1].

Шкідливе програмне забезпечення «Троянський кінь» класифікують у відповідності до того, яким чином впливають на роботу комп’ютерної мережі, як показано у таблиці 1.1.

Таблиця 1.1 – Класифікація шкідливого програмного забезпечення «Троянський кінь»

Тип	Опис
1	2
Віддалений доступ	Віддалений доступ дозволяється для неавторизованих користувачів
Надсилання даних	Існує загроза щодо надсилання конфіденційної інформації із мережі
Деструктивний	Здійснює видалення чи пошкодження файлів у системі

Кінець таблиці 1.1 – Класифікація шкідливого програмного забезпечення «Троянський кінь»

1	2
Proxy	За допомогою комп’ютера жертви здійснює атаки на третіх осіб
FTP	Вмикає на кінцевих пристроях несанкціоновані служби передачі файлів
Вимкнення захисту	Вимикає брандмауери та антивірусні програми
DoS	Завантажує канал передачі даних задля зупинки роботи мережі за допомогою надсилання великої кількості даних чи спеціально форматований пакет, котрий одержувач не може обробити і передача даних відбувається на мінімальних швидкостях чи зупиняється.

Хробаки здатні функціонувати, поширюватись та розмножуватись мережею самостійно, використовуючи для цього вразливості системи та спричиняючи сповільнення роботи мережі. Прикладом роботи мережевого хробака з використанням вразливості системи є SQL Slammer, котрий у 2003 році за 30 хв свого функціонування заразив понад 250 000 хостів.

Програми-вимагачі можуть заборонити доступ до комп’ютерної системи або даних із системи. Вони використовують різні алгоритми шифрування даних, а головною метою є отримання грошової винагороди.

1.1.2 Access Attacks

Задля отримання доступу до веб-акаунтів чи баз даних дана атака використовує відомі вразливості в службах автентифікації, FTP та веб-службах. Під час password attacks (атаки на пароль) зловмисник намагається підібрати пароль різними відомими методами, зокрема за словником чи Brute force. При spoofing attacks порушник намагається видати себе за іншу особу, фальсифікуючи дані.

Також при атаках на доступ можуть реалізовуватись інші типи: експлуатація довіри, перенаправлення портів, переповнення буфера та інші [2].

1.1.3 Атаки відмови в обслуговуванні

Ключовим завданням є пошук вразливостей, що пов’язані із системною пам’яттю, та їх подальше використання. Зокрема, для ОС Windows 10 існувала вразливість до відмови в обслуговуванні в драйвері AHCACHE.SYS. Спеціально створений файл Portable Executable міг спричинити перевірку помилок у ядрі Windows, що призводило до віддаленої відмови в обслуговуванні [3].

1.1.4 Атаки соціальної інженерії

Social Engineering Attacks – атаки, що намагаються маніпулювати людьми, використовуючи їх слабкості, з метою виконання певних дій чи розголошення конфіденційної інформації. [4] Задля реалізації даної атаки використовують різні методи (табл.1.2).

Таблиця 1.2 – Класифікація атак соціальної інженерії

Тип	Опис
1	2
Pretexting	Зловмисник вдає, що йому потрібні особисті або фінансові дані, щоб підтвердити особу одержувача
Phishing	Зловмисник надсилає шахрайську електронну пошту, яка маскується як надходження з законного надійного джерела, щоб обманом змусити одержувача встановити зловмисне програмне забезпечення на своєму пристрої або надати особисту чи фінансову інформацію
Spear phishing	Зловмисник створює цілеспрямовану фішингову атаку, призначену для конкретної особи чи організації
Spam	Також відомий як небажана пошта, це небажана електронна пошта, яка часто містить шкідливі посилання, зловмисне програмне забезпечення або оманливий вміст

Кінець таблиці 1.2– Класифікація атак соціальної інженерії

1	2
Something for Something	Іноді це називається «Quid pro quo», коли загрозливий суб'єкт запитує особисту інформацію від сторони в обмін на щось, наприклад подарунок
Baiting	Зловмисник залишає заражену шкідливим програмним забезпеченням флешку в публічному місці. Жертва знаходить диск і, нічого не підозрюючи, вставляє його у свій ноутбук, ненавмисно встановлюючи шкідливе програмне забезпечення
Impersonation	У цьому типі атаки загрозливий актор видає себе за когось іншого, щоб завоювати довіру жертви
Tailgating	Тут зловмисник швидко слідує за авторизованою особою в безпечне місце, щоб отримати доступ до безпечної зони.
Shoulder surfing	Це місце, де загрозливий актор непомітно оглядається через чиєсь плече, щоб викрасти їхні паролі чи іншу інформацію
Dumpster diving	Саме тут загрозливий актор нишпорить у сміттєвих баках, щоб знайти конфіденційні документи

1.1.5 Розвідувальні атаки

Розвідувальні атаки передують атакам доступу або атакам DoS. Оскільки їх головним завданням є збір інформації з метою виявлення вразливостей мережі чи даних про власника [5,6]. Дані атаки класифікують наступним чином (табл.1.3).

Таблиця 1.3 – Класифікація розвідувальних атак

Тип	Опис
1	2
Сканування мережі	Зловмисники сканують комп'ютерну мережу з метою відстеження включених пристроїв чи доступних портів

Кінець таблиці 1.3 – Класифікація розвідувальних атак

1	2
Отримання інформації з DNS	Зловмисники використовують DNS запити для отримання інформації
Фінгерпринтинг	Зловмисники збирають інформацію про ОС чи конфігурацію системи з метою подальшого використання для реалізації інших атак
Соціальний інжиніринг	Зловмисники зловживають довірою людей або застосовують маніпуляції для отримання доступу до інформації

1.2 Аналіз наявних методів виявлення та ідентифікації порушника в інформаційно-комунікаційних системах

Вейвлет-аналіз - це метод аналізу сигналів або даних, який базується на використанні вейвлет-функцій. Основна ідея вейвлет-аналізу полягає в тому, що сигнал розбивається на складові частини з різною частотною і просторовою інформацією. Це дозволяє виявити локальні особливості сигналу та аналізувати його. Вейвлет-аналіз є потужним інструментом для виявлення змін в сигналах, компресії даних, відновлення сигналів та багатьох інших задач обробки сигналів і зображень. Вейвлет-перетворення ділить часові ряди на високочастотні та низькочастотні послідовності. Відповідно до характеристик даних різних послідовностей встановлюється модель прогнозування. Вейвлет-нейронна мережа виконує різноманітні завдання щодо аналізу зображень, розпізнавання сигналів, а модифікована система здатна прогнозувати вторгнення та інше [7-9].

Статистичний аналіз - це методологія обробки даних, яка використовує статистичні методи для опису, виокремлення шаблонів, виявлення зв'язків та здійснення узагальнень на основі зібраних даних. Він забезпечує систематичний підхід до використання числових даних з метою отримання висновків та прийняття рішень [10]. Зокрема різні статистичні підходи застосовуються для виявлення

DDoS-атак [11]. А їх використання для виявлення атак є ефективним за рахунок того що вони адаптуються до змін у поведінці користувача та відсутні баз даних, які потребують систематичних оновлень [10,12].

Використання ентропії дозволяє виявляти аномальні зміни у розподілі даних, що можуть свідчити про втручання або незвичайну активність в мережі. Аналіз ентропії може бути застосований до різних типів даних, таких як мережевий трафік, системні журнали, поведінкові дані тощо. Ідентифікація порушника зазвичай відбувається шляхом порівняння поточного рівня ентропії з попередньо встановленим порогом. Якщо поточний рівень ентропії перевищує поріг, то це може свідчити про наявність порушення або незвичайної активності. Після виявлення аномалій можуть застосовуватись додаткові методи аналізу для ідентифікації конкретного типу атаки або порушення. Аналіз ентропії є одним із способів виявлення аномалій в інформаційно-комунікаційних системах, але важливо враховувати, що він може мати певні обмеження і не здатний виявити всі типи атак або порушень. [13-16]

Спектральний аналіз полягає в тому, що кожен сигнал може бути розкладений на різні частотні компоненти. Аналізуючи спектральну складову сигналу, можна виявити незвичайні або аномальні шаблони, які можуть свідчити про наявність порушника в мережі.

Фрактальний та мультифрактальний аналіз використовується для аналізу структури та характеристики трафіку, що передається в мережі. Основним завданням є виявлення та відслідковування самоподібності трафіку. Застосування фрактального аналізу дозволяє виявити фрактальні характеристики аномальної поведінки в мережі, яка може свідчити про зловмисні дії [17].

Сигнатурний метод може бути використаний для виявлення відомих атак. Сигнатури атак є унікальними характеристиками атаки, такими як певні послідовності байтів, значення підписів або інші показники, які ідентифікують конкретний тип атаки. Ці сигнатури розробляються на основі аналізу відомих атак або вразливостей. Коли IDS або IPS аналізують мережевий трафік або системні журнали, вони порівнюють ці дані зі зареєстрованими сигнатурами атак. Якщо

знайдено відповідність, то система може спрацювати і виконати певні заходи захисту, такі як блокування зловмисного трафіку, генерація сповіщень адміністраторам або автоматичне втручання. Мова опису сценаріїв застосовується для виявлення подій, котрі важко описати сигнатурним методом шляхом написання власних скриптів.

Експертні системи використовують експертні знання та досвід для вирішення проблеми. Вони побудовані на основі правил, логічних висловлювань або евристичних алгоритмів, які забезпечують механізми прийняття рішень.

Нечітку логіку може бути застосовано в ситуаціях, коли межі між нормальною та зловмисною поведінкою не чітко визначені або коли мова йде про невизначені чи неточні дані. Вона дозволяє моделювати та обробляти невизначеності, призначаючи ступені приналежності до різних категорій, а не сувору двійкову класифікацію [18-19].

Використання генетичного алгоритму для виявлення зловмисної активності в комп’ютерній мережі передбачає застосування принципів генетичної еволюції для пошуку оптимальних рішень для виявлення зловмисної поведінки. Генетичні алгоритми – це тип техніки оптимізації, натхненний процесом природного відбору. Важливо відзначити, що розробка ефективної відповідної функції, визначення відповідних представлень для рішень і налаштування параметрів алгоритму є вирішальними для успіху використання генетичного алгоритму. Крім того, генетичні алгоритми потребують інтенсивних обчислень, тому вони можуть бути придатними для автономного аналізу або оптимізації окремих компонентів більшої системи виявлення вторгнень. [20-26]

Машинне навчання передбачає самонавчання та розвиток комп'ютерної системи за підготовленими заздалегідь даними. Машина отримує великий набір даних і вчиться розпізнавати з них закономірності та шаблони, які роблять ці дані цінними. Машина аналізує навчальний набір даних, визначає характеристики та зв'язки між ними і використовує цю інформацію для вирішення конкретних завдань. У результаті дослідники прагнуть домогтися від штучного інтелекту можливості шукати відповіді питання і виконувати завдання [27-29].

1.3 Аналіз систем запобігання та виявлення вразливостей та вторгнень

Для забезпечення захисту потрібно використовувати комплексні системи захисту інформації. Вони розробляються та впроваджуються на підставі аналізу можливих загроз та об’єктів захисту [30].

Системи захисту комп’ютерних мереж є важливими для забезпечення безпеки системи та захисту інформації від несанкціонованого доступу (НСД), атак чи інших загроз. До найпоширеніших відносять брандмауер, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) [31]. Слід зазначити, що за несанкціонований доступ прийнято вважати доступ до інформації, який здійснюється з порушенням правил розмежування доступу [32-33].

Брандмауери є важливими компонентами безпеки мережі та відіграють вирішальну роль у захисті комп’ютерних мереж та конфіденційних даних від зловмисних дій. Вони служать першою ланкою захисту від зовнішніх загроз і допомагають запобігти несанкціонованому доступу, мережевим вторгненням і поширенню шкідливих програм. Брандмауер відстежує та контролює вхідний і вихідний мережевий трафік на основі заздалегідь визначених правил безпеки. Основне призначення полягає в застосуванні політики безпеки шляхом дозволу або блокування певних мережевих підключень. Брандмауери можуть бути реалізовані як апаратні пристрої, програмні програми або їх комбінації.

Брандмауер є одним із стандартних засобів мережевої безпеки [29], що дозволяє мінімізувати кількість атак на мережу [34]. Проте порти TCP/53 та UDP/53 ввімкнені, що становить вразливість безпеки DNS-тунелювання [35]. Також вважається, що внутрішні атаки відсутні, що дозволяє підключеним користувачам виконувати зловмисні дії [36]. Брандмауери на основі правил, незважаючи на усі переваги, мають ряд недоліків: наявність зайвих правил, труднощі при перемиканні між правилами, велика кількість правил впливає на швидкість [37]. Отож, для коректної ефективної роботи потрібно мати системного адміністратора мережі, що не доцільно для публічних мереж [38].

Система виявлення вторгнень (IDS) виконує моніторинг комп’ютерної

мережі на наявність зловмисних дій та атак шляхом автоматизації процесів виявлення вторгнень шляхом створення програмних продуктів [39-40]. IDS зазвичай працює шляхом аналізу мережевих пакетів, файлів журналів або системних подій для виявлення шаблонів або аномалій, які можуть вказувати на інцидент безпеки. Він порівнює поведінку з відомими сигнатурами атак або попередньо визначеними правилами, щоб визначити, чи відбулося вторгнення чи порушення. Коли виявляється підозріла активність, IDS генерує попередження або сповіщення, яке можна надіслати системним адміністраторам або центру безпеки для подальшого дослідження та реагування [41]. Зокрема Zeek IDS виявляє різні типи атак, що здійснюються з використанням DNS-трафіку, наприклад Fast flux, DNS-кеш-отруєння та спуфінг, посилення DNS для DDoS-атаки [42].

Є два основних типи IDS:

- Мережевий IDS (NIDS): цей тип IDS відстежує мережевий трафік, аналізуючи пакети, що проходять через мережу. Зазвичай він розгортається в стратегічних точках мережевої інфраструктури для перевірки трафіку та виявлення потенційних атак або порушень політики. NIDS може ідентифікувати різні мережеві атаки, такі як сканування портів, атаки на відмову в обслуговуванні (DoS) або спроби використання вразливостей.
- IDS на основі хоста (HIDS): HIDS інсталюється на окремих хост-системах (серверах або кінцевих точках) і відстежує дії, що відбуваються в цих системах. Він перевіряє системні журнали, цілісність файлів, поведінку користувачів та іншу інформацію про хост, щоб виявити підозрілу або несанкціоновану діяльність. HIDS може забезпечити більш детальну видимість конкретних загроз, пов’язаних із хостом, таких як неавторизований доступ, зараження шкідливим програмним забезпеченням або ненормальна поведінка системи.

Система запобігання вторгненням (IPS) — це пристрій або програмне забезпечення для захисту мережі, яке відстежує мережевий трафік на наявність потенційних загроз безпеці та вживає профілактичних заходів для запобігання або блокування зловмисних дій. Він призначений для доповнення та розширення

можливостей брандмауера. IPS працює, перевіряючи мережеві пакети в режимі реального часу, шукаючи шаблони або сигнатури, які відповідають відомим шаблонам атак або поведінці. Він аналізує як заголовок, так і вміст пакетів, щоб виявити потенційні загрози, такі як зловмисне програмне забезпечення, віруси, хробаки, атаки на відмову в обслуговуванні (DoS) та інші мережеві експлойти. Крім того, IPS також може виявляти та запобігати певним типам атак на прикладному рівні та спробам вторгнення. Коли IPS визначає підозрілий або зловмисний пакет, він може вжити різних дій, щоб зменшити загрозу. Ці дії можуть включати блокування пакета, припинення з’єднання або надсилання сповіщення адміністратору мережі для подальшого дослідження. Деякі просунуті системи IPS можуть навіть автоматично реагувати на загрози, змінюючи правила брандмауера, налаштовуючи засоби контролю доступу до мережі або змінюючи таблиці маршрутизації для захисту мережі. IPS є важливим компонентом багаторівневої стратегії безпеки мережі. Він забезпечує додатковий рівень захисту, крім традиційних брандмауерів і систем виявлення вторгнень (IDS). У той час як IDS в основному зосереджується на виявленні потенційних загроз і попередженні про них, IPS йде ще далі, активно запобігаючи або блокуючи зловмисні дії в режимі реального часу [43,39,38].

1.4 Визначення та класифікація штучних нейронних мереж

Штучна нейронна мережа (ШНМ) – це модель обчислювальної системи, яка імітує певні аспекти функціонування нейронів у мозку людини [44]. Вона призначена для оброблення інформації шляхом взаємодії багатьох простих обчислювальних одиниць, які називаються "нейронами". Нейрони в мережі взаємодіють шляхом передачі сигналів між собою, а це дозволяє мережі "вчитися" з досвіду та розв'язувати завдання, для яких є велика кількість вхідних даних та складні неявно визначені зв'язки. Нейронні мережі можуть використовуватися для різноманітних завдань, таких як класифікація, здійснення прогнозів, ініціалізація образів, обробка природних мов, аналіз даних тощо. Вони стали ключовим

інструментом в галузі машинного навчання та штучного інтелекту, дозволяючи розв'язувати завдання, які раніше вимагали складних програмних алгоритмів або великого обсягу ручної роботи. Структуру ШНМ наведено на рис.1.1.

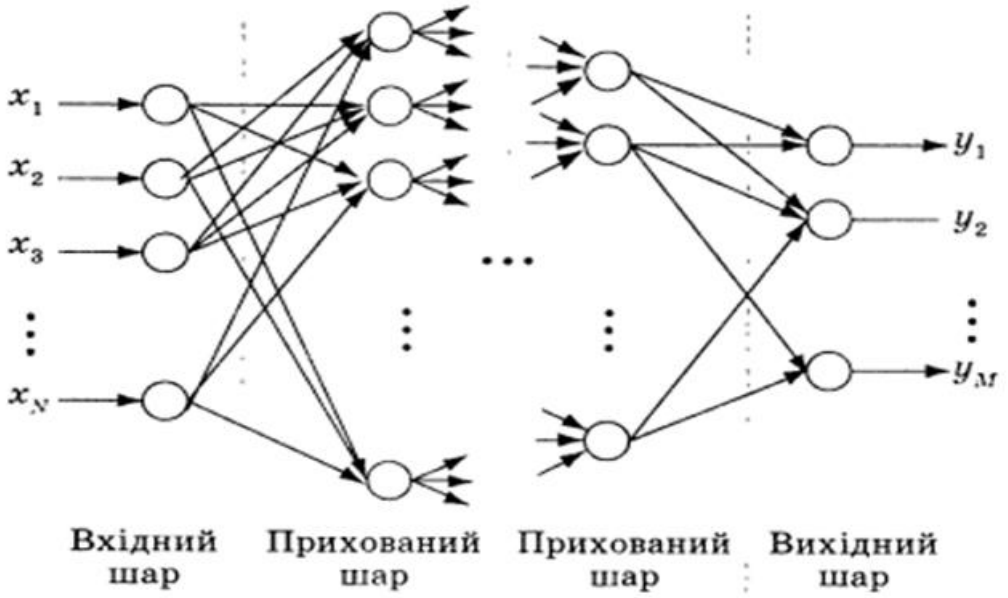

Рисунок 1.1 – Структура штучної нейронної мережі

Нейронна мережа прямого поширення – НМ, де за одним напрямом сигнали передаються від вхідного шару до вихідного шару нейронів через приховані шари, а результат опрацювання сигналу формує вихідний шар.

Одношаровий персептрон (Single-Layer Perceptron) – це найпростіша форма нейронної мережі (рис.1.2), яка має один шар нейронів. Кожен нейрон в цьому шарі приймає вхідні дані, здійснює додавання даних з урахуванням ваг та застосовує активаційну функцію, щоб виробити вихідний сигнал.

Багатошаровий персептрон (Multi-Layer Perceptron) - це форма нейронної мережі, що складається з багатьох шарів нейронів, включаючи вхідний, приховані та вихідний шари. Вхідний шар приймає вхідні дані, які потім поширюються через приховані шари, де вони обробляються та виокремлюються важливі ознаки. Остаточні результати передаються через вихідний шар, який генерує вихідні результати аналізу. Багатошаровий персептрон може вирішувати більш складні

задачі, які не є лінійно роздільними, завдяки нелінійній активаційній функції та можливості виокремлення багатошарової структури даних. Цей тип мережі може використовуватися для навчання на прикладах, надаючи здатність виявляти зв'язки та залежності між даними [44].

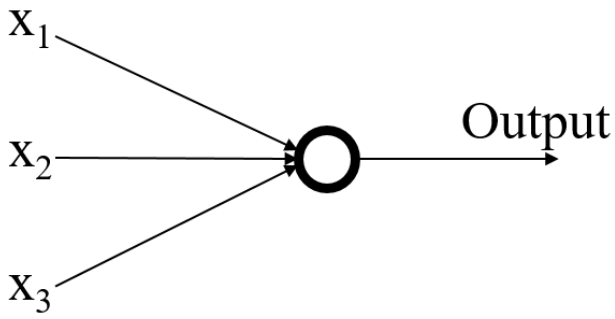

Рисунок 1.2 – Одношаровий персептрон

Етапи НМ прямого поширення в типовій нейронній мережі:

- Вхідний шар отримує вхідні дані, які можуть бути вектором або матрицею, що відображає характеристики прикладу, що обробляється.
- Між вхідним і вихідним шарами може бути один або кілька прихованих шарів. Кожен прихований шар складається з кількох нейронів, також відомих як вузли або одиниці. Нейрони одного шару з’єднані з нейронами наступного шару.
- Зважена сума це дані, що отримуються у результаті того як кожен нейрон у шарі отримує вхідні дані від попереднього шару, помножені на відповідні ваги. Зважені вхідні дані підсумовуються, як правило, разом із зміщенням, щоб обчислити загальний вхід для кожного нейрона.
- Після обчислення зваженої суми застосовується функція активації для введення нелінійності в мережу. Загальні функції активації включають сигмоподібну функцію, ReLU (випрямлену лінійну одиницю) або tanh (гіперболічний тангенс).
- Вихід кожного нейрона в шарі стає входом для нейронів у наступному шарі. Цей процес триває, поки дані не пройдуть через усі шари.
- Останнім шаром є вихідний, який створює передбачуваний вихід або ймовірність класу. Кількість нейронів у вихідному шарі залежить від характеру

проблеми. Наприклад, у задачі двійкової класифікації один нейрон представляє ймовірність належності до одного класу, а доповнення представляє ймовірність належності до іншого класу. Вихідний шар може використовувати різні функції активації залежно від проблеми. Наприклад, для двійкової класифікації сигмоїдна функція зазвичай використовується для стиснення результату між 0 і 1, що представляє ймовірність належності до певного класу. У багатокласовій класифікації функція softmax використовується для перетворення вихідних даних у ймовірності класу, сума яких дорівнює 1.

Завдяки ітерації цих кроків вхідні дані поширюються вперед через нейронну мережу, а остаточний прогноз генерується на вихідному шарі. Потім це передбачення порівнюється з основною міткою істинності, і продуктивність мережі оцінюється за допомогою функції втрат. Втрати використовуються для обчислення градієнтів під час фази зворотного поширення, що потім використовується для оновлення ваг і зміщень у мережі за допомогою алгоритмів оптимізації, таких як градієнтний спад, що дозволяє мережі покращувати свої прогнози з часом.

Нейронна мережа зі зворотним зв’язком (рекурентна нейронна мережа, RNN) — це тип нейронної мережі, яка має з’єднання, які дозволяють інформацію передавати по петлях. На відміну від нейронних мереж прямого зв’язку, які обробляють дані суворо послідовно, рекурентні нейронні мережі можуть включати зворотні зв’язки, які дозволяють їм зберігати інформацію про попередні вхідні дані.

Ключовою особливістю рекурентних нейронних мереж є наявність рекурентних зв’язків, які дозволяють передати вихід нейрона на певному кроці часу як вхідні дані тому ж нейрону або іншим нейронам у мережі на наступному кроці часу. Цей механізм зворотного зв’язку дозволяє мережі підтримувати внутрішню пам’ять або контекст про минулі вхідні дані, з якими вона стикалася [44].

Прямі зворотні зв'язки (Feedforward Connections) - це зв'язки між нейронами, які ведуть від одного шару до наступного і призначені для передачі обчислених результатів. У ШНМ із прямими зворотними зв’язками (рис.1.3) нейрони можуть мати зв'язки між нейронами різних шарів та нейронами одного шару. Тобто на вхід

певного нейрона може подаватися його вихідний сигнал. Це дає змогу отримати граничний активаційний стан оскільки нейрон підсилює чи сигнал перетворений його активаційною функцією.

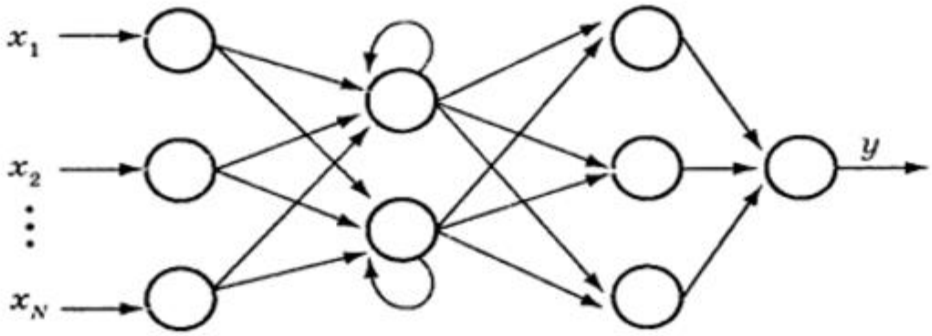

Рисунок 1.3 – Штучна нейронна мережа із прямими зворотними зв’язками

Нейронні мережі з непрямими зворотніми зв'язками - це тип багатошарових нейронних мереж, де зворотній зв'язок не обмежується лише між сусідніми шарами, а може перетнути декілька шарів в мережі. Цей вид нейронних мереж є також відомим як рекурентні нейронні мережі (Recurrent Neural Networks, RNN). В багатошаровій нейронній мережі з непрямими зворотніми зв'язками вихідний сигнал нейронів з одного шару може бути переданий на вхідні нейрони не тільки наступного шару, але і навіть більш пізніх шарів чи навіть на нейрони з тих самих шарів, з деяким затримкою. Це дозволяє мережі здійснювати більш глибокий аналіз та враховувати динаміку даних у часі (рис.1.4).

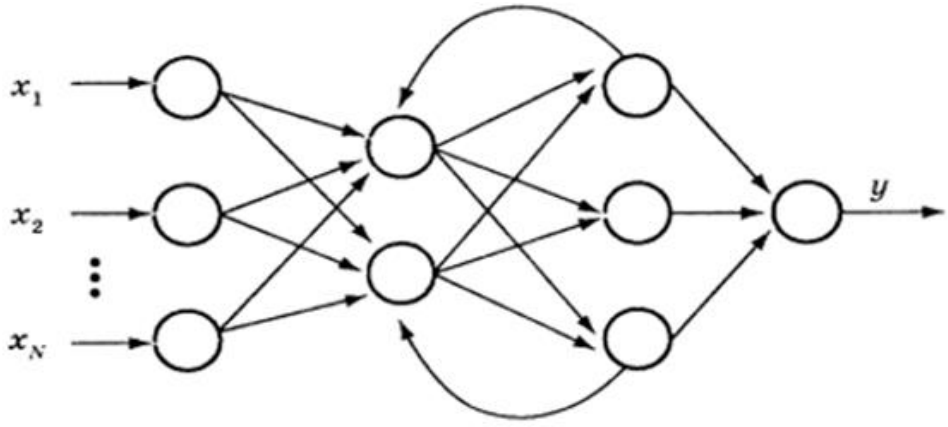

Рисунок 1.4 – Штучна нейронна мережа із непрямими зворотними зв’язками

Обчислювальний процес у рекурентній нейронній мережі включає наступні етапи:

- На кожному кроці часу t мережа отримує вхідний вектор або послідовність векторів, які можуть представляти, наприклад, елементи часового ряду або слова в реченні.
- Вхідні дані на кожному кроці часу поєднуються з внутрішнім станом мережі з попереднього кроку часу для обчислення активації нейронів у мережі.
- Повторювані з’єднання - активація нейронів на поточному кроці часу потім повертається в мережу через повторювані з’єднання, дозволяючи інформації перетікати від поточного кроку до майбутніх кроків.
- Вихід рекурентної нейронної мережі може бути отриманий на кожному кроці часу або лише на останньому кроці часу, залежно від конкретного завдання.

Повторювані нейронні мережі особливо корисні для завдань, які включають послідовні дані, такі як обробка природної мови, розпізнавання мовлення та прогнозування часових рядів. Захоплюючи тимчасові залежності в даних, RNN можуть моделювати контекст і довгострокові залежності ефективніше, ніж мережі прямого зв’язку.

ШНМ з латеральними зв'язками (рис.1.5), відомі також як бічні зв'язки, це варіант нейронної мережі, де існують зв'язки між нейронами в тому ж самому шарі.

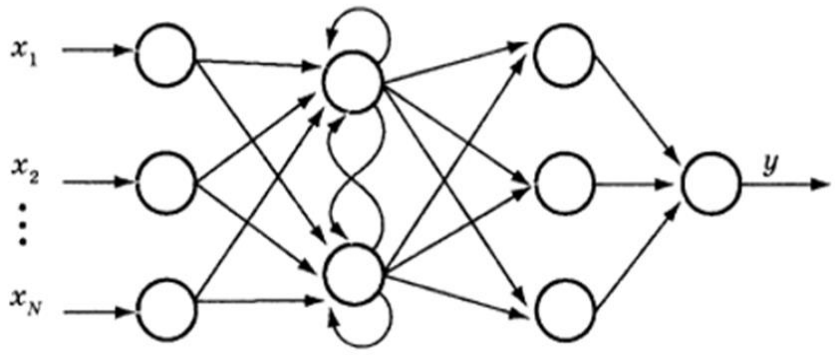

Рисунок 1.5 – Штучна нейронна мережа із латеральними зв’язками

Тобто, нейрони з одного шару можуть спілкуватися і взаємодіяти з нейронами з того ж самого шару. Це відрізняється від типових багатошарових

нейронних мереж, де зв'язки лише ведуть від одного шару до іншого. Латеральні зв'язки можуть мати різні форми та функції, включаючи вплив на активаційну функцію нейронів, передачу інформації між нейронами та підсилення зв'язків між нейронами.

Глибинне навчання – це поєднання методів, що використовують багатошарові штучні НМ з метою гарантування максимальної точності. До глибинного навчання можна віднести згорткові НМ, мережі довгої короткочасної пам’яті, рекурсивні НМ, мережі з пам’яттю та інші.

1.5 Навчання нейронної мережі

Навчання з вчителем (supervised learning, контрольоване) – це тип навчання НМ, котрий визначає правила за якими здійснюється зв’язок між вхідними даними та результатом аналізуючи навчальні набори даних із мітками. [45]

Існує два типи навчання:

- регресія - намагається передбачити результат;
- класифікація - визначає приналежність набору даних до тієї чи іншої категорії.

Контрольоване навчання дозволяє виявляти інформацію, щоб краще зрозуміти взаємозв’язки та закономірності в позначеному наборі навчальних даних. Недоліком такого навчання є необхідність використовувати різноманітні навчальні дані для ефективнішої роботи надалі.

Навчання без вчителя (unsupervised learning, неконтрольоване) – тип навчання НМ, для роботи якого не залучено навчальні набори даних та користувачі не контролюють модель.

До переваг неконтрольованого навчання можна віднести застосування для більш складних завдань порівняно з контрольованим навчанням, легше отримати навчальні дані. Проте результат алгоритм навчання може видавати менш точним.

Навчання з підкріпленням (reinforcement learning) – тип навчання НМ під час якого використовується метод проб і помилок, не потрібно статичні набори даних, а працює в динамічному середовищі на основі зібраного досвіду.

1.6 Система доменних імен

Система доменних імен (Domain Name System, DNS) - це розподілена ієрархічна система, яка використовується для перетворення зрозумілих для людини доменних імен (наприклад, www.example.com) на IP-адреси, які комп'ютери та мережеві пристрої можуть розуміти (наприклад, 75.88.12.10).

Для DNS запитів та відповідей на них застосовується 53 UDP-порт. TCP-порт призначений для обробки повідомлень при умові, що відповідь перевищує 512 байтів.

Останні дослідження загроз мережевої безпеки виявили, що понад 90% вразливостей шкідливим програмним забезпеченням використовують DNS для здійснення мережевих атак.

1.7 Засоби для аналізу DNS-трафіку

Deep packet inspection (DPI) - це метод перевірки вмісту пакетів даних, коли вони проходять через контрольну точку в мережі для виявлення та запобігання кібератакам, моніторингу моделей трафіку, боротьби зі зловмисним програмним забезпеченням, оптимізації серверів і аналізу поведінки користувачів [46].

DPI аналізує вміст пакетів даних за допомогою спеціальних правил, попередньо запрограмованих користувачем, адміністратором або постачальником послуг Інтернету. Потім вирішує, як впоратися з виявленими загрозами. DPI не тільки може визначити наявність загроз, але, використовуючи вміст пакета та його заголовок, він також може визначити, звідки вони надійшли. Таким чином DPI може точно визначити програму чи службу, яка запустила загрозу.

DPI може надати адміністраторам видимість усієї мережі, аналізуючи активність за допомогою евристичних методів , щоб виявити щось аномальне.

Недоліком використання DPI-системи є зіставлення сигнатур, оскільки ефективність забезпечується лише при регулярних оновлення баз. Крім того, цей метод працює лише проти відомих загроз або атак. Оскільки нові загрози виявляються щодня, а оновлення сигнатур може відбуватися періодично від одного разу на добу до одного разу на місяць у залежності від розробників.

Найпопулярнішими розробниками DPI-систем є Allot Communications, Procera Networks, Cisco, Sandvine, а вартість сягає від кількох тисяч до мільйонів доларів США. Що теж є суттєвим недоліком для використання у мережах не корпоративного рівня.

Пасивний моніторинг трафіку DNS — це метод аналізу мережі, який передбачає збір і аналіз даних трафіку DNS без активної взаємодії з DNS-серверами чи зміни запитів і відповідей DNS. Це ненав’язливий спосіб спостерігати за діяльністю DNS, що відбувається в мережі, і отримати уявлення про неї.

Інструменти чи системи пасивного моніторингу DNS фіксують трафік DNS під час проходження мережею. Після перехоплення пакетів DNS відбувається аналіз на рівні пакетів, щоб отримати відповідну інформацію. Цей аналіз може виявити різні аспекти трафіку DNS, такі як типи запитів, відповідей, IP-адреси, та інші параметри.

Пасивний моніторинг DNS є цінним для керування мережею, безпеки та усунення несправностей. Це може допомогти організаціям виявляти загрози, пов’язані з DNS, і реагувати на них, оптимізувати продуктивність DNS і отримати уявлення про шаблони використання мережі. Крім того, він може бути важливим інструментом для забезпечення відповідності та аудиту, оскільки забезпечує запис дій DNS у мережі , що дозволяє зберігати і аналізувати історію мережевої активності. Пасивний моніторинг DNS стає невід'ємною частиною комплексних систем мережевого управління та забезпечення безпеки, і він дозволяє ефективно виявляти, аналізувати і реагувати на події, пов'язані з DNS, що стає особливо важливим у світлі зростаючих загроз та вимог до мережевої безпеки.

Незважаючи на переваги, пасивний моніторинг має свої недоліки. Зокрема не відстежується трафік DNS у зашифрованих тунелях або трафік у підмережах, які не контролюються. Ця обмежена видимість може призвести до сліпих зон. Дана система не може блокувати шкідливі домени або змінювати поведінку DNS у реальному часі. А зашифрований DNS-трафік ускладнює аналіз і отримання інформації про діяльність DNS. Також захоплення та зберігання даних трафіку DNS може потребувати додаткових ресурсів. Щоб отримати корисну інформацію з даних, часто потрібні складні інструменти та досвід аналізу DNS. У деяких випадках розгортання датчиків або пристроїв пасивного моніторингу може викликати навантаження на мережу, що впливає на загальну продуктивність мережі, що особливо актуально в умовах інтенсивного трафіку.

Активне DNS-зондування, також відоме як DNS-розвідка або DNS-зондування, — це метод сканування мережі, який використовується для збору інформації про DNS і виявлення потенційних вразливостей або неправильних конфігурацій. На відміну від пасивного моніторингу DNS, який спостерігає за DNS-трафіком без активної взаємодії з DNS-серверами, активне DNS-зондування передбачає надсилання DNS-запитів на DNS-сервери для отримання відповідей і збору даних. Ця техніка зазвичай використовується для різних цілей, таких як адміністрування мережі, усунення несправностей і оцінка безпеки, але її також можуть використовувати зловмисники для розвідки та потенційних атак.

Суб’єкт, який проводить активне DNS-зондування, надсилає DNS-запити до певних DNS-серверів або зон DNS. Активне зондування DNS часто використовується як частина оцінки безпеки та тестування на проникнення для виявлення потенційних слабких місць в інфраструктурі DNS організації. Фахівці з безпеки можуть використовувати зібрану інформацію, щоб оцінити вразливість організації до атак, пов’язаних із DNS, таких як отруєння кешу DNS, атаки посилення DNS або викрадення домену.

Варто зазначити, що активне DNS-зондування може завдавати шкоди. Наприклад, підвищений трафік може перевантажити DNS-сервери або порушити їх нормальну роботу. Відповіді DNS можуть відрізнятися залежно від умов мережі,

конфігурації DNS-сервера та інших факторів. А помилки тлумачення або неповні дані можуть призвести до неправильних оцінок.

1.8 Постановка задачі

Мета кваліфікаційної роботи магістра полягає у розробці методу виявлення порушника в публічній мережі на основі аналізу вихідних DNS запитів нейронною мережею.

Для досягнення поставленої мети потрібно розв’язати наступні задачі дослідження:

- дослідити наявні методи та засоби аналізу мережевого трафіку, зокрема DNS;
- виконати аналіз існуючих нейронних мереж, в тому числі нейромереж глибокого навчання, для дослідження ефективності використання нейронних мереж різних типів;
- сформувати модель DNS-запитів;
- оцінити ефективність нейромереж різних типів для виявлення зловмисного трафіку у публічній мережі шляхом аналізу вихідних DNS запитів;
- розробити метод аналізу нейронною мережею вихідних DNS запитів із публічної мережі, що забезпечить кращу ефективність у порівнянні із наявними методами.

2 РОЗРОБКА МОДЕЛІ МЕРЕЖІ ТА ВИБІР НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ПОРУШНИКА В ПУБЛІЧНІЙ МЕРЕЖІ НА ОСНОВІ АНАЛІЗУ ВИХІДНИХ DNS ЗАПИТІВ

2.1 Модель DNS-запитів

Для того, щоб користувач зміг переглянути дані веб-сайту чи інформацію в додатку він має звернутися до ресурсу за доменним іменем. Послідовність дій реалізується на програмно-апаратному рівні наступним чином (рис.2.1):

- Користувач надсилає звертання до ресурсу.
- Дане звертання формує DNS-запит.
- DNS-запит через маршрутизатор отримує доступ до DNS-сервера. Зазвичай, маршрутизатор відіграє роль першого (найближчого) DNS-сервера.
- DNS-сервер перенаправляє запит до запитуваного ресурсу за допомогою IP-адреси.
- Після чого відповідь на запит повертається до користувача.

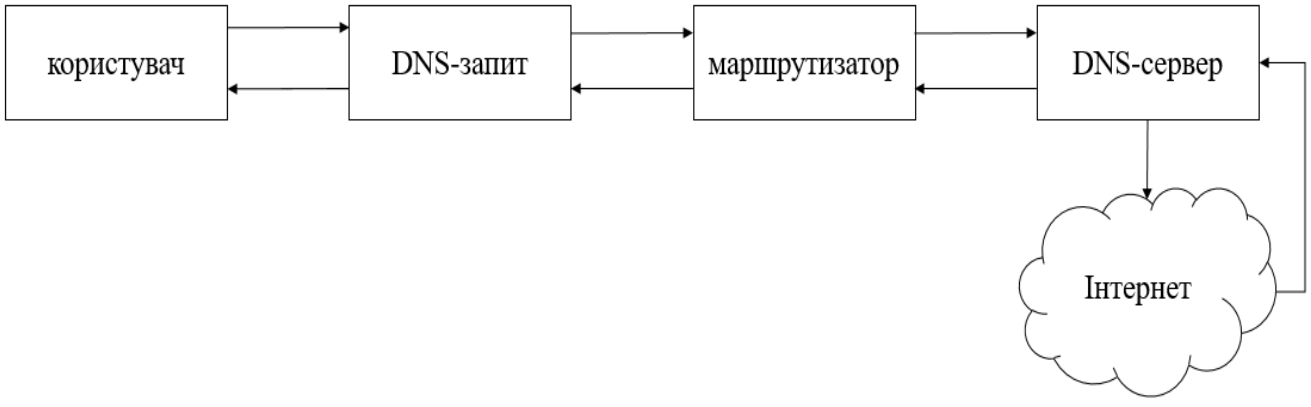

Рисунок 2.1 – Схема надсилання DNS-запитів та одержання результатів

З метою аналізу вихідного DNS-трафіку до описаної схеми мережі (рис.2.1) слід додати систему аналізу трафіку. Маршрутизатор має можливість надсилати повідомлення на кілька пристроїв одночасно. Саме тому систему доцільно встановити після маршрутизатора, як показано на рисунку 2.2.

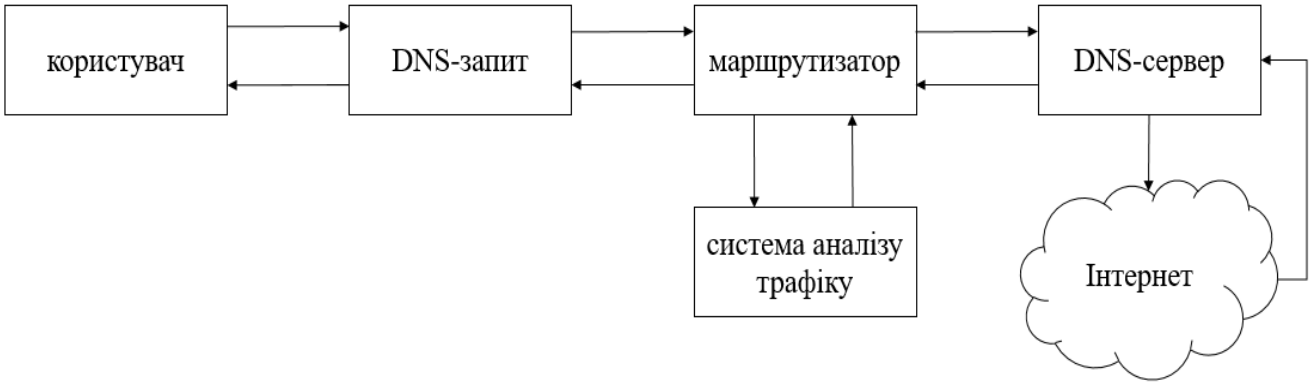

Рисунок 2.2 – Схема надсилання DNS-запитів із системою аналізу DNS-трафіку

DNS-повідомлення складається з 5 полів, формат якого зображено на рисунку 2.3.

16		21					28	32
Ідентифікатор	Q	Запит	A	T	R	V	B	Rcode
Лічильник запитів	Лічильник відповідей							
Лічильник Authority	Лічильник доповнень							

Рисунок 2.3 – Формат повідомлень DNS

Опис параметрів, що містяться у повідомленні наступний:

Ідентифікатор - 16-бітове поле для позначення відповідності між запитами і відгуками;

Q – query, 1-бітовий прапор запиту;

Запит – 4-бітовий опис типу повідомлення, де 0 – стандартний запит, 1 – зворотній запит, 2 – запит стану сервера;

A – authoritative answer, 1-бітовий прапорець, що показує відгук від сервера доменних імен;

T – truncation, 1-бітовий прапорець вказує на відхилення повідомлення;

R – 1-бітовий прапорець, який встановлюється щоб дозволити запит рекурсивним шляхом;

V – 1-бітовий прапорець підтримки рекурсивного сервісу;

B – зарезервоване 3-бітне поле;

Rcode – 4-бітове поле для позначення стану запиту;

Лічильник запитів – містить число записів у розділі запитів;

Лічильник відповідей – містить число записів про ресурси в розділі відповідей;

Лічильник Authority – визначає число записів про ресурси сервера імен у розділі authority (повноваження).

Лічильник доповнень - изначає число записів про ресурси сервера імен у додатковому розділі.

Протокол DNS під час роботи використовує 53 порт та протоколи TCP/UDP.

2.2 Несанкціонований доступ із використанням DNS запитів

2.2.1 DNS-флуд

Існує кілька способів атаки на DNS. Перший тип – створення обманного DNS-сервера внаслідок перехоплення запиту. Механізм цієї атаки дуже простий. Хакер – атакуючий, чекає на DNS-запит від комп'ютера жертви. Після того, як атакуючий отримав запит, він витягає з перехопленого пакету IP-адресу запитаного хоста. Потім генерується пакет, у якому порушник є цільовим DNS-сервером. Сама генерація пакету у відповідь така проста: хакер в помилковій відповіді жертві в полі IP DNS-сервера прописує свій IP. Тепер комп'ютер жертви приймає атакуючого за реальний DNS. Коли клієнт відправляє черговий пакет, атакуючий змінює IP-адресу відправника і пересилає далі на DNS. В результаті, справжній DNS-сервер вважає, що запити надсилає хакер, а не жертва. Таким чином, атакуючий стає посередником між клієнтом та реальним DNS-сервером. Далі хакер може виправляти запити жертви на власний розсуд і надсилати їх на реальний DNS. Але перехопити запит можна тільки якщо атакуюча машина знаходиться на шляху основного трафіку або в сегменті DNS-сервера [47].

Використовуючи простий DNS-флуд, порушник відправляє множинні DNS-запити на сервер DNS, переповнюючи сервер запитами і споживаючи його ресурси. Такий метод атаки є привабливим, оскільки він простий у виконанні і дозволяє приховати особистість порушників.

Порушник генерує DNS-пакети, які надсилаються за допомогою UDP-протоколу на DNS-сервер. Стандартний ПК може згенерувати 1000 DNS-запитів за секунду, тоді як звичайний DNS-сервер може обробити лише 10000 DNS-запитів за секунду. Іншими словами, для того, щоб вивести з ладу DNS-сервер, потрібно всього 10 комп'ютерів. Оскільки DNS-сервери переважно використовують UDP-протокол, порушникам не потрібно встановлювати з'єднання, і вони можуть змінити IP-адресу джерела та замаскуватися. Ця властивість також на руку порушникам – атаку, що виходить від безлічі змінених IP-адрес джерела, важче відбити, ніж ту, яка виходить від обмеженого списку IP-адрес.

2.2.2 Атака за допомогою відображених DNS-запитів

Якщо відсутній доступ до клієнтського трафіку, даний метод атаки застосовується віддалено. Для генерації хибної відповіді необхідно виконання кількох пунктів. По-перше, збіг IP-адреси відправника відповіді з адресою DNS-сервера. Потім, збіг імен, що містяться в DNS-відповіді та запиті. Крім того, DNS-відповідь має посилатися на той же порт, з якого було надіслано запит. Ну і, нарешті, у пакеті DNS-відповіді поле ID має збігатися з ID у запиті.

Завдяки асиметричному характеру атака за допомогою відображених DNS-запитів дозволяє створити ефект переповнення, маючи в розпорядженні обмежені ресурси.

Порушник відправляє DNS-запит на один або кілька сторонніх серверів DNS, які не є реальними об'єктами нападу. Порушники змінюють IP-адресу джерела DNS-запиту на IP-адресу цільового сервера (об'єкта нападу), тоді відповідь сторонніх серверів буде відправлено на сервер, який є метою нападу.

У процесі атаки використовується ефект посилення, у якому відповідь DNS-запит в 3-10 разів більше, ніж сам DNS-запит. Іншими словами, на атакований сервер надходить набагато більше трафіку в порівнянні з невеликою кількістю

запитів, згенерованих порушником. Атака за допомогою відображених запитів демонструє, що організації не потрібно володіти DNS-сервером, щоб стати об'єктом DNS-атаки, оскільки метою атаки є виведення з ладу Інтернет-з'єднання або міжмережевого екрану.

Атаки, що виконуються за допомогою відображених DNS-запитів, можуть включати декілька рівнів посилення:

- Природний – DNS-пакети, що надсилаються у відповідь на запит, у кілька разів більші за пакети, які надсилаються при запиті. Таким чином, навіть найбільша базова атака може отримати 3-4 кратне посилення.
- Вибірковий – відповіді на DNS-запити мають різний розмір: у відповідь на деякі DNS-запити надсилається коротка відповідь, у відповідь на інші відповіді набагато більше. Винахідливий порушник може спочатку визначити, які доменні імена у відповіді сервера мають більший розмір. Надсилаючи запити лише для таких доменних імен, порушник може досягати 10-кратного посилення.
- Настроєний вручну – на високому рівні порушники можуть розробити певні домени, для надсилання імен яких потрібні пакети величезних розмірів. Надсилаючи запити лише на такі спеціально створені доменні імена, порушник може досягати 100-кратного посилення.

Рівень анонімності збільшується разом з розміром атаки. Крім зміни SRC IP (як при простому DNS-флуді), атака сама по собі проводиться не безпосередньо - запити на сервер, що атакується, відправляються стороннім сервером.

2.2.3 Атака за допомогою рекурсивних DNS-запитів

Атака за допомогою рекурсивних запитів є найбільш складним та асиметричним методом атаки на DNS-сервер, для її організації потрібні мінімальні обчислювальні ресурси, а результат призводить до інтенсивного споживання ресурсів DNS-сервера, на який нападають.

За такої атаки використовуються особливості роботи рекурсивних DNS-запитів. У рекурсивних DNS-запитах, коли DNS-клієнт робить запит з ім'ям, яке відсутнє в кеш-пам'яті DNS-сервера, сервер відправляє повторювані запити іншим DNS-серверам доти, поки потрібний відповідь не буде відправлений клієнту.

Скориставшись особливостями цього процесу, злодій відправляє рекурсивні запити з використанням фальшивих імен, які, як він знає, не існує в кеш-пам'яті сервера. Щоб дозволити такі запити, DNS-сервер повинен обробити кожний запис, тимчасово зберігаючи його, і надіслати запит іншому DNS-серверу, а потім дочекатися відповіді. Інакше висловлюючись, споживається дедалі більше обчислювальних ресурсів (процесора, пам'яті і пропускну здатність), доки ресурси не закінчуються.

Асиметричний характер рекурсивної атаки та низька швидкість ускладнюють боротьбу з такими атаками. Рекурсивна атака може бути пропущена як системами захисту, так і людьми, які зосереджені на виявленні атак з великим обсягом. Атака типу Garbage DNS

Як має на увазі її назву, така атака переповнює DNS-сервер «сміттєвим» трафіком, відправляючи пакети даних великого розміру (1500 байт або більше) на його UDP-порт 53. Концепція такої атаки полягає в тому, щоб переповнити мережевий канал пакетами даних великого розміру. Зловмисники можуть генерувати потоки «сміттєвих» пакетів та за допомогою інших протоколів (UDP-порт 80 також часто використовується); але при використанні інших протоколів об'єкт може зупинити атаку, заблокувавши порт на рівні ISP без наслідків. Протокол, для якого такий захист недоступний, є протокол DNS, оскільки більшість організацій ніколи не заборонить цей порт.

2.3 Застосування згорткової нейронної мережі

Згорткова нейронна мережа (CNN) використовується для різних завдань. Проте найкраще проявили себе щодо виявлення об’єктів, класифікації та сегментації даних. Зокрема, у статті [48] запропоновано використовувати згорткові нейронні мережі для виявлення атак ботнетів. В [49] моделі CNN застосовуються для багатокласової системи класифікації з метою виявлення аномалій для мереж IoT. Дослідження щодо ефективності використання даних мереж для класифікації атак та виявлення аномальної поведінки наведено в [50]. Завдяки здібності

автоматично вивчати складні моделі та представляти необроблені дані [51], нейронна мережа може виявляти нові та складні атаки [52]. Також CNN здатна адаптувати набори даних під вирішення конкретних проблем [53] чи комбінувати з іншими методами [54]. Хоча нейронна мережа має свої недоліки, наприклад вона працює з групами подій фіксованого розміру [55].

CNN складається з кількох шарів згортки та об'єднання, а також може включати повнозв'язні шари (Fully Connected Layer, FC). Шари об'єднання зменшують розмірність даних, беручи невеликі блоки з виходу згорткових шарів і створюючи єдине вихідне значення для кожного блоку.

Початкові згорткові шари (Convolutional Layers) CNN використовують згорткові фільтри для виділення простих ознак. Згорткові операції дозволяють мережі автоматично визначати низько рівневі ознаки. Після згорткових шарів можуть бути додані пулінгові шари (Pooling Layers), які підсилюють виділені ознаки. Це допомагає знизити кількість параметрів і обчислень в мережі. Після згорткових і пулінгових шарів можуть бути додані повністю підключені шари (Fully Connected Layers), які призначені для обробки інформації на вищому шарі і генерації кінцевого результату. Вони можуть виконувати класифікацію, регресію або інші завдання в залежності від задачі. Завдяки такій ієрархічній архітектурі CNN можуть автоматично витягувати характеристики із даних на різних шарах абстракції, від простих ознак до складних функцій. Ця спроможність робить їх дуже ефективними для розпізнавання образів чи класифікації даних.

Під час навчання CNN вчиться пов'язувати отримані функції з правильними мітками через процес зворотного поширення та оптимізації. Після того, як CNN буде навчено, його можна використовувати для прогнозування нових даних, передаючи через мережу та вибираючи мітку з найвищою прогнозованою ймовірністю.

На рисунку 2.4 представлено загальну схему CNN, яка використовується для класифікації даних та складається з наступних шарів:

- Згортковий шар виконує операцію згортки на вхідних даних з набором доступних для навчання фільтрів. Фільтри — це невеликі матриці, які зсуваються

по усіх даних. На кожному кроці обчислюється скалярний добуток між фільтром і поточною областю вхідних даних і результат записується на відповідну позицію у вихідному шарі (називається картою функцій). Ця операція повторюється для кожного фільтра, що дозволяє визначити різні параметри або ознаки вхідних даних. В результаті отримується набір карт функцій, які представляють різні аспекти або характеристики вхідних даних. Ці карти функцій потім можуть бути передані наступним шарам мережі для подальшого аналізу та обробки. Згорткові шари є ключовими для ефективного витягування ознак.

- Шар об’єднання використовується для зменшення просторових розмірів карт об’єктів, створених згортковим шаром. Він працює з кожною картою функцій незалежно та зменшує її дискретизацію, беручи максимальне або середнє значення областей, що не перекриваються. Об'єднання допомагає зменшити кількість нейронів у подальших шарах мережі, тобто розмір кожної карти функцій зменшується, але важливі характеристики все ще зберігаються. Зменшення кількості нейронів після об'єднання допомагає зменшити обчислювальну складність мережі, що робить її більш ефективною для навчання та використання. Операція об'єднання може робити мережу більш стійкою до малих зміщень або змін у вхідних даних, оскільки вона об'єднує інформацію з більш широких областей. Два найпоширеніших типи об'єднання це максимальне об'єднання (Max Pooling), де обирається максимальне значення з області, і середнє об'єднання (Average Pooling), де обчислюється середнє значення. Операція об'єднання є важливою частиною архітектури CNN, оскільки вона допомагає знизити обсяги даних і покращити ефективність мережі.

- Шар активації вводить нелінійність у мережу шляхом застосування нелінійної функції активації до вихідних даних з попереднього шару. Основна функція активації полягає в тому, щоб додати нелінійний ефект до виходів нейронів. Це дозволяє нейронній мережі навчатися і виражати більш складні функції, а не обмежуватися лінійними перетвореннями. Без нелінійності мережа була б обмежена до лінійних операцій, і це суттєво обмежило б її здатність до

вирішення складних завдань. Найпоширеніші функції активації включають в себе ReLU, Sigmoid та Tanh.

- Шар нормалізації партії нормалізує вихід попереднього шару шляхом віднімання середнього значення та ділення на стандартне відхилення партії. Це допомагає зменшити внутрішній коваріативний зсув у мережі, що виникає під час навчання, коли розподіл входів до шару змінюється з кроку на крок. Внутрішній коваріативний зсув може сповільнювати навчання, тому шар нормалізації допомагає стабілізувати процес навчання, що: дозволяє використовувати більші швидкості навчання та отримувати кращі результати; зменшувати чутливість мережі до вибору початкових значень ваг, що полегшує навчання; допомагає уникнути перенавчання в мережах.
- На шарі вилучення випадковим чином вимикали певний відсоток нейронів на попередньому шарі та вони не брали участь у обчисленнях та передачі сигналу в мережі на цьому конкретному пакеті даних. Це допомагає змусити мережу вивчати більш надійні та роботоздатні функції, оскільки вона не може надмірно покладатися на певні нейрони під час навчання. Шар вилучення може бути застосований до попередніх шарів перед повністю підключеними шарами або на шарі вихідних шарів, в залежності від архітектури мережі і завдання.
- Повністю підключений шар з'єднує кожен нейрон (вузол) попереднього шару з кожним нейроном поточного шару. Це означає, що кожен вхідний сигнал впливає на кожен нейрон в цьому шарі. Зазвичай цей шар розташований в кінці мережі і використовується для вирішення конкретного завдання, такого як класифікація, регресія, або інші види обробки даних. Повністю підключені шари мають багато ваг, оскільки кожен з'єднується з кожним нейроном попереднього шару. Це може призводити до великої кількості параметрів, що потрібно навчити. Тому важливо використовувати різні техніки регуляризації.

Функції активації (Activ_Funcs) є важливим компонентом CNN, який вносить нелінійність у модель. Ця нелінійність має вирішальне значення, оскільки багато явищ реального світу демонструють складну, нелінійну поведінку, і модель, яка використовує лише лінійні операції, не зможе точно відобразити ці явища. Таким

чином, функція активації допомагає зробити CNN більш виразними та здатними моделювати ширший діапазон функцій.

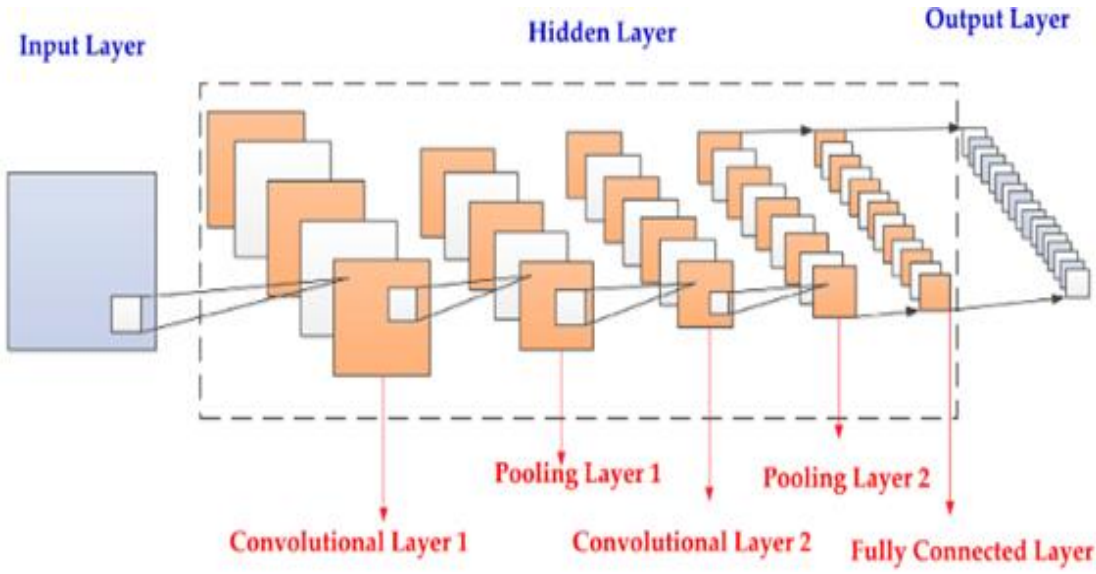

Рисунок 2.4 – Загальна схема згорткової нейронної мережі

Зазвичай використовувані функції активації включають випрямлену лінійну одиницю (ReLU), сигмоподібну функцію (Sigmoid) та функцію гіперболічного тангенса (tanh). ReLU (рис.2.5) є найбільш широко використовуваною функцією у сучасних CNN через її простоту та ефективність у зменшенні проблеми зникнення градієнта під час навчання.

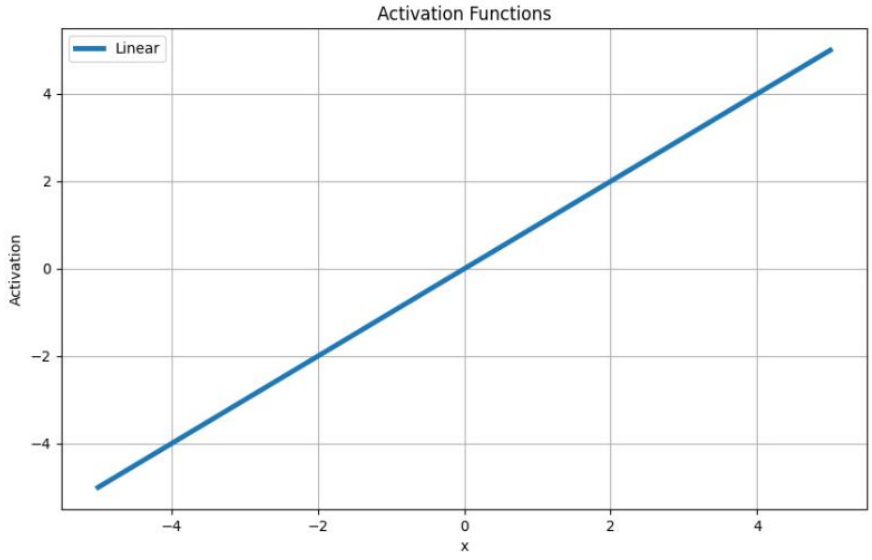

Рисунок 2.5 – Лінійна функція активації

Математично функція активації ReLU визначається як:

$$f(x) = \max(0, x), \tag{2.1}$$

де *x* - вхід до нейрона.

Ця функція повертає *x* якщо він більший або рівний нулю та 0 в іншому випадку, фактично «вимикаючи» будь-які від'ємні значення та залишаючи додатні значення незмінними. Ця проста нелінійна функція дозволяє краще вивчати складні функції в CNN і допомагає запобігти насиченню нейронів під час навчання. ReLU допомагає уникнути проблеми зникнення градієнта, яка може виникнути при використанні інших функцій активації, таких як сигмоїд або тангенс гіперболічний.

Сигмоїдна функція визначається як:

$$f(x) = \frac{1}{1+e^{-x}}, \tag{2.2}$$

де *x* - вхід до нейрона.

Сигмоїдна функція (рис.2.6) має характерну S-подібну форму та відображає будь-яке дійсне число на значення від 0 до 1, що робить її гарним вибором для задач двійкової класифікації.

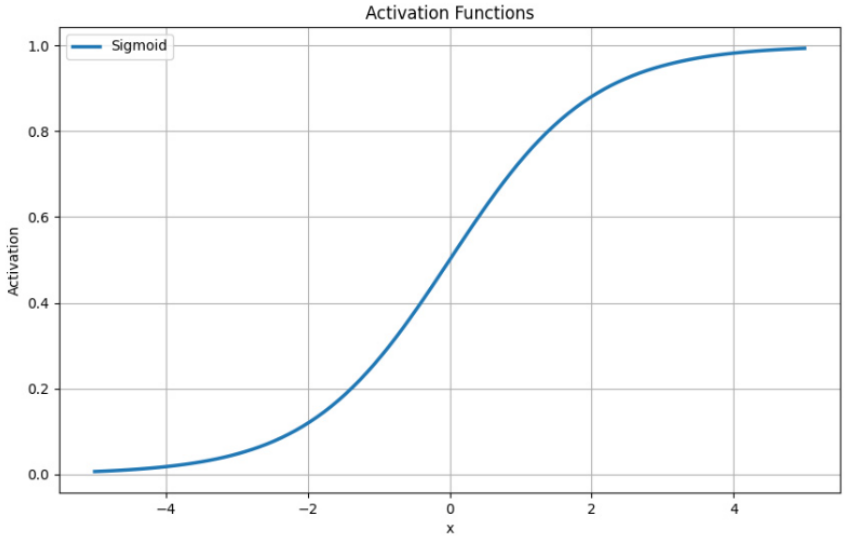

Рисунок 2.6 – Сигмоїдна функція активації

Проблема сигмоїдної функції виникає у глибоких нейронних мережах, і вона відома як "проблема зникнення градієнта". Сигмоїдна функція насичується при великих або малих вхідних значеннях, і це призводить до дуже малих похідних. Похідні, які дуже близькі до нуля, можуть сповільнювати процес навчання глибоких мереж, оскільки ваги не оновлюються належним чином під час зворотного поширення.

Функція гіперболічного тангенса визначається як:

$$tanh(x) = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}}, \tag{2.3}$$

де x - вхід до нейрона.

Оскільки графік поведінки тангенса схожий на сигмоїду, то його можна представити наступним чином:

$$tanh(x) = 2 * sigmoid(2x) - 1, \tag{2.4}$$

де x - вхід до нейрона.

Функція гіперболічного тангенса (рис.2.7) подібна до сигмоїдної функції в тому сенсі, що вона є нелінійною та приймає значення у діапазоні від -1 до 1.

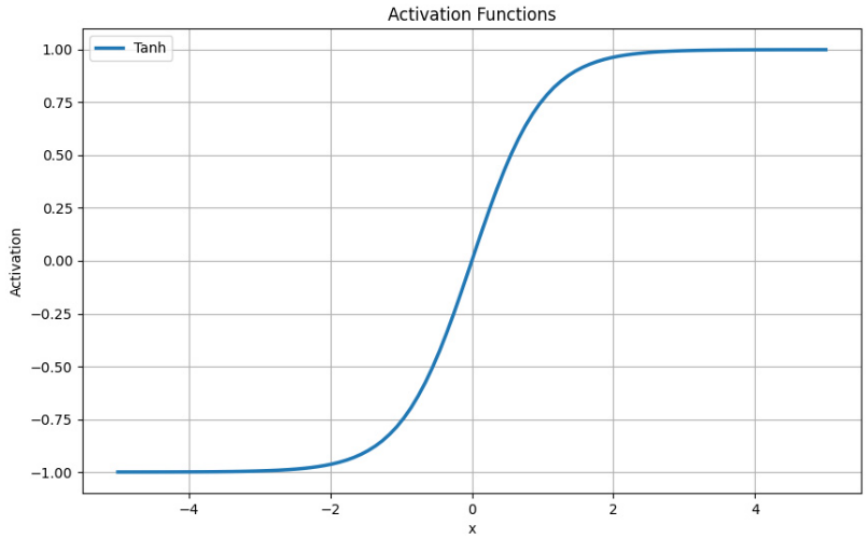

Рисунок 2.7 – Функція гіперболічного тангенса

Функція може приймати великі позитивні та негативні значення, але обмежена до діапазону від -1 до 1. Функція гіперболічного тангенса може страждати від проблеми зникнення градієнта, особливо при великих вхідних значеннях, і це може уповільнити навчання глибоких нейронних мереж.

Проте tanh має перевагу над сигмоїдною функцією в тому, що вона є центрованою навколо нуля, тобто tanh(0)=0, що може допомагати уникнути проблеми з центрування в градієнтах. Зокрема, tanh може бути корисною для завдань, де нуль є значущим значенням (наприклад, у випадках, коли дані мають нульове середнє значення).

На рисунку 2.8 зображено алгоритм навчання CNN, що використовується для аналізу вихідного DNS-трафіку.

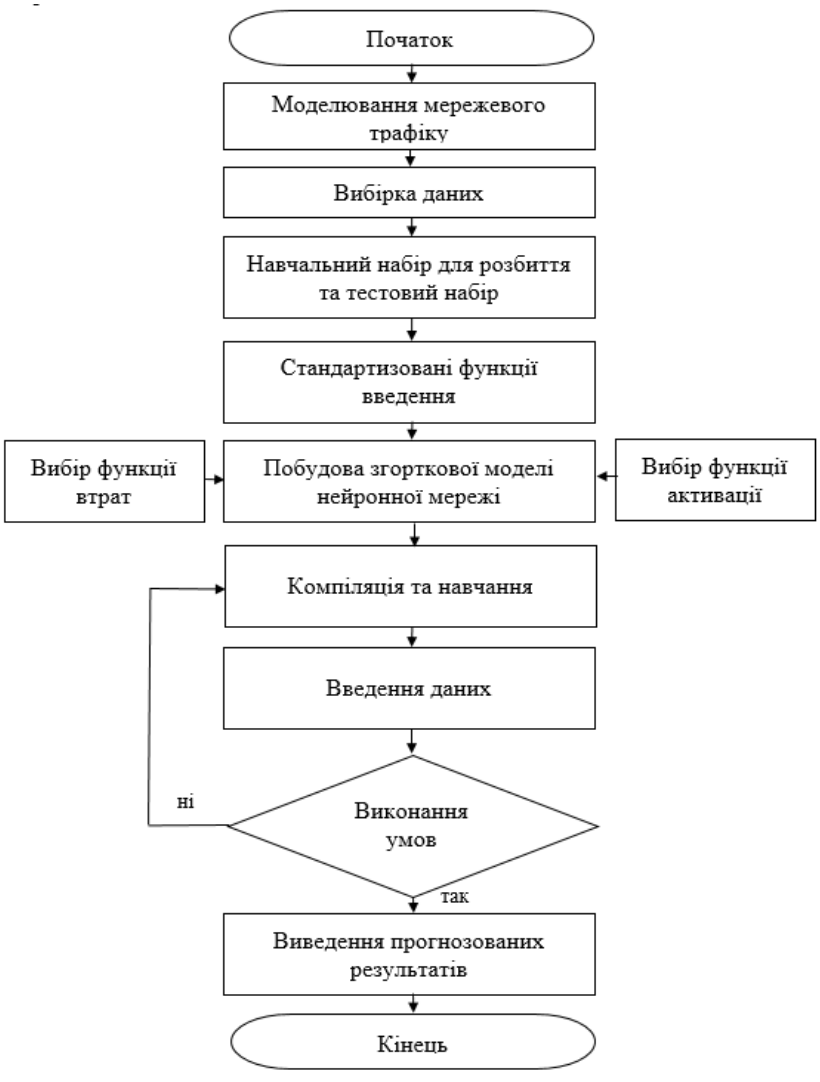

Рисунок 2.8 - Алгоритм навчання CNN

Дані поділено на взаємовиключні навчальні та тестові набори, що будуть вхідними даними для нейронної мережі. Функції введення стандартизовані. Будується CNN, і зразки навчального набору подаються в мережу під час коригування гіперпараметрів, щоб мінімізувати втрати на навчальному наборі та отримати точні прогнози від моделі. Після збереження навченої моделі дані прогнозу подаються в нейронну мережу для отримання прогнозованого типу трафіку шляхом аналізу повідомлень DNS-запитів. Згодом ці прогнози порівнюються з фактичними зразками, щоб перевірити точність прогнозної моделі.

2.4 Застосування нейронної мережі довгої короткостроковій пам'яті

Мережі довготривалої короткочасної пам'яті (LSTM) виникли як модифікація класичної рекурентної нейронної мережі (RNN), відрізняючись від неї структурою нейрона. Класичні RNN схильні до явища градієнта, що зникає та часто робить їх нездатними моделювати довгострокові залежності в даних. Мережі LSTM, з іншого боку, набагато стійкіші до цієї проблеми. Нейрон у мережі LSTM часто називають клітиною, він складається з набору воріт, які регулюють потік інформації.

Унікальні властивості пам’яті моделей LSTM дозволили їм знайти широкий спектр застосувань, наприклад, у прогнозуванні трафіку, виявлення обману на основі спостережень чи синтезі мовлення. Зокрема дану нейронну мережу можна використовувати для виявлення атак ботнетів [48,56] чи DDoS атак [57]. LSTM також можна використовувати для моделювання нелінійних динамічних процесів. У цьому випадку можна виявити, що моделі LSTM з відносно невеликою кількістю нейронів і внутрішніх ваг, а також короткими вхідними послідовностями легко навчаються і пропонують чудову якість моделювання. Моделі LSTM також можуть бути успішно реалізовані в алгоритмі прогнозного керування моделлю. Ефективність роботи LSTM описано у [58].

Структуру блоку пам’яті LSTM мережі зображено на рис 2.9.

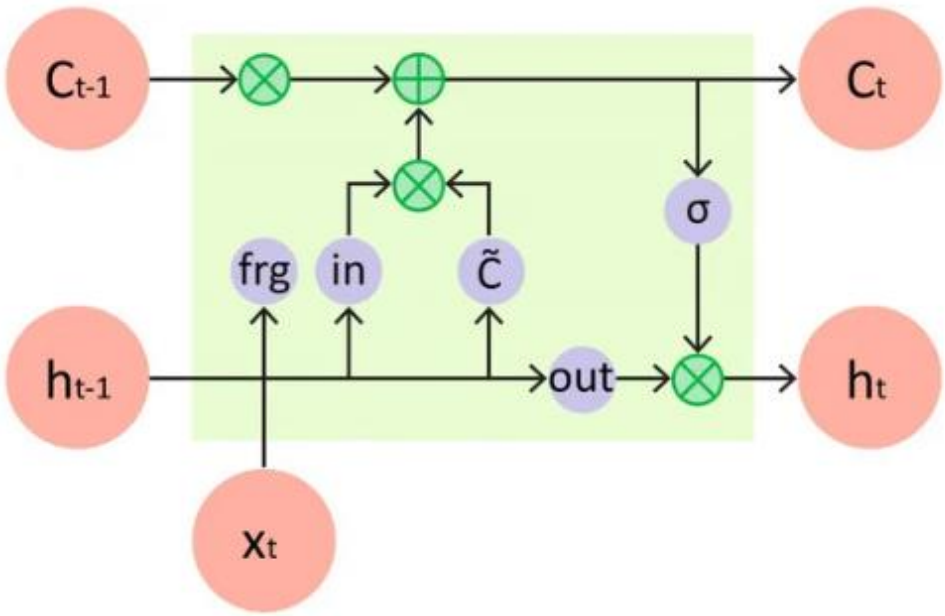

Рисунок 2.9 – Структура блоку пам’яті в шарі LSTM

Комірка отримує два важливі входи: вихідну послідовність, згенеровану попередньою коміркою LSTM, і значення прихованого стану з попередньої комірки h_{t-1}. У камері є троє воріт: ворота забуття f_t, вхідні ворота i_t, і вихідний затвор o_t. Забутий шлюз відповідає за визначення того, яка інформація повинна бути вилучена зі стану комірки. Вхідні ворота оновлюють стан комірки новою інформацією. Він складається з двох частин: сигмоїдного рівня, що називається «вхідним зворотним рівнем», який вирішує, які значення оновлювати, і рівня tanh, який створює вектор нових значень-кандидатів, які можна додати до стану. Вихідний вентиль визначає наступний прихований стан. Разом ці ворота та їхні відповідні функції керують потоком інформації в комірці LSTM, дозволяючи їй отримувати та зберігати відповідну інформацію, відкидаючи непотрібні або надлишкові дані.

У LSTM шлюз забуття відіграє вирішальну роль у визначенні того, які фрагменти інформації зберігати або викидати з наявної пам’яті, беручи до уваги надходження свіжих вхідних даних. Позначимо вхідний часовий ряд як $x=(x1,x2,\ldots,x_t)$, прихований стан комірки пам'яті як $h=(h1,h2,\ldots,h_t)$. Шлюз забуття приймає конкатенацію попереднього прихованого стану h_{t-1} і поточний вхід x_t як вхідні дані та створює забутий вектор f_t як результат формули:

$$f_t = \vartheta\big(W_f[h_{t-1}, x_t] + b_f\big), \tag{2.5}$$

де ϑ – сигмоїдальна функція активації; W_f – вагова матриця, що представляє вагові коефіцієнти, пов'язані з пропуском забуття, і визначає, наскільки сильно вхідні дані впливають на вектор забуття; b_f - вектор зсуву, який містить постійні значення, які додаються до зваженої суми цих вхідних даних, і його можна розглядати як член перехоплення в рівнянні забутих воріт.

Вагові коефіцієнти та значення зміщення вивчаються під час процесу навчання LSTM. LSTM використовує вхідний шлюз для регулювання надходження свіжих даних у комірку пам'яті, яка складається з двох компонентів: вхідний шлюз активації та гейт комірки пам'яті-кандидата. Ворота активації вхідних даних визначають, якою мірою нові вхідні дані повинні бути включені в комірку пам'яті, тоді як ворота комірки пам'яті-кандидата керують частиною нових даних, які повинні зберігатися в комірці пам'яті.

$$i_t = \vartheta(W_i[h_{t-1}, x_t] + b_i), \tag{2.6}$$

де i_t - вхідний вектор; b_i – вектор зміщення.

Кандидат в комірку пам'яті $\tilde{c}_t$ формується шляхом застосування функції активації гіперболічного тангенса до того самого набору вхідних даних:

$$\tilde{c}_t = \tanh(W_c[h_{t-1}, x_t] + b_c), \tag{2.7}$$

де $\tilde{c}_t$ - вектор комірки пам'яті-кандидата; W_c – вагова матриця; b_c - вектор зміщення.

Потім вхідний вектор і вектор комірки пам'яті-кандидата об'єднуються для оновлення попередньої комірки пам'яті c_{t-1}:

$$c_t = f_t \otimes c_{t-1} + i_t \otimes \tilde{c}_t \tag{2.8}$$

Останній вентиль, який є вихідним вентилем (output gate), в контексті LSTM-мережі відіграє важливу роль у керуванні потоком інформації. Він контролює передачу інформації від поточної комірки пам'яті до поточного прихованого стану, який є виходом LSTM на даному кроці часу. Вихідний вентиль визначає, якою частиною інформації, збереженої в комірці пам'яті, варто скористатися для формування виходу мережі на даному кроці часу. Він використовує сигмоїдну функцію для генерації вагового коефіцієнта для кожного елементу в поточній комірці пам'яті, який впливає на формування виходу. Це дозволяє враховувати релевантність кожного елементу пам'яті для задачі, яку вирішує мережа. Отже, вихідний вентиль визначає, яку частину інформації з комірки пам'яті слід враховувати у виході LSTM-мережі на кожному кроці часу, що робить його важливою складовою для забезпечення відповідності вихідних результатів завданню.

Вихідний вектор out_t отримується за допомогою формули:

$$o_t = \vartheta(W_o[h_{t-1}, x_t, c_t] + b_o) \tag{2.9}$$

Поточний прихований стан ht отримується за допомогою формул:

$$\widetilde{h_t} = \tanh(c_t), \tag{2.10}$$

де $\widetilde{h_t}$ – значення прихованого стану кандидата для поточного часового кроку мережі LSTM.

$$h_t = o_t \otimes \widetilde{h_t}, \tag{2.11}$$

де h_t – поточний прихований стан.

На рисунку 2.10 наведено схему алгоритму навчання LSTM, що використовується для аналізу вихідного DNS-трафіку. Мережа LSTM призначена для дмоделювання послідовних даних та виділення тимчасових ознак. Кожен шар

містить набір прихованих нейронів. Функція активації нейрона на кожному шарі представлена функцією ReLU для виконання нелінійних операцій. Після обробки даних у повнозв’язному шарі, результат подається на вхід до шару SoftMax. Функція SoftMax використовується для обчислення ймовірностей для кожного можливого класу під час процесу класифікації. Вона перетворює виходи з повнозв’язного шару в діапазон ймовірностей, де кожна ймовірність відображає ймовірність належності вхідного прикладу до певного класу. Такий підхід дозволяє визначити, до якого класу належить аналізований DNS-трафік на основі навчальних даних, і забезпечити подальшу класифікацію або дії відповідно до цього результату.

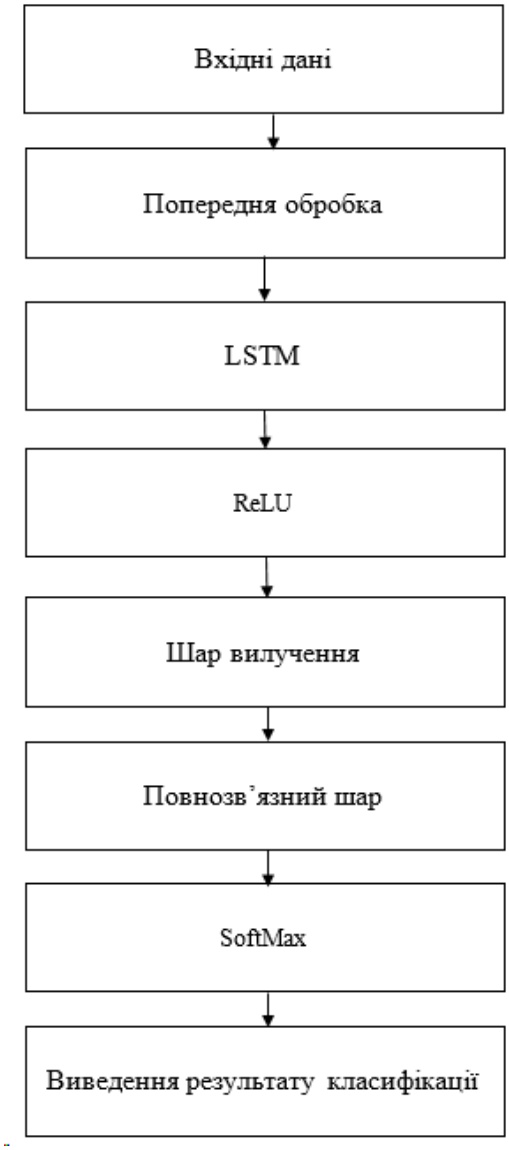

Рисунок 2.10 - Алгоритм навчання LSTM

2.5 Висновки до розділу

У другому розділі розроблено узагальнену схему публічної мережі задля забезпечення можливості аналізу вихідного DNS-трафіка, проаналізовано типову структуру повідомлень з метою вибору необхідних параметрів для дослідження наявності зловмисних дій у мереж.

Було проведено аналіз найпоширеніших типів атак, які використовують DNS-запити для своєї реалізації. Детально вивчено особливості атак, включаючи структуру DNS-запитів та відповідей, інтервали між запитами, використані для прихованої передачі даних.

Для дослідження та виявлення зловмисного DNS-трафіку було обрано використання згорткових нейронних мереж (CNN) та рекурентних мереж довготривалої та короткотривалої пам'яті (LSTM). Ці типи нейронних мереж відзначаються здатністю аналізувати послідовності даних і виділяти тимчасові залежності, що робить їх ефективними для обробки мережевого трафіку.

Вивчено будову та призначення різних шарів згорткової нейронної мережі, включаючи згорткові та пулінг-шари, а також повнозв’язний та шар SoftMax. Обрано функцію активації ReLU для виконання нелінійних операцій, що дозволяє мережі взаємодіяти зі складними шаблонами в мережевому трафіку.

Розроблено алгоритм навчання для мережі, який враховує попередньо визначені вхідні дані та спрямований на досягнення високої точності виявлення зловмисного DNS-трафіку.

Також надано опис алгоритму роботи блоку пам’яті в шарі LSTM та розглянуто, як здійснюється комунікація між різними шарами цієї архітектури. Розроблений алгоритм навчання для публічної мережі дозволяє мережі адаптуватися до різних умов та навчатися виявляти зловмисний DNS-трафік з високою ефективністю.

3 РЕАЛІЗАЦІЯ ТЕСТОВОГО СЕРЕДОВИЩА ТА ОЦІНКА ЕФЕКТИВНОСТІ НЕЙРОННИХ МЕРЕЖ CNN ТА LSTM ДЛЯ ВИЯВЛЕННЯ ПОРУШНИКА В ПУБЛІЧНІЙ МЕРЕЖІ НА ОСНОВІ АНАЛІЗУ ВИХІДНИХ DNS-ЗАПИТІВ

3.1 Метод виявлення порушника на основі аналізу вихідних DNS-запитів

Аналіз наявних методів виявлення та ідентифікації порушника в інформаційно-комунікаційних системах у параграфі 1.2 показав, що наявні системи націлені на захист мережі від стороннього втручання. Проте такі системи вимагають наявності фахівця, який буде здійснювати моніторинг роботи системи та оперативно реагувати на виявлення несанкціонованих дій, надавати технічну підтримку для користувачів в разі помилкового спрацювання. Існуючі системи не здійснюють аналіз трафіку, що виходить з мережі або ж підтримка їх роботоздатності є дороговартісною та їх застосування у публічних мережах є нерентабельним.

З метою виявлення зловмисних дій користувачами в публічній мережі стосовно ресурсів, що знаходяться поза мережею розроблено метод виявлення порушника на основі аналізу вихідних DNS-запитів (рис.3.1).

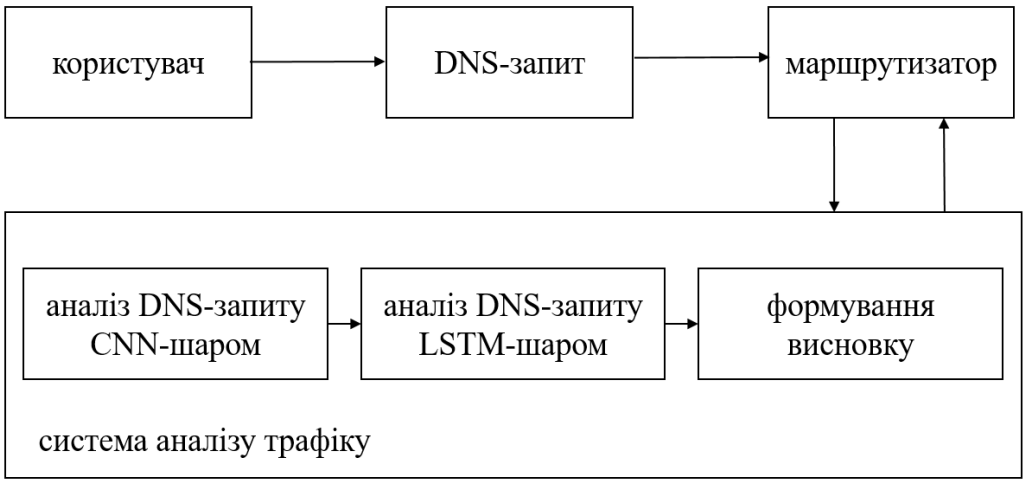

Рисунок 3.1 – Алгоритм роботи методу порушника на основі аналізу вихідних DNS-запитів

Послідовність роботи методу наступна:

1. отримання маршрутизатором DNS-запиту;
2. передача DNS-запиту на аналізатор;
3. аналіз DNS-запиту CNN-шаром нейронної мережі;
4. передача отриманих результатів на LSTM-шар нейронної мережі;
5. формування висновку про пропуск/блокування пакету з DNS-запитом;
6. модифікація налаштувань маршрутизатора для дозволу або блокування запитів від користувача.

3.2 Набори даних для навчання та тестування нейронних мереж

Набір даних KDD Cup 1999 є добре відомим набором даних, який використовується для досліджень і оцінки в області виявлення вторгнень і безпеки мережі. Він був створений у рамках змагань KDD Cup 1999 і широко використовується для розробки та тестування систем виявлення вторгнень. Його було створено для підтримки змагань KDD Cup 1999, метою яких було просування досліджень у сфері виявлення вторгнень, зокрема в контексті виявлення мережевих атак у комп'ютерних системах.

Набір даних містить дані про мережевий трафік, які імітують середовище комп'ютерної мережі. Він включає велику кількість мережевих підключень, кожне з яких представлено набором функцій, що описують різні аспекти мережевого трафіку, такі як тип протоколу, сервіс, тривалість тощо. Кожне мережеве з'єднання в наборі даних позначено як один із кількох класів, включаючи «дозволений» (нормальний мережевий трафік) та «заборонений» (різні типи атак) трафік.

Набір даних містить мітки для класифікації мережевих підключень за цими класами. Набір даних поділяється на навчальні та тестові вибірки. Навчальна вибірка використовується для навчання моделей виявлення вторгнень, а тестова вибірка використовується для оцінки продуктивності цих моделей.

Набір даних KDD99 широко використовувався в дослідженнях і експериментах для розробки та оцінки систем виявлення вторгнень, а також для

тестування алгоритмів машинного навчання та аналізу даних для програм безпеки мережі.

Набір даних KDD Cup 1999 містить близько п’яти мільйонів записів підключення. Важливо зазначити, що тестові дані не з того самого розподілу ймовірностей, що й навчальні дані, і включають конкретні типи атак, яких немає в навчальних даних. Набори даних містять загалом 24 типи тренувальних атак, а також додаткові 14 типів лише в тестових даних. Приклад з набору наведено на рис.3.2

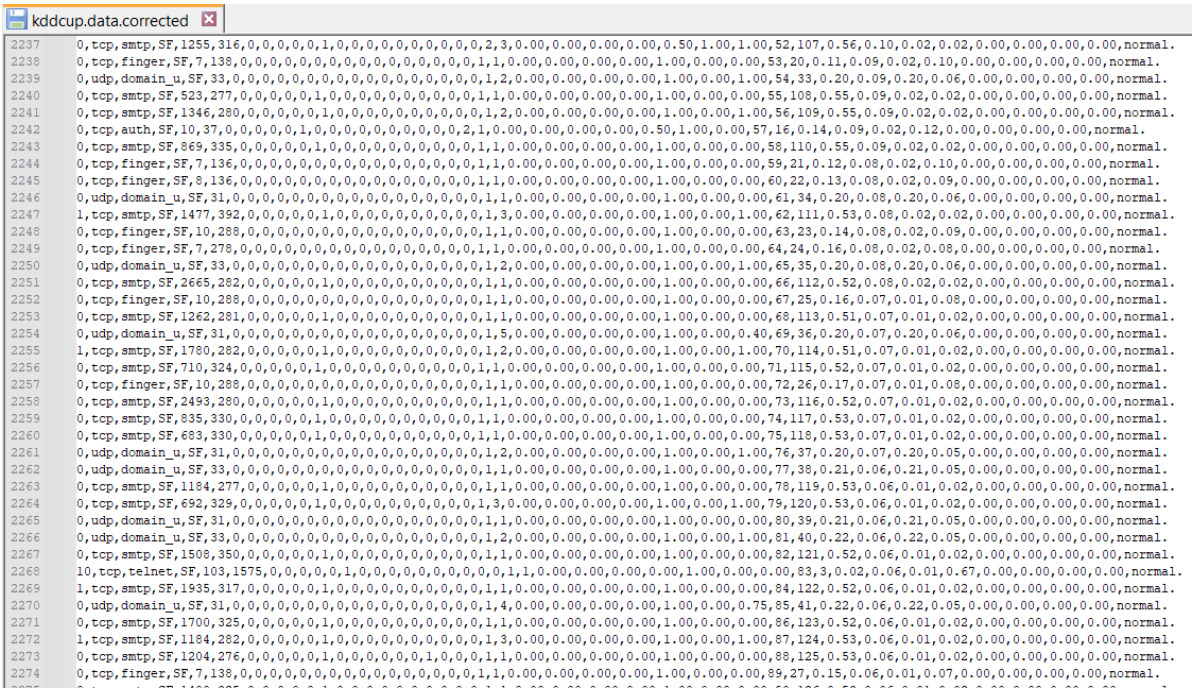

Рисунок 3.2 – Частина набору даних KDD Cup 1999

3.3 Тестове середовище

Для проведення дослідження щодо оптимального методу виявлення порушника у публічній мережі шляхом аналізу вихідного DNS-трафіку було розгорнуто локальне тестове середовище, котре ізольоване від інших мереж та не становить загрози при запуску атак чи інших зловмисних дій. Використано наступне обладнання:

- Маршрутизатор – Mikrotik RB1100 AH2 в якості маршрутизатора та пристрою, що надсилає DNS запити на аналіз.
- Точка доступу Ubiquiti UAP-AC-PRO, призначена для приєднання мобільних пристроїв;
- DNS сервер – HP ProLiant ML350 G6 на базі процесора Intel Xeon E5645, 144ГБ оперативної пам’яті та 1ТБ SSD накопичувач, на якому встановлено ОС Ubuntu 22.04, як модель DNS – сервера провайдера, що отримує усі DNS-запити від маршрутизатора;
- Сервер аналізу трафіку – HP ProLiant ML350 G6 на базі процесора Intel Xeon E5645, 144ГБ оперативної пам’яті та 4ТБ SSD накопичувач, на якому встановлено ОС Windows Server 2019, на якому проводиться аналіз DNS-пакетів запропонованим методом;
- Персональні комп’ютери - 10 штук на базі процесора i5-11400, 16Гб оперативної пам’яті та 500ГБ SSD накопичувача під керуванням ОС Windows 10 professional, які моделюють робочий та «хакерський» потік DNS запитів.

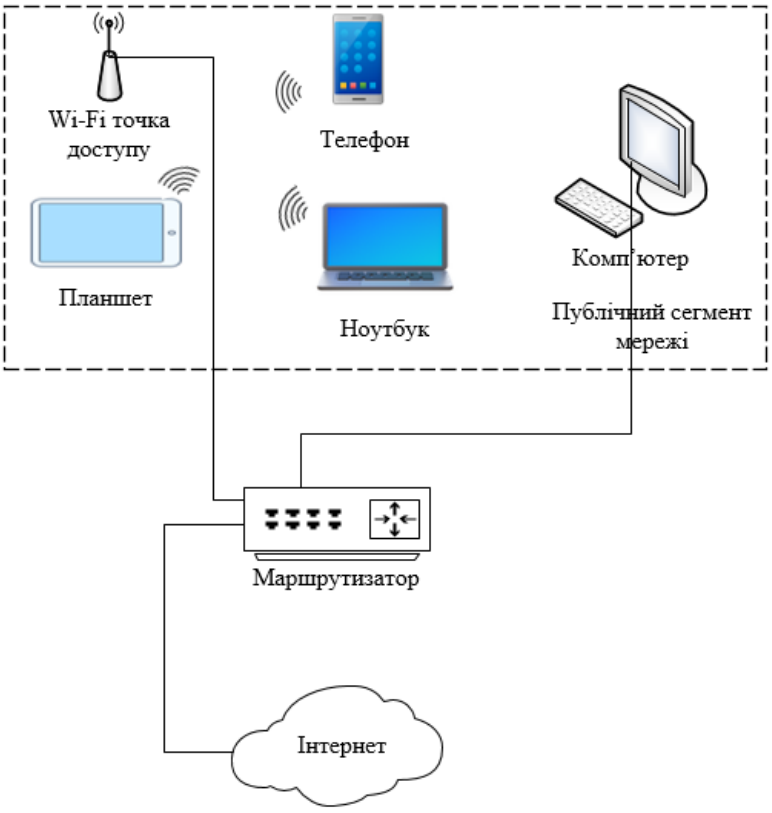

Рисунок 3.3 – Публічна мережа для проведення дослідження

До публічного сегмента мережі (рис.3.3) приєднано різні бездротові пристрої: мобільні телефони, планшети та інше. Точка доступу приєднується до маршрутизатора, на якому буде встановлена система аналізу трафіку.

Під час програмної реалізації було виконано попередню обробку даних, а саме імпортовано бібліотеки та списки функцій (рис.3.4), додано стовпці до набору даних, завантажено типи атак та створено відповідний словник, додано функції типів атак до набору даних.

```
import os
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
import time

# reading features list
with open("..\\kddcup.names", 'r') as f:
    print(f.read())
```

Рисунок 3.4 - Імпортування бібліотек і списку функцій

Далі здійснено поділ набору даних на навчальну та тестову вибірку (рис.3.5).

```
# Splitting the dataset
df = df.drop(['target', ], axis = 1)
print(df.shape)

# Target variable and train set
y = df[['Attack Type']]
X = df.drop(['Attack Type', ], axis = 1)

sc = MinMaxScaler()
X = sc.fit_transform(X)

# Split test and train data
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size = 0.2 , random_state = 42)
print(X_train.shape, X_test.shape)
print(y_train.shape, y_test.shape)
```

Рисунок 3.5 - Поділ набору даних

Після чого проведено навчання та тестування обраних нейронних мереж (рис.3.6).

```
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import accuracy_score

clfg = GaussianNB()
start_time = time.time()
clfg.fit(X_train, y_train.values.ravel())
end_time = time.time()
print("Training time: ", end_time-start_time)
start_time = time.time()
y_test_pred = clfg.predict(X_train)
end_time = time.time()
print("Testing time: ", end_time-start_time)
```

Рисунок 3.6 – Програмна реалізація навчання та тестування

3.4 Дослідження роботи згорткової нейронної мережі

Для оцінки ефективності навчання моделі CNN використовується матриця плутанини. У сфері аналізу мережевого трафіку матриця плутанини використовується для оцінки прогнозованих результатів порівняно з фактичними значеннями та вимірювання ефективності моделі. Для розрахунку необхідний набір тестових даних і даних перевірки, що містять значення отриманих результатів. Матриця плутанини зображена на рис.3.7.

Метрики якості наступні:

- TP (True Positive) – кількість спрацювань при яких виявлено зловмисні спрацювання, які дійсно є зловмисними;
- FP (False Positive) – кількість спрацювань при яких виявлено зловмисні спрацювання, але такими не є;
- TN (True Negative) – кількість спрацювань при яких не виявлено зловмисні спрацювання, які дійсно не є зловмисними;

- FN (False Positive) – кількість спрацювань при яких не виявлено зловмисні спрацювання, але які дійсно є зловмисними.

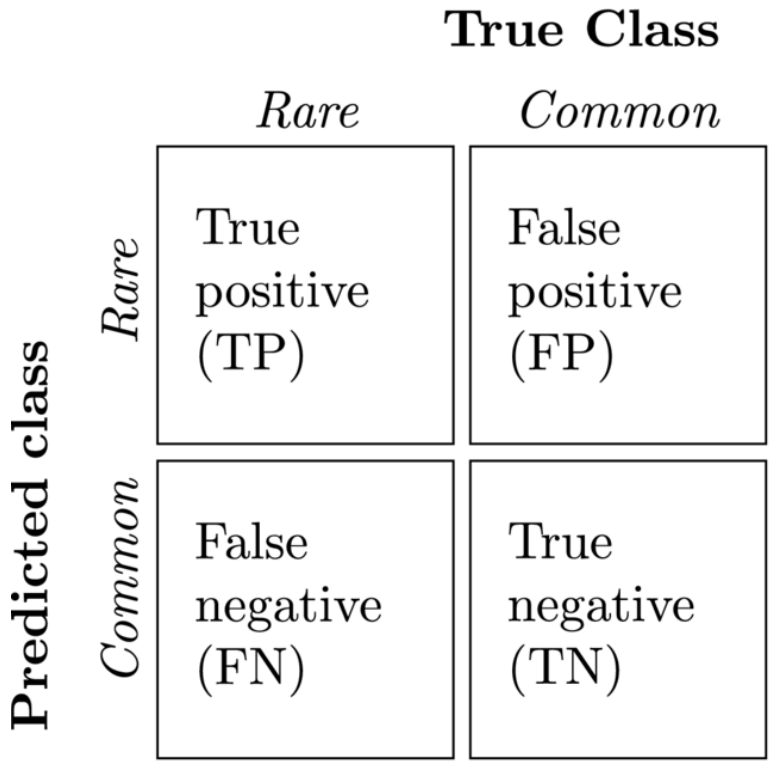

Рисунок 3.7 – Матриця плутанини

Повнота (Recall) вимірює здатність системи виявляти всі наявні зловмисні сесії (події або об'єкти) без пропуску жодної з них. Ця метрика допомагає оцінити наскільки ефективно система виявлення порушників впоралася з виявленням всіх справжніх загроз. Однак варто враховувати, що підвищення повноти може призводити до збільшення кількості хибних спрацьовувань (false positives), тобто помилкових виявлень, що не є зловмисними діями. Таким чином, повнота і точність (precision) є двома ключовими метриками, які важливо балансувати для досягнення оптимальної ефективності системи виявлення порушників. Метрика повноти обчислюється як частка правильно виявлених зловмисних сесій серед усіх дійсно наявних зловмисних сесій:

$$Recall = \frac{TP}{TP + FN} \tag{3.1}$$

Точність (Precision) вимірює наскільки вірно система класифікує об'єкти або події як зловмисні, коли вона виявляє їх як такі. Іншими словами, точність вказує на те, яка частина виявлень, визначених системою як зловмисні, є дійсно зловмисними. Точність важлива коли небажані наслідки хибно позитивних наслідків можуть бути критичними, наприклад, у випадку хибних звинувачень.

Проте важливо пам'ятати, що точність і повнота є взаємно зв'язаними метриками: підвищення точності може призводити до зниження повноти і навпаки. Також, оптимальний баланс між цими метриками залежить від конкретних вимог і цілей системи виявлення порушників.

Точність обчислюється як частка правильно визначених зловмисних об'єктів або подій серед усіх об'єктів або подій, які система визначила як зловмисні:

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

Акуратність (Accuracy) вимірює загальну точність системи, тобто частку правильних визначень (правильно виявлених та правильно не виявлених об'єктів або подій) серед усіх об'єктів або подій, які система спробувала визначити. Іншими словами, акуратність вказує на загальну точність системи виявлення, незалежно від того, чи є це визначення зловмисними чи незловмисними:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{3.3}$$

Помилка (Specificity) є метрикою, яка вимірює здатність системи виявлення зловмисників правильно ідентифікувати незловмисні об'єкти або події як незловмисні. Специфічність важлива, оскільки вона вказує на здатність системи уникати хибних спрацьовувань (false positives) – помилкових визначень об'єктів або подій як зловмисних. Висока специфічність означає, що система має мало хибних спрацьовувань і добре відокремлює незловмисні об'єкти або події від

зловмисних. Вона обчислюється як відношення кількості правильно визначених незловмисних об'єктів або подій до загальної кількості незловмисних об'єктів або подій:

$$Specificity = \frac{FP + FN}{TP + FP + TN + FN} \quad (3.4)$$

F-метрика (F1-score) об'єднує в собі дві метрики: точність та повноту. F-метрика дозволяє врахувати хибні позитивні (false positives) та хибні негативні (false negatives) при оцінці ефективності системи виявлення порушників. Доцільно застосовувати задля досягнення балансу між зменшенням хибних спрацьовувань і забезпеченням високої повноти системи. F-метрика обчислюється як гармонічне середнє значення між точністю і повнотою. Формула для обчислення F-метрики виглядає так:

$$F1\ score = \frac{Recall + Precision}{2} \quad (3.5)$$

Набір даних містить 5209460 елементів. Для навчання обрано 80% від набору даних KDD Cup 99- 4167568 записів, тестування містить 20% - 1041892 записів.

Результати метрик якості після навчання та тестування згорткової нейронної мережі відображено у таблиці 3.3

Таблиця 3.3 – Результати метрик якості після навчання та тестування

CNN	TP	TN	FP	FN
train	2392562	1452624	145356	177026
test	675812	279258	41104	45718

Повнота під час навчання складала:

$$Recall = \frac{2392562}{2392562 + 177026} * 100\% = 93{,}11\% \quad (3.6)$$

Точність під час навчання складала:

$$Precision = \frac{2392562}{2392562 + 145356} * 100\% = 94{,}27\% \quad (3.7)$$

Акуратність під час навчання складала:

$$Accuracy = \frac{2392562 + 1452624}{2392562 + 145356 + 177026 + 1452624} * 100\% = 92{,}26\% \quad (3.8)$$

Помилка під час навчання складала:

$$Specificity = \frac{145356 + 177026}{2392562 + 145356 + 1452624 + 177026} * 100\% = \\ = 7{,}74\% \quad (3.9)$$

F-метрика під час навчання складала:

$$F1\ score = \frac{93{,}11\% + 94{,}27\%}{2} = 93{,}69\% \quad (3.10)$$

Повнота під час тестування складала:

$$Recall = \frac{675812}{675812 + 45718} * 100\% = 93{,}66\% \quad (3.11)$$

Точність під час тестування складала:

$$Precision = \frac{675812}{675812 + 41104} * 100\% = 94{,}27\% \quad (3.12)$$

Акуратність під час тестування складала:

$$Accuracy = \frac{675812 + 279258}{675812 + 41104 + 45718 + 279258} * 100\% = 91{,}67\% \quad (3.13)$$

Помилка під час тестування складала:

$$Specificity = \frac{41104 + 45718}{675812 + 41104 + 279258 + 45718} * 100\% = 8{,}33\% \quad (3.14)$$

F-метрика під час тестування складала:

$$F1\ score = \frac{93{,}66\% + 94{,}27\%}{2} = 93{,}97\% \quad (3.15)$$

Порівнюючи результати навчання та тестування нейронної мережі (табл.3.4), слід відмітити, що тестова вибірка дала повноту на 0,55% більше за навчальну при тому ж значенні точності. Хоча зростає відсоток помилок.

Таблиця 3.4 – Порівняння результатів навчання та тестування CNN

CNN	Повнота	Точність	Акуратність	Помилка	F-метрика
train	93,11%	94,27%	92,26%	7,74%	93,69%
test	93,66%	94,27%	91,67%	8,33%	93,97%

На рисунку 3.8 відображено графічне порівняння якості виявлення зловмисного трафіку під час навчання та тренування згорткової нейронної мережі для аналізу вихідного DNS-трафіку.

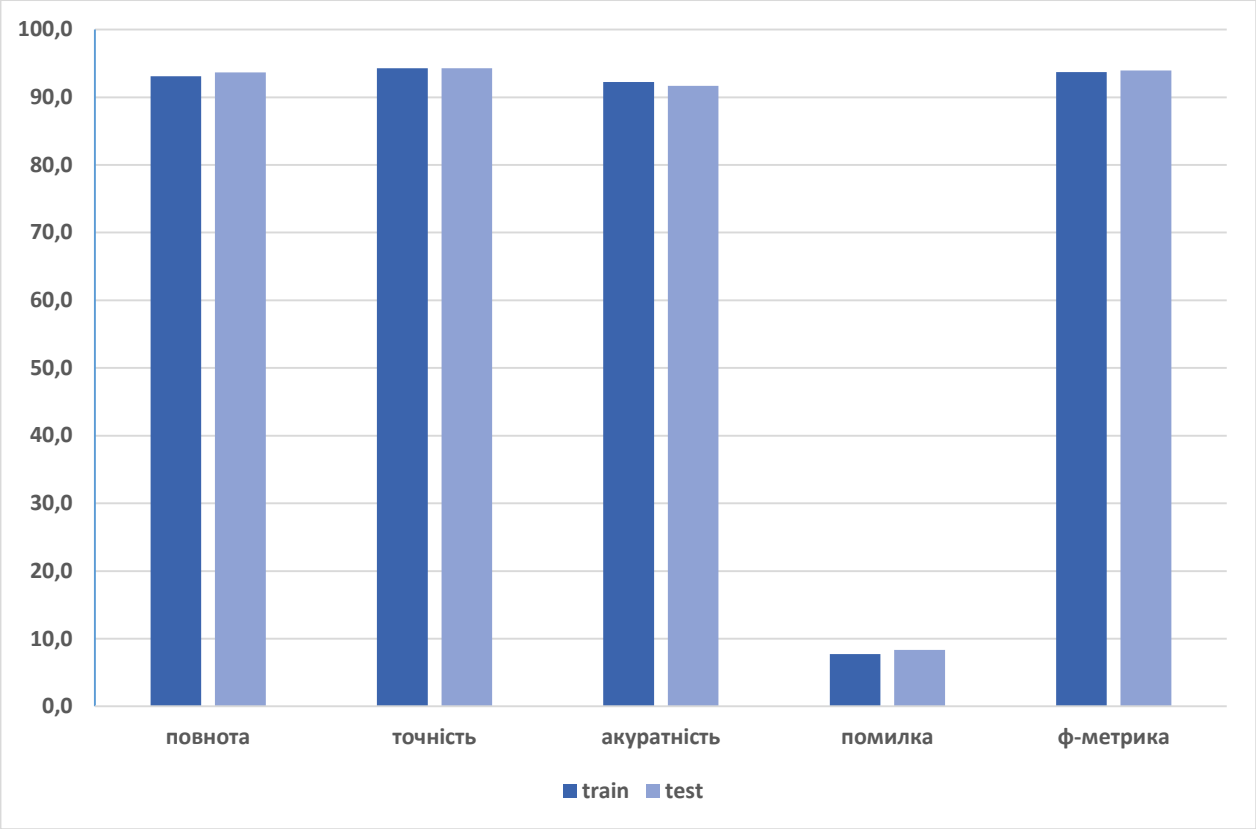

Рисунок 3.8 – Порівняння якості виявлення зловмисного трафіку

3.5 Дослідження роботи мережі довгої короткострокової пам'яті

Для навчання і тестування цієї мережі використовується та сама вибірка, що і для CNN: містить 5209460 елементів з яких обрано 80% навчальних записів, а для тестування 20% записів.

Результати метрик якості після навчання та тестування згорткової нейронної мережі відображено у таблиці 3.5

Таблиця 3.5 – Результати метрик якості після навчання та тестування

LSTM	TP	TN	FP	FN
train	2435476	1401256	115291	215545
test	694742	264400	34675	48075

Повнота під час навчання складала:

$$Recall = \frac{2435476}{2435476 + 215545} * 100\% = 91{,}87\% \quad (3.16)$$

Точність під час навчання складала:

$$Precision = \frac{2435476}{2435476 + 115291} * 100\% = 95{,}48\% \quad (3.17)$$

Акуратність під час навчання складала:

$$Accuracy = \frac{2435476 + 1401256}{2435476 + 115291 + 215545 + 1401256} * 100\% = 92{,}06\% \quad (3.18)$$

Помилка під час навчання складала:

$$Specificity = \frac{145356+177026}{2392562+145356+1452624+177026} * 100\% = 7{,}94\% \quad (3.19)$$

F-метрика під час навчання складала:

$$F1\ score = \frac{91{,}87\% + 95{,}48\%}{2} = 93{,}67\% \quad (3.20)$$

Повнота під час тестування складала:

$$Recall = \frac{694742}{694742 + 48075} * 100\% = 93{,}53\% \quad (3.21)$$

Точність під час тестування складала:

$$Precision = \frac{694742}{694742 + 34675} * 100\% = 95{,}25\% \quad (3.22)$$

Акуратність під час тестування складала:

$$Accuracy = \frac{694742 + 264400}{694742 + 34675 + 48075 + 264400} * 100\% = 92{,}06\% \quad (3.23)$$

Помилка під час тестування складала:

$$Specificity = \frac{34675 + 48075}{694742 + 34675 + 264400 + 48075} * 100\% = 7{,}94\% \quad (3.24)$$

F-метрика під час тестування складала:

$$F1\ score = \frac{93{,}53\% + 95{,}25\%}{2} = 94{,}39\% \quad (3.25)$$

Порівнюючи результати навчання та тестування нейронної мережі (табл.3.6), слід відмітити, що тестова вибірка дала повноту на 1,66% більше за навчальну та F-метрика на 0,72% більша при тестовій вибірці. Значення акуратності та помилки залишилися незмінними. Хоча при навчанні точність була на 0,23% більша.

Таблиця 3.6 – Порівняння результатів навчання та тестування CNN

LSTM	Повнота	Точність	Акуратність	Помилка	F-метрика
train	91,87%	95,48%	92,06%	7,94%	93,67%
test	93,53%	95,25%	92,06%	7,94%	94,39%

На рисунку 3.9 відображено графічне порівняння якості виявлення зловмисного трафіку під час навчання та тренування LSTM для аналізу вихідного DNS-трафіку.

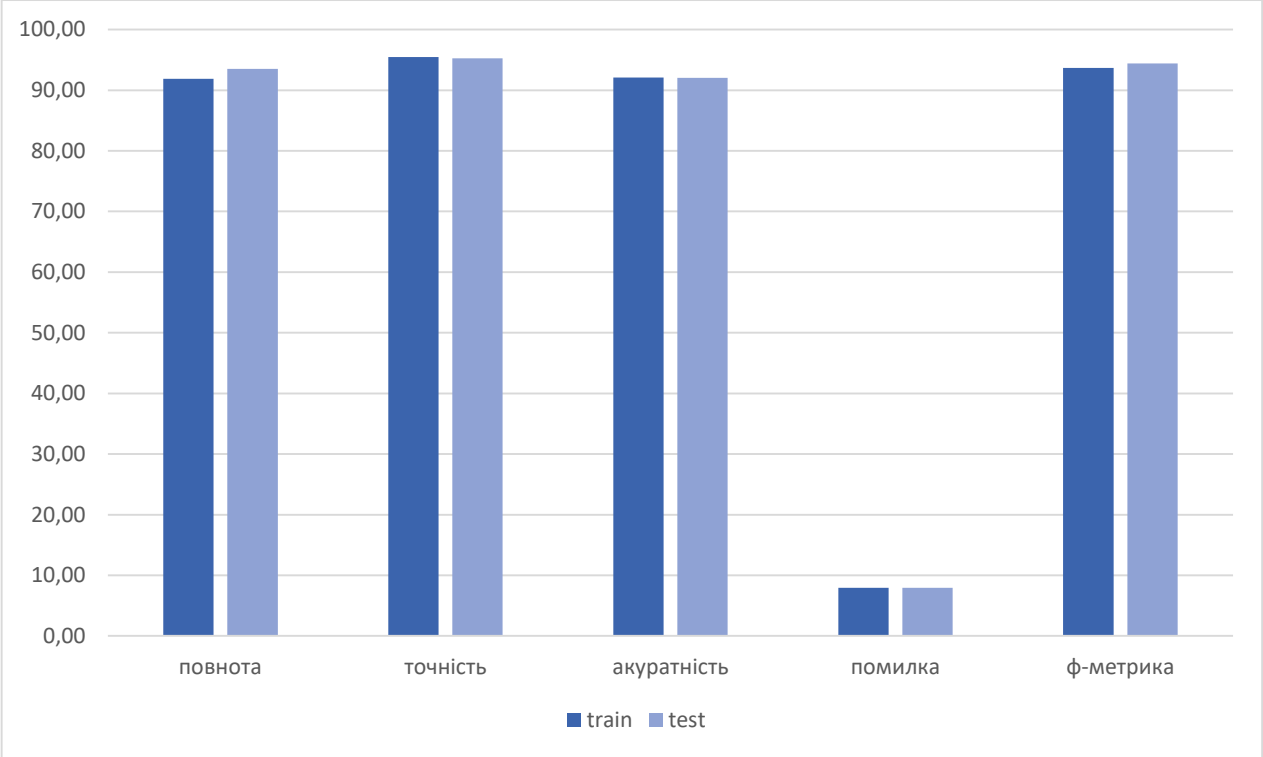

Рисунок 3.9 – Порівняння якості виявлення зловмисного трафіку

3.6 Висновки до розділу

У третьому розділі було важливо визначити набір даних, на основі якого проводилося навчання та тестування нейронних мереж типу CNN та LSTM для виявлення зловмисного DNS-трафіку. Для цього використовувався набір даних KDD Cup 99, який вже став стандартним набором для дослідження задач в області мережевої безпеки. Набір даних KDD Cup 99 включає в себе різноманітні записи мережевого трафіку, які включають нормальний мережевий трафік, а також дані, які представляють собою атаки та відхилення від стандартних мережевих патернів. Записи набору даних розділено на 80% навчальної вибірки та 20% тестової. Також описано середовище де було розгорнуто нейронні мережі.

У параграфі 3.4 проведено дослідження ефективності роботи згорткової нейронної мережі. Зокрема, визначено що точність сягає 94,27%, а помилки можуть досягати значення 8,33%. У параграфі 3.5 проведено дослідження ефективності роботи мережі довгої короткострокової пам’яті для якої точність сягає значення 95,25%, а відсоток помилок 7,94%.

4 ДОСЛІДЖЕННЯ РОБОТОЗДАТНОСТІ CNN-LSTM МЕРЕЖІ ДЛЯ ВИЯВЛЕННЯ ПОРУШНИКА В ПУБЛІЧНІЙ МЕРЕЖІ НА ОСНОВІ АНАЛІЗУ ВИХІДНИХ DNS-ЗАПИТІВ

4.1 Реалізація нейронної мережі CNN-LSTM

На рис.4.1 представлено схему роботи CNN-LSTM нейронної мережі, що демонструє послідовність подачі вхідних даних, обробку нейронними шарами та виведення результату.

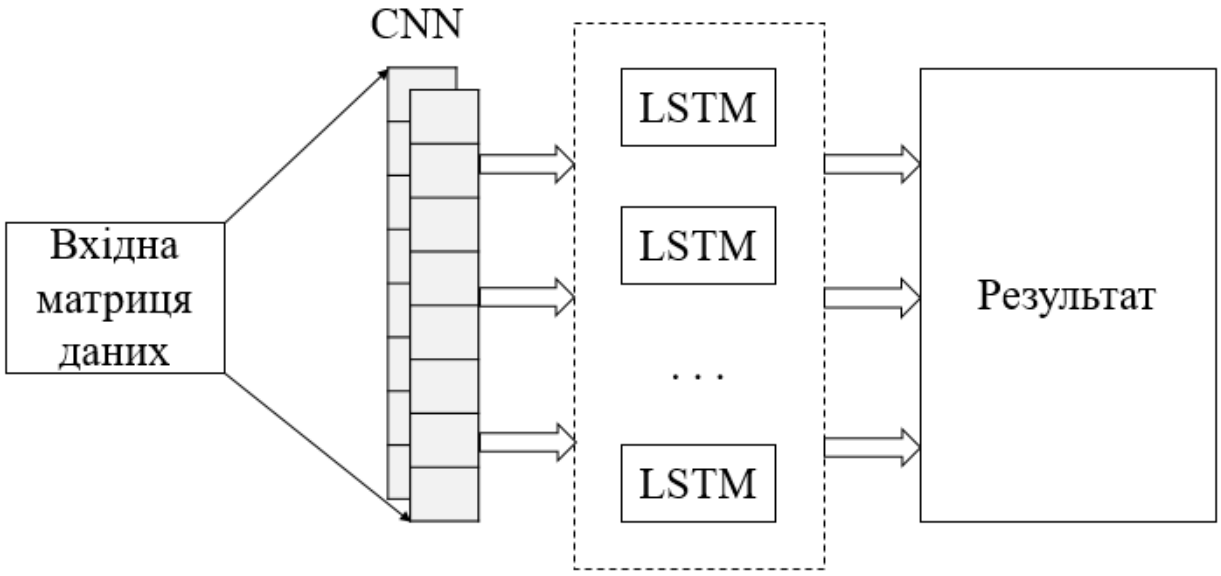

Рисунок 4.1 – Схема реалізації CNN-LSTM нейронної мережі

У розробленій гібридній архітектурі CNN-LSTM мережі першим шаром є CNN. Оскільки він здатний виявляти короткочасні залежності та закономірності між вхідними змінними. Даний шар є багатовимірним та може бути представлений наступною формулою:

$$k_t = \tanh(a_t X + b_t), \tag{4.1}$$

де X – вхідна матриця;

b_t – матриця зміщення;

a_t – вагова матриця;

k_t – вихідна функція;

t – номер фільтра, розмір якого становить ширину d та висоту I.

Вхідна матриця X представлена наступним чином:

$$X = \begin{bmatrix} x_{1.1} & x_{1.2} & \dots & x_{1.42} \\ x_{2.1} & x_{2.2} & \dots & x_{2.42} \\ \vdots & \vdots & & \vdots \\ x_{n.1} & x_{n.2} & \dots & x_{n.3} \end{bmatrix} \quad (4.1)$$

Вхідна матриця складається з 42 змінних, які представлені у форматі одновимірних масивів. Оскільки CNN мережа, яка буде першою для виконання, здатна працювати саме з одновимірними масивами даних. На етапі виконання CNN першочергово виконується обробка вхідних даних та визначення кількості нейронів у шарі. Вихідні дані передаються на шар LSTM. Він створює вихідні дані та приховане значення стану. У якості функції активації для шарів CNN буде ReLU, для шарів LSTM – Sigmoid.

4.2 Оцінка ефективності роботи нейронної мережі CNN-LSTM

Набір даних KDD Cup 99 для навчання та тестування розподілений аналогічно до параграфів 3.3 та 3.4.

Результати метрик якості після навчання та тестування згорткової нейронної мережі відображено у таблиці 4.1.

Таблиця 4.1 – Результати метрик якості після навчання та тестування

CNN-LSTM	TP	TN	FP	FN
train	2695476	1301256	75291	95545
test	799014	184168	28456	30254

Повнота під час навчання складала:

$$Recall = \frac{2695476}{2695476 + 95545} * 100\% = 96{,}58\% \quad (4.2)$$

Точність під час навчання складала:

$$Precision = \frac{2695476}{2694576 + 75291} * 100\% = 97{,}28\% \quad (4.3)$$

Акуратність під час навчання складала:

$$Accuracy = \frac{2695476 + 1301256}{2695476 + 75291 + 95545 + 1301256} * 100\% = 95{,}9\% \quad (4.4)$$

Помилка під час навчання складала:

$$Specificity = \frac{75291+95545}{2695476+75291+1301256+95545} * 100\% = 4{,}1\% \quad (4.5)$$

F-метрика під час навчання складала:

$$F1\ score = \frac{96{,}58\% + 97{,}28\%}{2} = 96{,}93\% \quad (4.6)$$

Повнота під час тестування складала:

$$Recall = \frac{802014}{802014 + 23154} * 100\% = 97{,}19\% \quad (4.7)$$

Точність під час тестування складала:

$$Precision = \frac{802014}{802014 + 22456} * 100\% = 97{,}28\% \quad (4.8)$$

Акуратність під час тестування складала:

$$Accuracy = \frac{802014 + 194268}{802014 + 22456 + 23154 + 194268} * 100\% = 95{,}62\% \quad (4.9)$$

Помилка під час тестування складала:

$$Specificity = \frac{22456 + 23154}{802014 + 22456 + 194268 + 23154} * 100\% = 4{,}38\% \quad (4.10)$$

F-метрика під час тестування складала:

$$F1\ score = \frac{97{,}19\% + 97{,}28\%}{2} = 97{,}24\% \quad (4.11)$$

Порівнюючи результати навчання та тестування нейронної мережі (табл.4.2), слід відмітити, що навчальна та тестова вибірки дали показник точності 97,28%, а відсоток помилок становив 4,1% та 4,38% відповідно.

Таблиця 4.2 – Порівняння результатів навчання та тестування CNN-LSTM

CNN-LSTM	Повнота	Точність	Акуратність	Помилка	F-метрика
Train	96,58%	97,28%	95,90%	4,10%	96,93%
Test	97,19%	97,28%	95,62%	4,38%	97,24%

На рисунку 4.2 відображено графічне порівняння якості виявлення зловмисного трафіку під час навчання та тренування CNN-LSTM для аналізу вихідного DNS-трафіку.

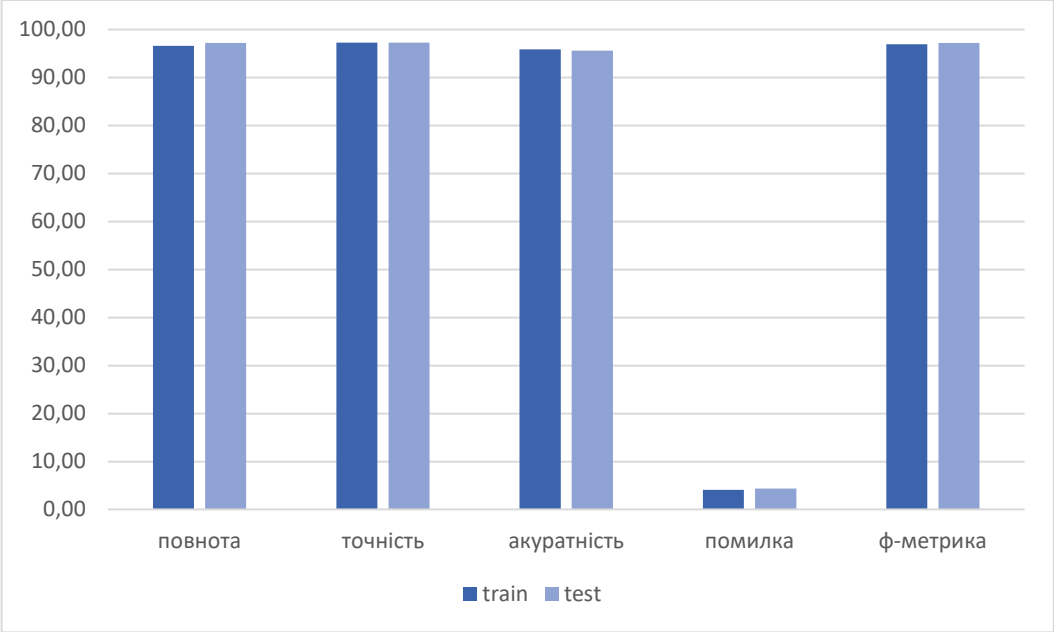

Рисунок 4.2 – Порівняння якості виявлення зловмисного трафіку

4.3 Порівняння ефективності роботи мереж CNN, LSTM, CNN-LSTM

Завдяки метрикам було оцінено продуктивність трьох архітектур нейронних мереж (табл.4.3) при ідентичному наборі даних під час тестування. Розглянуті архітектури включають згорткову нейронну мережу, довгу короткострокову пам'ять та мережу, що складається із поєднання згорткової нейронної мережі та мережі довгої короткострокової пам'яті.

Таблиця 4.3 - Порівняння результатів тестування нейронних мереж CNN, LSTM та CNN-LSTM

test	Повнота	Точність	Акуратність	Помилка	F-метрика
CNN	93,66%	94,27%	91,67%	8,33%	93,97%
LSTM	93,53%	95,25%	92,06%	7,94%	94,39%
CNN-LSTM	97,19%	97,28%	95,62%	4,38%	97,24%

На рисунку 4.3 представлено порівняння за метриками повноти, точності, акуратності та F-міри. Слід відмітити, що показник повноти у CNN-LSTM на 3,53% більший за відповідний показник у CNN та на 3,66% у LSTM. Показник точності у

CNN-LSTM більший на 3,01% у порівнянні з CNN та на 2,03% у порівнянні з LSTM. Акуратність роботи CNN-LSTM також має кращі показники у порівнянні з CNN та LSTM на 3,95% та 3,56% відповідно. F-метрика переважає у значеннях CNN-LSTM на 3,27% у порівнянні з CNN та на 2,85% у порівнянні з LSTM.

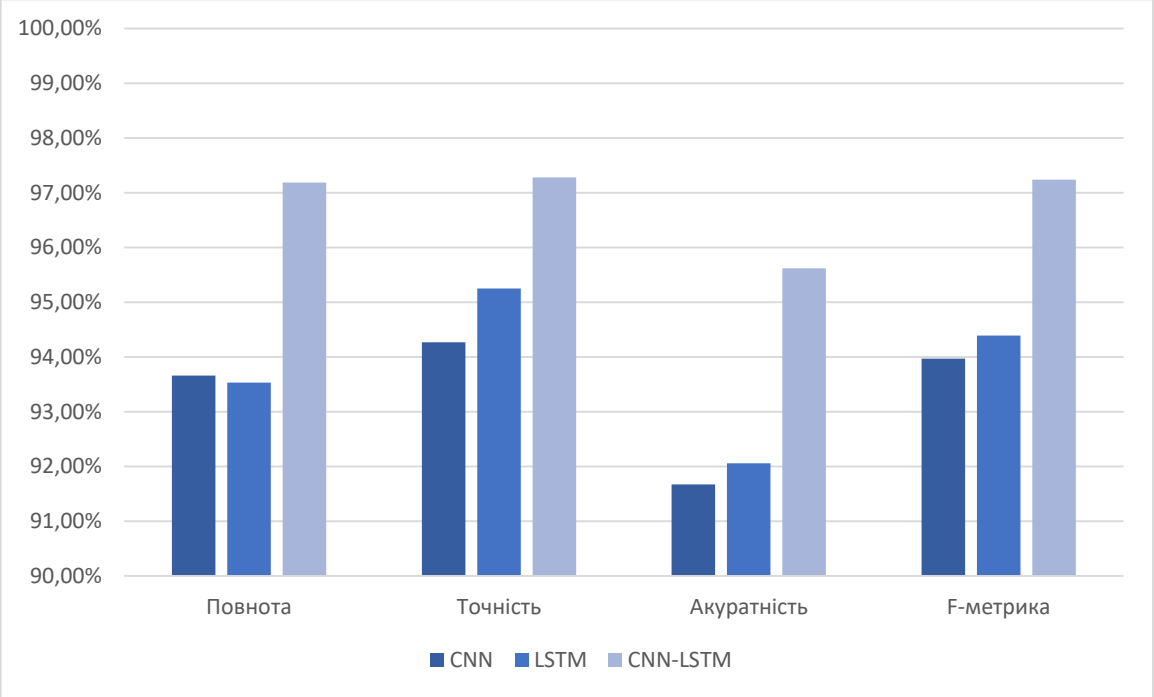

Рисунок 4.3 - Порівняння якості виявлення зловмисного трафіку нейронними мережами CNN, LSTM та CNN-LSTM за наступними метриками: повнота, точність, акуратність, F-метрика

Як видно з рис.4.4 метрика помилки CNN-LSTM при порівнянні якості виявлення зловмисного трафіку з нейронними мережами CNN та LSTM менша на 3,95% та 3,56% відповідно.

Результати порівняння метрик ефективності свідчать про те, що:

- CNN мережа має кращі показники за метрикою повноти у порівнянні з LSTM;
- LSTM мережа має кращі показники за метриками точності, акуратності та F-метрики у порівнянні з CNN;
- архітектурне поєднання CNN та LSTM в єдину мережу дає кращі результати за всіма метриками ефективності.

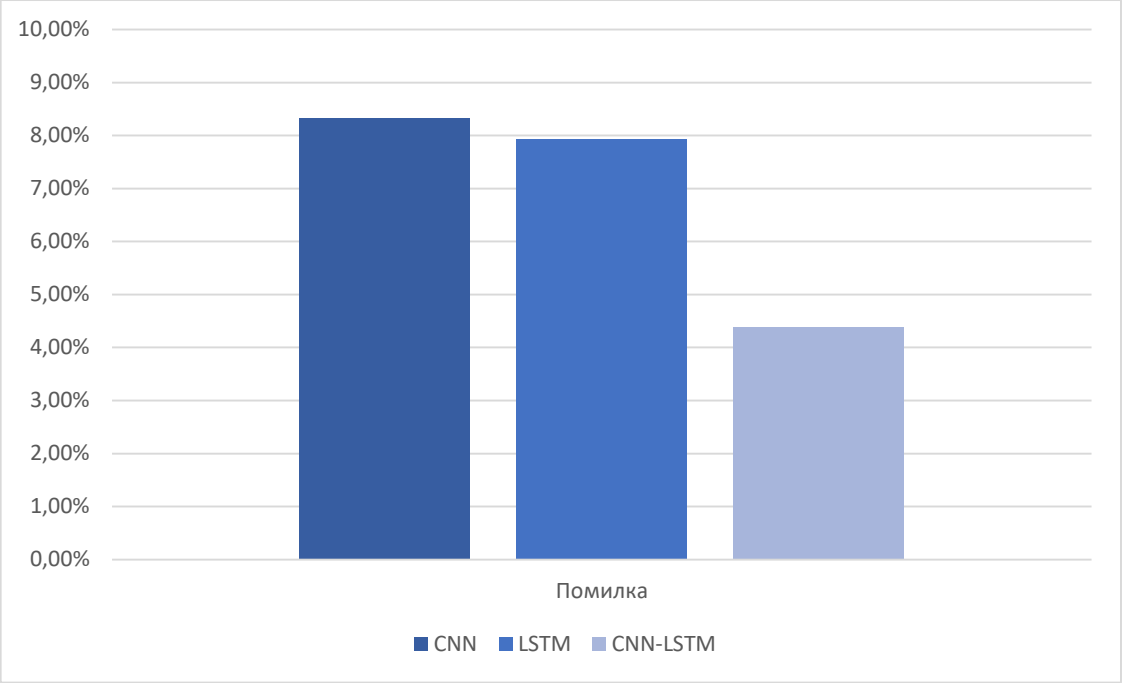

Рисунок 4.4 - Порівняння якості виявлення зловмисного трафіку нейронними мережами CNN, LSTM та CNN-LSTM за метрикою помилки

З метою оцінки достовірності результатів тестування нейронні мережі під'єднані у системі на одному рівні, як зображено на рис.4.5, де вхідний потік трафіку одночасно надсилається на три навчені штучні нейронні мережі.

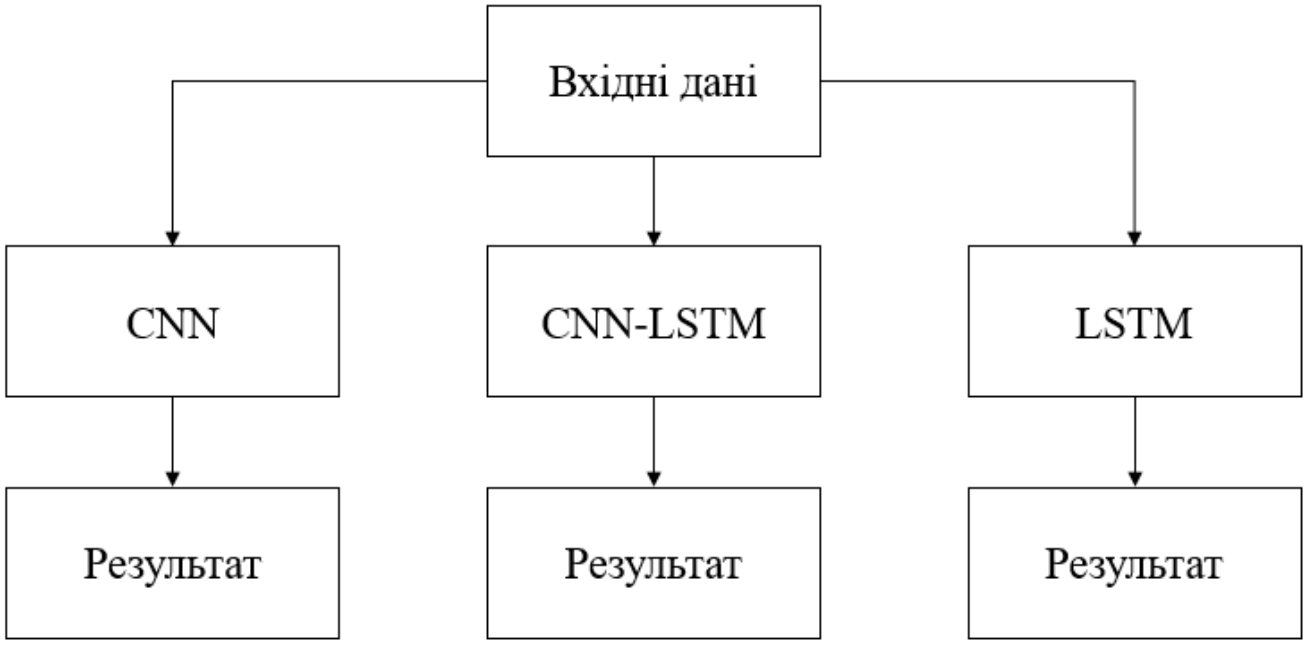

Рисунок 4.5 – Схема підключення нейромереж у системі

Для постановки експерименту у тестовому середовищі працює 10 користувачів, діяльність яких не була зловмисною. У мережі з використанням різних пристроїв у різні проміжки часу впродовж 6 годин було запущено 50 атак різних типів. Всього було запущено 10000 пакетів з яких 6000 пакетів вважаються безпечними та 4000 небезпечними. Дані експериментальних досліджень наведено у таблиці 4.4.

Таблиця 4.4 - Дані експериментальних досліджень для трьох нейромереж

	TP	TN	FP	FN
CNN	5640	3630	370	360
LSTM	5720	3580	420	280
CNN-LSTM	5840	3740	260	160

Повнота для CNN мережі склала:

$$Recall = \frac{5640}{5640 + 360} * 100\% = 94{,}00\% \tag{4.12}$$

Точність для CNN мережі склала:

$$Precision = \frac{5640}{5640 + 370} * 100\% = 93{,}84\% \tag{4.13}$$

Акуратність для CNN мережі склала:

$$Accuracy = \frac{5640 + 3630}{5640 + 3630 + 370 + 360} * 100\% = 92{,}7\% \tag{4.14}$$

Помилка для CNN мережі склала:

$$Specificity = \frac{370 + 360}{5640 + 3630 + 370 + 360} * 100\% = 7{,}3\% \quad (4.15)$$

F-метрика для CNN мережі склала:

$$F1\ score = \frac{94{,}00\% + 93{,}84\%}{2} = 93{,}92\% \quad (4.16)$$

Повнота для LSTM мережі склала:

$$Recall = \frac{5720}{5720 + 280} * 100\% = 95{,}33\% \quad (4.17)$$

Точність для LSTM мережі склала:

$$Precision = \frac{5720}{5720 + 420} * 100\% = 93{,}16\% \quad (4.18)$$

Акуратність для LSTM мережі склала:

$$Accuracy = \frac{5720 + 3580}{5720 + 420 + 280 + 3580} * 100\% = 93\% \quad (4.19)$$

Помилка для LSTM мережі склала:

$$Specificity = \frac{420 + 280}{5720 + 420 + 3580 + 280} * 100\% = 7\% \quad (4.20)$$

F-метрика для LSTM мережі склала:

$$F1\ score = \frac{95{,}33\% + 93{,}16\%}{2} = 94{,}25\% \quad (4.21)$$

Повнота для CNN-LSTM мережі склала:

$$Recall = \frac{5840}{5840 + 160} * 100\% = 97{,}33\% \quad (4.22)$$

Точність для CNN-LSTM мережі склала:

$$Precision = \frac{5840}{5840 + 260} * 100\% = 95{,}74\% \quad (4.23)$$

Акуратність для CNN-LSTM мережі склала:

$$Accuracy = \frac{5840 + 3740}{5840 + 260 + 160 + 3740} * 100\% = 95{,}8\% \quad (4.24)$$

Помилка для CNN-LSTM мережі склала:

$$Specificity = \frac{260 + 160}{5840 + 260 + 3740 + 160} * 100\% = 4{,}2\% \quad (4.25)$$

F-метрика для CNN-LSTM мережі склала:

$$F1\ score = \frac{97{,}33\% + 95{,}74\%}{2} = 96{,}54\% \quad (4.26)$$

Метриками було оцінено продуктивність трьох архітектур нейронних мереж. У таблиці 4.5 наведено результати оцінки цих архітектур з огляду на різні метрики. Розглянуті архітектури включають згорткову нейронну мережу, довгу короткострокову пам’ять та мережу, що складається із поєднання згорткової нейронної мережі та мережі довгої короткострокової пам’яті. Оцінка різних архітектур нейронних мереж дозволила визначити їхню ефективність у виявленні

зловмисного DNS-трафіку і визначити, яка з архітектур найкраще справляється з поставленою задачею.

Таблиця 4.5 - Порівняння результатів метрик ефективності під час експерименту роботи нейронних мереж CNN, LSTM та CNN-LSTM

test	Повнота	Точність	Акуратність	Помилка	F-метрика
CNN	94,00%	93,84%	92,70%	7,30%	93,92%
LSTM	95,33%	93,16%	93,00%	7,00%	94,25%
CNN-LSTM	97,33%	95,74	95,80%	4,20%	96,54%

На рисунку 4.6 представлено порівняння за метриками повноти, точності, акуратності та F-міри. Слід відмітити, що показник повноти у CNN-LSTM на 3,33% більший за відповідний показник у CNN та на 2% у LS5TM. Показник точності у CNN-LSTM більший на 1,9% у порівнянні з CNN та на 2,58% у порівнянні з LSTM. Акуратність роботи CNN-LSTM також має кращі показники у порівнянні з CNN та LSTM на 3,1% та 2,8% відповідно. F-метрика переважає у значеннях CNN-LSTM на 2,62% у порівнянні з CNN та на 2,29% у порівнянні з LSTM.

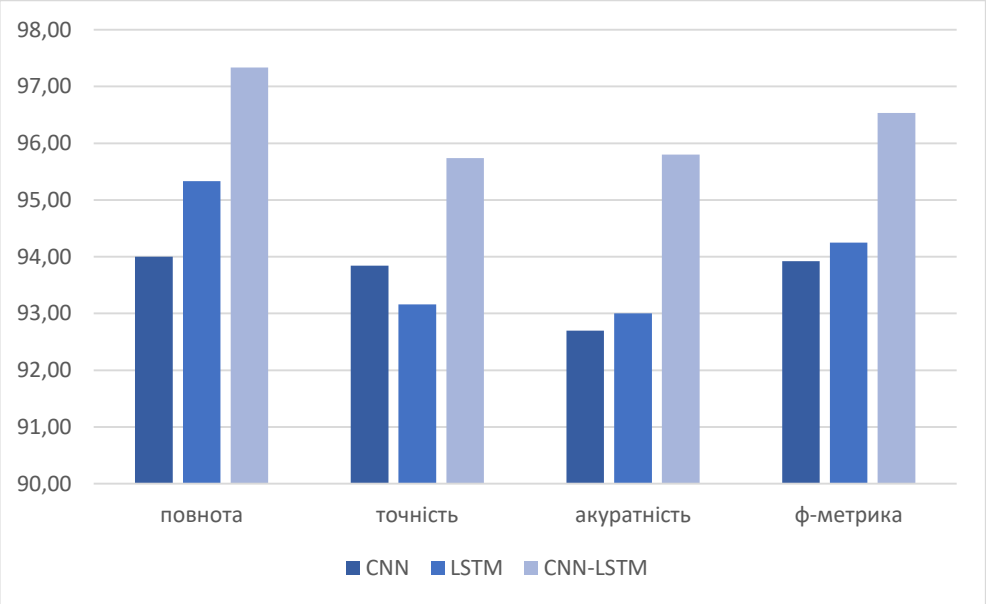

Рисунок 4.6 - Порівняння результатів метрик ефективності під час експерименту роботи нейронних мереж CNN, LSTM та CNN-LSTM

Як видно з рис.4.7 метрика помилки CNN-LSTM при порівнянні якості виявлення зловмисного трафіку з нейронними мережами CNN та LSTM менша на 3,1% та 2,8% відповідно.

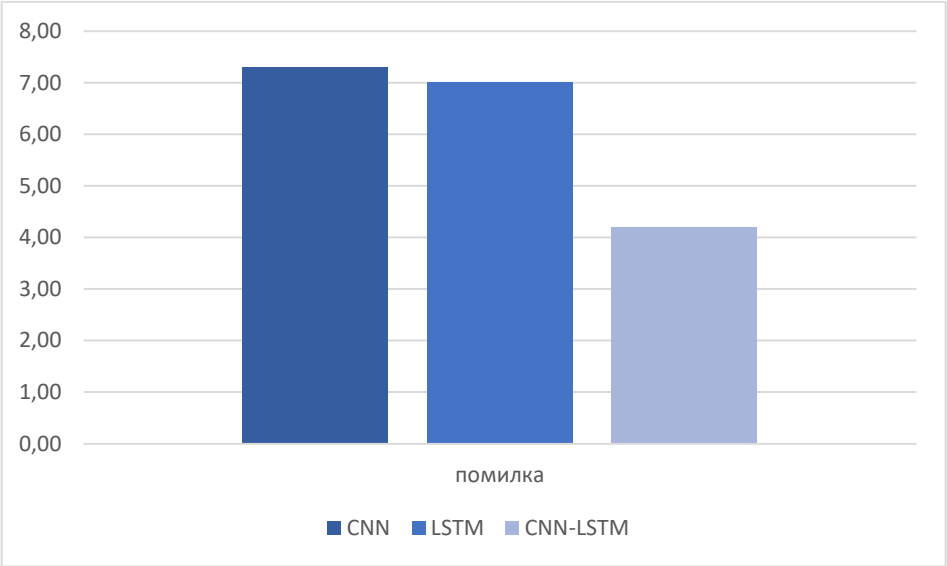

Рисунок 4.7 - Порівняння якості виявлення зловмисного трафіку нейронними мережами CNN, LSTM та CNN-LSTM за метрикою помилки

Результати порівняння метрик ефективності свідчать про те, що мережа CNN-LSTM має кращі показники у порівнянні з іншими мережами.

4.4 Висновки до розділу

В четвертому розділі розроблено нейронну мережу, що складається з поєднання архітектурних особливостей CNN та LSTM мереж.

Проведено навчання та тестування мережі CNN-LSTM з використанням набору даних KDD Cup 99. Результати роботи демонструють 97,19% повноти та 97,28% повноти при 4,38% помилок.

У третьому параграфі четвертого розділу проведено порівняння ефективності виявлення зловмисних дій при роботі різних мереж та визначено що мережа CNN-LSTM відображає кращий результат за всіма показниками.

ВИСНОВКИ

У рамках першого розділу було проведено класифікацію наявних загроз в комп'ютерних мережах, що становлять потенційну загрозу для користувачів та їх даних при використанні публічних мереж. Зокрема, було розглянуто особливості функціонування та застосування шкідливого програмного забезпечення, можливості реалізації атак на доступ та відмови в обслуговуванні, особливості розвідувальних атак та атак соціальної інженерії.

Було проведено аналіз наявних методів виявлення та ідентифікації порушника в інформаційно-комп'ютерних системах. Визначено, що часто використовуваним є сигнатурний метод, який має високий відсоток виявлення атак. Проте він є ефективним лише для відомих атак та потребує регулярного оновлення сигнатурних баз. Фрактальні аналізи для трафіку використовувати не доцільно, оскільки трафік у публічних мережах не є самоподібним. Експертні системи орієнтовані на вирішення вузьких задач, опираючись на наявні знання. Використовувати нечітку логіку рекомендовано якщо немає чітких меж, наприклад чіткого поділу всіх параметрів на «дозволене» та «заборонене». Проте слід розробляти велику кількість правил для одержання результату при всіх можливих значеннях усіх параметрів. Генетичні алгоритми не доцільно застосовувати для аналізу трафіку публічних мереж, оскільки для реалізації потрібно здійснювати інтенсивні обчислення, які можуть впливати на якість роботи мережі.

В межах першого розділу було проведено аналіз існуючих систем виявлення вразливостей та вторгнень. Наявні системи орієнтовані на захист мережі від стороннього зловмисного впливу та включають в себе виявлення аномалій, сигнатурний аналіз і аналіз вхідного та вихідного трафіку. Однак важко реалізувати системи, які можуть аналізувати вихідний трафік та вживати заходів у відповідь, оскільки це може вимагати великих ресурсів і відповідних прав доступу. Крім того, такі системи зазвичай застосовуються до захисту внутрішніх мереж підприємств і не використовуються для публічних сегментів мереж. Також проведено аналіз сучасних нейронних мереж та типи їх навчання.

У другому розділі описано особливості зловмисних дій у публічних мережах з використанням DNS-запитів, зокрема проаналізовано порти та протоколи, що можуть бути задіяні, інтенсивність трафіку та інше. Також обрано дві нейронні мережі, що найчастіше використовуються для схожого класу завдань: згорткову нейрону мережу та мережу довгокороткострокової дії. Визначено, що ці мережі відмінно підходять для аналізу мережевого трафіку та виявлення зловмисного трафіку. Розроблено алгоритми їх робити задля виконання поставленого завдання, визначено функції активації.

У третьому розділі було визначено та поділено записи набору даних KDD Kup 99 було поділено на навчальну та тестову вибірки задля подальшої роботи з нейронними мережами. Розгорнуто та описано тестове середовище у якому здійснено розгортання нейронних мереж з метою виявлення зловмисного трафіку. Також розгорнуто CNN та LSTM мережі. Проведено розрахунок ефективності цих мереж для виявлення зловмисного DNS-трафіку, що дозволило визначити, яка з них краще справляється з поставленою задачею.

Четвертий розділ містить опис реалізації нейронної мережі CNN-LSTM, зокрема розроблено алгоритм роботи мережі. Було навчено нейронну мережу та досліджено її ефективність.

Також у даному розділі проведено порівняння ефективності наявних розгорнутих нейромереж (CNN таLSTM) із розробленої мережею (CNN-LSTM). Визначено, що CNN-LSTM мережа має кращі показники точності та F-метрики при меншій кількості помилок.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Захист інформації в комп'ютерних системах: підручник / В. Д. Козюра та ін. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

2. Інформаційна безпека: навчальний посібник / Ю. Я. Бобало та ін. / за заг. ред. Ю. Я. Бобала та І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. - 580 с.

3. Cisco Talos. URL: https://cutt.ly/VwRyplFv (дата звернення: 8.09.2023).

4. Шматок О.С, Фіненко Ю.І, Єлізаров А.Б, Телющенко В.А. Класифікація загроз і ризиків сучасних інфокомунікаційних систем. *Вісник Університету «Україна». Серія: інформатика, обчислювальна техніка та кібернетика*. 2019. № 2 (23). С. 221-229. DOI: http://dx.doi.org/10.36994/2707-4110-2019-2-23-20

5. Dawadi, B.R.; Adhikari, B.; Srivastava, D.K. Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks. *Sensors.* 2023. Vol. 23, No 2. P. 2073. DOI: https://doi.org/10.3390/s23042073

6. Жаровський Р.О. Захист інформації у комп'ютерних системах : конспект лекцій. Тернопіль, 2019. - 268 с.

7. T. Guo, T. Zhang, E. Lim, M. López-Benítez, F. Ma, L. Yu. A Review of Wavelet Analysis and Its Applications: Challenges and Opportunities. *IEEE Access*. 2023. Vol. 10. PP. 58869-58903.

8. C. Zhang, H. Pan. Multi Resolution Prediction Model Based on Wavelet Analysis and Neural Network. *2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD).* 2021. PP. 299-303. DOI: 10.1109/ICAIBD51990.2021.9459082.

9. J. Hu Y. Zhang, C. Zou, J. Liu. Intrusion Prediction Algorithm Based on Modified Wavelet Neural Network. *4th International Conference on Information Communication and Signal Processing (ICICSP).* 2021, PP. 632-636. DOI: 10.1109/ICICSP54369.2021.9611991.

10. Tamara Radivilova, Lyudmyla Kirichenko, Maksym Tawalbeh, Andrii Ilkov. Виявлення аномалій в телекомунікаційному трафіку статистичними методами. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2021. №11, Том 3. с. 183-194.

11. Tianyu Wang, Li-Chiou Chen, Yegin Genc. A dictionary-based method for detecting machine-generated domains. *Information Security Journal: A Global Perspective*. 2021. Vol. 4. P. 205-218.

12. Zhengbing Hu, Roman Odarchenko, Sergiy Gnatyuk, Maksym Zaliskyi, Anastasia Chaplits, Sergiy Bondar, Vadim Borovik. Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior. *I. J. Computer Network and Information Security*. 2020, Vol. 6, PP.1-13. DOI: 10.5815/ijcnis.2020.06.01

13. P. Kumar, M. Tripathi, A. Nehra, M. Conti, C. Lal. SAFETY. Early Detection and Mitigation of TCP SYN Flood Utilizing Entropy in SDN. *IEEE Transactions on Network and Service Management*. 2018. Vol. 15, NO. 4. PP. 1545-1559. DOI: 10.1109/TNSM.2018.2861741.

14. T. Radivilova, L. Kirichenko, D. Ageiev and V. Bulakh. Classification Methods of Machine Learning to Detect DDoS Attacks. *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. 2019. PP. 207-210, DOI: 10.1109/IDAACS.2019.8924406.

15. Detection of DDoS attacks based on entropy-PCA in SDN. URL: https://hdl.handle.net/20.500.12939/2559 (дата звернення 17.09.2032).

16. L.Chen, Y. Deng. An improved evidential Markov decision making model. *Appl Intell*. 2022. Vol. 52. PP. 8008–8017.

17. P. Dymora, M. Mazurek. An Innovative Approach to Anomaly Detection in Communication Networks Using Multifractal Analysis. *Applied Sciences*. 2020. Vol. 10, No. 9. P. 3277.

18. Z. Chen, J. Zhu, S. Li, Y. Liu and T. Luo. Detection of False Data Injection Attacks on Load Frequency Control System with Renewable Energy Based on Fuzzy

Logic and Neural Networks. *Journal of Modern Power Systems and Clean Energy*. 2022. Vol. 10, No. 6. PP. 1576-1587. DOI: 10.35833/MPCE.2021.000546.

19. Vinícius de Miranda Rios, Pedro R.M. Inácio, Damien Magoni, Mário M. Freire. Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. *Computer Networks*. 2021. Vol. 186. PP. 1389-1286

20. R. Ghanbarzadeh, A. Hosseinalipour, A. Ghaffari. A novel network intrusion detection method based on metaheuristic optimisation algorithms. *J Ambient Intell Human Comput*. 2023. Vol. 14, PP. 7575–7592.

21. D. Mohamed, O. Ismael. Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing. *J Cloud Comp*. 2023. Vol. 12. P. 41.

22. J.B. Awotunde, F.E. Ayo, R. Panigrahi. A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks. *Int J Comput Intell Syst*. 2023. Vol. 16. P. 31.

23. S. Sheikhi, P. Kostakos. A Novel Anomaly-Based Intrusion Detection Model Using PSOGWO-Optimized BP Neural Network and GA-Based Feature Selection. *Sensors*. 2022. Vol. 22, No. 23. P. 9318.

24. A. Sahu, K. Davis. Inter-Domain Fusion for Enhanced Intrusion Detection in Power Systems: An Evidence Theoretic and Meta-Heuristic Approach. *Sensors*. 2022. Vol. 22, No. 6. P. 2100.

25. S. R. Khonde, V. Ulagamuthalvi. Blockchain: secured solution for signature transfer in distributed intrusion detection system. *Computer Systems Science and Engineering*. vol. 40, no.1, pp. 37–51, 2022.

26. A. Moubayed, M. Injadat, A. Shami. Optimized Random Forest Model for Botnet Detection Based on DNS Queries. *32nd International Conference on Microelectronics (ICM)*. 2020. PP. 1-4. DOI: 10.1109/ICM50269.2020.9331819.

27. А. Шевченко, Г. Застело, Є. Шпачинський. Аналіз застосування методів машинного навчання на основі штучних нейронних мереж для виявлення кіберзагроз. *Information Technology and Security*. 2019. Vol. 7, Iss. 1. DOI 10.20535/2411-1031.2019.7.1.184327

28. Тамара Савчук, Олександр Пупко. Класифікація даних за допомогою

нейронних мереж. *Вісник КрНУ імені Михайла Остроградського*. 2022. Випуск 2. ст. 55-60

29. Samuel Ndichu, Sylvester McOyowo, Henry Okoyo, Cyrus Wekesa. Detecting Remote Access Network Attacks Using Supervised Machine Learning Methods. *International Journal of Computer Network and Information Security(IJCNIS)*. 2023. Vol.15, No.2, PP. 48-61. DOI:10.5815/ijcnis.2023.02.04

30. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 https://tzi.com.ua/downloads/1.1-002-99.pdf

31. А.С. Янко, Р.А. Вигівський. Система захисту комп'ютерної мережі. Системи управління, навігації та зв'язку. Збірник наукових праць, 2022, 2(68), 91-94. https://doi.org/https://doi.org/10.26906/SUNZ.2022.2.091

32. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.99].

33. Ільєнко Анна Вадимівна, Ільєнко Сергій Сергійович, Кваша Діана Сергіївна, Мазур Яна Сергіївна. Практичні підходи щодо виявлення вразливостей в інформаційно - телекомунікаційних мережах. *Техніка науки про освіту в галузі кібербезпеки.* 2023. Випуск 3, Номер 19. DOI: 10.28925/2663-4023.2023.19.96108

34. International Journal of Soft Computing and Engineering. URL: https://www.ijitee.org/wp-content/uploads/papers/v8i11/I8206078919.pdf (дата звернення: 18.09.2023).

35. O. Abualghanam, H. Alazzam, B. Elshqeirat, M. Qatawneh, M. Almaiah. Real-Time Detection System for Data Exfiltration over DNS Tunneling Using Machine Learning. *Electronics*. 2023. Vol. 12, No. 6. P. 1467.

36. D. Sakhawat, A.N. Khan, M. Aslam, A.T. Chronopoulos. Agent-based ARP cache poisoning detection in switched LAN environments. *IET Netw*. 2019. Vol. 8. PP. 67-73.

37. Towards Securing Cloud Network using TreeRule Firewall. URL: https://www.ijitee.org/wp-content/uploads/papers/v8i9S4/I11420789S419.pdf (дата звернення: 14.09.2023).

38. M. Alicea, I. Alsmadi. Misconfiguration in Firewalls and Network Access Controls: Literature Review. *Future Internet*. 2021. Vol. 13, No. 11. P.283.

39. National Institute of Standards and Technology Special Publication 800-94 Natl. Inst. Stand. Technol. Spec. Publ. 800-94, 127 pages (February 2007)

40. F. Saidi, Z. Trabelsi, H. Ben Ghazela. Fuzzy Logic Based Intrusion Detection System as a Service for Malicious Port Scanning Traffic Detection. *IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*. 2019. PP. 1-9. DOI: 10.1109/AICCSA47632.2019.9035263.

41. Жилін А. В., Шаповал О. М., Успенський О. А.. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

42. A. Dakhgan, A. Hadi, J. Al Saraireh, D. Alrababah. Passive DNS Analysis Using Bro-IDS. *International Conference on New Trends in Computing Sciences (ICTCS).* 2017. PP. 121-126. DOI: 10.1109/ICTCS.2017.47.

43. I. Tereykovsky, A. Korchenko, T. Parashchuk, Y. Pedchenko. Open intrusion detection systems analysis. *Ukrainian Scientific Journal of Infor-mation Security*. 2018. Vol. 24, No. 3. PP. 201-216.

44. Субботін С. О. Нейронні мережі : теорія та практика: навч. посіб. Житомир : Вид. О. О. Євенок, 2020. – 184 с.

45. Нейронні мережі. Учбовий курс. URL: https://www.victoria.lviv.ua/library/students/nn/lecture.html (дата звернення: 20.09.2023).

46. Метод захисту трафіку від втручання dpi систем на базі використання doh та dot протоколів. URL: https://www.researchgate.net/publication/347886332_METOD_ZAHISTU_TRAFIKU_VID_VTRUCANNA_DPI_SISTEM_NA_BAZI_VIKORISTANNA_DOH_TA_DOT_PROTOKOLIV (дата звернення: 7.09.2023).

47. Микитишин А.Г., Митник М.М., Стухляк П.Д.. Комплексна безпека інформаційних мережевих систем : навч. посіб.. Львів : «Магнолія 2006», 2016. - 256 с

48. H. Alkahtani, T. H. Aldhyani. Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. *Secur. Commun. Netw*. 2021. DOI: 10.1155/2021/3806459

49. I. Ullah, Q. H. Mahmoud. Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks. *IEEE Access*. 2021. Vol. 9. PP. 103906–103926.

50. A. Salam, F. Ullah, F. Amin, M. Abrar. Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach. *Technologies*. 2023. Vol. 11, No. 4. P. 107.

51. F. Ullah, A. Salam, M. Abrar, M. Ahmad, F. Ullah, A. Khan, A. Alharbi, W. Alosaimi. Machine health surveillance system by using deep learning sparse autoencoder. *Soft Comput*. 2022. Vol. 26. PP. 7737–7750.

52. A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. Gomez. Attention is all you need. *In Proceedings of the 31st Conference on Neural Information Processing Systems (NIPS 2017)*. 2017. Vol. 30.

53. García, S.; Luengo, J.; Herrera, F. Data Preprocessing in Data Mining. *Springer*. 2015. Vol. 72. DOI: 10.1007/978-3-319-10247-4

54. S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, H. Gacanin. Hybrid deep learning for botnet attack detection in the internet-of-things networks. *IEEE Internet Things J*. 2020. Vol. 8. PP. 4944–4956.

55. Панчук Б.А. Виявлення бонет-трафіку на основі потоків, використовуючи ШІ // Проблеми програмування. 2022. № 3-4. С. 376-386.

56. A. K. Kumar, K. Vadivukkarasi, R. Dayana. A Novel Hybrid Deep Learning Model for Botnet Attacks Detection in a Secure IoMT Environment. *In Proceedings of the 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*. 2023. PP. 44–49.

57. A. Bashaiwth, H. Binsalleeh, B. AsSadhan. An Explanation of the LSTM Model Used for DDoS Attacks Classification. *Applied Sciences*. 2023. Vol. 13, No. 15. P. 8820.

58. A. Bibi, G. Sampedro, A. Almadhor, A. Javed, T. Kim. A Hypertuned

Lightweight and Scalable LSTM Model for Hybrid Network Intrusion Detection. *Technologies*. 2023. Vol. 11, No. 5. P. 121.

59. СОУ 207.01:2017. Текстові документи. Загальні вимоги. Хмельницький: ХНУ, 2017. 46 с. URL: https://msn.khnu.km.ua/pluginfile.php/466522/mod_resource/content/1/132_C%20T%20A%20H%20Д%20A%20P%20T%20чист%20.pdf

60. ДСТУ 8302:2015. Бібліографічне посилання. Загальні положення та правила складання. [Чинний від 2016-07-1]. Київ, 2016. 20 с. (Державна наукова установа ―Книжкова палата України імені Івана Федорова‖).

ДОДАТО Б ПЕРЕЛІК НАУКОВИХ ПРАЦЬ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

УДК 004.4

Тези доповідей

**VII Міжнародної науково-практичної конференції
до 30-ти річчя кафедри кібербезпеки та програмного забезпечення**

"Інформаційна безпека та комп'ютерні технології"

1 листопада 2023 року

Кропивницький 2023

УДК 004.4

Матеріали VII Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення: тези доповідей, 1 листопада 2023 р. – Кропивницький: ЦНТУ, 2023. – 135 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несуть автори.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

УДК 004.056

М.О. Ємець[1], Н.С.Петляк[1]
m.iemets@khmnu.edu.ua, npetlyak@khmnu.edu.ua
[1]Хмельницький національний університет, м. Хмельницький

ВИЯВЛЕННЯ ЗЛОВМИСНИКА В ПУБЛІЧНІЙ МЕРЕЖІ НА ОСНОВІ АНАЛІЗУ ВИХІДНИХ DNS-ЗАПИТІВ НЕЙРОННОЮ МЕРЕЖЕЮ

Однією з основних причин зростання кібератак є доступність технологій та інтернет-з'єднання для широкого кола людей і організацій. Загальнодоступні комп'ютерні мережі дозволяють користувачам легко підключатися до мережі Internet без обмежень. Але це також означає, що кіберзлочинці можуть використовувати анонімність і прихованість для виконання атак. Тому актуальним є питання аналізу дій користувачів у відкритих сегментах комп'ютерних мереж [1-2].

Статистичні дані різних організацій свідчать про те, що кількість атак які реалізуються за допомогою DNS-запитів суттєво зросла у 2022 році. Тому варто приділити особливу увагу аналізу саме DNS-запитів у публічних мережах [3].

Проведений аналіз наявних систем виявлення та запобігання вторгненням ефективно працює щодо різного роду загроз, проте вони націлені на захист системи від стороннього несанкціонованого впливу та не орієнтовані на аналіз роботи в середині мережі. А розгортання таких систем є дорогим та потребує наявності фахівця, що не доцільно для публічних мереж [4].

З метою виявлення зловмисних дій користувачами в публічній мережі стосовно ресурсів, що знаходяться поза мережею розроблено метод виявлення зловмисника на основі аналізу вихідних DNS-запитів. Послідовність роботи методу наступна:

1. отримання маршрутизатором DNS-запиту;
2. передача DNS-запиту на аналізатор;
3. аналіз DNS-запиту CNN-мережею;
4. передача отриманих результатів на LSTM шар;
5. формування висновку про пропуск/блокування пакету з DNS-запитом;
6. модифікація налаштувань маршрутизатора для дозволу або блокування запитів від користувача.

Вищеописаний метод реалізується за допомогою системи аналізу трафіку, яка у мережі буде знаходитися на одному рівні із DNS-сервером, щоб маршрутизатор зміг одночасно транслювати запити до сервера та системи. Схематично комп'ютерну мережу зображено на рис.1.

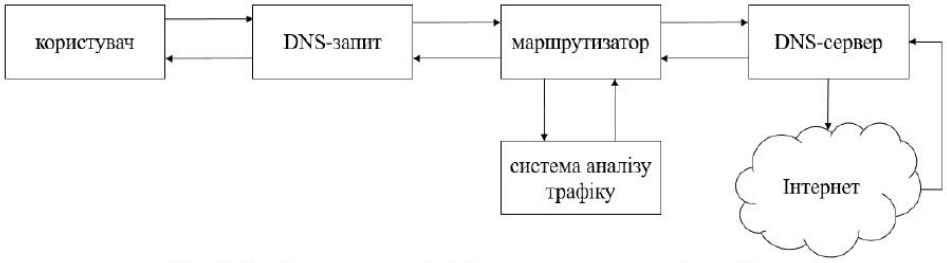

Рис. 1. Комп'ютерна мережа із під'єднаною системою аналізу трафіку

З метою дослідження ефективності запропонованого методу було розгорнуто локальне тестове середовище, що відокремлене від інших мереж та не становить небезпеки при запуску атак чи інших зловмисних дій. До проведення дослідження всі нейромережі були навчені та протестовані за допомогою набору даних KDD Kup 99, що широко використовується в дослідженнях і експериментах для розробки та оцінки систем виявлення вторгнень, а також для тестування алгоритмів машинного навчання. Вхідні дані одночасно надходили на три нейронні мережі: CNN, LSTM, CNN-LSTM. Схематично реалізацію підключення нейромереж зображено на рис.2. Далі відбувався аналіз запитів та виведення результатів роботи.

Під час експерименту було запущено 10 000 пакетів: 6 000 – безпечні, 4 000 – небезпечні. Дані експериментальних досліджень представлено у таблиці 1, де: TP – кількість пакетів, що визначено як зловмисні і вони дійсно такими є; TN – кількість пакетів, що визначено як нормальні і вони таким є; FP – кількість пакетів, що визначено як зловмисні, але вони не є такими; FN – кількість пакетів, що визначено як дозволені, але є зловмисними.

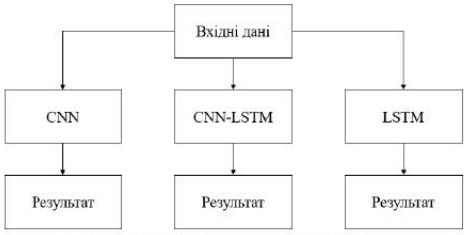

Рис. 2. Схема підключення нейромереж у системі

Таблиця 1

Дані експериментальних досліджень

	TP	TN	FP	FN
CNN	5640	3630	370	360
LSTM	5720	3580	420	280
CNN-LSTM	5840	3740	260	160

На основі даних із таблиці 1 було проведено розрахунки щодо метрик ефективності за трьома нейронними мережами. Точність дозволяє визначити, наскільки система правильно класифікує об'єкти або події як зловмисні без зайвих помилок та обчислюється як TP/(TP+FP). Акуратність вказує на загальну точність системи виявлення та рахується за формулою (TP+TN)/(TP+FP+FN+TN). Помилка вказує на здатність системи уникати хибних спрацьовувань, обчислюється як (FP+FN)/(TP+FP+TN+FN). F-метрика дозволяє врахувати FP та FN, обчислюється як середнє значення між точністю і повнотою. Результати відображено на рис.3.

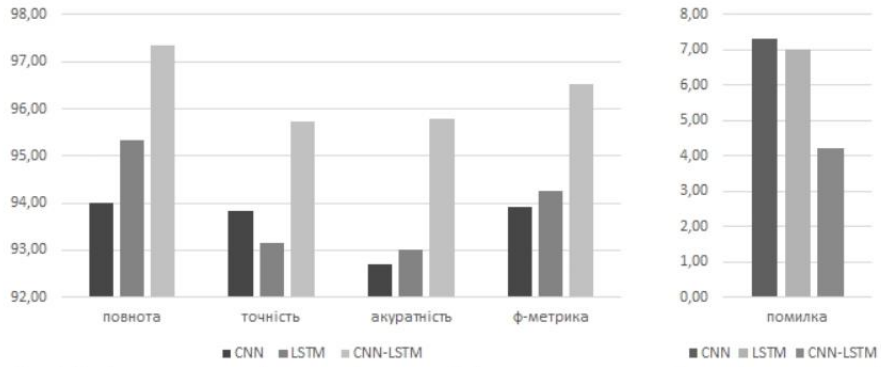

Рис. 3. Порівняння результатів метрик ефективності під час експерименту роботи нейронних мереж CNN, LSTM та CNN-LSTM

На основі отриманих даних можна зробити висновок, що поєднання CNN та LSTM мереж призвело до суттєвого покращення при роботі з DNS-запитами задля виявлення зловмисних дій у публічному сегменті мережі в порівнянні з роботою лише CNN чи лише LSTM мереж. Показник точності сягає 95,74% при F-метриці 96,54% та 4,2% помилок.

Список літератури

1. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

2. Шматок О.С, Фіненко Ю.І, Єлізаров А.Б, Телющенко В.А. Класифікація загроз і ризиків сучасних інфокомунікаційних систем. Вісник Університету «Україна». Серія: інформатика, обчислювальна техніка та кібернетика, № 2 (23), 2019, 221-229

3. T. Radivilova, L. Kirichenko, D. Ageiev and V. Bulakh, "Classification Methods of Machine Learning to Detect DDoS Attacks," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 207-210, doi: 10.1109/IDAACS.2019.8924406.

4. А. Шевченко, Г. Застело, Є. Шпачинський, Аналіз застосування методів машинного навчання на основі штучних нейронних мереж для виявлення кіберзагроз, Information Technology and Security. January-June 2019. Vol. 7. Iss. 1 (12) DOI 10.20535/2411-1031.2019.7.1.184327

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Ємця Максима Олександровича
ПІБ здобувача вищої освіти
студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

5.12.2023
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 121897 Назва: Метод виявлення порушника в мережі на основі аналізу вихідних DNS-запитів нейронною мережею Додано в БД: 2023-12-06 Автора: Ємець М.О. Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	85435	695	804 (1%)	11 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015975283

Дата перевірки:
06.12.2023 10:31:40 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.12.2023 10:46:49 EET

ID користувача:
100008300

Назва документа: **Ємець_плагіат**

Кількість сторінок: 76 **Кількість слів:** 13309 **Кількість символів:** 103160 **Розмір файлу:** 1.16 MB **ID файлу:** 1015654801

3.53%
Схожість

Найбільша схожість: 0.92% з Інтернет-джерелом (http://wiki.tneu.edu.ua/index.php?title=6_%D0%90%D1%82%D0%B0%D

3.26% Джерела з Інтернету	130	Сторінка 78
1.12% Джерела з Бібліотеки	128	Сторінка 79

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	2

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод виявлення порушника в мережі на основі аналізу вихідних DNS-запитів нейронною мережею

Автор: Ємець Максим Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Орленко Вікторія Сергіївна, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 3,53%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 0%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ В.С. Орленко

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Ємець Максим Олександрович

Тема Метод виявлення порушника в мережі на основі аналізу вихідних DNS-запитів нейронною мережею

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 82

1. Короткий зміст роботи та прийнятих В рамках роботи проведено дослідження проблем виявлення порушників у публічних сегментах мережі. В роботі поставлено та вирішено наступні задачі: проаналізувати наявні методи виявлення та ідентифікації порушників; дослідити поширені системи запобігання та виявлення вразливостей та вторгнень; дослідити ефективність та переваги, недоліки CNN та LSTM мережі для виявлення зловмисного DNS-трафіку; розробити метод виявлення зловмисного вихідного DNS-трафіку шляхом аналізу запитів у публічному сегменті мережі нейронною мережею

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми дослідження; її зв'язок із науковими програмами, планами, темами та сформульовано мету та основні завдання дослідження. У першому розділі було описано класифікацію мережевих загроз та досліджено наявні методи виявлення порушника в комп'ютерних мережах та систем запобігання та виявлення вразливостей та вторгнень. У другому розділі описано особливості реалізації атак із використанням DNS-запитів, застосування CNN та LSTM мереж для виявлення зловмисних дій у мережі. У третьому розділі розроблено метод виявлення порушника на основі аналізу вихідних DNS-запитів, визначено набір даних за допомогою якого буде здійснюватися навчання та тестування нейронних мереж, описано тестове середовище для проведення експериментів, проведено оцінку ефективності CNN та LSTM для вирішення поставленого завдання. У четвертому розділі представлено схему роботи CNN-LSTM мережі, проведено оцінку її ефективності та доведено наявність кращих результатів у порівнянні з використанням вищевказаних мереж.

4. Позитивні сторони роботи проекту полягають у зменшенні кількості атак реалізованих за допомогою публічних сегментів мереж.

5. Негативні сторони роботи У роботі не висвітлено шляхи впровадження та можливість оновлення системи в разі необхідності.

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що дипломна робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор Мартинюк Валерій Володимирович.

« 8 » грудня 2023 року _____ (підпис)