Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Гордєєва Богдана Віталійовича

на здобуття ступеня вищої освіти Бакалавра

Система виявлення вторгнень у мережі

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.2101018.20.01.04ПЗ

Виконав студент 4 курсу група КБ-20-1 Богдан ГОРДЄЄВ
Керівник канд. техн. наук, доцент Вікторія ОРЛЕНКО
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

12. 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гордєєву Богдану Віталійовичу

1 Тема роботи Система виявлення вторгнень у мережі

Керівник роботи к.т.н. доцент Вікторія ОРЛЕНКО

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 12.06.2024

3 Вихідні дані до роботи Змоделювати систему виявлення вразливостей у мережі за допомогою Matlab з використанням нечіткої логіки. Розробити схему включення системи в комп'ютерну мережу. Розробити алгоритм роботи системи виявлення вторгнень. Розгорнути тестове середовище для проведення оцінки ефективності. Провести розрахунок ефективності розробленої системи на основі проведених тестувань.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Огляд предметної області. Класифікація мережевих атак. Протоколи для віддаленого доступу. Аналіз існуючих систем виявлення вторгнень. Проектування системи виявлення вторгнень. Опис методів. Набір даних. Алгоритм роботи системи. Побудова комп'ютерної мережі із застосуванням системи. Реалізація системи виявлення вторгнень у мережі. Навчання нейронної мережі. Оцінка ефективності.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Моделювання системи виявлення вторгнень у мережі засобами Matlab. Алгоритм роботи системи виявлення вторгнень у мережі. Оцінка достовірності роботи системи виявлення вторгнень у мережі.

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент Богдан ГОРДЄЄВ

Керівник кваліфікаційної роботи Вікторія ОРЛЕНКО

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система виявлення вторгнень у мережі»

Автор роботи: студент групи КБ–20–1 Гордєєв Б.В.

Керівник роботи: к.т.н. доц. Орленко В.С.

Пояснювальна записка: 63с., 20 рисунки, 12 таблиць, 43 джерел, 3 креслення.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: КІБЕРПОЛІГОН, АТАКА, КОМП'ЮТЕРНА МЕРЕЖА, ПОЛІТИКА БЕЗПЕКИ, МОНІТОРИНГ МЕРЕЖЕВОГО ТРАФІКУ.

У даній кваліфікаційній роботі було здійснено розробку системи виявлення вторгнень у мережі. В ході роботи виконано наступні завдання: сформовано сигнатури пакетів даних мережевого трафіку; створено детальний алгоритм аналізу мережевого трафіку та виявлення зловмисних з'єднань; сформовано набір правил, які можуть однозначно класифікувати адміністратора мережі використовуючи для моделювання засоби Matlab; навчено нейронну мережу для виявлення бекдорів у трафіку; розроблено схему інтеграції розробленої системи виявлення вторгнень у мережі в існуючу комп'ютерну мережу, враховуючи необхідність мінімізації впливу на продуктивність мережі; налаштовано тестове середовище для перевірки різних сценаріїв кібератак; проведено аналіз результатів тестувань для оцінки ефективності розробленої системи.

10.06.2024

ABSTRACT

Topic of the qualification work: "Network intrusion detection system"

Author: student of group KB-20-1, Gordeev B. V.

Supervisor: Ph.D., Associate Professor Orlenko V. S.

Explanatory note: 63 pages, 20 figures, 12 tables, 43 sources, 3 diagrams.

LIST OF KEYWORDS: CYBER RANGE, ATTACK, COMPUTER NETWORK, SECURITY POLICY, NETWORK TRAFFIC MONITORING.

This qualification work involves the development of a network intrusion detection system. The tasks completed during the work include: the formation of data packet signatures for network traffic; creation of a detailed algorithm for analyzing network traffic and detecting malicious connections; formulation of a set of rules that can unambiguously classify network administrators using Matlab for modeling; training a neural network to detect backdoors in traffic; development of a scheme for integrating the developed intrusion detection system into the existing computer network while considering the need to minimize the impact on network performance; setting up a test environment to check various cyberattack scenarios; conducting an analysis of the test results to evaluate the effectiveness of the developed system.

10.06.2024

ЗМІСТ

ВСТУП

Проблема зловмисного трафіку в мережі полягає в тому, що кібератаки стають все більш розповсюдженими та руйнівними, постійно еволюціонуючи та знаходячи нові шляхи для проникнення в інформаційні системи. З розвитком технологій збільшується і кількість вразливостей, які можуть бути використані зловмисниками для проведення атак. Саме тому розробка систем виявлення та запобігання вторгнень стає критично важливою для забезпечення кібербезпеки.

Дана кваліфікаційна робота спрямована на розробку системи виявлення вторгнень у мережі шляхом налаштування віддаленого доступу.

До завдань, які потрібно виконати в рамках роботи, варто віднести:

– використати засоби Matlab та нечіткої логіки для створення прототипу майбутньої системи, оскільки нечітка логіка дозволяє обробляти невизначеність та імітувати людське мислення при прийнятті рішень в умовах невизначеності, що є доречним при аналізі мережевого трафіку, де поведінка може бути аномальною, але не обов'язково зловмисною;

– описати спосіб включення розробленої системи у наявну комп'ютерну мережу. Важливо врахувати, що система повинна бути інтегрована таким чином, щоб не вплинути на продуктивність мережі, водночас забезпечуючи ефективне виявлення потенційних загроз;

– створити детальний алгоритм, який визначає, як система буде аналізувати мережевий трафік і визначати потенційні зловмисні з’єднання. Алгоритм має включати методи виявлення зловмисних пакетів, аналіз поведінки мережі та відповідні реакції на виявлені загрози;

– налаштування тестової платформи, де будуть випробовуватися різні сценарії кібератак для перевірки ефективності та надійності системи. Тестування дозволить внести необхідні корективи перед повною інтеграцією;

– проведення аналізу результатів тестувань для оцінки ефективності розробленої системи.

1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Класифікація мережевих атак

Мережеві атаки - це спроби незаконного доступу до мережевих ресурсів, даних чи систем, з метою порушення їх цілісності, конфіденційності або доступності за допомогою програмних чи апаратних засобів [1].

Класифікацію мережевих атак [2-8] зображено на рисунку 1.1.

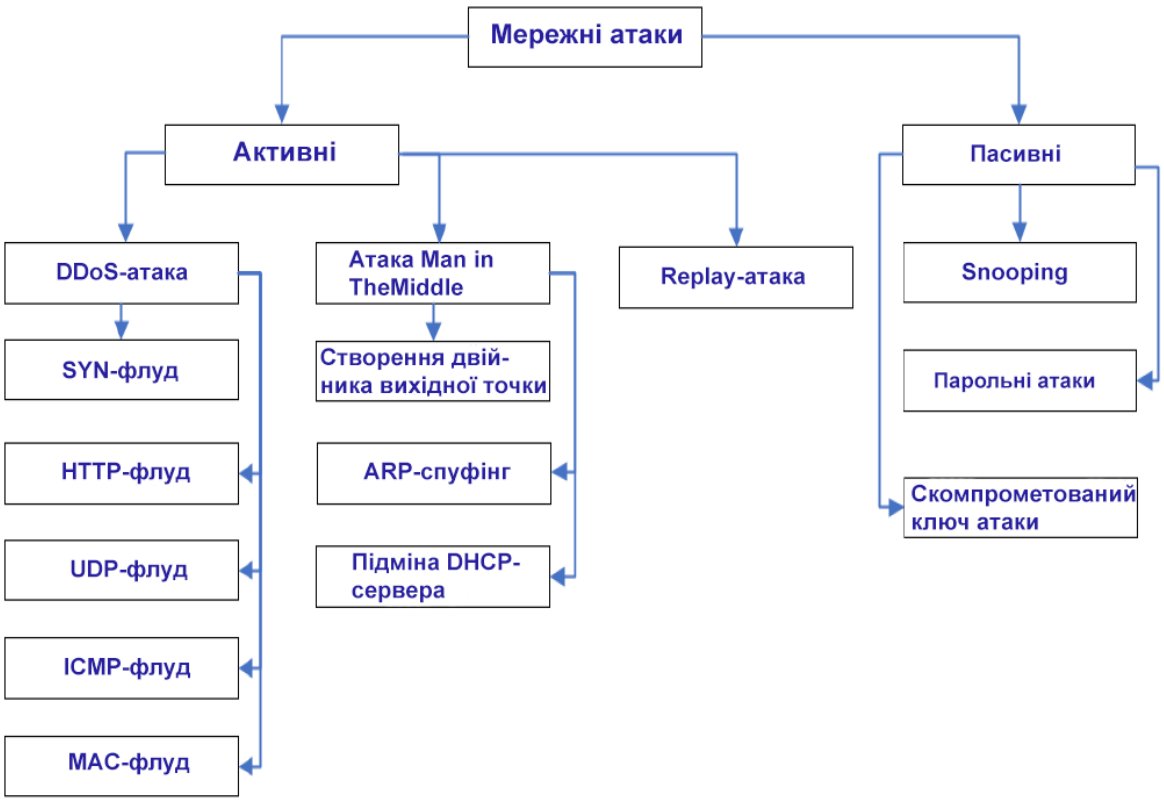


Рисунок 1.1 - Класифікація мережевих атак

Перехоплення пакетів є формою мережевої атаки, при якій зловмисник отримує доступ до пакетів даних, які пересилаються через мережу. Ця атака дозволяє зловмиснику зловживати конфіденційними даними, такими як паролі або номери кредитних карток, якщо передача даних не зашифрована. Зловмисник може аналізувати і змінювати зміст перехоплених пакетів, що ставить під загрозу

приватність та безпеку користувачів мережі [9-11]. Найпоширенішими методами є: sniffing, ARP Spoofing, DNS Spoofing.

Атаки на паролі використовуються для незаконного отримання доступу до комп’ютерів, систем або акаунтів користувачів. Ці атаки спираються на те, що багато користувачів використовують слабкі, часто використовувані або легко вгадувані паролі, що робить їх вразливими до злому. Існують два основних типи атак на паролі: атака на основі словника та атака грубою силою. Під час атаки на основі словника зловмисник використовує словник або список часто використовуваних паролів для спроби зламати пароль. Він послідовно перевіряє кожне слово зі словника, намагаючись знайти відповідність з паролем користувача. Цей метод ефективний, якщо пароль занадто слабкий або широко використовуваний. Під час атаки грубою силою зловмисник спробує всі можливі комбінації символів, цифр і літер, щоб знайти правильний пароль. Це означає, що зловмисник буде випробовувати кожну можливу комбінацію паролю. Цей метод є найбільш часо- та ресурсоємним, але дозволяє зловмиснику зламати найбільш складні паролі [12-14].

Сканування портів - це метод мережевої атаки, в якому зловмисник намагається визначити, які служби або програми працюють на цільовому комп'ютері шляхом сканування TCP/UDP портів. За допомогою цього сканування зловмисник спробує встановити з'єднання з різними портами на цільовому комп'ютері для виявлення, які з них відкриті. Виявивши відкриті порти TCP/UDP, зловмисник може дізнатися, які служби чи програми працюють на цільовому комп'ютері, а також які програмні продукти використовуються. В остаточному підсумку, ця інформація може допомогти зловмиснику здійснити атаку на вразливості в програмному забезпеченні цільового комп'ютера та, можливо, зламати його. Такі атаки можуть бути виконані з метою отримання несанкціонованого доступу до системи або для виконання інших шкідливих дій на цільовому комп'ютері. Додатково, сканування портів часто використовується як попередній етап більш складних атак, таких як SQL ін'єкції чи переповнення буфера, які можуть використовувати слабкі місця специфічних служб, знайдених

під час сканування. Важливим заходом захисту від таких атак є використання брандмауерів, налаштування правил для обмеження доступу до необхідних портів та постійне оновлення програмного забезпечення, щоб запобігти експлуатації відомих вразливостей [15-17].

Перевірка ping, відома також як "ping-сканування", представляє собою метод мережевої атаки, при якому зловмисник надсилає ping-пакети типу ICMP ECHO до різних IP-адрес у мережі з метою визначити, які з них відповідають пакетами типу ICMP ECHO REPLY [18]. Це дозволяє зловмиснику виявити активні комп'ютери в мережі, а також виявити відсутність відповіді від певних IP-адрес. Ця інформація може бути використана для ідентифікації потенційних цільових комп'ютерів для подальших атак або для виявлення вразливостей в мережевій інфраструктурі. Потенційно зловмисник може використати результати перевірки ping для складання списку активних IP-адрес і подальшого проведення цільових атак, таких як сканування портів або впровадження шкідливих програм.

Dumpster diving - це процес пошуку корисної інформації для зловмисників у сміттєвих контейнерах компанії, яка може бути використана для атак на їхню мережу або системи [19]. Наприклад, під час dumpster diving може бути виявлена інформація, така як імена співробітників, документи з внутрішніми процедурами компанії, відомості про продукти програмного забезпечення, моделі пристроїв мережевої інфраструктури та інше. Ця інформація може бути використана для проведення соціально-інженерних атак або як джерело для підготовки більш точно спрямованих мережевих атак. Наприклад, зловмисник може використовувати отриману інформацію для аналізу мережевої інфраструктури та ідентифікації слабких місць, що дозволить їм ефективніше здійснювати атаки на цільові системи.

Кейлоггер - це тип програмного забезпечення для спостереження, яке вважається або шпигунським програмним забезпеченням, або законним інструментом моніторингу, залежно від того, як воно використовується. Він записує кожне натискання клавіш на клавіатурі комп’ютера у файл журналу, зазвичай без відома користувача. Цей журнал може містити будь-який тип

введеної інформації, як-от електронні листи, паролі, миттєві повідомлення та пошукові запити в Інтернеті. Кейлоггери можуть бути програмними або апаратними. Програмні кейлоггери – це програми, інстальовані на комп'ютері, часто зловмисно, для моніторингу та запису натискань клавіш. З іншого боку, апаратні кейлоггери — це фізичні пристрої, які можна під'єднати до клавіатури комп'ютера або вбудувати в апаратне забезпечення для виконання того самого завдання. Основним використанням клавіатурних шпигунів є отримання несанкціонованого доступу до конфіденційних даних, таких як паролі та інформація про кредитні картки, що може призвести до крадіжки особистих даних і фінансового шахрайства. Однак існують також легальні програми клавіатурних шпигунів, як-от програмне забезпечення для батьківського контролю, яке дозволяє батькам стежити за діяльністю своїх дітей в Інтернеті, або інструменти, які використовують роботодавці для нагляду за використанням працівниками комп'ютерів компанії для забезпечення продуктивності та безпеки. Незалежно від наміру, використання клавіатурних шпигунів викликає значні проблеми конфіденційності та етики та регулюється в багатьох юрисдикціях. Дуже важливо переконатися, що їх використання відповідає правовим стандартам і поважає права особи на конфіденційність [20-22].

Соціальна інженерія - це метод атаки, при якому особа з високим рівнем майстерності в міжособистісних взаємодіях маніпулює іншими з метою отримання конфіденційної інформації про мережу, яка потім може бути використана для крадіжки даних. Ці атаки можуть включати в себе відправку фішингових електронних листів, телефонні дзвінки, відвідування особисто або інші способи взаємодії з потенційною жертвою. Мета соціальної інженерії - залучити людей до розголошення конфіденційної інформації або виконання дій, що можуть створити вразливості в мережі або системах безпеки. Наприклад, соціальні інженери можуть вигадати схеми, що надихають довіру, або створювати фальшиві ситуації, щоб отримати доступ до облікових даних або паролів. Особливо небезпечні атаки соціальної інженерії, оскільки вони можуть обходити технічні заходи безпеки, які існують у мережі [23-24].

1.2 Вразливості комп’ютерної мережі

Вразливість - це слабкість або недолік у системі, програмному забезпеченні або алгоритмі, який може бути використаний зловмисниками для здійснення атаки або порушення безпеки. Вразливості можуть виникати через помилки в дизайні, програмуванні, конфігурації або експлуатації системи. Це може бути незахищений доступ до конфіденційної інформації, можливість виконання небажаних дій або втручання у роботу системи. Вразливості можуть бути використані зловмисниками для здійснення різних видів атак, таких як витік даних, внедрення коду, аутентифікаційні атаки тощо.

CWE (Common Weakness Enumeration) — це система класифікації вразливостей безпеки, які призводять до вразливостей у програмних продуктах. Mitre CWE підтримується Національним відділом кібербезпеки та US-CERT. Він упорядковує недоліки та дефекти за понад 600 категоріями, намагаючись їх усунути, скеровуючи розробників у створенні більш стійких продуктів. Системи організації безпеки, автоматизації та реагування (SOAR) використовують CWE для автоматизації процесів відновлення [25]. Оцінка CVSS, що коливається від 0,0 до 10,0, показує ступінь серйозності вразливості, від найменшої до найбільш серйозної. Фахівці з безпеки можуть використовувати списки CWE для виявлення та усунення вразливостей. Кожен CWE містить різні шаблони атак і пов’язані з ними недоліки, що дозволяє організаціям налаштовувати системи виявлення на основі їх толерантності до ризику. CWE полегшує ідентифікацію загальних уразливостей у різних мовах, апаратному забезпеченні, доменах і архітектурних принципах. Прозорість є ключовим елементом ініціативи CWE, що забезпечує відкритість щодо процесу розробки та джерел, які використовуються для списку CWE. Така прозорість зміцнює довіру між учасниками Спільноти CWE та заохочує включення CWE у їхні практики. Крім того, прозорість поширюється на майбутніх користувачів, надаючи їм можливість переглянути та дізнатися про процес створення списку CWE. Для досягнення цієї мети вихідні документи, використані для створення Списку CWE, будуть доступні на веб-сайті.

CVE (Common Vulnerabilities and Exposures) - це база даних, що містить інформацію про відомі уразливості в інформаційній безпеці. Кожній уразливості присвоюється унікальний ідентифікаційний номер у форматі CVE-рік-номер, а також містить опис і ряд загальнодоступних посилань з описом [26]. Цей перелік використовується IT-спеціалістами та дослідниками безпеки для отримання детальної інформації про вразливості та визначення пріоритетів у їх виправленні на основі оцінки вразливостей. Інформація про вразливість CVE розміщена на веб-сайті організації CVE (https://cve.mitre.org/), некомерційної організації, що була заснована Массачусетським технологічним інститутом у 1999 році. Ця інформація є загальнодоступною.

Веб-сайт CVE надає обмежену інформацію, і CVE в основному використовується для призначення унікальних ідентифікаторів. Щоб отримати додаткову інформацію про вразливості потрібно звернутися до інших ресурсів, таких як веб-сайти постачальників IT та інші бази даних вразливостей. Застосування CVE у продуктах безпеки передбачає ефективне оновлення інформації про вразливості під час розробки продуктів, щоб допомогти їм виявити якнайбільше вразливостей CVE та забезпечити безпеку користувачів мережі.

Common Vulnerability Scoring System (відома також як CVSS Scores) - загальна система оцінки вразливостей, яка забезпечує числове представлення серйозності вразливості інформаційної безпеки у межах від 0 до 10. Оцінка 0 позначає менш важливу вразливість, у порівнянні з оцінкою 10, яка означає найвищий рівень серйозності [27]. Оцінки CVSS зазвичай використовуються командами інформаційної безпеки як частина програми керування вразливостями, щоб встановити точку порівняння між вразливостями та визначити пріоритети усунення цих вразливостей. CVSS є відкритою структурою, яка підтримується Форумом груп реагування на інциденти та безпеки (FIRST), некомерційною організацією зі штаб-квартирою в США, що налічує понад 500 організацій-членів по всьому світу. Використовуючи CVSS для встановлення пріоритетів уразливостей, потрібно спочатку звернутися до найкритичніших і зменшити загальний ризик для організації. Оцінка CVSS враховує багато факторів,

включаючи вектор атаки, складність атаки, потрібні привілеї, взаємодію з користувачем, область застосування, конфіденційність, цілісність та доступність.

Вразливість мережі визначається як будь-яка слабка точка або недолік у програмному забезпеченні, апаратному забезпеченні або організаційних процесах. Ці вразливості стають джерелом потенційних загроз безпеці, оскільки їх можна використовувати для несанкціонованого доступу або атак на мережеву інфраструктуру. Наприклад, вразливість в програмному забезпеченні може дозволити хакерам використовувати шкідливий код для проникнення в систему та отримання незаконного доступу до конфіденційної інформації. Однак вразливості також можуть виникати через недостатній контроль доступу або погане керування конфігурацією пристроїв, що також може створювати ризики для безпеки мережі.

Гетерогенна мережа - це мережа, яка складається з різних типів пристроїв, програмного забезпечення, архітектур і технологій. У гетерогенних мережах можуть бути використані різноманітні комп'ютери, сервери, маршрутизатори, комутатори, мобільні пристрої та інші пристрої з різними операційними системами, мережевими протоколами та конфігураціями. Гетерогенні мережі можуть виникати через різноманітність технологій, які використовуються в організації з різними потребами та вимогами. Такі мережі можуть бути складними для управління та підтримки через різницю в характеристиках і налаштуваннях пристроїв, а також можуть потребувати спеціалізованих методів інтеграції для забезпечення взаємодії між різнорідними компонентами. Слід зазначити, що переважна більшість комп’ютерних мереж є саме гетерогенними. Тому безпеку мережі потрібно розглядати не лише як єдиний цілісний об’єкт, а й аналізувати вразливості окремих компонентів. Важливо впроваджувати різні рівні безпеки та засоби захисту, які враховують специфіку кожного компонента мережі. Наприклад, застосування багаторівневих систем виявлення інтрузій та засобів шифрування може значно підвищити безпеку даних, що передаються через мережу. Також рекомендується проводити регулярні аудити безпеки для ідентифікації та усунення потенційних вразливостей у мережі, що може включати все від простих оновлень програмного забезпечення до складних процедур зміни

конфігурації обладнання. Приклад такої мережі із різними вразливостями на кінцевих пристроях показано на рисунку 1.2 [28].

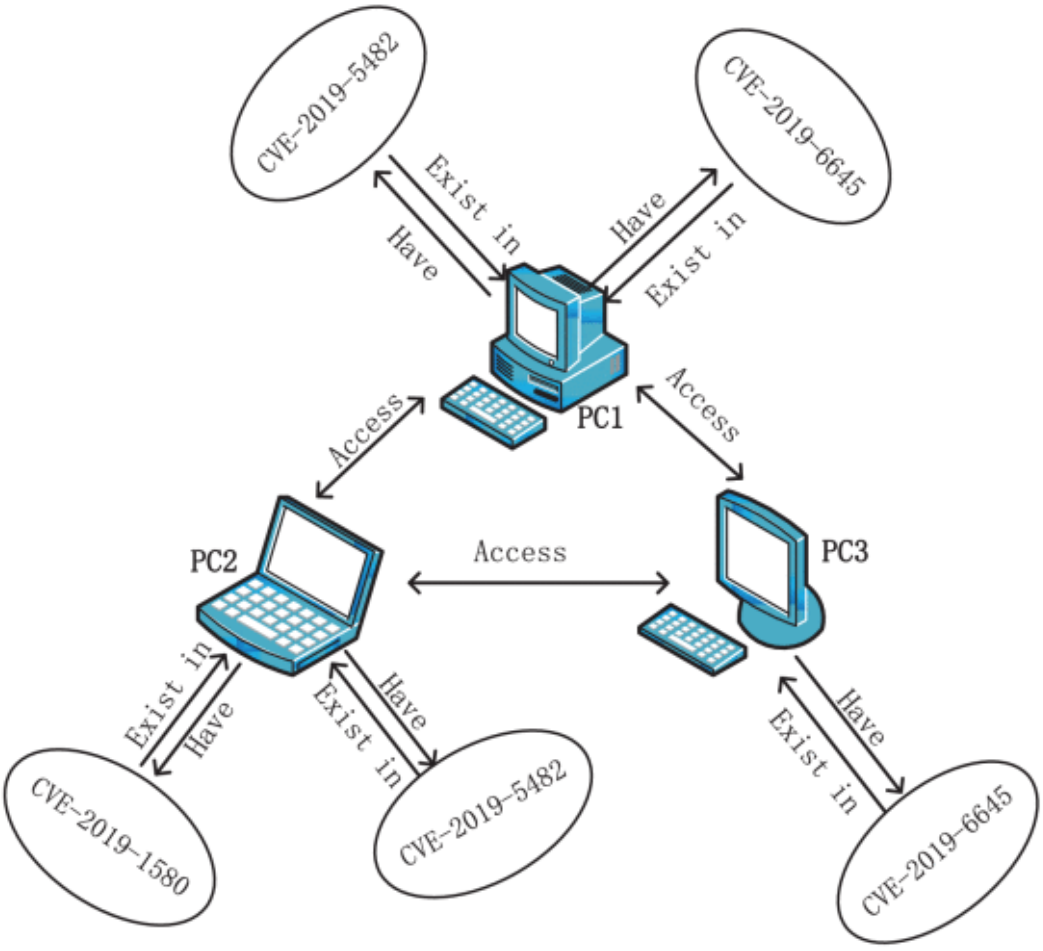


Рисунок 1.2 – Гетерогенна мережа із різними вразливостями на кінцевих пристроях

Якщо зловмисник планує, до прикладу, атаку на базу даних, то реалізувати атаку можна двома варіантами:

– намагатися знайти вразливості сховища із даними та експлуатувати їх задля проникнення й подальшої несанкціонованої роботи над даними;

– знайти вразливість будь-якого кінцевого пристрою в мережі та експлуатувати її задля проникнення в мережу, а далі проникати до сховища із даними та здійснювати несанкціоновані дії над ними у якості локального користувача мережі.

Приклад мережі із можливими шляхами проникнення у мережу показано на рисунку 1.3.

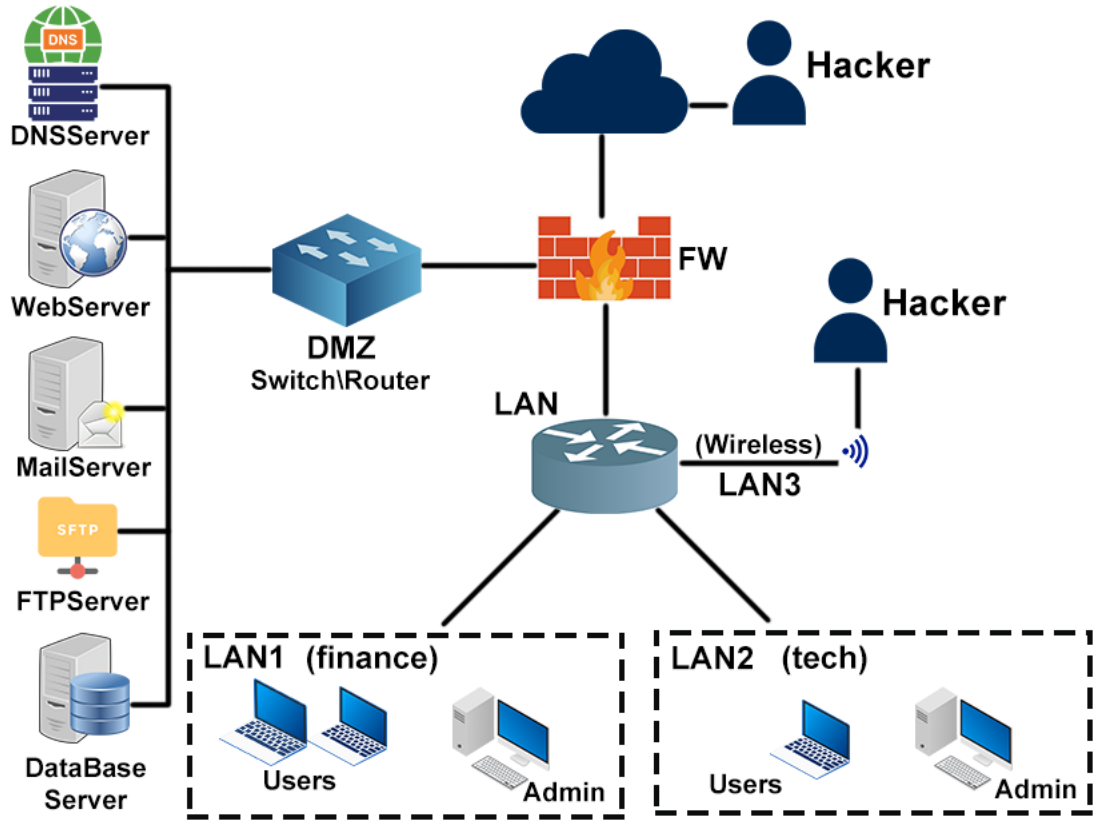


Рисунок 1.3 - Можливі шляхи проникнення у мережу

Перший тип несанкціонованого доступу до мережі доцільно використовувати якщо є достатня кількість ресурсів та часу для реалізації атаки. Оскільки серверне обладнання та центральні комутуючі пристрої зазвичай мають достатній рівень захисту від зовнішніх користувачів, адміністратори здійснюють аналіз мережевої активності та вчасне оновлення програмних продуктів.

При другому типі зловмисник може при менших затратах часу та ресурсів швидше реалізувати атаку. Адже дослідження вказують на те, що кінцеві пристрої мають нижчий рівень захисту та необізнаність користувачів. Прикладом може слугувати відкриття фішингового файлу працівником відділу кадрів через необізнаність при вимкненому антивірусному програмному продукті, оскільки той забороняв перехід на певні веб-ресурси в особистих цілях. Після проникнення

у мережу, зловмисник може діяти як локальний користувач, що дасть змогу обминути ряд параметрів захисту кінцевої потрібної цілі.

Тому є актуальним виявлення несанкціонованого віддаленого доступу до мережі. Адже несанкціонований віддалений доступ може слугувати у якості backdoor, оскільки їх створення є першочерговим завданням зловмисника. Наявність backdoor дає змогу зловмиснику приєднуватися до мережі повторно. Їх виявлення зможе призупини атаку на кінцевий об’єкт атаки (до початку безпосередньої атаки на кінцевий об’єкт атаки) чи пом’якшити атаку (у разі початку реалізації атаки на кінцевий об’єкт атаки).

Проявами використання backdoor може бути:

– передача зашифрованого backdoor-файлу;

– запуск нового процесу для створення підпроцесів, багатопроцесорного керування кількома процесами та генерування псевдотерміналу pty;

– читання та запис системних файлів;

– заміна загальних системних командних файлів, щоб отримати системні дозволи (читання та запису в пам’ять «StringIO», копіювання файлу «shutil», блокування файлу «fcntl» і функції сімейства «exec»);

– виконання системних команд, зокрема функцій «system», «command», «exec_command»;

– моніторинг системи та отримання інформації про неї, включаючи використання системного моніторингу через "psutil" та збір інформації про апаратне забезпечення системи через "WMI";

– взаємодія між сервером та клієнтом за допомогою віддаленого доступу, зокрема використовуючи протоколи для під’єднання за допомогою SSH, FTP, RDP чи VPN [29-32].

Описані варіанти прояву можна відслідкувати лише під час несанкціонованого доступу на кінцевий пристрій, аналізуючи дії в реальному часі. Проте останній пункт дає змогу аналізувати наявність backdoor у мережі до початку несанкціонованих дій на кінцевому пристрої. Тому доцільно аналізувати протоколи, що можуть використовуватися для віддаленого доступу.

1.3 Протоколи віддаленого доступу

Telnet є протоколом клієнт-серверної взаємодії, який базується на обміні символьною інформацією через з'єднання TCP. Цей протокол дозволяє віддалено керувати комп'ютерами шляхом текстового введення та виведення. Зазвичай встановлюється з’єднання клієнт-сервер через 23 TCP-порт, де віддалено керований пристрій діє як сервер і очікує на команди від клієнта. Telnet використовується для віддаленого керування пристроями, такими як сервери, маршрутизатори та інші мережеві пристрої, через текстовий інтерфейс [33]. Однак важливо відзначити, що Telnet не забезпечує шифрування даних, які передаються між клієнтом і сервером, що робить його вразливим до перехоплення даних. Це може призвести до витоку конфіденційної інформації, такої як паролі, команди та інші дані, передані в процесі сесії. У сучасних мережах, де безпека є критично важливою, рекомендується використовувати більш захищені альтернативи, такі як SSH (Secure Shell), який надає шифрування всіх переданих даних, що значно знижує ризик несанкціонованого доступу. Також Telnet може бути налаштований для використання у скриптах автоматизації для управління мережевими пристроями на основі текстових команд. Це може спростити адміністрування мережі, дозволяючи адміністраторам налаштовувати та моніторити пристрої без необхідності фізично бути присутнім біля них.

FTP - це стандартний мережевий протокол, призначений для передачі файлів між різними хостами через мережу на основі протоколу TCP. Цей протокол дозволяє користувачам легко завантажувати файли з віддалених серверів, що робить його популярним методом обміну контентом між пристроями або для публікації файлів на веб-сайтах [34]. Крім того, FTP широко використовується в автоматизованих процесах, таких як оновлення програмного забезпечення і створення резервних копій. Доступ до нього можна отримати за допомогою різних FTP-клієнтів, і він сумісний з більшістю операційних систем. Універсальність і надійність FTP у поєднанні з його можливістю захисту через FTPS і SFTP забезпечили його постійну актуальність у різноманітних бізнес- та особистих

програмах. Це включає все, від простого обміну файлами до складних корпоративних систем, які покладаються на FTP для щоденної обробки даних і зв’язку. Загальні порти FTP:

– порт 21 - за замовчуванням для FTP і використовується для передачі команд управління;

– порт 20 - передача даних в активному режимі;

– порт 990 - стандартний порт для FTPS (FTP через SSL/TLS), який використовується для захищеного з'єднання FTP.;

– порт 989 - використовується для активного режиму передачі даних по захищеному FTP (FTPS);

– порт 22 - використовується для SFTP (Secure File Transfer Protocol) через SSH (захищену оболонку).

SSH - це мережевий протокол, який забезпечує захищений спосіб доступу до віддаленого комп'ютера через незахищену мережу. Він зашифровує дані, що передаються по мережі, і має надійні механізми ідентифікації, що гарантують, що лише авторизовані користувачі можуть отримати доступ до віддаленого комп'ютера [35]. SSH часто використовується в програмах для адміністрування серверів, передачі файлів та інших мережевих задач, де важлива безпека з'єднання.

Загальні порти SSH:

– порт TCP 22 використовується для безпечного обміну даними через SSH, зокрема для віддаленого входу в систему та виконання команд. SSH забезпечує шифрований канал зв'язку в архітектурі клієнт-сервер, і його широко використовують системні адміністратори для безпечного керування віддаленими серверами.

– порт TCP 2222 використовується як альтернатива порту 22 для SSH-з'єднань.

– порт TCP 8022 - це інший нестандартний порт, іноді використовуваний для SSH-з'єднань. Він менш поширений, ніж порти 22 або 2222.

– порт TCP 222 використовується деякими програмами, такими як Microsoft Office Communications Server, для забезпечення безпечного зв'язку між клієнтами і серверами.

– порт TCP 2200 використовується для підключень до віддалених робочих столів, наприклад, у системах Virtual Network Computing (VNC) або Windows Remote Desktop.

Протокол віддаленого робочого стола (RDP) є внутрішнім протоколом, розробленим компанією Microsoft, який забезпечує можливість користувачам отримувати віддалений доступ до систем, що працюють на платформі Windows, та керувати ними через графічний інтерфейс користувача (GUI) [36]. Алгоритм роботи RDP-протоколу показано на рисунку 1.4.

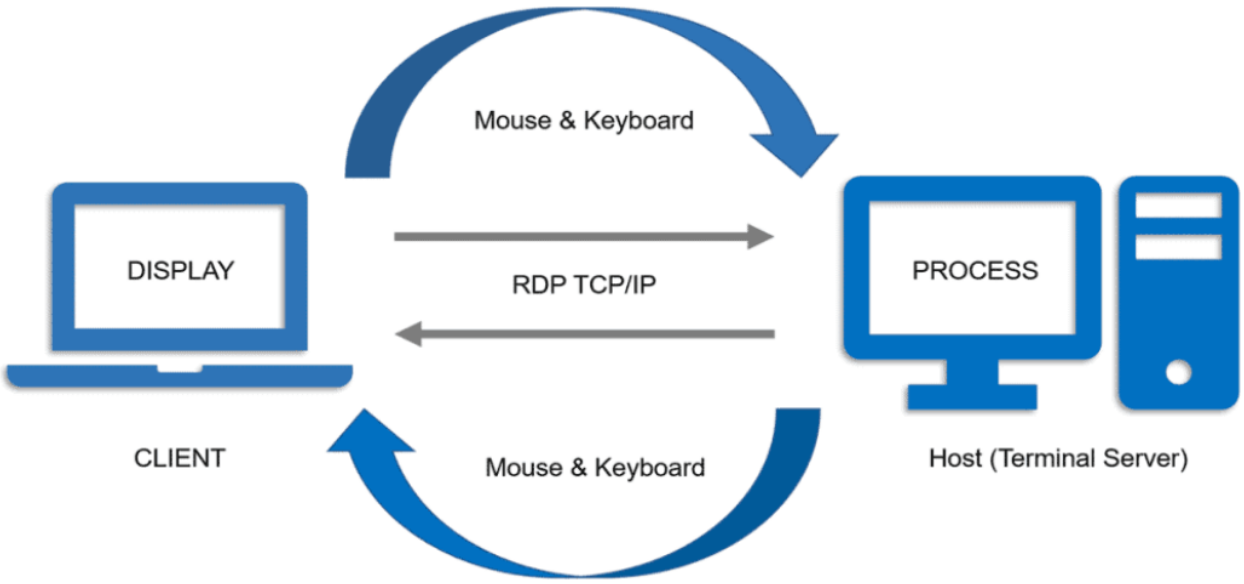


Рисунок 1.4 – Алгоритм роботи RDP-протоколу

За допомогою RDP користувач може взаємодіяти зі робочим столом віддаленої системи так само, як у разі фізичного присутності, що дозволяє виконувати різноманітні завдання, такі як запуск програм, доступ до файлів і друкування документів з будь-якого місця. RDP використовується для віддаленого адміністрування серверів та робочих станцій, надаючи ідеальне рішення для підтримки IT-інфраструктури в компаніях, які мають філії в різних

географічних локаціях. Він також є важливим інструментом для роботи в режимі телекомунікацій, дозволяючи співробітникам ефективно працювати з дому. Для забезпечення безпеки, Microsoft впровадила ряд захисних механізмів у RDP, включно з шифруванням, аутентифікацією на рівні мережі (NLA), яка вимагає аутентифікації перед встановленням власне з'єднання RDP. Це значно ускладнює несанкціонований доступ до системи через RDP. Втім, безпека RDP все ще може бути під загрозою від таких атак, як "Man-in-the-Middle" або брутфорс атаки на паролі, що вимагає від адміністраторів систем вживати додаткових заходів безпеки, таких як VPN, двофакторна аутентифікація або обмеження доступу до RDP через корпоративну мережу.

Протокол тунелювання точка-точка (Point-to-Point Tunneling Protocol) – це протокол, винайдений компанією Cisco Systems для організації VPN через мережі комутованого доступу [37]. На сьогоднішній день PPTP став стандартним протоколом VPN, який майже у всіх операційних системах та комунікаційних пристроях. Це дозволяє користувачам використовувати його без необхідності встановлення додаткового програмного забезпечення. Його перевагою також є низьке споживання обчислювальних ресурсів, що забезпечує високу швидкість роботи. PPTP працює, створюючи звичайну PPP сесію із протилежною стороною за допомогою протоколу Generic Routing Encapsulation (GRE). Для ініціації та управління GRE-з'єднанням використовується друге з'єднання на TCP-порту 1723. Однак через необхідність створення двох мережевих сесій можуть виникати труднощі при налаштуванні PPTP-з'єднання за мережевим екраном. Дані, що передаються через PPTP, шифруються протоколом MPPE, який включає алгоритм шифрування RSA RC4 з ключем довжиною до 128 біт.

Протокол тунелювання на другому рівні (Layer 2 Tunnel Protocol, L2TP) - це мережевий протокол, який базується на протоколі PPP на канальному рівні. Оскільки L2TP не надає шифрування і конфіденційності трафіку, для забезпечення безпеки даних при використанні VPN на основі L2TP, зазвичай застосовується протокол шифрування IPSec (IP Security) [38]. Комбінацію L2TP та IPSec називають L2TP/IPSec (RFC3193). Для L2TP використовується протокол

UDP, де порт 1701 використовується як порт відправника та одержувача для ініціалізації тунелю, порт UDP-500 використовується для обміну ключами шифрування, порт UDP-4500 для операцій NAT, а протокол 50 (ESP) використовується для передачі зашифрованих даних через IPSec.

Найпоширеніші порти VPN включають 1194 для OpenVPN UDP і порт TCP 443, 500 для IPsec/IKEv2 і 1723 для PPTP.

Ось список протоколів VPN, які найчастіше використовуються, і номери портів, які мають бути відкритими для роботи програмного забезпечення:

– протокол тунелювання «точка-точка» (PPTP) використовує TCP-порт 1723;

– протокол тунелювання другого рівня (L2TP) використовує порти 1701 TCP, 500 UDP і 4500 UDP;

– безпека Інтернет-протоколу (IPSec) використовує порти 500 UDP і 4500 UDP;

– протокол тунелювання захищених сокетів (SSTP) використовує TCP-порт 443;

– OpenVPN використовує порти 1194 UDP і 443 TCP;

– WireGuard, один з наймолодших, найшвидших і безпечних протоколів VPN, за замовчуванням використовує UDP-порт 51820;

– L2TP використовує TCP-порт 1701, UDP-порт 4500 і UDP-порт 500;

– IPSec використовує UDP-порти 4500 і 500;

– IKEv2 використовує порти UDP 4500 і 500;

– SSTP використовує TCP-порт 443;

– PPTP використовує TCP-порт 1723. Цей протокол є досить старим, але все ще іноді знаходить своє використання, наприклад, для доступу до Microsoft RAS.

Деякі з найпоширеніших портів VPN включають: порт 1194 для OpenVPN UDP, порт 443 для OpenVPN TCP, порт 1702 для L2TP, порт 500 для IPSec і IKEv2, і порт 1723 для PPTP.

OpenVPN представляє собою комплексне рішення з відкритим вихідним кодом для створення VPN-інфраструктури на базі бібліотеки OpenSSL та

протоколів SSL/TLS. У типовій конфігурації OpenVPN використовується протокол UDP для передачі даних через порт 1194. Проте VPN-з'єднання може бути легко налаштоване для роботи через протокол TCP на будь-якому порту, наприклад, на 443 TCP-порту. Це дозволяє приховати трафік OpenVPN під звичайний HTTPS, що дозволяє уникнути блокування з боку міжмережевих екранів.

IPsec — це набір протоколів, які використовуються для встановлення безпечних з'єднань у мережі. Фактично, сама назва є абревіатурою від Internet Protocol Security. Використовується UDP-порт 500 та IP-порти 50 і 51. IPsec підтримує шифрування та аутентифікацію між двома точками в інтернеті, гарантуючи конфіденційність, цілісність даних, та аутентичність джерела інформації [39]. Ці протоколи можуть застосовуватися у двох режимах: транспортному та тунельному. Транспортний режим захищає повідомлення всередині пакетів IP, тоді як тунельний режим шифрує цілий пакет, включно з його заголовком.

Основні компоненти IPsec включають AH (Authentication Header), що забезпечує аутентифікацію джерела та гарантує незмінність даних в мережі, та ESP (Encapsulating Security Payload), що забезпечує шифрування даних для конфіденційності, а також аутентифікацію джерела. Крім того, IPsec використовує механізми, як-от IKE (Internet Key Exchange), для управління ключами та взаємної аутентифікації між пристроями на початку сесії з'єднання. IKE використовує порт UDP 500 для обміну ключами між хостами. Порт 50 використовується для ESP, що надає шифрування, та порт 51 використовується для AH.

1.4 Аналіз існуючих систем виявлення вторгнень

Система виявлення вторгнень (IDS) - це програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до комп'ютерної системи або мережі, а також несанкціонованого управління ними [40]. IDS працює шляхом моніторингу та аналізу поведінки користувачів та мережевого трафіку з

метою виявлення аномальних та підозрілих дій, таких як мережеві атаки, спроби підвищення привілеїв, неавторизований доступ до важливих ресурсів та дії шкідливого програмного забезпечення.

Мережева система виявлення вторгнень (NIDS, від англ. Network intrusion detection system) — це інструмент безпеки, призначений для моніторингу й аналізу мережевого трафіку на наявність ознак зловмисної діяльності чи спроб неавторизованого доступу [41]. NIDS постійно відстежує весь вхідний і вихідний мережевий трафік. Він працює на рівні мережі та аналізує трафік, що проходить через всю мережу. Для виявлення загроз в основному використовуються методи виявлення на основі сигнатур. Це передбачає зіставлення спостережуваної мережевої активності з базою даних відомих сигнатур або шаблонів атак. Якщо збіг знайдено, генерується сповіщення. Деякі NIDS також використовують виявлення аномалій, що передбачає визначення базової лінії нормальної активності мережі. Будь-яке значне відхилення від цього базового рівня позначається як потенційно шкідливе.

Системи виявлення вторгнень на рівні хоста (HIDS, від англ. Host-based intrusion detection system) спрямовані на моніторинг та аналіз подій, які відбуваються в межах окремої комп'ютерної системи або хоста. На відміну від мережевих систем виявлення вторгнень (NIDS), які аналізують мережевий трафік, HIDS спостерігає за системними запитами, лог-файлами активності додатків, змінами у файловій системі та іншими процесами, що відбуваються на рівні конкретного хоста. Ця система використовується для виявлення вторгнень та потенційних загроз для безпеки системи на самому хості, зокрема атак зловмисників, шкідливих програм та інших аномалій, що можуть виникнути в результаті компрометації конкретної системи.

Системи виявлення вторгнень засновані на прикладних протоколах (Application Protocol-based Intrusion Detection System, APIDS) - це система або агент, який моніторить та аналізує дані, що передаються з використанням специфічних для певних програм протоколів. спеціалізується на виявленні аномальних або підозрілих дій, що відбуваються на рівні протоколів додатків, та

на запобіганні можливим загрозам безпеці, пов'язаним із додатками [42]. APIDS розміщується між процесом і групою серверів, що контролюють та аналізують протоколи додатків, що передаються між пристроями, з метою виявлення порушень безпеки та інцидентів в обробці даних.

Протокол-орієнтована система виявлення вторгнень (ProtocolBased intrusion detection system, PIDS) відстежує і аналізує комунікаційні протоколи, що використовуються між системами або користувачами. Зазвичай встановлений на веб-сервері, PIDS використовується для моніторингу та аналізу протоколу, який використовується комп'ютерною системою. Ця система виявлення вторгнень відстежує динамічну поведінку та стан протоколу, зазвичай розташовуючись на передньому кінці сервера, де відбувається спостереження та аналіз зв'язку між підключеним пристроєм і захищеною системою. Типовим використанням PIDS є моніторинг HTTP або HTTPS потоку на передньому кінці веб-сервера;

Гібридна систем виявлення вторгнень (Hybrid intrusion detection system, Hybrid IDS) поєднує численні техніки та методології виявлення для підвищення загальної ефективності виявлення вторгнень [43]. Ця система зазвичай об’єднує виявлення на основі сигнатур, яке передбачає порівняння моделей відомих атак на вхідний трафік або системну активність, і виявлення на основі аномалій, яке визначає відхилення від нормальної поведінки.

У залежності від завдання захисту (аналіз вхідного трафіку, пошук аномалій, захист хоста) може використовуватися одна або кілька вище описаних систем у мережі. Проте кожна із систем може застосовувати різні методи щодо виявлення вторгнення.

Сигнатурні методи виявлення вторгнень описують атаки за допомогою формальних моделей, таких як символьні рядки або семантичні вирази. Ці методи виявлення вторгнень захищають систему лише в разі, коли відома сигнатура атаки, наприклад, фрагмент вірусного коду, і ця сигнатура включена до бази даних системи запобігання вторгнень (IPS). Спочатку застосовувався розробниками антивірусів, термін "сигнатура атаки" використовувався для перевірки системних файлів на наявність ознак шкідливої діяльності. IDS, ґрунтуючись на сигнатурах,

зазвичай виявляє вхідний мережевий трафік, шукаючи послідовності та шаблони, які відповідають певній сигнатурі атаки. Їх можна розпізнати в заголовках мережевих пакетів, а також в послідовностях даних, що відповідають відомим шкідливим програмам або іншим зловмисним шаблонам. Сигнатура атаки також може бути виявлена в мережевих адресах призначення або джерела, а також у певних послідовностях даних або серіях пакетів. Виявлення на основі сигнатур використовує відомий список індикаторів компрометації (IOC). Ці індикатори можуть включати певні дії мережевих атак, відомі послідовності байтів і шкідливі домени. Крім того, вони можуть містити рядки тем електронних листів і хеші файлів.

Методи виявлення аномалій або статистичні методи - це техніки, що базуються на виявленні відхилень у функціонуванні інформаційно-телекомунікаційних систем від їх звичайного режиму роботи. Системи, що побудовані на даному методі, проходять навчання при нормальних умовах та орієнтуються на вказані правила. Саме тому характеризуються великою кількістю хибних спрацювань. Система виявлення аномалій використовує машинне навчання для того, щоб навчити систему розпізнавати нормальний базовий рівень. Базовий рівень відображає звичайну поведінку системи, і потім вся мережева активність порівнюється з цим базовим рівнем. Замість пошуку відомих IOC, IDS на основі аномалій просто виявляє будь-яку незвичайну поведінку, що може викликати сповіщення. За допомогою IDS на основі аномалій все, що не відповідає існуючому нормальному базовому рівню, наприклад, спроба користувача ввійти в систему поза стандартним робочим часом, додавання нових пристроїв до мережі без авторизації або потік нових IP-адрес, які намагаються встановити з'єднання з мережею, підніме потенційний прапор для занепокоєння. Недоліком тут є те, що багато нешкідливих дій буде позначено просто як нетипове. Збільшена ймовірність помилкових спрацьовувань під час виявлення вторгнень на основі аномалій може призвести до необхідності додаткового часу та ресурсів для аналізу всіх повідомлень про можливі загрози. У той же час цей потенційний недолік також робить виявлення вторгнень на основі аномалій

здатним виявляти експлойти нульового дня.

Метод виявлення вторгнень за допомогою штучного інтелекту - це підхід до виявлення потенційних загроз та атак на комп'ютерні системи, який використовує різноманітні техніки і методи штучного інтелекту, такі як машинне навчання, нейронні мережі, генетичні алгоритми та інші. Ці методи використовуються для аналізу великого обсягу даних і виявлення відхилень або аномалій, які можуть вказувати на потенційні загрози безпеці.

Аналіз існуючих систем виявлення вторгнень вказує на те, що вони не здатні виявляти зловмисників у мережі або ж приймати несанкціоновані дії як нормальний трафік. Проте системи можуть здійснювати захист окремих вузлів чи від зовнішнього впливу.

1.5 Постановка завдання

Кібератаки є найбільшими загрозами для різноманітних інформаційних систем. А зростання їх масштабів, швидкості та складності вимагає постійного пошуку нових методів виявлення вразливостей та способів захисту.

Завданням даної роботи є розробка системи виявлення вразливості у мережі.

Задля виконання поставленого завдання слід виконати наступні кроки:

– змоделювати майбутню систему за допомогою Matlab з використанням нечіткої логіки;

– розробити схему включення системи в комп’ютерну мережу;

– розробити алгоритм роботи системи виявлення вторгнень у мережі;

– розгорнути тестове середовище для проведення випробувань;

– здійснити розрахунок ефективності розробленої системи на основі проведених тестувань.

2.1 Опис методів, які застосовуються для розробки системи

Для реалізації системи виявлення вторгнень у мережі, дослідивши особливості бекдорів та віддалену роботу адміністраторів системи, доцільно використовувати поєднання нечіткої логіки та нейронної мережі. У якості середовища моделювання буде використано Matlab.

Метод сигнатурного аналізу описує вторгнення через формальну модель, яка може включати символьні рядки, семантичні вирази та інше. Перевірка сигнатур є першим методом для виявлення вторгнень, який полягає у порівнянні послідовностей з попередньо відомими сигнатурами. Сигнатура, як правило, є характерною фразою чи командою, що пов'язана з конкретним видом вторгнення. У разі збігу з відомою сигнатурою, система генерує сповіщення про зловмисні дії. Сигнатурний метод захищає від хакерських або вірусних атак, якщо сигнатура вже відома і включена до бази даних системи запобігання вторгнень (IPS). Ефективність сигнатурної IPS залежить від швидкості оновлення бази даних, повноти визначених сигнатур та використання алгоритмів порівняння. Перевагами сигнатурного аналізу є його низька обчислювальна складність та відносно невелика вартість впровадження. Реалізувати метод сигнатурного аналізу будемо за допомогою нечіткої логіки.

У звичайному розумінні, логіка визначає механізм мислення, що має бути строго формалізованим. Однак у реальності існує не лише один тип логіки, наприклад, булева, але стільки, скільки потребуємо, оскільки вибір відповідної системи аксіом визначає все. Після того, як аксіоми встановлені, всі твердження, що будуються на їх основі, мають бути бездоганними і не суперечливими за правилами даної системи аксіом. Нечітка логіка представляє собою розширення класичної логіки, де істинність розглядається як лінгвістична змінна з різними рівнями: "дуже істинно", "більш-менш істинно", "не дуже хибно" і т.д. Ці

лінгвістичні значення виражені у вигляді нечітких множин. Основна відмінність від класичної логіки полягає в тому, що замість "Істини" і "Хибності" в нечіткій логіці використовується ступінь істинності, який приймає значення від 0 (Хибності) до 1 (Істина) включно. Таким чином, логічні операції не можуть бути представлені таблицями істинності, але задаються функціями, які тільки в крайніх випадках, коли значення змінних дорівнюють виключно 1 або 0, зводяться до таблиць істинності операцій класичної логіки.

Основи нечіткої логіки були започатковані в кінці 1960-х роках Лотфі А. Заде, американським математиком, який створив теорію нечітких множин. Термін "нечітка логіка" зазвичай використовується в двох різних сенсах. У вузькому сенсі це логічне числення, яке є розширенням багатозначної логіки. У широкому сенсі, що переважає в сучасному використанні, нечітка логіка еквівалентна теорії нечітких множин. З цієї точки зору, нечітка логіка у вузькому сенсі є розділом нечіткої логіки в широкому сенсі. Проте до його недоліків відносяться обмежена ефективність у виявленні нових, невідомих атак, а також проблема невчасного оновлення бази сигнатур.

Нейронні мережі (штучні нейронні мережі, ШНМ). Нейронні мережі це набір інструментів для різних застосувань, таких як кластеризація даних, виділення ознак та зменшення розмірності. Для виявлення атак нейронні мережі навчаються на прикладах різних типів вторгнень і використовуються для розпізнавання поведінки системи, що піддається атаці. Для виявлення аномалій нейронні мережі навчаються на прикладах нормальної поведінки системи і запускаються в режимі розпізнавання. Якщо значення параметрів відрізняються від реальної поведінки системи, вважається, що в системі є аномалія. Для побудови моделі поведінки користувача використовуються такі параметри: час доби, коли користувач зазвичай працює, набір вузлів, з яких користувач ініціює робочу сесію, та характеристики використання ресурсів системи.

Рекурентна нейронна мережа (RNN) - це тип нейронної мережі, яка має вбудовану пам'ять, що дозволяє їй зберігати інформацію про попередні вхідні дані і робити прогнози. У процесі роботи RNN використовує попередні вихідні дані як

частину нового вхідного сигналу, що дозволяє їй використовувати здобуті знання з минулих кроків для вдосконалення прогнозів. Ці нейронні мережі особливо ефективні для аналізу послідовних даних, таких як дані про мережевий трафік. Структуру рекурентної нейронної мережі показано на рисунку 2.1.

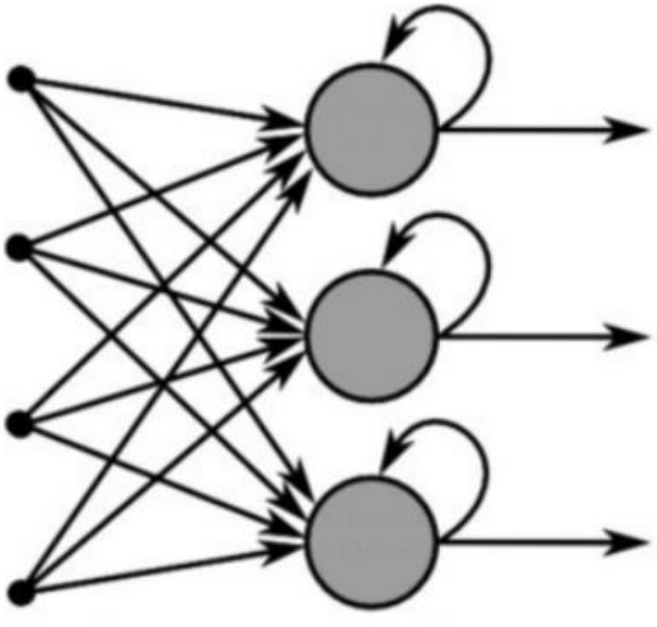


Рисунок 2.1 - Структура рекурентної нейронної мережі

Мережі довготривалої короткочасної пам'яті (LSTM) є розвиненою версією рекурентних нейронних мереж, яка в основному розширює їх здатність до зберігання інформації. Це особливо корисно для виявлення важливих зв'язків в даних, що протягом тривалого часу мають значення. LSTM вирішує проблему зникнення градієнтів, яка виникає в звичайних RNN, що дозволяє йому ефективно навчатися на тривалих послідовностях даних і забезпечує високу точність прогнозів.

LSTM мають здатність зберігати інформацію на тривалий період часу, що робить їх схожими на пам'ять комп'ютера. Вони можуть читати, записувати та видаляти інформацію зі своєї пам'яті. Ця пам'ять може бути розглянута як закрита клітинка, яка приймає рішення про збереження або видалення інформації на основі її важливості. Вагові коефіцієнти, які вивчаються алгоритмом, визначають

важливість інформації з плином часу.

У структурі LSTM присутні три вентиля: вхідний, забуття та вихідний (рисунок 2.2). Ці вентилі контролюють, чи допускається нова інформація, чи вона видаляється як неважлива, чи впливає на вихідні дані на поточному кроці часу. Вони регулюються аналоговими сигмоїдами, які забезпечують плавне зміщення відсотків відсутності до повної активації, що дозволяє ефективно використовувати зворотне поширення.

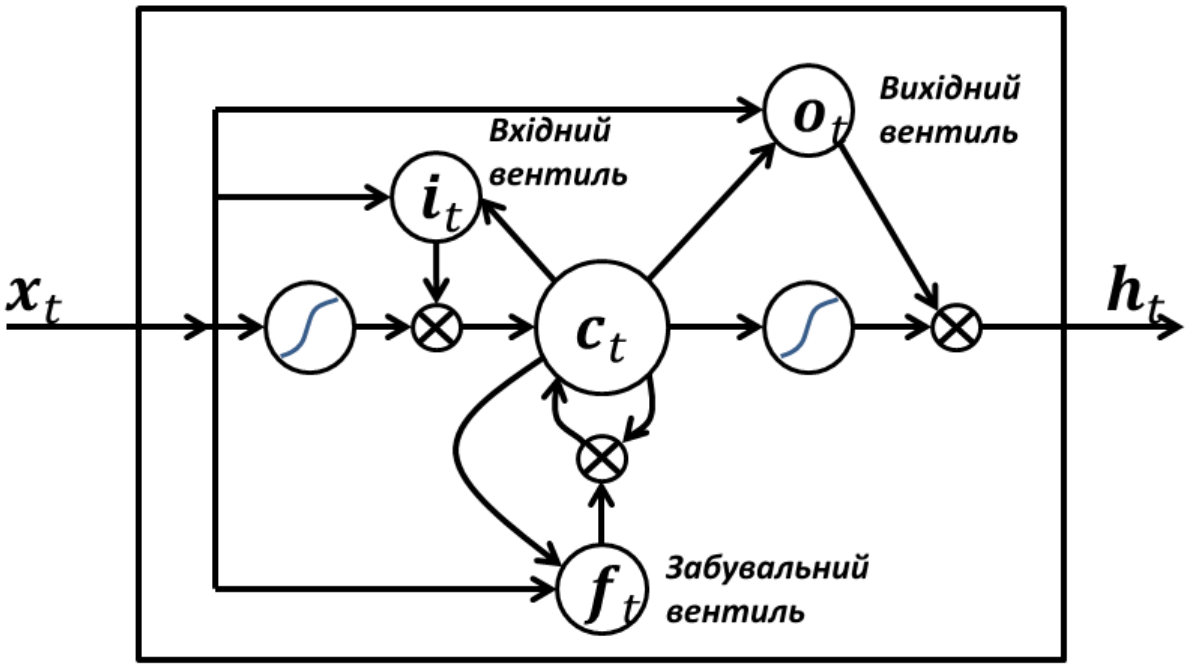


Рисунок 2.2 - Структура LSTM

Завдяки LSTM проблема зникнення градієнтів вирішується, оскільки вони забезпечують достатньо круті градієнти, що дозволяє ефективно навчати мережу на довгих послідовностях даних і зберігати високу точність моделі.

2.2 Набір даних UNSW-NB 15

Для тестування та доведення ефективності буде використано набір даних UNSW-NB 15. Дані набору UNSW-NB 15 були створені в Cyber RangeLab Австралійського центру кібербезпеки (ACCS) за допомогою інструменту IXIA

Perfect Storm. Цей набір містить гібрид звичайної діяльності та атакованої поведінки. Для захоплення 100 ГБ необробленого трафіку використовувався інструмент Tcp-dump. Дванадцять алгоритмів і інструментів, таких як Argus, Bro-IDS, були використані для створення UNSW-NB15. Загалом набір містить 25 40 044 позначених екземплярів, кожен з яких класифіковано як нормальний або атакуючий. Розподіл з'єднань між цими двома групами подано в таблиці 2.1.

Таблиця 2.1 – Деталі даних у наборі даних UNSW-NB15

Назва	Кількість
Загальна кількість подій	2540044
Нормальний трафік	2218761
Атаки	321283

У наборі даних присутні дев'ять типів атак, крім однієї групи, що представляє звичайні дані. Ці атаки класифікуються як Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode та Worms. Типи атак наведено в таблиці 2.2.

Таблиця 2.2 - Опис категорій атаки набору даних UNSW-NB15

Тип трафіку	Опис
1	2
Normal	Трафік без загрози
Fuzzing	Автоматизований процес пошуку помилок програмного забезпечення, які можна зламати, шляхом випадкової подачі різних перестановок даних у цільову програму, доки одна з цих перестановок не виявить уразливість
Analysis	Загальний тип для опису сканування портів, проникнення спаму та файлів html

Кінець таблиці 2.2

1	2
DOS	Позбавляє законних користувачів можливості використовувати веб-сервіси через переповнення мережі/сервера недійсними спробами автентифікації, що призводить до збою або зупинки
Exploits	Код, який використовує вразливість програмного забезпечення або недолік безпеки. Часто вбудовується в шкідливе програмне забезпечення, що забезпечує досить легке та швидке розповсюдження.
Generic	Атака на секретні ключі шифрів працює проти всіх блокових шифрів
Reconnaissance	Набір простих прийомів, які збирають інформацію про цільову мережу/сервер, наприклад nmap
Shellcode	Набір інструкцій/операторів, які вводяться та виконуються програмою з недоліками. Безпосередньо керує регістрами та функціями програми
Worms	Шкідливий код, що самовідтворюється. Споживає забагато системної пам’яті та пропускної здатності мережі. Знижує доступність систем.

Розподіл у наборі даних UNSW-NB15 відповідно до категорій показано в таблиці 2.3

Таблиця 2.3 - Поділ набору даних відповідно до категорій

Категорія	Кількість
1	2
Normal	2218761
Fuzzing	24246

Кінець таблиці 2.3

1	2
Analysis	2677
Backdoor	2329
DOS	16353
Exploits	44525
Generic	215481
Reconnaissance	13987
Shellcode	1511
Worms	174

Набір містить 45 функцій, включаючи мітку класу. Опис функцій та їх типи наведено в таблиці 2.4. Атрибути мають різні типи даних: деякі номінальні, деякі числові, а деякі представляють часові мітки.

Таблиця 2.4 - Опис функцій набора даних UNSW-NB15

№	Назва	Опис
1	2	3
1	id	Ідентифікатор
2	dur	Загальна тривалість
3	proto	Протокол, який використовується при підключенні
4	service	Мережева служба, що використовується підключенням (http, ftp, ssh та ін.)
5	state	Стан та залежний від нього протокол (ACC, CLO та ін.)
6	spkts	Кількість пакетів від джерела до пункту призначення
7	dpkts	Кількість пакетів від пункту призначення до джерела
8	sbytes	Кількість надісланих байт за одне з'єднання
9	dbytes	Кількість прийнятих байт за одне з'єднання
10	rate	Швидкість передачі та прийому даних Ethernet

Продовження таблиці 2.4

1	2	3
11	sttl	Час життя від джерела до пункту призначення
12	dttl	Час життя від пункту призначення до джерела
13	sload	Кількість відправлених біт за секунду
14	dload	Кількість прийнятих біт за секунду
15	sloss	Кількість відправлених пакетів, які повторно передані або відкинуті
16	dloss	Кількість прийнятих пакетів, які повторно передані або відкинуті
17	sinpkt	Час прибуття між пакетами джерела (мсек)
18	dinpkt	Час прибуття між пакетами від пункту призначення (мсек)
19	sjit	Джиттер від джерела (мсек)
20	djit	Джиттер від пункту призначення (мсек)
21	swin	Максимальний обсяг даних, який може бути надісланий
22	stcpb	Порядковий номер джерела при TCP-з'єднанні
23	dtcpb	Порядковий номер пункту призначення при TCP з'єднанні
24	dwin	Максимальний об'єм даних, який може бути отриманий
25	tcprtt	Сума «synack» і «ackdat» при підключенні TCP
26	synack	Час між пакетами SYN і SYN_ACK при підключенні TCP
27	ackdat	Час між пакетами SYN_ACK і SYN при підключенні TCP
28	smean	Середнє значення розміру відправленого пакета
29	dmean	Середнє значення розміру прийнятого пакета

Продовження таблиці 2.4

1	2	3
30	trans_depth	Глибина підключення транзакцій http-запиту / відповіді
31	response_body_len	Розмір даних, що передаються серверною службою http
32	ct_srv_src	Кількість підключень, які містять одну ту ж саму службу і адресу джерела зі 100 підключень останнім часом
33	ct_state_ttl	№ для кожного стану відповідно до конкретного діапазону значень часу життя джерела / призначення
34	ct_dst_ltm	Кількість підключень з одним і тим же адресним призначенням у 100 підключеннях за даними останнього часу
35	ct_src_dport_ltm	Кількість підключень з одним і тим же адресом джерела і портом призначення в 100 підключеннях за даними останнього часу
36	ct_dst_sport_ltm	Кількість підключень з одним і тим же адресним призначенням і вихідним портом у 100 підключеннях за даними останнього часу
37	ct_dst_src_ltm	Кількість підключень одного і того ж адреса джерела й отримувача в 100 підключеннях останнім часом
38	is_ftp_login	Якщо доступ до сеансу ftp здійснюється за допомогою логіну користувача та паролю, то 1, 0
39	ct_ftp_cmd	Кількість потоків, для яких є команда в сеансі ftp
40	ct_flw_http_mthd	Кількість потоків, у яких є такі методи, як Get і Post, у службі http.
41	ct_src_ltm	Кількість підключень з однією і тією ж адресою джерела в 100 підключеннях за даними останнього часу
42	is_sm_ips_p orts	Якщо джерело рівня IP-адрес призначення і номера портів одинакові, то 1, інакше 0

Кінець таблиці 2.4

1	2	3
43	ct_srv_dst	Кількість підключень, які містять одну та ту саму послугу і адреса призначення з 100 підключень за даними останнього часу (31).
44	attack_cat	Назва кожної категорії атак.
45	label	Якщо є атака, то 1, інакше 0

Необроблені мережеві пакети з набору даних UNSW-NB 15 були розроблені генератором трафіку IXIA для моделювання гібриду сучасної реалістичної легальної та штучної зловмисної активності. Вихідні файли для цього набору даних були надані розробниками у різних форматах (pcap, BRO, Argus і CSV) і впорядковані за датою. Файли CSV набору даних складалися з 45 об'єктів з мітками класів і категорій атак і були підготовлені для використання в оцінці NIDS під назвами UNSW-NB15_1.CSV, UNSW-NB15_2.CSV, UNSWNB15_3.CSV і UNSW-NB15_4.CSV. Чотири файли, названі UNSW-NB15_2.CSV, UNSWNB15_3.CSV і UNSW-NB15_4.CSV, містять записи даних як для звичайних подій, так і для атак.

Із набору даних слід відділити для подальшого використання дані, які потрібні для ідентифікації бекдорів, та нормальний трафік. Результат розподілу показано в таблиці 2.5.

Таблиця 2.5 - Розподіл у частині набору даних UNSW-NB15

Категорія	Навчальний набір	Тестовий набір
Normal	5321	1587
Backdoors	1746	583

Для оптимізації кількості параметрів, які будуть використовуватися слід визначити кореляцію між різними характеристиками набору даних UNSW-NB15. Відповідну діаграму кореляції Пірсона продемонстровано на рисунку 2.3.

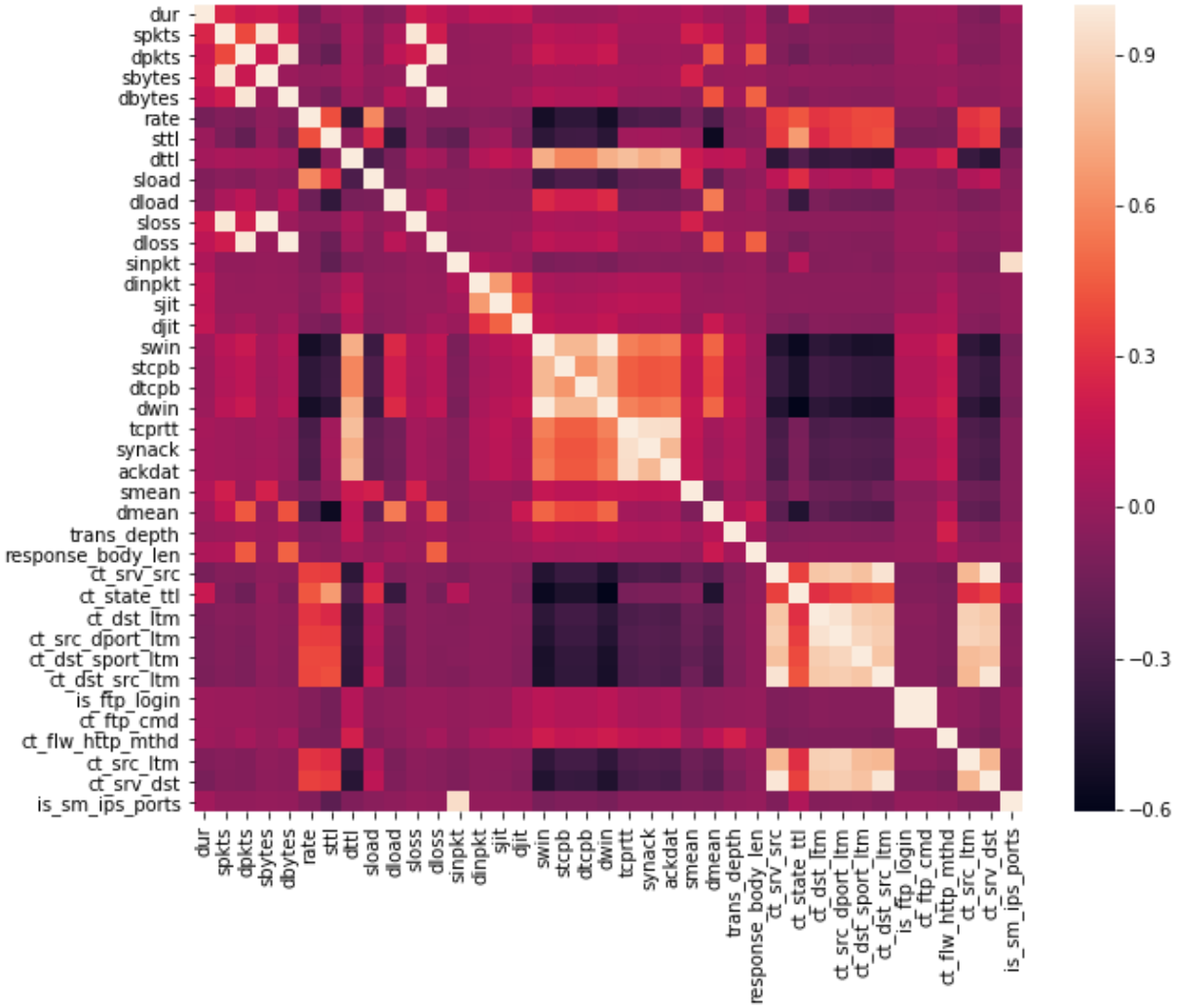


Рисунок 2.3 – Набір кореляційних даних

Дві характеристики співвідносяться між собою коефіцієнтом кореляції Пірсона. Він забезпечує вимірювання ступеня узгодженості між двома змінними. Коефіцієнт змінюється від 1 до +1, при цьому -1 вважається дуже пов'язаним, 1 розглядається як негативний, а 0 не демонструє жодної кореляції. Набір даних містить низку характеристик мережевого трафіку. Повністю корельованими парами функцій є {sbytes, sloss}, {dbytes, dloss}, {swin, dwin}, {ct_srv_src, ct_dst_src_ltm}, {is_ftp_login, ct_ftp_cmd}. Щоб уникнути надмірності, буде видалено частину функцій з цих пар, а саме sloss, dloss, dwin, ct_dst_src_ltm, ct_ftp_cmd.

Потрібно видалити із набору даних параметри, які не пов'язані із атакою типу Backdoors. Таким чином із набору будуть використовуватися наступні

функції: id, dur, proto, service, state, sttl, dttl, sload, dload, sinpkt, dinpkt, swin, stcpb, dtcpb, tcprtt, smean, dmean, is_ftp_login, is_sm_ips_p orts, attack_cat, label.

Варто додати параметри, які будуть використані при формуванні правил аналізу трафіка засобами нечіткої логіки, а саме IP, port, time, де:

– IP – IP-адреса із якої надходять запити на приєднання;

– port – порт до якого відбувається звернення;

– time – час коли відбувається звернення.

2.3 Алгоритм роботи системи

Для того, щоб адміністратор системи міг безперешкодно працювати віддалено, в налаштуваннях доступу можуть бути передбачені віддалені входи в систему. Саме тому слід враховувати, що не всі бекдори однозначно будуть зловмисними. Щоб при аналізі трафіка адміністратора системи не блокувало як зловмисного користувача слід розробити набір правил, які будуть вказувати з певною ймовірністю на адміністратора. Будемо вважати, що результат 0.8-1.0 - це трафік, який надходить від адміністратора. Трафік, який після перевірки правилами буде знаходитися в діапазоні 0-0.8, слід додатково перевіряти засобами нейронної мережі, котра навчена виявляти бекдори.

Для формування правил будемо використовувати наступні функції та їх значення задля прийняття рішення чи належить мережевий трафік адміністратору мережі.

– IP: «дозволено», «невідомо», «заборонено»;

– port: «дозволено», «невідомо», «заборонено»;

– time: «дозволено» чи «заборонено»;

– protocol: «дозволено», «невідомо», «заборонено»;

– service: «дозволено», «невідомо», «заборонено».

Налаштування лінгвістичних означень для параметра port показано на рисунку 2.4.

PROPERTY EDITOR: INPUT

Name: port

Range: [0 1]

Number of MFs: 3

Evenly Distribute MFs

Name	Type	Parameters
дозволено	Trapezoidal	[0 0 0.08 0.37]
невідомо	Trapezoidal	[0.12 0.25 0.64 0.87]
заборонено	Trapezoidal	[0.53 0.77 1 1]

Рисунок 2.4 - Налаштування лінгвістичних означень для критерія port

Область визначення лінгвістичних означень для параметра IP показана на рисунку 2.5.

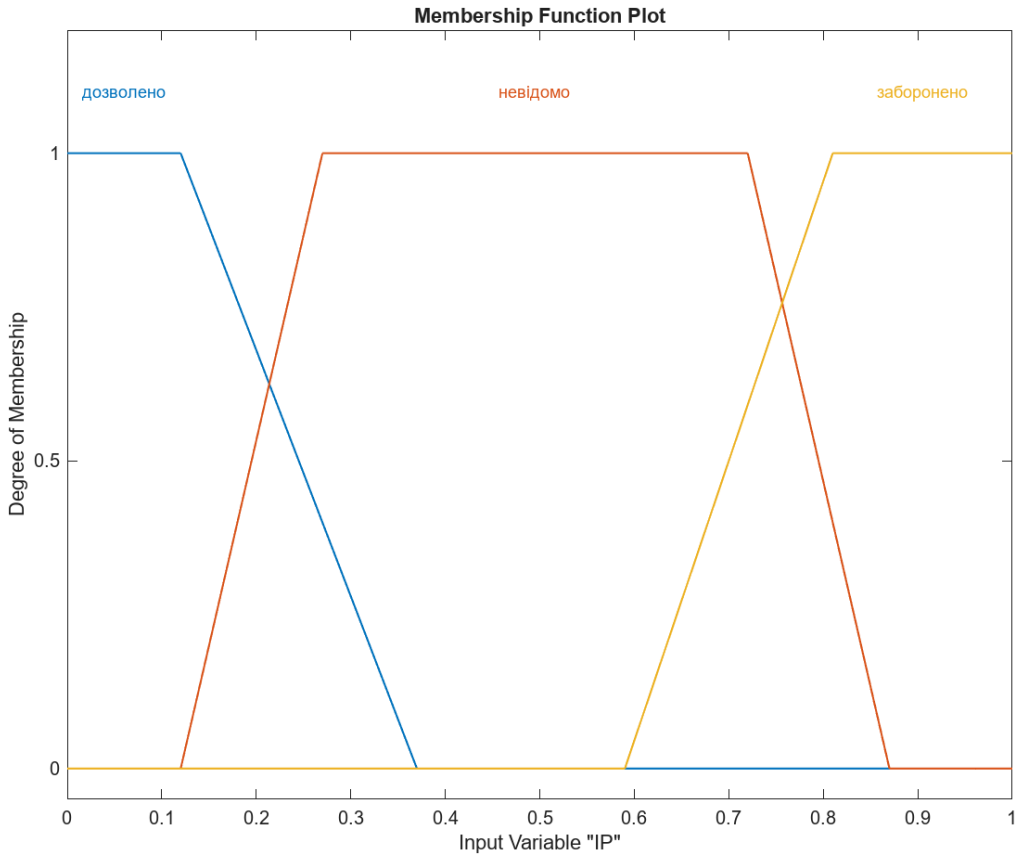


Рисунок 2.5 – Графік функції приналежності для параметра IP

Приклад формування правил показаний на рисунку 2.6.

	Rule	Weight	Name
1	If IP is заборонено and port is заборонено then output1 is bad	1	rule1
2	If IP is невідомо and time is заборонено and proto is заборонено then output1 is bad	1	rule2
3	If IP is дозволено and port is дозволено and time is дозволено then output1 is good	1	rule3
4	If IP is дозволено and port is дозволено then output1 is good	1	rule4
5	If IP is невідомо and port is заборонено and time is заборонено then output1 is bad	1	rule5

Рисунок 2.6 – Формування правил

Структура системи нечіткого виводу для класифікації ознак за допомогою Matlab показана на рисунку 2.7.

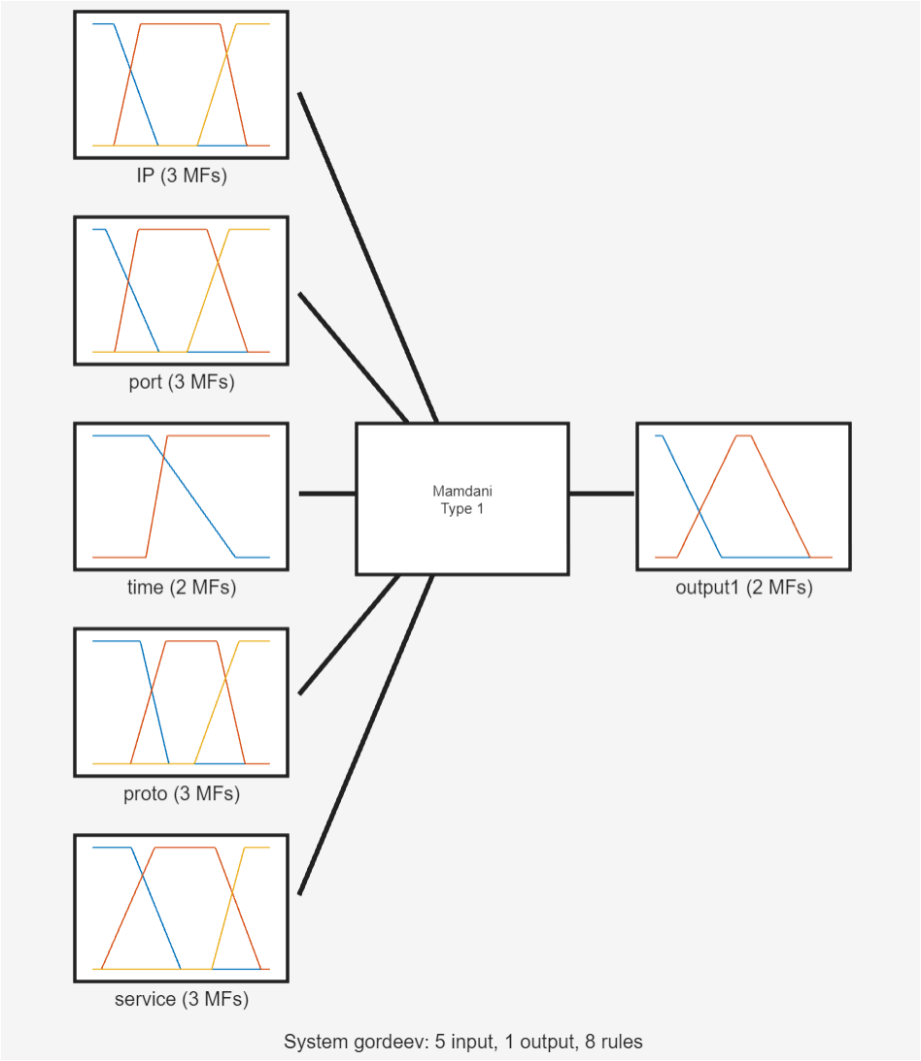


Рисунок 2.7 – Структура системи нечіткого логічного висновку

За допомогою візуалізації можна переглянути результати. Приклади

варіантів візуалізації результатів показано на рисунках 2.8-2.9.

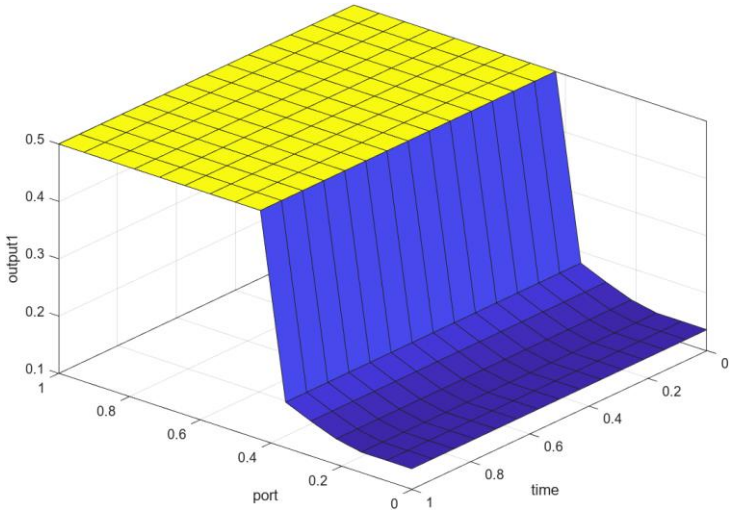


Рисунок 2.8 - Виведення результатів нечіткої моделі через 3D графік

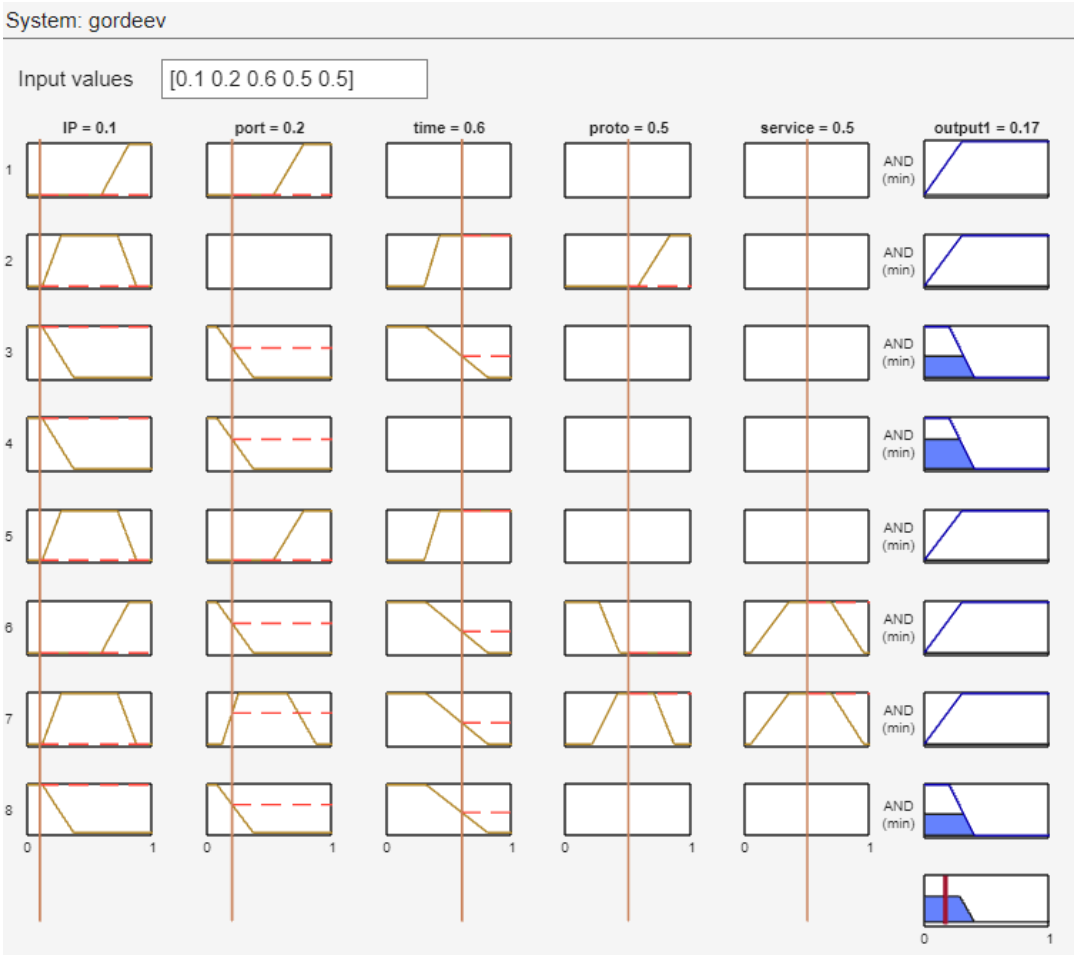


Рисунок 2.9 – Візуалізація нечіткого висновку

Наступним етапом класифікації трафіку буде аналіз тих даних, які не

визнано трафіком, який з’являється в мережі в наслідок дій адміністратора мережі. Для цього буде застосовано нейронну мережу. Доцільно використати рекурентну нейронну мережу, а саме мережу довгострокової короткочасної пам’яті (LSTM).

Впровадження методу включає кілька етапів:

– підготовка даних;

– навчання нейронної мережі;

– тестування даних за допомогою навченої нейронної мережі.

Оскільки перший крок, який включає в себе формування та попередню обробку даних для навчання та тестування нейронної мережі, виконано у параграфі 2.2 даного розділу, то далі буде проходити етап навчання нейронної мережі.

Алгоритм підготовки та навчання нейронною мережею представлено на рисунку 2.9.

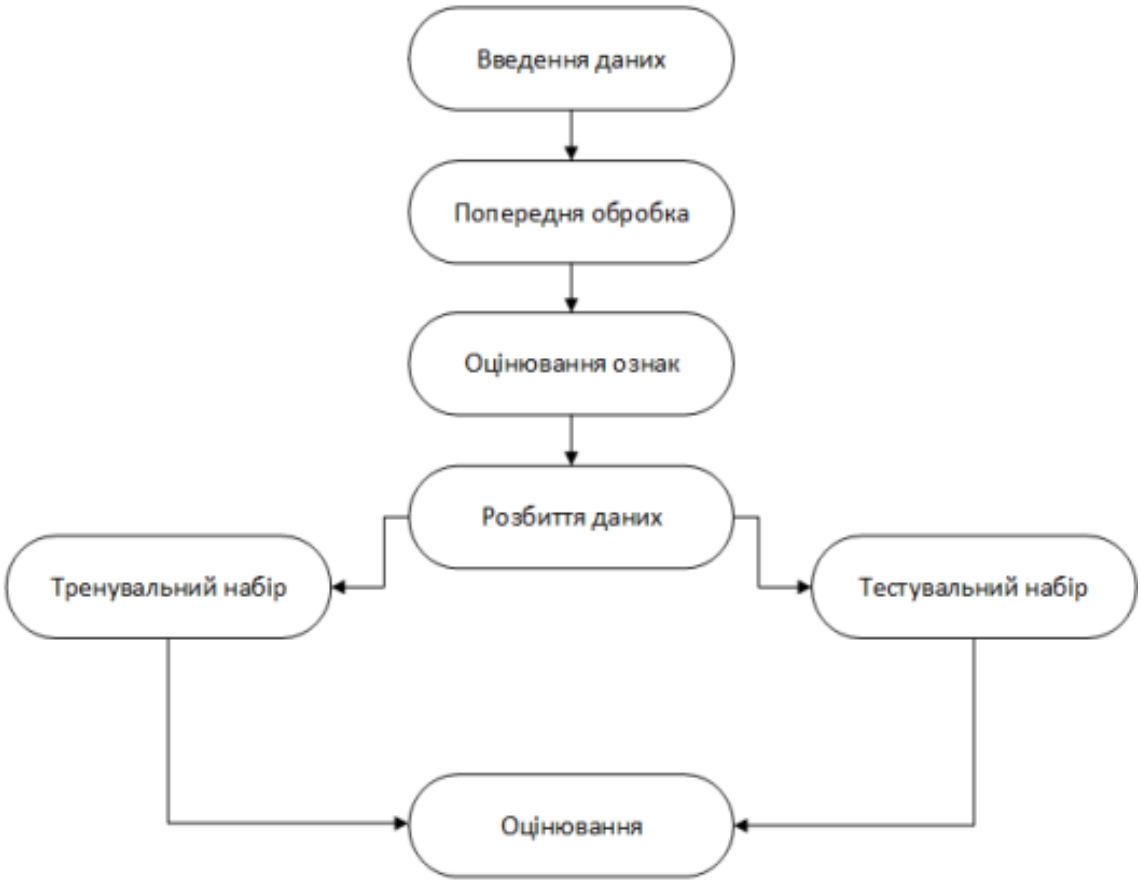


Рисунок 2.9 - Алгоритм підготовки та навчання нейронною мережею

На основі вище викладеного графічно алгоритм роботи системи виявлення вторгнень у мережі можна відобразити як на рисунку 2.10.

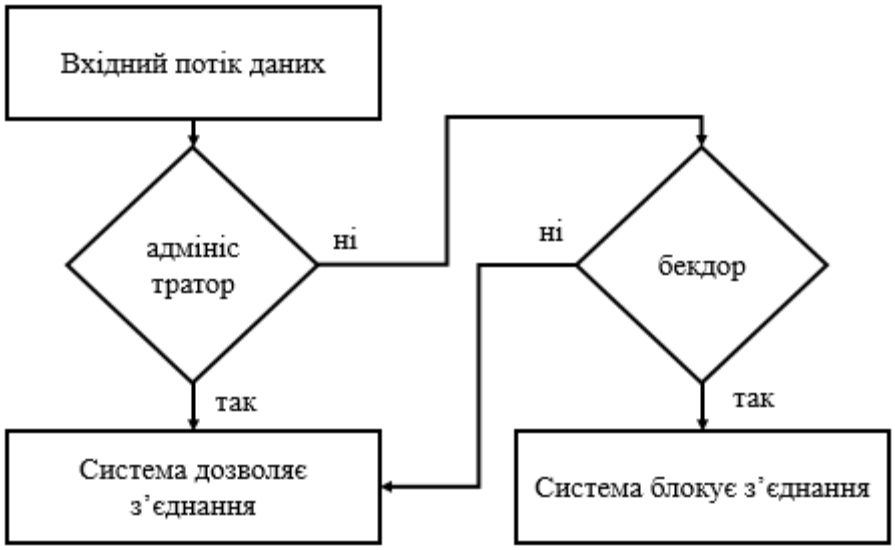


Рисунок 2.10 - Алгоритм роботи системи виявлення вторгнень у мережі

2.4 Побудова мережі

Комп'ютерна мережа складається із великої кількості мережевих пристроїв (комутатори, маршрутизатори та інше), які забезпечують комутацію, налаштування політик доступу та розмежування підмереж. До кінцевих пристроїв можна віднести персональні комп'ютери, ноутбуки, мобільні телефони та інші. Саме ці пристрої є найбільш вразливими до несанкціонованих дій. Також, зазвичай, у мережі є адміністратор із привілейованими правами й можливістю підключатися до мережі не лише локально, а й віддалено. Найбільш цінними для зловмисників є сервера, які використовують для зберігання даних. Схему такої мережі показано на рисунку 2.11. Слід зазначити, що порушник, проникнувши у мережу, першочергово налаштує віддалений доступ для подальшої роботи. Порушники можуть використовувати віддалений доступ для дослідження цільової системи або мережі, щоб знайти слабкі точки та вразливості, які можуть бути використані для майбутніх кібератак. Також віддалений доступ може допомогти порушникам збирати інфраструктуру для створення ботнету - мережі

комп'ютерів або інших пристроїв, які можна використовувати для виконання розподілених атак, спаму, генерації фальшивого трафіку тощо. Порушники можуть використовувати віддалений доступ для видалення, пошкодження або регулярного викрадення даних. Це може призвести до серйозних матеріальних збитків, втрати конфіденційності або навіть втрати даних, що є критичними для діяльності бізнесу або приватного життя.

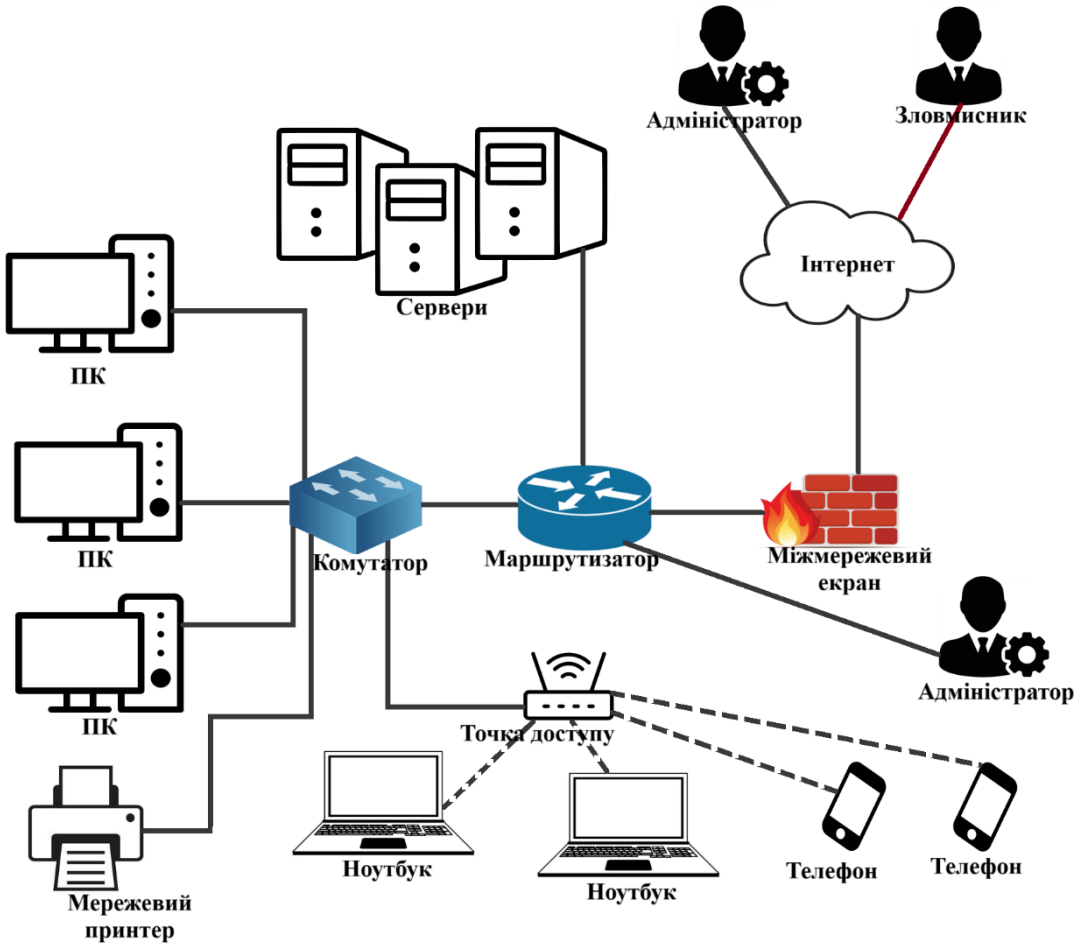


Рисунок 2.11 – Схема мережі

2.5 Схема включення розробленої системи у мережу

Для того, щоб можна аналізувати трафік на наявність бекдорів, які потенційно можуть бути реалізовані на будь-якому кінцевому пристрої, систему виявлення треба розміщати перед входом трафіка на маршрутизатор.

Таке розміщення має кілька переваг:

– дозволяє виявляти потенційно шкідливий трафік ще до того, як він потрапить у зовнішню мережу;

– централізоване розміщення системи дозволяє керувати та моніторити трафік з одного центрального місця, що полегшує адміністрування та нагляд за безпекою мережі;

– може реагувати на потенційні загрози миттєво, блокуючи або відхиляючи шкідливий трафік ще до того, як він зможе завдати шкоди системі або мережі;

– виявлення потенційно шкідливого трафіку на маршрутизаторі дозволяє попереджувати можливі загрози та реагувати на них до того, як вони стануть критичними.

Схему комп'ютерної мережі із підключеною системою показано на рисунку 2.12.

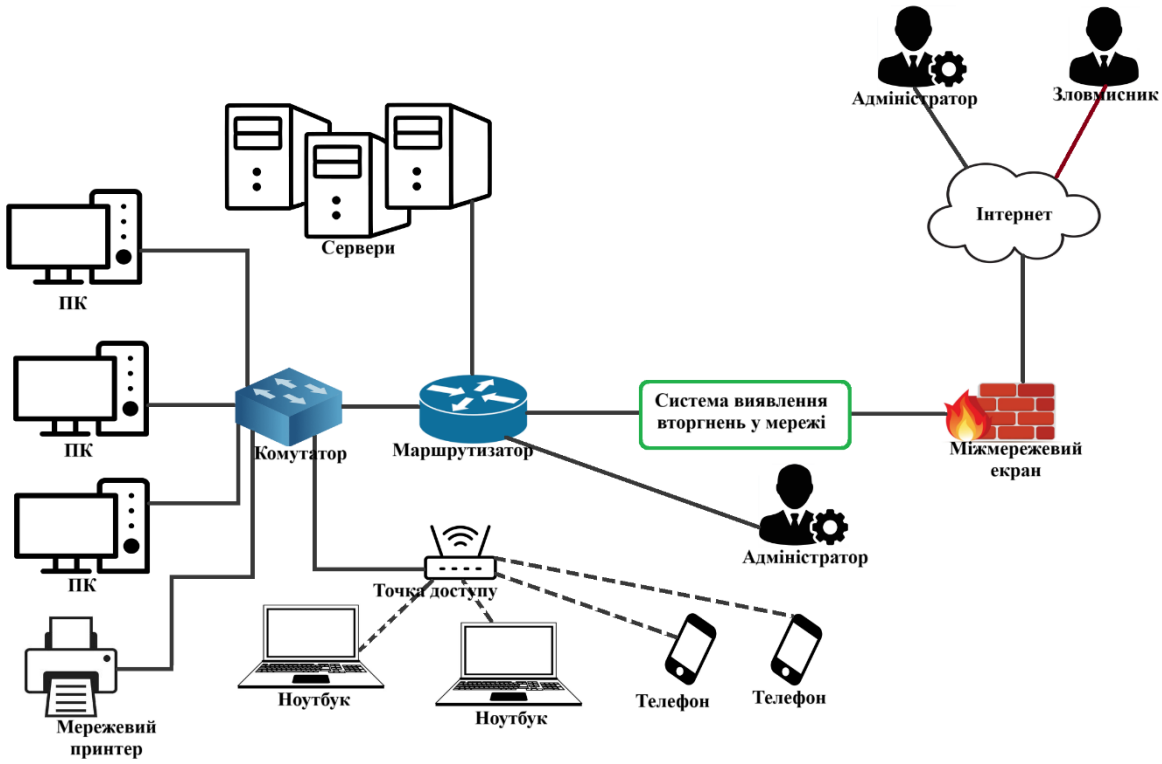


Рисунок 2.12 - Схема включення системи виявлення вторгнень у мережі

2.6 Висновки до розділу

У першому параграфі описано метод сигнатурного аналізу, який

реалізовано за допомогою засобів нечіткої логіки. Також відображено переваги рекурентної нейронної мережі довгої короткочасної пам’яті для аналізу мережевого трафіку.

В другому параграфі деталізовано набір даних UNSW-NB15. А саме:

– описано категорії набору даних й визначено які з них потрібні для виявлення віддаленого доступу;

– описано функції набору даних;

– оптимізовано кількість параметрів із набору даних за допомогою коефіцієнту кореляції Пірсона, оскільки повністю корельовані дані були частково видалені;

– для ідентифікації адміністратора мережі було додано ряд параметрів, які застосовуються при формуванні правил.

В третьому параграфі сформовано правила за допомогою нечіткої логіки для ідентифікації адміністратора у мережі. Також продемонстровано налаштування лінгвістичних змінних та графіки функцій приналежності для параметрів. Результати сформованої та налаштованої моделі показано за допомогою візуалізації. Після налаштування блоку, де використовується нечітка логіка, відбувається навчання нейронної мережі та тестування.

У параграфі 2.4 продемонстровано комп’ютерну мережу із можливими шляхами підключення адміністратора мережі. А параграф 2.5 вказує на оптимальне розташування системи виявлення вторгнень у мережі.

3 СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ У МЕРЕЖІ

3.1 Навчання нейронної мережі

Навчання з вчителем є ключовим підходом у галузі машинного навчання, де алгоритм тренується на великій кількості даних, які вже містять відповіді. Цей метод використовується для того, щоб навчити модель правильно відповідати на питання або розпізнавати певні закономірності, використовуючи вхідні дані разом із відповідями. Основна мета - вивчити коректні зв'язки між вхідними та вихідними даними, щоб у подальшому здатність моделі узагальнювати була високою і вона могла коректно працювати з новими, невідомими даними.

Основні етапи навчання з вчителем нейронної мережі:

– при підготовці даних виконується збір та підготовка навчальних даних, визначення та відокремлення наборів даних для тренувань та тестувань. Важливо також провести стандартизацію або нормалізацію даних для ефективнішого навчання;

– вибір архітектури нейронної мережі, включаючи кількість шарів, кількість нейронів у кожному шарі, функції активації тощо;

– ініціалізація моделі, тобто налаштування початкових параметрів та використання алгоритмів оптимізації для мінімізації помилок в прогнозах моделі на навчальних даних;

– навчання моделі для мінімізації помилок результатів;

– оцінка ефективності навчальної моделі за допомогою тестового набору даних для визначення її точності та генералізації.

Під час навчання з вчителем нейронна мережа здійснює аналіз вхідних даних та здійснює пошук оптимальних ваг та зсувів, щоб вона могла відповідати на вхідні дані з відповідними відповідями. Такий підхід дозволяє вирішувати різноманітні завдання, від класифікації до регресії та виявлення аномалій.

Детальний опис набору даних, поділ на навчальну та тестову вибірку

знаходиться в параграфі 2.2.

3.2 Тестування системи

Дослідження роботи системи в процесі розробки та по завершенню буде відбуватися в кілька етапів:

– під час навчання нейронної мережі;

– під час тестування нейронної мережі;

– в реальній мережі;

– в реальній мережі із набором правил нечіткої логіки для ідентифікації адміністратора.

При оцінюванні якості роботи системи та її окремих компонентів буде застосовано матрицю плутанини, яка зображена на рисунку 3.1.

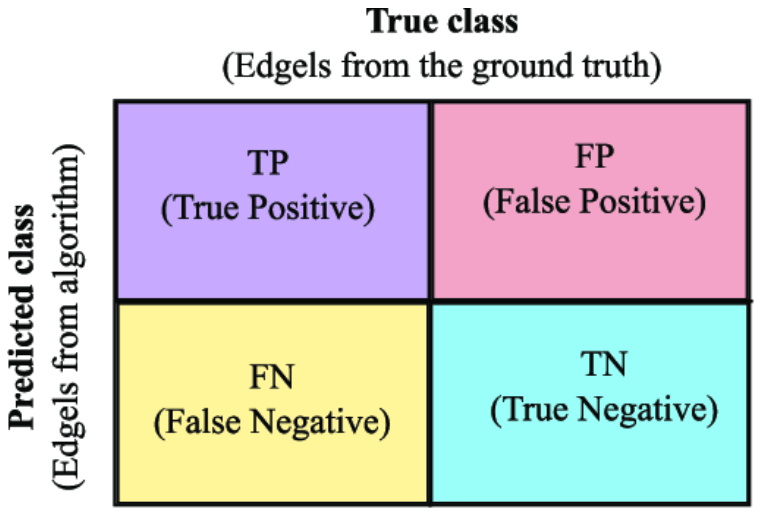


Рисунок 3.1 – Матриця плутанини

У даному випадку:

– TP (True Positive, істинно позитивний) – справжній позитивний результат (TP) виникає, коли система правильно визначає фактичний позитивний випадок. У контексті кібербезпеки це стосується кількості випадків, коли система правильно ідентифікувала фактичні бекдори як бекдори. Це має вирішальне значення для забезпечення того, щоб загрози не були упущені та були належним

чином усунені;

– FP (False Positive, псевдо позитивний) – хибнопозитивний результат виникає, коли система неправильно визначає негативний випадок (не загрозу) як позитивний (загрозу). Наприклад, це стосується кількості разів, коли система неправильно позначала безпечні файли або процеси як бекдори. Велика кількість помилкових спрацьовувань може призвести до непотрібних дій, збоїв і марнування ресурсів, оскільки незагрозливі елементи помилково сприймаються як небезпека;

– TN (True Negative, істинно негативний)– коли система правильно визначає негативний випадок. Це кількість потоків даних або процесів, які правильно визначено як звичайний трафік, який не становить загрози. Це важливо для підтримки ефективності системи та уникнення надмірної тривоги;

– FN (False Negative, псевдо негативний) – хибнонегативний результат виникає, коли системі не вдається визначити позитивний випадок. У описаному сценарії це стосується кількості бекдорів, які неправильно позначені як звичайний трафік. Помилкові негативи особливо небезпечні, оскільки вони представляють загрози безпеці, які система не виявила, потенційно дозволяючи зловмисним діям продовжуватись непоміченими.

Розуміння цих показників є важливим для оцінки ефективності та надійності системи виявлення. Ідеальна система мінімізує як помилкові спрацьовування, так і помилкові негативи, водночас максимізуючи справжні позитивні та справжні негативні сигнали, таким чином точно ідентифікуючи загрози, не перевантажуючи систему помилковими тривогами.

При навчання нейронної мережі у середовищі моделювання було отримано результати, які відображено у таблиці 3.1

Таблиця 3.1 – Результати навчання нейромережі

LSTM (навчання)	TP	TN	FP	FN
	1581	5167	154	165

При тестуванні нейронної мережі у середовищі моделювання було отримано результати, які відображено у таблиці 3.2.

Таблиця 3.2 – Результати тестування нейромережі на наборі даних UNSW-NB15

LSTM (тестування)	TP	TN	FP	FN
	1694	5239	82	52

Для дослідження в реальній мережі було налаштовано локальну мережу, яка складалася із трьох серверів різного призначення, маршрутизатора, ПК, точки доступу та ноутбуків, як показано у параграфі 2.4 на рисунку 2.11. У параграфі 2.5 описано включення системи у мережу. Тестування відбувалося протягом семи календарних днів по 24год кожного дня.

Для здійснення віддаленого доступу адміністратором було використано базові програми, застосовано типові IP-адреси, здійснювалися класичні дії. Зловмисних потоків трафіку у мережі було 28596, а кількість потоків нормального трафіку складала 68715. Загалом проаналізовано 97311 потоків трафіку.

Спочатку протестовано роботу системи у мережі без набору правил для ідентифікації адміністратора. Результати наведено в таблицях 3.3 та 3.4.

Таблиця 3.3 – Результат роботи системи у мережі

LSTM (мережа)	TP	TN	FP	FN
	1694	5239	82	52

Таблиця 3.4 – Час виявлення атаки системою у мережі при використанні різних протоколів

Протокол	Середній час виявлення, с
1	2
FTP	1.33

Кінець таблиці 3.4

1	2
IPSec	0.81
L2TP	0.97
OpenVPN	1.32
PPTP	0.95
RDP	0.89
SSH	1.04
SSTP	1.16
Telnet	1.27

Далі протестовано роботу системи у мережі із набором правил, які використовуються для ідентифікації адміністратора. Слід зазначити, що дії адміністратора та інших користувачів, порушника були ідентичними до попереднього тестування. Тому результати аналізу трафіку залишилися незмінними, як показано у таблиці 3.5. Результати часу, який затрачено для визначення віддаленого доступу порушником, наведено в таблиці 3.6.

Таблиця 3.5 - Результати аналізу трафіку

LSTM (мережа із ідентифікацією адміністратора)	TP	TN	FP	FN
	1694	5239	82	52

Таблиця 3.6 - Час для визначення віддаленого доступу порушником

Протокол	Середній час виявлення, с
1	2
FTP	1.14
IPSec	0.69
L2TP	0.83

Кінець таблиці 3.6

1	2
OpenVPN	1.25
PPTP	0.81
RDP	0.76
SSH	0.98
SSTP	1.03
Telnet	1.14

3.2 Доведення ефективності

На основі отриманих даних можна розрахувати наступні показники продуктивності:

- повнота (Recall) – це метрика, яка вимірює співвідношення достовірно ідентифікованих позитивних випадків нормальноих потоків трафіку) до загальної кількості реально позитивних випадків у даних. Іншими словами, recall показує, наскільки ефективно система виявляє позитивні випадки серед всіх реальних позитивних випадків. Високий показник повноти гарантує, що майже всі реальні позитивні випадки будуть виявлені системою, хоча це також може призвести до підвищення кількості помилкових позитивних результатів:

$$Recall = \frac{TP}{TotalActuallyYes}, \tag{3.1}$$

де

$$TotalActuallyYes = TP + FN \tag{3.2}$$

- точність (Precision) – це метрика, яка вимірює співвідношення достовірно ідентифікованих зловмисних потоків трафіку до загальної кількості ідентифікованих потоків як зловмисних. Ця метрика допомагає оцінити, наскільки

ефективно система ідентифікує дійсно зловмисні дії серед усіх виявлених як такі. Висока точність означає, що більшість потоків, ідентифікованих як зловмисні, дійсно є такими, але це також може вказувати на можливість існування високої кількості помилково негативних результатів, тобто зловмисні дії, які система не виявила.:

$$Precision = \frac{TP}{TotalPredictedYes}, \tag{3.3}$$

де

$$TotalPredictedYes = TP + FP \tag{3.4}$$

- акуратність (Accuracy) – вимірює частку загальної кількості правильних визначень (істинно позитивних та істинно негативних результатів) серед усіх аналізованих випадків. Це означає, що акуратність показує, наскільки ефективно система або модель здатна правильно ідентифікувати як позитивні, так і негативні класи:

$$Accuracy = \frac{TP + TN}{TotalInstances} \tag{3.5}$$

де

$$TotalInstances = TP + FP + FN + TN, \tag{3.6}$$

- помилка (Specificity) – це метрика, яка вимірює здатність системи правильно ідентифікувати незловмисні об'єкти або події як незловмисні. Це важливий показник для визначення того, наскільки добре система уникає помилкових позитивних результатів, тобто помилкового визначення нормальних, безпечних ситуацій як загрозливих:

$$Specificity = \frac{FP + FN}{TP + FP + TN + FN} \quad (3.7)$$

- F1-оцінка (F1-score) – це статистична міра, використовувана для оцінки точності бінарного класифікатора, яка бере до уваги як точність, так і повноту для обчислення середнього гармонічного значення цих двох характеристик. Ця оцінка дуже корисна в ситуаціях, де класи є незбалансованими, тобто один клас значно переважає над іншим, і є потреба знайти баланс між виявленням позитивних випадків та уникненням помилково позитивних випадків:

$$F1score = \frac{Recall + Precision}{2} \quad (3.8)$$

Повнота під час навчання нейромережі:

$$Recall = \frac{1581}{1581 + 165} * 100\% = 90{,}55\% \quad (3.9)$$

Точність під час навчання нейромережі:

$$Precision = \frac{1581}{1581 + 154} * 100\% = 91{,}12\% \quad (3.10)$$

Акуратність під час навчання нейромережі:

$$Accuracy = \frac{1581 + 5167}{1581 + 154 + 165 + 5167} * 100\% = 95{,}49\% \quad (3.11)$$

Помилка під час навчання нейромережі:

$$Specificity = \frac{154 + 165}{1581 + 154 + 165 + 5167} * 100\% = 4{,}51\% \quad (3.12)$$

F1-оцінка під час навчання нейромережі:

$$F1\ score = \frac{90{,}55\% + 91{,}12\%}{2} = 90{,}84\% \quad (3.13)$$

Повнота під час тестування нейромережі:

$$Recall = \frac{1694}{1694 + 52} * 100\% = 97{,}02\% \quad (3.14)$$

Точність під час тестування нейромережі:

$$Precision = \frac{1694}{1694 + 82} * 100\% = 95{,}38\% \quad (3.15)$$

Акуратність під час тестування нейромережі:

$$Accuracy = \frac{1694 + 5239}{1694 + 82 + 52 + 5239} * 100\% = 98{,}1\% \quad (3.16)$$

Помилка під час тестування нейромережі:

$$Specificity = \frac{82 + 52}{1694 + 82 + 52 + 5239} * 100\% = 1{,}9\% \quad (3.17)$$

F1-оцінка під час тестування нейромережі:

$$F1\ score = \frac{97{,}02\% + 95{,}38\%}{2} = 96{,}2\% \quad (3.18)$$

Повнота під час тестування у комп’ютерній мережі:

$$Recall = \frac{27837}{27837 + 759} * 100\% = 97{,}35\% \quad (3.19)$$

Точність під час тестування у комп’ютерній мережі:

$$Precision = \frac{27837}{27837 + 1692} * 100\% = 94{,}27\% \quad (3.20)$$

Акуратність під час тестування у комп'ютерній мережі:

$$Accuracy = \frac{27837 + 67023}{27837 + 1692 + 759 + 67023} * 100\% = 97{,}48\% \quad (3.21)$$

Помилка під час тестування у комп'ютерній мережі:

$$Specificity = \frac{1692 + 759}{27837 + 1692 + 759 + 67023} * 100\% = 2{,}52\% \quad (3.22)$$

F1-оцінка під час тестування у комп'ютерній мережі:

$$F1\ score = \frac{97{,}35\% + 94{,}27\%}{2} = 95{,}81\% \quad (3.23)$$

Порівнюючи результати тестування (таблиця 3.7), слід відмітити, що навчена нейромережа у середовищі моделювання дала показник помилки 1,9%, а повнота становить 97,02%. Після таких результатів у комп'ютерній мережі відсоток помилок становив 2,52%, а повнота 97,35%.

Таблиця 3.7 – Порівняння результатів навчання та тестування

Метрика / Середовище	Повнота	Точність	Акуратність	Помилка	F1-оцінка
Навчання	90,55%	91,12%	95,49%	4,51%	90,84%
Тестування	97,02%	95,38%	98,1%	1,9%	96,2%
Тестування у мережі	97,35%	94,27%	97,48%	2,52%	95,81%

Графічне представлення для порівняння метрик повноти, точності та акуратності показано на рисунку 3.2.

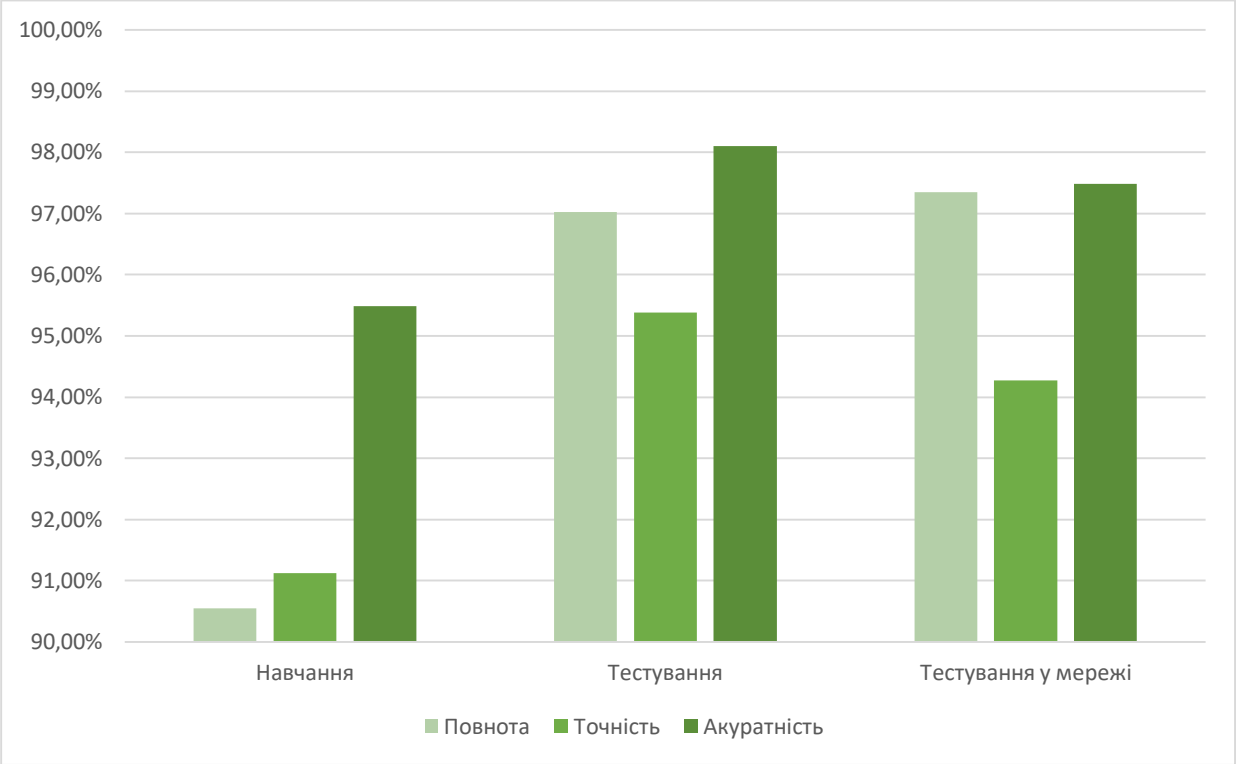


Рисунок 3.2 - Порівняння метрик повноти, точності та акуратності на всіх етапах тестування

Графічне представлення для порівняння метрики F1-оцінки показано на рисунку 3.3.

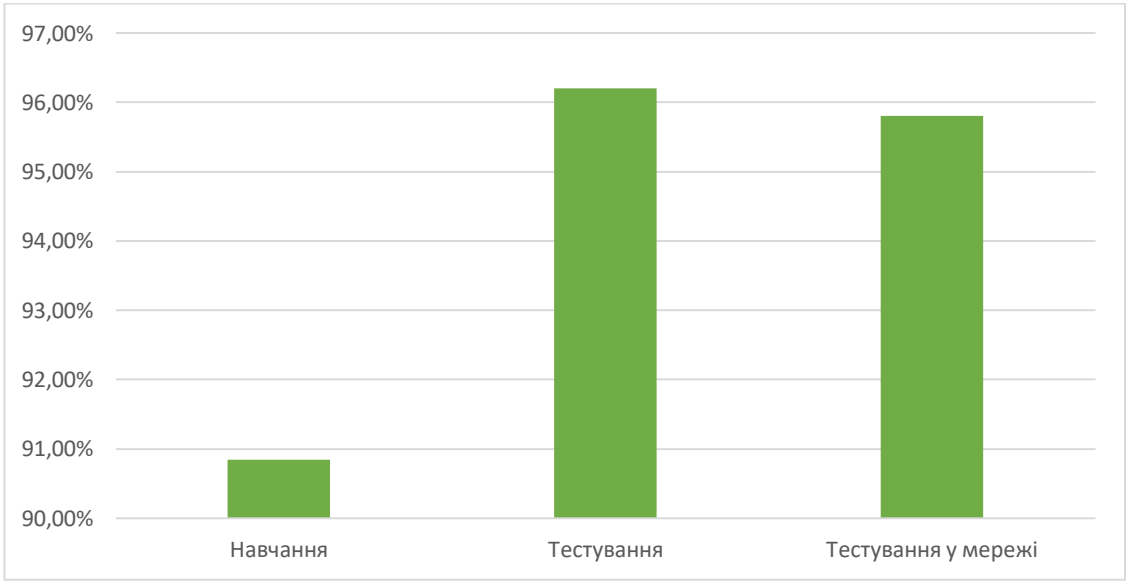


Рисунок 3.3 – Порівняння метрики F1-оцінки на всіх етапах тестування

Графічне представлення для порівняння метрики помилки показано на рисунку 3.4.

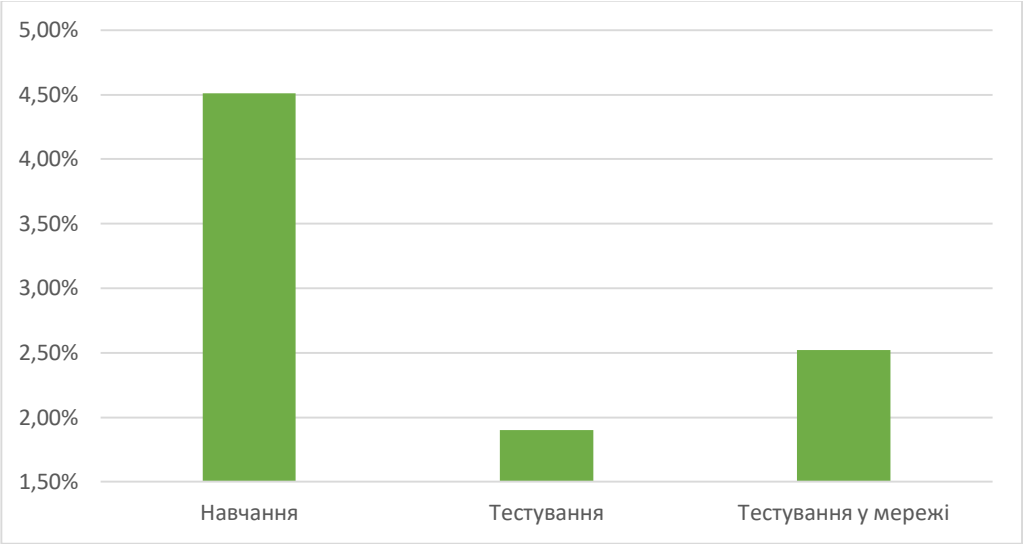


Рисунок 3.4 – Порівняння метрики помилки на всіх етапах тестування

Графічне представлення для порівняння середнього часу виявлення віддаленого доступу без ідентифікації трафіку адміністратора та з ідентифікацією відображено на рисунку 3.5.

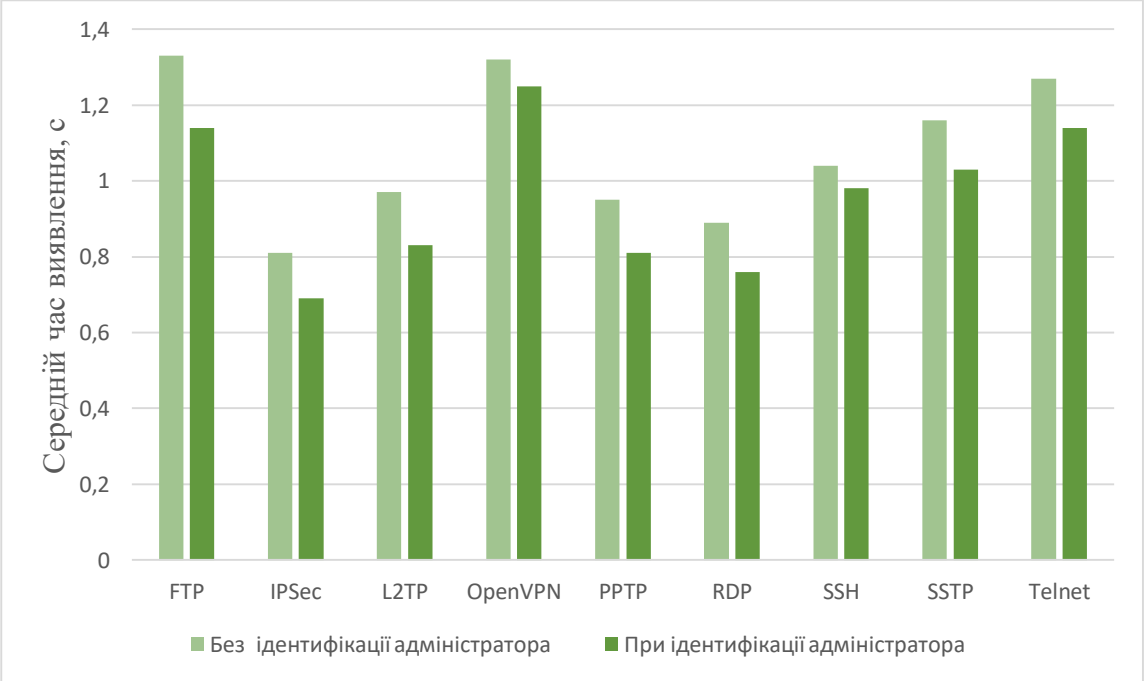


Рисунок – Порівняння без та з ідентифікацією трафіку адміністратора мережі

3.3 Висновки до розділу

У даному розділі було проведено навчання та тестування нейронної мережі, що використовує навчання з вчителем. Через цей підхід змогли досягти значних успіхів у точності та ефективності виявлення бекдорів у мережі. Основною перевагою навчання з вчителем є його здатність ефективно узагальнювати навчальні дані та застосовувати отримані знання для ідентифікації нових, невідомих раніше випадків. Впродовж дослідження було проведено різні етапи роботи з моделлю: від підготовки даних, їх нормалізації, вибору архітектури мережі, її тренування до оцінки результативності. Тестування в реальному середовищі підтвердило ефективність розробленої системи і дало змогу оцінити її практичну придатність. На завершення, дослідження підтверджує важливість розробки та застосування комплексних систем машинного навчання для забезпечення кібербезпеки. Результати роботи показують, що застосування нейронних мереж дозволяє значно підвищити рівень захисту мережевих систем від зловмисних загроз, а також забезпечити високу адаптивність та гнучкість у виявленні та нейтралізації потенційних атак.

ВИСНОВКИ

Проблема зловмисного трафіку в мережі стає все більш актуальною через зростання кількості та складності кібератак. Це підкреслює важливість розробки ефективних систем виявлення вторгнень для забезпечення кібербезпеки. У даній кваліфікаційній роботі було здійснено розробку системи виявлення вторгнень у мережі за допомогою Matlab та нечіткої логіки.

В ході роботи виконано наступні завдання:

– змодельовано систему виявлення вторгнень за допомогою Matlab та нечіткої логіки, що дозволило обробляти невизначеність і аномалії в мережевому трафіку;

– розроблено схему інтеграції системи в існуючу комп'ютерну мережу, враховуючи необхідність мінімізації впливу на продуктивність мережі;

– створено детальний алгоритм аналізу мережевого трафіку та виявлення зловмисних з’єднань;

– налаштовано тестове середовище для перевірки різних сценаріїв кібератак;

– проведено аналіз результатів тестувань для оцінки ефективності розробленої системи.

Детально описано метод сигнатурного аналізу, реалізований за допомогою засобів нечіткої логіки. Також відображено переваги рекурентної нейронної мережі довгої короткочасної пам’яті для аналізу мережевого трафіку, що забезпечує ефективне виявлення зловмисних дій. Здійснено детальний аналіз набору даних UNSW-NB15. Визначено категорії даних, необхідні для виявлення віддаленого доступу, оптимізовано кількість параметрів за допомогою коефіцієнту кореляції Пірсона та додано нові параметри для формування правил ідентифікації адміністратора мережі. Створено правила за допомогою нечіткої логіки для ідентифікації адміністратора мережі, налаштовано лінгвістичні змінні та графіки функцій приналежності. Результати показано за допомогою візуалізації, а також проведено навчання і тестування нейронної мережі для

підвищення точності та ефективності системи.

Проведене навчання нейронної мережі з використанням навчання з вчителем дозволило досягти значних успіхів у точності та ефективності виявлення бекдорів у мережі. Основною перевагою цього підходу є здатність узагальнювати навчальні дані та застосовувати отримані знання для ідентифікації нових, невідомих раніше випадків.

Тестування в реальному середовищі підтвердило ефективність розробленої системи і дало змогу оцінити її практичну придатність. Дослідження підтверджує важливість розробки та застосування комплексних систем машинного навчання для забезпечення кібербезпеки. Результати роботи показують, що застосування нейронних мереж дозволяє значно підвищити рівень захисту мережевих систем від зловмисних загроз, а також забезпечити високу адаптивність та гнучкість у виявленні та нейтралізації потенційних атак.

Розробка та впровадження систем виявлення вторгнень на основі нечіткої логіки та нейронних мереж є важливою для сучасної кібербезпеки. Вона забезпечує надійний захист від постійно еволюціонуючих загроз, підвищуючи рівень безпеки інформаційних систем і мереж. А подальші дослідження та вдосконалення даної системи сприятимуть створенню ще більш ефективних інструментів для боротьби з кібератаками, забезпечуючи безпеку і стабільність роботи мережевих інфраструктур.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Задерейко О. В. Комп’ютерні мережі [Електронний ресурс] : навчальний посібник / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса, 2022. – 249 с.

2. Мєшков, В. (2023). Аналіз систем інтелектуального моніторингу трафіку комп’ютерної мережі для систем виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security, 1, 85–92, doi: https://doi.org/10.32782/IT/2023-1-11

3. Голубничий Д.Ю. Технології аудиту кібербезпеки інформаційних систем / Д.Ю. Голубничий, О.В. Коломійцев, В.Ф. Третяк, С.Г. Рязанін // Scientific Collection «InterConf», (36): with the Proceedings of the 7th International Scientific and Practical Conference «Challenges in Science of Nowadays» (November 26 - 28, 2020) in Washington, USA: EnDeavours Publisher, 2020. – Pp. 333 – 342.

4. Shpinareva, I. M., A. A. Yakushina, L. A. Voloshchuk, і N. D. Rudnichenko. «Detection and Classification of Network Attacks Using the Deep Neural Network Cascade». Вісник сучасних інформаційних технологій, вип. 4, вип. 3, Березень 2021, с. 244-5, doi:10.15276/hait.03.2021.4.

5. Толкаченко, Є. А., Данилюк, В. С., Семенюк, М. О., Фльора, А. С. Огляд сучасних методів в системах виявлення вторгнень для потреб інформаційнотелекомунікаційних систем спеціального призначення. Водний транспорт, 2021, 57-61

6. Fotiadou, K.; Velivassaki, T.-H.; Voulkidis, A.; Skias, D.; Tsekeridou, S.; Zahariadis, T. Network Traffic Anomaly Detection via Deep Learning. Information 2021, 12, 215. https://doi.org/10.3390/info12050215

7. Ahamed, Uthumansa & Fernando, Shantha. (2020). Identifying the Impacts of Active and Passive Attacks on Network Layer in a Mobile Ad-hoc Network: A Simulation Perspective. International Journal of Advanced Computer Science and Applications. 11. 600-605. 10.14569/IJACSA.2020.0111173.

8. Passive Attack in Cybersecurity. URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-passive-attack

(дата звернення 17.03.2024)

9. Kovtsur, M., Muthanna, A., Konovalova, V., Georgii, A., Olga, S. (2023). Study of Methods for Remote Interception of Traffic in Computer Networks. In: Abd El-Latif, A.A., Maleh, Y., Mazurczyk, W., ELAffendi, M., I. Alkanhal, M. (eds) Advances in Cybersecurity, Cybercrimes, and Smart Emerging Technologies. CCSET 2022. Engineering Cyber-Physical Systems and Critical Infrastructures, vol 4. Springer, Cham. https://doi.org/10.1007/978-3-031-21101-0_26

10. Bloch, F., Chatterjee, K. and Dutta, B. (2023), Attack and interception in networks. Theoretical Economics, 18: 1511-1546. https://doi.org/10.3982/TE5122

11. Walters, R. (2023). Illegal Interception of Data. In: Cybersecurity and Data Laws of the Commonwealth. Springer, Singapore. https://doi.org/10.1007/978-981-99-3935-0_17

12. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333. https://doi.org/10.3390/electronics12061333

13. W. Jia, "Analysis on Password Attack Model and Password Generation," 2022 International Conference on Computers, Information Processing and Advanced Education (CIPAE), Ottawa, ON, Canada, 2022, pp. 145-149, doi: 10.1109/CIPAE55637.2022.00038.

14. Ali Hameed Yassir Mohammed; Dziyauddin, Rudzidatul Akmam; Liza Abdul Latiff. International Journal of Advanced Computer Science and Applications; West Yorkshire Vol. 14, Iss. 1, (2023). DOI:10.14569/IJACSA.2023.0140119

15. Baah, E.K. et al. (2022). Enhancing Port Scans Attack Detection Using Principal Component Analysis and Machine Learning Algorithms. In: Ahene, E., Li, F. (eds) Frontiers in Cyber Security. FCS 2022. Communications in Computer and Information Science, vol 1726. Springer, Singapore. https://doi.org/10.1007/978-981-19-8445-7_8

16. J. Zhao, L. Yang, C. Zhang and J. Zhang, "Research on the Speed and Accuracy of Full Port Scanning," 2023 IEEE 6th Information Technology,Networking,Electronic and Automation Control Conference (ITNEC),

Chongqing, China, 2023, pp. 1159-1162, doi: 10.1109/ITNEC56291.2023.10082257.

17. H. Wu, Z. Shao, G. Cheng, X. Hu, J. Ren and W. Wang, "Detecting Slow Port Scans of Long Duration in High-Speed Networks," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 3405-3410, doi: 10.1109/GLOBECOM48099.2022.10001708.

18. Nmap for PenTester. URL: https://medium.com/@rajeevranjancom/nmap-for-pentester-2ad0b4e9ec (дата звернення 7.04.2024)

19. Jajula, S.K., Tripathi, K., Bajaj, S.B. (2023). Review of Detection of Packets Inspection and Attacks in Network Security. In: Dutta, P., Chakrabarti, S., Bhattacharya, A., Dutta, S., Piuri, V. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems, vol 491. Springer, Singapore. https://doi.org/10.1007/978-981-19-4193-1_58

20. Ruhani, A. B., & Zolkipli, M. (2023). Keylogger: The Unsung Hacking Weapon. Borneo International Journal EISSN 2636-9826, 6(1), 33-43. Retrieved from https://majmuah.com/journal/index.php/bij/article/view/339

21. What is a keylogger? URL: https://www.malwarebytes.com/keylogger (дата звернення 18.04.2024)

22. Sharma, Hitesh and Singh, Sheshank and Sharma, Anil and Singh, Manpreet, Detecting and Defending Keystroke Logger Attacks (May 5, 2023). Kilby 100: 7th International joint conference on computing sciences, http://dx.doi.org/10.2139/ssrn.4485464

23. Siddiqi, M.A.; Pak, W.; Siddiqi, M.A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. Appl. Sci. 2022, 12, 6042. https://doi.org/10.3390/app12126042

24. Kaouthar Chetioui, Birom Bah, Abderrahim Ouali Alami, Ayoub Bahnasse, Overview of Social Engineering Attacks on Social Networks, Procedia Computer Science, Volume 198,2022,Pages 656-661,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2021.12.302.

25. Common Weakness Enumeration: CWE. URL: https://cwe.mitre.org/ (дата звернення 23.04.2024)

26. CVE. URL: https://cve.mitre.org/ (дата звернення 23.04.2024)

27. Common Vulnerability Scoring System version 4.0: Specification Document. URL: https://www.first.org/cvss/specification-document (дата звернення 17.05.2024)

28. W. Wang, F. Shi, M. Zhang, C. Xu and J. Zheng, "A Vulnerability Risk Assessment Method Based on Heterogeneous Information Network," in IEEE Access, vol. 8, pp. 148315-148330, 2020, doi: 10.1109/ACCESS.2020.3015551.

29. Liu, Yingqi and Shen, Guangyu and Tao, Guanhong and Wang, Zhenting and Ma, Shiqing and Zhang, Xiangyu. Complex Backdoor Detection by Symmetric Feature Differencing, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), June, 2022, pp. 15003-15013

30. Robin Mayerhofer and Rudolf Mayer. 2022. Poisoning Attacks against Feature-Based Image Classification. In Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy (CODASPY '22). Association for Computing Machinery, New York, NY, USA, 358–360. https://doi.org/10.1145/3508398.3519363

31. Kaiyang Wang, Huaxin Deng, Yijia Xu, Zhonglin Liu, Yong Fang, Multi-target label backdoor attacks on graph neural networks, Pattern Recognition,Volume 152, 2024, 110449, ISSN 0031-3203, https://doi.org/10.1016/j.patcog.2024.110449.

32. Y. Li, S. Zhang, W. Wang and H. Song, "Backdoor Attacks to Deep Learning Models and Countermeasures: A Survey," in IEEE Open Journal of the Computer Society, vol. 4, pp. 134-146, 2023, doi: 10.1109/OJCS.2023.3267221.

33. Introduction to TELNET. URL: https://www.geeksforgeeks.org/introduction-to-telnet/ (дата звернення 19.04.2024)

34. What Is File Transfer Protocol (FTP) and What Is It Used for? URL: https://www.investopedia.com/terms/f/ftp-file-transfer-protocol.asp (дата звернення 19.04.2024)

35. What is the Secure Shell (SSH) Protocol? | SSH Academy. URL: https://www.ssh.com/academy/ssh/protocol (дата звернення 20.04.2024)

36. What is remote desktop protocol (RDP)? URL: https://www.techtarget.com/searchenterprisedesktop/definition/Remote-Desktop-

Protocol-RDP (дата звернення 21.04.2024)

37. Understanding Point-to-Point Tunneling Protocol (PPTP). URL:https://wwwdisc.chimica.unipd.it/luigino.feltre/pubblica/unix/winnt_doc/pppt/understanding_pptp.html (дата звернення 25.04.2024)

38. Layer 2 Tunnel Protocol. URL: https://www.ibm.com/docs/en/i/7.4?topic=concepts-layer-2-tunnel-protocol (дата звернення 25.04.2024)

39. What is IPsec (Internet Protocol Security)? URL: https://www.pynetlabs.com/what-is-ipsec-internet-protocol-security/ (дата звернення 27.04.2024)

40. Коробейнікова, Т & Цар, О. (2023). АНАЛІЗ СУЧАСНИХ ВІДКРИТИХ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ. Grail of Science. 317-325. 10.36074/grail-of-science.12.05.2023.050.

41. What is Intrusion Detection Systems (IDS)? How does it Work? URL: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system (дата звернення 28.04.2024)

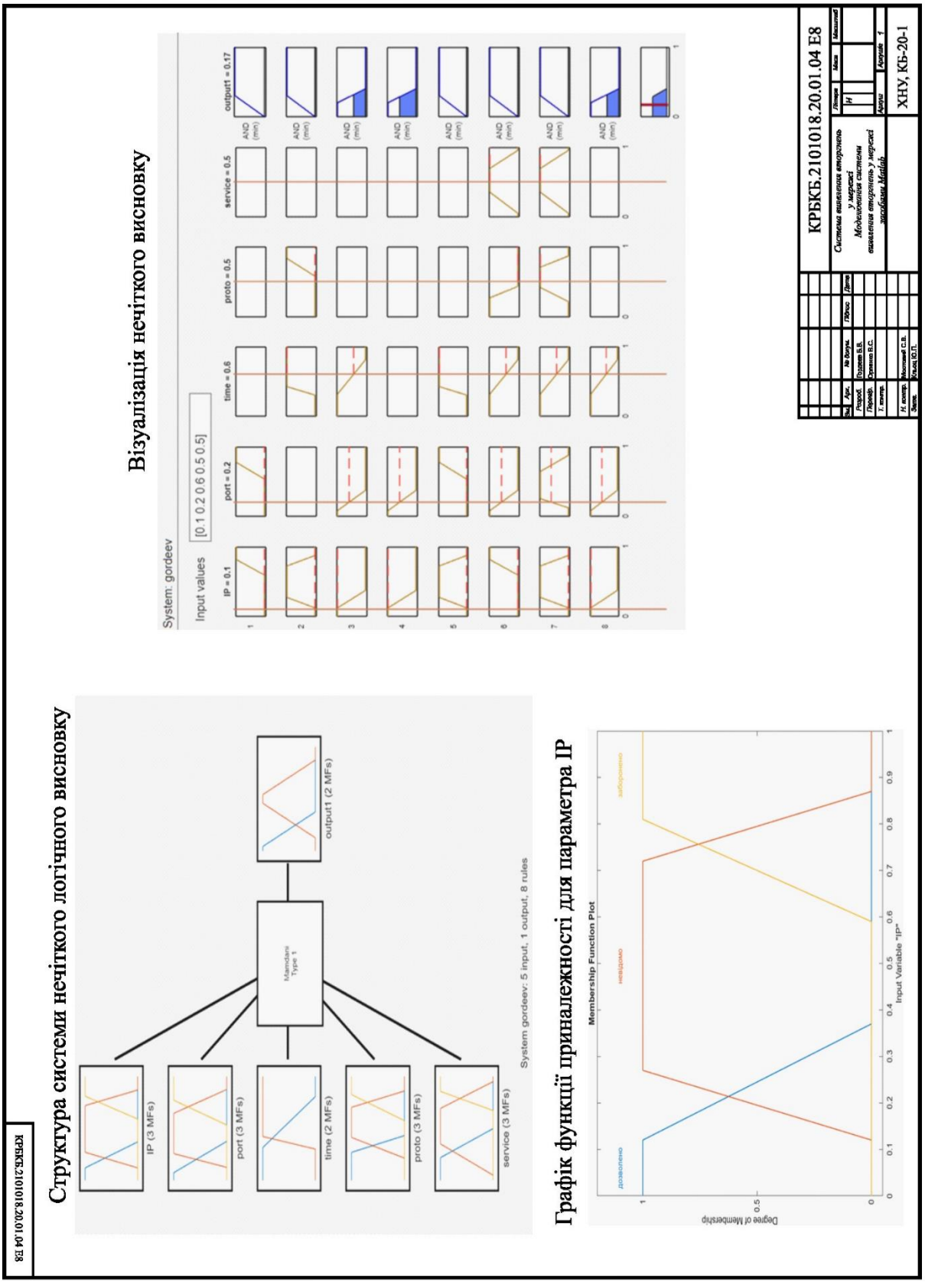
42. Hosted IDS: Host-based intrusion detection system. URL: https://cybersecurity.att.com/solutions/host-intrusion-detection-system (дата звернення 3.05.2024)

43. Maheswaran, N., Bose, S., Logeswari, G., Anitha, T. (2023). Hybrid Intrusion Detection System Using Machine Learning Algorithm. In: Khanna, A., Polkowski, Z., Castillo, O. (eds) Proceedings of Data Analytics and Management . Lecture Notes in Networks and Systems, vol 572. Springer, Singapore. https://doi.org/10.1007/978-981-19-7615-5_30

ДОДАТОК А

(обов'язковий)

Копія графічної частини



Алгоритм підготовки та навчання нейронною мережею

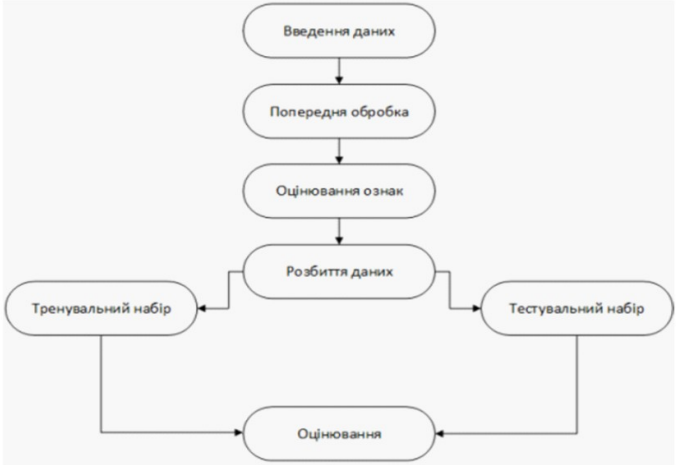
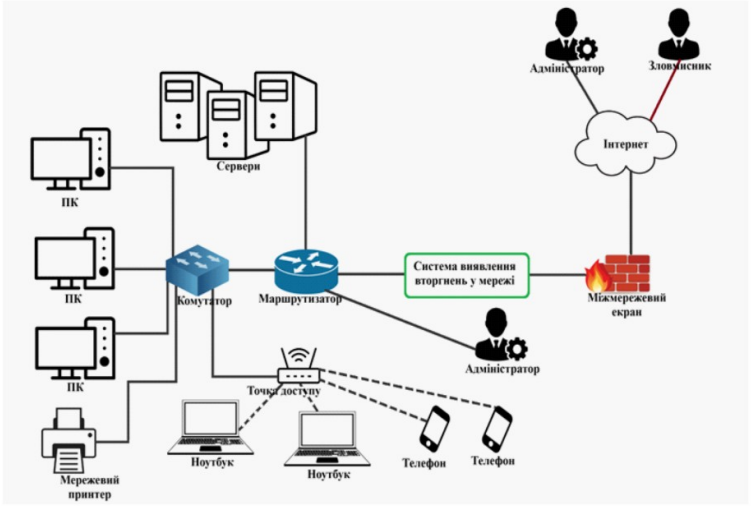
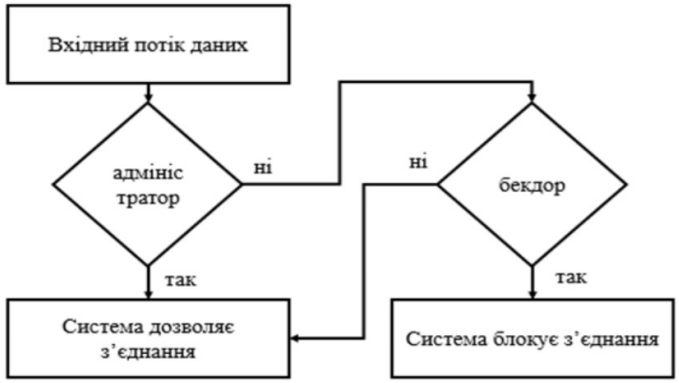


Схема включення системи виявлення вторгнень у мережі

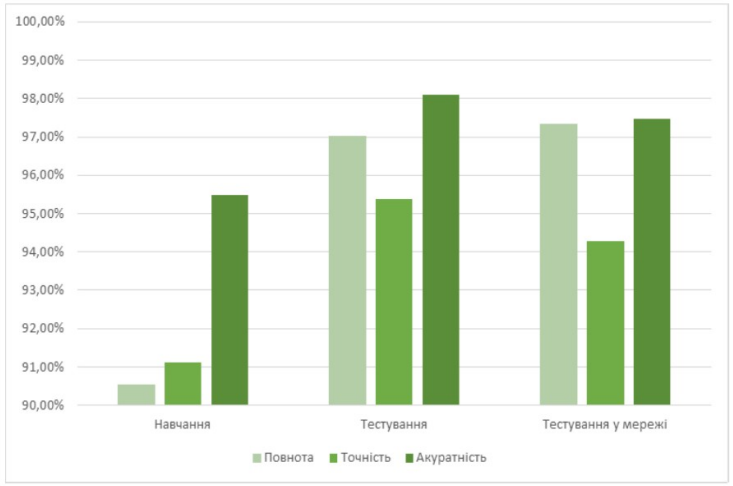


Алгоритм роботи системи виявлення вторгнень у мережі

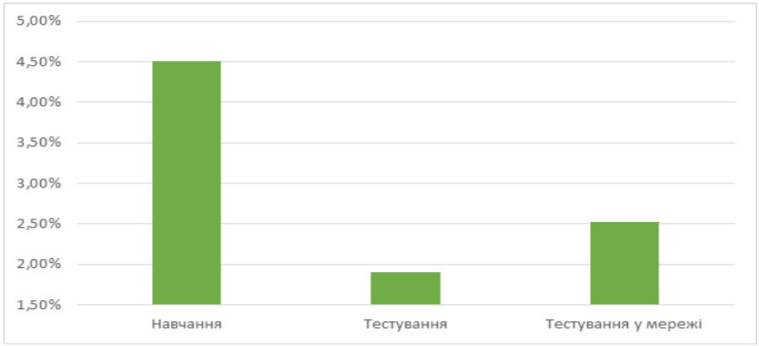


					КРБКБ.2101018.20.01.04 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	*Система виявлення вторгнень у мережі* *Алгоритм роботи системи виявлення вторгнень у мережі*	Літера: Н; Маса; Масштаб
Розроб.		Годзєв Б.В.				
Перевір.		Орлянко В.С.				Аркуш 1; Аркушів
Т. контр.						
Н. контр.		Мостовий С.В.			ХНУ, КБ-20-1	
Затв.		Кільоц Ю.П.				

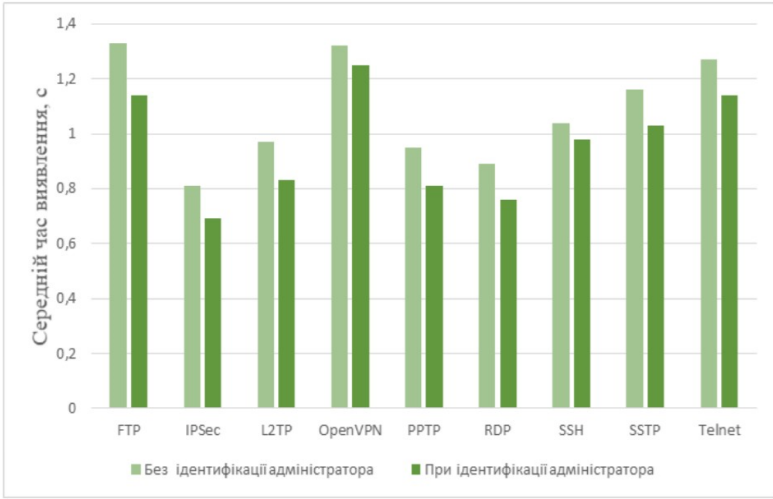
Порівняння метрик повноти, точності та акуратності на всіх етапах тестування



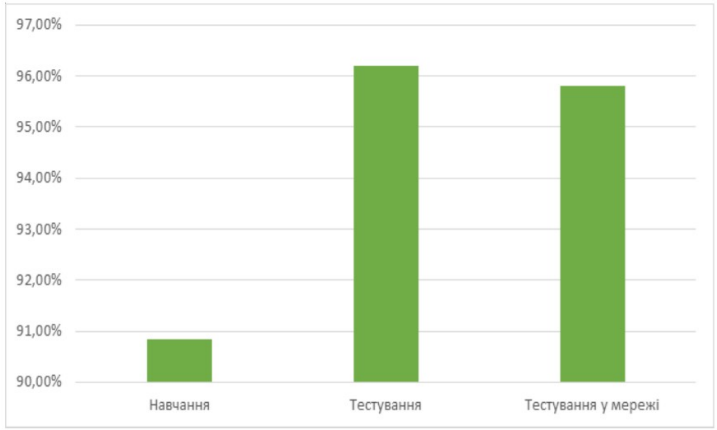
Порівняння метрики помилки на всіх етапах тестування



Порівняння роботи системи виявлення вторгнень у мережі без та з ідентифікацією трафіку адміністратора мережі



Порівняння метрики F1-оцінки на всіх етапах тестування



						КРБКБ.2101018.20.01.04 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлення вторгнень у мережі. Оцінка достовірності роботи системи виявлення вторгнень у мережі	Літера	Маса	Масштаб
Розроб.		Годаєв Б.В.				Н		
Перевір.		Орленко В.С.				Аркуш	Аркушів 1	
Т. контр.						ХНУ, КБ-20-1		
Н. контр.		Мостовий С.В.						
Затв.		Кільох Ю.П.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Гордєєва Богдана Віталійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений 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.

10.06.2024
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

	Документ		Сумарний збіг по Базі Даних	
ID: 129625 Назва: Система виявлення вторгнень у мережі Додано в БД: 2024-06-11 Автора: Гордєєв Б.В, Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	69698	569	944 (1%)	12 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016347107

Дата перевірки:
11.06.2024 12:37:42 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
11.06.2024 22:32:02 EEST

ID користувача:
100008300

Назва документа: **Гордєєв_записка плагіат**

Кількість сторінок: 59 **Кількість слів:** 10219 **Кількість символів:** 79671 **Розмір файлу:** 5.42 MB **ID файлу:** 1016148839

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

2.6%
Схожість

Найбільша схожість: 0.79% з джерелом з Бібліотеки (ID файлу: 1016148836)

1.9% Джерела з Інтернету	131	Сторінка 61
1.21% Джерела з Бібліотеки	35	Сторінка 62

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	1
Підозріле форматування	9 сторінок

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: Система виявлення вторгнень у мережі

Автор: Гордєєв Богдан Віталійович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Орленко Вікторія Сергіївна, канд. техн. наук, 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 97,4%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Вікторія ОРЛЕНКО

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Гордєєв Богдан Віталійович

Тема Система виявлення вторгнень у мережу

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 63.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена система виявлення вторгнень у мережу. Система базується на пошуку бекдорів. Складається з двох компонентів: засобами нечіткої логіки визначається віддалений доступ адміністратора мережі, а весь інший мережевий трафік що не ідентифікований як дозволений адміністративний доступ аналізується навченою нейронною мережею. Для розробки системи було проведено детальний аналіз протоколів віддаленого доступу та побудовано алгоритми роботи.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі роботи описано класифікацію мережевих атак та характеристику протоколів віддаленого доступу. Другий розділ присвячено опису набору даних та його нормалізації, який використовуватиметься для навчання та тестування, розроблено алгоритм роботи системи, описано правила нечіткої логіки для ідентифікації адміністратора. В третьому розділі проведено навчання нейронної мережі, здійснено розрахунок достовірності роботи системи.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Вона полягає у захисті системи від несанкціонованого доступу.

5. Негативні сторони роботи В разі компрометації облікового запису адміністратора чи використання параметрів, які характеризують діяльність адміністратора, порушники можуть проникнути до комп'ютерної мережі видавши себе за легітимного користувача відповідно до правил нечіткої логіки .

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

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

« 12 » червня 2024 (підпис)