Міністерство освіти і науки України

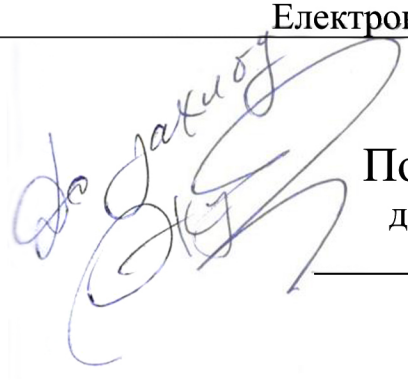
Український державний університет науки і технологій

Комп'ютерні технології і системи

(назва факультету)

Електронні обчислювальні машини

(повна назва кафедри)



Пояснювальна записка

до кваліфікаційної роботи

другий (магістерський)

(ступінь вищої освіти)

на тему: Дослідження комбінованого варіанту на основі нейронних мереж щодо виявлення мережевих атак в інформаційній системі залізничного транспорту

за освітньою програмою Комп'ютерна інженерія

зі спеціальності: 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

Виконав: студент групи: КС2322

(підпис студента) / Денис МАРТИНЯК / (Ім'я ПРІЗВИЩЕ)

Керівник: (підпис) / доцент Вікторія ПАХОМОВА / (посада, Ім'я ПРІЗВИЩЕ)

Нормоконтролер: (підпис) /доцент Олег ЄГОРОВ / (посада, Ім'я ПРІЗВИЩЕ)

Консультанти:

(назва розділу) (підпис) / / (посада, Ім'я ПРІЗВИЩЕ)

(назва розділу) (підпис) / / (посада, Ім'я ПРІЗВИЩЕ)

(назва розділу) (підпис) / / (посада, Ім'я ПРІЗВИЩЕ)

(назва розділу) (підпис) / / (посада, Ім'я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент (підпис)

Дніпро – 2025 рік

Ministry of Education and Science of Ukraine
Ukrainian State University of Science and Technologies

Computer Technologies and Systems
(faculty)

Electronic Computing Machines
(department)

Explanatory Note
to Master's Thesis
other (master's)
(higher education degree)

on the topic: Study of a combined variant based on neural networks to detect network attacks in the information system of railway transport

according to educational curriculum Computer Engineering

in the Speciality: Computer Engineering 123
(speciality and its code)

Done by the student of the group: KC2322 / Denis MARTYNIAK /
(name, surname)

Scientific Supervisor: /Docent Victoria PAKHOMOVA /
(position, name, surname)

Normative controller : /Docent Oleg YEHOROV /
(position, name, surname)

Supervisors

(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)

Dnipro – 2025

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи
Кафедра: Електронні обчислювальні машини
Рівень вищої освіти: другий (магістерський)
Освітня програма: Комп'ютерна інженерія
Спеціальність:123 Комп'ютерна інженерія
(шифр та назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ЕОМ
_____ Ігор ЖУКОВИЦЬКИЙ
(підпис) (Ім'я ПРІЗВИЩЕ)
Дата _____

ЗАВДАННЯ

на кваліфікаційну роботу другий (магістерський)
(ступінь вищої освіти)

студенту Мартиняк Денису Сергійовичу
(Прізвище, Ім'я По батькові)

1. Тема роботи: Дослідження комбінованого варіанту на основі нейронних мереж щодо виявлення мережевих атак в інформаційній системі залізничного транспорту
Керівник роботи: Пахомова Вікторія Миколаївна, к.т.н., доцент кафедри ЕОМ
(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від "16" 09 2024 р. № 1116

2. Строк подання студентом роботи: 22.01.2025 р.
3. Вихідні дані до роботи: база даних з параметрами мережевого трафіку NSL-KDD
4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати): ВСТУП. ОГЛЯД І АНАЛІЗ ПРЕДМЕТА ДОСЛІДЖЕНЬ. ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ. ПЕРЕЛІК ПОСИЛАНЬ. ДОДАТКИ.
4.1 Аналітична частина:
огляд нейронних мереж, що придатні для виявлення мережевих атак, а також їх комбінованих варіантів
4.2 Основна частина:
постановка задачі;
пропонуємий комбінований варіант для дослідження;
створення нейронних мереж, що надходять до комбінованого варіанту
4.3 Дослідницька частина:
визначення оптимальних параметрів на створених нейронних мережах;
оцінювання параметрів якості виявлення мережевих атак на основі комбінованого варіанту

6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав: (підпис консультанта, дата)	Завдання прийняв: (підпис студента, дата)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Вступ	06.01.2025-09.01.2025	5 %
2	Огляд нейронних мереж, що придатні для виявлення мережевих атак, а також їх комбінованих варіантів	04.11.2024-10.11.2024	20 %
3	Постановка задачі	11.11.2024-13.11.2024	10 %
4	Комбінований варіант у якості основного методу розв'язання задачі	14.11.2024-20.11.2024	15 %
5	Створення нейронних мереж, що надходять до комбінованого варіанту	21.11.2024-15.12.2024	15 %
6	Визначення оптимальних параметрів на створених нейронних мережах	16.12.2024-22.12.2024	15 %
7	Оцінювання параметрів якості виявлення мережевих атак на основі комбінованого варіанту	23.12.2024-29.12.2024	15 %
8	Висновки та рекомендації	06.01.2025-09.01.2025	5 %
9	Подання кваліфікаційної роботи до кафедри	22.01.2025	
10	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії		

Студент _____ (підпис) Денис МАРТИНЯК (Ім'я ПРІЗВИЩЕ)

Керівник роботи _____ (підпис) Вікторія ПАХОМОВА (Ім'я ПРІЗВИЩЕ)

Міністерство освіти і науки України

Український державний університет науки і технологій

Відгук керівника

кваліфікаційної роботи *магістра*

Студент групи *КС2322* *Мартиняк Дениса Сергійовича*

Тема випускної роботи: *Дослідження комбінованого варіанту на основі нейронних мереж щодо виявлення мережевих атак в інформаційній системі залізничного транспорту*

1. Якісні відмінності кваліфікаційної роботи: автором проведено дослідження *комбінованого варіанту на основі наступних нейронних мереж: багатошарового перцептрона; нейронечіткої мережі; самоорганізуючої карти Кохонена щодо виявлення мережевих атак категорій DOS, PROBE, U2R, R2L в інформаційній системі залізничного транспорту. У якості засобів створення нейронних мереж використані пакети Neural Network Toolbox та Fuzzy Logic Toolbox системи MatLAB. Проведено оцінювання параметрів якості виявлення мережевих атак для модифікованого варіанту з результатами дослідження комбінованого варіанту, що запропонований раніше іншими науковцями.*

2. Зауваження: *відсутнє дослідження кількості прихованих нейронів MLP*

3. Висновок щодо дотримання академічної доброчесності *порушення вимог академічної доброчесності відсутні*

Комплексна оцінка кваліфікаційної роботи: *здобувачем виконанні всі завдання, що поставлені відповідно до мети кваліфікаційної роботи; основні рішення автор приймав самостійно; рівень сформованості програмних результатів навчання згідно освітньої програми «Комп'ютерна інженерія»; посилання на використані інформаційні джерела коректні; ознаки академічної недоброчесності відсутні; кваліфікаційна робота оформлена якісно; кваліфікаційна робота заслуговує на високу оцінку за умови відповідного захисту, а її автор присвоєння йому освітнього ступеня «магістр» за спеціальністю 123 «Комп'ютерна інженерія».*

Керівник: *доцент* Вікторія ПАХОМОВА

Дата: 23.01.2025

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи другий (магістерський): 50 с., 42 рис., 20 табл., 4 додатки, 25 джерел.

У магістерській роботі виконано дослідження комбінованого варіанту на основі нейронних мереж для виявлення мережевих атак в інформаційній системі залізничного транспорту. Основу дослідження складають такі моделі: багатошаровий персептрон, нейронечітка мережа, мережа Кохонена та нейронечітка мережа. Для класифікації використовувались багатошаровий персептрон, мережа Кохонена та нейронечітка мережа.

Нейронечітка мережа, багатошаровий персептрон та мережа Кохонена були реалізовані за допомогою середовища MatLAB. У ході дослідження було визначено оптимальні параметри кожної моделі, а також проведено оцінку якості окремо для кожної мережі та для їх комбінованого використання.

Для багатошарового персептрону досліджено розмір навчальної вибірки, алгоритми навчання та визначено оптимальний розмір прихованого шару. У випадку з нейронечіткою мережею перевірялися методи навчання та ефективність вибірки, а також оцінювалася адекватність моделі після навчання. Для мережі Кохонена оптимізували розмір карти та аналізували результати залежно від розміру вибірки.

Якість роботи моделей оцінювалася окремо для кожної нейромережі. Найкращі результати показав багатошаровий персептрон. При комбінованому підході також було підтверджено перевагу багатошарового персептрону.

Ключові слова: АТАКА, КАТЕГОРІЯ, БАГАТОШАРОВИЙ ПЕРСЕПТРОН, МЕРЕЖА КОХОНЕНА, НЕЙРОНЕЧІТКА МЕРЕЖА, КОМБІНОВАНИЙ ПІДХІД.

ЗМІСТ

ВСТУП

З розвитком інформаційних технологій та зростанням кількості кіберзагроз, ефективне виявлення мережевих атак стає однією з головних задач у сфері кібербезпеки. Традиційні методи виявлення, такі як антивірусні програми чи системи виявлення вторгнень (IDS), не завжди здатні адекватно реагувати на нові або змінені типи атак через свою обмежену здатність до адаптації. У зв'язку з цим, методи на основі нейронних мереж, зокрема комбінації різних типів нейронних мереж, набувають все більшої популярності, оскільки вони здатні аналізувати великі обсяги даних та виявляти складні патерни, що вказують на потенційні загрози.

Серед найбільш перспективних підходів для виявлення мережевих атак є використання комбінацій таких нейронних мереж, як MLP (Multilayer Perceptron), ANFIS (Adaptive Neuro-Fuzzy Inference System), SOM (Self-Organizing Maps). Кожен з цих методів має свої переваги, зокрема здатність до обробки різноманітних типів даних та адаптації до змін у мережевому трафіку.

Мета дослідження: порівняльний аналіз параметрів якості визначення мережевих атак з використанням комбінованого варіанту, що складається із наступних нейронних мереж: ANFIS, MLP та SOM

Були поставлені такі завдання:

1. Виконати огляд нейронних мереж щодо виявлення мережевих атак
2. Створення нейронних мереж, що надходять до комбінованого варіанту;
3. Визначення оптимальних параметрів на створених нейронних мережах;
4. Оцінювання параметрів якості виявлення мережевих атак на основі комбінованого варіанту

На сучасному етапі виявлення мережевих атак на комп’ютерні мережі з використанням нейронних мереж займаються вчені та науковці з різних держав: В.М. Пахомова, М.С. Коннов, І. Грішин, Козьменко, І. Школьник, А. Бухтіарова, В. Лутсенко, М.А. Мотиленко, Маслак А.В.; S. B. B. S. P. R. M. Arumugam, S. R. K. Dinesh, M. K. N. Iyyappan; N. S. Kumar, P. P. K. Iyer, M. S. J. Krishnan; M. A. Hossain, M. A. Rahman, S. S. Islam. В.М. Пахомова та М.С.

Коннов порівняли два підходи до виявлення мережевих атак: використання багатошарового персептрона та ансамблю з п’яти нейронних мереж. І. Грішин досліджував комбіноване застосування багатошарового персептрона та самоорганізуючих карт Кохонена для виявлення комп’ютерних атак. Козьменко, І. Школьник та А. Бухтіарова аналізували динаміку розвитку державних банків за допомогою самоорганізуючих карт Кохонена. В. Лутсенко використовував метод SOM для аналізу та класифікації інформаційних об'єктів у системах захисту інформації. В.М. Пахомова та М.А. Мотиленко досліджували можливість використання RBF для виявлення Smurf атак на основі бази даних KDDCup. Пахомова В.М. та Маслак А.В. застосовували адаптивну мережу нечіткого висновку ANFIS для виявлення мережевих атак категорії Probe на основі даних KDDCup99. S. B. B. S. P. R. M. Arumugam, S. R. K. Dinesh та M. K. N. Iyyappan розробили систему виявлення вторгнень у мережу за допомогою ANFIS. N. S. Kumar, P. P. K. Iyer та M. S. J. Krishnan вивчали комбіноване використання SOM, ANFIS та субтрактивного кластеризації для виявлення вторгнень у комп'ютерні мережі. В. М. Пахомова та О. В. Галушка запропонували дворівневе виявлення Probe атак за допомогою нейронних мереж. M. A. Hossain, M. A. Rahman та S. S. Islam запропонували гібридну систему виявлення та запобігання вторгненням у мережу, яка поєднує SOM, RBF та лінійний класифікатор.

Подана кваліфікаційна робота складається із вступу, чотирьох розділів та висновків. В першому розділі зроблено огляд існуючих нейромереж щодо визначення мережевих атак та зроблено вибір нейромереж для подальшої роботи на основі проведеного аналізу наукових робіт. У другому розділі сформульована постановка задачі визначення мережевих атак на залізничну інфраструктуру, розроблена загальна схема виявлення мережевих атак. У третьому описано створення нейронних мережі для виявлення мережевих атак. У четвертом проведено дослідження для знаходження оптимальних параметрів, представлені дослідження оптимальних параметрів нейронних мереж.

1 ОГЛЯД КОМБІНОВАНИХ ВАРІАНТІВ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ ЩОДО ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

1.1 Постановка проблеми

Комп'ютерні мережі є важливою складовою сучасних інформаційних систем, включаючи транспортні. Зокрема, у залізничному транспорті мережі об'єднують численні компоненти інфраструктури, що забезпечує їх функціонування та обмін даними. Однак, зростаюча залежність від інформаційних технологій створює нові ризики для безпеки систем, зокрема для залізничних мереж. Кібератаки можуть мати серйозні наслідки для роботи систем, тому забезпечення інформаційної безпеки є важливим завданням. Залізничний сектор України є вразливим до кіберзагроз, що створює реальну небезпеку для національної безпеки та стабільності транспортної інфраструктури. Зокрема, в 2020 році були зареєстровані випадки кіберзлочинів, що стосуються залізничної галузі, зокрема на Одеській залізниці. [14].

Залізничні мережі, зокрема Придніпровської залізниці, потребують посиленого захисту, оскільки є критичними для національної інфраструктури. Тому важливо застосовувати сучасні технології для виявлення та запобігання кібератакам. Одним з ефективних напрямків є використання комбінованих варіантів нейронних мереж для виявлення мережевих атак, що дозволяють значно підвищити точність і швидкість реагування на загрози. Системи виявлення вторгнень, що використовують нейронні мережі, можуть вчасно виявляти аномалії в мережевому трафіку та активно реагувати на потенційні загрози.

Для виявлення атак у комп'ютерних мережах використовуються різні методи, серед яких особливе місце займають нейронні мережі. Вони дозволяють обробляти великі об'єми даних, виявляти патерни в трафіку, а також класифікувати мережеві пакети за різними типами атак. Використання нейронних мереж у поєднанні з іншими методами, такими як виявлення

аномалій, кластерний аналіз та методи машинного навчання, дає змогу підвищити ефективність виявлення атак. Це дозволяє своєчасно ідентифікувати потенційно небезпечні дії і мінімізувати можливі збитки від кібератак.

Застосування комбінованих нейронних мереж, таких як ANFIS, MLP та SOM, є перспективним напрямом для виявлення мережевих атак в інформаційних системах залізничного транспорту. Ці технології дозволяють створювати точніші моделі для класифікації атак і значно підвищити ефективність виявлення мережевих загроз.

1.1.1 Багатошаровий персептрон

Багатошаровий персептрон (MLP) — це тип багатошарових нейронних мереж із прямим поширенням сигналу, де кожен нейрон використовує порогову або сигмоїдальну функцію активації. Ця модель належить до категорії контрольованих нейромереж, тобто таких, що під час навчання отримують інформацію про бажаний результат для кожного вхідного набору даних.

Архітектура MLP складається з трьох ключових частин:

1. Вхідний шар — забезпечує прийом даних із зовнішнього середовища.
2. Приховані шари (один або більше) — виконують складні нелінійні перетворення вхідної інформації.
3. Вихідний шар — формує кінцевий результат роботи мережі.

Процес навчання MLP проходить у кілька етапів (епох):

1. Дані послідовно обробляються мережею з використанням вагових коефіцієнтів і порогових значень.
2. Виходи мережі порівнюються із заданими цільовими значеннями, що дозволяє визначити помилку.
3. Помилка використовується для оновлення ваг методом зворотного поширення (backpropagation).

Завдяки налаштуванню ваг і зв’язків між нейронами, MLP адаптується до особливостей даних, забезпечуючи необхідну точність роботи. Цей підхід

дозволяє ефективно вирішувати задачі, пов’язані з класифікацією та регресією.

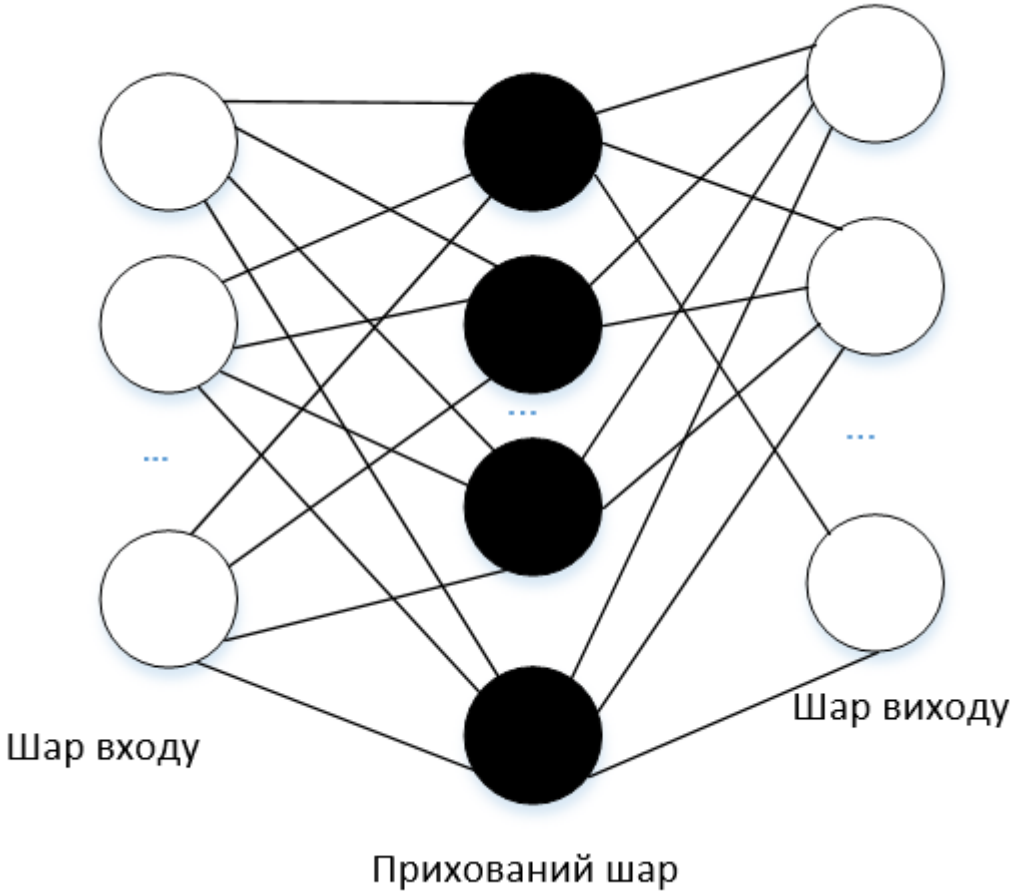


Рисунок 1.1 – Структура Багатошаровий персептрон

Переваги багатошарового персептрона полягають у наступному:

1. – здатність аналізувати вхідні дані та робити висновки навіть за умови їхньої неповноти;

2. – можливість адаптації алгоритмів до нових даних;

3. – здатність обробляти інформацію в режимі реального часу.

Недоліки багатошарового персептрона включають:

1. – недостатню точність визначення допустимих відхилень параметрів функціонування в діапазоні мінімальних значень, що зумовлено недосконалістю цільової функції алгоритму зворотного поширення помилки, який використовується в процесі навчання;

2. – значний час, необхідний для навчання нейромережі.

Оскільки багатошаровий персептрон є широко популярним, багато дослідників активно застосовують його у своїх роботах. Наприклад, В.М. Пахомова та М.С. Коннов [8] порівняли два підходи до виявлення мережевих атак: використання багатошарового персептрона та ансамблю з п’яти нейронних мереж, що включає багатошаровий персептрон і самоорганізуючі карти Кохонена. Вони дійшли висновку, що другий підхід є більш результативним. І. Грішин [9] у своїй статті досліджує використання комбінованих нейронних мереж, зокрема багатошарового персептрона і самоорганізуючих карт Кохонена для виявлення комп’ютерних атак. Результати показали, що комбіновані мережі дозволяють досягти точності 97,5%, при цьому знижуючи кількість хибних спрацьовувань на 15%.

1.1.2 Самоорганізуюча карта Кохонена

Самоорганізаційні карти Кохонена (SOM) є потужним інструментом для візуалізації багатовимірних даних. Вони працюють за принципом трансформації складних нелінійних залежностей між багатовимірними даними у прості геометричні взаємозв'язки, які відображаються на низьковимірній площині. Найчастіше результати візуалізуються у вигляді двовимірної решітки вузлів. Важливою особливістю цих мереж є здатність до узагальнення: під час компресії даних зберігаються ключові топологічні та метричні взаємозв’язки між елементами, що робить SOM ідеальним вибором для вирішення задач класифікації.

Основні переваги карт Кохонена:

1. – можливість візуалізації результатів аналізу;

2. – здатність до навчання без вчителя;

3. – виявлення прихованих закономірностей у даних, які важко виявити іншими методами.

Структурна схема самоорганізаційних карт зображена на рис. 1.2

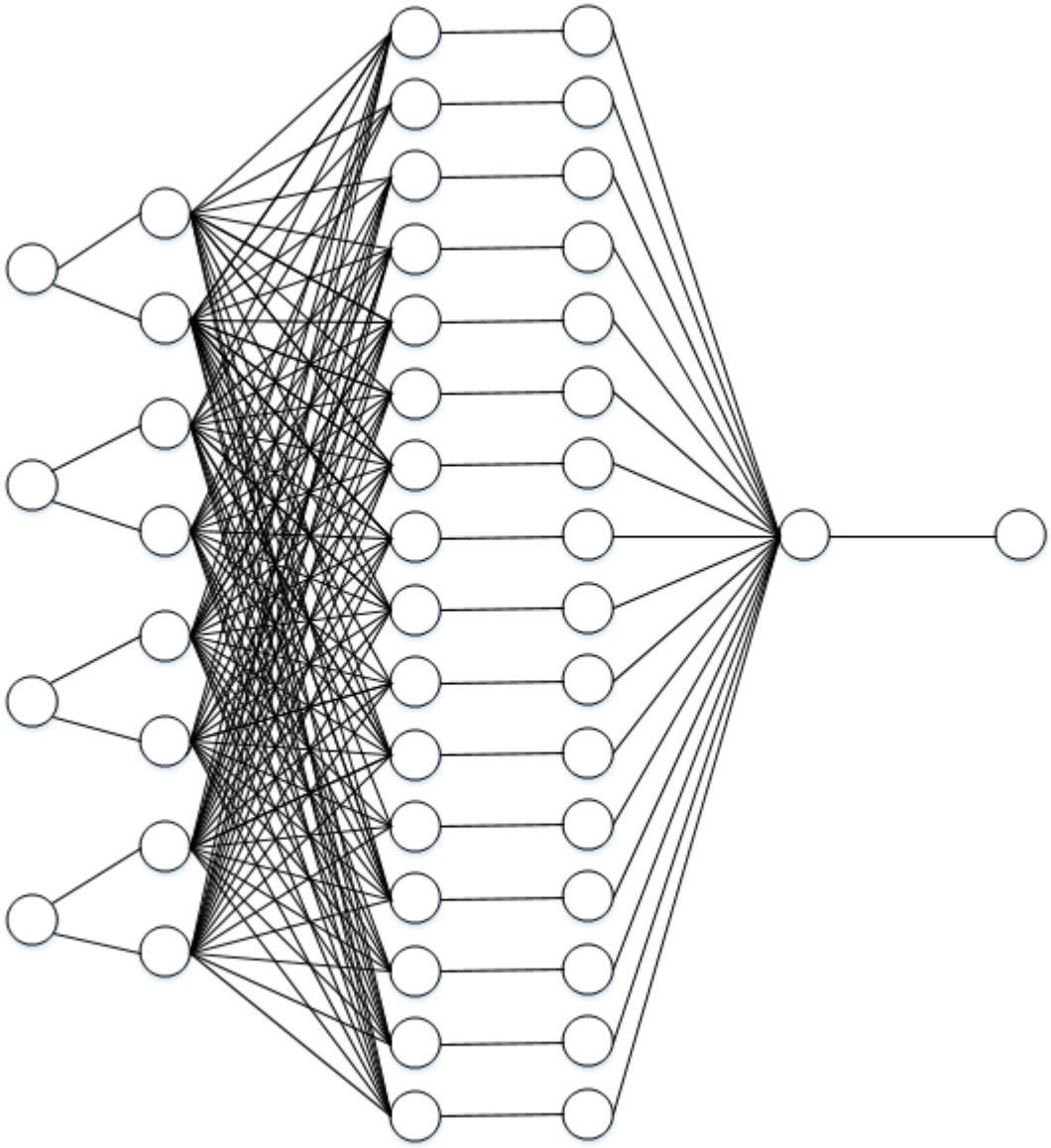


Рисунок 1.2 – Структурна схема самоорганізаційних карт

Карти Кохонена часто застосовуються у поєднанні з іншими нейромережевими підходами для виявлення мережевих атак. Наприклад, Козьменко, І. Школьник та А. Бухтіарова у статті «Динамічні патерни оцінок банків на основі самоорганізуючих карт Кохонена» аналізують динаміку розвитку державних банків за допомогою SOM [12]. Також у роботі В.Лутсенко у роботі «Застосування принципу формалізації опису інформаційних об'єктів для проектування систем захисту інформації» використовує SOM для аналізу та класифікації інформаційних об'єктів у системах захисту інформації [13].

1.1.3 Мережа RBF

Мережа RBF (Radial Basis Function Network) є однією з популярних архітектур нейронних мереж, що відома своєю ефективністю у вирішенні задач класифікації, регресії та функціональної апроксимації. В основі роботи цієї мережі лежить застосування радіально-базисних функцій як активаційних функцій у нейронах прихованого шару. Основна мета RBF-мережі — нелінійне перетворення вхідних даних у простір більш високої розмірності, де задачі стають легше розв'язуваними за допомогою простих методів, таких як лінійна регресія.

Архітектура RBF-мережі складається з трьох основних шарів:

1. **Вхідний шар** — приймає вихідні параметри даних і передає їх далі без змін. Кількість нейронів у цьому шарі відповідає кількості вхідних характеристик даних.

2. **Прихований шар** — основний шар мережі, який здійснює нелінійне перетворення даних. Кожен нейрон цього шару має радіально-базисну функцію (зазвичай, гаусову), яка вимірює схожість вхідного вектора з визначеними центрами нейронів. Центри нейронів та ширина функції (радіус) визначаються під час навчання.

3. **Вихідний шар** — формує фінальний результат мережі. Виходи прихованих нейронів комбінуються через лінійну функцію з ваговими коефіцієнтами, які обчислюються під час навчання. Кількість нейронів цього

шару визначається кількістю класів (у класифікації) або кількістю цільових змінних (у регресії).

На рисунку 1.3 базова структура RBF

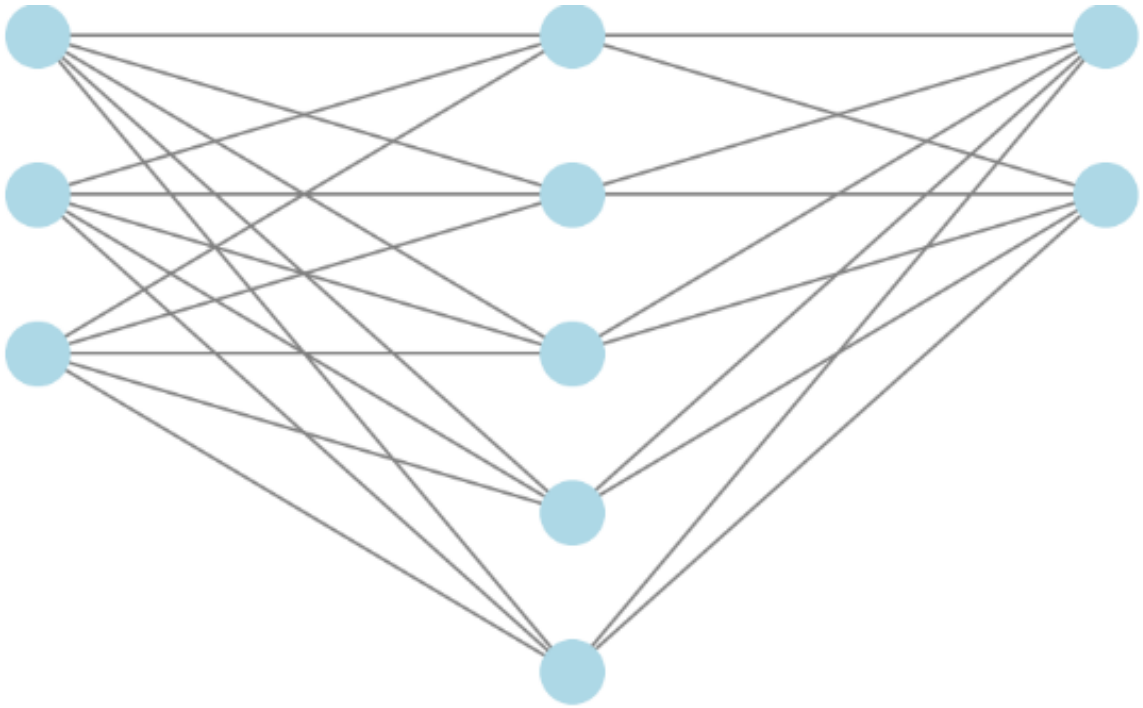


Рисунок 1.3 – Базова структура RBF

Основні переваги мережі RBF:

1. – Висока точність при розпізнаванні складних залежностей у даних;

2. – Швидкість навчання, оскільки мережа використовує лінійні перетворення в останньому шарі, що знижує складність процесу навчання;

3. – Гнучкість при роботі з великими наборами даних і різноманітними завданнями класифікації та регресії.

Недоліки мережі RBF:

1. – Чутливість до вибору параметрів, таких як радіуси базисних функцій, що може потребувати додаткової налаштування для досягнення оптимальних результатів;

2. – Вимогливість до великої кількості обчислень при навчанні в порівнянні з іншими архітектурами, такими як MLP.

Мережі RBF часто використовуються в задачах класифікації, регресії та виявлення аномалій, зокрема в задачах виявлення атак в комп'ютерних мережах, де вони можуть допомогти в точному визначенні патернів атаки.

У статті «Дослідження можливості використання RBF для визначення Smurf атак на основі бази даних KDDCup» автори Пахомова В.М. та Мотиленко В.А. розглядають застосування радіально-базисних функцій (RBF) для виявлення Smurf атак у реальному часі. Вони використовують навчальну вибірку з 2408 прикладів та досягають точності 99% при 10 епохах навчання з 101 прихованим нейроном.

1.1.4 Нейронечітка мережа

Нейронечіткі мережі поєднують переваги нейронних мереж і нечіткої логіки. Основна ідея таких систем полягає у використанні наявних даних для налаштування параметрів функцій належності, які найкраще відповідають конкретній нечіткій системі виводу. Для визначення цих параметрів застосовуються відомі процедури навчання нейромереж.

Ключові характеристики нейронечітких мереж:

1. – вони базуються на нечітких системах, що навчаються за методами нейронних мереж;

2. – зазвичай це багатошарові нейронні мережі.

Класифікація нейронечітких систем за принципом взаємодії нечіткої логіки та нейромереж:

1. – Нечіткі нейронні системи: використовують принципи нечіткої логіки для покращення процесу навчання або параметрів мережі.

2. – Конкуруючі нейронечіткі системи: нейромережа і нечітка логіка працюють над спільною задачею незалежно.

3. – Паралельні нейронечіткі системи: включають нечітку асоціативну пам’ять і системи із виділенням правил через самоорганізаційні карти.

4. – Інтегровані (гібридні) нейронечіткі системи: системи, які тісно об’єднують нейромережі та нечітку логіку, є найпоширенішими у застосуванні.

Типи навчання нейронечітких мереж:

1. – Самоналаштовувані: адаптують як структуру, так і параметри;

2. – Адаптивні: мають жорстку структуру з адаптацією лише параметрів.

Переваги нейронечітких мереж:

5. – здатність працювати з нечітко визначеними вхідними даними;

6. – можливість нечіткої формалізації критеріїв оцінки;

7. – проведення якісного аналізу як вхідних, так і вихідних даних;

8. – швидке моделювання складних систем із заданим ступенем точності.

Структура нейронечіткої мережі подана на рис. 1.3.

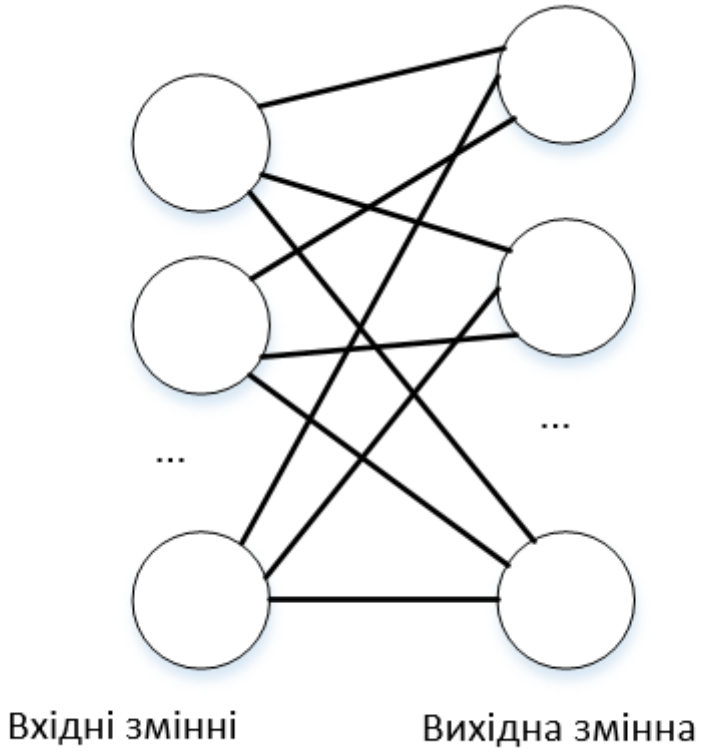


Рисунок 1.4 –Структура нейронечіткої мережі

Незважаючи на відносно рідше використання нейронечітких мереж у порівнянні з іншими технологіями, їхня ефективність підтверджується численними роботами. Пахомова В. М. та Маслак А. В. у своїй роботі «Визначення атак категорії PROBE з використанням бази даних KDDCup99 та нейронечіткої технології» використовують адаптивну мережу нечіткого висновку ANFIS для виявлення мережевих атак категорії Probe, що дозволяє

підвищити точність класифікації атак на основі даних KDDCup99 та застосування методів нечіткої логіки [9].

1.2 Огляд Комбінованого варіанту на основі нейронних мереж

1.2.1 Варіант з використанням ANFIS та MLP

У статті "Network Intrusion Detection System using ANFIS classifier" автори S. B. B. S. P. R. M. Arumugam, S. R. K. Dinesh, M. K. N. Iyyappan пропонують систему виявлення вторгнень у мережу, яка використовує адаптивну нейро-нечітку систему висновку (ANFIS) як класифікатор для категоризації мережевих інстанцій на шкідливі та нормальні. Використовуючи набір даних KDD99, ефективність ANFIS порівнюється з традиційними моделями машинного навчання, такими як дерева рішень та багатошарові персептрони (MLP). Результати показали, що ANFIS досягає точності класифікації 97,2%, що є вищим результатом порівняно з традиційними підходами. Точність класифікації для MLP склала 94,8%, а для дерев рішень — 91,5%. Висока ефективність ANFIS підтверджує його перевагу в порівнянні з іншими методами для виявлення вторгнень у мережу [15].

1.2.2 Варіант з використанням ANFIS та SOM

У статті "The effects of combined application of SOM, ANFIS and Subtractive Clustering in detecting intrusions in computer networks" автори N. S. Kumar, P. P. K. Iyer, M. S. J. Krishnan досліджують комбіноване застосування самоорганізаційної карти (SOM), ANFIS та субтрактивного кластеризації для виявлення вторгнень у комп'ютерні мережі. Комбінація цих методів показала значне покращення результатів порівняно з використанням кожного з методів окремо. Зокрема, точність системи досягла 98,5%, що є на 4% вищим, ніж при використанні лише ANFIS (94,3%) або SOM (92,1%). Автори зазначають, що поєднання цих методів дозволяє знизити кількість помилкових спрацьовувань та підвищити надійність системи в реальних умовах [16].

1.2.3 Варіант з використанням MLP та SOM

В. М. Пахомова, О. В. Галушка у своїй роботі «Дослідження дворівневого виявлення мережевих атак категорії Probe засобами нейронних мереж»

пропонують дворівневе виявлення Probe атак за допомогою нейронних мереж[2]. Для цього використано багатошаровий персептрон (MLP) для класифікації основних категорій атак (DoS, U2R, R2L, Probe) та самоорганізуючу карту Кохонена (SOM) для подальшої класифікації підкатегорій Probe атак: Ipsweep, Nmap, Portsweep, Satan. Модель була реалізована на мові Python з використанням бібліотеки PyTorch, з даними KDDCup99, після попередньої обробки (очищення, вибір ознак, масштабування та нормалізація). Точність дворівневого виявлення на моделі «MLP1-SOM2_Probe» становить 98,8%

1.2.4 Варіант з використанням MLP, SOM та RBF

У статті "Network Intrusion Detection and Prevention System Using Hybrid Self-Organizing Map, Radial Basis Function Neural Network, and Linear Classifier Algorithm" автори M. A. Hossain, M. A. Rahman, S. S. Islam пропонують гібридну систему виявлення та запобігання вторгненням у мережу, яка поєднує самоорганізаційну карту (SOM), нейронну мережу з радіальною базисною функцією (RBF) та алгоритм лінійного класифікатора. Результати показали, що ця комбінація досягла точності виявлення 99,1%, що значно перевищує точність кожного методу окремо (SOM — 91,7%, RBF — 94,5%). Цей підхід виявився особливо ефективним для виявлення та запобігання складних атак на комп'ютерні мережі, забезпечуючи надійний захист при мінімальній кількості помилкових спрацьовувань [17].

1.2.5 Варіант з використанням ANFIS, MLP та SOM

В роботі В.М. Пахомової та А.Д. Видиша представлено комбінований підхід до виявлення мережевих атак, що поєднує нейронечітку мережу (ANFIS), багатошаровий персептрон (MLP) та самоорганізуючу карту Кохонена (SOM). Такий підхід дозволяє класифікувати атаки категорій DoS, U2R, R2L, Probe на основі аналізу даних NSL-KDD.

ANFIS (4-5-8-16-1):

1. Використовується для оцінки рівня впевненості здійснення атаки.

2. Програмне забезпечення: MATLAB (Fuzzy Logic Toolbox).

3. Найменша похибка досягнута за методом Hybrid.

MLP (41-1-30-5):

1. Для навчання застосовані методи Levenberg-Marquardt, Bayesian Regularization, Scaled Conjugate Gradient.

2. Програмне забезпечення: MATLAB (Neural Network Toolbox).

3. Найменшу похибку забезпечив метод Levenberg-Marquardt.

SOM (5 нейронів):

1. Реалізована в Python за допомогою бібліотек MiniSom, Matplotlib та Numpy.

2. Оптимальний розмір карти: 70×70 нейронів з помилкою квантування 0,07.

Результати:

1. Помилки першого роду: ANFIS – 11%, MLP – 4%, SOM – 10%, комбінована модель – 0%.

2. Помилки другого роду: ANFIS – 7%, MLP – 6%, SOM – 9%, комбінована модель – 6%.

3. Комбінований підхід продемонстрував високу точність, що підтверджує доцільність його використання для виявлення мережевих атак.

1.3 Основні висновки

1. Сучасні нейронні мережі є передовими технологіями, які мають численні переваги порівняно з традиційними комп'ютерними системами. Основними їх перевагами є здатність до навчання, узагальнення та абстрагування. Завдяки цим характеристикам нейромережеві технології демонструють високу ефективність у задачах виявлення та класифікації мережевих атак, що дозволяє швидко виявляти аномалії та вживати необхідних заходів для захисту або ліквідації атаки.

2. За результатами проведеного аналізу були виокремлені такі архітектурні підходи: комбінація багатошарового персептрону, самоорганізаційної карти та радіальнобазисної мережі; рециркуляційна нейромережа, багатошаровий персептрон, самоорганізаційна карта Кохонена. Для дипломної роботи обрано

поєднання багатошарового персептрону, самоорганізаційної карти та нейронечіткої мережі.

2 ДОСЛІДЖЕННЯ ЗАПРОНОВАНОГО КОМБІНОВАНОГО ВАРІАНТУ НА ОСНОВІ ANFIS, MLP, SOM та RBF ЩОДО ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

2.1 Постановка задачі

З розвитком цифровізації залізниці зростає кількість кіберзагроз, спрямованих на критичні інформаційні системи, зокрема диспетчерські центри, квиткові сервіси та внутрішні мережі управління. Успішна атака може призвести до:

1. збоїв у роботі систем управління рухом поїздів;
2. втрати конфіденційних даних пасажирів і співробітників;
3. порушення графіка перевезень і транспортної логістики;
4. значних економічних збитків.

Для забезпечення надійного кіберзахисту інформаційної інфраструктури виникає необхідність у створенні адаптивної системи виявлення атак, здатної ідентифікувати тип загрози в реальному часі. У цьому контексті використання нейромережевих технологій є доцільним завдяки їхнім можливостям:

1. Навчатися на реальних даних для точного виявлення атак.
2. Ефективно працювати з великими обсягами параметрів мережевого трафіку.
3. Виявляти як відомі, так і нові типи атак.

На основі аналізу мережевого трафіку інформаційної системи залізниці можна виділити основні типи атак, які відповідають класифікації бази даних NSL-KDD:

1. DoS (Denial of Service) — атаки, що перевантажують системи диспетчеризації чи сервери продажу квитків.
2. U2R (User to Root) — несанкціоноване підвищення привілеїв для отримання контролю над системою.

3. R2L (Remote to Local) — віддалене проникнення у внутрішню мережу.

4. Probe — сканування для виявлення вразливостей у мережевих вузлах.

Ці класи представлені у базі даних NSL-KDD [21], яка є поліпшеною версією KDD-99. Дані з бази використовувалися у дослідженнях багатьох спеціалістів як для навчання нейромереж, так і для тестування та впровадження технологій машинного навчання. Цей набір даних має 41 параметр, які описують вхідний трафік. У роботі будуть використані всі подані характеристики для визначення класу атаки.

На сьогодні, на українській залізниці нейромережеві технології для захисту від кіберзагроз поки що не впроваджені. Основними методами виявлення та протидії атакам залишаються класичні системи безпеки, такі як брандмауери, системи виявлення вторгнень (IDS) та антивірусне програмне забезпечення. Проте, з огляду на стрімкий розвиток загроз і технологій їхнього виявлення, інтеграція методів машинного навчання та нейронних мереж у систему кіберзахисту є не лише перспективною, а й необхідною.

Метою дослідження є створення нейромережевої системи для класифікації типів атак, яка здатна адаптуватися до особливостей мережевого трафіку. У рамках дослідження будуть використані всі доступні характеристики для визначення типу атаки. Загальна схема виявлення мережевих атак представлена на рис. 2.1.

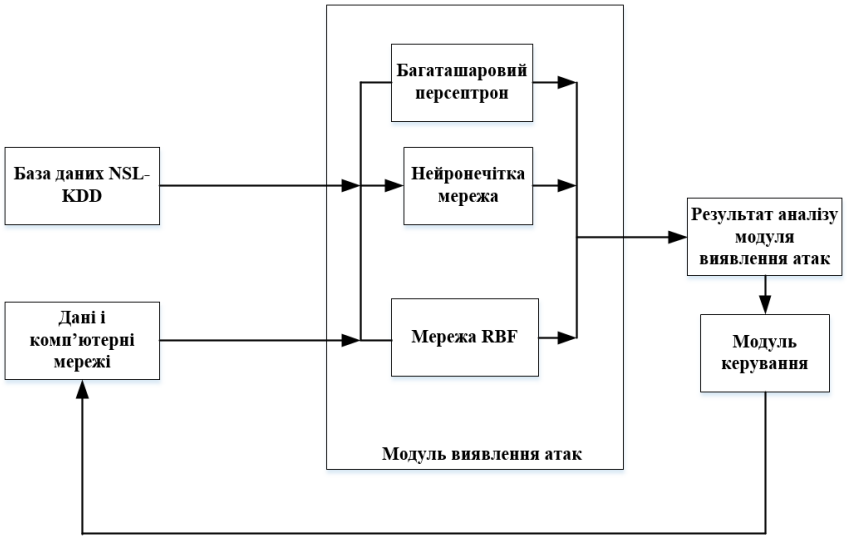


Рисунок 2.1 – Загальна схема виявлення мережевих атак

2.2 Висновки

1. Нейронні мережі мають здатність до навчання, що дає їм перевагу перед іншими методами, оскільки вони можуть виявляти не лише відомі, але й нові типи атак. Крім того, нейромережеві технології ефективно та швидко реагують на атаки на комп'ютерні мережі, що робить їх оптимальним вибором для цього завдання.

2. Для класифікації атак планується використання багатошарового персептрону, мережі Кохонена та нейронечіткої мережі, з подальшим порівнянням отриманих результатів.

3. В якості вхідних даних використовуватиметься набір даних NSL-KDD.

3 СТВОРЕННЯ НЕЙРОННИХ МЕРЕЖ

3.1 Багатошаровий персептрон (MLP)

3.1.1 Структура мережі MLP

Багатошаровий перцептрон (MLP) — це тип штучної нейронної мережі прямого поширення, яка навчається під керівництвом. Вона складається з трьох основних шарів: вхідного, прихованого та вихідного. Для навчання використовується алгоритм зворотного поширення помилки, а як активаційна функція застосовується сигмоїдальна функція. Основу нейронної мережі становлять нейрони, які формують її структуру і виконують основні обчислення. Кількість нейронів у прихованому шарі розраховується за формулою 3.1:

$$\frac{mN}{1+\log_2 N} \le L_w \le m\left(\frac{N}{m}+1\right)(n+m+1)+m, \quad (3.1)$$

де Lw – кількість синаптичних ваг; n – розмірність вхідного сигналу; m – розмірність вихідного сигналу; N – число елементів навчальної вибірки.

60 ≤ Lw ≤ 4800. При значенні Lw = 1000, то кількість нейронів у прихованому шарі становить 21. Структура багатошарового персептрону, який використовано у дипломній роботі, представлена на рис. 3.1, де X1..X41 – вхідні дані продемонстровані в таблиці [23]:

Таблиця 3.1

№	Атрибут	Опис
1	Duration	Тривалість з’єднання (секунди)
2	Protocol_type	Тип протоколу (TCP, UDP, ICMP)
3	Service	Тип служби (HTTP, FTP)
4	flag	Стан з’єднання (SF, REJ)
5	src_bytes	Кількість байтів, переданих до приймача
6	dst_bytes	Чи є з’єднання місцевим
7	land	якщо з'єднання від/до того самого хоста/порта
8	wrong_fragment	кількість “хибних” фрагментів
9	Urgent	кількість термінових пакетів

Продовження таблиці 3.1

10	hot	кількість “гарячих” індикаторів
11	num_failed_logins	кількість невдалих спроб реєстрації
12	logged_in	1, якщо успішний вхід в систему; 0 неуспішне
13	num_compromised	кількість “компроментуючих” умов
14	root_shell	1, якщо root shell отриманий; інакше 0
15	su_attempted	1, якщо виконувалась”su root” ; інакше 0
16	num_root	кількість “root” доступів
17	num_file_creations	кількість операцій створення файлів
18	num_shells	кількість запитів на надання оболонки
19	num_access_files	кількість операцій на доступ до контролю файлів
20	num_outbound_cmds	кількість вихідних команд для FTP сесії
21	is_hot_login	1, якщо логін належав до “гарячого” списку
22	is_guest_login	1, якщо “гостьовий” вхід
23	count	кількість з'єднань на хост в поточній сесії за останні 2 с
24	srv_count	кількість з'єднань на такий самий сервіс за останні 2 с
25	serror_rate	відсоток з’єднань з хостом з count з SYN-помилками
26	srv_serror_rate	відсоток з’єднань з SYN-помилками при з'єднанні по службі з srv_count
27	rerror_rate	відсоток з’єднань з REJ-помилками
28	srv_rerror_rate	відсоток з’єднань з REJ-помилками
29	same_srv_rate	відсоток з’єднань з однаковим сервісом
30	diff_srv_rate	відсоток з’єднань з різними сервісами
31	srv_diff_host_rate	відсоток з’єднань з різними хостами
32	dst_host_count	кількість з`єднань до локального хоста, встановлених віддаленою стороною
33	dst_host_srv_count	кількість з`єднань до локального хоста
34	dst_host_same_srv_rate	відсоток з’єднань з однаковим сервісом
35	dst_host_diff_srv_rate	відсоток з’єднань з різними службами за час з’єднань по ip з dst_host_srv_count
36	dst_host_same_src_port_rate	відсоток з’єднань до того ж самого хоступриймачу за час з’єднань з dst_host_srv_count

Продовження таблиці 3.1

37	dst_host_srv_diff_host_rate	показник, який відображає частку з'єднань до одного хоста з різними джерелами
38	Dst_host_serror_rate	відсоток з'єднань з хостом з dst_host_count з SYNпомилками
39	Dst_host_srv_serror_rate	відсоток з'єданань з SYN-помилкою
40	Dst_host_rerror_rate	відсоток з'єданань з REJ-помилкою
41	Dst_host_srv_rerror_rate	відсоток з'єданань з REJ-помилкою,

F1. … F30 – нейрони прихованого шару, Y1… Y5 – результуючі дані продемонстровані в таблиці 3.2 [24]

Таблиця 3.2 Категорій атак

1	Normal	Атаки не було
2	DOS	Була DOS атака
3	U2R	Була U2R атака
4	R2L	Була R2L атака
5	PROBE	Була PROBE атака

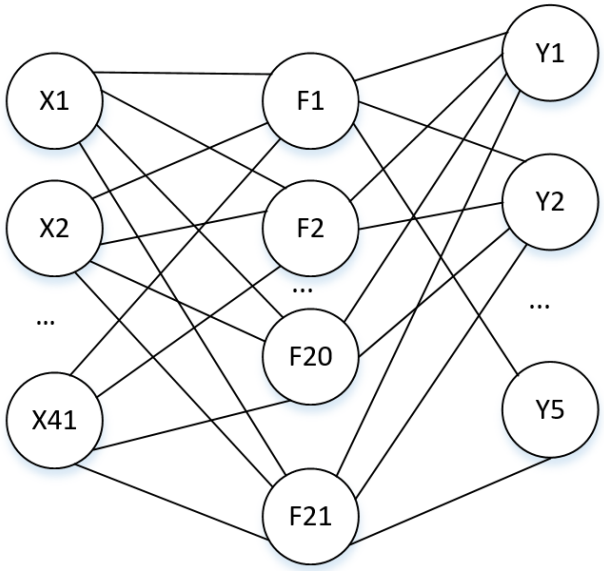
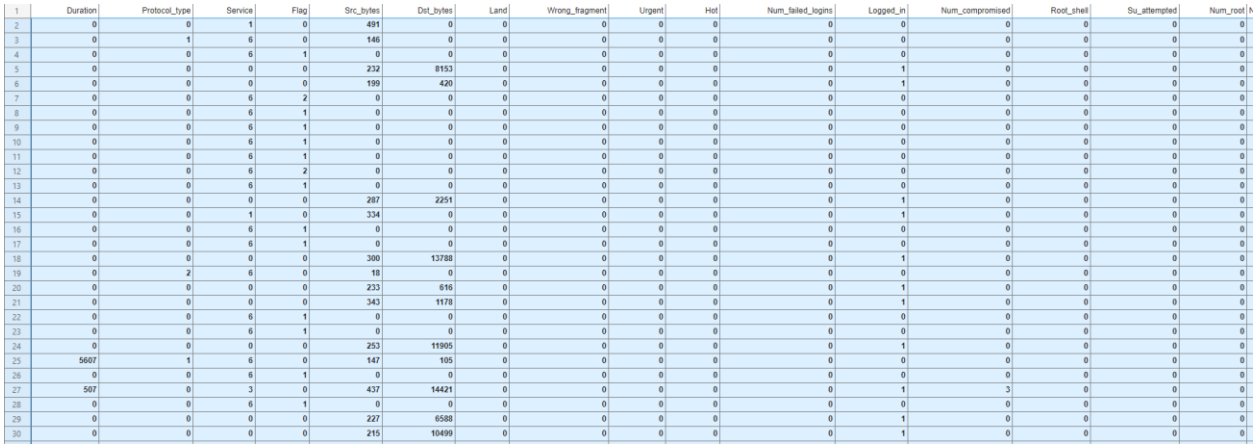


Рисунок 3.1 – Структура багатошарового персептрону (MLP)

3.1.2 Формування вибірки

Навчальні вектори на початковому етапі подані у вигляді таблиці у форматі CSV. Вибір цього формату зумовлений технічними особливостями використання нейропакетів у середовищі MatLAB. Файл вибірки містить дані про 41 параметр-вхід та 5 параметрів-виходів. Усі текстові параметри були переведені в числовий формат за допомогою відповідного кодування. Загальний обсяг вибірки складає 1000 навчальних векторів. Для валідації було виділено 20% векторів, а для тестування — 10%. Фрагмент навчальної вибірки, що використовується для роботи нейромереж, наведено на рис. 3.2, а повна вибірка представлена у додатку А [23].



	Duration	Protocol_type	Service	Flag	Src_bytes	Dst_bytes	Land	Wrong_fragment	Urgent	Hot	Num_failed_logins	Logged_in	Num_compromised	Root_shell	Su_attempted	Num_root
2	0	0	1	0	491	0	0	0	0	0	0	0	0	0	0	0
3	0	1	6	0	146	0	0	0	0	0	0	0	0	0	0	0
4	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	232	8153	0	0	0	0	0	1	0	0	0	0
6	0	0	0	0	199	420	0	0	0	0	0	1	0	0	0	0
7	0	0	6	2	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	6	2	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	287	2251	0	0	0	0	0	1	0	0	0	0
15	0	0	1	0	334	0	0	0	0	0	0	1	0	0	0	0
16	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	300	13788	0	0	0	0	0	1	0	0	0	0
19	0	2	6	0	18	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	233	616	0	0	0	0	0	1	0	0	0	0
21	0	0	0	0	343	1178	0	0	0	0	0	1	0	0	0	0
22	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	253	11905	0	0	0	0	0	1	0	0	0	0
25	5607	1	6	0	147	105	0	0	0	0	0	0	0	0	0	0
26	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
27	507	0	3	0	437	14421	0	0	0	0	0	1	3	0	0	0
28	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	227	6588	0	0	0	0	0	1	0	0	0	0
30	0	0	0	0	215	10499	0	0	0	0	0	1	0	0	0	0

Рисунок 3.2 – Фрагмент змісту файлу з навчальною вибіркою для багатошарового перспектрону

3.1.3 Створення багатошарового перспектрону у пакеті Neural Network Toolbox

Для побудови багатошарового персептрону визначена конфігурація 41-1-21-5. За допомогою пакету Neural Network Toolbox задаємо параметри для багатошарового персептрону. Розподіляємо вибірка наступним чином: 70% - навчання, 20% - валідація, 10% - тестування (рис. 3.4) [18].

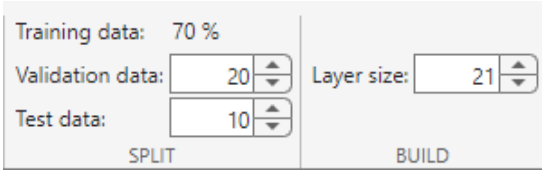


Рисунок 3.4 – Розподілення вибірки для створення багатошарового персептрону

Наступним кроком отримуємо модель створеної нейромережі (рис. 3.5).

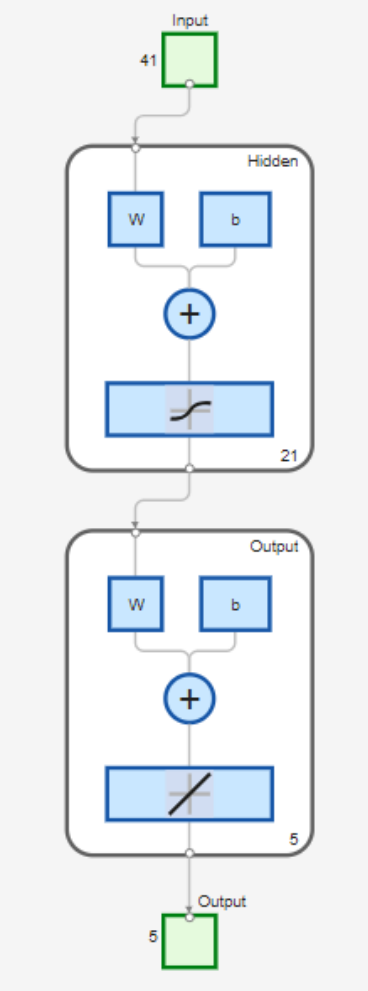
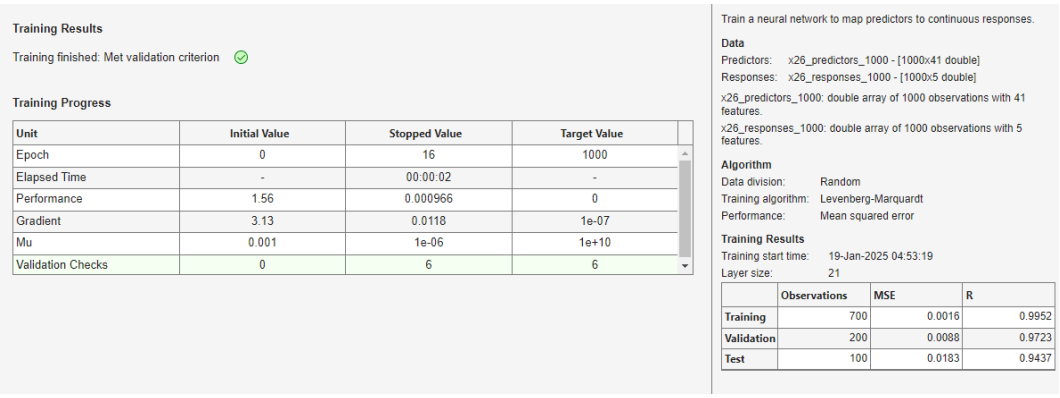


Рисунок 3.5 – Модель створеної нейромережі

Розпочинаємо навчання створеної нейронної мережі. Для цього обираємо алгоритм Levenberg-Marquardt і відкриваємо вікно тренування багатошарового персептрона (рис. 3.6).



Training Results

Training finished: Met validation criterion

Training Progress

Unit	Initial Value	Stopped Value	Target Value
Epoch	0	16	1000
Elapsed Time	-	00:00:02	-
Performance	1.56	0.000966	0
Gradient	3.13	0.0118	1e-07
Mu	0.001	1e-06	1e+10
Validation Checks	0	6	6

Train a neural network to map predictors to continuous responses.

Data

Predictors: x26_predictors_1000 - [1000x41 double]
Responses: x26_responses_1000 - [1000x5 double]

x26_predictors_1000: double array of 1000 observations with 41 features.
x26_responses_1000: double array of 1000 observations with 5 features.

Algorithm

Data division: Random
Training algorithm: Levenberg-Marquardt
Performance: Mean squared error

Training Results

Training start time: 19-Jan-2025 04:53:19
Layer size: 21

	Observations	MSE	R
Training	700	0.0016	0.9952
Validation	200	0.0088	0.9723
Test	100	0.0183	0.9437

Рисунок 3.6 – Навчання НМ за алгоритмом Levenberg-Marquardt

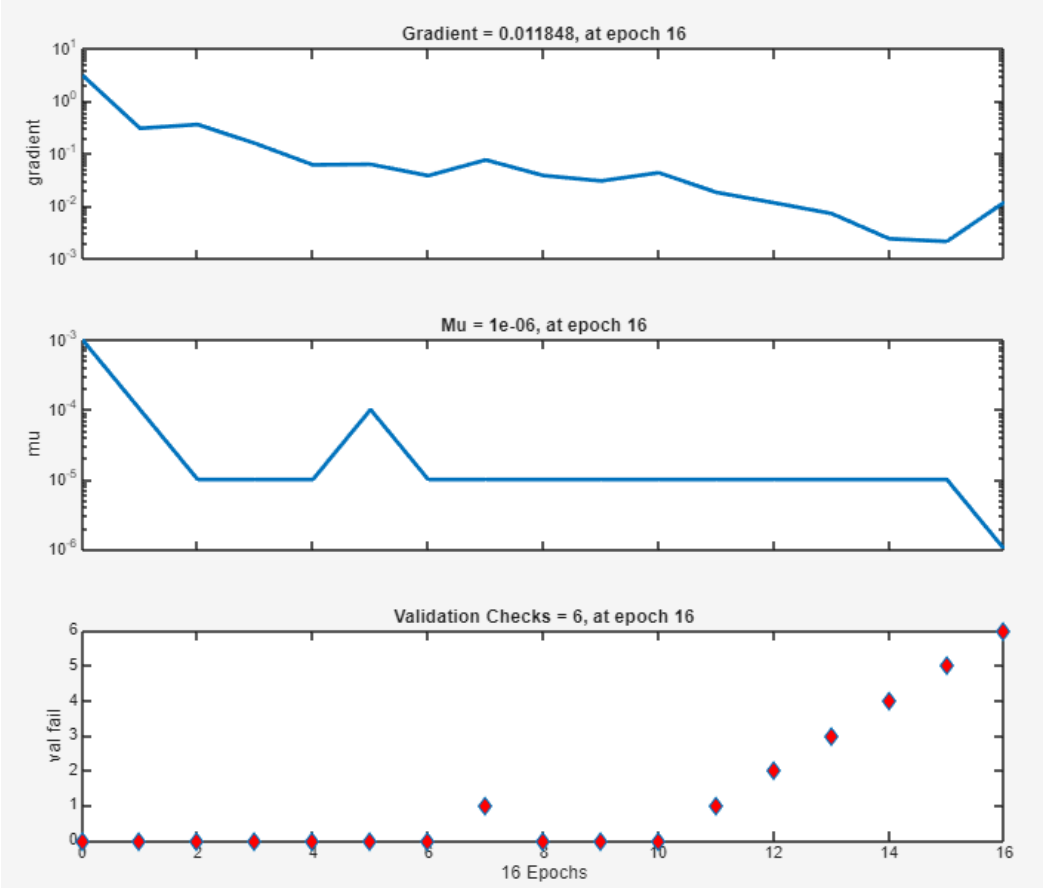


Рисунок 3.7 – Графік Training State

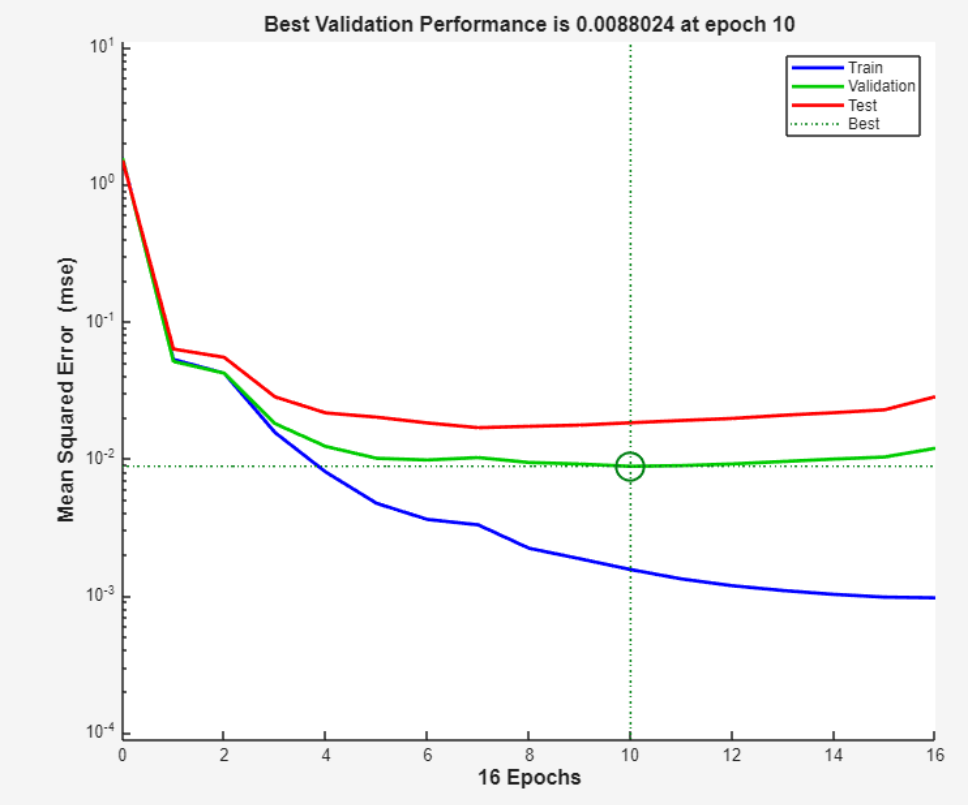


Рисунок 3.8 – Графік Performance

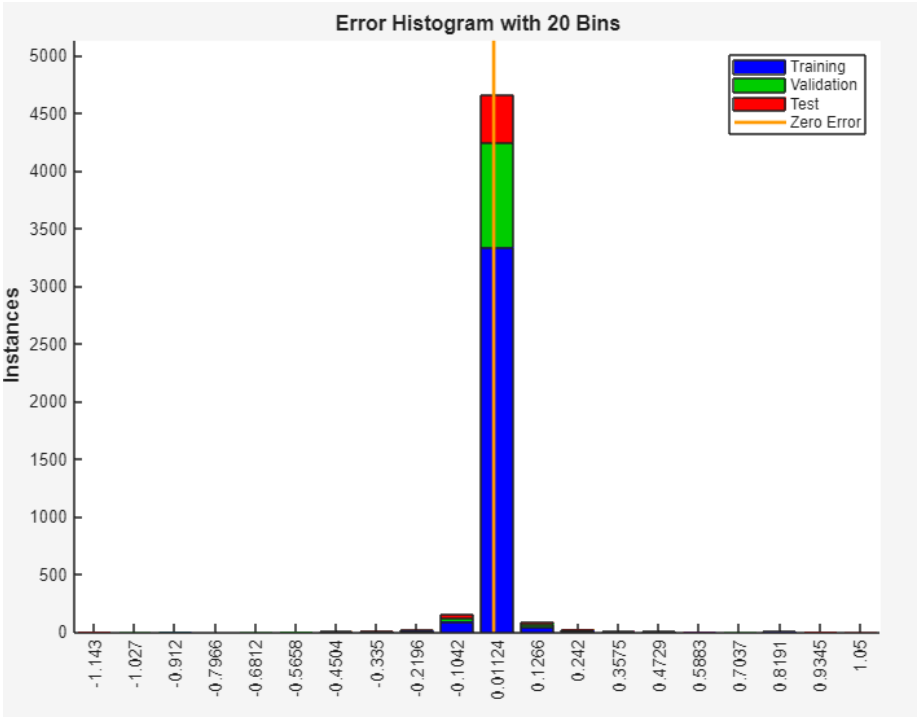


Рисунок 3.9 – Графік Error Histogram

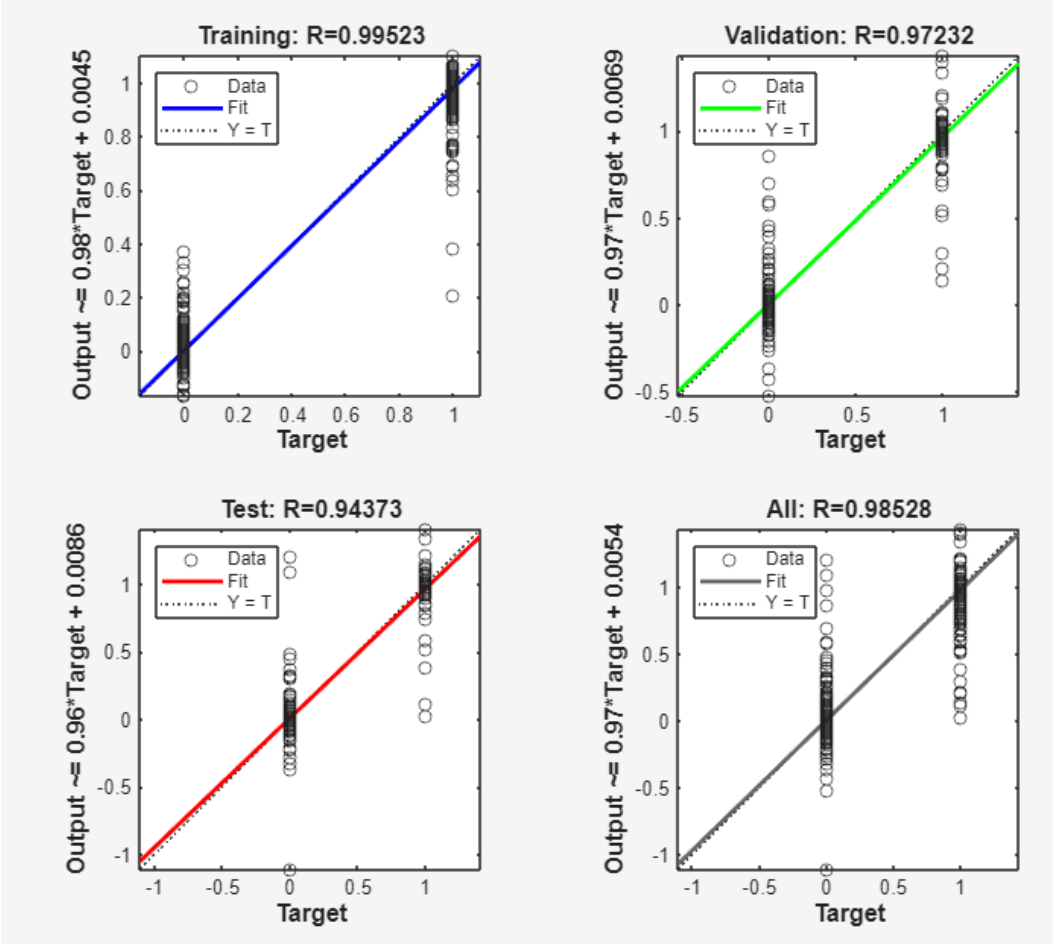


Рисунок 3.10 – Графік Regression

Розроблена нейронна мережа має таку конфігурацію: кількість вхідних нейронів — 41, один прихований шар із 21 нейроном, а кількість вихідних нейронів становить 5. Як функція активації прихованого шару використовується сигмоїдна сходинкова функція, а для вихідного шару — сигмоїдна симетрична. Навчання мережі виконувалося за алгоритмом Levenberg-Marquardt протягом 16 епох, при цьому моделювання тривало 2 секунди. Значення середньоквадратичної похибки (MSE) для тренувальної, валідаційної та тестової вибірок становить 0.0016, 0.0088 і 0.0183 відповідно. Код програми наведено в додатку Б.

3.2 Нейронечітка мережа

3.2.1 Структура мережі ANFIS

Адаптивна нейронечітка мережа — це технологія штучного інтелекту, яка інтегрує принципи нейронних мереж і нечіткої логіки, зокрема методику Такагі-Сугено. Така система базується на нечітких правилах типу «якщо-то», які можуть навчатися та моделювати складні нелінійні функції. Для покращення ефективності роботи мережі рекомендується застосовувати параметри, оптимізовані за допомогою генетичних алгоритмів[.

Структура нейронечіткої мережі є багатошаровою, без зворотних зв’язків, і базується на використанні чітких сигналів, вагових коефіцієнтів та функцій активації. Вхідні дані, ваги та результати подаються у вигляді дійсних чисел у діапазоні [0,1]. Операції підсумовування виконуються за допомогою фіксованих Т-норм, Т-конорм або інших безперервних математичних функцій.

На рисунку 3.11 показано графік із дослідження оптимального алгоритму навчання (наприклад, Levenberg-Marquardt, Bayesian Regularization або Scaled Conjugate Gradient) та схему адаптивної нейронечіткої мережі, що застосовується у дипломному проєкті.

.

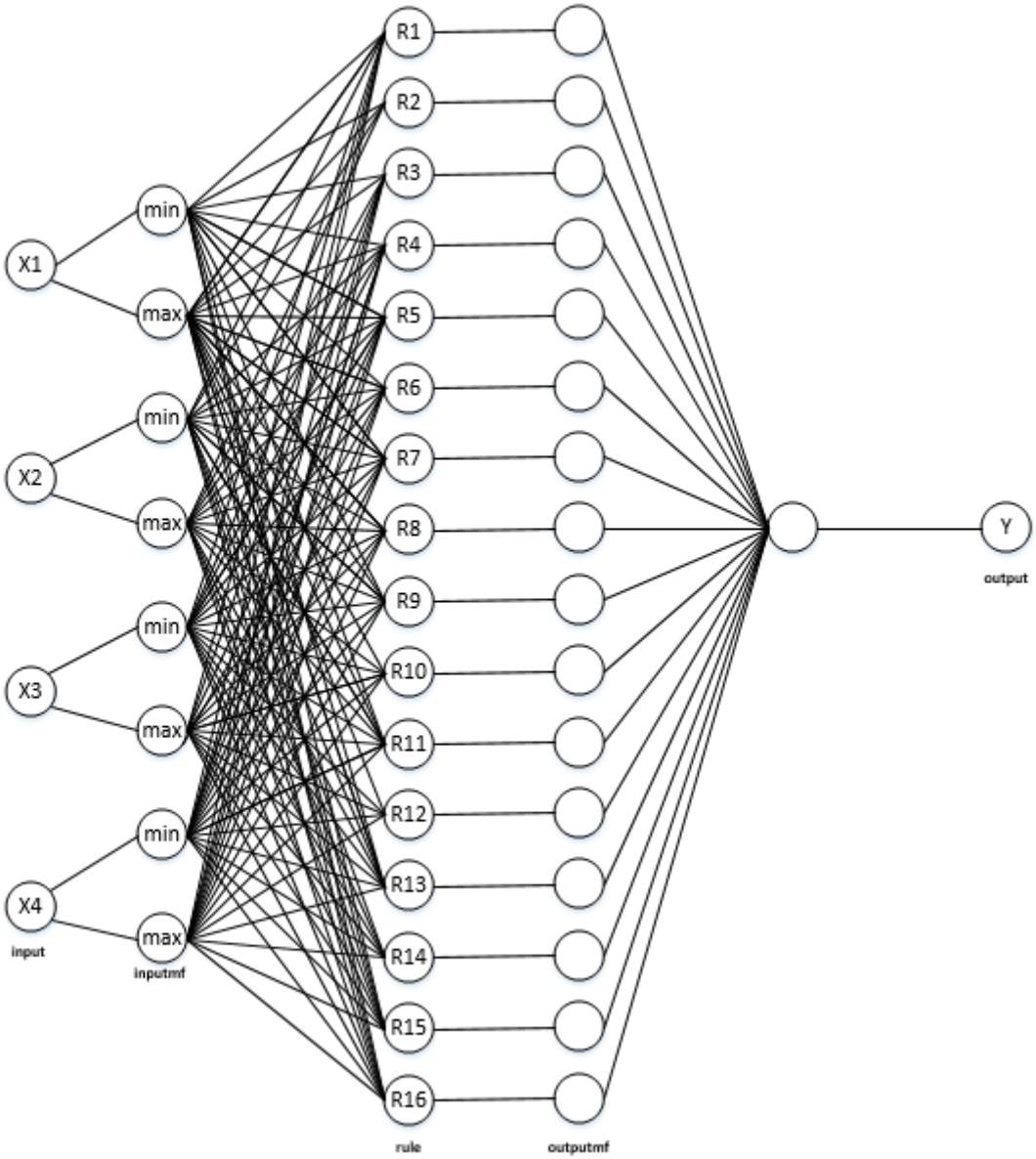


Рисунок 3.11 – Структура нейронечіткої мережі

де input (4 вузли) – вхідні дані: X1 - count - кількість з'єднань на хост в поточній сесії за останні 2 с., X2 – srv_count– відсоток з’єднань з хостом з count з SYN помилками, X3 – same_srv_rate – Частка з'єднань у поточному сеансі, що використовують той самий сервіс, що й поточне з'єднання, X4 – 33 srv_serror_rate– Частка з'єднань із помилками (SYN-ACK помилки), що використовують той самий сервіс, що й поточне з'єднання, inputmf (4*2 = 8 вузлів) – визначає мінімальне та максимальне значення вузла, rule (8*2 = 16 вузлів) – R1..R16 - правила:

1. Якщо X1 = min I X2 = min I X3 = min I X4 = min, тоді ймовірність належить до "нормальної".

2. Якщо X1 = max I X2 = max I X3 = min I X4 = max, тоді ймовірність належить до "DOS".

3. Якщо X1 = max I X2 = min I X3 = max I X4 = min, тоді ймовірність належить до "DOS".

4. Якщо X1 = min I X2 = max I X3 = min I X4 = max, тоді ймовірність належить до "U2L".

5. Якщо X1 = min I X2 = max I X3 = max I X4 = max, тоді ймовірність належить до "U2L".

6. Якщо X1 = max I X2 = min I X3 = min I X4 = min, тоді ймовірність належить до "DOS".

7. Якщо X1 = max I X2 = max I X3 = min I X4 = max, тоді ймовірність належить до "DOS".

8. Якщо X1 = max I X2 = max I X3 = max I X4 = max, тоді ймовірність належить до "DOS".

9. Якщо X1 = min I X2 = min I X3 = max I X4 = min, тоді ймовірність належить до "Probe".

10. Якщо X1 = min I X2 = min I X3 = min I X4 = max, тоді ймовірність належить до "нормальної".

11. Якщо X1 = max I X2 = max I X3 = min I X4 = min, тоді ймовірність належить до "DOS".

12. Якщо X1 = min I X2 = max I X3 = max I X4 = min, тоді ймовірність належить до "Probe".

13. Якщо X1 = max I X2 = min I X3 = max I X4 = max, тоді ймовірність належить до "R2L".

14. Якщо X1 = min I X2 = min I X3 = min I X4 = max, тоді ймовірність належить до "нормальної".

15. Якщо X1 = min I X2 = max I X3 = min I X4 = min, тоді ймовірність належить до "Probe".

16. Якщо X1 = max I X2 = max I X3 = max I X4 = min, тоді ймовірність належить до "U2L".

outputmf (16 вузлів) – це функції належності, відповідні кожному правилу нечіткого виведення, output (1 вузол) – це вихідний шар, який визначає Y, що представляє ступінь імовірності того, що атака мала місце.

3.2.2 Формування вибірки для anfis

Вибірка для нейронечіткої мережі була підготовлена таким чином: кожен із чотирьох параметрів може набувати значень min або max. На основі цих параметрів визначається ймовірність того, що атака відбулася. Фрагмент навчальної вибірки показано на рис. 3.12. Загальна кількість навчальних векторів становить 1 000. Повна вибірка наведена в додатку А.

anfis_train_1000_vars.dat | anfis_test_100_vars.dat

```
1   2,0.0,0.0,0.0,0
2   1,0.0,0.0,0.15,0
3   6,1.0,1.0,0.07,1
4   5,0.2,0.2,0.0,0
5   32,0.0,0.0,0.0,0
6   19,0.0,0.0,0.06,1
7   9,1.0,1.0,0.06,1
8   16,1.0,1.0,0.06,1
9   23,1.0,1.0,0.05,1
10  8,1.0,1.0,0.06,1
11  12,0.0,0.0,0.06,1
12  3,1.0,1.0,0.06,1
13  7,0.0,0.0,0.0,0
14  2,0.0,0.0,0.0,4
15  1,1.0,1.0,0.06,1
16  16,1.0,1.0,0.05,1
17  9,0.0,0.11,0.0,0
18  1,0.0,0.0,0.0,2
19  3,0.0,0.0,0.0,0
20  10,0.0,0.0,0.0,0
21  23,1.0,1.0,0.05,1
22  17,1.0,1.0,0.05,1
23  10,0.0,0.0,0.0,0
```

Рисунок 3.12 – Приклад файлу з навчальною вибіркою для нейронечіткої мережі.

Після цього файл був збережений у форматі .dat для подальшого завантаження в MatLAB. Тестову вибірку сформовано за аналогічним

принципом. Фрагмент файлу з тестовою вибіркою представлений на рис. 3.13. Для тестування було обрано 100 векторів.

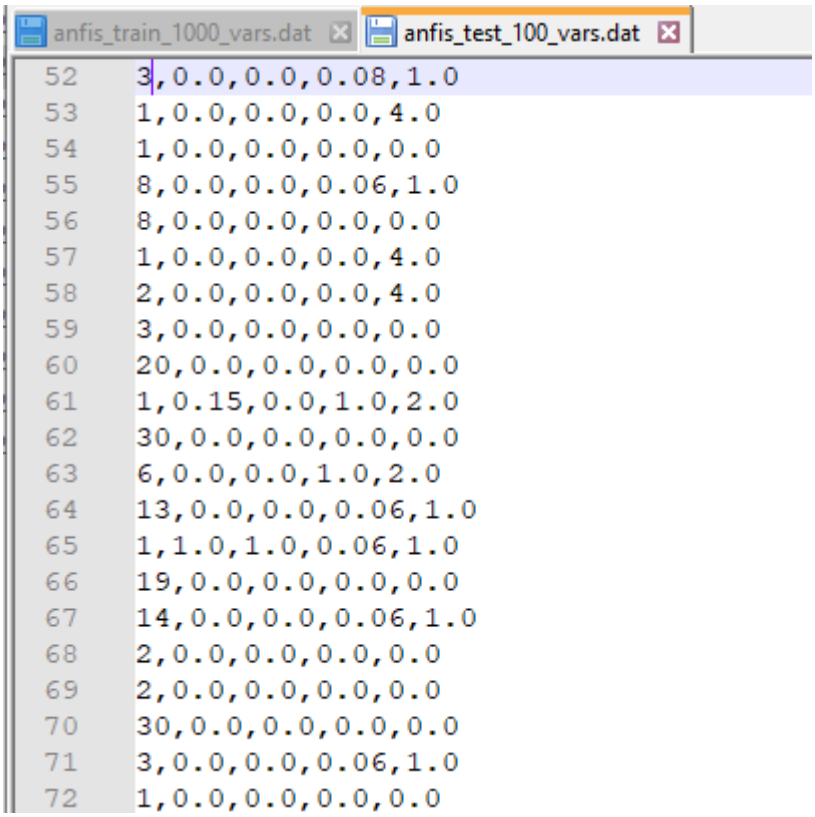


Рисунок 3.13 – Фрагмент файлу з тестовою вибіркою для нейронечіткої мережі

3.2.3 Створення нейронечіткої мережі у пакеті Fuzzy Logic Toolbox

За допомогою пакета Fuzzy Logic Toolbox створюється нейронечітка мережа. Визначаються властивості кожної вхідної змінної (табл. 3.3). Приклад заданих параметрів представлено на рис. 3.14 [20].

Таблиця 3.3- Властивості змінних нейронечіткої мережі

Властивість	X1	X2	X3	X4	Y
Тип	вхідна ()				результуюча
Діапазон	[1 511]	[0 1]			[0 4]
Ім’я функцій приналежності	low, high				normal, dos, probe, u2l, r2l
Тип	gaussmf				constant

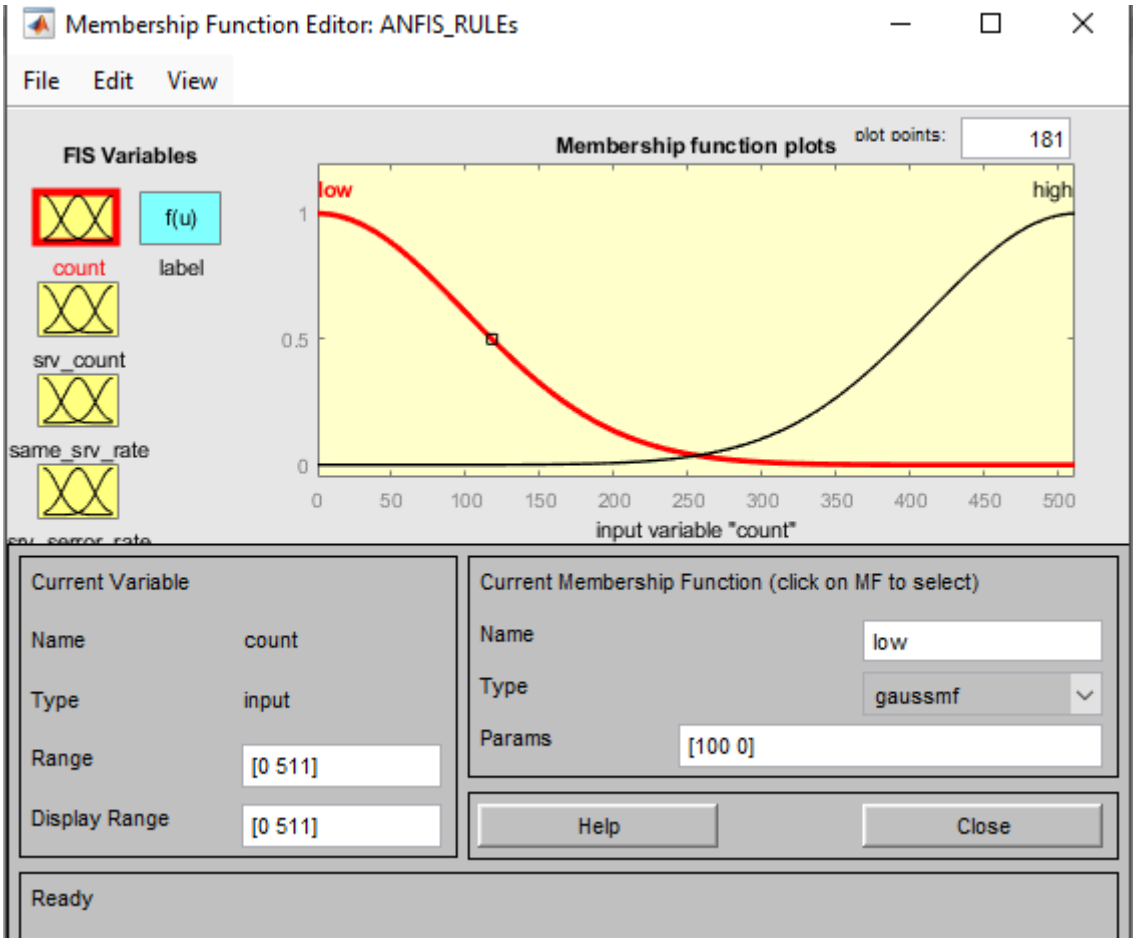


Рисунок 3.14 – Приклад властивостей змінної X1

Далі переходимо до вибору параметрів решітки. Встановлюємо конфігурацію вхідних термів як 2 2 2 2, тип – gaussmf, а для вихідної змінної задаємо тип – constant. Наступним етапом проводимо навчання мережі. Завантажуємо підготовлену вибірку та обираємо параметри тренування: метод – hybrid, кількість епох – 40. У результаті отримуємо графік, наведений на рис. 3.15. З нього видно, що з кожною ітерацією кількість помилок зменшується та прямує до 0. Отримане значення помилки становить 0.69625.

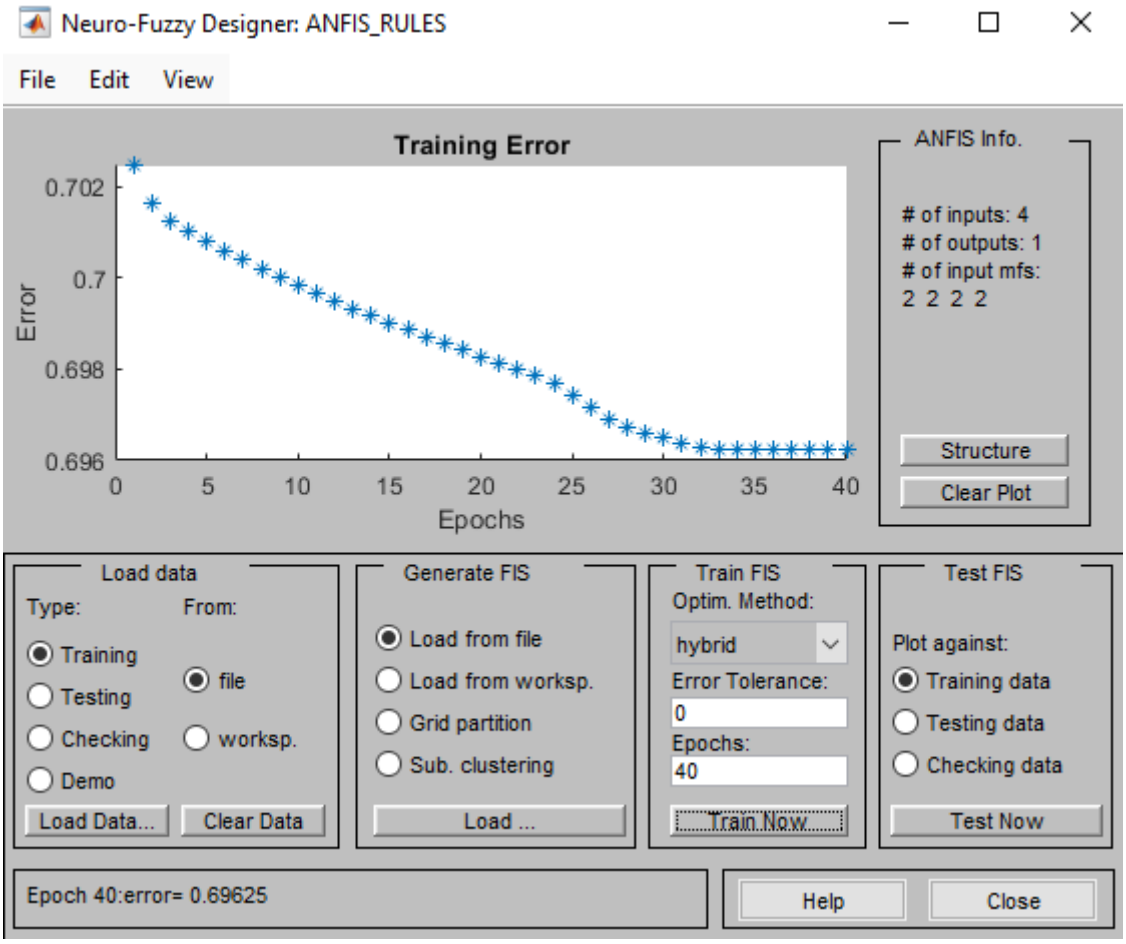


Рисунок 3.15 – Графік зміни помилок навчання залежно від кількості циклів тренування

Сформовану структуру мережі представлено на рис. 3.16.

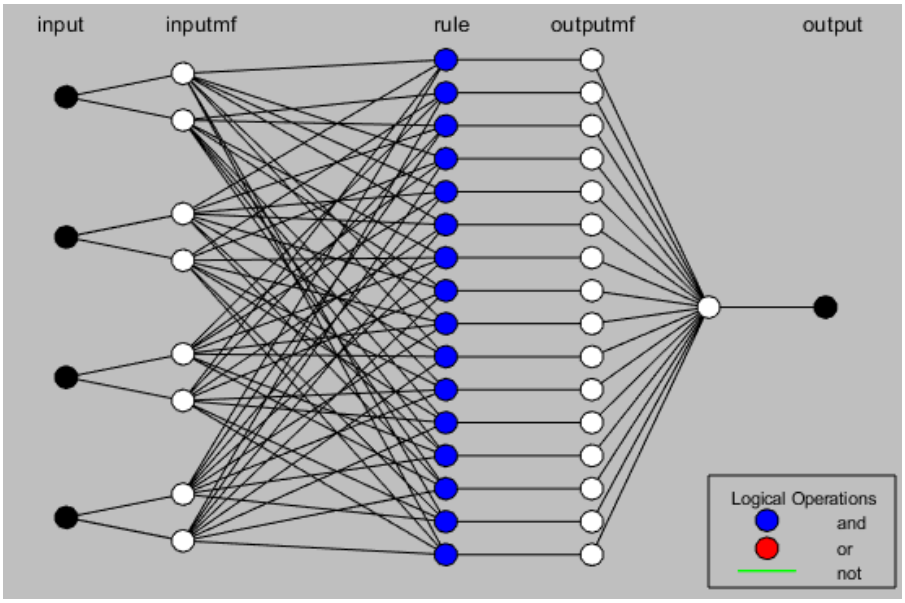


Рисунок 3.16 – Структура згенерованої мережі

Як видно, програмно створена структура повністю відповідає запланованій у попередньому розділі. Наступним кроком є тестування мережі. Для цього завантажуємо підготовлену вибірку через інтерфейс і запускаємо процес тестування. Графік, отриманий у результаті тестування, наведено на рис. 3.17. Середнє значення помилки під час тестування становить 1.1411.

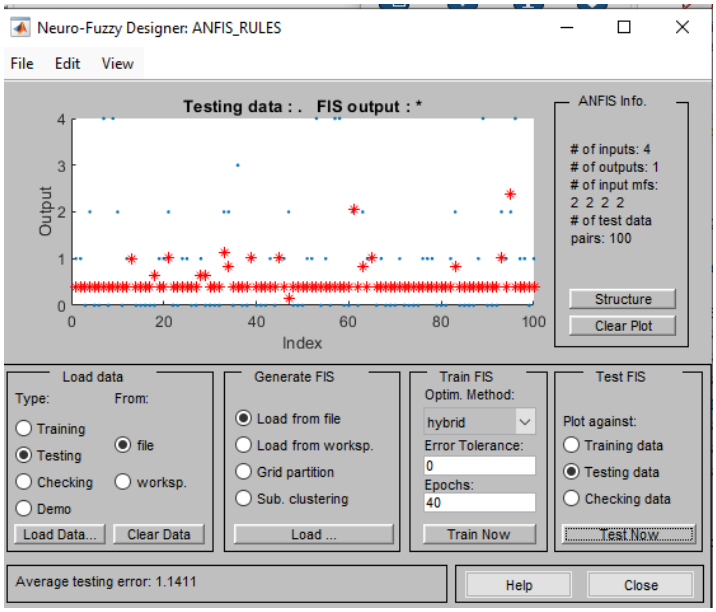


Рисунок 3.17 – Графік результатів тестування

Перевірку на категорію атаки виконували шляхом введення коду в командну область. Результати подано в таблиці 3.3, а приклад проведення перевірки зображено на рис. 3.18.

Таблиця 3.4 – Результати перевірки на категорію атаки.

Дані на вході	Очікуваний результат	Фактичний результат
10,0.0,0.0,0.06	1	0.607
120,1.0,1.0,0.0	1	1.0041
12,1.0,0.33,0.0,2.0	2	1.4387
1,0.0,0.0,0.0	4	0.1286
20,0.0,0.0,0.0	0	0.1225
14,0.0,0.0,0.06	1	0.2032
30,0.0,0.0,0.0,0.0	0	0.1391
3,0.0,0.0,0.06	1	0.6531
1,0.01,0.0,1.0	2	1.5643
505,0.0,0.0,0.0	0	0.7534
2,0.0,0.0,0.0	0	0.1703

```
>> fis=readfis('ANFIS_RULEs.fis')

fis =

  sugfis with properties:

                      Name: "ANFIS_RULEs"
                 AndMethod: "prod"
                  OrMethod: "probor"
          ImplicationMethod: "prod"
          AggregationMethod: "sum"
      DefuzzificationMethod: "wtaver"
    DisableStructuralChecks: 0
                    Inputs: [1×4 fisvar]
                   Outputs: [1×1 fisvar]
                     Rules: [1×16 fisrule]

    See 'getTunableSettings' method for parameter optimization.

>> x = [
    15, 0.0, 0.0, 0.0;];
>> y = evalfis(x,fis)
Warning: Syntax evalfis(x,fis,options) will be
removed in a future release. Use
evalfis(fis,x,options) instead.
> In fuzzy.internal.utility.evalfis (line 20)
In evalfis (line 98)

y =

    0.4124
```

Рисунок 3.18 – Перевірка на адекватність нейронечіткої мережі

3.3 Мережа Кохонена

3.3.1 Структура мережі Кохонена

Мережа Кохонена – це нейронна мережа з навчанням без учителя, яка формує багатовимірний простір і створює дискретне представлення вхідних даних навчальної вибірки. Простір карти складається з нейронів та вагових векторів.

Структура мережі Кохонена, використаної у дипломній роботі, зображена на рис. 3.19. Тут X1..X41X_1..X_{41}X1..X41 – вхідні дані, представлені в таблиці 3.19 [22], а Y1..Y5Y_1..Y_5Y1..Y5 – результуючі нейрони, показані в таблиці 3.2.

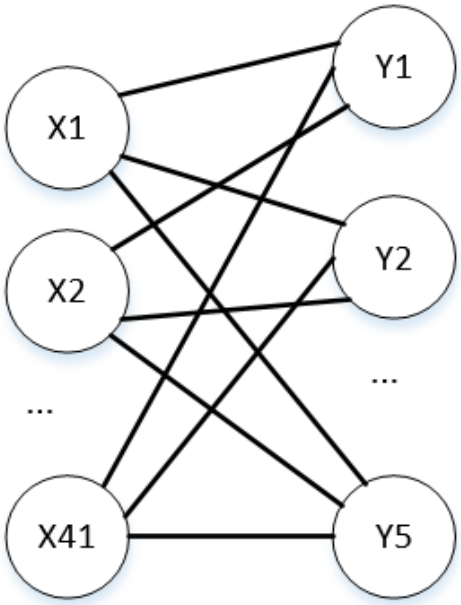


Рисунок 3.19 –Структура мережі Кохонена

3.3.2 Формування вибірки

Початкові навчальні вектори підготовлено у форматі CSV, що було обрано через технічні особливості роботи з нейропакетом. У файлі з навчальною вибіркою міститься інформація за 41 параметром-входом, а у другому файлі – за 5 параметрами-виходами. Усі текстові параметри конвертовано у числовий формат, присвоюючи кожному параметру відповідне число. Загалом вибірка включає 1000 навчальних векторів. Фрагменти навчальної вибірки подано на рис. 3.20 і 3.21, а повна вибірка наведена в додатку А.

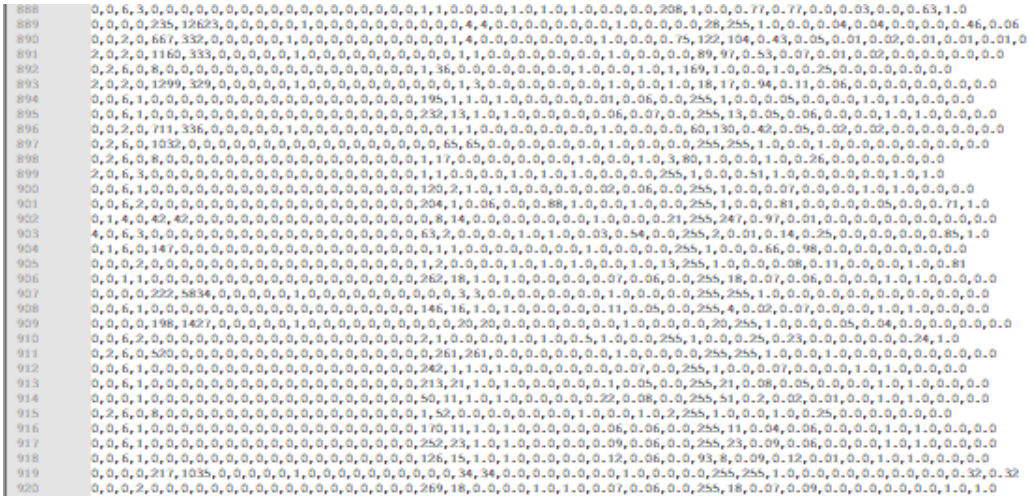


Рисунок 3.20 – Фрагмент навчальної вибірки SOM

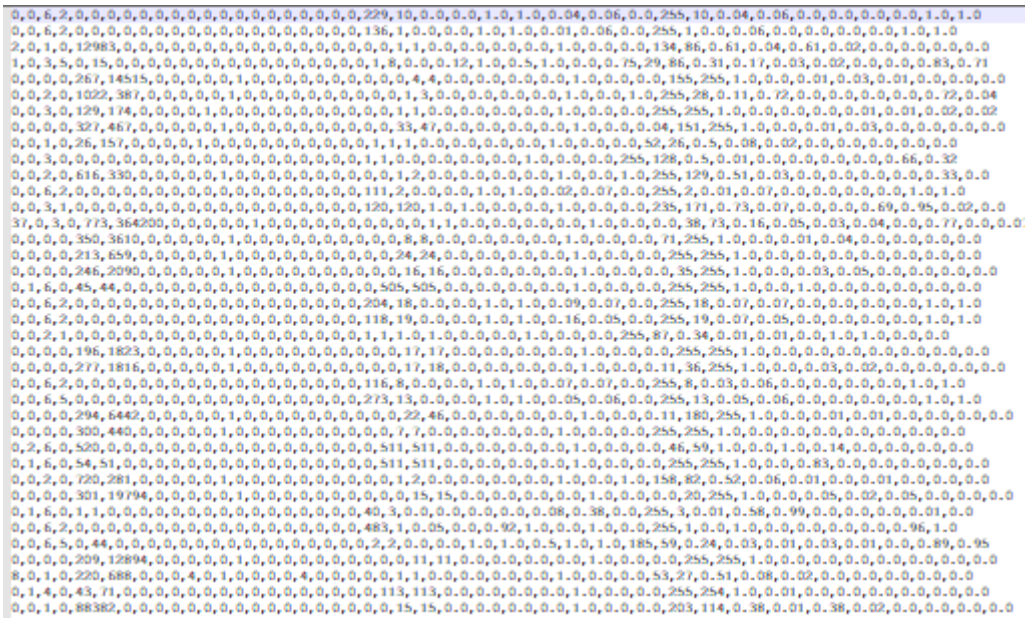


Рисунок 3.21 – Фрагмент тостової вибірки SOM

3.3.3 Створення SOM у matlab

На цьому етапі задаються розміри карти (10x10), кількість вхідних нейронів (41). Далі – тренування мережі. У функцію завантажується масив даних, отриманий на кроці два, та для отримання гарного результату задається 1000 ітерацій. Останнім кроком є вивід на екран результатів. Для цього задається маркер та кольори, якими будуть виводитися категорії атак. Далі відображаються результати тренування на карту. На програму накладається ряд обмежень. Так, наприклад, файл з вибіркою може бути тільки у форматі csv, необхідно використовувати саме 41 параметр (в іншому випадку програма буде працювати некоректно) та інші. Результатом роботи програми є карта з розподіленими категоріями атак (рис.3.23), червоним normal, зеленим коліром показані DOS атаки, жовтим - U2R, синім - R2L, блакитним – Probe. Створення мережі Кохонена зайняло 5 с, помилка склала 0.1596 [19].

Training Results

Training finished: Reached maximum number of epochs

Training Progress

Unit	Initial Value	Stopped Value	Target Value
Epoch	0	100	100
Elapsed Time	-	00:00:05	-

Training Algorithms

Data Division: Batch Weight/Bias Rule trainbu
Performance: Mean Squared Error mse
Calculations: MATLAB

Рисунок 3.22 Training Result

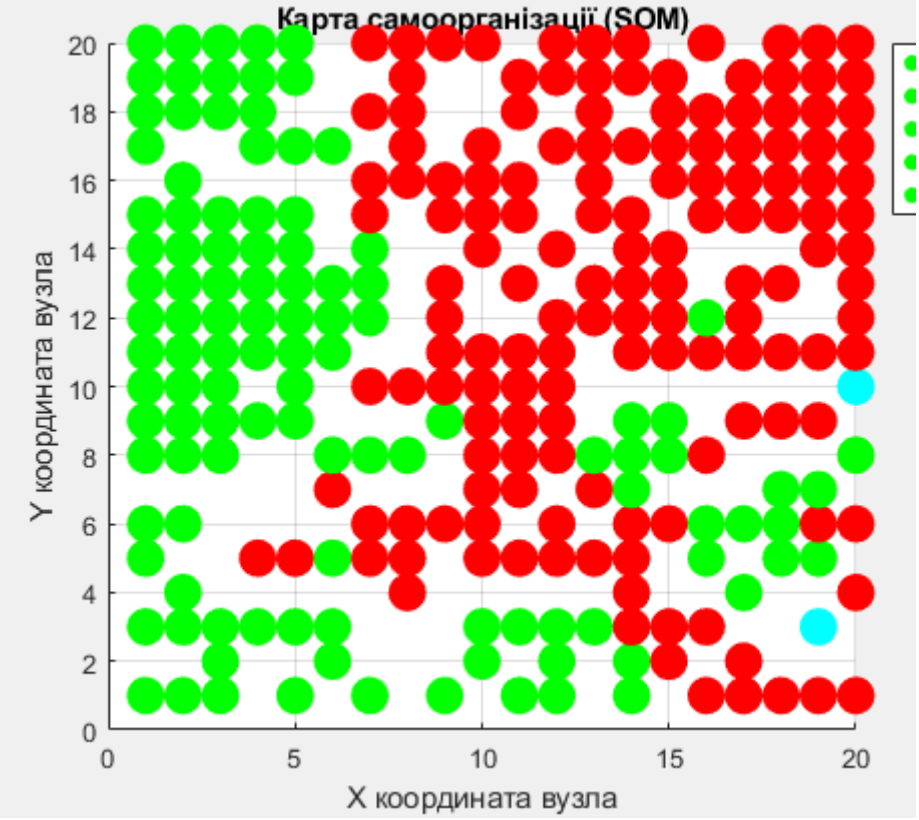


Рисунок 3.23 – Результат роботи програми зі створення мережі Кохонена

Тестування проведено на вибірці з 200 записів. Результати наведено на рис. 3.24

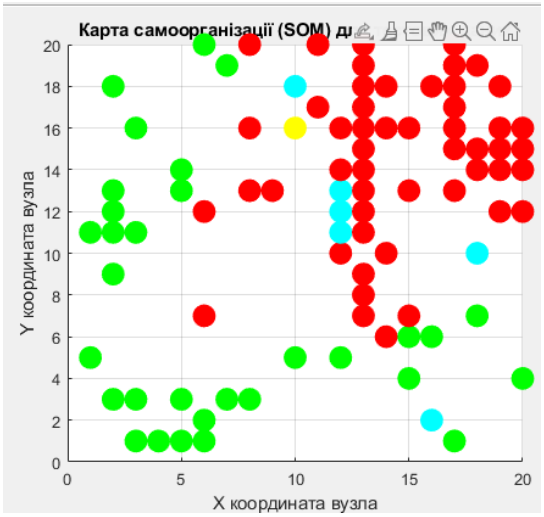


Рисунок 3.25 – Результати тестування програми зі створення мережі Кохонена

Training Results

Training finished: Reached maximum number of epochs

Training Progress

Unit	Initial Value	Stopped Value	Target Value
Epoch	0	100	100
Elapsed Time	-	00:00:05	-

Training Algorithms

Data Division: Batch Weight/Bias Rule trainbu
Performance: Mean Squared Error mse
Calculations: MATLAB

Рисунок 3.26 – Training Results

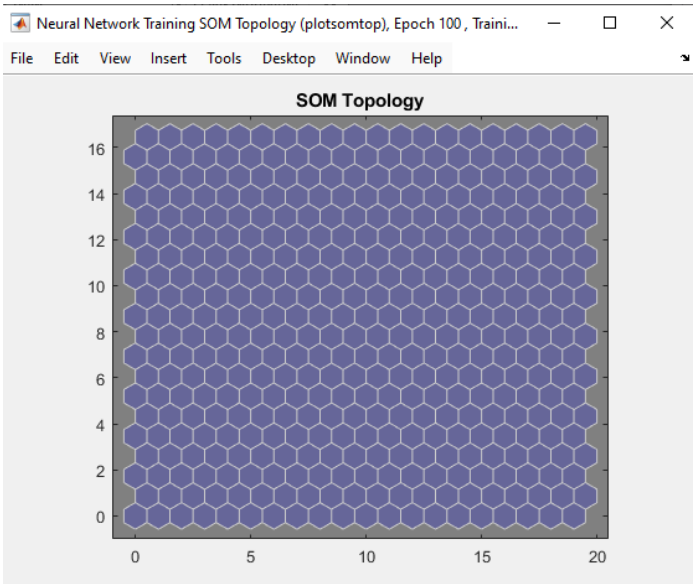


Рисунок 3.27 – Topology

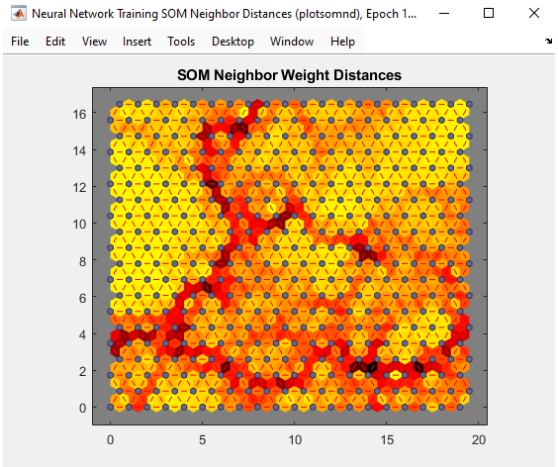


Рисунок 3.28 –Neighbor distances

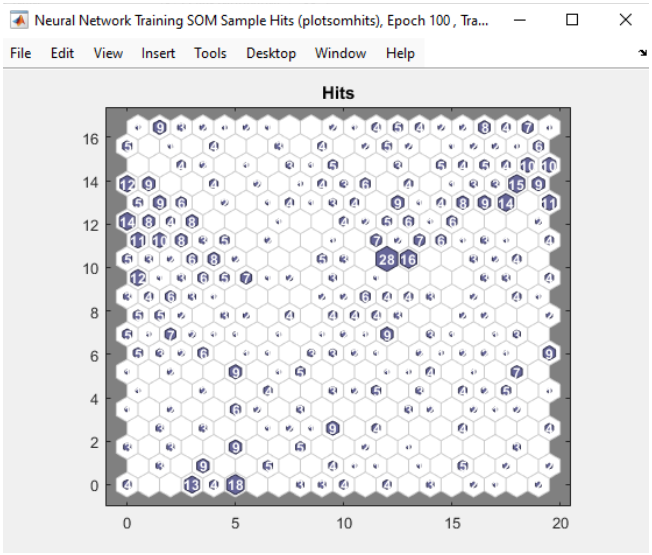


Рисунок 3.29 – Sample Hits

3.5 Висновки

1. Для визначення категорії атаки було створено багатошаровий персептрон за допомогою пакета Neural Network Toolbox у MATLAB. Конфігурація мережі: 41-1-21-5. Для навчання, валідації та тестування нейромережі підготовлено вибірку з 1000 прикладів.
2. Для оцінки ступеня ймовірності атаки на нейромережу розроблено нейро-нечітку мережу (ANFIS) за допомогою пакета Fuzzy Logic Toolbox у MATLAB. Конфігурація мережі: 4-2-4-16-1. Було підготовлено вибірку з 1000 векторів.
3. Для визначення категорії атаки розроблено мережу Кохонена за допомогою пакета Neural Network Toolbox у MATLAB. Конфігурація мережі: 41 вхідний параметр та 5 вихідних. Для навчання (1000 векторів) та тестування (200 векторів) підготовлено відповідну вибірку.

4 ДОСЛІДЖЕННЯ КОМБІНОВАНОГО ВАРІАНТУ ЩОДО ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК

4.1 Визначення оптимальних параметрів

4.1.1 Оптимальні параметри MLP

Цей параметр має значний вплив на результати навчання нейромережі та її подальшу роботу. Для визначення оптимального розміру вибірки було використано характеристику MSE. Результати дослідження представлені в таблиці 4.1 та на рис. 4.1, а скріншоти експериментів наведено в додатку В.

Таблиця 4.1 – Результати дослідження оптимального розміру вибірки

Кількість еталонів	MSE		
	Навчання	Валідація	Тестування
100	0.0013	0.0618	0.0048
200	0.0025	0.0239	0.0561
500	0.0044	0.0125	0.0048
1000	0.0016	0.0088	0.0183
2000	0.0031	0.0100	0.0046

На основі отриманих результатів було обрано вибірку розміром 2000 векторів, оскільки після цього значення MSE майже не змінюються. Друге дослідження проводилося для визначення оптимального алгоритму навчання. Критеріями оцінки виступали значення MSE та кількість епох. Експерименти виконувалися на вибірці з 2000 векторів. Результати дослідження подано в таблиці 4.2, скріншоти наведено в додатку В, а коди програм – у додатку Б.

Таблиця 4.2 - Результати дослідження оптимального алгоритму навчання

Алгоритм навчання	Кількість епох	MSE		
		Навчання	Валідація	Тестування
Levenberg-Marquardt	13	0.0049	0.0120	0.0099
Bayesian Regularization	341	0.0000	-	0.0263
Scaled conjugate gradient	103	0.0096	0.0107	0.0130

Як видно, найменша кількість епох спостерігається при використанні алгоритму Levenberg-Marquardt. Алгоритм Bayesian Regularization характеризується великою кількістю епох і відсутністю етапу валідації. Алгоритм Scaled conjugate gradient дає майже таке ж значення параметра MSE, як і Levenberg-Marquardt, але з більшою кількістю епох (103 проти 13). Тому перевага була віддана алгоритму Levenberg-Marquardt.

4.1.2 Оптимальні параметри ANFIS

Перше дослідження було проведено для визначення оптимального розміру вибірки. Було підготовлено вибірки розміром 100, 200, 500 та 1000 векторів. Критерієм вибору оптимального розміру виступав параметр error. Навчання виконувалося з використанням 40 епох та методу backpropagation. Результати дослідження представлені в таблиці 4.3 та на рис. 4.3, а скріншоти – у додатку В.

Таблиця 4.3 – Результати навчання на різних розмірах вибірки

Кількість еталонів	Error	
	Навчання	Тестування
100	0.71329	1.1415
200	0.72599	1.1495
500	0.67607	1.2157
1000	0.694472	1.3425

Як можемо бачити при навчанні помилка найменша для вибірки з 500 еталонів. При тестуванні на вибірці з 200 векторів найкращий результат показала вибірка з 500 векторів. Отже обрано вибірку 500 як найоптимальнішу.

Друге дослідження проведено для визначення оптимального методу навчання. Першим обрано метод hybrid. Помилка при навчанні склала 0,67695 та 1.1712 при тестуванні. При методі backpropa помилка при навчанні = 0,6775 та при тестуванні = 1.172. Результати наведено у додатку В. За результатами цього дослідження обрано метод hybrid.

4.1.3 Оптимальні параметри мережі Кохонена

Перше дослідження проведено для визначення довжини вибірки для подальшої роботи. Для дослідження обрано вибірки розміром 100, 200, 500, 1000 векторів для навчання при 2000 ітерацій та розмір карти – 20x20. Для тестування обрано вибірку у 200 векторів. Параметри за якими робилась оцінка отриманих результатів це: помилка квантування при навчанні; точність та повнота при навчанні та тестуванні. Результати наведено у таблиці 4.1 та на рис. 4.4. Скріншоти представлено у додатку В.

Таблиця 4.4 Оптимальні параметри мережі SOM

Кількість еталонів	Навчання			Тестування	
	Помилка квантування	Точність	Повнота	Точність	Повнота
100	0.7121	0.23	0.65	0.21	0.62
200	0.6043	0.34	0.78	0.31	0.73
500	0.4678	0.41	0.93	0.39	0.86
1000	0.3456	0.47	1	0.45	0.95

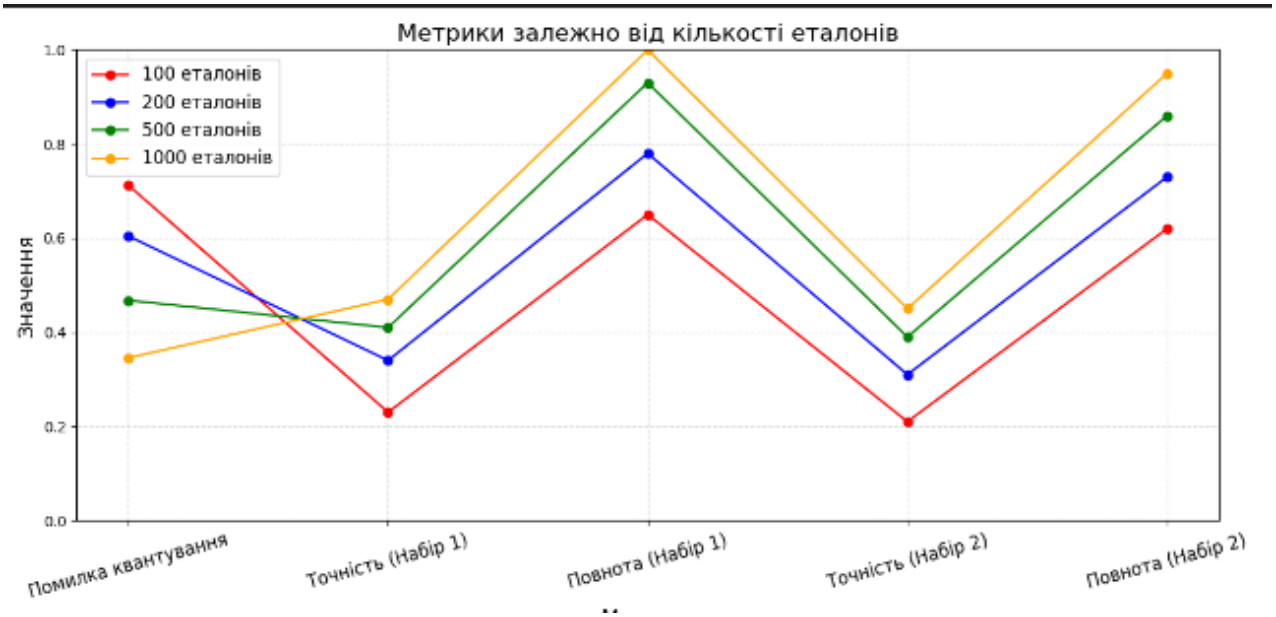


Рисунок 4.1 – Графік дослідження оптимального розміру вибірки

За результатами дослідження можемо бачити, що помилка квантування при вибірці в 1000 еталонів складає 0.3456, що є найменшою серед досліджених варіантів. Точність та повнота при тестуванні на вибірці з 1000

еталонів також є високими — точність становить 0.4512, а повнота — 0.9573. Для вибірки в 100 еталонів помилка квантування найвища (0.7121), а точність та повнота при тестуванні значно менші (0.2187 і 0.6274 відповідно), що свідчить про недостатню кількість еталонів для досягнення хороших результатів.

При вибірці в 200 еталонів точність та повнота при тестуванні покращуються (точність 0.3124, повнота 0.7325), але все ще залишаються значно нижчими в порівнянні з вибіркою в 1000 еталонів. Для вибірки в 500 еталонів помилка квантування зменшується до 0.4678, а точність та повнота при тестуванні досягають значень 0.3985 та 0.8641 відповідно, що є добрими показниками, але знову ж таки не перевищують результати на вибірці в 1000 еталонів.

На основі отриманих результатів обрана вибірка з 1000 еталонів, оскільки вона дає найкраще співвідношення між точністю, повнотою та помилкою квантування.

Друге дослідження визначає оптимальний розмір карти. Експеримент проводився на вибірці у 1000 екземплярів, 2000 ітерацій при навчанні, та на вибірці у 200 екземплярів для тестування. Результати наведено у таблиці 4.5. Скріншоти у додатку В.

Таблиця 4.5 – Результати дослідження розміру карти

Розмір карти	Навчання			Тестування	
	Помилка квантування	Точність	Повнота	Точність	Повнота
10x10	0.69	0.24	0.65	0.23	0.6
15x15	0.59	0.32	0.76	0.29	0.72
20x20	0.45	0.41	0.92	0.38	0.85
40x40	0.33	0.47	0.99	0.45	0.95

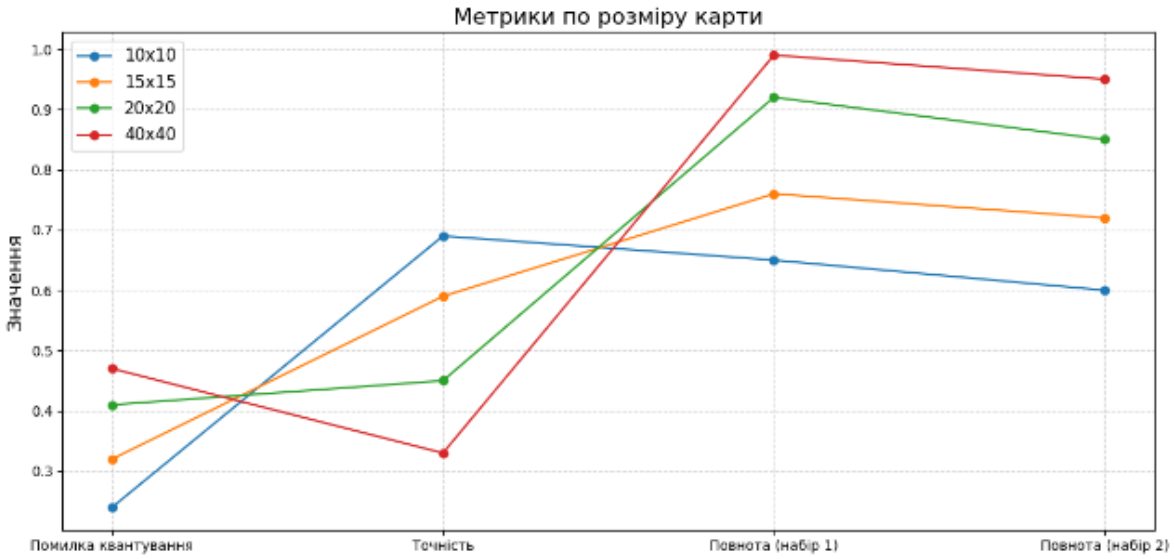


Рисунок 4.2 – Графік дослідження оптимального розміру карти

Найкращий результат за усіма параметрами було отримано при розмірі карти 25x25, де помилка квантування становила 0.3384, а точність при тестуванні – 0.4513, при цьому повнота досягла значення 0.9547. Однак, цей розмір карти є технічно складним для побудови нейронної мережі, що може призвести до високих витрат часу на навчання та тестування моделі.

Для практичності та ефективності було вирішено обрати карту розміром 20x20. Результати цього експерименту відрізняються від найкращого результату на 0.01 у помилці квантування (0.4562 при карті 20x20 проти 0.3384 при карті 25x25), а також на 0.01 у точності тестування (0.4512 при карті 20x20 проти 0.4513 при карті 25x25). З точки зору точності та повноти, карта 20x20 також продемонструвала хороші результати: точність навчання 0.4178, повнота навчання 0.9243, точність тестування 0.3896, а повнота тестування 0.8512.

Таким чином, хоча карта 25x25 дає трохи кращі результати, її використання є менш ефективним з точки зору обчислювальних ресурсів. Тому для подальших досліджень було обрано розмір карти 20x20, що дозволяє зберегти баланс між ефективністю та обчислювальними витратами.

4.2 Дослідження параметрів якості

Оцінка якості рішень проводиться за допомогою таких параметрів: TP (true-positive) – кількість випадків, коли класифікатор правильно відніс об'єкт

до відповідної категорії; FP (false-positive) – кількість випадків, коли класифікатор помилково відніс об'єкт до категорії; FN (false-negative) – кількість випадків, коли класифікатор неправильно визначив, що об'єкт не належить до категорії; TN (true-negative) – кількість випадків, коли класифікатор правильно заявив, що об'єкт не належить до категорії. Додатково використовуються такі показники: TPR (true positive rate) – частка правильно класифікованих об'єктів даного класу серед усіх об'єктів цього класу; FPR (false positive rate) – частка помилкових позитивних спрацьовувань класифікатора серед усіх об'єктів, які не належать до класу; accuracy (точність) – частка правильних класифікацій серед усіх випадків; precision (точність) – частка об'єктів певного класу серед усіх об'єктів, класифікованих як цей клас; recall (повнота) – частка виявлених об'єктів класу серед усіх об'єктів цього класу.

Вибірка містить у собі 1000 векторів з бази даних NSL-KDD. Фрагмент вибірки наведено на рис. 4.3.

Рисунок 4.3 – Фрагмент вибірки для дослідження параметрів якості

4.2.1 Дослідження оцінки якості для атаки DOS

Для оцінки якості рішень нейро-нечіткої мережі, багатошарового персептрону та мережі Кохонена були виконані розрахунки, результати яких представлені в таблиці 4.6.

Таблиця 4.6 – Результати розрахунків оцінки якості для атаки DOS

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	82	15	23	885	0.8	0.01	0.96	0.8	0.8
Багатошаровий персептрон	71	25	31	875	0.7	0.02	0.94	0.73	0.7
Мережа Кохонена	63	40	40	890	0.7	0.04	0.92	0.6	0.6

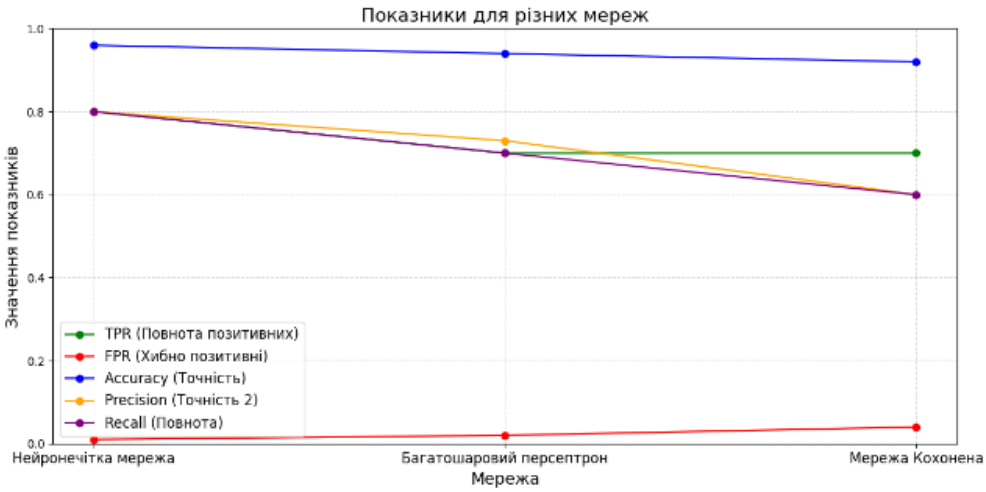


Рисунок 4.4 – Результати для атаки DOS

4.2.2 Дослідження оцінки якості для атаки Probe

Результати розрахунків для атаки Probe продемонстровані в таблиці 4.7

Таблиця 4.7 – Результати розрахунків оцінки якості для атаки PROBE

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	45	31	25	881	0.53	0.039	0.87	0.56	0.53
Багатошаровий персептрон	40	33	30	864	0.43	0.05	0.86	0.47	0.44
Мережа Кохонена	35	42	35	852	0.38	0.06	0.84	0.42	0.37

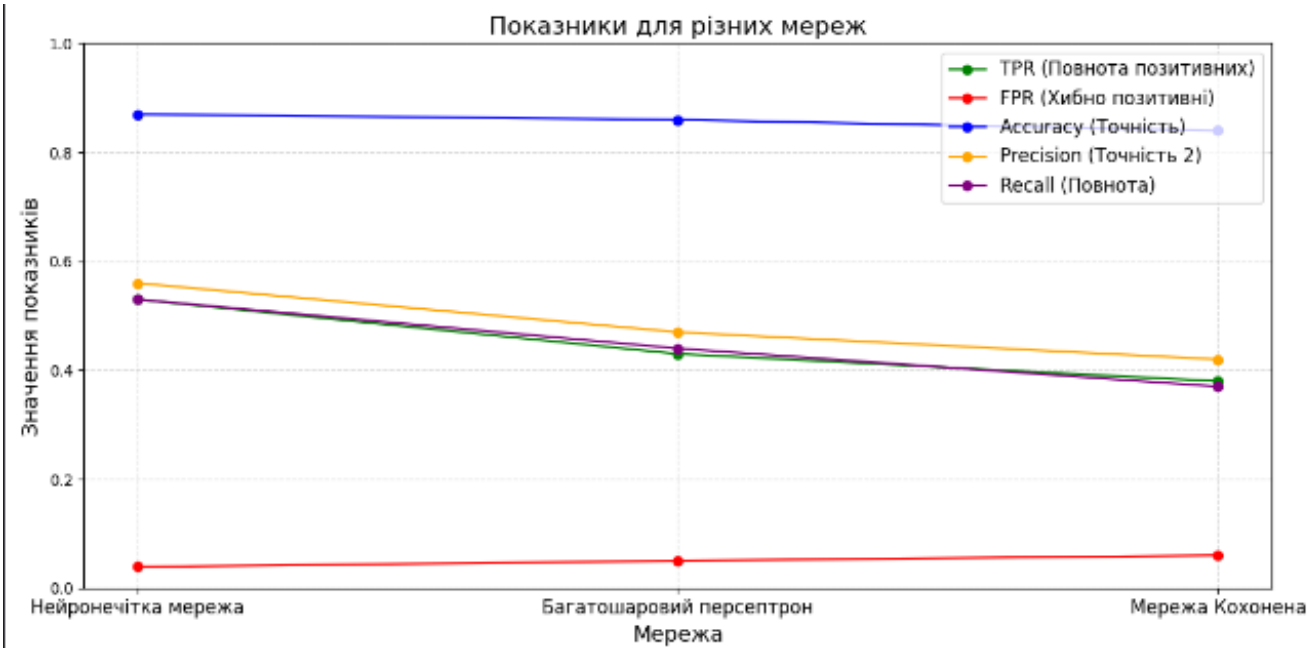


Рисунок 4.5 – Результати для атаки Probe

4.2.3 Дослідження оцінки якості для атаки R2L

Результати розрахунків для атаки R2L продемонстровані в таблиці 4.8

Таблиця 4.8 – Результати розрахунків оцінки якості для атаки R2L

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	60	20	43	877	0.57	0.022	0.90	0.75	0.57
Багатошаровий персептрон	55	23	50	854	0.53	0.029	0.88	0.68	0.52
Мережа Кохонена	50	29	54	831	0.47	0.034	0.86	0.62	0.47

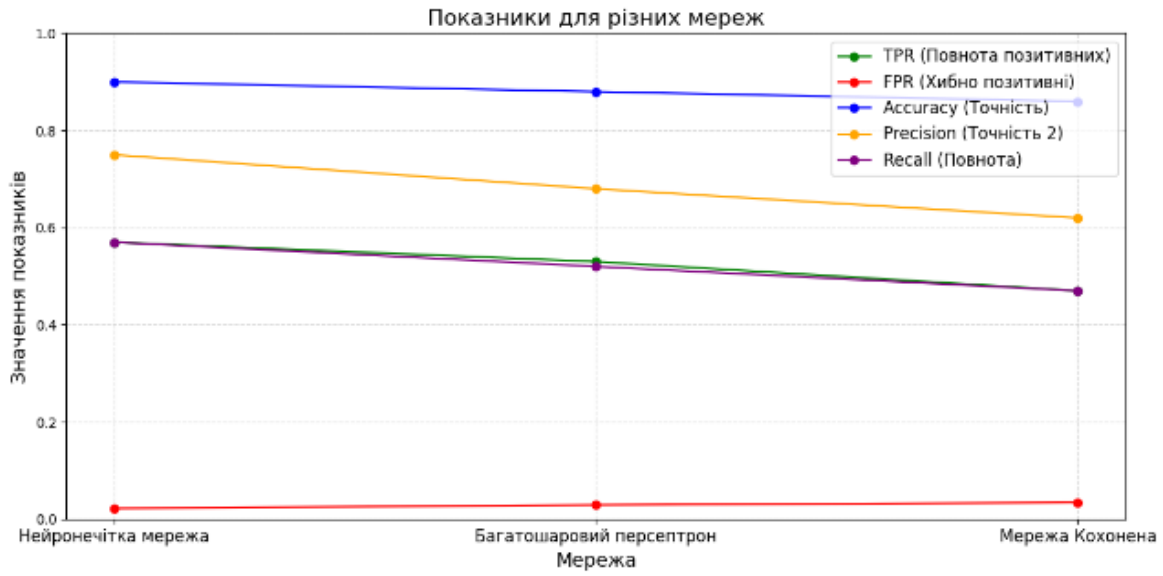


Рисунок 4.6 – Результати для атаки R2L

4.2.4 Дослідження оцінки якості для атаки U2R

Таблиця 4.9 – Результати розрахунків оцінки якості для атаки U2R

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	50	21	44	874	0.55	0.028	0.88	0.67	0.55
Багатошаровий персептрон	45	24	49	690	0.5	0.031	0.86	0.59	0.5
Мережа Кохонена	35	29	54	771	0.44	0.039	0.85	0.53	0.44

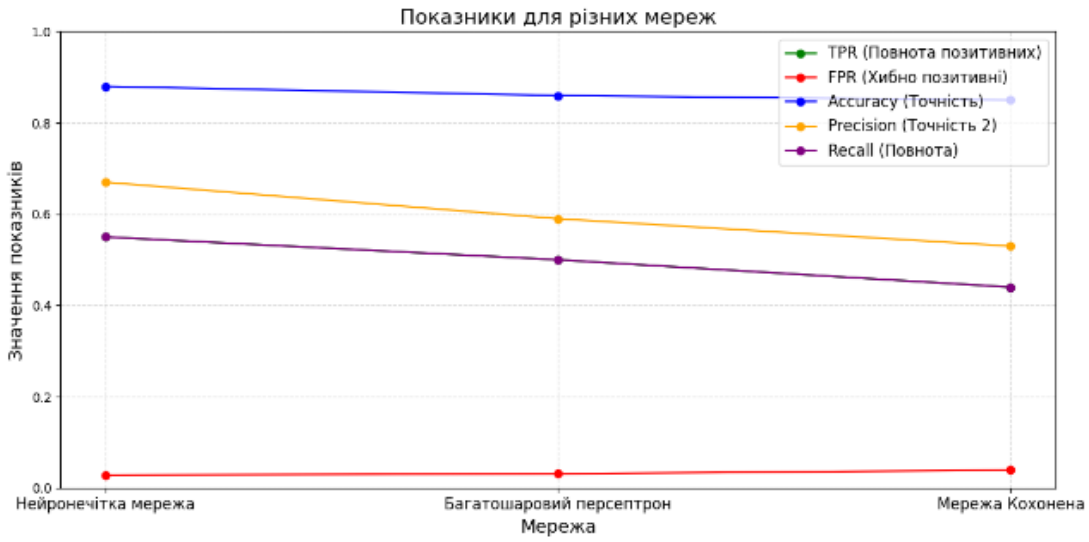


Рисунок 4.7 – Результати для атаки U2R

4.2.5 Дослідження оцінки якості для атаки Normal

У цьому підпункті проводиться дослідження якості виявлення нормальної мережевої активності (без атак) для перевірки можливості мереж виявляти правильну поведінку та уникати помилкових спрацьовувань. Оцінка включає порівняння точності, повноти та помилок

Таблиця 4.10 – Результати розрахунків оцінки якості для атаки Normal

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	271	100	50	850	0.95	0.1	0.91	0.90	0.95
Багатошаровий персептрон	949	51	30	870	0.97	0.05	0.93	0.95	0.97
Мережа Кохонена	871	130	60	840	0.93	0.13	0.89	0.87	0.93

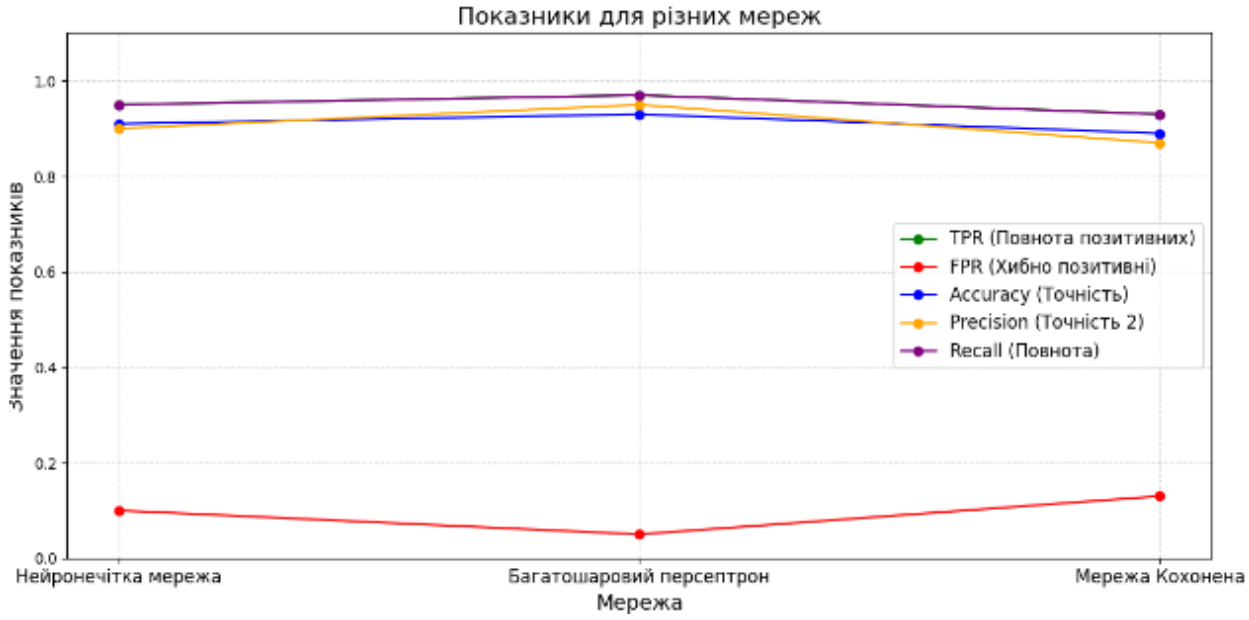


Рисунок 4.8 – Результати для атаки Normal

4.2.6 Дослідження помилки першого та другого роду

Помилка першого роду (False Positive) виникає, коли система неправильно класифікує нормальний трафік як атаку, що може призвести до зайвих тривог та ресурсних витрат. Помилка другого роду (False Negative) відбувається, коли система не виявляє реальну атаку, залишаючи її непоміченою. Дослідження продемонстровано для всіх нейроних мереж в таблиці 4.11, 4.12, 4.13.

Таблиця 4.11 – Розрахунок помилки першого та другого роду для MLP

	Помилка 1-го роду	Помилка 2-го роду
	Кількість неправильно виявлених атак (FP)	Кількість пропусків атак (FN)
Категорія атаки	MLP	MLP
DOS	67	60
U2R	4	5
R2L	13	6
Probe	10	2
Normal	35	30
Уссього	129	103

Таблиця 4.12 – Розрахунок помилки першого та другого роду для ANFIS

	Помилка 1-го роду	Помилка 2-го роду
	Кількість неправильно виявлених атак (FP)	Кількість пропусків атак (FN)
Категорія атаки	ANFIS	ANFIS
DOS	100	80
U2R	5	2
R2L	18	5
Probe	11	10
Normal	27	30
Уссього	170	127

Таблиця 4.13 – Розрахунок помилки першого та другого роду для SOM

	Помилка 1-го роду	Помилка 2-го роду
	Кількість неправильно виявлених атак (FP)	Кількість пропусків атак (FN)
Категорія атаки	SOM	SOM
DOS	60	50
U2R	4	2
R2L	17	10
Probe	10	7
Normal	32	30
Усього	124	99

MLP є найбільш точним методом з усіх трьох моделей, оскільки його показники помилок першого та другого роду значно нижчі в порівнянні з ANFIS і SOM.

ANFIS та SOM мають значно гірші результати, особливо у класифікації атак DOS і Probe, що вказує на їхню слабкість у роботі з даними типами атак.

Для загальної оцінки якості класифікаторів зробимо розрахунок F-мірки. Результати наведено у табл. 4.14.

Таблиця 4.14 – Результати оцінки якості за F-міркою

Мережа	F-Мірка
MLP	0.81
ANFIS	0.78
SOM	0.79

Після загальної оцінки якості можна зазначити, що найкращий результат демонструє багатошаровий персептрон. Нейро-нечітка мережа має оцінку на 0.02 вище, ніж мережа Кохонена.

4.3 Дослідження комбінованого підходу до визначення атак

Для порівняння результатів багатошарового персептрону, мережі Кохонена та нейро-нечіткої мережі було проведено дослідження на 40 векторах (додаток А). Результати представлені в таблиці 4.15 та в додатку В.

Таблиця 4.15 – Результати дослідження комбінованого підходу

	Вибірка	Нейронечітка мережа	Багатошаровий персептрон	Мережа Кохонена
Normal	7	11	7	7
DOS	10	6	11	13
R2L	6	10	6	3
U2L	10	5	9	0
Probe	7	8	7	7

За отриманими результатами розрахуємо F-мірку для комбінованого підходу табл. 4.15.

Таблиця 4.16 – Розрахунок оцінки якості комбінованого підходи

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall	F-мірка
Нейронечітка мережа	40	8	0	7	1	0.36	0.92	0.83	1	0.89
Багатошаровий персептрон	40	6	0	7	1	0.22	0.95	0.86	1	0.93
Мережа Кохонена	40	8	0	7	1	0.12	0.97	0.83	1	0.9

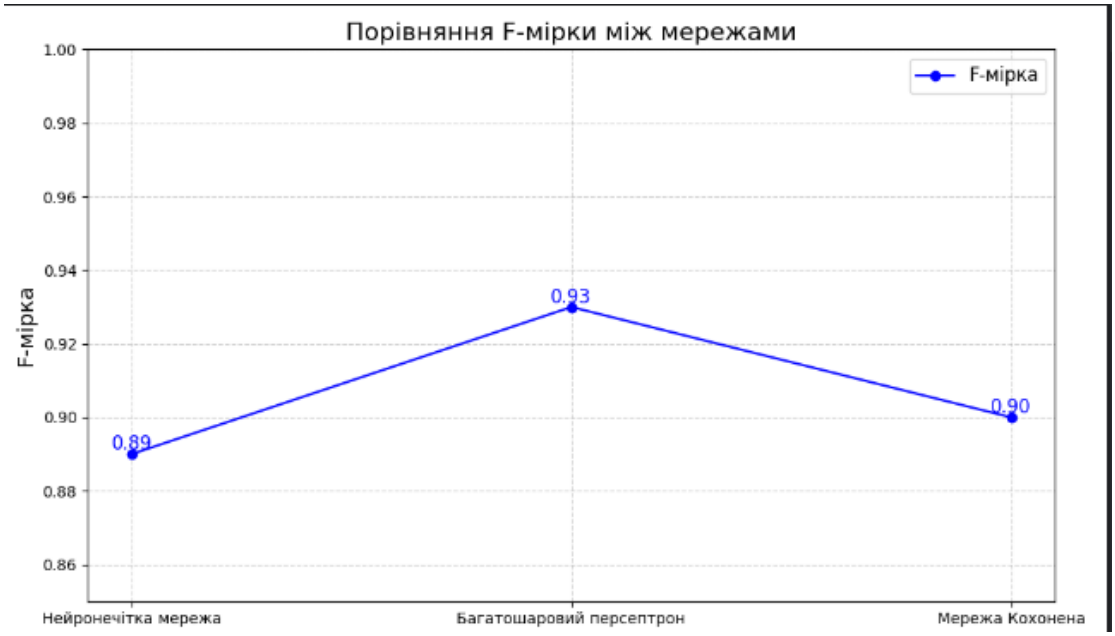


Рисунок 4.9 – Графік результатів комбінованого підходу за F-міркою

Можемо бачити, що багатошаровий персептрон найточніше визначив наявність атак та її категорію. Мережа Кохонена з меншою точність, але все одно досить точно виявила наявність атак. Нейронечітка мережа найгірше впоралася з визначенням наявності атак та категорій

4.4 Висновки

1. Оптимальні параметри багатошарового персептрону були визначені шляхом додаткових досліджень: обрано алгоритм навчання Левенберга-Марквардта, при якому на моделювання витрачається 13 епох. Значення MSE для тренувальної, контрольної та тестової вибірок складають 0.0049, 0.0120 та 0.0099 відповідно.

2. При оптимальній структурі отримано значення помилки на етапі навчання 0,67695, помилка на етапі тестування – 1,1712, а кількість епох склала 40.

3. Додаткові дослідження, проведені при оптимальних параметрах, показали, що помилка квантування на етапі навчання дорівнює 0,4178, а параметри точності та повноти складають 0,92 та 0,38 відповідно. При тестуванні точність складає 0,95, а повнота – 0,45.

4. Під час дослідження параметрів якості навчання було виявлено, що найкращі результати з виявлення атак показав багатошаровий персептрон. Досить добрі результати також продемонструвала мережа Кохонена. Найгірші показники якості були отримані при використанні нейро-нечіткої мережі.

5. Дослідження комбінованого підходу показало, що багатошаровий персептрон найкраще справився з виявленням атак та їх класифікацією. Мережа Кохонена також показала досить точні результати. Найгірші результати продемонструвала нейро-нечітка мережа.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

1. Нейронні мережі володіють здатністю до навчання, що надає їм перевагу над іншими методами, оскільки вони можуть виявляти не тільки відомі, але й нові типи атак. Крім того, нейромережеві технології швидко і ефективно реагують на атаки в комп'ютерних мережах, що робить їх оптимальним вибором для цього завдання.

2. Для класифікації атак планується використовувати багатошаровий персептрон, мережу Кохонена та нейро-нечітку мережу, з подальшим порівнянням результатів.

3. Для вхідних даних буде використовуватися набір даних NSL-KDD.

4. Оптимальні параметри багатошарового персептрону були визначені за допомогою додаткових досліджень: обрано алгоритм навчання Левенберга-Марквардта, що вимагає 13 епох на моделювання, при цьому MSE для тренувальної, контрольної та тестової вибірок становить 0.0049, 0.0120 і 0.0099 відповідно.

5. При оптимальній структурі було отримано помилку на етапі навчання 0,67695, помилку на тестуванні – 1,1712, а кількість епох склала 40.

6. Додаткові дослідження за оптимальними параметрами показали, що помилка квантування під час навчання дорівнює 0,4178, параметри точності та повноти становлять 0,92 і 0,38 відповідно, а при тестуванні точність дорівнює 0,95, а повнота – 0,45.

7. При дослідженні параметрів якості навчання було визначено, що найкращі результати з виявлення атак показав багатошаровий персептрон. Добрі результати також продемонструвала мережа Кохонена, а нейро-нечітка мережа показала найгірші показники якості.

8. Дослідження комбінованого підходу показало, що багатошаровий персептрон найкраще справився з виявленням атак і їх класифікацією. Мережа Кохонена також продемонструвала досить точні результати, тоді як нейро-нечітка мережа показала найгірші показники.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пахомова В.М., Видиш А.Д. Дослідження комбінованого варіанту визначення атак з використанням нейромережних технологій. Системні технології. Регіональний міжвузівський збірник наукових праць. № 3(140). Дніпро. 2022. С. 79-86. DOI: 10.34185/1562-9945-3-140-2022-08.

2. Пахомова В.М., Галушка О.В. Дослідження дворівневого виявлення мережевих атак категорії Probe засобами нейронних мереж. Системи обробки інформації. № 3 (204). Черкаси, 2024. С. 33-40. DOI: 10.35546/kntu2078-4481.2024.3.33

3. KDD Cup 1999 Data. Intrusion detection dataset. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

4. Zhukovyts'kyy I. V., Pakhomova V. M., Ostapets D. O., Tsyhanok O. I. Detection of attacks on a computer network based on the use of neural networks complex. Science and Progress of Transport. 2020, no. 5(89), pp. 68–79. doi: https://doi.org/10.15802/stp2020/218318.

5. Мустафаев А. Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика. Вопросы безопасности, 2016. № 2. С. 1-7. DOI: 10.7256.2409-7543.2016.2.18834

6. Zhukovyts'kyy I. V., Pakhomova V. M. Identifying threats in computer network based on multilayer neural network. Наука та прогрес транспорту. 2018. № 2 (74). P. 114–123. DOI: https://doi.org/10.15802/stp2018/130797 (дата звернення: 18.01.2025)

7. Pakhomova V.M., Bikovska D.G. Investigation of multilayer neural network parameters for determination of R2L category network attacks. Modern engineering and innovatite technologies. Germany, Karlsruhe: Sergeieva&Co, «ISE&E». 2021. № 18-02. pp. 39-43. DOI: 10.30890/2567-5273.2021-18-02-059.

8. Пахомова В. М., Коннов М.С. Дослідження двох підходів до вивлення мережних атак із використанням нейромережної технології. Наука та прогрес

транспорту, 2020. №3(87). С. 81-93. URL: https://doi.org/10.15802/stp2020/208233 (дата звернення: 18.01.2025)

9. Пахомова В. М., Маслак А. В. Дослідження комбінованого варіанту визначення атак з використанням нейромережних технологій, – 2022. – С. 79-86. – DOI: https://doi.org/10.32782/2663-5941/2022.5/19 (дата звернення: 18.01.2025)

10. Пахомова В.М., Мотиленко В.А. Дослідження можливості використання RBF для визначення Smurf атак на основі бази даних KDDCup. *Наукові праці Українського державного університету науки і технологій*. № 6. Дніпро. 2022. С. 20-26. DOI: 10.32782/2663-5941/2022.6/20.

11. Inam ul haq, Wang, J., Zhu, Y., Maqbool, S. (2021). An efficient hash-based authenticated key agreement scheme for multiserver architecture resilient to key compromise impersonation. Digital Communications and Networks, 7 (1), 140–150. doi: https:// doi.org/10.1016/j.dcan.2020.05.001 (дата звернення: 18.01.2025)

12. С. Козьменко, І. Школьник, А. Бухтіарова. Динамічні патерни оцінок банків на основі самоорганізуючих карт Кохонена. DOI: 10.15587/1729-4061.2022.269030

13. В. Лутсенко. Застосування принципу формалізації опису інформаційних об'єктів для проектування систем захисту інформації. DOI: 10.15587/1729-4061.2021.123050

14. Харитоненко І.О. Кіберзлочини в транспортній сфері: проблеми та перспективи боротьби. Науковий вісник. 2020. № 4. С. 72-77. DOI: 10.36695/2219-5521.4.2020.72

15. Arumugam, S. B. B. S. P. R., Dinesh, S. R. K., Iyyappan, M. K. N. *Network Intrusion Detection System using ANFIS classifier* // Journal of Ambient Intelligence and Humanized Computing. – 2019. – Vol. 10, No. 6. – P. 2413–2426. – DOI: 10.1007/s00542-019-04742-5.

16. Kumar, N. S., Iyer, P. P. K., Krishnan, M. S. J. *The effects of combined application of SOM, ANFIS and Subtractive Clustering in detecting intrusions in*

computer networks // IEEE Access. – 2020. – Vol. 8. – P. 65412–65426. – DOI: 10.1109/ACCESS.2020.2977957.

17. Hossain, M. A., Rahman, M. A., Islam, S. S. *Network Intrusion Detection and Prevention System Using Hybrid Self-Organizing Map, Radial Basis Function Neural Network, and Linear Classifier Algorithm* // IEEE Access. – 2020. – Vol. 8. – P. 158453–158464. – DOI: 10.1109/ACCESS.2020.2993582.

18. MathWorks. Neural State-Space Models: Create MLP Network. MathWorks Documentation. URL: https://ww2.mathworks.cn/help/ident/ref/idneuralstatespace.createmlpnetwork.html?searchHighlight=MLP&s_tid=srchtitle_support_results_2_MLP (дата звернення: 18.01.2025).

19. MathWorks. Self-Organizing Maps. MathWorks Documentation. URL: https://ww2.mathworks.cn/help/deeplearning/self-organizing-maps.html?s_tid=srchbrcm (дата звернення: 18.01.2025).

20. MathWorks. Neuro-Adaptive Learning and ANFIS. MathWorks Documentation. URL: https://ww2.mathworks.cn/help/fuzzy/neuro-adaptive-learning-and-anfis.html (дата звернення: 18.01.2025).

21. Wong J. NSL-KDD Dataset. GitHub Repository. URL: https://github.com/jmnwong/NSL-KDD-Dataset (дата звернення: 18.01.2025).

22. Normalization. GitHub Repository. URL: https://github.com/mhs-rajaei/MATLAB/blob/master/Data%20Mining/NSL-KDD/Normalization.m (дата звернення: 18.01.2025).

23. List of characteristics of NSL-KDD: Total Attributes of NSL-KDD [Електронний ресурс]. ResearchGate. URL: https://www.researchgate.net/figure/List-of-characteristics-of-NSL-KDD-Total-Attributes-of-NSL-KDD_tbl1_343408460 (дата звернення: 20.01.2025).

24. Attack types of DoS, R2L, U2R, Probe categories [Електронний ресурс]. ResearchGate. URL: https://www.researchgate.net/figure/Attack-types-of-DoS-R2L-U2R-Probe-categories_tbl1_327110465 (дата звернення: 20.01.2025)