МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Український державний університет науки і технологій

Кафедра «Електронні обчислювальні машини»

«ДО ЗАХИСТУ»

Завідувач кафедри

(підпис) проф Жуковицький І.В. (ПІБ)

«20» 12 2021 р.

ДИПЛОМНА РОБОТА

на здобуття освітнього ступеня «магістр»

Галузь знань 12 Інформаційні технології

(шифр) (назва)

Спеціальність 123 Комп'ютерна інженерія

(код) (повна назва)

Тема «Визначення атак на комп'ютерну мережу з використанням нейромережної технології»

Theme «Identification of attacks on a computer network using neural network technology»

Керівник дипломного проекту	доц. (посада)	(підпис)	Хахлюва В.М. (ПІБ)
Консультант розділу з БЖД	доц. (посада)	(підпис)	Сабін О.Ю (ПІБ)
Нормоконтролер	доцент (посада)	(підпис)	Молчанов В.О. (ПІБ)
Студент групи	КС 20.1 (група)	(підпис)	Видиш А.Д. (ПІБ)
Student	Vydysh Anastasiia (family name)		

Дніпро
2021

Довідка

про відсутність плагіату у випускній кваліфікаційній роботі

Міністерство освіти і науки України

Український державний університет науки і технологій

Кафедра Електронно-обчислювальних машин

ДОВІДКА

За результатами перевірки випускної кваліфікаційної роботи здобувача вищої освіти Вуцин Анастасій Денисівич

(прізвище, ім'я, по батькові)

на тему: Визначення атак на комп'ютерну мережу з використанням нейромережевої технології

в роботі не виявлено порушень академічної доброчесності.

Керівник ВКР _____

Український державний університет науки і технологій

Факультет _____КТС_____ кафедра _____ЕОМ_____
Спеціальність _____123 Комп'ютерна інженерія_____

«ЗАТВЕРДЖУЮ»
Завідувач кафедри

_____
(підпис)
«___»_____20_ р.

ЗАВДАННЯ

до дипломної роботи на здобуття освітнього ступеня _____магістра_____
(освітнього ступеня)

студента групи КС2021____Видиш Анастасії Денисівни_____
(номер групи) (ПІБ)

1 Тема дипломної роботи __«Визначення атак на комп'ютерну мережу з використанням нейромережної технології»

_____

затверджена наказом по університету від «_31_»_серпня_____20_21_ р. № _508-СТ____.

2 Термін подання студентом закінченої роботи__09.12.2021_____

3 Вихідні дані до дипломної роботи__відкрита база, що має параметри мережевоготрафіку «NSL-KDD»_____

_____

4 Зміст пояснювальної записки (перелік питань до розробки) _Вступ 1 Огляд нейронних мереж щодо визначення мережевих атак 2 Постановка задачі визначення мережевих атак 3 Створення нейронних мереж щодо виявлення мережевих атак 4 Дослідження комбінованого варіанту щодо визначення мережевих атак 5 Охорона праці та безпека в надзвичайних ситуаціях Висновки

_____

5 Перелік креслень (демонстраційного матеріалу) _____

_____

_____

_____

_____

6 Розділи та консультанти

Розділ	Консультант	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях	Саблін О. І.		

КАЛЕНДАРНИЙ ПЛАН

Назва розділу	Термін виконання	Обсяг розділу, %
Вступ		5
Огляд нейронних мереж щодо визначення мережевих атак		20
Постановка задачі визначення мережевих атак		10
Створення нейронних мереж щодо виявлення мережевих атак		30
Дослідження комбінованого варіанту щодо визначення мережевих атак		20
Охорона праці та безпека в надзвичайнихситуаціях		10
Висновки		5

Дата видачі завдання: « »_____20 р.

Керівник дипломної роботи _____ _____

(підпис) (ПІБ)

Завдання прийняв до виконання _____ _____

(підпис) (ПІБ)

РЕФЕРАТ

Видиш А. Д. Визначення атак на комп’ютерну мережу з використанням нейромережної технології. Український державний університет науки та технологій, кафедра електронних обчислювальних машин. Дипломна магістерська робота. 72 с. 34 рис. 13 табл. 49 джерел. 4 додатка.

У дипломній магістерській роботі виконано огляд нейронних мереж для визначення мережевих атак на комп’ютерну мережу. Математичний апарат – багатошаровий персептрон, нейронечітка мережа та мережа Кохонена. Для визначення ступеню імовірності атаки на комп’ютерну мережу використовується нейронечітка мережа. Для виявлення атаки та визначення її категорії – багатошаровий персептрон та мережа Кохонена. Нейронечітка мережа та багатошаровий персептрон створені за допомогою MatLAB, мережа Кохонена написана на мові програмування Python. На основі цих нейромереж проведені дослідженні: визначення оптимальних параметрів кожної нейромережі, визначення показників оцінки якості кожної нейромережі окремо та визначення показників оцінки якості при комбінованому підході. Для багатошарового персептрону було досліджено розмір вибірки та алгоритми навчання, розрахован розмір прихованого шару. Для нейронечіткої мережі було перевірено оптимальність розміру вибірки, методи навчання. Після навчання нейронечіткої мережі була зроблена перевірка на адекватність. Для мережі Кохонена зроблена перевірка розміру вибірки та підібраний оптимальний розмір карти. Оцінка якості проводилася для кожної нейромережі окремо – найкращий результат показав багатошаровий персептрон. При дослідженні оцінки якості для комбінованого підходу кращий результат отримано для багатошарового персептрона.

АТАКА, КАТЕГОРІЯ, БАГАТОШАРОВИЙ ПЕРСЕПТРОН, МЕРЕЖА КОХОНЕНА, НЕЙРОНЕЧІТКА МЕРЕЖА, КОМБІНОВАНИЙ ПІДХІД, ЯКІСТЬ.

ЗМІСТ

ВСТУП

Сучасний світ неможливо уявити без комп'ютерних мереж: як локальних, так і глобальних. Тому питання мережевої безпеки стає все більш злободенним. Наразі методики виявлення атак можна підсилити використанням нейронних мереж, що підтверджує актуальність теми магістерської дипломної роботи.

Метою магістерської дипломної роботи є визначення атак на комп'ютерну мережу з використанням нейромережної технології аналіз нейронних мереж щодо виявлення мережевих атак. Відповідно до мети поставлені наступні задачі:

–виконати огляд нейронних мереж, щодо визначення мережевих атак;

–створити нейромережі для виявлення мережевих атак та категорій;

–визначити оптимальні параметри нейронних мереж;

–провести дослідження параметрів якості кожної нейромережі окремо та комбінованого підходу.

На сучасному етапі виявленням мережевих атак на комп'ютерну мережу з використанням нейронних мереж займаються вчені та науковці з різних держав:, Читракар Р., Хуанг Ч., Цзинвэй Хуанг, Збигнев Калбарчик, Дэвид М. Николь, Кесавулу Редді Е., Бочков М. В., Бурлаков М. Е., Васильев В. І., Веселов В.В., Грішанов К.М., Ельманов О.А., Жульков Є. В., Жуков В. Г., Жуковицький І. В., Карелов І. Н., Коннов М. С., Кораблев Н. М., Котов В. Д., Литвиненко В.І, Мустафаєв А. Г., Пахомова В. М., Саламатов Т. А., Фролов П. В. та ін. Так, Пахомова В. М. та Коннов М. С. досліджували два підходи до виявлення мережевих атак з використанням нейромережної технології. Вчений Мустафаєв А. Г. розробляв нейромережеву систему виявлення комп'ютерних атак на основі аналіза мережевого трафіка на основі MLP та SOM. Кандидат технічних наук Жульков Є. В. займався розробкою модульних нейронних мереж для виявлення класів мережевих атак. Вчені Фролов П. В., Чухраєв І. В., Грішанов К.М. застосували штучні нейронні мережі MLP, RBF, SOM у системах виявлення вторгнень. Бочков М. В. займався реалізацією методів виявлення програмних атак та протидії програмному пригніченню в комп'ютерних мережах на основі нейронних мереж та генетичних алгоритмів оптимізації. Науковці Веселов В.В., Ельманов О.А., Карелов І. Н. розробили комплекс

моніторингу інформаційних систем на основі нейромережевих технологій. Цзинвэй Хуанг, Збигнев Калбарчик, Дэвид М. Николь зробили наукову роботу на тему виявлення вторгнень за допомогою латентного розміщення Діріхде. Читракар Р., Хуанг Ч. провели дослідження на тему виявлення вторгнень на основі аномалій з використанням підходу гібрідного навчання, що поєднує кластеризацію k-Medoids і наївну байєсову класифікацію. Кесавулу Редді Е. представив свою роботу з виявлення вторгнень у комп'єтерні мережі за допомогою нейромереж та їх застосування.

Представлена магістерська дипломна робота складається із вступу, п’яти розділів та висновків. У розділі 1 виконаний огляд існуючих нейромереж щодо визначення мережевих атак та зроблено вибір нейромереж для подальшої роботи на основі проведеного аналізу наукових робіт. У розділі 2 сформульована постановка задачі визначення мережевих атак на комп’ютерну мережу, розроблена загальна схема виявлення мережевих атак. У розділі 3 описано створені нейронні мережі для виявлення мережевих атак, проведено дослідження для знаходження оптимальних параметрів. У розділі 4 представлені дослідження оптимальних параметрів нейронних мереж. У розділі 5 подані основні нормативи з трудової безпеки, правила безпеки та першочергові дії при надзвичайних ситуаціях, правила надання домедичної допомоги.

Результати дипломної магістерської роботи доповідались на XIVМіжнародній науково-практичній конференції «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті» (15-16 грудня 2020), Всеукраїнській науково-технічній конференції молодих учених, магістрантів та студентів «Науково-технічний прогрес на транспорті» (29 березня 2021), а також на 81 Всеукраїнській науково-технічній конференції молодих учених, магістрантів та студентів «Наука і сталий розвиток транспорт» (28 листопада 2021), що відбулись в Дніпровському національному університеті залізничного транспорту імені академіка В. Лазаряна в 2020-2021 р. Тези доповідей опубліковані у відповідних збірникахдо конференцій (додаток Г)

1 ОГЛЯД НЕЙРОННИХ МЕРЕЖ ЩОДО ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК

1.1 Постановка проблеми

Комп’ютерні мережі є важливою частиною нашого життя. У віртуальному світі можливо спілкуватися з друзями, робити покупки та читати наукові статті. На підприємствах мережа об’єднує багато робочих станцій, що забезпечує безперебійну роботу. Але треба пам’ятати про безпеку інформації у мережах: кібератаки – біч сучасного світу. З січня по грудень 2020 року було відкрито 496 кримінальних проваджень пов’язаних з кіберзлочинами в Україні, спрямованими на критично важливі об’єкти інфраструктури [1]. Тому протидія атакам у віртуальному світі є гострим та актуальним питанням.

Велика частка кібератак припадає на державні підприємства. Мережа Придніпровської залізниці є критичним об’єктом і тому потребує посиленого захисту. Основна мета забезпечення інформаційної безпеки – зведення збитків до мінімуму, при цьому зберігання конфіденційності, доступності та цілісності.

Наразі існує комплекс програмно-апаратних засобів захисту – застосування firewall, систем вторгнень, моніторінгу та інші. Firewall - це система на основі програмного або апаратного забезпечення, яка є своєрідним посередником між безпечними та неперевіреними мережами, а також їх частинами [2]. Головна функція брандмауера — фільтрація шкідливого та потенційно небезпечного контенту та з’єднань [3]. Системи виявлення вторгнень – це системи,які збирають інформацію з різних системних і мережевих джерел, а потім аналізують інформацію про ознаки вторгнення та зловживання [4]. Системи виявлення вторгнень можуть розпізнавати такі атаки як: code injection, brute-force, network activity та багато інших. Ці засоби є відносно дієвими при застосуванні у комплексі.

Системи виявлення вторгнень класифікуються за такими критеріями:

–по типу об’єкта моніторингу – вузлові та мережеві;

–по типу архітектури – централізовані та розподілені;

–по типу аналізу – зі збереженням стану та без;

–по типу виявлення атак – виявлення аномалій, виявлення зловживань, виявлення порушень у протоколі;

–по типу реагування – активні та пасивні [5].

Оскільки у кіберзахисті важливо як умога швидше виявляти атаки, то найчастіше використовуються активні системи.

Для визначення мережевих атак використовується декілька методів:

–виявлення аномалій - поведінкова біометрія, статистичний аналіз, нейронні мережі, експертні системи, кластерний аналіз, Support vector machines;

–виявлення зловживань - графи сценаріїв атак, Support vector machines, нейронні мережі, експертні системи, методи засновані на специфікаціях, аналіз систем станів, Multivariate Adaptive Regression Splines, сигнатурні методи, штучні імунні системи [6].

Нейронні мережі - є дієвим методом для виявлення атак. Переваги нейронних мереж: можливість працювати з великим об’ємом даних; здатність до самонавчання; можливість виділити низьку ознак, за якими можна провести класифікацію мережевих пакетів; розпізнавання атаки у режимі реального часу [7].

1.2 Нейронні мережі для визначення мережевих атак

1.2.1 Багатошаровий персептрон

Багатошаровий персептрон – клас багатошарових мереж прямого розповсюдження, де кожен обчислювальний елемент може використовувати порогову або сигмоідальну функцію активації [6]. Багатошаровий персептрон можна віднести до контрольованих нейромереж. Тобто мережа «знає» бажаний вихід для кожного даного вхідного елемента [6, 9].

Багатошаровий персептрон складається із вхідного шару, одного або декількох прихованих шарів та вихідного. Під час навчання кожен вузол здійснює просту обробку даних з вагами та порогами, які обираються вільно на першому етапі навчання. Етапи навчання нейромережі називаються епохами а прогресують ітераційно. Під час кожної епохи дані циклічно оброблюються: аналізуються та порівнюються цільові та поточні значення ефективних вихідних параметрів, оцінюється помилка, яка використовується для коригування ваг. У результаті на

виході маємо дані відповідно до характеристик ваг та вузлів. Таким чином, можна отримати мережу з потрібним відгуком, якщо змінити характер зв’язку між вузлами та значення початкових ваг [9, 10]. Схематично зобразити багатошаровий персептрон можна так:

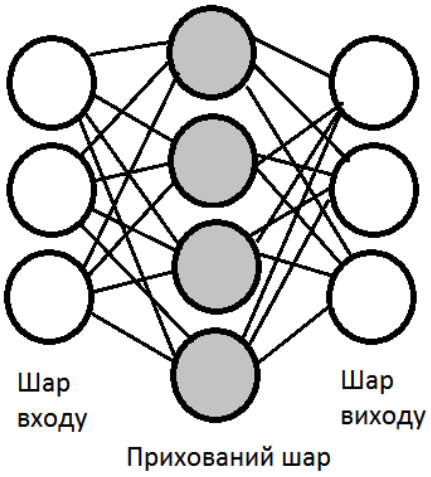


Рисунок 1.1 – Структурна схема багатошарового персептрону

Переваги багатошарового персептрону такі [11]:

–можливість аналізувати вхідні дані та робити висновки, навіть якщо дані неповні;

–можливість алгоритмів адаптуватися до нових даних;

–можливість обробляти дані у режимі реального часу.

До недоліків багатошарового персептрону можна віднести [12]:

–низька достовірність визначення допустимих відхилень параметрів поточного функціонування в області мінімальних значень. Ця проблема спричинена неадекватністю цільового функціоналу алгоритму зворотного поширення помилки (використовується під час навчання);

–великий час навчання нейромережі.

Оскільки багатошаровий персептрон є популярною технологією, то багато науковців проводять свої дослідження за допомогою багатошарового персептрона. Так, наприклад, В.М. Пахомова та М.С. Коннов проводили дослідження та порівняли

два підходи до виявлення мережевих атак за допомогою багатошарового персептрону та ансамблю з п’яти нейромереж (багатошаровий персептрон та самоорганізаційні карти Кохонена), де найефективнішим став другий підхід [13]. А.Г. Мустафаев розробив програму у нейропакеті MatLAB багатошарового персептрона, яка класифікує атаки на мережу [14]. Кандидат технічних наук Жульков Є. В. у своєму авторефераті займався розробкою модульних нейронних мереж для виявлення класів мережевих атак серед яких є багатошаровий персептрон [15]. А. В. Гришин викладає у науковій статті результати створення комплексу нейромереж (багатошаровий персептрон та самоорганізаційні карти Кохонена) для вирішення задачі виявлення комп'ютерних атак [16].

1.2.2 Самоорганізаційна карта Кохонена

Самоорганізаційна карта Кохонена є ефективним інструментом для візуалізації багатовимірних даних.

Суть роботи самоорганізаційної карти полягає у перетворенні нелінійних статичних співвідношень між багатовимірними даними і простих геометричних зв’язків між точками даних на пристрої відображення низької розмірності. Найчастіше зображенням є двовимірна сітка вузлів. Самоорганізаційна карта має таку властивість як узагальнення. Тобто здійснюється стиснення інформації при чому зберігаються найбільш важливі топологічні чи метричні зв’язки між елементами даних. Таким чином ця нейромережа ідеально підходить для вирішення задач класифікації [20].

Переваги мережі Кохонена [20]:

–візуалізація результату аналізу;

–навчання мережі без вчителя;

–виявлення закономірностей в даних, які можуть бути не явні.

Структурна схема самоорганізаційних карт придставлена на рис. 1.2.

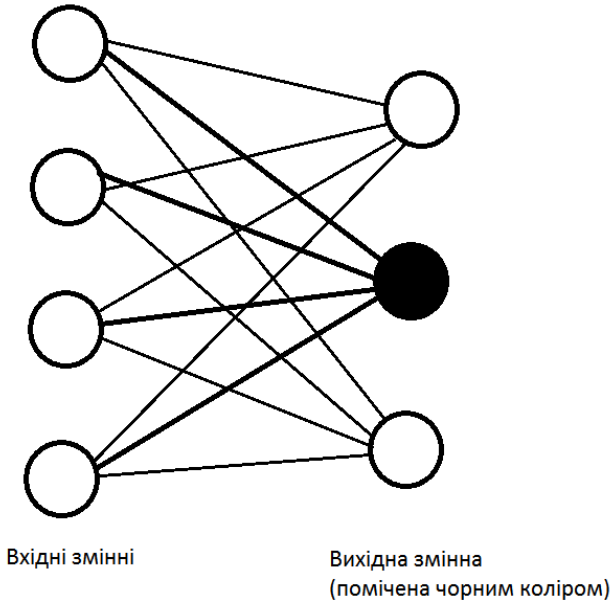


Рисунок 1.2 - Структурна схема самоорганізаційної карти Кохонена

Самоорганізаційні карти Кохонена часто використовують у ансамблі чи комбінаціях з іншим нейромережевими технологіями для виявлення атак на мережу. Так, Браницький О. О., Тимофіїв А. В. та Котенко І. В. у своїй роботі «Виявлення аномальних мережевих з'єднань на основі гібридізації методів обчислювального інтелекту» проводять дослідження алгоритму генетико-конкуруючого навчання мережі Кохонена [22]. Вчені Фролов П. В., Чухраєв І. В., Грішанов К.М. застосували штучні нейронні мережі MLP, RBF, SOM у системах виявлення вторгнень [23]. Науковці Веселов В.В., Ельманов О.А., Карелов І. Н. розробили комплекс моніторингу інформаційних систем на основі нейромережевих технологій [24].

1.2.3 Нейронечітка нейромережа

Нейронечітка нейромережа дозволяє об'єднати в собі переваги нейронних мереж і систем нечіткого висновку. Головна ідея, яка знаходиться в основі гібрідних систем, полягає в тому, щоб використовувати існуючи вибірки даних для визначення параметрів функцій приналежності, які б найкраще відповідали конкретній системі нечіткого виводу. При цьому для знаходження параметрів застосовуються відомі процедури навчання НМ [17].

Основними властивостями нейронечіткої мережі є [18]:

–нейронечіткі мережі засновані на нечітких системах, які навчаються за допомогою методів, використовуваних у нейромережах;

–нейронечітка мережа зазвичай є багатошаровою нейронною мережею. Перший шар становить вхідні змінні, середній становить нечіткі правила, а третій – вихідні змінні. Ваги підключення відповідають нечітким множинам вхідних і вихідних змінних;

–нейронечітка мережа завжди може бути інтерпретована як система нечітких правил;

–процедура навчання враховує семантичні властивості нечіткої системи. Це виражається в обмеженні можливих модифікацій, які застосовуються до параметрів, що налагоджуються.

За способом взаємодії нечіткої логіки та нейромереж поділяють на такі класи [18]:

–нечіткі нейронні системи. В цьому випадку в нейронних мережах застосовуються принципи нечіткої логіки для прискорення процесу налагодження або поліпшення інших параметрів;

–конкуруючі нейронечіткі системи. У таких моделях нечітка система і нейронна мережа працюють над однією задачею, не впливаючи на параметри одна одної;

–паралельні нейронечіткі системи. Такий клас поділяється на типи – нечітка асоціативна пам’ять та системи із виділенням нечітких правил шляхом використання самоорганізаційних карт;

–інтегровані (гібридні) нейронечіткі системи – системи з тісною взаємодією нечіткої логіки і нейронних мереж. Ці системи використовуються найчастіше.

За характером навчання виділяють такі типи [18]:

–самоналагоджувані нейронечіткі мережі – з адаптацією структури та параметрів;

–адаптивні нейронечіткі мережі – із жорсткою структурою та адаптацією параметрів мережі.

Нейронечіткі мережі також поділяються за методом оптимізації та типом параметрів адаптації.

Переваги нейронечіткої мережі наступні [18]:

–можливість оперувати вхідними даними, заданими нечітко;

–можливість нечіткої формалізації критеріїв оцінки і порівняння

–можливість проведення якісних оцінок як вхідних даних, так і виведених результатів;

–можливість проведення швидкого моделювання складних динамічних систем і їхній порівняльний аналіз із заданим ступенем точності.

Структуру нейронечіткої мережі можно представити наступним чином (рис. 1.3):

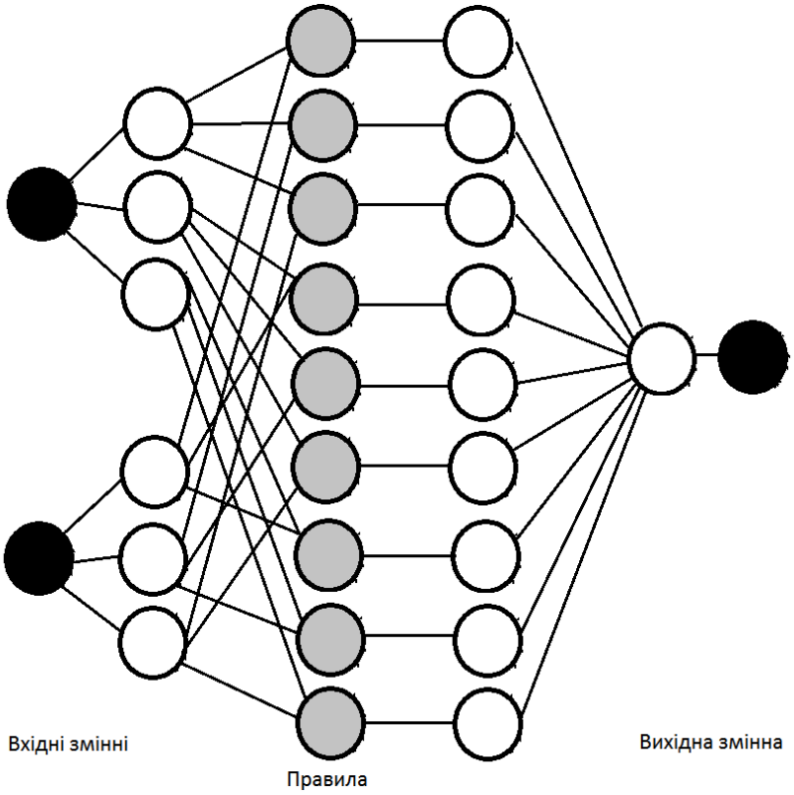


Рисунок 1.3 - Структурна схема нейронечіткої мережі

Наразі нейронечітка менш вживана технологія у дослідженнях вчених, проте є суттеві роботи. Асланов К.Дж. та Байрамов Х. використовували нейронечітку систему для вирішення проблеми класифікації загроз у комп’ютерних мережах у дисертаційній роботі [21].

1.3 Сучасні системи виявлення атак

Для виявлення атак на комп'ютерні мережі існує наступне рішення – системи виявлення та запобігання вторгнення (Intrusion detection systems, IDS і Intrusion prevention systems, IPS).

Системи виявлення вторгнень – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу або вторгнення до комп'ютерної мережі [25]. До аномальних дій на мережу можна віднести: несанкціонований доступ до конфіденційних даних, спроби підвищення привілеїв доступу окремих користувачів чи груп, спроби використання уразливих частин програмного забезпечення та інші.

Використання IPS-систем переслідує декілька цілей [26]:

–виявити вторгнення або мережеву атаку і запобігти їх;

–спрогнозувати можливі майбутні атаки і виявити вразливості для запобігання їх подальшого розвитку;

–виконати документування існуючих загроз;

–забезпечити контроль якості адміністрування з точки зору безпеки,особливо в великих і складних мережах;

–отримати корисну інформацію про проникнення, які мали місце, для відновлення і коригування викликали проникнення факторів;

–визначити розташування джерела атаки по відношенню до локальної мережі, що важливо при прийнятті рішень про розташування ресурсів в мережі.

Системи IDS аналогічні IPS, кожна IPS має у собі IDS для роботи у реальному часі та можливості автоматично блокувати мережеві атаки.

IDS зазвичай складається з:

–бази даних вразливостей;

–терміналу управління для налаштування системи, моніторингу стану мережі;

–системи збору подій;

–системи аналізу подій;

–системи логування подій та результати аналізу.

Загальна класифікація сучасних підходів до детектування мережевих атак може бути представлена наступним чином [26,27]:

–За типом об'єкта моніторингу – хостові СВВ та мережеві СВВ.

–По архітектурі – централізовані та розподілені.

–За технологією аналізу – без збереження стану та зі збереженням стану.

–За методом виявлення атак – системи виявлення зловживань, системи виявлення аномалій та системи виявлення порушень в протоколі.

–За способом реагування – пасивні та активні.

Можливі підходи до реалізації систем, які використовують нейромережеві технології:

–комбінацію з багатошарового персептрону, самоорганізаційної карти, радіально-базисної мережі у своїй роботі приводять вчені Фролов П. В., Чухраєв І. В., Грішанов К.М.;

–рециркуляційна нейромережа, багатошаровий персептрон, самоорганізаційна карта Кохонена використовують у дослідженні Ю. Г. Ємельянова, А. А. Талалаєв, І. П. Тищенко, В. П. Фраленко;

–комбінацію багатошарового персептрона та рециркуляційної нейромережі використовують у своїх дослідженнях у Брестському державному технічному університеті.

У Брестському державному технічному університеті у лабораторії штучних нейронних мереж пропонуються різні підходи до побудови систем виявлення атак за допомогою нейромережевих технологій. Наприклад, комбінуючи багатошаровий персептрон та рециркуляційну нейромережу науковці змогли отримати потужний інструмент для виявлення та класифікації атак [29]. Схематично представлена робота системи на рис. 1.4.

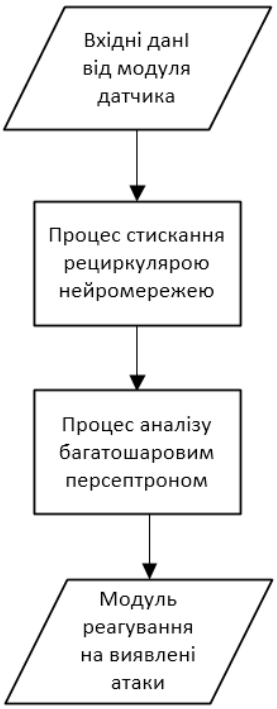


Рисунок 1.4 – Схематичне зображення роботи системи виявлення атак, запропонована Брестським державним технічним університетом

Ю. Г. Ємельянова, А. А. Талалаєв, І. П. Тищенко, В. П. Фраленко у своїй роботі «Нейромережева технологія виявлення мережевих атак на інформаційні ресурси» пропонують технологію нейромережевого моніторингу мережевих атак з використанням IDS Snort. Для нейромережевого моніторингу використовуються комбінації: рециркуляційна нейромережа, багатошаровий персептрон, самоорганізаційна карта Кохонена [30]. Схематично зображена робота запропонованої системи на рис. 1.5.

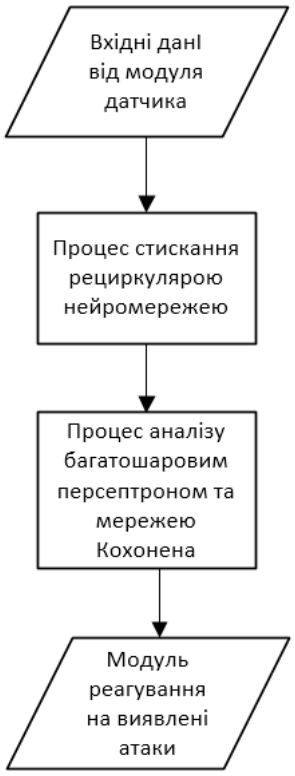


Рисунок 1.5 – Схематичне зображення роботи системи виявлення атак, запропонована Ю. Г. Ємельянова, А. А. Талалаєв, І. П. Тищенко, В. П. Фраленко

1.4 Висновки

1. Наразі нейронні мережі досить розвинені та мають ряд переваг перед традиційними комп’ютерними системами: здатність до навчання, здатність до узгодження та абстрагування. Завдяки цьому нейромережеві технології показують високі результати у вирішенні задач виявлення та класифікації мережевих атак. Це дозволяє швидко виявити аномалію та прийняти необхідні заходи для захисту від атаки або її ліквідування.

2. За результатами огляду наявної інформації для вирішення задачі виявлення та класифікації мережевих атак можна використовувати такі технології: багатошаровий персептрон, мережа Кохонена, радіально-базисна нейромережа, рециркуляційна нейромережа нейронечітка нейромережа. Для подальшої роботи обрано багатошаровий персептрон, нейронечітка нейромережа, мережа Кохонена.

3. На основі проведеного аналізу було виділено такі архітектурні підходи: комбінацію з багатошарового персептрону, самоорганізаційної карти, радіально-базисної мережі; рециркуляційна нейромережа, багатошаровий персептрон, самоорганізаційна карта Кохонена; комбінацію багатошарового персептрона та рециркуляційної нейромережі. Для дипломної роботи обрано комбінацію з багатошарового персептрону, самоорганізаційної карти та нейронечіткої мережі.

2 ПОСТАНОВКА ЗАДАЧІ ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК

2.1 Необхідність використання нейромережної технології щодо визначення мережевих атак на комп'ютерну мережу

Разом з розвитком цифрових технологій та комп'ютерних мереж почастилися випадки атак на сервера та комп'ютерні мережі. Не завжди встановлені засоби захисту справляються з своєю задачею, оскільки атаки здійснюються дуже швидко та різноманіття способів виводу систем із ладу збільшується. Для того, щоб швидко та точно виявляти атаки, навіть які з'явилися щойно, ідеально підходять нейронні мережі: багатошаровий перцептрон, мережа Кохонена, нейронечітка мережа (гібридна система) [31].

Атаки поділяються на наступні категорії [32]: DoS; U2R; R2L; Probe.

DoS (Denial of Service, «відмова в обслуговуванні») – це атака на цільову систему з метою завдати шкоду шляхом навантаження системи до стану відмови. Таким чином звичайні користувачі не мають можливості доступу до системи. Найчастіше атака виконується на веб-додатки, сайти – відправляється дуже велика кількість запитів до серверів, сервери не витримують навантаження. Даний тип атак розділяється на: back, land, neptune, pod, smurf, teardrop.

U2R (User to Root, «отримання привілеїв користувачем») – ця атака має на меті отримання звичайним користувачем прав адміністратора. Дана атака небезпечна тим, що отримав привілеї користувач отримує повний доступ до системи та інформації, яка у ній знаходиться. Даний тип атак розділяється на: buffer_overflow, loadmodule, perl, rootkit.

R2L (Remote to Local, «віддаленно-локально») – це атака на систему шляхом доступу до неї з віддаленого комп'ютера незареєстрованого користувача.

Тип атаки розділяється на: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster.

Probe – атака полягає у скануванні мережевих портів для отримання захищеної інформації. Розділяють цю атаку на: ipsweep, nmap, portsweep, satan.

Ці класи представлені у базі даних NSL-KDD [33], 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 використовуватися усі подані характеристики для визначання класу атаки. Загальна схема виявлення мережевих атак представлена на рис. 2.1.

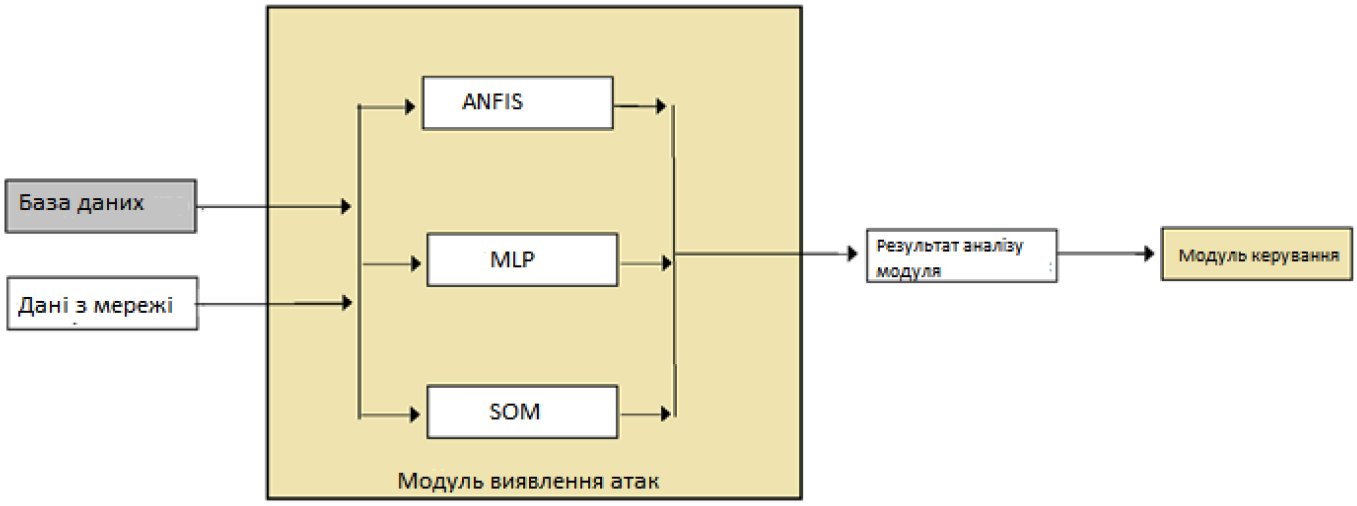


Рисунок 2.1 - Загальна схема виявлення мережевих атак

2.2 Висновки

Нейромережі мають властивість навчатися – це дає перевагу перед іншими методами, оскільки нейромережева технологія дозволяє визначити не тільки існуючи атаки, а й нові. До того ж нейромережеві технології працюють швидко та ефективно у визначенні атаки на комп’ютерну мережу тому обрано цей метод. За допомогою багатошарового персептрону, мережі Кохонена та нейронечіткої мережі пропонується визначити категорії атак та порівняти отримані результати, оскільки результати можуть різнитися. У якості початкових даних використовується набір даних NSL-KDD.

3 СТВОРЕННЯ НЕЙРОННИХ МЕРЕЖ ЩОДО ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

3.1 Багатошаровий персептрон

3.1.1 Структура нейронної мережі

Багатошаровий персептрон – це клас штучних нейронних мереж прямого поширення з навчанням з вчителем, що складається з наступних шарів: вхідний, прихований, результуючий. У цій нейромережі використовуєтья алгоритм зворотного поширення помилки, у якості активаційної функції використовується сигмоїдальна.

З нейронів складається мережа, безпосередньо з якою далі проводиться уся робота.

За формулою 3.1 визначається число нейронів прихованого шару.

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

де L_w – кількість синаптичних ваг; n – розмірність вхідного сигналу; m – розмірність вихідного сигналу; N – число елементів навчальної вибірки [13].

$66 \le L_w \le 4940$. Якщо L_w взяти 1500, то кількість нейронів у прихованому шарі складає 30. За допомогою пакету Neural Network Toolbox задаємо параметри для багатошарового персептрону. Структура багатошарового персептрону, який використовується у дипломній роботі, представлена на рис. 3.1, де X1..X41 – вхідні дані:

X1 – duration - Тривалість (у секундах) з’єднання

X2 – protocol_type – тип протоколу транспортного рівня

X3 – service – сервис прикладного рівня

X4 – flag – статус з'єднання

X5 - src_bytes - кількість байтів від джерела до призначення

X6 – dst_bytes - кількість байтів відповіді клієнту

X7 – land - 1, якщо з'єднання від/до того самого хоста/порта

X8 - wrong_fragment - кількість “хибних” фрагментів

X9 - urgent - кількість термінових пакетів

X10 - hot - кількість “гарячих” індикаторів

X11 - num_failed_logins - кількість невдалих спроб реєстрації

X12 - logged_in - 1, якщо успішний вхід в систему; 0 неуспішне

X13 - num_compromised - кількість “компроментуючих” умов

X14 - root_shell - 1, якщо root shell отриманий; інакше 0

X15 - su_attempted - 1, якщо виконувалась”su root” ; інакше 0

X16 - num_root - кількість “root” доступів

X17 - num_file_creations - кількість операцій створення файлів

X18 - num_shells - кількість запитів на надання оболонки

X19 - num_access_files - кількість операцій на доступ до контролю файлів

X20 – num_outbound_cmds - кількість вихідних команд для FTP сесії

X21 - is_hot_login - 1, якщо логін належав до “гарячого” списку

X22 - is_guest_login - 1, якщо “гостьовий” вхід

X23 - count - кількість з'єднань на хост в поточній сесії за останні 2 с.

X24 – srv_count - кількість з'єднань на такий самий сервіс за останні 2 с.

X25 – serror_rate – відсоток з’єднань з хостом з count з SYN-помилками

X26 – srv_serror_rate – відсоток з’єднань з SYN-помилками при з'єднанні по службі з srv_count

X27 – rerror_rate - відсоток з’єднань з REJ-поммилками

X28 – srv_rerror_rate - відсоток з’єднань з REJ-поммилками

X29 – same_srv_rate – відсоток з’єднань з однаковим сервісом

X30 – diff_srv_rate – відсоток з’єднань з різними сервісами

X31 – srv_diff_host_rate – відсоток з’єднань з різними хостами

X32 – dst_host_count - кількість з`єднань до локального хоста, встановлених віддаленою стороною

X33 – dst_host_srv_count - кількість з`єднань до локального хоста,

X34 – dst_host_same_srv_rate – відсоток з’єднань з однаковим сервісом

X35 – dst_host_diff_srv_rate – відсоток з’єднань з різними службами за час з’єднань по ip з dst_host_srv_count

X36 – dst_host_same_src_port_rate - відсоток з’єднань до того ж самого хосту-приймачу за час з’єднань з dst_host_srv_count

X37 – dst_host_srv_diff_host_rate

X38 – dst_host_serror_rate – відсоток з’єднань з хостом з dst_host_count з SYN-помилками

X39 – dst_host_srv_serror_rate – відсоток з’єданань з SYN-помилкою

X40 – dst_host_rerror_rate – відсоток з’єданань з REJ-помилкою

X41 – dst_host_srv_rerror_rate - відсоток з’єданань з REJ-помилкою,

F1…F30 – нейрони прихованого шару, Y1..Y5 –результуючі дані:

Y1 – normal – атаки не було (1 0 0 0 0)

Y2 – dos – була DOS атака (0 1 0 0 0)

Y3 – u2r – була U2R атака (0 0 1 0 0)

Y4 – r2l – була R2L атака (0 0 0 1 0)

Y5 – probe – була PROBE атака (0 0 0 0 1)

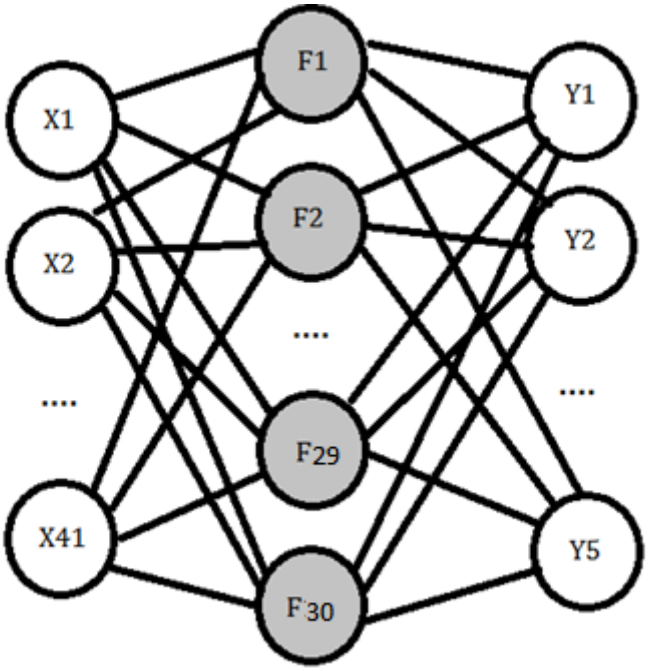
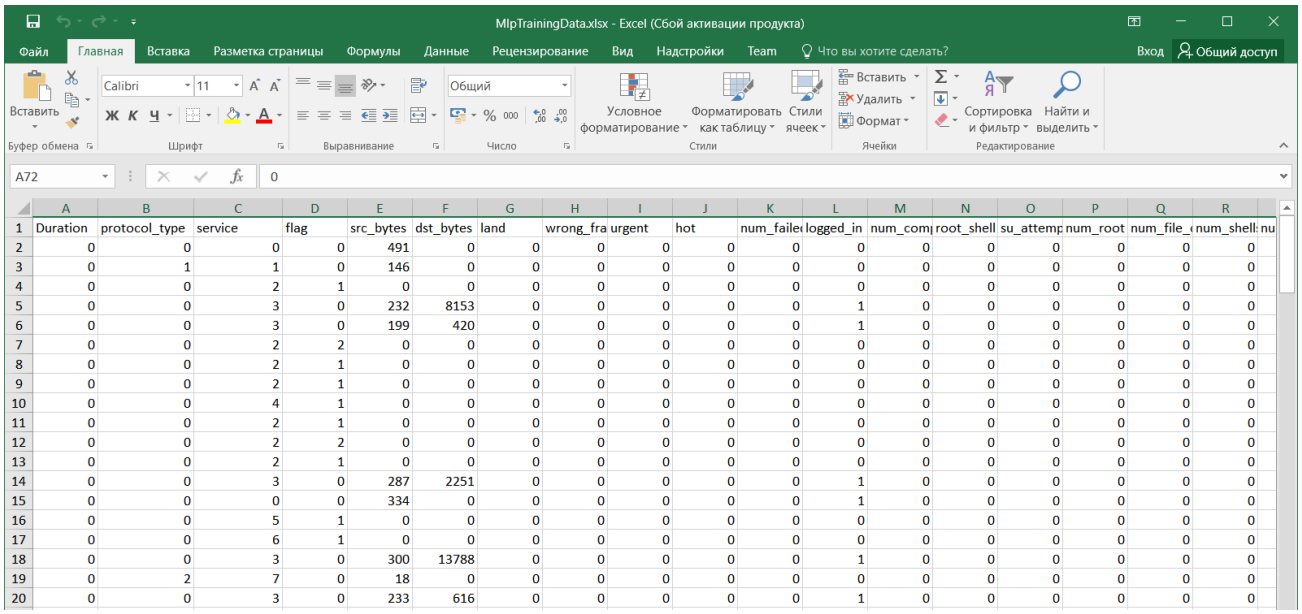


Рисунок 3.1 – Структура багатошарового персептрону

3.1.2 Формування вибірки

Початкові навчальні вектори сформовано у вигляді таблиці у форматі csv. Вибір даного формату обумовлено технічними особливостями роботи нейропакетів у MatLAB. У файлі з вибіркою знаходяться відомості за 41 параметром-входом та 5 параметрами-виходами. Усі текстові параметри переведено у числову інформацію, ставлячи параметру у відповідність число. Усього вибірка містить у собі 10000 навчальних векторів. Для валідації взято 20 % векторів та тестування взято 10 % векторів. Фрагмент навчальної вибірки для нейромереж наведено на рис. 3.2. Повна



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fra	urgent	hot	num_faile	logged_in	num_com	root_shell	su_attemp	num_root	num_file_(	num_shell
2	0	0	0	0	491	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	1	1	0	146	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	3	0	232	8153	0	0	0	0	0	1	0	0	0	0	0	0
6	0	0	3	0	199	420	0	0	0	0	0	1	0	0	0	0	0	0
7	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	3	0	287	2251	0	0	0	0	0	1	0	0	0	0	0	0
15	0	0	0	0	334	0	0	0	0	0	0	1	0	0	0	0	0	0
16	0	0	5	1	0	0	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	0	0
18	0	0	3	0	300	13788	0	0	0	0	0	1	0	0	0	0	0	0
19	0	2	7	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	3	0	233	616	0	0	0	0	0	1	0	0	0	0	0	0

вибірка наведена у додатку А.

Рисунок 3.2 – Фрагмент змісту файлу з навчальною вибіркою для нейромережі

3.1.3 Побудова багатошарового персептрону у пакеті Neural Network Toolbox

Для побудови багатошарового персептрону визначена конфігурація 41-1-30-5. Сигмоїдальну сходинкову функцію використано як активаційну функцію прихованого шару(рис. 3.3(а)).

$$OUT_{jl} = \frac{1}{1 + e^{-NET_{jl}}}. \qquad (3.2)$$

Лінійну функцію використано як активаційну функцію вихідного шару (рис. 3.3(б)). Вихідний вектор значень задається у вигляді $Y=\{y_i\}$, де $y_i = OUT_i$, $i=\overline{1,m}$.

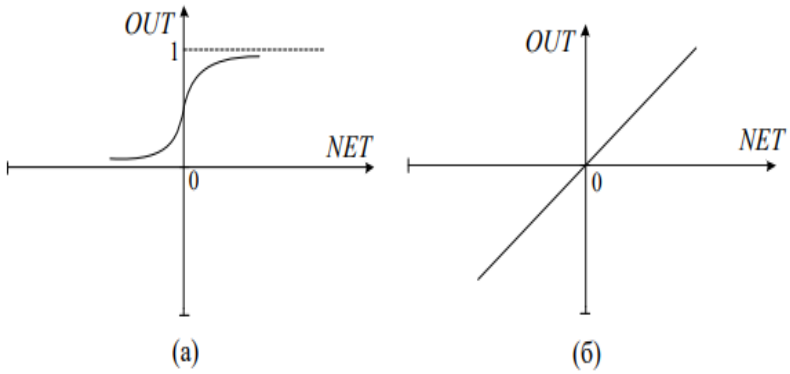


Рисунок 3.3 – Графіки функцій активації: (а) сигмоїдальної; (б) лінійної

За допомогою пакету Neural Network Toolbox задаємо параметри для багатошарового персептрону. Розподіляємо вибірка наступним чином: 70% - навчання, 20% - валідація, 10% - тестування (рис. 3.4).

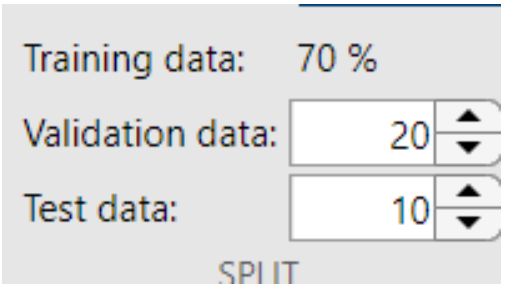


Рисунок 3.4 – Розподілення вибірки для створення багатошарового персептрону

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

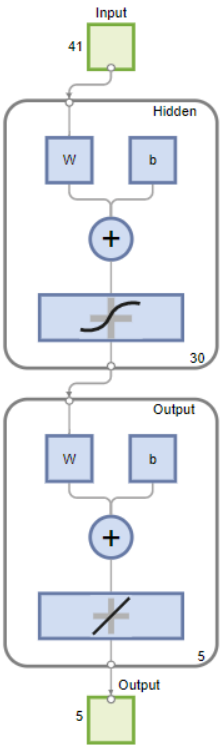


Рисунок 3.5 – Модель створеної нейромережі

Далі тренуємо створену нейромережу. Обираємо алгоритм навчання Levenberg-Marquardt та переходимо до вікна тренування багатошарового персептрону (рис. 3.6).

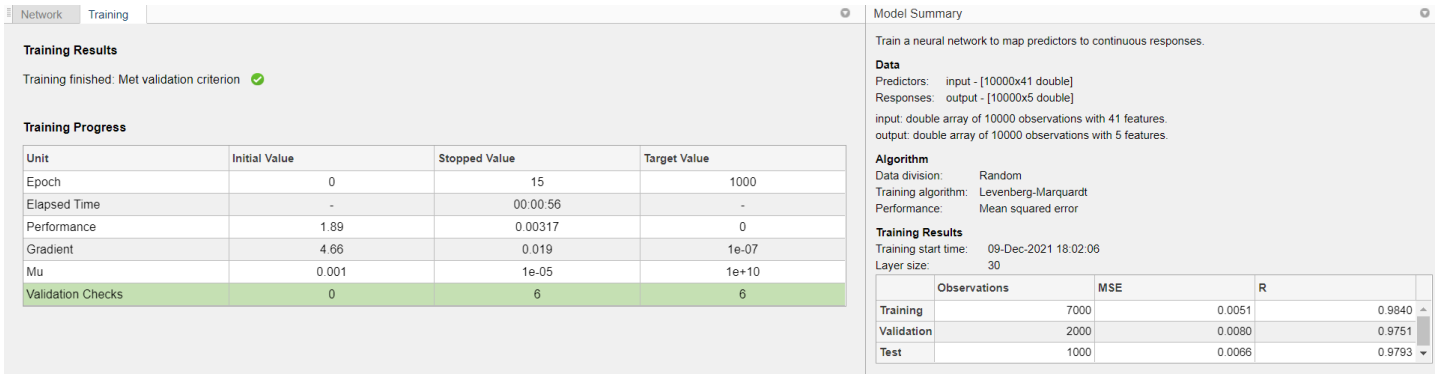


Рисунок 3.6 – Навчання НМ за алгоритмом Levenberg-Marquardt

Після тренування отримуємо графіки Performance (рис. 3.7), Training State (рис. 3.8), Error Histogram (рис. 3.9), Regression (рис. 3.10).

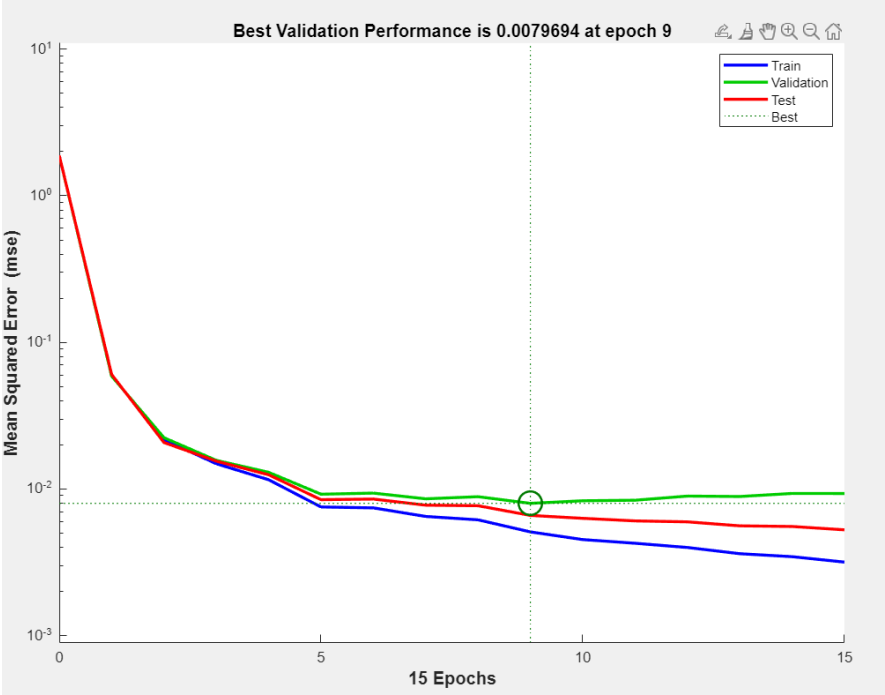


Рисунок 3.7 - Графік Performance

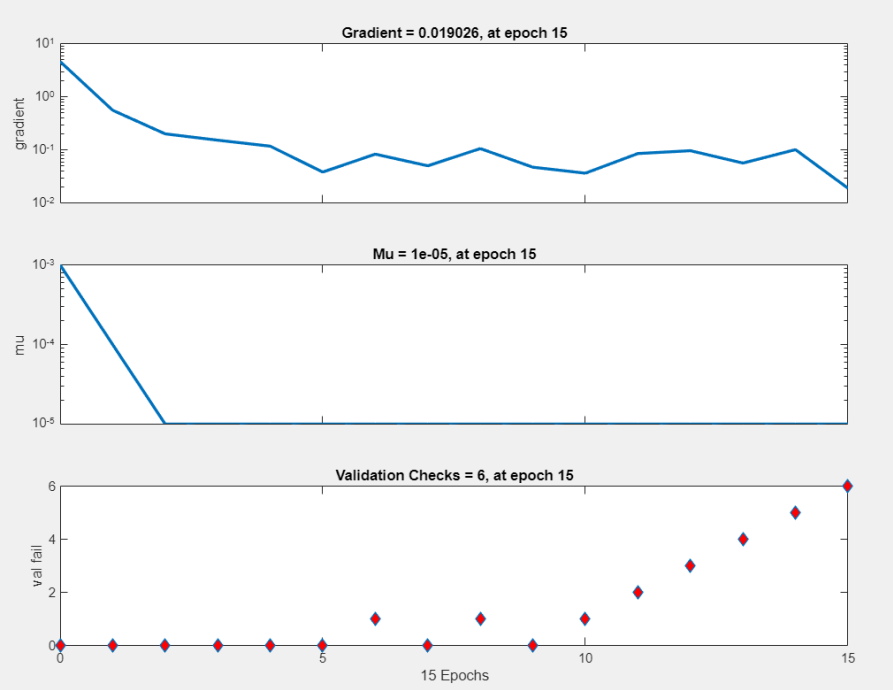


Рисунок 3.8 – Графік Training State

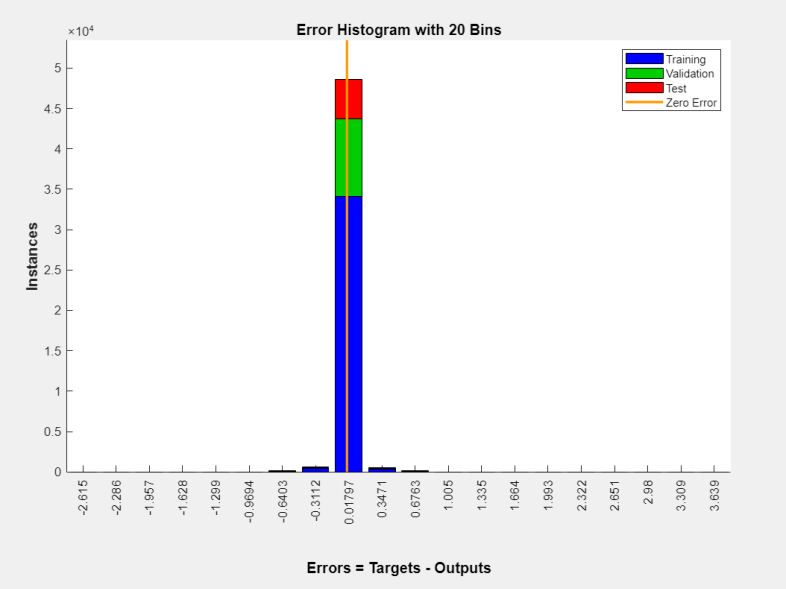


Рисунок 3.9 – Графік Error Histogram

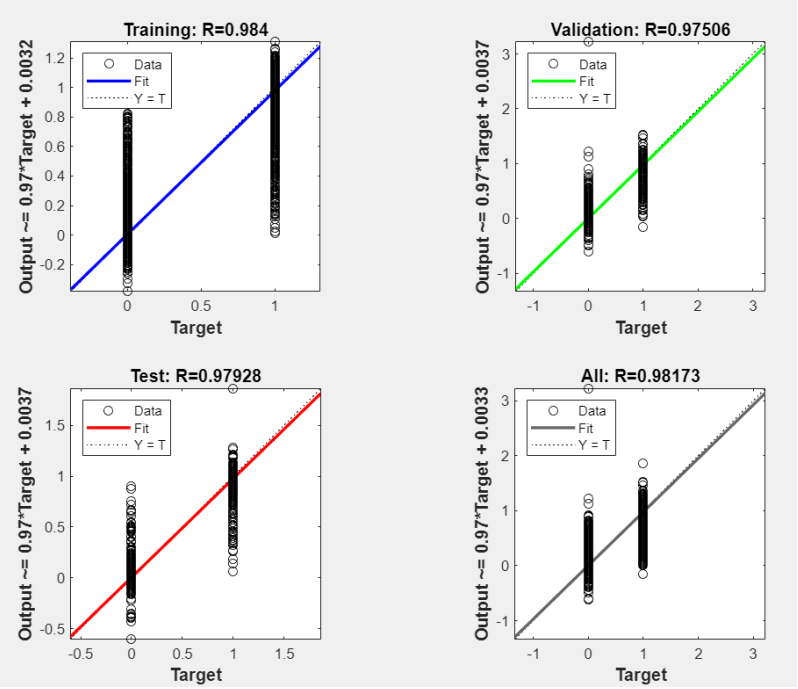


Рисунок 3.10 – Графік Regression

Отримана нейронна мережа має конфігурацію: кількість вхідних нейронів – 41, кількість прихованих шарів – 1, кількість нейронів у прихованому шарі – 30, кількість вихідних нейронів – 5. Функція прихованого шару – сигмоїдна сходинкова, функція активації вихідного шару – сигмоїдна симетрична. Навчання нейронної мережі проводилося за алгоритмом Левенберга-Марквардта протягом 15 епох, затрачений час на моделювання НМ складає 56 с, MSE для тренувальної, контрольної та тестової вибірок дорівнює 0.0051, 0.0080, 0.0066 відповідно. Код програми представлений у додатку Б.

3.1.4 Визначення оптимальних параметрів MLP

Перше дослідження проведено для визначення розмірності вибірки

Цей параметр суттево впливає на результати навчання нейромережі, а також на її подальшу роботу. Для визначення найоптимальнійшої вибірки взято характеристику MSE. Результати наведено у табл. 3.1 та на рис. 3.11, скріншоти дослідження у додатку В.

Таблиця 3.1 – Результати дослідження оптимального розміру вибірки

Кількість еталонів	MSE		
	Навчання	Валідація	Тестування
500	0,0002	0,0196	0,0222
5000	0,0028	0,0076	0,0054
10000	0,0051	0,0080	0,0066
15000	0,0061	0,0089	0,0071

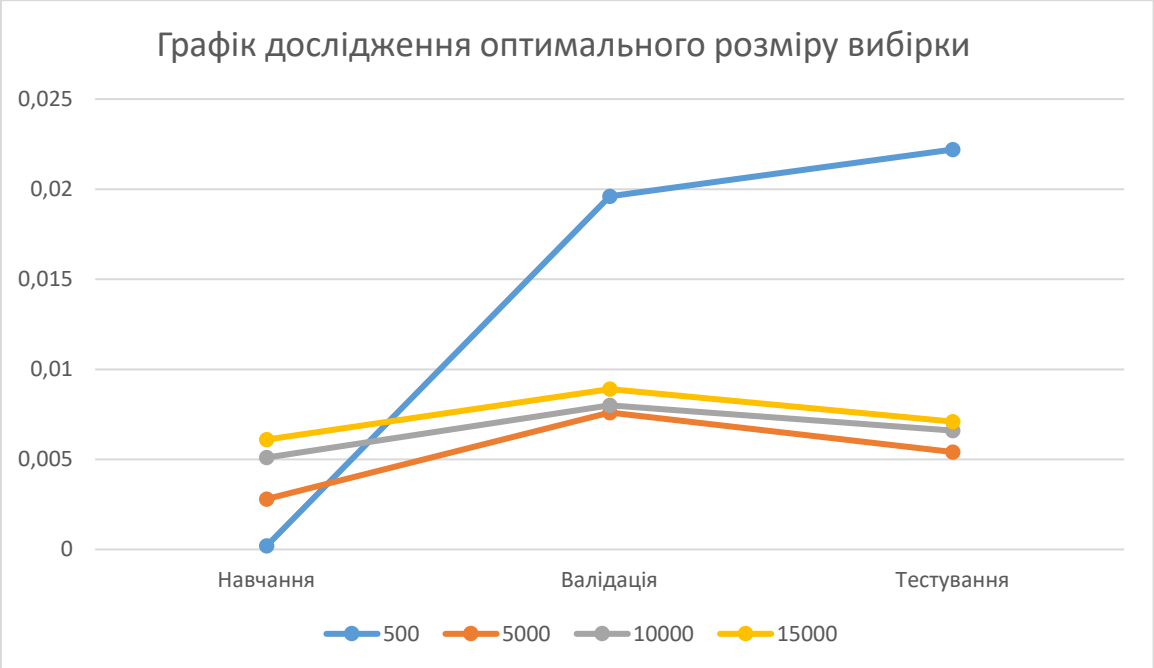


Рисунок 3.11 – Графік дослідження оптимального розміру вибірки

Виходячи з отриманих результатів обрано вибірку розміром 10000 векторів, оскільки після цього параметри MSE майже не змінюються.

Друге дослідження проведено для визначення алгоритму навчання. Критерієм для визначення оптимального алоритму є MSE та кількість епох. Дослідження проволиться на вибірці у 10000 векторів. Результати наведено у табл. 3.2, скріншоти представлено у додатку В та на рис. 3.12, коди програм у додатку Б.

Таблиця 3.2 - Результати дослідження оптимального алгоритму навчання

Алгоритм навчання	Кількість епох	MSE		
		Навчання	Валідація	Тестування
Levenberg-Marquardt	15	0,0051	0,0080	0,0066
Bayesian Regularization	1000	0,0005	-	0,0043
Scaled conjugate gradient	248	0,0071	0,0071	0,0066

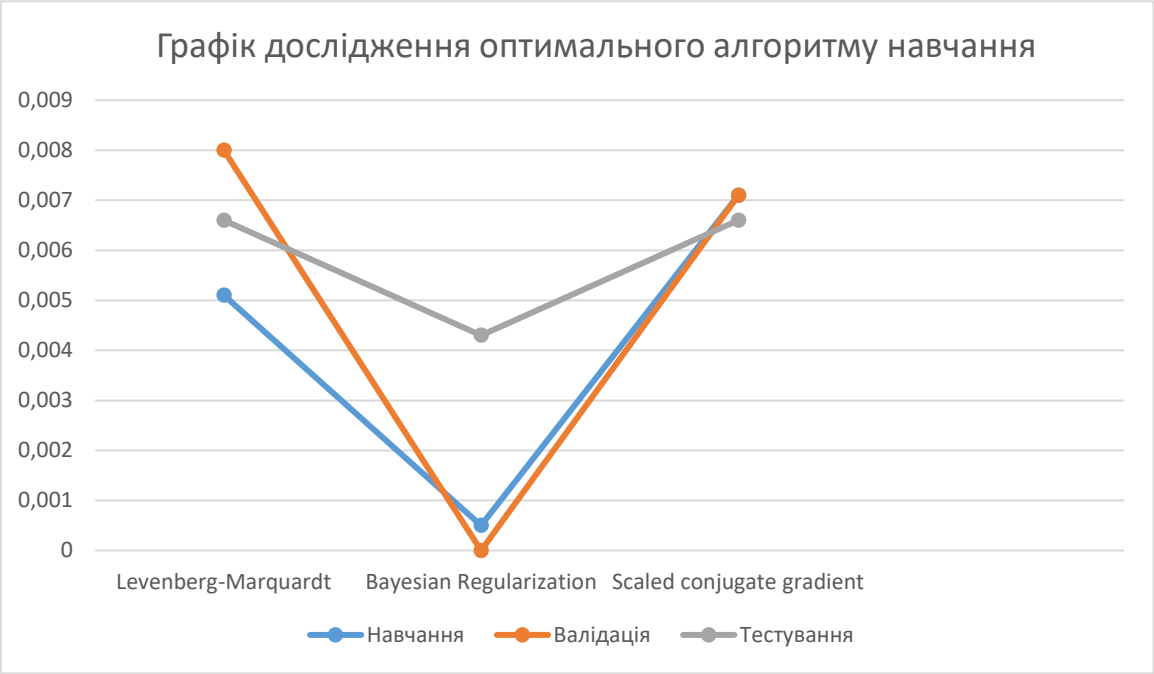


Рисунок 3.12 – Графік дослідження оптимального розміру вибірки

Як бачимо найменша кількість епох за алгоритмом Levenberg-Marquardt. У алгоритмі Bayesian Regularization дуже велика кількість епох та немеє етапу валідації. У алгоритмі Scaled conjugate gradient параметр MSE має майже таке саме значення як і при алгоритмі Levenberg-Marquardt, але більша кількість епох, ніж при алгоритмі Levenberg-Marquardt (248 у порівнянні з 15). Тому перевагу віддано алгоритму Levenberg-Marquardt.

3.2 Нейронечітка мережа

3.2.1 Структура нейронечіткої мережі

Адаптивна нейронечітка мережа – це система з області штучного інтелекту, які поєднують методи штучний нейронних мереж та систем на нечіткій лозіці виводу

Такаги-Сугено. У такій системі вивід відповідає набору нечітких правил «якщо-то». Дані правила мають здібність до навчання апроксимування нелінійних функцій. Рекомендується для більш ефективної роботи використовувати параметри, отримані за допомогою генетичного алгоритму.

Нейронечітка мережа є багатошаровою нейромережею спеціальної структури без зворотних зв'язків, в якій використовується не нечіткі сигнали, ваги та функції активації. Значення входів, ваг та виходів є дійсним числами з проміжку [0,1]. Операція підсумовування виконується за допомогою фіксованої Т-Норми, Т-Конорми або іншої безперервної операції. [13]

Структура системи адаптивної нейронечіткої мережі, яка використовується у дипломному проекті представлена на рис. 3.13,

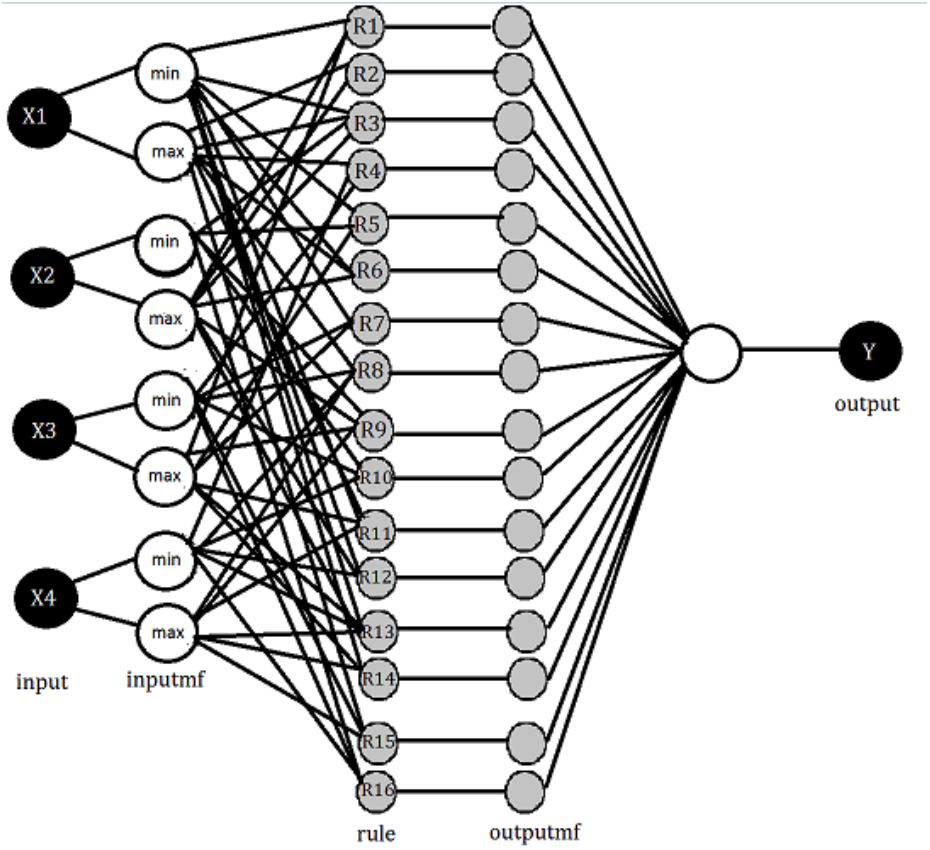


Рисунок 3.13 – Структура нейронечіткої мережі

де input (4 вузли) – вхідні дані: X_1 - count - кількість з'єднань на хост в поточній сесії за останні 2 с., X_2 – serror_rate – відсоток з'єднань з хостом з count з SYN-помилками, X_3 – diff_srv_rate – відсоток з'єднань з різними сервісами, X_4 –

dst_host_diff_srv_rate – відсоток з'єднань з різними службами за час з'єднань по ip з dst_host_srv_count, inputmf (4*2 = 8 вузлів) – визначає мінімальне та максимальне значення вузла, rule (8*2 = 16 вузлів) – R1..R16 - правила:

1) якщо X1 = мінімальне значення I X2 = мінімальне значення I X3 = мінімальне значення I X4 = мінімальне значення, тоді імовірність низького ступеню;
2) якщо X1 = максимальне значення I X2 = мінімальне значення I X3 = мінімальне значення I X4 = мінімальне значення, тоді імовірність низького ступеню;
3) якщо X1 = мінімальне значення I X2 = максимальне значення I X3 = мінімальне значення I X4 = мінімальне значення, тоді імовірність низького ступеню;
4) якщо X1 = мінімальне значення I X2 = мінімальне значення I X3 = максимальне значення I X4 = мінімальне значення, тоді імовірність низького ступеню;
5) якщо X1 = мінімальне значення I X2 = мінімальне значення I X3 = мінімальне значення I X4 = максимальне значення, тоді імовірність низького ступеню;
6) якщо X1 = мінімальне значення I X2 = мінімальне значення I X3 = максимальне значення I X4 = максимальне значення, тоді імовірність середнього ступеню;
7) якщо X1 = максимального значення I X2 = максимального значення I X3 = мінімальне значення I X4 = мінімальне значення, тоді імовірність середнього ступеню;
8) якщо X1 = максимального значення I X2 = мінімальне значення I X3 = мінімальне значення I X4 = максимального значення, тоді імовірність середнього ступеню;
9) якщо X1 = мінімальне значення I X2 = максимального значення I X3 = максимального значення I X4 = мінімальне значення, тоді імовірність середнього ступеню;

10) якщо X1 = мінімальне значення І X2 = максимального значення І X3 = мінімальне значення І X4 = максимального значення, тоді імовірність середнього ступеню;
11) якщо X1 = максимального значення І X2 = мінімальне значення І X3 = максимального значення І X4 = мінімальне значення, тоді імовірність середнього ступеню;
12) якщо X1 = максимального значення І X2 = максимального значення І X3 = максимального значення І X4 = максимального значення, тоді імовірність високого ступеню;
13) якщо X1 = максимального значення І X2 = максимального значення І X3 = максимального значення І X4 = мінімальне значення, тоді імовірність високого ступеню;
14) якщо X1 = максимального значення І X2 = максимального значення І X3 = мінімальне значення І X4 = максимального значення, тоді імовірність високого ступеню;
15) якщо X1 = максимального значення І X2 = мінімальне значення І X3 = максимального значення І X4 = максимального значення, тоді імовірність високого ступеню;
16) якщо X1 = мінімальне значення І X2 = максимального значення І X3 = максимального значення І X4 = максимального значення, тоді імовірність високого ступеню,

outputmf (16 вузлів) – функція приналежності для кожного правила нечіткого виводу, output (1 вузол) – вихідний шар: Y-який ступень імовірності, що атака відбулася

3.2.2 Формування вибірки

Вибірка для нейронечіткої мережі підготовлена наступним чином: кожен з чотирьох параметрів може прийняти значення min або max. Завдяки цим параметрам визначається з якою імовірністю відбулася атака. Фрагмент змісту навчальної вибірки представлено на рис. 3.14. Усього 15000 навчальних векторів. Повна вибірка наведена у додатку А.

```
135;1.00;0.06;0.07;1
24;1.00;0.08;0.04;1
148;0.00;0.00;0.00;0
2;0.00;0.00;0.02;0
206;0.00;0.06;0.08;1
175;0.10;1.00;0.84;1
4;0.00;0.00;0.00;0
63;0.00;0.08;0.07;1
1;0.00;0.00;0.04;0
1;0.00;0.00;0.58;1
52;1.00;0.08;0.02;1
125;0.00;0.06;0.07;1
168;1.00;0.06;0.06;1
1;0.00;0.00;0.00;0
145;1.00;0.06;0.05;1
3;0.00;0.67;0.01;0
```

Рисунок 3.14 – Фрагмент файлу з навчальною вибіркою для нейронечіткої мережі

Далі цей файл збережено у форматі .dat для завантаження у MatLAB.

Тестова вибірка підготовлена за таким самим принципом. Фрагмент змісту файлу з тестовою вибіркою наведено на рис. 3.15. Для тестування обрано 1000

```
2;0.00;0.00;0.03;0
13;0.00;0.15;0.60;0
123;1.00;0.07;0.05;1
5;0.20;0.00;0.00;0
30;0.00;0.00;0.00;0
121;0.00;0.06;0.07;1
166;1.00;0.06;0.05;1
117;1.00;0.06;0.07;1
270;1.00;0.05;0.05;1
133;1.00;0.06;0.06;1
205;0.00;0.06;0.07;1
199;1.00;0.06;0.07;1
```

векторів.

Рисунок 3.15 – Фрагмент файлу з тестовою вибіркою для нейронечіткої мережі

3.2.3 Побудова нейронечіткої мережі у пакеті Fuzzy Logic Toolbox

За допомогою пакета Fuzzy Logic Toolbox будуємо нейронечітку мережу. Задаємо властивості кожній вхідній змінній (табл. 3.2). Приклад заданих параметрів на рис. 3.16.

Таблиця 3.2- Властивості змінних нейронечіткої мережі

Властивість	X1	X2	X3	X4	Y
Тип	вхідна ()				результуюча
Діапазон	[1 511]	[0 1]			[0 2]
Ім`я функцій приналежності	min, max				min, medium, max
Тип	gaussmf				constant

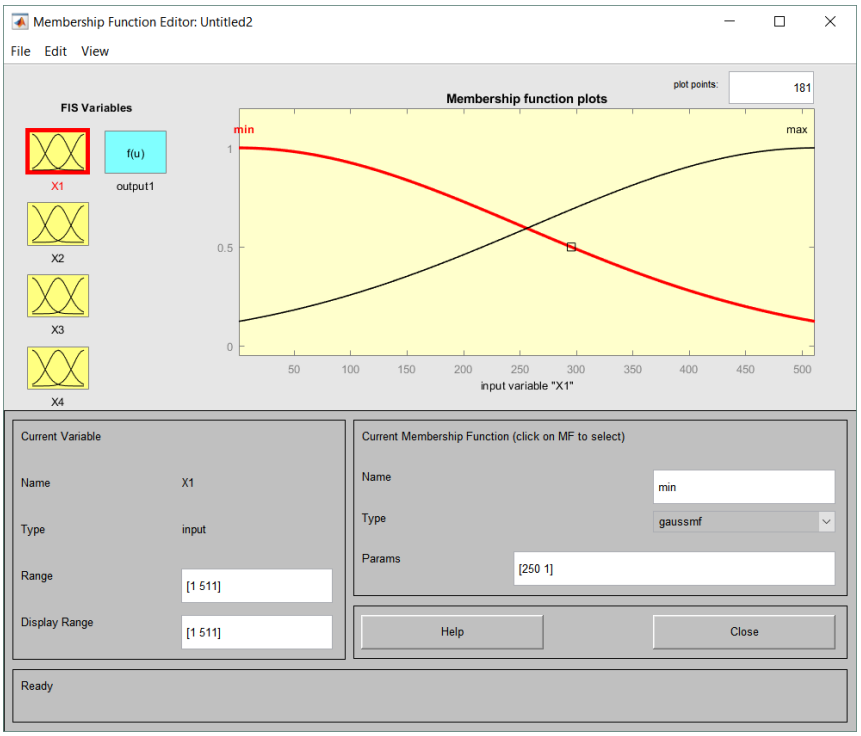


Рисунок 3.16 – Приклад властивостей змінної X1

Наступним кроком переходимо до обрання параметрів решітки. Задаємо конфігурацію вхідних термів 2 2 2 2, тип gaussmf та для вихідної змінної вказуємо тип constant. Далі навчаємо мережу. Завантажуємо підготовлену вибірку, обираємо параметри для тренування: метод hybrid, кількість епох 40. Отримуємо наступний графік (рис. 3.17). Можемо бачити, що з кожною ітерацією кількість помилок зменшується та направляється до 0. Отримана помилка = 0.47238.

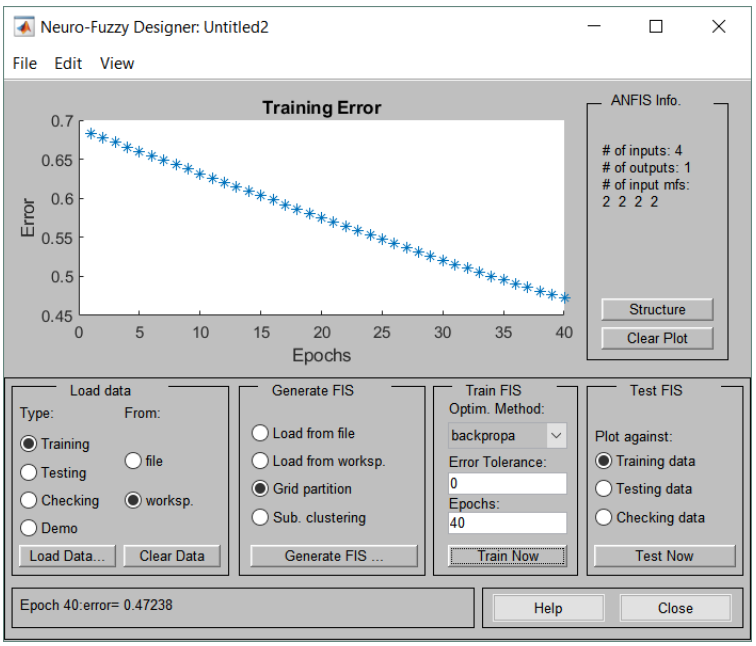


Рисунок 3.17 – Графік залежності помилок навчання від кількості циклів навчання

Згенеровану структуру мережі показано на рис. 3.18.

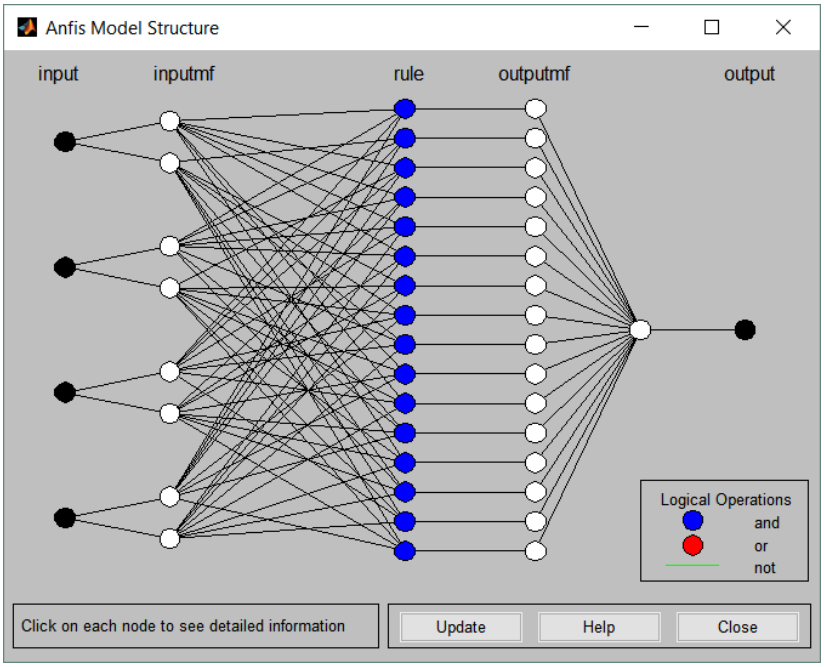


Рисунок 3.18 – Структура згенерованої мережі

Як бачимо програмно отримали таку саму структуру, як і планували у розділі вище. Наступний етап – це тестування мережі. Завантажуємо вибірку у інтерфейсі та запускаємо тестування. Графік, який отримали у результаті тестування, приведено на рис. 3.19. Середня помилка під час тестування = 0.29856.

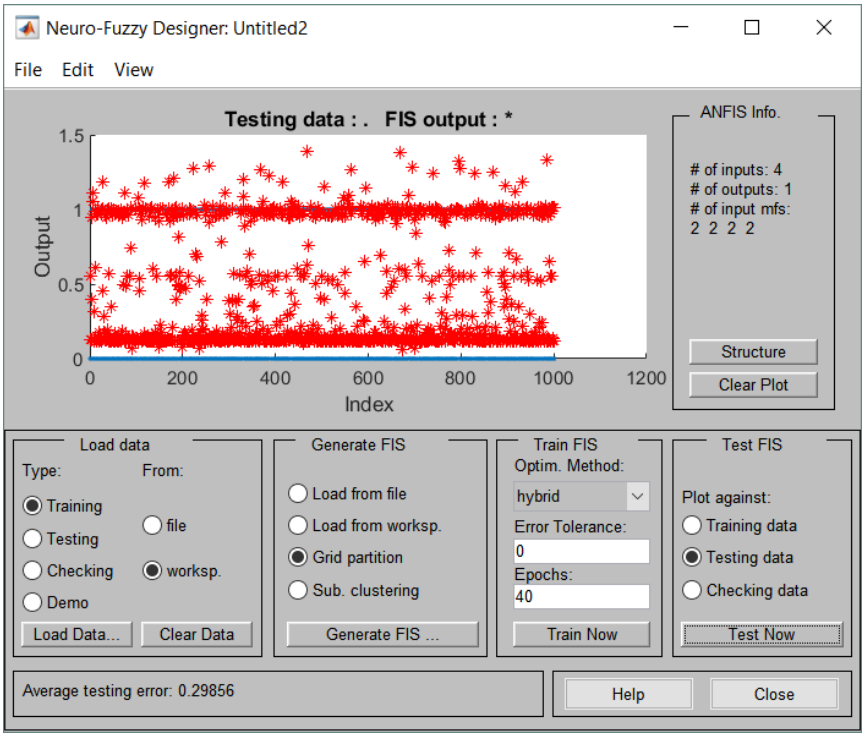


Рисунок 3.19 – Графік результатів тестування

Перевірка на адекватність проводилася шляхом введення коду у командну область. Результати наведено у таблиці 3.3. Приклад виконання перевірки на рис.3.20.

Таблиця 3.3 – Результати перевірки на адекватність

Дані на вході	Очікуваний результат	Фактичний результат
[2 0 0 0.03]	0	0,1410
[233 1 0.06 0.07]	1	1,0004
[280 1 0.05 0.06]	1	1,0108
[8 0 0 0]	0	0,1225
[2 0 1 0.31]	1	0,5324
[22 0 0 0]	0	0.1286
[228 1 0.07 0.07]	1	1.0042
[120 0 0 0.01]	0	0.2069
[73 0 0 0.02]	0	0.1725
[135 1 0.06 0.07]	1	0.9703
[24 1 0.08 0.04]	1	0.9478
[206 0 0.06 0.08]	1	0.8414
[3 0 0.67 0.54]	0	0.5894
[300 1 0.06 0.07]	1	1.0243

```
>> fis = readfis('F:\Diplom\NNL_Train.fis')%

fis =

  sugfis with properties:

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

    See 'getTunableSettings' method for parameter optimization.

>> 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 18)
In evalfis (line 98)

y =

   -0.7747
```

Рисунок 3.20 – Перевірка на адекватність нейронечіткої мережі

3.2.4 Визначення оптимальних параметрів ANFIS

Перше дослідження проведено для визначення оптимального розміру вибірки. Підготовлено вибірки розміром 500, 5000, 10000, 15000 векторів. Параметр за яким вибираємо оптимальний розмір – error. Навчання проводиться при 40 епохах та методі backpropa. Результати наведено у таблиці 3.3 та на рис. 3.21, скріншоти у додатку В.

Таблиця 3.3 – Результати навчання на різних розмірах вибірки

Кількість еталонів	error	
	Навчання	Тестування
500	0,47371	0,46165
5000	0,4741	0,46072
10000	0,47393	0,46956
15000	0,47238	0.4601

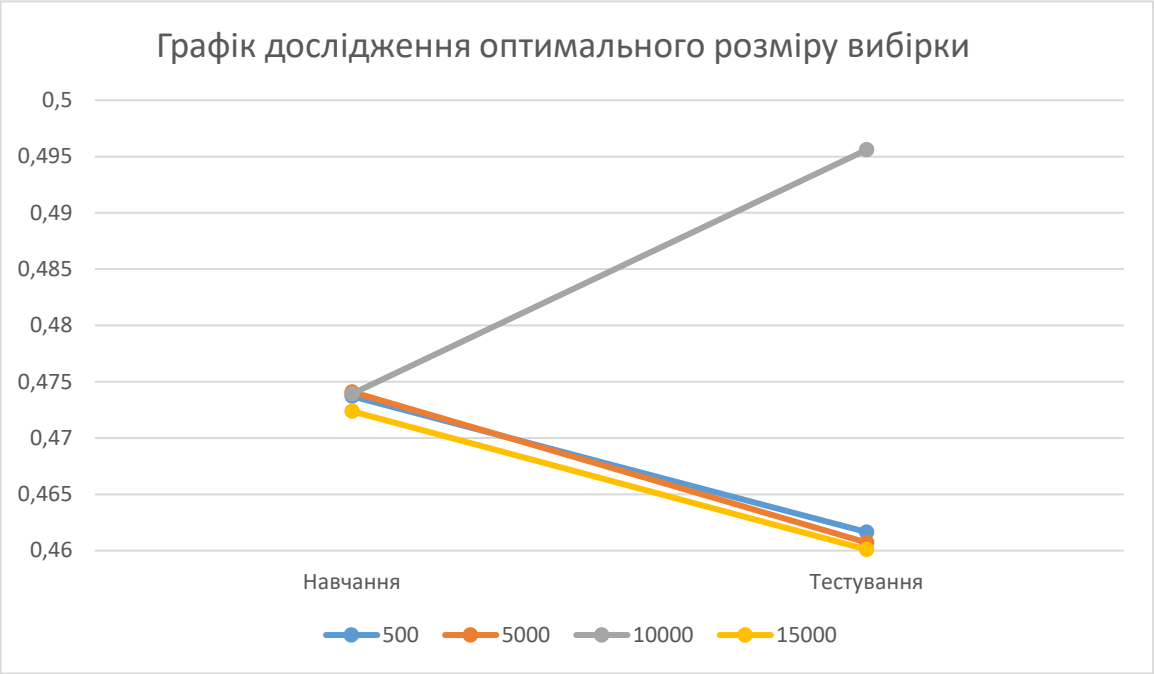


Рисунок 3.21 - Графік дослідження оптимального розміру вибірки

Як можемо бачити при навчанні помилка найменша для вибірки з 15000 еталонів. При тестуванні на вибірці з 1000 векторів найкращий результат показала вибірка з 15000 векторів. Отже обрано найбільшу вибірку як найоптимальнішу.

Друге дослідження проведено для визначення оптимального методу навчання. Першим обрано метод backpropa. Помилка при навчанні склала 0,47238 та 0.4601 при тестуванні. При методі hybrid помилка при навчанні = 0,30778 та при тестуванні = 0,29856. Результати наведено у додатку В. За результатами цього дослідження обрано метод hybrid.

3.3 Мережа Кохонена

3.3.1 Структура мережі Кохонена

Мережа Кохонена – нейронна мережа з навчанням без вчителя (використовується конкурентне навчання), яка конструює багатовимірний простір та створює дискретне представлення вхідних просторів навчальних вибірок. Простір карти складається з нейронів та вагових векторів.

Структура мережі Кохонена, яка використовується у дипломній роботі, представлена на рис.3.22, де X1..X41 – вхідні дані, які представлені у п. 3.1,

Y1..Y5 – результуючі нейрони:

Y1 – normal – атаки не було (0)

Y2 – dos – була DOS атака (1)

Y3 – n2l – була N2L атака (2)

Y4 – r2l – була R2L атака (3)

Y5 – probe – була PROBE атака (4)

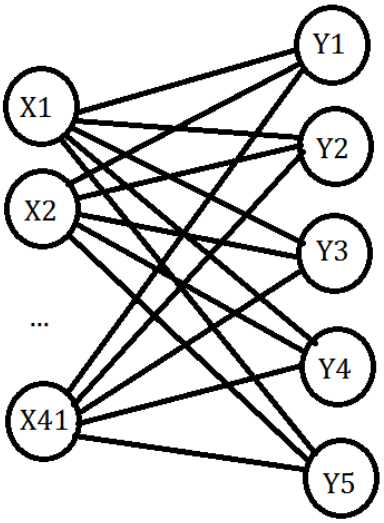
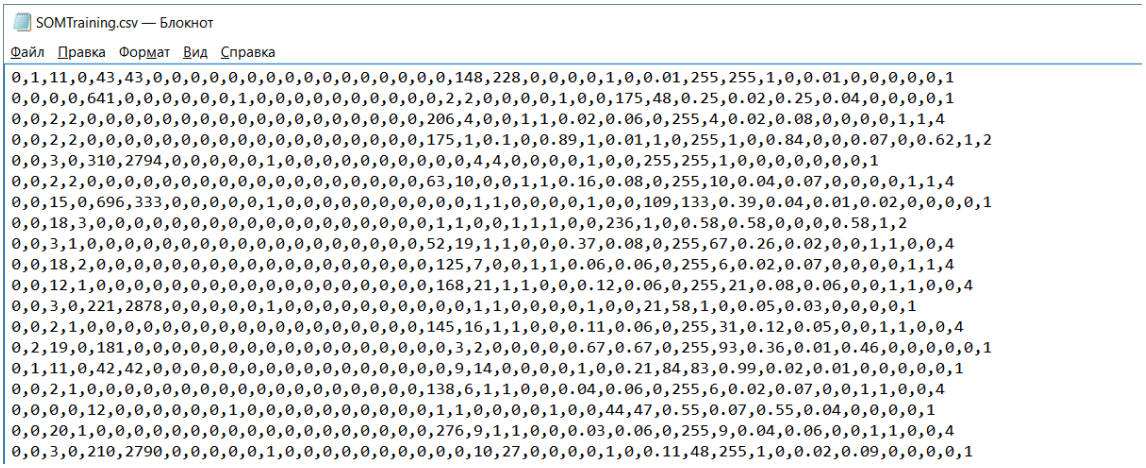


Рисунок 3.22 – Структура мережі Кохонена

3.3.2 Формування вибірки

Початкові навчальні вектори сформовано у вигляді таблиці у форматі csv. Вибір даного формату обумовлено технічними особливостями роботи бібліотеки мови Python. У файлі з вибіркою знаходяться відомості за 41 параметром-входом та 5 параметрами-виходами. Усі текстові параметри переведено у числову інформацію, ставлячи параметру у відповідність число. Усього вибірка містить у собі 15000 навчальних векторів. Фрагмент навчальної вибірки наведено на рис. 3.23. Повна вибірка наведена у додатку А.


SOMTraining.csv — Блокнот

Файл Правка Формат Вид Справка

```
0,1,11,0,43,43,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,148,228,0,0,0,0,1,0,0.01,255,255,1,0,0.01,0,0,0,0,0,1
0,0,0,0,641,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,2,2,0,0,0,0,1,0,0,175,48,0.25,0.02,0.25,0.04,0,0,0,0,1
0,0,2,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,206,4,0,0,1,1,0.02,0.06,0,255,4,0.02,0.08,0,0,0,0,1,1,4
0,0,2,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,175,1,0,1,0,0.89,1,0,0.01,1,0,255,1,0,0.84,0,0,0,0.07,0,0.62,1,2
0,0,3,0,310,2794,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,4,4,0,0,0,0,1,0,0,255,255,1,0,0,0,0,0,0,1
0,0,2,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,63,10,0,0,1,1,0.16,0.08,0,255,10,0.04,0.07,0,0,0,0,1,1,4
0,0,15,0,696,333,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,109,133,0.39,0.04,0.01,0.02,0,0,0,0,1
0,0,18,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,1,0,0,236,1,0,0.58,0.58,0,0,0,0.58,1,2
0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,52,19,1,1,0,0,0.37,0.08,0,255,67,0.26,0.02,0,0,1,1,0,0,4
0,0,18,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,125,7,0,0,1,1,0.06,0.06,0,255,6,0.02,0.07,0,0,0,0,1,1,4
0,0,12,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,168,21,1,1,0,0,0.12,0.06,0,255,21,0.08,0.06,0,0,1,1,0,0,4
0,0,3,0,221,2878,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,21,58,1,0,0.05,0.03,0,0,0,0,1
0,0,2,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,145,16,1,1,0,0,0.11,0.06,0,255,31,0.12,0.05,0,0,1,1,0,0,4
0,2,19,0,181,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,2,0,0,0,0,0.67,0.67,0,255,93,0.36,0.01,0.46,0,0,0,0,0,1
0,1,11,0,42,42,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,9,14,0,0,0,0,1,0,0.21,84,83,0.99,0.02,0.01,0,0,0,0,0,1
0,0,2,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,138,6,1,1,0,0,0.04,0.06,0,255,6,0.02,0.07,0,0,1,1,0,0,4
0,0,0,0,12,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,44,47,0.55,0.07,0.55,0.04,0,0,0,0,1
0,0,20,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,276,9,1,1,0,0,0.03,0.06,0,255,9,0.04,0.06,0,0,1,1,0,0,4
0,0,3,0,210,2790,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,10,27,0,0,0,0,1,0,0.11,48,255,1,0,0.02,0.09,0,0,0,0,1
```

Рисунок 3.23 – Фрагмент змісту файлу з навчальною вибіркою для нейромереж

3.3.3 Побудова мережі Кохонена на мові Python

Для побудови мережі Кохонена було обрано мову програмування Python з додатковими бібліотеками. Вхідними даними програми є 41 параметр з бази даних NSL-KDD, які представлено у вигляді двохвимірної карти (50x50). Структура програми наведена на рис. 3.24. Повний код програми у додатку Б.

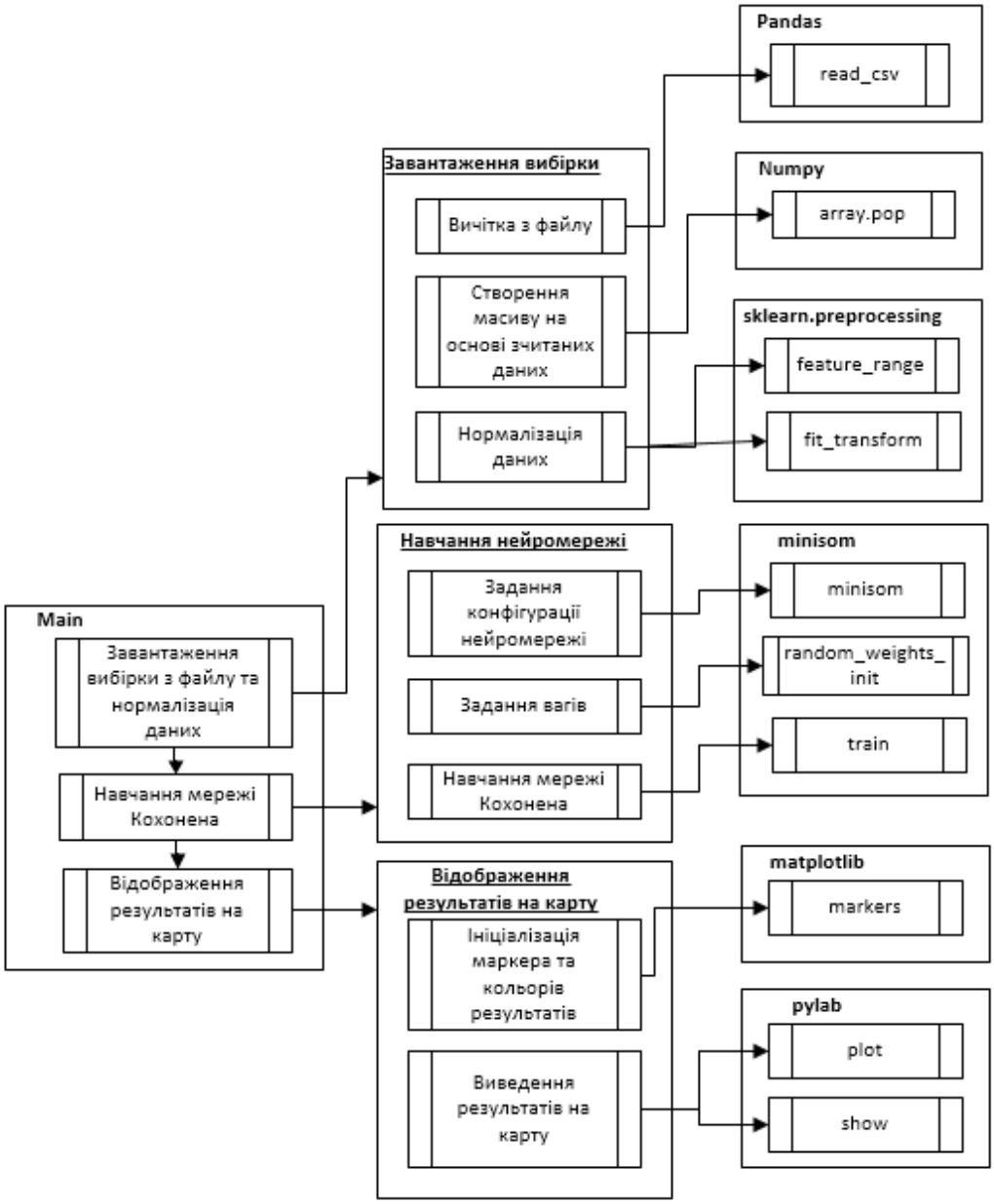


Рисунок 3.24 - Структура програми мережі Кохонена

Перший крок – підключення необхідних бібліотек: MiniSom, Matplotlib та Numpy.

MiniSom – реалізація самоорганізуючих карт на основі Numpy. Завдяки цій бібліотеці можливо швидко та легко проектувати, розробляти та навчати мережу Кохонена [37].

Matplotlib – дана бібліотека обрана для графічного відображення результатів моделювання мережі [38].

Numpy – бібліотека з великою кількістю математичних функцій, які будемо використовувати під час створення мережі Кохонена [39].

Другим кроком є підключення файлів csv з підготовленої вибіркою та збереження цих даних у масив змінних для подальшої роботи.

Третім етапом відбувається нормалізація отриманих даних.

На четвертому кроці відбувається налаштування нейромережі. На цьому етапі задаються розміри карти (50x50), кількість вхідних нейронів (41), сигма (1) та ваги випадковим чином.

Далі – тренування мережі. У функцію завантажується масив даних, отриманий на кроці два, та для отримання гарного результату задається 50 000 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.3.25), червоним коліром показані DOS атаки, зеленим - U2R, синім - R2L, жовтим – Probe. Створення мережі Кохонена зайняло 3 хв. 43 с, помилка склала 0,072.

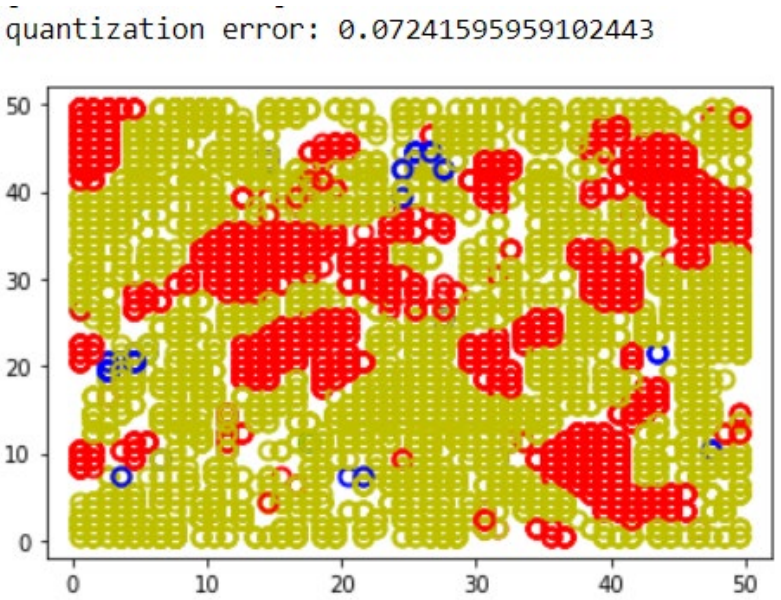
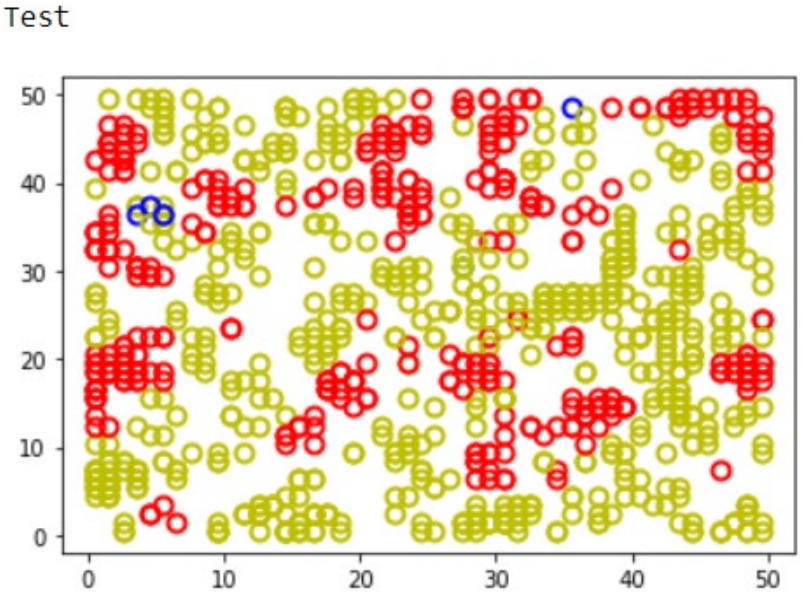


Рисунок 3.25 – Результат роботи програми зі створення мережі Кохонена

Тестування проведено на вибірці з 1000 записів. Результати наведено на рис.



3.26.

Рисунок 3.26 – Результати тестування програми зі створення мережі Кохонена

3.3.4 Визначення оптимальних параметрів мережі Кохонена

Перше дослідження проведено для визначення довжини вибірки для подальшої роботи. Для дослідження обрано вибірки розміром 500, 5000, 10000, 15000 векорів для навчання при 50000 ітерацій та розмір карти – 50x50. Для тестування обрано вибірку у 1000 векторів. Параметри за якими робилась оцінка отриманих результатів це: помилка квантування при навчанні; точність та повнота при навчанні та тестуванні. Результати наведено у таблиці 3.4 та на рис. 3.27. Скріншоти представлено у додатку В.

Таблиця 3.4 – Результати навчання та тестування на різних розмірах вибірки

Кількість еталонів	Навчання			Тестування	
	помилка квантування	точність	повнота	точність	повнота
500	0,001	1	1	0,89	0,85
5000	0,06	0,86	0,98	0,90	0,94
10000	0,07	0,86	0,82	0,85	0,95
15000	0,07	0,88	0,76	0,89	0,95

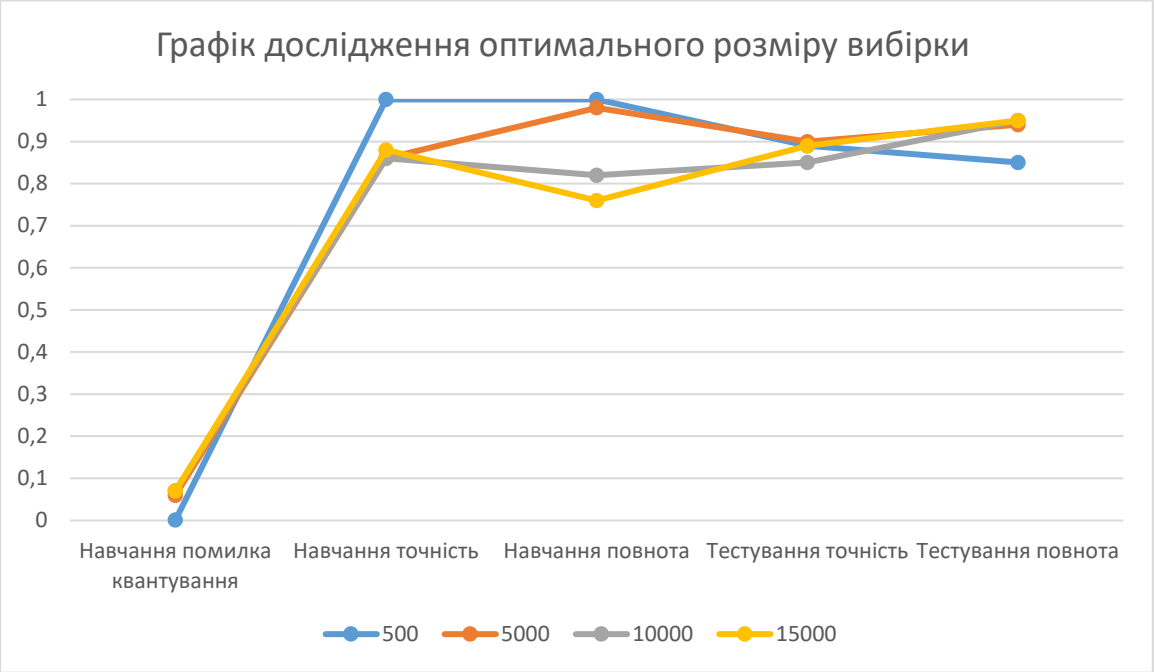


Рисунок 3.27 – Графік дослідження оптимального розміру вибірки

За результатами дослідження можемо бачити, що помилка на 10000 та 15000 рівна, але точність та повнота при тестуванні на вибірці 15000 більша. При 5000 результати тестування у порівнянні з вибіркою у 15000 майже рівні, але помилка квантування нижча. При вибірці у 500 векторів точність та повнота при навчанні були визначені некоректно. На основі цього обрано вибірку у 15000 векторів.

Друге дослідження визначає оптимальний розмір карти. Експеримент проводився на вибірці у 15000 екземплярів, 5000 ітерацій при навчанні, та на виибірці у 1000 екземплярів для тестування. Результати наведено у таблиці 3.5. Скріншоти у додатку В.

Таблиця 3.5 – Результати дослідження розміру карти.

Розмір карти	Навчання			Тестування	
	помилка квантування	точність	повнота	точність	повнота
30x30	0,1	0,85	0,75	0,93	0,89
50x50	0,07	0,88	0,76	0,89	0,95
70x70	0,06	0,88	0,78	0,99	0,95
100x100	0,05	0,88	0,78	1	0,95

Найкращий результат за усіма параметрами отримано при розмірі карти 100x100, але технічно це дуже складний варіант побудови мережі. Тому вирішено обрати карту розміром 70x70, оскільки результати цього експерименту відрізняються від

найкращого результату на 0.01 при помилці квантуванні та на 0.01 у точності тестуванні.

3.4 Висновки

1. Для визначення категорії атаки складено багатошаровий персептрон за допомогою пакета Neural Network Toolbox у MatLAB. Конфігурація мережі 41-1-30-5. Для навчання, валидації та тестування нейромережі було підготовлено вибірку даних у 10000 прикладів. Оптимальні параметри багатошарового персептрона було визначено за допомогою додаткових досліджень: обрано алгоритм навчання Левенберга-Марквардта, при якому затрачений час на моделювання складає 15 епох, MSE для тренувальної, контрольної та тестової вибірок дорівнює 0.0061, 0.0089, 0.0071 відповідно.

2. Для визначення ступеню імовірності атаки на нейромережу створена нейронечітка мережа (ANFIS) за допомогою пакета Fuzzy Logic Toolbox у MatLAB. Конфігурація мережі наступна: 4-2-4-16-1. Підготовлено вибірку у 15000 векторів. Проведено додаткові дослідження на нейронечіткій мережі. При оптимальній структурі отримано значення помилки при навчанні дорівнює 0,3, помилка при тестуванні – 0,29 та кількість епох склала 40.

3. Для визначення категорії атак запрограмована мережа Кохонена на мові програмування Python. Конфігурація мережі: 41 вхідний параметр, 5 вихідних. Вибірку для навчання (15000 векторів) та тестування (1000 векторів) мережі підготовлено. Додаткові дослідження проведені, при оптимальних параметрах результат при навчанні помилки квантування дорівнює 0,66, параметри точності та повноти слали 0,88 та 0,78 відповідно, а при тестуванні точність = 0,99, повнота = 0,95.

4 ДОСЛІДЖЕННЯ КОМБІНОВАНОГО ВАРІАНТУ ЩОДО ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК

4.1 Дослідження параметрів якості

Оцінка якості рішень проводиться за параметрами TP (true-positive) – класифікатор вірно відніс об’єкт до категорії, FP (false-positive) – класифікатор невірно відніс об’єкт до категорії, FN (false-negative) – класифікатор невірно вказує, що об’єкт не належить до категорії, TN (true-negative) – класифікатор вірно стверджує, що об’єкт не належить до категорії, TPR (true positive rate) - показує частку знайдених об'єктів класу загальному числу об'єктів класу, FPR (false positive rate) - показує частку неправильних спрацьовувань класифікатора до загальної кількості об'єктів за межами класу, accuracy (точність) - показує частку правильних класифікацій, precision (точність) - показує частку об'єктів класу серед об'єктів, виділених класифікатором, recall (повнота) - показує частку знайдених об'єктів класу загальному числу об'єктів класу.

Вибірка містить у собі 10000 векторів з бази даних NSL-KDD. Фрагмент вибірки наведено на рис. 4.1.

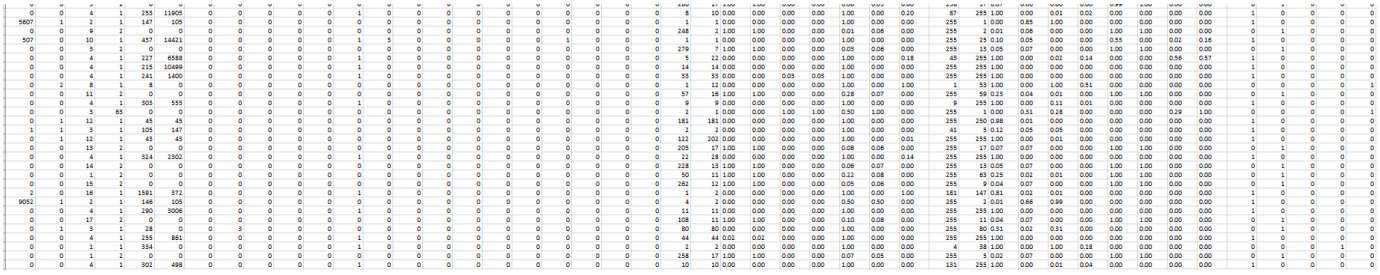


Рисунок 4.1 – Фрагмент вибірки для дослідження параметрів якості

Для оцінки якості рішень нейронечіткої мережі, багатошарового персептрону та мережі Кохонена проведено розрахунки та представлено результати у таблиці 4.1.

Таблиця 4.1 – Результати розрахунків оцінки якості для атаки DOS

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	3412	1885	108	4595	0,97	0,29	0,80	0,64	0,97
Багатошаровий персептрон	3656	1772	111	4458	0,97	0,28	0,81	0,67	0,97
Мережа Кохонена	3371	964	102	5563	0,97	0,13	0,89	0,73	0,96

Результати моделювання для атаки DOS показані на рис. 4.2.

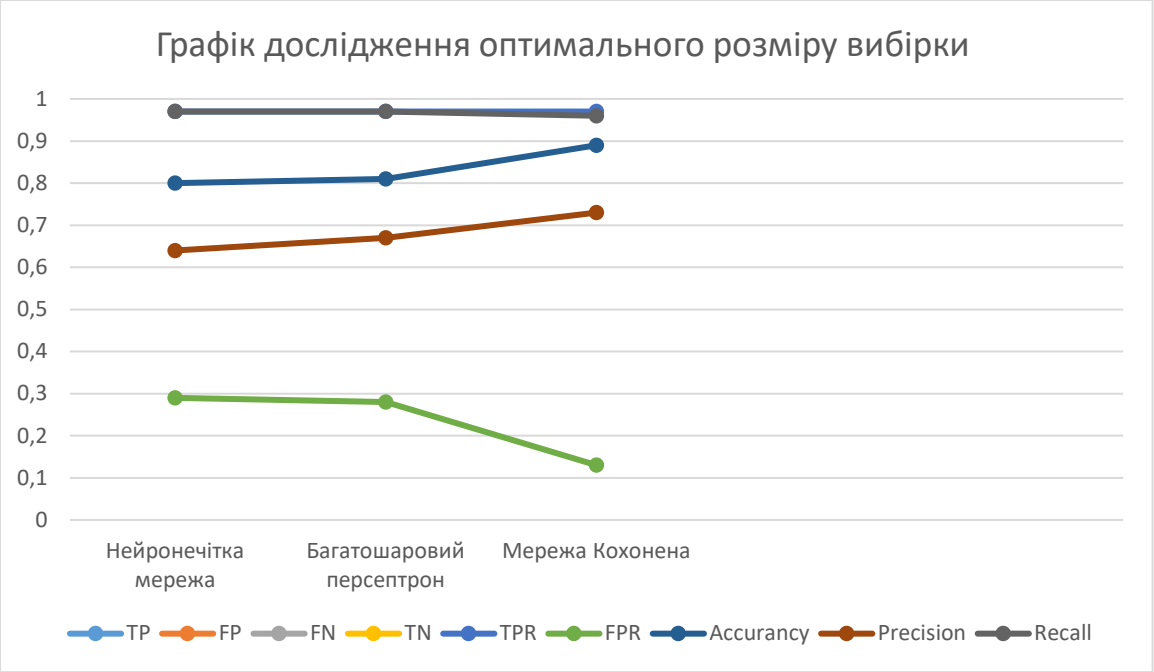


Рисунок 4.2 - Результати моделювання для атаки DOS

Таблиця 4.2 – Результати розрахунків оцінки якості для атаки U2R

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	13754	473	520	253	0,96	0,65	0,93	0,97	0,96
Багатошаровий персептрон	1	2	4	9993	0,2	0	1	0,33	0,2
Мережа Кохонена	0	0	6	9994	0	0	1	0	0

Результати моделювання для атаки U2R показані на рис. 4.3.

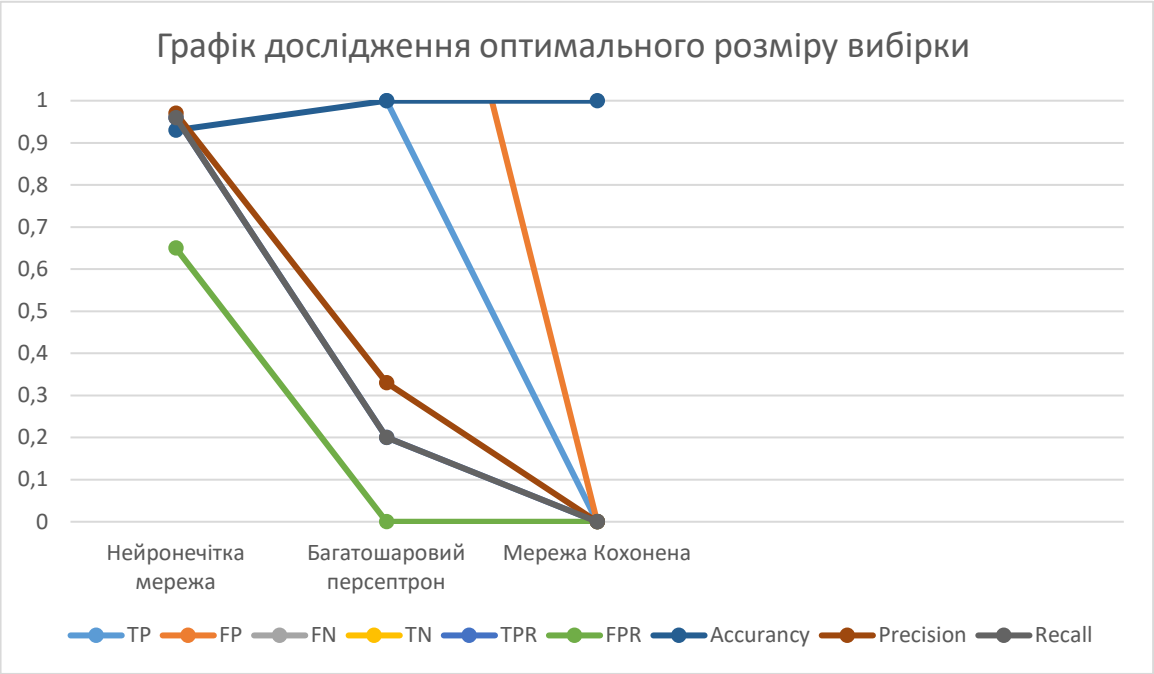


Рисунок 4.3 - Результати моделювання для атаки U2R

Таблиця 4.3 – Результати розрахунків оцінки якості для атаки R2L

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	13754	473	520	253	0,96	0,65	0,93	0,97	0,96
Багатошаровий персептрон	110	8	5	9877	0,96	0	1	0,93	0,96
Мережа Кохонена	84	10	26	9880	0,76	0	1	0,89	0,76

Результати моделювання для атаки R2L показані на рис. 4.4.

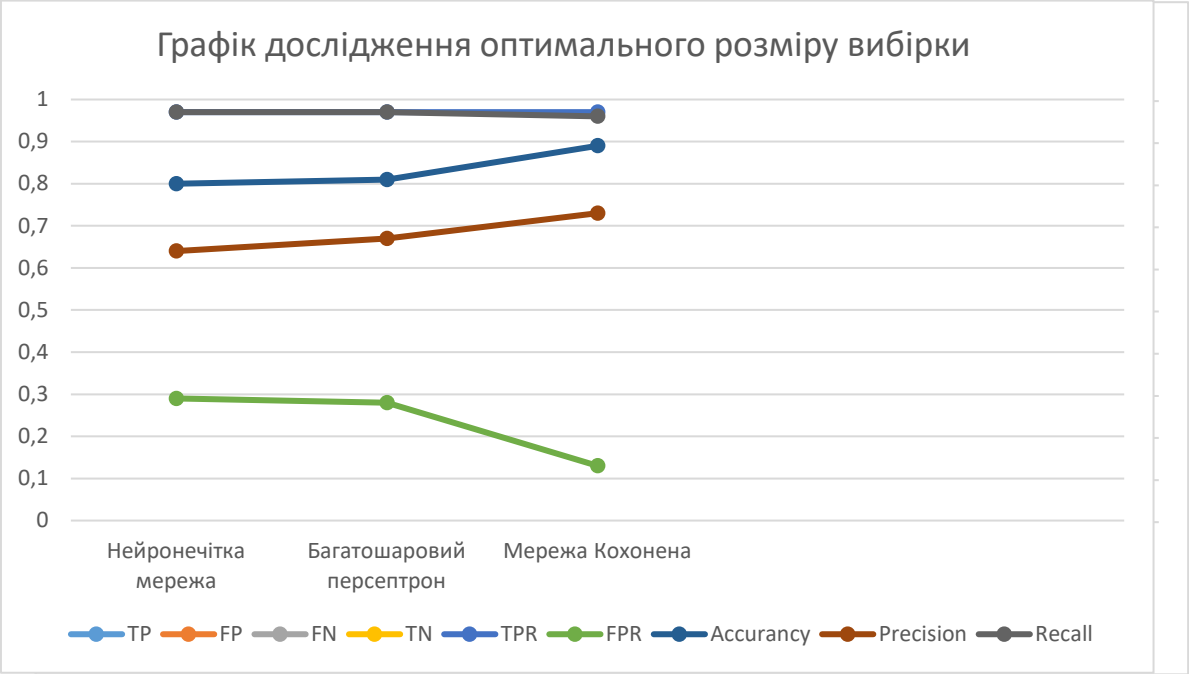


Рисунок 4.4 - Результати моделювання для атаки R2L

Таблиця 4.4 – Результати розрахунків оцінки якості для атаки Probe

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	1380	983	520	253	0,96	0,65	0,93	0,97	0,96
Багатошаровий персептрон	1307	36	2	8655	1	0	1	0,97	1
Мережа Кохонена	1082	30	42	8990	0,96	0	0,99	0,97	0,96

Результати моделювання для атаки Probe показані на рис. 4.5.

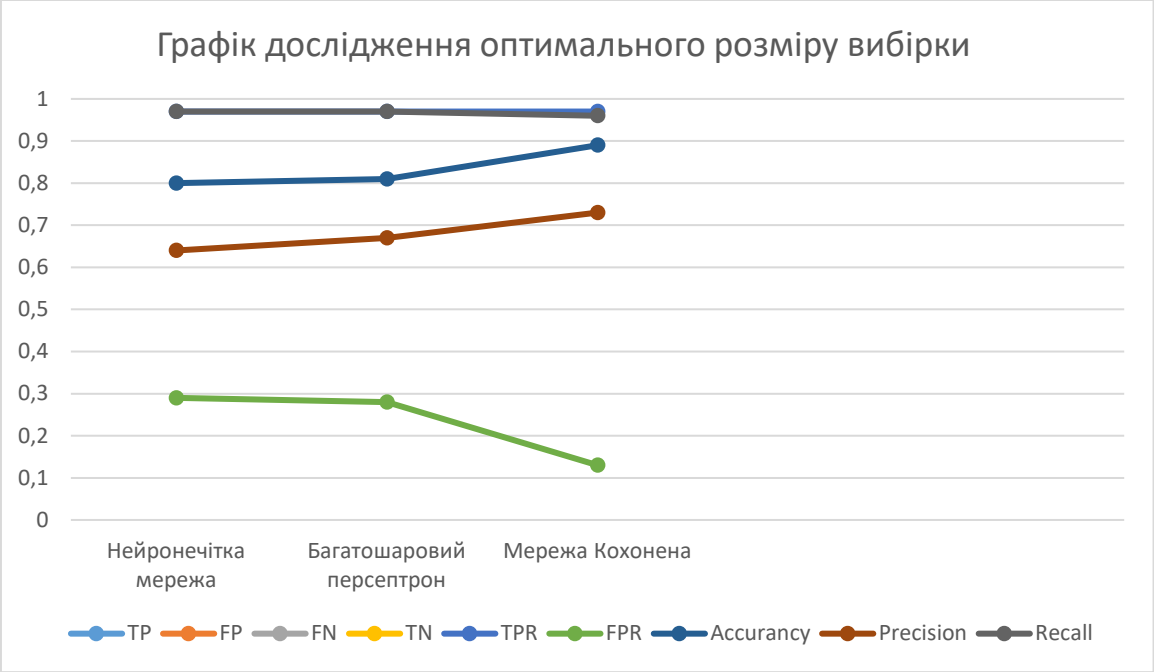


Рисунок 4.5 - Результати моделювання для атаки R2L

Таблиця 4.5 – Результати розрахунків оцінки якості для категорії Normal

Мережа	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall
Нейронечітка мережа	137	673	520	1253	0,96	0,65	0,93	0,97	0,96
Багатошаровий персептрон	7990	103	65	1842	0,99	0,05	0,98	0,99	0,99
Мережа Кохонена	6843	323	54	2780	0,99	0,1	0,96	0,95	0,99

Результати моделювання для категорії Normal показані на рис. 4.6.

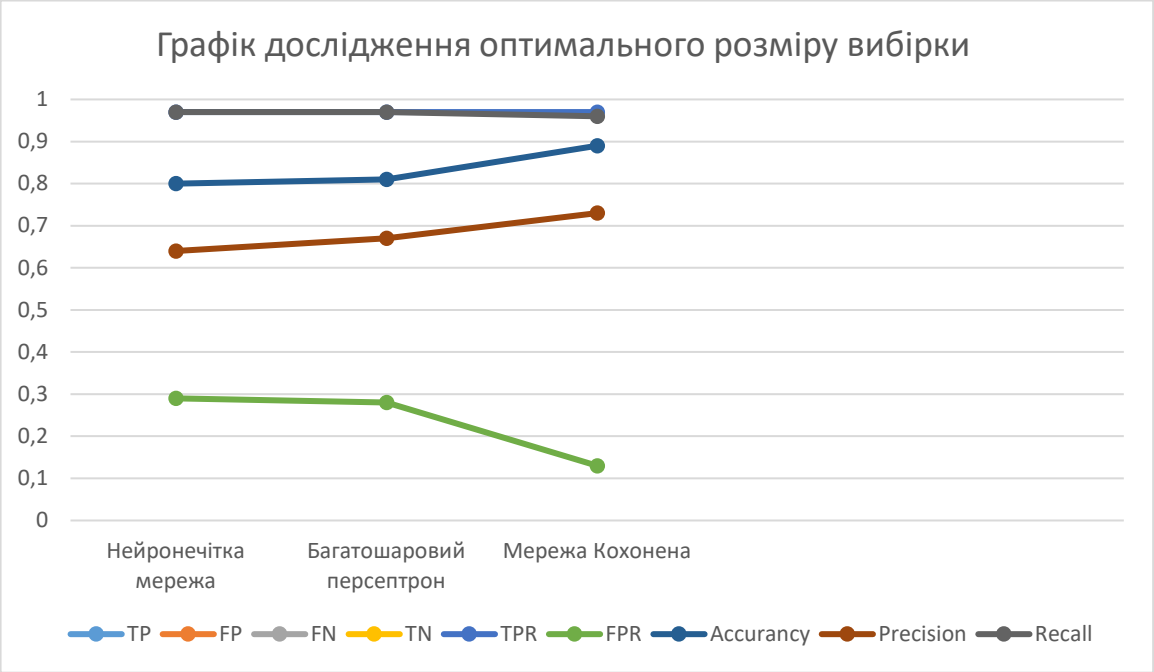


Рисунок 4.6 - Результати моделювання для атаки R2L

Помилка 1-го роду			Помилка 2-го роду	
Кіл-ть неправильно виявлених атак (FP)			Кіл-ть пропусків атак (FN)	
Ступінь імовірності атаки	**Нейронечітка мережа**		**Ступінь імовірності атаки**	**Нейронечітка мережа**
Високий	125		Високий	135
Середній	189		Середній	207
Низький	159		Низький	178
Усього	**473**		Усього	**520**

Рисунок 4.7 – Розрахунок помилки першого та другого роду для нейронечіткої мережі

Помилка 1-го роду			Помилка 2-го роду	
Кіл-ть неправильно виявлених атак (FP)			Кіл-ть пропусків атак (FN)	
Категорія атаки	**MLP**		**Категорія атаки**	**MLP**
Dos	60		Dos	75
U2R	1		U2R	0
R2L	16		R2L	5
Probe	71		Probe	58
Normal	19		Normal	15
Усього	**167**		Усього	**153**

Рисунок 4.8 – Розрахунок помилки першого та другого роду для MLP

Помилка 1-го роду	
Кіл-ть неправильно атак (FP)	
Категорія атаки	**SOM**
Dos	109
U2R	5
R2L	0
Probe	52
Normal	15
Усього	**181**

Помилка 2-го роду	
Кіл-ть пропусків атак (FN)	
Категорія атаки	**SOM**
Dos	51
U2R	3
R2L	3
Probe	21
Normal	10
Усього	**88**

Рисунок 4.9 – Розрахунок помилки першого та другого роду для мережі Кохонена

З отриманих результатів можна бачити, що нейронечітка мережа та багатошаовий персептрон визначає ступінь імовірності атаки з точністю = 0,97. Проте багатошаровий персептрон має кращі показники другого параметру точності та повноти. У той час мережа Кохонена має найгірші показники оцінки якості.

Для загальної оцінки якості класифікаторів зробимо розрахунок F-мірки. Результати наведено у табл. 4.2.

Таблиця 4.6 – Результати оцінки якості за F-міркою

Мережа	F-мірка
Нейронечітка мережа	0.96
Багатошаровий персептрон	0.97
Мережа Кохонена	0.83

Після загальної оцінки якості можемо бачити, що найкращий результат показує багатошаровий персептрон. Нейронечітка мережа у порівнянні з мережею Кохонена має оцінку вище на 0.13.

4.2 Дослідження комбінованого підходу до визначання атак

Для порівняння результатів від багатошарового персептрону, мережі Кохонена та нейронечіткої мережі було проведено дослідження на 50 векторів (додаток А). Результати наведено у табл. 4.3 та у додатку В.

Таблиця 4.7 – Результати дослідження комбінованого підходу

	Вибірка	Нейронечітка мережа	Багатошаровий персептрон	Мережа Кохонена
Normal	27	-	28	31
DOS	17	-	16	17
U2R	0	-	0	0
R2L	1	-	1	0
Probe	5	-	5	1
Висока імовірність	23	14	-	-
Середня імовірність	-	7	-	-
Низька імовірність	27	29	-	-

За отриманими результатами розрахуємо F-мірку для комбінованого підходу табл. 4.8, рис. 4.5.

Таблиця 4.8 - Розрахунок оцінки якості комбінованого підходи

	TP	FP	FN	TN	TPR	FPR	Accurancy	Precision	Recall	F-мірка
Нейронечітка мережа	21	3	0	27	1,00	0,10	0,94	0,88	1,00	0,9375
Багатошаровий персептрон	32	1	0	27	1,00	0,04	0,98	0,97	1,00	0,984848
Мережа Кохонена	18	5	0	27	1,00	0,16	0,90	0,78	1,00	0,891304

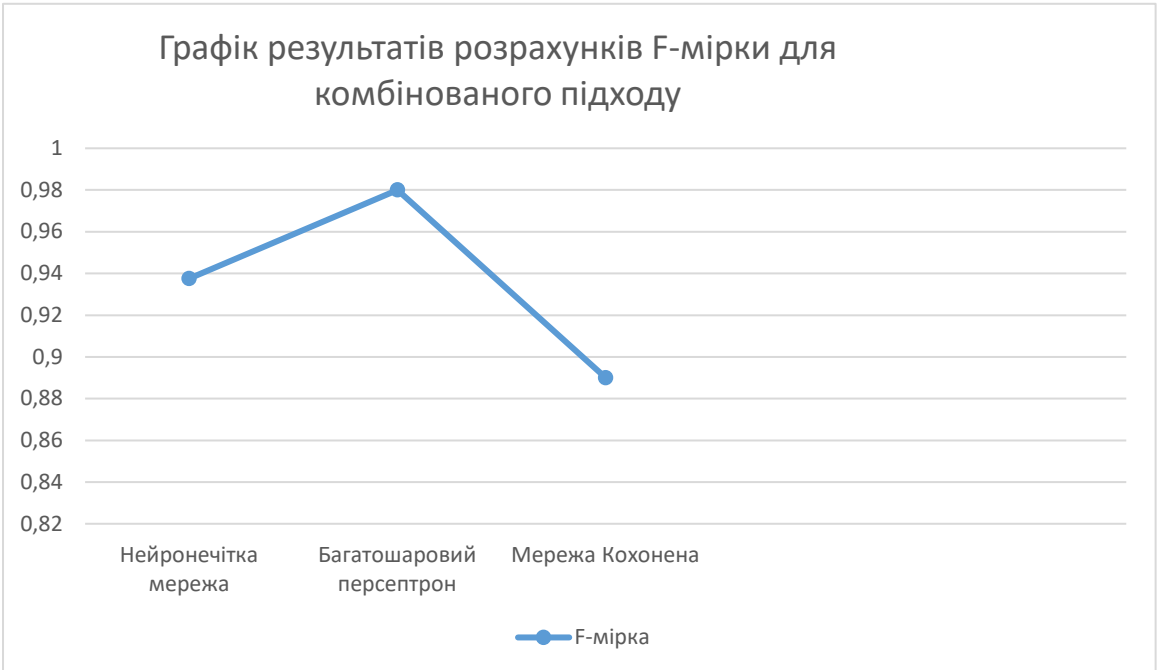


Рисунок 4.5 – Графік результатів комбінованого підходу за F-міркою

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

4.3 Висновки

1. При дослідженні параметрів якості навчання було визначено, що найточніші результати виявлення атак дав багатошаровий персептрон. Непоганий результат отримано при роботі з нейронечіткою мережею. Мережа Кохонена у розрахунках показує найгірший результат параметрів якості.

2. Дослідження комбінованого підходу показало, що багатошаровий персептрон найраще зміг показати наявність атаки та їхні категорії. Нейронечітка мережа також показала досить точні результати. Найгірші показники виявилися у мережі Кохонена.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХСИТУАЦІЯХ

5.1 Вимоги безпеки при виконанні робіт на робочому місці

У всіх професійних галузях питання охорони та безпеки праці стоїть на першому місці. Тому багато державних нормативних документів регулюють цю сферу при роботі за комп'ютером та з електропристроями: закон України "Про охорону праці" [40], нормативно-правові акти з охорони праці «Правила безпечної експлуатації електроустановок споживачів» [41], НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час робот з екранними пристроями» [42] та інші.

Так, відповідно до нормативно-правових актів з охорони праці [41, 42] під час роботи з електронно-обчислювальними пристроями з відео-дисплейними терміналами та периферійними пристроями необхідно:

–очищати перед початком роботи щодень екран від пилу та іншихзабруднень;

–щодня перед початком роботи оператор електронно-обчислювальної машини повинен перевірити своєробоче місце на наявність ознак пошкодження обладнання;

–перед початком роботи оператор електронно-обчислювальної машини повинен перевірити правильність підключення обладнання електронно-обчислювальної машини до електромережі;

–перед початком роботи оператор електронно-обчислювальної машини повинен перевіритиправильність організації робочого місця;

–обладнання, принесене у холодну пору року з вулиці в робочеприміщення, можна підключати до електричної мережі тільки після того, як температура обладнання зрівняється з температурою повітря відповідногоробочого приміщення;

–про виявлення несправності обладнання або інших факторів, які створюють загрозу для життя або здоров'я працівників, необхідно негайно інформувати свого безпосереднього керівника.

При роботі з електронно-обчислювальними машинами з відео-дисплейними терміналами та периферійними пристроями категорично забороняються наступні дії:

–виконувати на робочому місці, ремонт та налагодження електронно-обчислювальної машини;

–відключати захисні пристрої, самочинно проводити зміни у конструкції та складі електронно-обчислювальної машини або їх технічне налагодження;

–працювати з відео-дисплейними терміналами, у яких під час роботи з'являються нестабільне зображення на екрані, нехарактерні сигнали тощо;

–зберігання біля електронно-обчислювальної машини дискет, паперу, інших носіїв інформації,запасних блоків, деталей тощо;

–допускання попадання вологи на поверхню системного блоку;

–доторкання до задньої панелі системного блоку при включеному живленні;

–вимикання живлення під час виконання активного завдання;

–приймання напоїв та їжі на робочому місці.

Робочі місця повинні розроблятися з урахуванням освітлення та контрасту між екраном та довкіллям [42, 43], ергономіки, відповідати антропологічним та психофізіологічним нормам, враховувати можливості здійснити рухи або зміну положення тіла [41].

Мікроклімат у виробничих приміщеннях з робочими місцями програмістів-розробників з екранними пристроями має постійно відповідати вимогам «Санітарних норм мікроклімату виробничих приміщень» ДСН 3.3.6.042-99 [45], що було затверджено постановою Головного державного санітарного лікаря України від 01 грудня 1999 року №42.

На робочому місці стіл або робоча поверхня повинні мати низьку відбивну здатність, достатньо ергономічні розміри та мати гнучкість при розміщенні клавіатури, екрана, документів, обладнання, тощо. Крісло повинно бути стійким, регулюватися за висотою та нахилом та дозволяти працівнику займати зручне положення.

5.2 Шкідливі виробничі фактори на робочому місці

На організм працівника впливає ряд виробничих факторів, розумове та фізичне навантаження. До негативних факторів відноситься:

–підвищена або знижена температура;

–підвищена або знижена вологість;

–недостатня освітленість;

–підвищений рівень шуму;

–підвищена іонізація повітря;

–підвищений рівень електромагнітних випромінювань;

–нервово-психічні перевантаження.

З цих причин дуже важливо правильно організувати робоче місце, відповідно до законодавчих документів. Розглянемо рекомендації, що надаються у нормативно-правових актах.

Об’єм приміщення на одного працівника повинна складати 20 $м^3$, а площа приміщень - не менше 6 $м^2$ зурахуванням максимального числа працівників в одну зміну [44].

Оптимальні мікрокліматичні умови виробничого приміщення для категорій Іа та Іб наведено у табл. 5.1, 5.2 відповідно до ДСН 3.3.6.042-99., що затверджено Постановою Головного державного санітарного лікаря України №42 від 1 грудня 1999 року [45], нормативно-правові акти з охорони праці «Правила безпечної експлуатації електроустановок споживачів» [41] та НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час робот з екранними пристроями» [40].

Таблиця 5.1. – Оптимальні мікрокліматичні умови виробничого приміщення, для категорій Іа та Іб легких робіт

Період року	Категорія робіт	Температура повітря	Відносна вологість	Швидкість руху, м/сек.
Холодний період року	Легка Іа	22 – 24	60 – 40	0,1
	Легка Іб	21 – 23	60 – 40	0,1
Теплий період року	Легка Іа	23 – 25	60 – 40	0,1
	Легка Іб	22 – 24	60 – 40	0,2

Таблиця 5.2. – Допустимі мікрокліматичні умови виробничого приміщення, для категорій Іа та Іб легких робіт.

Період року	Категорія робіт	Температура, град.С				Відносна вологість (%)	Швидкість руху, м/сек.
		Верхня межа		Нижня межа			
		На постійних робочих місцях	На непостійних робочих місцях	На постійних робочих місцях	На непостійних хробочих місцях		
Холодний період року	Легка Іа	25	26	21	18	75	не більше 0,1
	Легка Іб	24	25	21	18	75	не більше 0,2
Теплий період року	Легка Іа	28	30	22	20	55 - при 28 град. С	0,2 - 0,1
	Легка Іб	28	30	21	19	60 - при 27 град. С	0,3 - 0,1

Оптимальні рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентнірівні звуку на робочих місцях, мають відповідати вимогам що наведені у таблиці 5.3 – Допустимі рівні звуку, еквівалентні рівні звуку і рівні звукового тиску в октавних смугах частот відповідно до [45].

Таблиця 5.3 – Допустимі рівні звуку, еквівалентні рівні звуку і рівні звукового тиску в октавних смугах частот для програміста

Вид трудової діяльності	Рівні звукового тиску в дБ в октавних смугах із середньогеометричними частотами, Гц									
	31,5	3	125	250	500	1000	2000	4000	8000	Рівні звуку, еквівалентні рівні звуку, дБА/дБАекв.
Програмісти ЕОМ	86	1	61	54	49	45	42	40	38	50

Нормативним параметром природного освітлення на робочому місці відповідно до державних будівельних норм ДБН В.2.5-28:2018 «Природнеі штучне освітлення», що затверджено наказом Мінрегіону №264 від 3 жовтня 2018 року [44] є коефіцієнт природного освітлення. Коефіцієнт природного освітлення встановлюється в

залежності від розряду виконуваних зорових робіт. Робота програміста відноситься до робіт середньої точності (IV розряд зорових робіт, мінімальний розмір об'єкту розрізнення складає 0,5-1,0мм), для яких при використанні бокового освітлення КПО=1,5%. Для IV розряда зорових робіт мінімальна освітленість складає 300-500 лк.

Розрахунок штучного освітлення для кімнати площею 16,165 м^2, ширина якої складає 3,05м, довжина – 5,3м, висота – 3м за методом коефіцієнта використання світлового потоку наведено далі.

Для визначення потрібної кількості світильників, які повинні забезпечити нормований рівень освітленості, необхідно визначити світловий потік, що падає на робочу поверхню за формулою (5.1):

$$F = \frac{ESKZ}{n}, \qquad (5.1)$$

де F – світловий потік, що розраховується, Лм;

EE – нормована мінімальна освітленість, Лк Е = 300 Лк;

SS – площа освітлюваного приміщення;

KK – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (К = 1,5)

ZZ – відношення середньої освітленості до мінімальної (Z =1,1);

n– коефіцієнт використання світлового потоку, (залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{ст.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{ст}$ = 50 % і $\rho_{стел}$ = 50%.)

Обчислимо індекс приміщення за формулою (5.2)

$$i = \frac{S}{h(A+B)}, \quad (5.2)$$

де S – площа приміщення, S = 16,165м^2;

h – розрахункова висота підвісу, h = 2,9 м;A – ширина приміщення, A = 3,05 м;

B – довжина приміщення, B = 5,3 м.

Підставивши значення отримаємо: i = 0,67. Знаючи індекс приміщення, знаходимо n = 0,22. Підставимо всі значення у формулу для визначення світлового потоку F.

$$F = \frac{300 * 16.165 * 1.1 * 1.5}{0.22} = 33371.25 \text{ Лм}$$

Для освітлення використані люмінісцентні лампи типу ЛБ 40-1, світловий потік яких F=4320 Лм. Розрахуємо необхідну кількість ламп у всітильниках за формулою (5.3)

$$N = \frac{F}{F_Л} \quad (5.3)$$

де N – кількість ламп, що визначається;F – світловий потік;

$F_л$ – світловий потік ламп

$$N = \frac{33371.25}{4320} = 8,4 = 9$$

В приміщені кожен світильник комплектується двома лампами, тобто необхідно використовувати 4 світильника з 2 працюючими лампами. Схема розташування світильників наведено на рисунку 5.1.

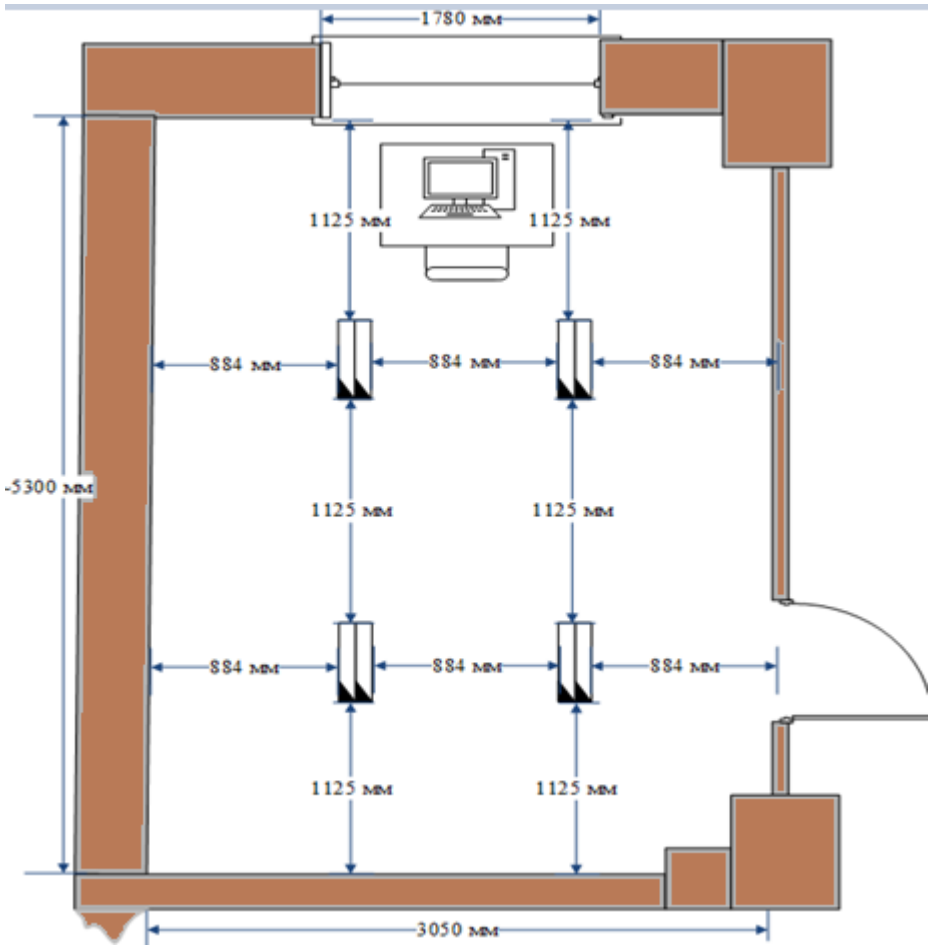


Рисунок 5.1 – Схема розташування світильників

Таким чином не задовольняється достатні умови штучного освітлення. Рекомендується додати ще один світильник.

5.3 Дій працівників в аварійних ситуаціях

У випадку аварійної ситуації працівник зобов’язаний [46]:

–при виявленні будь-яких неполадок в роботі персонального комп'ютера програміст повинен припинити роботу, вимкнути комп'ютер і повідомити про це безпосереднього керівника для організації ремонту;

–при попаданні під електричну напругу негайно вимкнути живлення та надати першу допомогу;

–при будь-яких випадках порушень роботи технічного обладнання негайно викликати представника технічної служби;

–при нещасному випадку, отруєнні, раптовому захворюванні необхідно негайно надати першу допомогу потерпілому, викликати лікаря або допомогти;

–доставити потерпілого до лікаря, а потім повідомити керівника про те, що трапилося;

–у випадку виникнення різі в очах, різкого погіршення зору, виникненняголовного болю, больових почуттів у пальцях та кистях рук, посилення серцебиття – негайно припинити роботу з використанням ЕОМ, повідомити про те, що сталося, свого безпосереднього керівника й звернутися до медичної установи;

–якщо обладнання загоряється, то необхідно негайно вимкнути його від електромережі, ужити заходів щодо ліквідації вогню за допомогою вуглекислотного або порошкового вогнегасник.

При ураженні електричним струмом необхідно виконувати наступний алгоритм надання першої домедичної допомоги[46]:

–як можливо швидше відокремити потерпілого від джерела струму.

–викликайти швидку, якщо це необхідно.

–покласти та/або зігріти людину.

–закрити опіки - якщо у потерпілого є опіки, їх треба накрити стерильною марлею або чистою гладкою тканиною.

–якщо з'являються ознаки шоку - блювання, слабкість, сильна блідість, - трохи підняти ноги, підклавши під ступні валик з речей.

–якщо потерпілий погано дихає або не дихає зовсім, негайно зробити штучне дихання рот в рот.

–якщо у людини немає пульсу і відсутній серцебиття, крім штучного дихання, необхідний непрямий масаж серця.

При пожежі необхідно виконувати наступний алгоритм надання першої домедичної допомоги[46]:

–якщо горить одяг - погасити полум'я, щільно накривши людину ковдрою або будь-яким шматком тканини. Обпалені ділянки одягу акуратно розрізати у запобігання подальшої травматизації шкіри.

–якщо рана закрита необхідно охолоджувати водою уражену ділянку

–на поверхню рани слід накласти стерильну пов'язку.

–дати випити велику кількість рідини (чай, вода і тому подібне).

–негайно викликати швидку медичну допомогу.

–при можливості знеболити потерпілого.

Загальними правилами надання до медичної допомоги є наступними [46]:

–перш за все оглянути місце пригоди і впевнитись в особистій безпеці і безпеці постраждалого;

–провести первинний огляд постраждалого;

–викликати швидку медичну допомогу;

–провести вторинний огляд постраждалого, з метою виявлення пошкоджень, які потребують надання домедичної допомоги.

ВИСНОВКИ

1. Після аналізу наукових джерел для вирішення задачі визначення мережевих атак було обрано три нейромережі: багатошаровий персептрон, нейронечітка мережа, мережа Кохонена.

2. Багатошаровий персептрон та нейронечітка мережа створені за допомогою MatLAB, мережа Кохонена запрограмована на мові Python. Нейронечітка мережа визначає імовірність атаки, а багатошаровий персептрон та мережа Кохонена – наявність атаки та категорію.

3. На створених мережах проведені дослідження: визначення оптимальних параметрів нейронних мереж (перше дослідження), оцінка якості отриманих рішень (друге дослідження) та оцінка якості комбінованого підходу (третє дослідження).

4. У першому дослідженні для визначення оптимальних параметрів багатошарового персептрону було досліджено розмір вибірки та алгоритми навчання, розрахован розмір прихованого шару. Для нейронечіткої мережі було перевірено оптимальність розміру вибірки, методи навчання. Після навчання нейронечіткої мережі була зроблена перевірка на адекватність. Для мережі Кохонена зроблена перевірка розміру вибірки та підібраний оптимальний розмір карти. Результати досліджень оцінбвалися за параметром MSE. Так, наприклад, для визначення категорій мережевих атак на основі багатошарового персептрону обрано конфігурацію 41-1-30-5, розмір вибірки для навчання 10000 та алгоритм навчання Levenberg-Marquardt.

5. У другому дослідженні було розрахувано оцінку якості отриманих рішень на трьох нейромережах. За результатами цього дослідження отримали, що багатошаровий персептрон показав найкращий результат при навчанні.

6. У третьому дослідженні був проведен експеримент з комбінованим підходом до визначення атак на комп’ютерні мережі. Для оцінки результатів проведено розрахунок F-мірки. За цим показником найкращий результат показує багатошаровий персептрон.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Служба безпеки України. 460 кібератак і 20 хакерських угруповань нейтралізувала СБУ з початку року. URL: https://ssu.gov.ua/novyny/460-kiberatak-i-20-khakerskykh-uhrupovan-neitralizuvala-sbu-z-pochatku-roku (дата звернення: 27.03.2021).

2. Державний університет телекомунікацій. Брандмауер як основний захист систем інформаційного і кібернетичного напряму. Переваги та недоліки. URL: http://www.dut.edu.ua/ua/news-1-569-8737-brandmauer-yak-osnovniy-zahist-sistem-informaciynogo-i-kibernetichnogo-napryamu-perevagi-ta-nedoliki_kafedra-cistem-tehnichnogo-zahistu-informacii (дата звернення: 15.11.2021).

3. ESET. Брандмауер. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/ (дата звернення: 15.11.2021).

4. Dhangar K., Kulhare D., Khan A. A Proposed Intrusion Detection System.International Journal of Computer Applications. 2013. Vol. 65, N 23. p.p. 46-50.

5. Котов В. Д. Современное состояние проблемы обнаружения сетевыхвторжений. Уфа : «Вестник УГАТУ» , 2012. С. 198-204.

6. Лукацкий А. В. Обнаружение атак СПб.: БХВ-Петербург, 2003. 608 с.

7. Саймон Хайкин Нейронные сети. Москва: «Вильямс», 2008. 1104 с.

8. Апанель Е. Н. Нейронауки: достижения и перспективы. «Медицинскиеновости», 2013. № 10. С. 6-11.

9. Пахомова В. М. Теорія проектування комп’ютерних мереж: методичнівказівки до виконання курсового проект. Дніпровск. нац. ун-т залізн. трансп. ім. акад. В. Лазаряна, 2019. 60 с.

10. Пахомова В. М. Можливості розвитку комп’ютерних мереж у автоматизованих системах залізничного транспорту: монографія. Дніпро: Дніпропетр. нац. ун-т залізн. трансп. ім. акад. В. Лазаряна, 2015. 207 с.

11. Крыжановский А. В. Применение искусственных нейронных сетей в системах обнаружения атак. «Технические науки», 2008. 2 с.

12. Терейковський І. Вдосконалення алгоритму навчання багатошарового перспетрону, призначеного для розпізнавання мережевих атак. «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», 2012. № 2. 6 с.

13. Пахомова В. М. Методичні вказівки до виконання лабораторних робіт з дисципліни «Теорія проектування комп'ютерних мереж». *Дніпро: ДІІТ*, 2019. - 60 с.

14. Мустафаев А. Г. Нейросетеваясистема обнаружения компьютерных атак на основе анализа сетевого трафика. Вопросы безопасности. 2016. № 2. С. 1–7. DOI: https:// doi.org/10.7256.2409-7543.2016.2.18834 (дата звернення: 15.11.2021).

15. Пахомова В. М., Коннов М.С. Дослідження двох підходів до вивлення мережних атак із використанням нейромережної технології. URL: http://stp.diit.edu.ua/article/view/208233 (дата звернення: 15.11.2021).

16. Жульков Е.В., Платонов В.В. Применение модульного подхода к построению нейронных сетей для поиска аномалий. Проблемы информационной безопасности. Компьютерные системы. 2006. №3. С. 30-34.

17. Гришин А.В. Нейросетевые техонологии в задачах обнаружения компьютерных атак. Информационные технологии и вычислительные системы. 2011.С.53-64.URL: https://lider.diit.edu.ua/pluginfile.php/89943/mod_resource/content/1/%D0%93%D1%80%D0%B8%D1%88%D0%B8%D0%BD_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82.pdf (дата звернення: 15.11.2021).

18. Змістовий модуль 6. Експертні системи. Інтелектуальні інформаційні системи (4 год). URL: https://studfile.net/preview/5474324/page:3/ (дата звернення: 15.11.2021).

19. Кохонен Т. Самоорганизующиеся карты. 2014. URL: http://www.studentlibrary.ru/book/ISBN9785996313488.html (дата звернення: 16.11.2021).

20. Пахомова В. М. Прогнозування обсягу мережевого трафіка в інформаційно-телекомунікаційній системі Придніпровської залізниці на основі нейронечіткої мережі. - Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту. 2016. №6(66). - С.105–114. - URL: https://lider.diit.edu.ua/pluginfile.php/92394/mod_resource/content/1/vdnuzt_2016_6_13%20%281%29.pdf (дата звернення:16.11.2021).

21. Асланов К.Дж., Байрамов Х. Построение интеллектуальных интегрированных систем информационной безопасности в открытых корпоративных сетях.URL:https://lider.diit.edu.ua/pluginfile.php/89940/mod_resource/content/1/Aslanov-Kamran1.pdf (дата звернення:16.11.2021).

22. Браницкий А. А., Тимофеев А. В., Котенко И. В. Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта. URL:https://lider.diit.edu.ua/pluginfile.php/89942/mod_resource/content/1/branitskiy_dissertatio_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82.pdf (дата звернення: 16.11.2021).

23. Фролов П.В., Чухраев И. В., Гришанов К. М. Применение искусственных нейронных сетей в системах обнаружения вторжений. *Системный администратор*. 2018. №9(190) – URL: http://samag.ru/archive/article/3724 (дата звернення:16.11.2021).

24. Веселов В. В., Елманов О. А., Карелов И. Н. Комплекс мониторинга информационных систем на основе нейросетевых технологий -Нейрокомпьютеры: разработка и применение. 2001. № 12.

25. Системи детектування атак. URL:https://helpiks.org/8-59876.html (дата звернення:16.11.2021).

26. Обзор корпоративных IPS-решений. URL: https://www.anti-malware.ru/IPS_russian_market_review_2013 (дата звернення: 16.11.2021).

27. Котов В. Д., Васильев В. И. Система обнаружения сетевых вторженийна основе механизмов иммунной модели. «*Известия Южного федерального университета. Технические науки*», 2011. 10 с.-URL: https://cyberleninka.ru/article/n/sistema-obnaruzheniya-setevyh-vtorzheniy-na- osnove-mehanizmov-immunnoy-modeli/viewer (дата звернення: 16.11.2021).

28. Котов В. Д., Васильев В. И. Современное состояние проблемы обнаружения сетевых вторжений. «*Вестник Уфимского государственного авиационного технического университета*», 2012. 7 с. - URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-problemy-obnaruzheniya-setevyh-vtorzheniy/viewer (дата звернення: 16.11.2021).

29. Технологии обнаружения сетевых атак. – *Брестский государственный технический университет* –URL: https://www.bstu.by/~opo/templates_c/%25%25A1%5EA14%5EA14FF5EA%25%25index.html.php (дата звернення: 17.11.2021).

30. Ю. Г. Емельянова, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы - Программные системы: теория и приложения : электрон. научн. журн. 2011. № 3(7), с. 3–15. URL: http://psta.psiras.ru/read/ psta2011_3_3-15.pdf (дата звернення: 17.11.2021)

31. Пахомова В. М. Дослідження інформаційно-телекомунікаційної системи залізничного транспорту з використанням штучного інтелекту. *Дніпро: Вид-во ПФ «Стандарт - Сервіс»*, 2018. 220 с.

32. Internet Security Threat Report URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-242019-en.pdf (дата звернення: 22.12.2020).

33. NSL-KDD dataset. URL: https://www.unb.ca/cic/datasets/nsl.html (дата звернення: 18.02.2021)

34. MLP documentation. URL: https://www.mathworks.com/help/deeplearning/ug/train-and-apply-multilayer-neural-networks.html (дата звернення 20.04.2021)

35. Anfis documentation. URL: https://www.mathworks.com/help/fuzzy/anfis.html (дата звернення 10.05.2021)

36. Дьяконов В. П. MATLAB. Полный самоучитель. – ДМК Пресс, 2012. – 768 с.: ил.

37. MiniSom documentation. URL: https://github.com/JustGlowing/minisom

38. Matplotlib documentation. URL: https://matplotlib.org/stable/api/_as_gen/matplotlib.pyplot.html

39. Numpy documentation. URL: https://numpy.org/doc/stable/user/whatisnumpy.html

40. Закон України «Про охорону праці» згідно з Постановою Верховної Ради України № 345-VI від 2 вересня 2008 року

41. НПАОП 40.1–1.21–98 «Правила безпечної експлуатації електроустановок споживачів». Затверджено: наказ Держнаглядохоронпраці України № 4 від 9 січня 1998 року

42. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час робот з екранними пристроями». Затверджено: наказ Міністерства соціальної політики України «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями»№ 207 від 14 лютого 2018 року.

43. ДСанПІН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин». Затверджено Постановою Головного державного санітарного лікаря України

№ 7 від 10 грудня 1998 року.

44. ДБН В.2.5-28:2018 «Природне і штучне освітлення». Затверджено наказом Мінрегіону № 264 від 3 жовтня 2018 року.

45. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Затверджено Постановою Головного державного санітарного лікаряУкраїни № 42 від 1 грудня 1999 року.

46. Ненько С. К., Полівода Л. А. Надання першої медичної допомоги при надзвичайних ситуаціях, Херсон: «Навчально-методичний центр цивільного захисту та безпеки життєдіяльності Херсонської області», 2014, 28 с.

47. Видиш А. Д., Пахомова В. М. Аналіз нейронних мереж щодо виявлення мережевих атак. - Тези доповіді з XIVМіжнародній науково-практичній конференції «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті», 2020 – 145 с.

48. Vydysh A. D., Pakhomova V. M., Shpak I. V. Analysis of neural networks to detect network attacks. - Тези доповіді з Всеукраїнської науково-технічній конференції молодих учених, магістрантів та студентів «Науково-технічний прогрес на транспорті», 2021 – 54 с.

49. Видиш А. Д., Пахомова В. М. Визначення категорії мережевих атак на комп’ютерну мережу з використанням нейронечіткої мережі - Тези доповіді з 81 Всеукраїнської науково-технічній конференції молодих учених, магістрантів та студентів “Наука і сталий розвиток транспорту”, 2021 – с. 23-24