МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ЗАЛУЖНИЙ Василь Вікторович

Нейромережні моделі та методи протидії атакам на мережеві ресурси інформаційних систем/ Neural network models and methods for countering attacks on network resources of information systems.

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -22
Ю.М. Якубець

Науковий керівник
к.т.н., доцент І.З. Якименко

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

ЗМІСТ

ВСТУП

Актуальність. У сучасних умовах системи протидії кібератакам є одними з основних засобів захисту інформації мережевих ресурсів інформаційних систем. Хоча використовуються такі системи вже не одне десятиліття, їх розробкою займається багато висококваліфікованих спеціалістів, а створенню відповідної науково-методичної бази присвячено велику кількість робіт, проте практичний досвід вказують на наявність у системах протидії мережевим кібератакам ряду суттєвих недоліків. Основним із них є недостатня точність розпізнавання всієї номенклатури мережевих кібератак, що підтверджується відомими випадками успішного злому систем захисту інформації у низці світових країн. Крім цього, впровадження відомих засобів протидії мережевим кібератакам у системи захисту інформації вітчизняних інформаційних систем викликає необхідність їх складної адаптації до варіативності умов використання. Також недоліками відомих коштів протидії кібератакам на мережеві ресурси інформаційних систем є висока вартість та відсутність докладної науково-технічної документації. Дослідження вчених вказують на те, що розпізнавання мережевих кібератак є використання в них апарату штучних нейронних мереж. Це пояснюється доведеною перспективним шляхом підвищення ефективності коштів ефективністю застосування СР для вирішення подібних завдань провідними розробниками засобів захисту інформації (компанії Cisco, Symantec) та доведеною адаптивністю нейромережевих засобів (НСР) до різноманітних умов застосування. Методологічну та теоретичну основу для ефективного впровадження НСР у СПА становлять теоретичні розробки та досвід створення систем захисту інформації як українських, так і зарубіжних вчених та ін.

Мета кваліфікаційної роботи базується на розробці ефективних нейроних моделей та методів протидії кібератакам,що адаптуються до умов експлуатації і способів швидко реагувати на нові види кібератак.

Для досягнення мети потрібно вирішити ряд взаємопов’язаних задач :

- провести аналіз можливостей нейромережових засобів протидії кібератакам на мережові ресурси інформаційних систем;

- поставити науково-практичне завдання протидії кібератакам на мережеві ресурси інформаційних систем;
- побудувати концептуальну модель забезпечення ефективності нейромережевої протидії кібератакам;
- побудувати модель правил визначення ефективних видів нейромережевих моделей;
- розробити модель формування параметрів начальних прикладів;
- розробити нейромережеву модель протидії мережевим кібератакам за допомогою експертних знань.

Об'єкт дослідження процеси протидії кібератакам на мережеві ресурси інформаційних систем.

Предмет дослідження - нейромережеві моделі, методи та засоби протидії кібератакам на мережеві ресурси інформаційних систем.

Методи дослідження - методи теорії цифрового оброблення сигналів, нейронних мереж, експертного аналізу, математичної статистики та оптимізації.

Наукова новизна – побудовану методологічну базу нейромережевого розпізнавання кібератак на мережеві ресурси інформаційних систем базується на розроблених у кваліфікаційному дослідженні нових нейромережевих моделях і методах, які забезпечили можливість створення ефективної нейромережевої системи протидії атакам на мережеві ресурси інформаційних систем.

Практична значимість роботи полягає у розробці нейромережевих моделей і методів розпізнавання кібератак.

Публікації та апробація ВКР.

1. Якубець Ю.М.Нейромережеві моделі і методи протидії атакам / Матеріали науково-практичного симпозіуму «Захист інформації». – Тернопіль, 2023. – С.184-188

2. Якубець Ю.М., Дмитрів Ю.М. Нейромережі моделі і методи протидії атакам автоматів / Збірник матеріалів проблемної наукової міжгалузевої

конференції ««Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2023). – Тернопіль, 2023. – С.42-45.

1. АНАЛІЗ МОЖЛИВОСТЕЙ НЕЙРОМЕРЕЖОВИХ ЗАСОБІВ ПРОТИДІЇ КІБЕРАТАКАМ НА МЕРЕЖОВІ РЕСУРСИ ІНФОРМАЦІЙНИХ СИСТЕМ.

1.1.Науково-практичне завдання протидії кібератакам на мережеві ресурси інформаційних систем

На першому, найбільш складному етапі завдання протидії кібератакам зводиться до ідентифікації подій, пов'язаних з реалізацією в кібернетичному просторі загроз безпеці ресурсів інформаційних систем з урахуванням їх уразливостей. Іншими словами, дана ідентифікація це виявлення та класифікація будь-яких видів несанкціонованих дій по відношенню до цих ресурсів. У цій роботі акцент ставиться на розпізнавання кібератак, що реалізуються за допомогою використання мережевого трафіку, оскільки результати вказують на те, що в даний час саме такий тип кібератак є одним з найбільш небезпечних. Надалі цей тип кібератак називатимемо мережевими кібератаками. Розпізнавання мережевих кібератак можна визначити як процес моніторингу (реєстрації та аналізу) параметрів мережевого трафіку на наявність ознак порушення політики безпеки та спроби поставити під загрозу конфіденційність, цілісність, доступність, або обійти механізми безпеки хоста чи мережі.

Традиційно для розпізнавання різнорідних кібератак використовуються СПА, які представляють комплекс засобів, призначених для моніторингу подій, що відбуваються в ІС, для подальшого аналізу з метою визначення ознак порушення безпеки об'єкта моніторингу. Також зазначимо, що близьке до СПА призначення мають системи аналізу безпеки (сканери безпеки, системи пошуку подразників), обманні системи, системи контролю цілісності, системи аналізу журналів безпеки. Однак такі системи мають суттєво інший характер оброблюваної інформації, в них необхідно використовувати інші методи

розпізнавання, а отже, їх методологія побудови та експлуатації значно відрізняється від СПА і в цій роботі вони не розглядаються.

Особливістю СПА, яка призначена для протидії мережевим кібератакам є виключно моніторинг мережевого трафіку. Подібні системи захоплює потік даних із мережі, реалізують певні методи аналізу цих даних сигналізують про результати аналізу, а у випадку виявлення кібератаки можуть спричинити спрацювання системи реагування. Основним завданням такої системи є виявлення мережевої кібератаки режим реального часу. Крім цього, можуть бути вирішено наступні завдання:

- Спрогнозувати можливі майбутні мережеві кібератаки та виявити уразливості для запобігання їх подальшому розвитку. Атакуючий зазвичай виконує ряд попередніх дій, таких як, наприклад, мережне зондування (сканування) або інше тестування для виявлення
- вразливостей цільової системи
- Виконати документування наявних загроз.
- Забезпечити контроль якості адміністрування з погляду безпеки, особливо у великих та складних мережах.
- Отримати корисну інформацію про проникнення, що мали місце, для відновлення та коригування факторів, що викликали проникнення.
- Визначити розташування джерела мережевої кібератаки щодо локальної мережі (зовнішні або внутрішні атаки), що важливо при прийнятті рішень про розташування ресурсів у мережі.
- Сучасні мережеві СПА зазвичай складаються з п'яти функціональних
- компонентів, а саме:
- Модуль збору даних – призначений для реєстрації параметрів мережного трафіку, що передається відповідно до різних протоколів.
- Модуль зберігання даних, яким накопичуються первинні статистичні дані та результати аналізу.

- Модуль аналізу – приймає інформацію з модулів збирання та зберігання в даних та аналізує дані на наявність ознак мережевої кібератаки.
- Результат спрацьовування модуля – розпізнаний стан захищеності мережного ресурсу. У найпростішому випадку (системи визначення атак) розпізнаються лише два стани – нормальний або стан реалізації мережевий кібератаки. У сучасних мережевих СПА додатково розпізнаються відомі види мережевих кібератак. Крім цього, може розраховуватися ймовірність (достовірність) кожного із заздалегідь визначених станів захищеності. Це збільшує гнучкість реалізації захисних заходів.
- Модуль реагування – активується у тому випадку, коли аналізуючий механізм визначив наявність кібератаки. Якщо СПА діє автономно, то результатом спрацьовування даного модуля є сигналізація про параметри кібератаки. У разі інтеграції СПА із системою реагування на кібератаку реалізується певний набір захисних заходів.
- Консоль управління, призначена для налаштування інших модулів та системи в цілому.

Типова послідовність функціонування сучасної мережевої СПА показано рисунку 1.1. Поширена класифікація мережевих СПА здійснюється з точки зору локалізації параметрів РІС, що захищається. До класу host-based відносяться СПА, призначені для протидії кібератакам, спрямованих на конкретний вузол мережі. У свою чергу СПА цього класу поділяються ще на три групи:

- Системи протидії кібератакам на рівні прикладного програмного забезпечення, що виявляють атаки на конкретні програми (наприклад, веб-сервер). Прикладом такої системи є RealSecure OS Sensor або WebStalker Pro.
- Системи протидії кібератакам лише на рівні операційної системи.Прикладом такої системи є RealSecure Server Sensor чи Intruder Alert.
- Системи протидії кібератакам на рівні системи керування базами даних, що виявляють атаки на конкретні системи упра

вління БД.

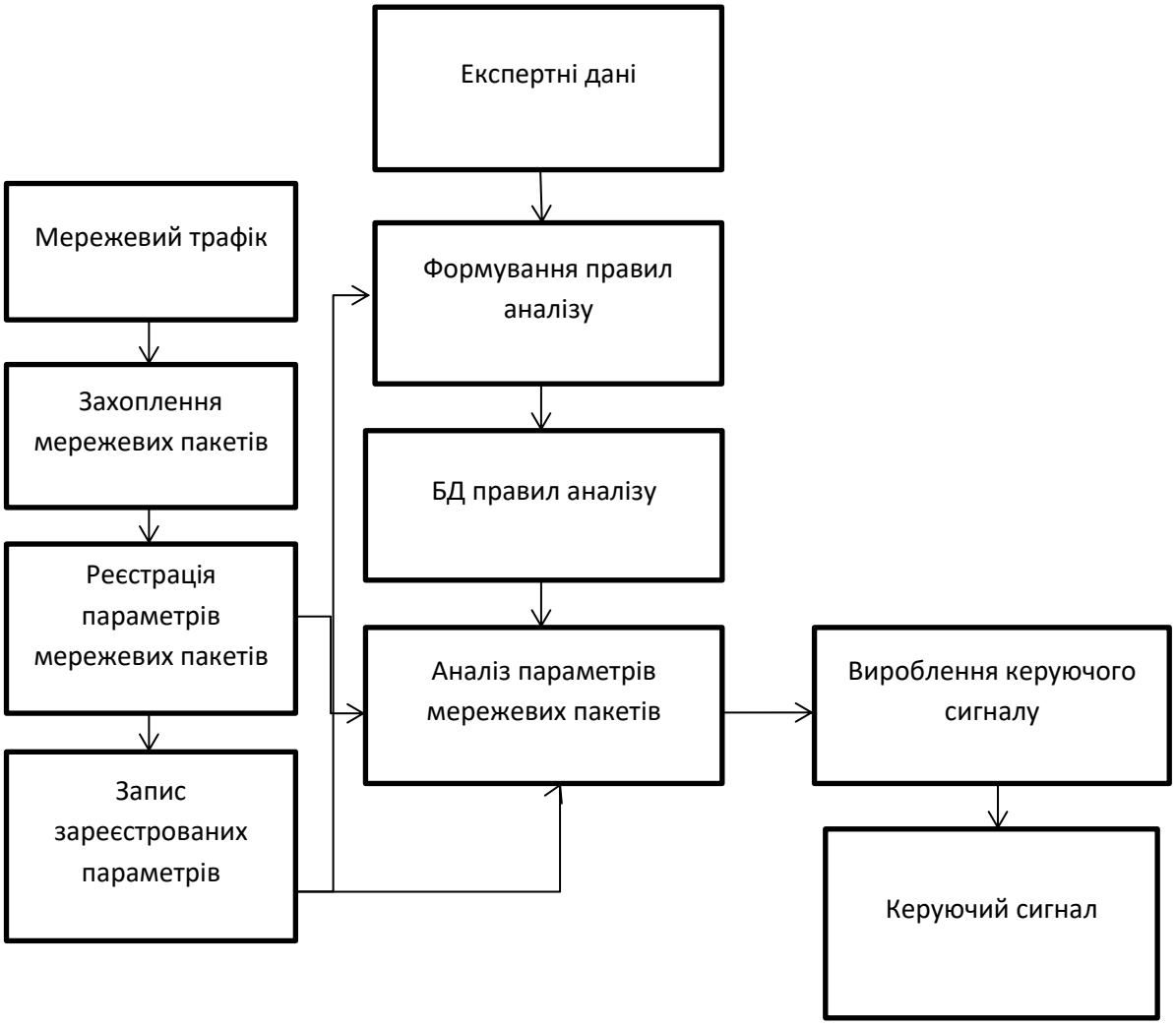

Рисунок 1.1 – Типова послідовність функціонування мережевої СПА

Перевагами host-based СПА є: можливість стежити за подіями локально щодо хоста, можливість функціонувати в оточенні, в якому мережевий трафік зашифровано, не вимагають додаткового функціональність мережевих пристроїв. До недоліків таких систем відносять: відсутність централізованого управління, мале покриття моніторингу, відбір обчислювальних потужностей хоста, що захищається, вразливість до атак на відмову в обслуговуванні.

Також виділяють СПА, призначені для протидії мережевим кібератакам, спрямованих на всю мережу чи сегмент мережі. Такі СПА належать до класу network-based. До цього класу належать основні комерційних СПА. Як приклад

можна назвати різні модифікації апаратно-програмних комплексів Cisco IPS, IBM Proventia та StoneGate IPS. Також до цього класу мережевих СПА можна віднести один із найбільш відомих некомерційних програмних комплексів Snort. Ці системи визначають кібератаки, захоплюючи та аналізуючи мережеві пакети. Слухаючи мережевий сегмент, СПА класу network-based може перехоплювати та аналізувати мережевий трафік від кількох хостів, які приєднані до мережному сегменту, і таким чином розпізнавати мережеві кібератаки на ці хости.

До переваг таких СПА відносять: можливість централізованого керування, відсутність впливу на продуктивність мережі. Недоліками є: висока ресурсомісткість, складність налаштування, неможливість аналізу зашифрованої інформації, неможливість розпізнавання результату атаки. Як показує практика та результати, основним напрямом удосконалення сучасних СПА є підвищення ефективності аналізу мережного трафіку.

1.2 Аналіз процесу протидії мережевим кібератакам.

В даний час процес протидії мережевим кібератакам реалізується з використанням двох основних методів: визначення аномалій та визначення зловживань. Робота аналізатора щодо аномалій виходить з припущення, що ознакою атаки є відхилення поточних величин параметрів мережевого трафіку від величин, характерних для нормального стану мережевих PIC (шаблонів нормальної поведінки) Для визначення шаблоном нормальної поведінки застосовуються статистичні моделі . У деяких СПА формується комплексний показник аномалій. При формуванні даного показника для визначення взаємозв'язків між показниками використовуються підступні матриці. Також використовується підхід до визначення аномалій з використанням методу прогнозу подій, що дозволяє виявити кібератаку на ранніх етапах її здійснення. Суть методу полягає у прогнозуванні кібератаки на основі аналізу попередніх

подій, пов'язаних із об'єктом захисту. Переваги методу аномалій полягають у наступному:

- Можливість визначення мережевої кібератаки без знання конкретних деталей (сигнатури).
- Детектори аномалій можуть створювати інформацію, яка надалі використовуватиметься визначення сигнатур мережевих кібератак.

До важливих недоліків способу аномалій відносять:

- Тривалий термін формування шаблону нормальної поведінки.
- Високий рівень помилкових спрацьовувань, обумовлений недостатньою адаптацією моделей шаблонів нормальної поведінки до складної динаміки параметрів мережевого трафіку.

Особливо складно адаптувати модель шаблону нормальної поведінки до можливої реконфігурації комп'ютерної мережі, що захищається. Навіть незначна зміна структури або складу мережі може спричинити значну зміну шаблону нормальної поведінки. посилюється тим, що складання та актуалізація шаблону нормального поведінки для конкретної ІС, що потребує значних зусиль. Ситуація висококваліфікованих спеціалістів. Тому використання методу аномалій для розпізнавання кібератак на мережеві ресурси універсальних ІС дуже обмежено.

СПА, які використовують метод визначення зловживань, аналізують послідовність подій, пов'язаних з діяльністю об'єкта захисту та порівнюють їх із зразками відомих атак. Такі зразки називають шаблоном атак, а сам метод називають методом визначення атак на основі сигнатур. По причині неповноти інформації та наявності шумів під час реєстрації параметрів безпеки труднощі викликає розрахунок відповідності шаблону атаки реальних подій щодо об'єкта захисту. У базовому випадку мережева кібератака певного виду розпізнається лише у разі повного збігу параметрів мережного запиту з відповідною сигнатурою. Крім цього, для розрахунку відповідності застосовуються такі підходи: експертний, аналіз переходів, моделювання атак. При застосуванні експертного підходу відомі кібератаки описуються у вигляді деякого набору

правил, виконання яких сигналізує про їхню реалізацію. Підхід на підставі аналізу переходів передбачає подання мережевий кібератаки у вигляді послідовності переходів об'єктів захисту з одного стану до іншого. При моделюванні кібератак попередньо сформовані послідовності подій, характерні для реалізації кібератаки порівнюються з поточними показниками. В результаті порівняння формується висновок про можливість здійснення кібератаки. Часто використовуються статистичні моделі зміни параметрів безпеки ІС при кібератаку. Загалом метод визначення зловживань дозволяє достатньо ефективно виявляти кібератаки відомих типів за низького показника помилкових спрацьовувань, але не дозволяє виявити кібератаку, зразок якої не відомий. Водночас мережеві кібератаки постійно змінюються через індивідуальності підходів зловмисників та регулярних змін у програмне забезпечення та апаратні засоби цільових систем. Через великої кількості видів зазначених кібератак, динамічного та нечіткого певного характеру їхніх параметрів дуже складно оперативно підтримувати в актуальному стані основу правил експертної системи. Тому в сучасних мережевих СПА для аналізу сигнатур використовуються рішення, що базуються на теорії штучного інтелекту. З них найбільш апробованими є нейромережеві моделі та методи. Це пояснюється доведеною здатністю НС аналізувати неповні/спотворені дані зі складним характером, узагальнювати накопичену статистичну інформацію, а також оперативно реалізувати розрахунок вихідного сигналу у вигляді ймовірності (достовірності) розпізнаного стану. Ще однією перевагою застосування аналізатора на основі НС є можливість використання як у СПА класу network-based, так і в СПА класу host-based. Загальноприйнято, що сучасні СПА мають розпізнавати такі класи мережевих кібератак: IP-спуфінг, відмова в обслуговуванні (Denial of Service), підбір парольних даних, атака на рівні додатків, мережна розвідка, переадресація портів.

Атака типу IP-спуфінг полягає в тому, що зловмисник, що знаходиться всередині локальної мережі або поза нею, видає себе за санкціонованого користувача. Як правило, для цього зловмисник використовує або IP-адреса, що

знаходиться в межах діапазону санкціонованих IP-адрес, або авторизується зовнішньою адресою, якій дозволяється доступ до певних мережевих ресурсів. Атаки IP-спуфінгу часто є відправною точкою для інших атак. Класичний приклад – атака DoS, яка починається з чужої адреси, що приховує справжню особистість хакера. Атаки з метою викликати відмову в обслуговуванні або DoS-атаки відрізняються від атак інших типів тим, що націлені на те, щоб зробити PIC недоступним для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи чи програми. В разі використання деяких серверних програм (таких як Web-сервер або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих додатків, і тримати їх у зайнятому стані, не допускаючи обслуговування пересічних користувачів. У ході атак DoS можуть використовувати звичайні Інтернет-протоколи, такі як TCP та ICMP. Більшість атак DoS розраховано не на програмні помилки або проломи в системі безпеки, але в загальні слабкості системної архітектури. Деякі атаки зводять до нуля продуктивність мережі, переповнюючи її небажаними та непотрібними пакетами або повідомляючи неправдиву інформацію про поточний стан мережних ресурсів. Коли атака даного типу проводиться одночасно через безліч пристроїв, то її називають розподіленою DoS-атакою (distributed DoS, DDoS). Підбір парольних даних може бути реалізований за допомогою цілого ряду методів, таких як простий перебір (brute force attack), троянський кінь, IP-спуфінг та сніффінг пакетів. Хоча логін та пароль часто можна отримати за допомогою IP-спуфінгу та сніфінгу пакетів, хакери нерідко намагаються підібрати пароль та логін, використовуючи для цього численні спроби доступу. Такий підхід називається простого перебору.Атаки на рівні додатків можуть проводитись декількома способами. Найпоширеніший із них – використання добре відомих уразливостей серверного програмного забезпечення Використовуючи ці вразливості, можна отримати доступ до комп'ютера від імені користувача, що працює з додатком (зазвичай це буває не простий користувач, а привілейований адміністратор із правами системного доступу).

Відомості про атаки на рівні додатків широко публікуються, щоб дати адміністраторам можливість виправити проблему за допомогою корекційних модулів . Однак ця ж інформація дозволяє зловмисникам використовувати виявлені уразливості. Мережевою розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних та додатків. Як правило, мережева розвідка проводиться під час підготовки більш небезпечної атаки. Мережева розвідка проводиться у формі запитів DNS, ехо-тестування та сканування портів.

Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом та які адреси цього домену надано. Ехо-тестування адрес, розкритих з допомогою DNS, дозволяє побачити, які хости реально працюють у даній середовище. Отримавши список хостів, зловмисник використовує засоби сканування портів, щоб скласти повний список послуг, що підтримуються цими хостами. Це надає зловмиснику можливість провести аналіз характеристик додатків, які працюють на хостах. Переадресація портів є різновидом зловживання довірою, коли зламаний хост використовується для передачі через між мережевий екран трафіку, який інакше був би обов'язково відбракований.

1.3 Аналіз нейромережевих моделей та методів протидії кібератакам.

У роботі запропоновано систему виявлення вторгнень з використанням СРР, призначена для розпізнавання різних видів DDoS атак. Запропоновано використовувати ДСП, структура якого адаптована до виду DDoS атаки. Як приклад рисунку 1.2 представлена архітектура ДСП, призначеного для розпізнавання мережевих кібератак, що реалізуються на рівні протоколу TCP. Запропоновано механізм роботи НР, інтегрованої у систему виявлення. Передбачається використовувати вказану систему для виявлення мережевих кібератак, сигнатури яких представлені в БД KDD-99. Для виявлення використано НСМ типу МСП та показано, що використання МСП доцільно з точки зору високої обчислювальної потужності. Крім цього, у роботі представлено опис чисельних експериментів, результати яких доводять

ефективність застосування МСП. У роботі описано бінарний нейромережевий метод (БНМ) виявлення мережевих атак. Особливістю методу є використання так званої бінарної СР, позитивними властивостями якої є можливість обробки вхідної інформації, яка має фрактальну структуру, а також пряма обчислювальна процедура навчання. У роботі запропоновано метод виділення мережевих атак із типового мережного трафіку (ВСА). Метод передбачає використання тришарового персептрон. Вибір виду НСМ та оптимізація її параметрів обґрунтовано позицій багатокритеріальної оптимізації Як критерії оптимізації використані критерії, що відображають гнучкість та функціональність НСМ.Також у роботі описано процедуру попередньої обробки параметрів мережевого трафіку, які застосовуються для складання навчальної та тестової вибірки.

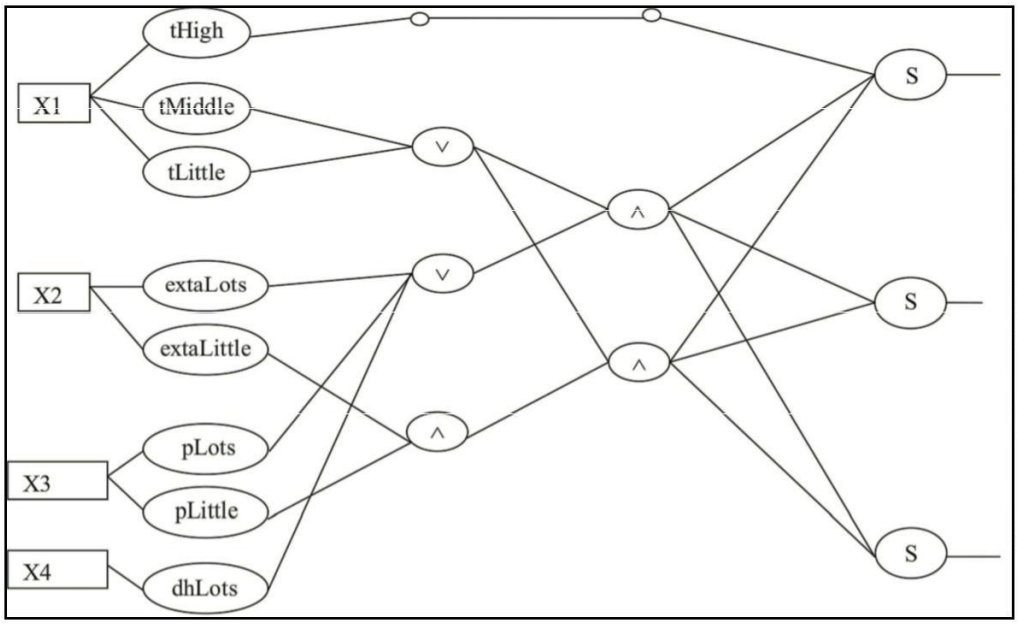

Рисунок 1.2 - Архітектура ДСП для розпізнавання мережевих кібератак рівні протоколу TCP

У роботі запропоновано метод використання нейронної гібридної мережі структури (НСГС), призначений виявлення мережевих атак на веб-сервер. Запропонована мережа – це комбінація НСМ виду ТК та МСП. Передбачено, що джерелом вхідних даних ПСМ є параметри мережевого трафіку по кожному

з протоколів IP, TCP, HTTP, HTTPS, CGI, SQLNet. Для перетворення параметрів мережного трафіку до вигляду, придатного для обробки в НСМ, використана спеціальна процедура, аналогічна процедурі обробки образів когнітивної графіки для мінімізації розмірності вхідних даних Крім цього, на одному з етапів методу реалізується оптимізація процесу навчання НМР. Критерієм оптимізації є мінімізація помилки розпізнавання. У роботах описаний спосіб виявлення DDoS-атак (СОД). Показано результати досліджень, які доводять доцільність застосування нечітких СР, які навчаються за допомогою нечітких експертних правил. Спосіб переважно орієнтований виявлення DDoS-атаки типу SYN Flood. Обґрунтовано застосування п'яти лінгвістичних змінних, що характеризують різні параметри мережного трафіку:$\boldsymbol{X_1}$– час отримання пакетів; $\boldsymbol{X_2}$ – відсоток пакетів з різних зовнішніх ір-адрес, $\boldsymbol{X_3}$ - відсоток пакетів з різних портів, $\boldsymbol{X_4}$ – відсоток пакетів із пошкодженими заголовками, $\boldsymbol{Y}$ – ступінь упевненості. Саме ці змінні є вхідними параметрами СР. Розроблено предикатні правила виду: Якщо $\boldsymbol{X_1}$ = "великий" → $\boldsymbol{Y}$ → "висока". Структура класифікатора показано рисунку 1.3. На рисунку 1.3 символом позначено нечіткий нейрон «АБО», символом – нечіткий нейрон "І", а позначення tLittle, tMiddle, tHigh, extraLittle, extraLots, pLittle, pLots, dhLots відповідають функціям активації нечітких змінних. Запропоновано подати нечіткий класифікатор у вигляді СР з прямим поширенням сигналу, що навчається за допомогою модифікованого алгоритму зворотного розповсюдження помилки. Модифікація полягає в пристосування класичного алгоритму до нечітких нейронів «І» та «АБО».

Нейросітковий підхід до виявлення мережевих атак (ПВСА) на комп'ютерні системи наведено у роботі. Акцент ставиться на розпізнавання атак, сигнатури яких представлені у БД KDD-99. Згідно даних цієї БД, кількість вхідних параметрів – 41. Як критерій вибору оптимального типу нейромережевої моделі запропоновано використовувати мінімум обсягу навчальної вибірки. Шляхом аналізу літературних джерел визначено, що до допустимих типів СР належать ТК, МСП з одним прихованим шаром нейронів

та мережу радіальної базисної функції (РБФ).

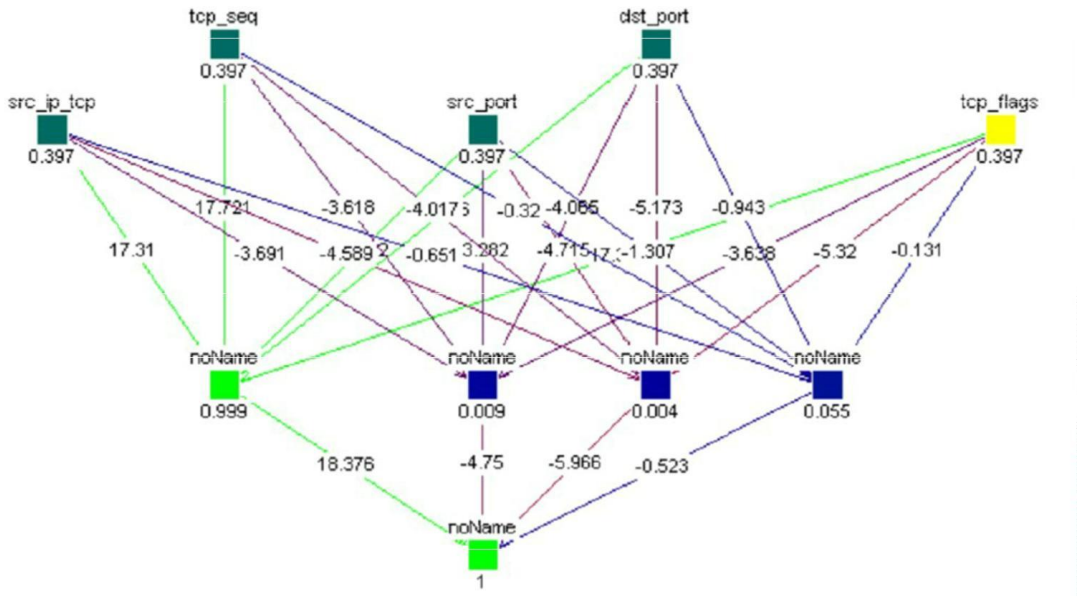

Рисунок 1.3 – Схема нечіткого класифікатора для виявлення SYN Flood-атак.

Зазначено, що для ТК мінімальний об'єм навчальної вибірки (L) має 2 рази перевищувати кількість вхідних нейронів (n), тобто:

$$L \approx 2n, \tag{1.1}$$

Для МСП та РБФ запропоновано обсяг навчальної вибірки розраховувати так:

$$L \approx W/\varepsilon \tag{1.2}$$

де W – кількість синаптичних зв'язків, ε – припустима помилка навчання.

Надалі, зроблена спроба визначити оптимальну структуру МСП. Заявлено, що певна експериментальна кількість прихованих нейронів дорівнює $m = 10$. При цьому кількість вихідних нейронів рівно 2. Відповідно до (1.1, 1.2), необхідний обсяг навчальної вибірки ТК становить $L = 82$ прикладів, а для МСП та РБФ при ε = 0.1, L = (m(n + 3) + 2) / ε = 4420. Тому оптимальним

типом НСМ обрано ТК. Зазначимо, що правильність розрахованих величин викликає сумніви, адже згідно теорії НС, при заданій точності навчання кількість прихованих нейронів МСП безпосередньо залежить від величини навчальної вибірки. Далі проводиться оптимізація структури ТК. Неявно використаний критерій максимізації точності навчання ,також використано процедуру попередньої обробки вхідних параметрів.

Адаптивна система виявлення атак (АСОА) описана також у роботі .Система призначена для розпізнавання мережевих атак та базується на спільної роботи ТК та МСП, які виконують завдання кластеризації та класифікація даних. Виявлення атак, яке проводиться у декілька етапів стало можливим завдяки тому, що в базу даних експертної системи вносилася інформація про зміни у поведінці конкретної об'єкт протягом деякого відрізка часу. Доводиться, що оптимізація архітектури дозволить підвищити точність та оперативність розпізнавання. У як вхідні дані використані параметри мережевого трафіку по протоколу TCP. Для обробки вхідних даних використано метод ковзного тимчасового вікна. ТК використана для попередньої

обробки даних, що надходять на вхід МСП, з метою їх стиснення та підвищення інформативності. Наведено математичний вираз для розрахунку частоти визначення нейрона в позиції $(\boldsymbol{i},\boldsymbol{j})$ як нейрон-переможця:

$$\Delta \mathrm{w}_{\mathrm{jk}}(i) = -\eta(y_n(i) - f(x_1))\varphi()v_n(i))y_n \qquad (1.3)$$

де η – кількість разів, коли нейрон у позиції (i, j) був переможцем,

r – відстань між центрами кластерів,

x - довжина вхідного вектора.

Надалі ця частота використовується для визначення центрів та меж кластерів. Структура МСП оптимізована з погляду обсягу контрольованих ресурсів.

Нейросітна технологія виявлення та класифікації мережевих атак (ОКСА)

описана у роботі . У технології запропоновано використання тришарової НС, яка навчається на підставі методу зворотного

поширення помилки. При цьому для розпізнавання кожного виду мережного атаки застосовується окрема СР. Як вхідні параметри пропонується використання параметрів мережного трафіку за стеком протоколів TCP/IP. У навчальну вибірку пропонується використовувати дані з бази даних KDD-99. Наведено словесний опис та фрагменти програмного коду для підготовки вхідних даних із цієї бази даних до виду вхідних параметрів СР. При цьому однією з цілей підготовки є зменшення

обсягу навчальної вибірки СР. Опис підходів до оптимізації архітектури та параметрів нейромережевої моделі відсутні.

Метод розпізнавання аномалій мережевого трафіку (РОСТ), розроблений у роботі . Методом передбачено використання СР типу МСП. В якості вхідних даних НС використано параметри заголовків IP-дейтаграм. Вибір архітектури СР базується на затвердженні про високих апроксимаційних можливостях МСП. МСП складається з трьох шарів нейронів. Кількість нейронів першого (вхідного) шару – 18, що дорівнює числу параметрів заголовка IP-дейтаграми. Кількість нейронів у вихідномушарі 2. Вихід нейрона №1 відповідає за наявність аномалії, а вихід нейрона №2 за безпечний стан трафіку. Наведено вирази для розрахунку кількості нейронів у прихованому шарі. Таким чином, метод передбачає оптимізацію параметрів архітектури СР. Для спрощення створеннярепрезентативної вибірки розроблено метод уточнюючих сигнатур, суть якого полягає у введенні додаткових штучно створених сигнатур, що описують апріорно аномальний трафік. Таким чином, у метод в неявному вигляді можна використовувати експертні дані про мережеві атаках.

У роботі запропоновано схему виявлення мережевих атак на основі комплексування нейронних, імунних та нейронечітких класифікаторів (СОСА). Основними особливостями запропонованої схеми є багаторівневий аналіз мережевого трафіку, а також використання різних адаптивних, у тому числі і нейромережевих, модулів у процесі виявлення атак. Для зменшення кількості

використовуваних для аналізу ознак запропоновано використовувати спосіб основних компонент. Проведено обчислювальні експерименти на двох відкритих наборах даних із використанням різних способів комбінування класифікаторів. У роботі запропонований метод побудови сукупного класифікатора трафіку (ПСКТ) Метод призначений для ієрархічної класифікації 22 типів мережевих атак, представлених у БД KDD-99. Для для обробки даних навчальної вибірки використаний метод головних компонент. Метод передбачає використання 22 НММ, кожна з яких має бути навчена для розпізнавання конкретного типу мережевої атаки. НСМ являє собою двошарову НС з 12 вхідними нейронами та 2 вихідними нейронами, один із яких відповідає за наявність, а другий за відсутність атаки. Як прихований шар використаний шар Кохонена. Для запобігання ситуації, коли кілька НСМ одночасно сигналізують про власне типі атаки, на другий вихід кожної з них передається мінімальне евклідове відстань між вхідним чином та еталоном:

$$E_j = \min_1 \sqrt{\left(x_1 - w_{1,j}\right)^2} + \cdots + \left(x_{12} - w_{12,j}\right)^2, \quad (1.4)$$

де x_i- і-ий вхідний параметр,

$w_{i,j}$- ваговий коефіцієнт зв'язку між i-им і вхідним та j-им прихованим нейроном.

Надалі класифікується атака, НСМ якої має мінімальну евклідову відстань. У роботі також описано механізми оптимізації навчання та функціонування НСМ.

Алгоритм перетворення параметрів трафіку (АППТ) описаний уроботі. Алгоритм призначений для отримання з мережевого трафіку вхідних даних для нейромережевої системи виявлення мережевих атак. У якій вхідна інформація зазначеного алгоритму використовуються параметри Сесії TCP. Перетворення параметрів трафіку застосовується з метою зменшення кількості вхідних параметрів СР та збільшення їх інформативності та реалізується за допомогою

математичного апарату, заснованого на методі основних компонентів. В АППТ оптимізація архітектури та параметрів нейромережевої моделі не передбачено. Також зазначимо, що роботи мають аналогічний характер.

Нейросітна система виявлення комп'ютерних атак на основі аналізу мережевого трафіку (НСОК) описано у роботі. Задекларовано розробка методу аналізу вхідного трафіку на основі тришарової СР.

Показано, що розрахунок топологи НСМ повинен бути реалізований з урахуванням заходу

Вапника-Червоненкіса виду:

$$\mathrm{K} \times \mathrm{N} \leq \mathrm{VC}_{\mathrm{dim}} \leq \mathrm{N}_{\mathrm{w}} \times (1 + \lg \mathrm{N}_{\mathrm{n}}) \qquad (1.5)$$

де N – розмірність даних на вході;

K – кількість нейронів у прихованому шарі,

N_w – загальна кількість ваги мережі,

N_n – загальна кількість нейронів мережі.

Наведено результати навчання та тестування спроектованої СР, які показують можливість її успішного застосування для вирішення завдання виявлення мережевих комп'ютерних атак. Висунуто припущення, що найкращі результати можуть бути отримані в обчислювальних системах, що використовують обмежений набір мережевого програмного забезпечення, що дозволяє більш ефективно формувати ознаки нормальної поведінки для виявлення атак.

Нейросітна технологія виявлення мережевих атак (ТОСА) на інформаційні ресурси описані в роботі. У технології передбачено модуль стиснення вхідних даних, що базується на застосуванні

нейромережевого аналога методу основних компонентів – рециркуляційної нейронної мережі (РНС)

із двома шарами нейронів. Структура РНС показана рисунку 1.4.

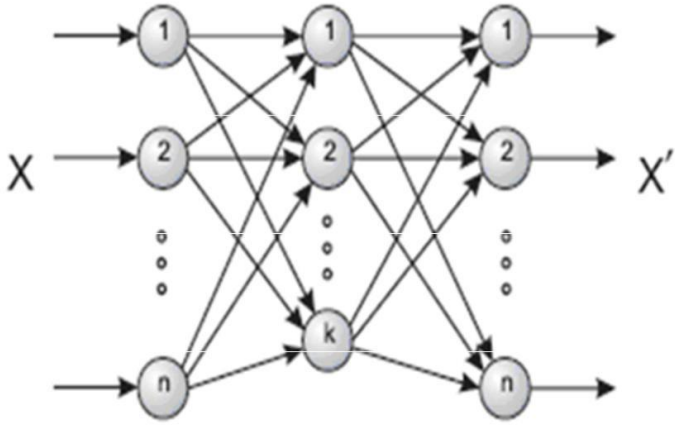

Рисунок 1.4 - Структура рециркуляційної нейронної мережі

Перший шар, що складається з k нейронів, дозволяє керувати кількістю інформаційних ознак (x), а другий шар, що складається з n нейронів, дозволяє проводити фільтрацію даних (x '). Налаштування першого шару дозволяють отримати стиснуту до k ознак форму подання вхідного n-мірного об'єкта, тобто визначити головні компоненти. У методі шляхом чисельних експериментів доведено можливість використання ТК та МСП для виявлення мережевих атак, сигнатури яких представлені у базі даних KDD-99.

У роботі запропоновано метод виявлення вторгнень у інформаційну систему з урахуванням нейронних мереж (МОВ). Вказаний метод базується на комбінованому застосуванні методів пошуку сигнатури атаки та виявлення аномалій у роботі користувача. В процесі розробки методу запропоновано підхід до вирішення задачі класифікації образів, полягає у поданні вхідних даних у вигляді сигнатур та віднесення їх до класів атаки чи безпечним процесам користувача. На основі моделі безпечної роботи користувача в ІВ та запропонованого підходу до спрощення завдання обробки інформації, синтезована структура нейромережевої системи виявлення атак Також у роботі проведено дослідження щодо визначення оптимальних параметрів алгоритмів навчання СР, що включають вибір методів формування репрезентативних учнів множин, оцінку якості функціонування СР, а також пошук оптимальних значень параметрів.

Також, запропоновано систему виявлення аномалій, використовує апарат штучних імунних систем та нейронних мереж (СОАСТ). Описуються структура, алгоритми функціонування та програмна реалізація системи виявлення аномалій В системі передбачений модуль попередньої обробки вхідних параметрів, джерелом даних для якого є статистика параметрів мережевих запитів. Обґрунтовано застосування НМР типу карти Кохонена. Описано механізм оптимізації параметрів ПСМ.

Робота присвячена розробці НСМ виявлення DDOS-атак (НСМРЧ), що навчається із застосуванням методу рою частинок. Використаний МСП з двома прихованими шарами, побудований на сигмоїдальній логістичній функції активації. Кількість вхідних сигналів – 28. У прихованих шарах кількість нейронів становить 28 та 14, у вихідному шарі міститься 2нейрону. Подана модель видає відповіді (1, 0) та (0, 1), що характеризують наявність чи відсутність атаки. Для оптимізації параметрів навчання МСП застосовано метод рою частинок, що є евристичний метод оптимізації, який, за рахунок імітації соціальної поведінки рою біологічних об'єктів, що не вимагає знання точного градієнта оптимізованої функції. У роботі розроблено відповідний математичний апарат, показано результати чисельних експериментів. У роботі запропоновано НСС виявлення мережевих кібератак на основі розпізнавання аномального мережевого трафіку (НССАСТ) Використана НСМ з прямим проходженням сигналу, що навчається за допомогою алгоритму зворотного розповсюдження помилки. Запропоновано процедуру оптимізації методу навчання Як джерело даних використана БД NSL-KDD. Система виявлення вторгнень на базі глибокої нейронної мережі (РАДНС) розроблена в роботі. Система призначена для використання у системі захисту інформації автомобілів. В системі передбачені модулі попередньої обробки вхідних даних НСМ та оптимізації процесу навчання. За допомогою експериментів показано, що використання глибокої НСМ дозволяє значно підвищити точність виявлення вторгнень. Нейромережна методологія оцінки параметрів безпеки Інтернет-орієнтованих інформаційних систем (НМОПБ) представлено також в

нашій роботі]. Серед проаналізованих дана робота є найбільш фундаментальної. У ній набули подальшого розвитку теоретичні положення побудови НСР оцінки ПБ, які полягають у розроблених підходах до розпізнавання поступових та несподіваних кібератак, визначення оптимального виду НСМ, доцільності застосування НСР, класифікації статистично подібних кібератак, застосуванні продукційних правил для подання експертних знань, параметрів оцінки ефективності НРР. Також розроблені моделі створення та використання НСР оцінки ПБ, які за рахунок застосування розроблених теоретичних положень дозволяють: визначити перелік оцінюваних ПБ, а також зменшити ресурсомісткість створення НСМ. На основі вказаних моделей розроблено низку методів, що дозволяють підвищити ефективність використання НРР. Так, метод подання експертних знань для НРР оцінки ПБ, дозволяє забезпечити оперативність розпізнавання та розширити безліч типів кібератак, котрим відсутні статистичні дані.

Метод визначення тимчасових характеристик використання НСР оцінки ПБ завдяки використанню розроблених аналітичних залежностей між очікуваними та допустимими термінами розробки забезпечує можливість визначення доцільності застосування зазначених засобів визначення ефективності розробки нейромережевих засобів оцінки параметрів безпеки за рахунок застосування запропонованих параметрів оцінки ефективності та сформованого інтегрального показника ефективності дозволяє вибрати найбільш ефективний засіб. Застосування методу дозволило визначити, що у відомих НРР розпізнавання мережевих кібератак недостатньо повно розроблений механізм формування навчальної вибірки при кодуванні очікуваного вихідного сигналу, не враховується близькість еталонів класів, що розпізнаються. Крім цього, такі засоби недостатньо адаптовані до застосування сучасних типів НММ. На основі взаємопов'язаного використання розроблених підходів, моделей та методів розроблено комплексну методологію нейромережевої оцінки ПБ, яка дозволяє значно розширити функціональні можливості НРР та вибрати з них найбільш ефективне.

З позицій сформульованої мети дослідження найбільший інтерес у цією роботі представляє запропонований список параметрів, характеризують ефективність НРР. Зазначимо, що нестача цього переліку випливає із досить загального характеру роботи, яка спрямована на оцінку ПБ для розпізнавання широкого кола кібератак та вразливостей Інтернет-орієнтованих ІС. Тому, з урахуванням зазначених раніше обмежень, при оцінці НРР розпізнавання кібератак на мережеві РІС запропонований перелік є багато в чому надлишковим. Водночас у ньому недостатньо повно враховані особливості оцінки ефективності НСР при розпізнавання мережевих кібератак.

1.4 Шляхи вдосконалення нейромережевих засобів протидії кібератакам

В результаті проведеного аналізу встановлено, що підвищення ефективності сучасних НСМ розпізнавання мережевих кібератак йде шляхом забезпечення них певних можливостей, які в характеризуються з допомогою параметрів, поданих у таблиці 1.1. Також зроблено висновок про те, що ефективність НРР розпізнавання у значній ступеня залежить від повноти та представницькості навчальної вибірки, яка застосовується для навчання сучасних НСМ, закладених у них основі, а також від того, чи враховується під час кодування очікуваного вихідного сигналу близькість еталонів розпізнаваних мережних класів кібератак. Цей висновок сформульовано на підставі аналізу результатів роботи, в якій обґрунтовано метод застосування СР для розпізнавання голосові сигнали. За рахунок цього, запропоновано використання параметрів E_{OB} та E_{KBC}, опис яких також наведено в таблиці 1.1. Надалі представлений у таблиці 1.1 перелік параметрів може бути розширено.

Таблиця 1.1 – Параметри оцінки ефективності нейромережевих засобів

Назва параметра	Опис параметра
$E_{по}$	Попередня обробка вхідних параметрів
$E_{ота}$	Оптимізація типу архітектури

$E_{опа}$	Оптимізація параметрів архітектури
$E_{омо}$	Оптимізація методу навчання
$E_{веп}$	Можливість навчання за допомогою експертних правил
$E_{пна}$	Можливість застосування у методі перспективних типів нейромережевих архітектур
$E_{оцп}$	Можливість принципової оцінки доцільності застосування СР для вирішення поставленого завдання
$E_{ов}$	Наявність процедури формування навчальної вибірки з різнорідних статистичних даних
$E_{квс}$	Наявність процедури кодування очікуваного вихідного сигналу НСМ, що враховує близькість еталонів класів мережевих кібератак, що розпізнаються.

Величини запропонованих параметрів у першому наближенні можна оцінити за бінарною шкалою: 0 або 1. Параметр дорівнює 0, коли відповідна можливість у НРР не забезпечується і 1 у протилежному випадку. Для проаналізованих випадків величини зазначених параметрів наведено в таблиці 1.2. При цьому для всіх проаналізованих методів $E_{квс} = 0$. Тобто більшості з проаналізованих методів не реалізовано процедуру формування навчальної вибірки. Крім того, використання запропонованих критеріїв дозволяє визначити інтегральний показник ефективності НРР (E_{Σ}) за допомогою наступного виразу:

$$E_{\Sigma} = \sum_{i=1}^{9} \alpha_i E_i \tag{1.6}$$

де α_i – ваговий коефіцієнт і-го критерію.

Визначити найбільш ефективну НРР можна, скориставшись виразом:

$$\max_{E_i} = \{E_1, E_2, .. E_I\} \tag{1.7}$$

Де I – кількість видів НСМ, E_i – інтегральний показник ефективності і-го НСР.

У загальному випадку визначення вагових коефіцієнтів потребує окремого дослідження, а базовому варіанті можна припустити, що $\alpha_1 = 1$.

Таблиця 1.2 – Величини параметрів, що характеризують ефективність нейромережевих моделей та методів

МЕТОД	ПАРАМЕТР								
	$E_{ПО}$	$E_{ОТА}$	$E_{ОПА}$	$E_{ОМО}$	$E_{БЕП}$	$E_{ПНА}$	$E_{ОПП}$	$E_{ОБ}$	$E_{КВС}$
АППТ	1	0	0	0	0	0	0	0	0
НСОВ	0	1	0	0	0	0	0	0	0
ТОСА	1	1	0	0	0	0	0	0	0
РАСТ	0	1	1	0	0	0	0	0	0
ВСА	0	1	1	0	0	0	0	0	0
ПСКТ	1	0	0	0	0	0	0	0	0
ПВСА	1	1	0	1	0	0	0	0	0
АСОА	1	1	1	0	0	0	0	0	0
СОД	0	1	0	1	0	0	0	0	0
БНМ	0	1	0	1	0	0	0	1	0
ОКСА	1	0	0	0	0	0	0	1	0
МОВ	1	0	0	0	0	0	0	0	0
НСОК	1	0	0	0	0	0	0	0	0
НСГС	1	0	0	0	0	0	0	1	0
СОСА	1	0	0	0	0	0	0	1	0
НМОПБ	1	1	1	1	1	1	1	0	0
СОВНС	1	0	1	0	0	0	0	0	0
СОАСТ	1	1	1	1	0	0	0	0	0
НСМРЧ	1	0	0	1	0	0	0	0	0
НССАСТ	1	0	1	1	0	0	0	0	0
СОВГНС	1	0	1	1	0	1	0	0	0

Зазначимо, що практична цінність даних таблиці 1.2 полягає у окреслення недоліків та перспектив удосконалення сучасних нейромережевих методів та моделей. Наприклад, величина $E_{ОТА} = 0$ свідчить про те, що до недоліків методу АППТ можна віднести недостатню оптимізацію виду архітектури НМР. Це свідчить про можливість ідповідного вдосконалення вказаних методів. При цьому величина параметра E_{Σ} дозволяє оцінити інтегральну ефективність нейромережевого методу. Також у результаті проведеного аналізу доведено, що у сучасних СРК в основному використовуються класичні типи НСМ, які в тій чи Іншою мірою адаптовані до умов поставленого завдання. Це дозволяє звузити коло допустимих сучасних видів НСМ, що у свою чергу дозволяє підвищити оперативність визначення моделі, оптимальної з точки зору

поставленого завдання. Таким чином, з'являється можливість підвищення оперативності створення відповідних СРК.

В результаті аналізу науково-практичних робіт присвячених розробці та експлуатації систем розпізнавання кібератак на мережеві ресурси інформаційних систем загального призначення показано, що однією з основних шляхів розвитку зазначених систем є впровадження в них методів аналізу мережевого трафіку, що базуються на сучасних рішеннях теорії штучних нейронних мереж. Також визначено, що актуальним завданням є впровадження нейромережевих засобів розпізнавання у мережеві системи розпізнавання кібератак, що використовують метод визначення зловживань для розпізнавання кібератак типу IP-спуфінг, відмова в обслуговуванні, підбір парольних даних, атака на рівні додатків, мережевої розвідки та переадресація портів. Також аналіз нейромережевих методів розпізнавання мережевих кібератак. дозволив визначити, що підвищення їх ефективності багато в чому пов'язане з адаптацією до очікуваних умов експлуатації, які багато в чому залежать від умов формування прикладів навчальної вибірки. Ще одним напрямом підвищення ефективності є використання сучасних видів нейромережевих моделей, що дозволяють у різних умовах експлуатації забезпечити високу точність розпізнавання кібератак У результаті виникає необхідність удосконалення методологічної бази нейромережевого розпізнавання мережевих кібератак та розробки на цій базі методу створення навчальної вибірки та методу створення, відповідних нейромережевих засобів. Для апробації запропонованих рішень доцільно розробити нейромережну систему та провести дослідження її ефективності.

2. РОЗВИТОК МЕТОДОЛОГІЧНОЇ БАЗИ НЕЙРОМЕРЕЖОВОГО ПРОТИДІЇ КИБЕРАТАКАМ НА ІНФОРМАЦІЙНИХ СИСТЕМ

2.1 Концептуальна модель забезпечення ефективності нейромережевої протидії кібератакам

Результати досліджень, проведених у першому розділі даної кваліфіц роботи, вказують на те, що важливим напрямком розвитку СПА на мережеві РІС є впровадження в них НРР розпізнавання кібератак. Для цього необхідно вирішити наукове завдання нейромережевого розпізнавання. кібератак на основі аналізу підконтрольних на експлуатації параметрів функціонування ІВ. Особливістю сформульованого завдання є необхідність теоретичного обґрунтування характеристик нейромережевих моделей та методів, адаптованих до умов впровадження у сучасні СПА. До вказаних умовам належать допустимий термін розробки, можливість залучення трудових ресурсів, наявність доступу до баз даних шаблонів атак та шаблонів нормальної поведінки, необхідні навчання НСМ, особливості системи контролю функціональних параметрів ІВ та допустимий обсяг обчислювальних ресурсів, що споживає СПА. Вирішення цього наукового завдання дозволить вирішити практичне завдання розпізнавання мережевих кібератак на підставі схожості параметрів мережевого трафіку із сигнатурами (шаблонами) відомих мережевих кібератак. При цьому завдання фіксації параметрів функціонування ІВ, попередньої фільтрації таких параметрів, а також сигналізації про виявлені кібертаки вважаються вирішеними і в цій кваліфікаційній роботі не розглядаються. Відповідно до певних рекомендацій, відправним пунктом рішення сформульованого завдання стала розробка концептуальної моделі забезпечення ефективності нейромережевого розпізнавання кібератак на мережеві РІС. У зв'язку з тим, що очікуваний практичний результат кваліфікаційної роботи передбачає створення програмно-апаратного комплексу, то для визначення ефективності процесу нейромережевого

розпізнавання кібератак на мережеві РІС передбачено використовувати термінологію в галузі захисту інформації, комп'ютерної та програмної інженерії. Також визначено, що в контексті завдання даного кваліфікаційного дослідження концептуальна модель, перш за все, призначена для формалізації причинно-наслідкових зв'язків, які властиві процесу розпізнавання кібератак на мережеві РІС, визначених необхідністю підвищення рівня захищеності сучасних ІС. Крім цього, в концептуальної моделі враховано:

− Умови функціонування НСР розпізнавання кібератак на мережеві РІС, обумовлені характером взаємодії окремих частин СПА та компонентами ІВ.

− Необхідність реалізації ефективного використання НСМ для розпізнавання кібератак функціонування і основні напрями покращення його

− Можливість управління НСР та визначення його настроюваних змінних.

На наступному етапі побудови концептуальної моделі з урахуванням загальноприйнятою технологією використання НСМ визначено, що процес нейромережевого розпізнавання кібератакповинен передбачати формування параметрів навчальних прикладів, формування навчальної вибірки, визначення виду та параметрів НСМ та використання НСМ для розпізнавання.

Призначення складових даної діаграми полягає в наступному:

− Формування параметрів навчальних прикладів – визначення для кожного виду кібератак безлічі вхідних та вихідних параметрів та способу їх кодування.

− Формування навчальної вибірки – визначення такої множини навчальних прикладів, що відповідає стандартам кібератак. Кількість, якість та номенклатура прикладів мають бути достатніми для навчання НМР.

− Визначення виду та параметрів НСМ – визначення для використання такого виду НСМ, з такими параметрами, які найповніше відповідають умов завдання розпізнавання кібератак на мережеві ресурси конкретної ІС.

− Використання НСМ – розпізнавання кібератак на мережевих РІС. Слід врахувати, що використання НСМ спричиняє додаткове навантаження на ІВ, що може спричинити вичерпання обчислювальних ресурсів.

Використання цього твердження дозволило побудувати показану на рисунку 2.1 діаграму декомпозиції нейромережевого розпізнавання кібератак на мережеві РІС.

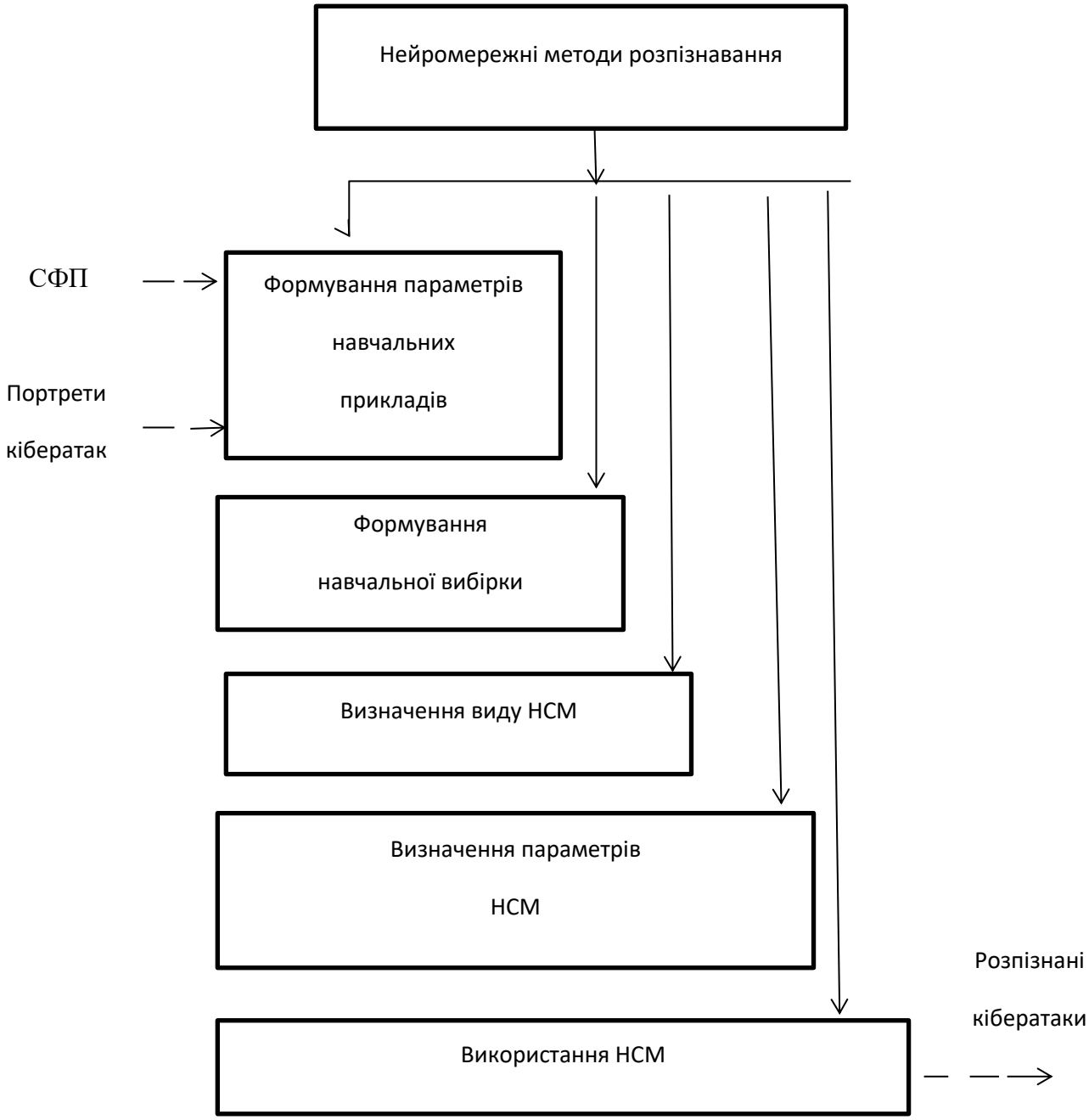

Рисунок 2.1 – Діаграма декомпозиції нейромережевого розпізнавання кібератак

Наступним етапом створення концептуальної моделі стала розробка показаної на рисунку 2.2 схеми компонентів НСС розпізнавання кібератак. У схемі враховано особливості реалізації НСС, призначені для розпізнавання кібератак на мережеві РІС, та результати розділу 1, які стосуються недоліків відомих НСР для розпізнавання кібератак на мережеві МАЛ.

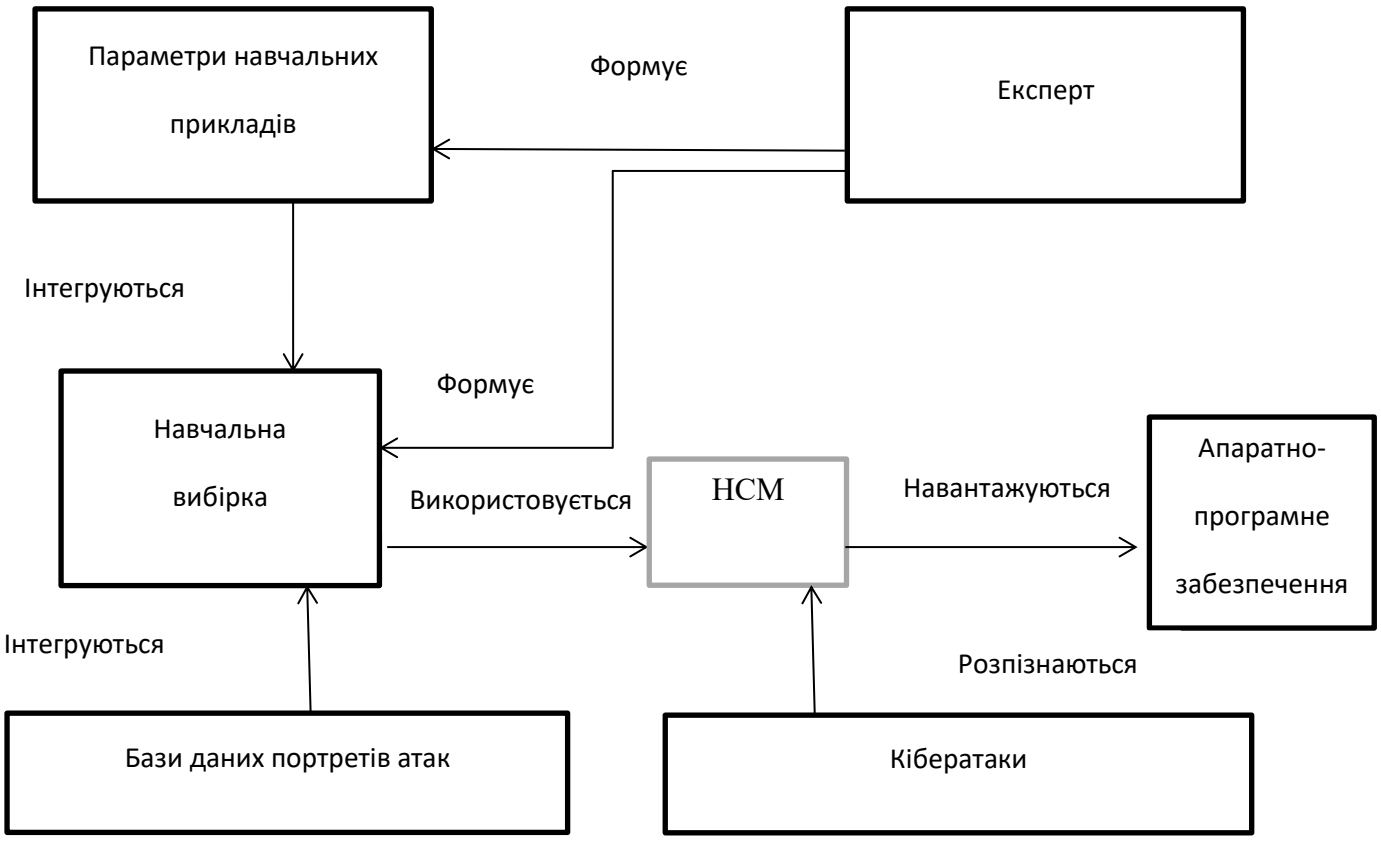

Рисунок 2.2 – Схема взаємодії компонентів НСС розпізнавання кібератак

Таким чином, у процесі розробки враховано:

− Недосконаліть методів формування параметрів навчальних прикладів для НММ, призначених для розпізнавання кібератак на мережеві РІС.

− Тривалий період формування навчальної вибірки для НСМ у разіобмежений доступ до баз даних портретів кібератак.

−Складність доступу до існуючих баз даних портерів кібератак.

− Додаткове навантаження на апаратно-програмне забезпечення ІС за рахунок функціонування НРР.

Тому у схемі передбачена можливість формування параметрів навчальних прикладів та навчальної вибірки за допомогою експертних даних. Аналіз даних, показаних на рисунку 2.1 та рисунку 2.2, дозволяє стверджувати, що на ефективність нейромережевого розпізнавання кібератак на мережеві РІС впливають ряд чинників, показаних рисунку 2.3

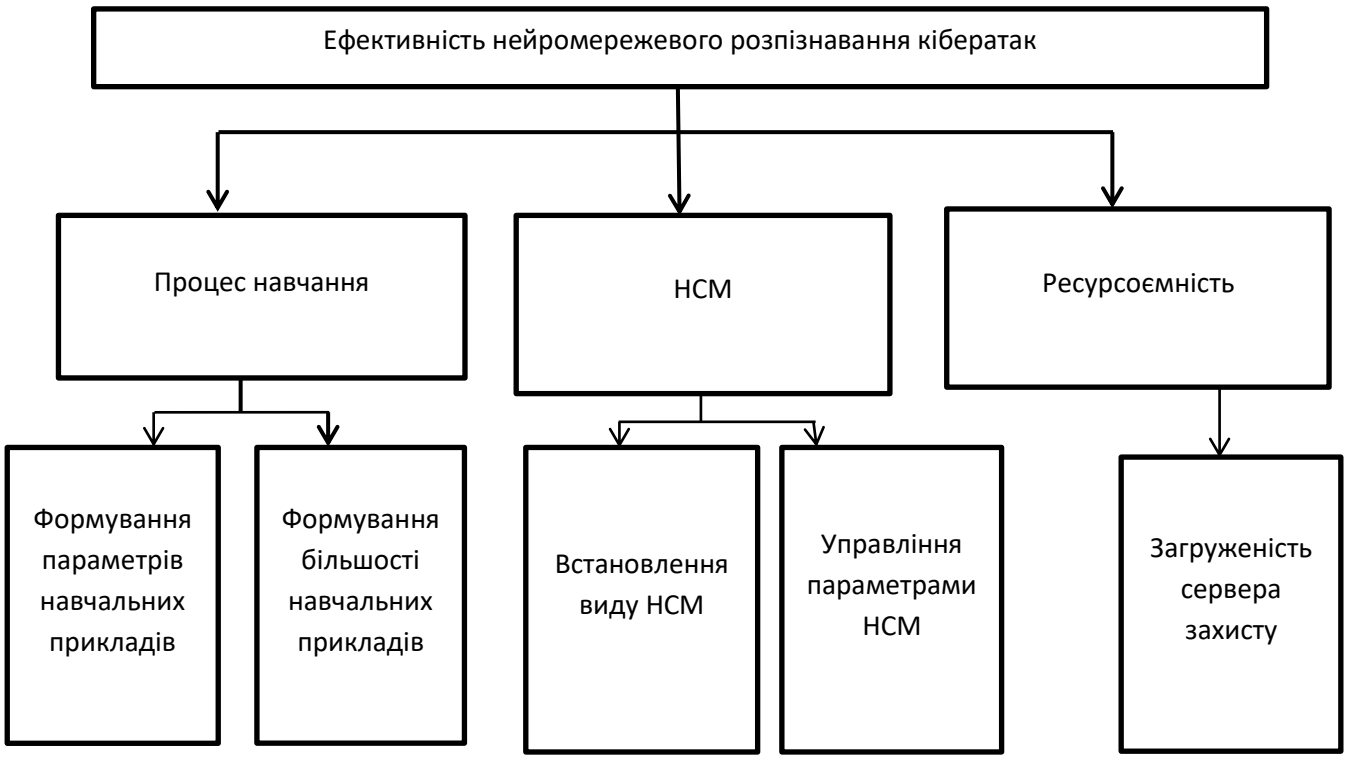

Рисунок 2.3 - Фактори, що впливають на ефективність розпізнавання

Окрім цього, можна стверджувати, що ефективність нейромережевого розпізнавання доцільно оцінювати як з точки зору ефективності процесу використання НСР, так і з точки зору ефективності процесу навчання НСМ. При цьому показники ефективності мають відображати тривалість, ресурсоємність і точність названих процесів. Таким чином, обґрунтовано показані на рисунку 2.4 показники оцінки ефективності нейромережевого розпізнавання кібератак на мережеві РІС.

У результаті визначено, що в аналітичному вигляді концептуальну модель забезпечення ефективності процесу нейромережевого розпізнавання кібератак на мережеві РІС можна відобразити за допомогою виразів:

$$E_{\Sigma} = f(E_{НСР}, E_{ОВ}) \quad (2.1)$$

$$E_{НСР} = f(e_1, e_2, e_3,) \quad (2.2)$$

$$E_{ОВ} = f(e_4, e_5) \quad (2.3)$$

де E_{Σ} - інтегральна ефективність процесу, $E_{\text{НСР}}$ - ефективність створення і використання НСР, $E_{\text{ОВ}}$ - ефективність створення навчальної вибірки, e_1 – e_2- визначення параметрів НСР, e_3 - ресурсоємність використання НСР, e_4 - визначення параметрів навчальних прикладів, e_5 - формування навчальних прикладів. визначення ефективних видів НСМ, e_2 - визначення параметрів НСМ, e_3 - ресурсоємність використання НСР, e_4 - визначення параметрів навчальних прикладів, e_5 - формування навчальної вибірки.

Рисунок 2.4 - Показники оцінювання ефективності нейромережевого розпізнавання

Аналіз розробленої концептуальної моделі дає змогу стверджувати, що для ефективного нейромережевого розпізнавання кібератак необхідно доповнити методологічну базу низкою принципів і заснованих на них моделей процесів використання НСР. Надалі необхідно застосувати отримані елементи методологічної бази для розроблення нейромережевих моделей і методів розпізнавання мережевих кібератак.

2.2 Принципи використання нейронних мереж

Принцип допустимості використання виду НСМ для розпізнавання кібератак на мережеві РІС. Як показують результати першого розділу, основним фактором, який впливає на формування безлічі допустимих видів НСМ, є можливість їхнього ефективного навчання. Для цього за допустимий час необхідно: визначити безліч вхідних і вихідних параметрів НСМ, провести кодування зазначених параметрів, створити навчальну вибірку, реалізувати процес навчання. Виконання першої процедури реалізується на підготовчому етапі розроблення НСР. Тому увагу акцентовано на другу і третю процедури. При цьому прийнятний термін створення навчальної вибірки і навчання НСМ визначається на підставі вимог до створення СПА:

$$t_{\Sigma} \leq t_d \tag{2.4}$$

де t_{Σ} - загальний строк навчання НСМ розпізнавання кібератак, t_d - прийнятний строк створення НСР розпізнавання кібератак.

Таким чином, принцип допустимості використання і-го виду НСМ можна задати за допомогою правила:

$$If\ t_{\Sigma}(net_i) \leq t_d \rightarrow net_i \in Net_d \tag{2.5}$$

де net_i - i -ий вид НСМ;

net_d - множина допустимих видів НСМ.

Принцип визначення множини ефективних видів НСМ для розпізнавання кібератак на мережеві РІС. Відповідно до результатів п. 1.3 та висновків [8] для визначення множини видів НСМ, що забезпечать ефективне розпізнавання кібератак на мережеві РІС, пропонується використовувати процедуру вигляду:

$$Net_a \rightarrow Net_d \rightarrow Net_e \tag{2.6}$$

де $\mathrm{Net}_{\mathrm{a}}$ – множина доступних видів НСМ;

$\mathrm{Net}_{\mathrm{d}}$ – множина допустимих видів НСМ,

$\mathrm{Net}_{\mathrm{e}}$ – множина ефективних видів НСМ.

Принцип оцінювання ефективності виду НСМ, призначеної для розпізнавання кібератак на мережеві РІС. За аналогією з [21] вважатимемо, що серед множини допустимих і-ий вид НСМ є найефективнішим, якщо для нього функція ефективності набуде максимального значення:

$$\underset{V_1}{\mathrm{Max}} = \{V_1, V_2, .. V_1\} \tag{2.7}$$

де I - кількість видів НСМ;

V_i - функція ефективності i-го виду НСМ.

Розрахунок функції ефективності виконується так:

$$V_i = \sum_{k=1}^{K} a_k R_k(net_i),\ net_i \in net_d, i = 1, \dots I \tag{2.8}$$

де $\alpha_k = [0..1]$ ваговий коефіцієнт k-го критерію ефективності;

net_i - i-ий вид НСМ;

Net_d - множина допустимих видів НСМ;

K - кількість критеріїв ефективності; виду;

$R_k(net_i)$ - значення *k*-го критерію для НСМ *i*-го Відповідно до результатів [9 с. 27 - 30, 24], під *k*-им критерієм визначення ефективності виду НСМ розумітимемо міру забезпечення в НСМ *k*-ї вимоги задачі розпізнавання мережевих кібератак.

Принцип визначення очікуваного вихідного сигналу НСМ для портретів кібератак. Значення вихідного сигналу має відображати схожість навчальних прикладів. У протилежному випадку навчання НСМ може істотно погіршитися. Тому вихідний сигнал для портретів кібератак пропонується описати виразом:

$$Y_\phi = f(d_\phi) \tag{2.9}$$

де Y_Φ - очікувані вихідні сигнали НСМ для кібератак виду Φ;

d_Φ - множина мір схожості між компонентами Φ .

Принцип використання експертних знань для формування навчальної вибірки. За аналогією з [28], цей принцип передбачає, що навчальні приклади можна формувати на підставі експертних знань щодо кібератак у вигляді продукційних правил виду:

$$If\ x_1 \in \left[X_1^{min}, X_1^{max}\right]_l \wedge \ldots x_k \notin \left[X_k^{min}, X_k^{max}\right]_l \ldots \wedge x_K \in \left[X_K^{min}, X_1^{max}\right]_l \rightarrow Y \tag{2.10}$$

де $x_1, \ldots x_K$ - параметри, що ідентифікують кібератаку;

$[x_1^{min}, x_1^{max}], \ldots, [x_K^{min}, x_K^{max}]$ - задані діапазони $x_{1,\ldots}\, x_{k,}$

K - кількість ідентифікуючих параметрів,

Y - результат продукційного правила (очікувана кібератака).

Розроблені принципи стали основою для створення моделей процесів використання НСМ для розпізнавання кібератак.

2.3 Модель правил визначення ефективних видів нейромережевих моделей

Деталізувавши вираз (2.5), який відповідає принципу допустимості використання і-го виду НСМ для розпізнавання кібератак на мережеві РІС, отримаємо:

$$t_{\Sigma}(net_i) = t_v + t_l(net_i) \tag{2.11}$$

де t_v - час створення навчальної вибірки, $t_l\ (net_i\ )$ - час визначення параметрів моделі для *i*-го виду НСМ.

Зазначимо, що в першому наближенні значення $t_l\ (net_i\ )$ приблизно дорівнює часу визначення вагових коефіцієнтів синаптичних зв'язків НСМ. При цьому, з погляду розв'язання задачі визначення тільки принципової можливості використання певного виду НСМ, створення навчальної вибірки зводиться до формування такої кількості навчальних прикладів, яку вважають достатньою для якісного навчання НСМ.

В соответствии с [17], это количество зависит от количества входных параметров НСМ и в базовом случае рассчитывается так:

$$P_{min} \approx 10N_x \tag{2.12}$$

де P_{min} – мінімально допустима кількість навчальних прикладів, N_x – кількість вхідних параметрів НСМ.

Також можна прийняти, що:

$$t_v = \bar{t_v} P_{min} \tag{2.13}$$

де $\bar{t_v}$ - середній час створення одного навчального прикладу.

Очевидно, що величина $\bar{t_v}$ є індивідуальною для конкретного мережевого РІС і залежить від багатьох чинників: організації процесу створення навчальної

вибірки, апаратно-програмного забезпечення тощо. Визначити величину $\bar{t}_v$ можливо шляхом експертного оцінювання.

Після підстановки (2.12) у (2.13) отримаємо:

$$t_v = 10\bar{t}_v N_x \tag{2.14}$$

Своєю чергою, згідно з даними [7], для приблизної оцінки часу визначення значень вагових коефіцієнтів синаптичних зв'язків НСМ необхідно врахувати вид цієї моделі, швидкість її апаратно-програмної реалізації, кількість навчальних прикладів, кількість вхідних і вихідних параметрів, а також допустиму величину помилки навчання.

За певної структури для НСМ *i*-го виду тривалість процесу визначення вагових коефіцієнтів можна оцінити так:

$$t_l(net_i) = \tau \times L_i \times W_i \times K_{o,i} \tag{2.15}$$

де τ - тривалість однієї навчальної ітерації для одного синаптичного зв'язку; W_i - кількість синаптичних зв'язків для *i*-го виду НСМ; L_i - кількість нейронів; це $K_{o,i}$ - кількість ітерацій у процесі навчання.

При цьому

$$K_{o,i} = f_{o,i}(\varepsilon, P) \tag{2.16}$$

де $f_{o,i}$ $(\varepsilon\ ,P)$- залежність кількості ітерацій від помилки навчання і кількості навчальних прикладів для НСМ *i*-го виду; - допустима помилка навчання НС; *P* - кількість навчальних прикладів.

Відповідно до [10], під час приблизних розрахунків для множини видів НСМ $\boldsymbol{net_1}$, що складається з НСМ на основі PNN, мережі адаптивної резонансної теорії, ТК, РБФ, АНС, що навчаються шляхом безпосереднього запам'ятовування навчальних прикладів або з використанням правил Гебба,

Ойя, корелятивного чи дельта правил, для оцінювання тривалості навчання можна використати вираз (2.17). Для оцінки тривалості навчання множини видів НСМ $\boldsymbol{net_2}$, що складається з НСМ, які базуються на МСП і навчаються за допомогою градієнтних методів або генетичних алгоритмів, можна використовувати вираз (2.18).

$$t_l(net_1) \approx k_1 \tau e^{-\varepsilon} P(N_x + N_y) \quad (2.17)$$

$$t_l(net_2) \approx k_2 \tau e^{-\varepsilon} P^2 (N_x + N_y)^2 \quad (2.18)$$

де $t_1\,(net_1)$– тривалість визначення вагових коефіцієнтів для видів НСМ, які належать до net_1 ; $t_1\,(net_2)$– тривалість визначення вагових коефіцієнтів для видів НСМ, які належать до net_2 ; k_1 - коефіцієнт пропорційності для видів НСМ, які входять до net_1; τ - тривалість однієї обчислювальної операції процесу навчання; P - кількість навчальних прикладів; N_y - кількість вихідних параметрів; k_2 - коефіцієнт пропорційності для видів НСМ, які входять до net_2 ; - емпіричний коефіцієнт.

Зазначимо, що вирази (2.17, 2.18) отримано за умови послідовного обчислення сигналів штучних нейронів, що входять до складу НСМ, що є характерним за її загальноприйнятої реалізації на поширеній комп'ютерній техніці. Крім цього, прийнято передумову, що структура НСМ та обчислювальні можливості виду НСМ достатні для отримання допустимої помилки навчання.

Як свідчать результати першого розділу, з точки зору розпізнавання кібератак на мережеві РІС найбільш перспективними видами НСМ є РБФ, ТК, МСП, PNN, ГНС. Для РБФ, ТК і PNN приблизну тривалість навчання можливо оцінити за допомогою виразу (2.17), а для МСП і ГНС доцільно використовувати вираз (2.18). Відповідно [7], для заданої програмної реалізації НСМ тривалість однієї обчислювальної операції процесу

навчання (τ) здебільшого залежить від обчислювальної потужності апаратного забезпечення контуру розпізнавання кібератак у системі захисту мережевих РІС.

Допустиму помилку навчання НСМ (ε) можна розрахувати за допомогою [20] на підставі вимог до точності розпізнавання кібератак на мережеві РІС. У першому наближенні величини τ і ε можливо визначити шляхом експертного оцінювання.

При визначенні принципової можливості використання НСМ доцільно орієнтуватися на мінімально допустиму кількість навчальних прикладів. Враховуючи в (2.17) і (2.18) залежність (2.12), отримаємо:

$$t_l(net_1) \approx 10k_1\tau e^{-\varepsilon}N_x(N_x + N_y) \quad (2.19)$$

$$t_l(net_1) \approx 10k_2\tau e^{-\chi\varepsilon}N_x^2(N_x + N_y)^2 \quad (2.20)$$

Підстановка (2.14, 2.19) і (2.14, 2.20) у (2.11) дає змогу деталізувати вираз для розрахунку загального часу навчання НСМ:

$$t_\Sigma(net_1) \approx 10\overline{t_v}N_x + 10k_1\tau e^{-\varepsilon}N_x(N_x + N_y) \quad (2.21)$$

$$t_\Sigma(net_2) \approx 10\overline{t_v}N_x + 100k_2\tau e^{-\chi\varepsilon}N_x^2(N_x + N_y)^2 \quad (2.22)$$

де $t_\Sigma(net_1)$ – загальний час навчання для НСМ зі складу net_1; $t_\Sigma(net_2)$- загальний час навчання для НСМ зі складу net_2 . Після тривіальних спрощень (2.21, 2.22) отримаємо:

$$t_\Sigma(net_1) = 10N_x(\overline{t_v} + k_1\tau e^{-\varepsilon}(N_x + N_y)) \quad (2.23)$$

$$t_\Sigma(net_2) = 10N_x(\overline{t_v} + 1 - k_2\tau e^{-\chi\varepsilon}N_x(N_x + N_y)) \quad (2.24)$$

Результати теоретичних праць, присвячених НС [17], дають змогу стверджувати, що $k_1 \approx 0{,}1$, $k_2 \approx 0{,}001$, $\chi \approx 1$. Також на підставі [33] шляхом експертного оцінювання визначено, що максимально допустима помилка навчання НСМ, що використовуються в системі розпізнавання кібератак на

мережеві РІС, $\varepsilon \approx 0{,}05$. Підставивши зазначені величини в (2.23, 2.24), отримаємо:

$$t_{\Sigma}(net_1) \approx 10N_x(\overline{t_v} + 0{,}1\tau e^{-0{,}05}(N_x + N_y)) \quad (2.25)$$

$$t_{\Sigma}(net_2) \approx 10N_x(\overline{t_v} + 0{,}01\tau e^{-0{,}05}N_x(N_x + N_y)) \quad (2.26)$$

Враховуючи, що $e^{-\mathbf{0.05}}$= 0,951229 ≈ 1, отримаємо:

$$t_{\Sigma}(net_1) \approx 10N_x(\overline{t_v} + 0{,}1\tau(N_x + N_y)) \quad (2.27)$$

$$t_{\Sigma}(net_2) \approx 10N_x(\overline{t_v} + 0{,}01\tau N_x(N_x + N_y)) \quad (2.28)$$

Результати першого розділу і дані [58] вказують на те, що в першому наближенні під час розпізнавання мережевих кібератак множина вхідних параметрів НСМ може відповідати безлічі параметрів мережевого трафіку.

Також дані [8] свідчать про те, що кількість елементів кожної із зазначених множин не перевищує 50. Оскільки на вхід НСМ, крім безпосередньо зареєстрованих параметрів, можуть подаватися й інші параметри, у першому наближенні приймемо, що кількість вхідних параметрів НСМ $N_x = 50...100$. Оскільки вирази (2.25, 2.26) мають приблизний характер і орієнтуючись на визначення максимального терміну навчання приймаємо:

$N_x + N_y \approx 100$. Ця передумова дає змогу модифікувати (2.29, 2.30) таким чином:

$$t_{\Sigma}(net_1) \approx 1000(\overline{t_v} + 10\tau) \quad (2.29)$$

$$t_{\Sigma}(net_2) \approx 1000(\overline{t_v} + 100\tau) \quad (2.30)$$

Оскільки $t_{\Sigma}(net_1) > t_{\Sigma}(net_2)$, то з урахуванням виразів (2.29, 2.30) правило визначення допустимості використання виду НСМ для розпізнавання кібератак на мережеві РІС (2.6) можна деталізувати таким чином:

$$If 1000\ (\bar{t_v} + 10\tau) \leq t_d \rightarrow net_1 \in Net, \quad (2.31)$$

$$If 1000(\bar{t_v} + 10\tau) \leq \bar{t}_d \rightarrow Net = \{net_1, net_2\} \quad (2.32)$$

Умова (2.31) визначає допустимість використання для розпізнавання кібератак на мережеві РІС НСМ на основі АНС, ТК, СНС, РБФ, PNN, мереж адаптивної резонансної теорії. Умова (2.32) доповнює допустиму множину НСМ моделями на основі МСП і ГНС.

Розглянемо приблизну оцінку допустимого терміну створення НСМ розпізнавання кібератак на мережеві РІС. Врахуємо, що розробка зазначеної НСМ є лише однією зі складових загального процесу створення СЗІ. Тому

$$t_d = k_{nsm} \times t_{max} \quad (2.33)$$

де t_{max} - максимально допустимий строк розроблення СЗІ; k_{nsm} - коефіцієнт пропорційності між t_d і t_{max} . Відповідно до [97], під час оціночних розрахунків можна прийняти, що тривалість розроблення НСМ займає приблизно чверть усього терміну створення ЗЗІ. Тому:

$$k_{nsm.} \approx 0{,}25. \quad (2.34)$$

Використавши (2.36), вирази (2.33, 2.34) модифіковано так:

$$If 1000(\bar{t_v} + 10\tau) \leq 7{,}5 \times 10^6 \rightarrow net_1 \in Net \quad (2.35)$$

$$If 1000(\bar{t_v} + \tau) \leq 7{,}5 \times 10^6 \rightarrow Net = \{net_1, net_2\} \quad (2.36)$$

Вирази (2,31, 2.32, 2.35, 2.36) є правилами для визначення допустимих видів НСМ, призначених для розпізнавання кібератак на мережеві РІС. Застосування цих правил до множини доступних НСМ дає змогу перейти до

визначення множини ефективних видів НСМ. Для цього сформовано відповідну множину критеріїв ефективності. Розробка базувалася на запропонованому принципі оцінювання ефективності НСМ, призначених для розпізнавання кібератак на мережеві РІС. Також використано результати [33], у яких визначено перелік критеріїв ефективності оцінювання параметрів безпеки ІС. У процесі розроблення визначено, що з позицій кваліфікаційного дослідження, вимоги до НСМ характеризують їхню здатність до навчання, обчислювальні можливості та технічну реалізацію. У свою чергу вимоги до здатності до навчання визначаються можливостями:

– Використання прикладів з різною кількістю вхідних параметрів. Ця вимога істотно спрощує організацію процесу збирання та попереднього опрацювання реальних статистичних даних.

– Використання навчальної вибірки, обсяг якої менший за кількість вхідних параметрів, тобто на вибірці в ≤100 прикладів. Виконання цієї вимоги дає змогу розпізнавати нові види кібератак, статистика яких непредставницька.

– Непропорційного представлення в навчальній вибірці розпізнаваних класів.

– Застосування навчальних прикладів, у яких відсутній очікуваний вихідний сигнал.

– Навчання на зашумлених навчальних прикладах.

– Засвоювати навченій НСМ нові навчальні приклади без повного перенавчання.

– Паралельного навчання. У цьому випадку НСМ може навчатися по частинах.

– Стабільного навчання. У цьому випадку НСМ за прийнятний період навчання гарантовано забезпечує достатню похибку навчання, яка в теорії

НС традиційно розраховується за допомогою виразу:

$$\varepsilon = N_{true} \,/\, N_{\Sigma} \tag{2.37}$$

де N_{true} - кількість правильно розпізнаних навчальних прикладів;

N_{Σ} - загальна кількість навчальних прикладів.

– Мінімізації терміну навчання, який в основному визначається кількістю навчальних ітерацій. Зазначимо, що тривалість навчання НСМ зі складу множини net1, можливо цінувати за допомогою виразу (2.29), а тривалість навчання НСМ зі складу net2 - за допомогою виразу (2.30).

– Забезпечити високий рівень автоматизації навчання, що в разі використання якісної навчальної вибірки залежить від кількості параметрів НСМ, які емпірично налаштовуються.

– Можливість подання в НСМ явних експертних знань.

– Вимоги до обчислювальних ("інтелектуальних") можливостей НСМ визначаються.

– Відношенням кількості навчальних прикладів, які може запам'ятати НСМ до кількості синаптичних зв'язків у цій моделі.

– Помилкою інтерполяції даних, що характеризує можливість правильного розпізнавання прикладів, які хоча й не ввійшли до навчальної вибірки, але параметри яких перебувають між межами параметрів навчальних прикладів.

– Помилку екстраполяції даних, яка характеризує можливість правильного розпізнавання прикладів, параметри яких лежать поза межами параметрів навчальних прикладів.

– Можливістю вербалізації навченої НСМ, що має на увазі під собою забезпечення отримання явних правил, за допомогою яких НС приймає рішення.

Перелік критеріїв ефективності, що відповідають зазначеним вимогам, показано в додатку А. За аналогією з [9], прийнято, що значення запропонованих критеріїв можуть змінюватися в межах від 0 до 1. При цьому для *i*-го виду НСМ значення *k*-го критерію дорівнює 1, якщо відповідна *k*-та вимога повністю забезпечується в даному виді НСМ і дорівнює 0, якщо не забезпечується. Якщо *k*-а вимога забезпечується частково, то величина $R_k \in$

]0,1[і може бути визначена за допомогою експертного оцінювання. Значення елементів множини критеріїв (R_a) для апробованих видів НСМ показано в додатку Б.

Відповідно до принципу оцінювання ефективності виду НСМ для розпізнавання кібератак на мережеві РІС, кількість критеріїв ефективності K у виразі (2.8) дорівнює 19. Також у першому наближенні будемо вважати:

$$Net_a = Net_d = \{\text{МСП}, \text{ГНМ}, \text{ТК}, \text{PNN}, \text{РБФ}\} \quad (2.38)$$

Таким чином, кількість допустимих видів НСМ $I = 5$, що дає змогу трансформувати вираз (2.8) для розрахунку функції ефективності *i*-го виду НСМ таким чином:

$$V_i = \Sigma_{k=1}^{19} a_k R_k(net_i), net_1 \in \{\text{МСП}, \text{ГНМ}, \text{ТК}, \text{PNN}, \text{РБФ}\}\ i = 1, \dots 5\,. \quad (2.39)$$

Зазначимо, що за допомогою вагового коефіцієнта $\boldsymbol{a_k}$ враховується значущість *k*-го критерію ефективності для конкретного прикладного завдання розпізнавання кібератак на мережеві РІС. На практиці множину значень вагових коефіцієнтів (α) можна отримати за допомогою експертного оцінювання. У результаті можна стверджувати, що правило формування множини ефективних видів НСМ визначається виразом (2.40), а правило знаходження найефективнішого виду НСМ визначається виразом (2.41).

$$If(net) \geq \Delta_V \wedge net \in Net_d \rightarrow net \in Net_e \quad (2.40)$$

$$If \max_i = \{V(net_1), \dots V_1\}, net_i \in Net \rightarrow net_i = net_e^{\max} \quad (2.41)$$

де $V(net_1)$ ефективність НСМ, яка розраховується за допомогою виразу (2.39),

Δ_V - мінімально допустима ефективність НСМ.

2.4 Модель формування параметрів навчальних прикладів

У загальному випадку процес нейромережевого аналізу *k*-го прикладу контрольованих на експлуатації параметрів КСС з метою розпізнавання мережевої кібератаки і-го виду можна відобразити виразом виду:

$$NNet(R(k)) \rightarrow S(Ka_i) \tag{2.42}$$

де *NNet* - оператор нейромережевого аналізу,

R - множина контрольованих на експлуатації параметрів КСС,

R(*k*) - значення доданків *R* для *k*-го прикладу,

S (Kai) - сигнал НСМ про реалізацію кібератаки і-го виду.

Під час формування прикладів слід брати до уваги необхідність попереднього опрацювання доданків *R* для їх приведення до вигляду, придатного до використання в НСМ. Методологія такого оброблення досить докладно сформована в [81] і зводиться до реалізації різних процедур центрування та нормалізації. Результатом обробки є множина вхідних параметрів НСМ X . При цьому для загального випадку досить складним завданням є визначення переліку доданків *R*. Однак, відповідно до [49], для задачі розпізнавання мережевих кібератак номенклатура контрольованих на експлуатації параметрів КСС обмежена номенклатурою параметрів мережевого трафіку.

Також зазначимо, що *S* (*Kai*) - це множина чисел, що характеризує результат розпізнавання. У базовому випадку *S* (*Kai*) може набувати тільки бінарні значення: 0 - кібератаки немає, 1 - кібератака є. У більш складних випадках *S* (*Kai*) - це множина дійсних чисел, які інтерпретуються як імовірність або впевненість у реалізації кібератаки. У разі використання НСМ, що навчаються без учителя, у навчальних прикладах *S* (*Kai*) відсутній, у протилежному випадку *S* (*Kai*) потрібно заздалегідь визначити у вигляді очікуваного вихідного сигналу *Y*(*Kai*).

Таким чином, модель формування параметрів *k*-го навчального прикладу, що описує реалізацію кібератаки і-го виду, можна записати у вигляді:

$$\begin{cases} R(k)_{Ka_i} \to X(k)_{Ka_i} \\ S(k)_{Ka_i} \to X(k)_{Ka_i} \end{cases} X(k)_{Ka_i} \Leftrightarrow Y(Ka_i) \qquad (2.43)$$

де $(k)_{Ka_i} \to X(k)_{Ka_i}$ - процедура адаптації контрольованих параметрів КСС до НСМ,

$S(k)_{Ka_i} \to X(k)_{Ka_i}$ - процедура визначення очікуваного вихідного сигналу НСМ,

$X(k)_{Ka_i} \Leftrightarrow Y(Ka_i)$ - процедура зіставлення вхідних і вихідних параметрів.

Розглянемо процедуру $X(k)_{Ka_i} \Leftrightarrow Y(Ka_i)$. Скористаємося сформульованим принципом про необхідність врахування в очікуваному вихідному сигналі близькості зазначених еталонів. Відповідно до можливих структурних рішень НСМ необхідно розглянути два випадки формування вихідного сигналу [87]. У першому випадку вихідний сигнал НСМ реалізується за допомогою одного нейрона у вихідному шарі:

$$N_y = 1 \qquad (2.44)$$

де N_y - кількість нейронів у вихідному шарі.

У другому випадку кількість нейронів у вихідному шарі дорівнює кількості розпізнаваних станів захищеності мережевих РІС:

$$N_y = K_s \qquad (2.45)$$

де K_s - кількість розпізнаваних станів захищеності.

Деталізуємо перший випадок. Під час аналізу захищеності кожній з можливих кібератак, а також кожному з можливих безпечних станів

мережевого РІС ставлять у відповідність деякий діапазон величин вихідного сигналу. У базовому випадку можна припустити, що величини діапазонів для різних станів захищеності різні [5]. Крім того, для навчальних прикладів, які відповідають еталонам станів захищеності, вихідний сигнал дорівнюватиме середині зазначеного діапазону. У разі використання сигмоїдальної функції активації нейронів вихідного шару вихідний сигнал перебуває в межах від 0 до 1:

$$y \in]0..1[\tag{2.46}$$

де y - вихідний сигнал НСМ.

За умови рівномірного квантування діапазону можливих значень у очікуваний вихідний сигнал для еталона довільного і-го стану захищеності розраховується так:

$$y_{s_i} = \frac{1}{K_s} \times i - \frac{0{,}5}{K_s} = \frac{i-0{,}5}{K_s} \tag{2.47}$$

де i - номер станів захищеності.

Схожість станів захищеності у виразі (2.47) можливо врахувати тільки за рахунок того, що схожі стани захищеності повинні мати близькі номери.

Деталізуємо другий випадок. У навчальному прикладі для еталона і-го стану вихідний сигнал відповідного i-го нейрона дорівнює 1. При цьому порядок нумерації вихідних нейронів може бути довільним. Водночас виникає необхідність визначення очікуваного вихідного сигналу для всіх інших вихідних нейронів, які не відповідають цьому еталону. Зазначимо, що нейрони, які відповідають станам захищеності, близьким до еталона, повинні мати схожі величини вихідного сигналу. Так, базуючись на результатах [89], можна стверджувати, що в прикладі для еталона кібератаки типу loadmodule величина вихідного сигналу відповідного нейрона повинна менше відрізнятися від величини вихідного сигналу нейрона

кібератаки типу rootkit, ніж від величини вихідного сигналу нейрона кібератаки типу "шторм запитів". Тобто

$$|y_{[a]} - y_{[o]}| < |y_{[a]} - y_{[б]}| \tag{2.48}$$

де $y_{[a]}$, $y_{[o]}$, $y_{[б]}$ - вихідні сигнали нейронів, які відповідають кібератакам loadmodule, rootkit, "шторм запитів". По суті, визначення очікуваного вихідного сигналу НСМ для другого випадку є дещо ускладненим варіантом першого випадку, який зводиться до розрахунку числової оцінки близькості станів захищеності. При цьому відомі аналітичні методи такого розрахунку [63] вирізняються великою складністю. Водночас аналіз і розпізнавання кібератак на мережеві РІС - це задачі, які досить ефективно розв'язуються експертами в галузі захисту інформації [10]. Тому доцільно визначати оцінку ступеня схожості параметрів кібератак і параметрів безпечних станів на основі експертних даних. Базуючись на [23], пропонується використовувати статистичні методи обробки експертних даних. У цьому разі отримані від експертів кількісні дані опрацьовуються з метою оцінювання колективної думки експертної групи, оцінювання узгодженості думок експертів та оцінювання їхньої компетентності. Для визначення оцінок використовують статистичні методи точкового та інтервального оцінювання. Для цього рекомендується, щоб кількість експертів була не меншою за 10. Процедура експертного оцінювання ступеня близькості станів захищеності. Нехай у результаті опитування експертної групи, яка складається з m учасників, отримано такі дані:

$$\begin{matrix} x_{1,1} & \dots & x_{n,1} & \dots & x_{N,1} \\ \dots & \dots & \dots & \dots & \dots \\ x_{1,m} & \dots & x_{n,m} & \dots & x_{N,m} \\ \dots & \dots & \dots & \dots & \dots \\ x_{1,M} & \dots & x_{n,M} & \dots & x_{N,M} \end{matrix} \tag{2.49}$$

де $x_{n,m}$ - оцінка ступеня схожості *n*-го об'єкта (стану захищеності) *m*-им експертом; *N* - кількість об'єктів (станів захищеності); *M* - кількість експертів.

Середня колективна оцінка n-го стану захищеності розраховується за допомогою формули:

$$x_n = \frac{1}{M} \times \Sigma_{m=1}^{M} x_{n,m} \ , \tag{2.50}$$

де $x_{n,m}$- оцінка ступеня схожості n-го стану захищеності m-им експертом, n =1...N.

Дисперсія середньої колективної оцінки визначається так:

$$\sigma^2 = (M-1)^{-1} \times \Sigma_{m-1}^{M} (x_{n,m} - x_n)^2 \tag{2.51}$$

Для визначення статистичної значущості отриманих результатів необхідно вказати довірчий інтервал, у який оцінювана величина потрапляє із заданою довірчою ймовірністю P.

Задавшись імовірністю помилки $P_{\boldsymbol{n}}$ (рівнем значущості) можна визначити інтервал, у який оцінювана величина потрапляє з імовірністю (1 - $P_{\boldsymbol{n}}$):

$$I_{x_n} = (x_n - \varepsilon_{pn,}\, x_n + \varepsilon_{pn,}) \tag{2.52}$$

Величина ε_{pn} визначає межі довірчого інтервалу і розраховується так:

$$\varepsilon_{pn,} = \ t_p \times \sigma_n \,/\, \sqrt{M} \tag{2.53}$$

де t_p - коефіцієнт.

Вважається, що оцінювана величина має нормальний розподіл із центром x_i і дисперсією σ . Коефіцієнт t_p має розподіл Стьюдента з (N-1) ступенями

свободи і визначається за допомогою даних, які для окремих значень довірчої ймовірності P показано в таблиці 2.1.

Ступінь узгодженості експертних думок визначається за допомогою коефіцієнта варіації γ_n , який розраховується за формулою:

$$\gamma_n = \sigma / x_n \tag{2.54}$$

Таблиця 2.1 – Значення коефіцієнта t_P

P	0,8	0,85	0,9	0,95
t_p	1,282	1,439	1,643	1,960

Розрахований за допомогою виразу (2.92) коефіцієнт варіації γ_n визначає відносну величину діапазону зміни оцінок експертів відносно середнього значення колективної оцінки x_n . Вважається, що узгодженість експертних думок задовільна, якщо всі $\gamma_n < 0{,}3$, і мінімально достатня, якщо всі $\gamma_n < 0{,}2$.

У протилежному випадку процедуру експертного оцінювання слід повторити, з урахуванням результатів [38]. Оцінка компетентності експертів може визначатися за двома коефіцієнтами: об'єктивним коефіцієнтом компетентності та коефіцієнтом відносної самооцінки експерта [76].

У цьому розділі розв'язувалося наукове завдання розвитку методологічної бази нейромережевого розпізнавання кібератак на мережеві ресурси інформаційних систем. Основні результати розділу такі:

- Набула подальшого розвитку концептуальна модель, яка за рахунок конкретизації параметрів оцінювання та чинників, що впливають на ефективність процесу нейромережевого розпізнавання кібератак, дала змогу деталізувати напрями подальших досліджень.
- Отримали подальший розвиток принципи використання нейронних мереж для розпізнавання мережевих кібератак, які за рахунок врахування

ступеню забезпечення нейромережевою моделлю характеристик поставленої задачі, співвіднесення очікуваних вихідних сигналів нейромережевої моделі зі схожістю кібератак між собою та використання продукційних правил під час формування навчальних прикладів, забезпечують можливість підвищення ефективності нейромережевих моделей.

- Набула подальшого розвитку модель правил визначення ефективних видів нейромережевих моделей, у якій за рахунок реалізації запропонованих принципів забезпечується можливість формалізації визначення ефективних видів нейромережевих моделей, що дасть змогу підвищити їхню точність та оперативність створення.
- Вперше розроблено модель формування навчальних прикладів, яка за рахунок використання запропонованого принципу визначення очікуваного вихідного сигналу забезпечує можливість підвищення точності та зменшення терміну навчання нейромережевих моделей.

3 РОЗРОБКА НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ І МЕТОДІВ РОЗПІЗНАВАННЯ КІБЕРАТАК

3.1 Нейромережева модель протидії мережевим кібератакам за допомогою експертних знань

Базуючись на запропонованому принципі використання експертних знань для формування навчальної вибірки, визначено, що відповідно до [6], у першому наближенні в якості ідентифікуючих параметрів кібератак, що застосовуються в продукційних правилах виду (2.12), можливо використовувати параметри мережевого трафіку [13]. Завдяки цьому припущенню вираз (2.11, 2.12) модифікується таким чином:

$$If\ x_1 = X_1 \wedge \ldots \wedge x_K = K_X \rightarrow Y_l, l = 1..L, \quad (3.1)$$

$$If\ x_1 \in \left[X_1^{min}\ X_1^{max}\right]_l \wedge \ldots \wedge x_K \in \left[X_K^{min}\ X_K^{max}\right]_l \rightarrow Y_l, l = 1..L \quad (3.2)$$

де $x_1, \ldots x_K$ - значення вхідних параметрів НСМ;

К - кількість параметрів мережевого трафіку;

$\left[X_1^{min}\ X_1^{max}\right]$, ..., $\left[X_K^{min}\ X_K^{max}\right]$ - задані діапазони x_1, ... x_K- номер продукційного правила;

L - кількість продукційних правил.

У разі використання як бази для формування експертних правил БД KDD-99 [105] кількість вхідних параметрів НСМ дорівнюватиме К=41, що дорівнює кількості полів зазначеної бази даних. Зазначимо, що значення цих полів відповідають значенням мережевого трафіку за протоколом TCP. Також слід зазначити, що в разі використання бази даних KDD-99 результатом продукційного правила може бути або висновок про один із 22 видів кібератак, або про нормальний мережевий запит. У разі визначення продукційних правил виразом (3.1) завдання експертів полягає у визначенні значень X_1, X_2,... X_K, а у

разі визначення продукційних правил виразом (3.2) завдання експертів полягає у визначенні меж діапазонів $\left[X_1^{min}\ X_1^{max}\right]$,... , $\left[X_K^{min}\ X_K^{max}\right]$

Результати аналізу [25], вказують на те, що найповніше пристосовані для навчання за допомогою продукційних правил НСМ виду PNN і MPNN. Разом із цим проведений аналіз вказує на те, що негативними особливостями PNN і MPNN є низька інформативність вихідного сигналу. У цих НСМ значення вихідного сигналу вказують тільки на те, ймовірність якої події більша - реалізації кібератаки чи нормальної. Це не дає змоги використовувати в СЗІ встановлених порогових значень імовірності кібератаки/нормального стану або порогового значення різниці між цими ймовірностями. Таким чином, у СЗІ, блок розпізнавання якої функціонує на основі мережі MPNN неможливо впровадити захисні правила вигляду:

$$If\ \Theta_{Ka} > \Delta_{ka} \rightarrow Z \tag{3.3}$$

$$If\ \Theta_{Nm} < \Delta_{Nm} \rightarrow Z \tag{3.4}$$

$$If\ (\Theta_{Ka} - \Theta_{Nm}) > \Delta_{\Delta} \rightarrow Z \tag{3.5}$$

$$If \Omega_i > \Delta_i \rightarrow Z \tag{3.6}$$

де Θ_{Ka}, Θ_{Nm} - імовірність реалізації кібератак;

Θ_{Nm} - імовірність нормального стану;

Z - захисні заходи;

Ω_i - імовірність кібератаки *i*-го виду;

Δ_{ka} , Δ_{Nm} , Δ_{Δ} , Δ_i - порогові значення.

Крім цього, недостатня інформативність вихідного сигналу НСМ не дає змоги ЗЗІ гнучко реагувати на різноманітні комбінації параметрів мережевого трафіку, а також не дає змоги реєструвати параметри станів захищеності, вірогідність яких є відмінною від максимально вірогідного стану. Можливість реєстрації таких параметрів могла б дозволити створити базу даних, призначену для уточнення правил розпізнавання відомих видів кібератак і формування правил розпізнавання невідомих видів кібератак.

Для виправлення зазначених недоліків, базуючись на [33] визначено, що вихідна інформація мережі MPNN, призначеної для розпізнавання кібератак на мережеві PIC, має бути доповнена:

Ймовірностями реалізації відомих видів кібератак.

Імовірністю реалізації найімовірнішого виду кібератаки.

Імовірністю реалізації кібератаки.

Імовірністю нормального стану.

Для цього моделі PNN і MPNN мають бути доповнені відповідними вихідними зв'язками, а також додатковим шаром нейронів, призначеним для розрахунку ймовірностей відомих видів кібератак.

Модифікована структура PNN, призначена для розпізнавання стану мережевих PIC на підставі продукційних правил виду (3.1), показана на рисунку 3.1, а структура MPNN, адаптована до використання продукційних правил виду (3.2), показана на рисунку 3.2.

Структурно модифікована PNN складається з 5 нейронних шарів. Це вхідний шар (Lnin), шар образів (Ln_{in}), перший шар підсумовування (Ln_{s1}), другий шар підсумовування (Ln_{s2}) і шар порівняння (Ln_{coll}).

Як і в класичній мережі PNN, нейрони вхідного шару тільки передають дані із зовнішнього середовища до нейронів шару образів. Шар образів призначений для запам'ятовування параметрів навчальних прикладів для всіх класів, які має розпізнавати НС. Відповідно кількість нейронів шару образів дорівнює кількості навчальних прикладів, які запам'ятала НС. На рисунку 3.1 нейрони шару образів умовно розділені на групи, які відповідають відомим видам кібератак і нормальному стану мережевого PIC. Так наприклад, нейрони позначені 1_{KaN} ... L_{KaN} відповідають навчальним прикладам *N*-го виду кібератак, а нейрони позначені 1_{Nm} ... M_{Nm} відповідають навчальним прикладам нормального стану. У загальному випадку, кількість навчальних прикладів для кожного виду кібератак і для нормального стану може бути різною.

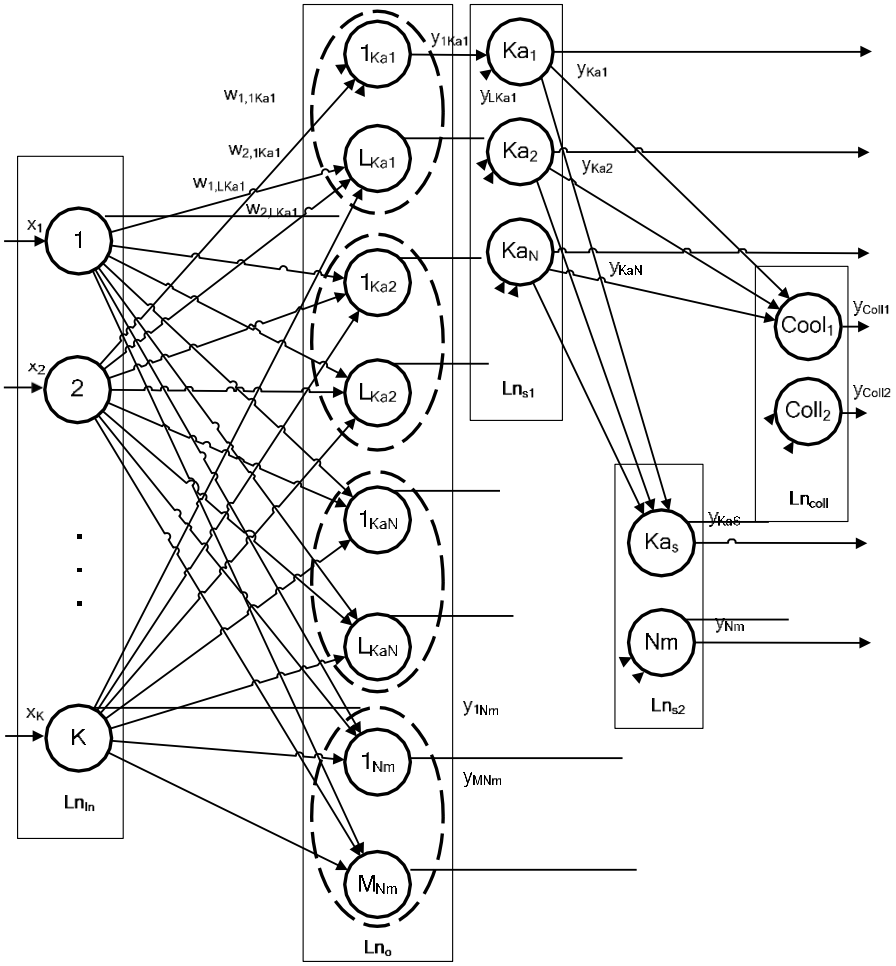

Рисунок 3.1 - Структура модифікованої PNN

Завданням першого шару підсумовування є розрахунок імовірності реалізації кожного виду кібератак, відомого для нейромережі. Тому нейрони цього шару асоціюються з відомими видами кібератак Ka_1, Ka_2, ... KaN, а їхня кількість дорівнює кількості зазначених видів кібератак (N). Другий шар підсумовування призначений для визначення загальної ймовірності всіх видів кібератак і ймовірності нормального стану мережевого PIC. Цей шар містить два нейрони. Нейрон Ka_s використовується для розрахунку загальної ймовірності кібератак, а нейрон Nm - для розрахунку ймовірності нормального стану. Завданням шару порівняння є визначення виду найімовірнішої кібератаки, а також виду найімовірнішого стану захищеності. Вид найімовірнішої кібератаки визначається нейроном $Coll_1$, а найімовірніший стан захищеності (кібератака реалізується або нормальний стан) визначається нейроном $Coll_2$.

Структура зв'язків між шарами Ln_{in} і Ln_o повнозв'язкова. При цьому кожен нейрон вхідного шару пов'язаний прямим зв'язком із кожним нейроном шару образів. Вагові коефіцієнти цих зв'язків дорівнюють компонентам навчальних прикладів:

$$w_{1,l} = X_1, w_{2,l} = X_2, \dots w_{K,l} = X_K, \tag{3.7}$$

де l - номер нейрона шару образів, що відповідає номеру продукційного правила виду (3.1),

K - кількість вхідних параметрів,

X_1 , X_2 ,.... X_K - компоненти l -го продукційного правила виду.

Для прикладу на рисунку 3.1 показано вагові коефіцієнти зв'язків між першим вхідним нейроном і l_{Ka1}... L_{Ka1}, l_{Ka2}... L_{Ka2} нейронами шару образів. Зазначимо, що вагові коефіцієнти всіх інших зв'язків у мережі PNN дорівнюють 1. У нейронах шару образів як функцію активації використовують функцію Гауса. Вихідний сигнал довільного l-го з нейронів шару образів, розраховується так:

$$y_l = \Sigma_{k=1}^{K} \exp(-(w_{k_l,l} - x_k)^2 / 2\sigma^2) \tag{3.8}$$

де $w_{k_l,l}$ - ваговий коефіцієнт зв'язку між k-им нейроном вхідного шару і l-им нейроном шару образів,

x_k - величина k-го вхідного сигналу,

K - кількість вхідних параметрів,

σ - радіус функції Гауса.

Зазначимо, що відповідно до [17] радіус функції Гауса $\sigma \in [0{,}3 \dots ,0{,}7]$. Структура зв'язків між шаром образів і першим шаром підсумовування має особливість. З нейроном першого шару підсумовування зв'язуються тільки ті нейрони шару образів, що відповідають параметрам виду кібератаки, з якою асоційований цей нейрон. Наприклад, як показано на рисунку 3.1, нейрони

l_{Ka1}... L_{Ka1} зв'язуються тільки з нейроном Ka_1. У нейронах шарів підсумовування застосовується лінійна функція активації. Вихідний сигнал для довільного n-го нейрона першого шару підсумовування розраховується так:

$$y_{Ka_n} = \frac{\Sigma_{l=1}^{L_{Ka_1}} y_{l_{Ka_1}}}{L_{Ka_1}}, \quad (3.9)$$

де L_{Ka_1}- кількість нейронів шару образів, пов'язаних із n-им нейроном першого шару підсумовування,

$y_{l_{Ka_1}}$- вихідний сигнал l-го нейрона шару образів, пов'язаного з n-им нейроном першого шару підсумовування.

Величини вихідних сигналів $y_{l_{Ka_1}}$,... $y_{l_{Ka_n}}$ свідчать про ймовірність реалізації кожного відомого виду кібератак Ka_1 ,... Ka_N . Ці сигнали становлять частину вихідної інформації мережі PNN. Крім цього вони передаються і нейрон Cool_1 шару порівняння та в нейрон Ka_s другого шару підсумовування. Вихідний сигнал цього нейрона розраховується так:

$$y_{Ka_s} = \frac{\Sigma_{n-1}^{N} y_{Ka_n}}{N}, \quad (3.10)$$

де N - кількість відомих видів кібератак.

Величина y_{Ka_s} , яка свідчить про сумарну ймовірність реалізації всіх видів кібератак також є частиною вихідної інформації мережі PNN. Крім цього подальшої обробки. y_{Ka_s} передається в нейрон $Cool_2$ шару порівняння для подальшої обробки.

Вихідний сигнал нейрона Nm другого шару підсумовування є оцінкою ймовірності нормального стану мережевого PIC. Цей нейрон пов'язаний тільки з тими нейронами шару образів, які асоційовані з навчальними прикладами нормального стану. Величина вихідного сигналу нейрона Nm розраховується так:

$$y_{Nm} = \frac{\Sigma_{m=1}^{M_{Nm}} y_{Nm_m}}{M_{Nm}}, \quad (3.11)$$

де M_{Nm} - кількість нейронів шару образів, які відповідають навчальним прикладам нормального стану,

y_{Nm_m} - вихідний сигнал m-го нейрона шару образів, що відповідає m-му прикладу нормального стану.

Як і y_{Ka_s} сигнал у Nm що є частиною вихідної інформації мережі передається в нейрон $Cool_2$. У нейронах $Cool_1$ і $Cool_2$ проводять визначення найімовірнішого виду кібератаки і визначення найімовірнішого стану захищеності - кібератака реалізується/нормальний стан. На рисунку 3.1 відповідні вихідні сигнали позначено як y_{Coll_1} і y_{Coll_2}.

Основною відмінністю модифікованої мережі MPNN від модифікованої мережі PNN є наявність шару фільтрації (на рисунку 3.2 позначено - Ln_f), нейрони якого призначені для фільтрації значень компонент вхідного сигналу відповідно до продукційного правилом виду (3.2). При цьому завданням деякого f_l^{xk} -го нейрона є фільтрація вхідного параметра x_k відповідно до *l*-го продукційного правила розпізнавання. Фільтрація сигналу здійснюється завдяки використанню функції активації виду:

$$\exists x_k \left[X_k^{max}, X_k^{min}\right]_l \rightarrow y_l^{f_{xk}} = x_k, \exists x_k \notin \left[X_k^{max}, X_k^{min}\right]_l \rightarrow y_l^{f_{xk}} = 0 \quad (3.12)$$

де x_k - значення k-го вхідного параметра, $y_l^{f_{x_k}}$- вихідний сигнал y_l^{xk} -го нейрона СФ.

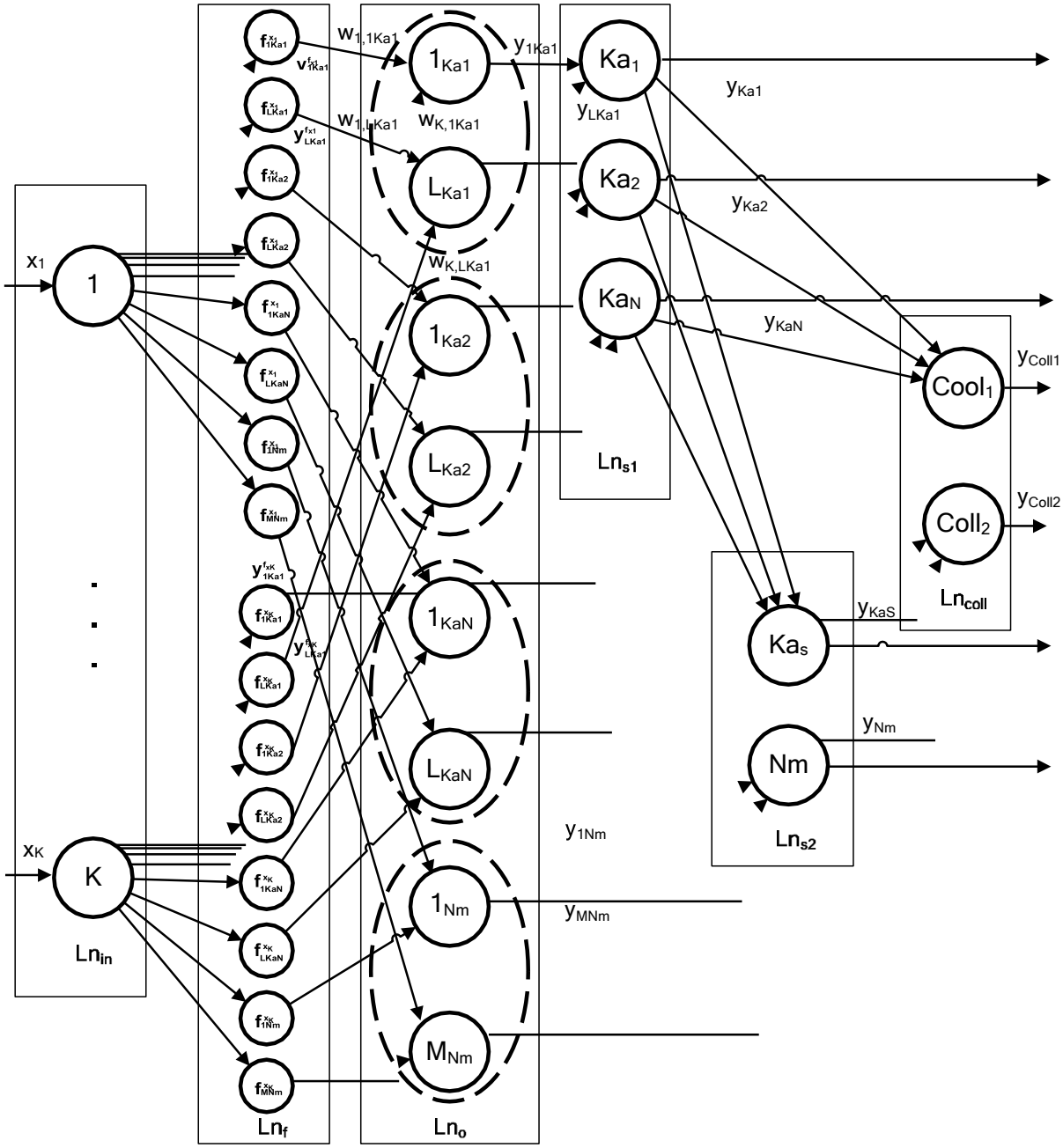

Рисунок 3.2 - Структура модифікованої MPNN

Вагові коефіцієнти між нейронами шару фільтрації та нейронами шару образів розраховуються так:

$$w_{f_l^{xk}} = \frac{X_k^{max} - X_k^{min}}{2} \tag{3.13}$$

де l - номер нейрона шару образів, що відповідає номеру продукційного

правила вигляду (3.2),

f_l^{xk}- нейрон, що фільтрує сигнал від x_k-го вхідного нейрона до l-го нейрона шару образів,

k - кількість вхідних параметрів,

$V_k^{max} V_k^{min}$ - компоненти l-го продукційного правила вигляду.

Також зауважимо, що всі вагові коефіцієнти зв'язків між вхідними нейронами та нейронами шару фільтрації дорівнюють 1. Тому на рисунку 3.2 їх не показано.

Для внесення в мережу PNN l-го продукційного правила виду (3.1), що визначає наявність кібератаки виду Ka_j необхідно:

- Внести в шар образів новий нейрон l_{kan}.
- Зв'язати нейрон l_{kan} із вхідними нейронами та відповідно до виразу (3.7) встановити для цього нейрона вагові коефіцієнти вхідних зв'язків.
- Внести в перший шар підсумовування новий нейрон Ka_j.
- Зв'язати нейрон Ka_j з нейроном l_{kan}.
- Зв'язати нейрон Ka_j з нейроном Ka_S, який розраховує сумарну ймовірність реалізації кібератак усіх відомих видів.

Для внесення в мережу PNN m-го продукційного правила виду (3.1), що визначає нормальний стан мережевого PIC необхідно:

1) Внести в шар образів новий нейрон m_{Nm}.

2) Зв'язати нейрон m_{Nm} із вхідними нейронами та, використавши вираз (3.7), установити для нього вагові коефіцієнти вхідних зв'язків рівними відповідним компонентам продукційного правила.

3) Зв'язати нейрон m_{Nm} з нейроном Nm, який розраховує сумарну ймовірність нормального стану мережевого PIC.

У навчанні мережі MPNN є деякі відмінності, пов'язані зі складнішим характером продукційних правил, на яких вона навчається. Для запам'ятовування нею продукційного правила виду (3.2) етап два поділяється на три кроки:

1) У шар фільтрації вносять додаткові нейрони, призначені для фільтрації

значень вхідних параметрів відповідно до компонентів продукційного правила. Кількість нових фільтрувальних нейронів дорівнює кількості вхідних параметрів НСМ.

2) Нові фільтрувальні нейрони зв'язуються з вхідними нейронами та з нейроном кулі образів, який було внесено в мережу на попередньому етапі. 3) Використовуючи вираз (3.13), встановлюються вагові коефіцієнти зв'язків між нейронами шару образів і нейронами шару фільтрації.

У режимі розпізнавання стану захищеності мережевого PIC, PNN і MPNN функціонують так:

1) На вхід НС подається вектор параметрів $\{x\}_K$, який характеризує невідомий стан захищеності мережевого PIC.

2) Для MPNN розраховуються вихідні сигнали нейронів кулі фільтрації. Для цього використовується вираз (3.12). Для PNN цей етап не виконується.

3) З використанням виразу (3.8), розраховується вихідний сигнал кожного з нейронів кулі образів Ka_1, Ka_2,... Ka_N.

4) Визначаються ймовірності кожного з відомих видів кібератак. Для цього, з використанням виразу (3.9), розраховується вихідний сигнал кожного з нейронів першого шару підсумовування.

5) Визначається інтегральна ймовірність усіх видів кібератак. Для цього з використанням виразу (3.10) розраховується вихідний сигнал нейрона Kas, що належить другому шару підсумовування.

6) Визначається інтегральна ймовірність нормального стану мережевого PIC. Для цього з використанням виразу (3.11) розраховується вихідний сигнал нейрона Nm, що належить другому шару підсумовування.

7) Визначається найбільш імовірна кібератака. Для цього за допомогою нейрона $Cool_1$, розраховується у якого нейрона першого шару підсумовування вихідний сигнал має найбільше значення. Вихідний сигнал $y_{Cool_1} = k$, де k - номер нейрона першого шару підсумовування з найбільшим вихідним сигналом. Кібератака, асоційована з цим нейроном, вважається найбільш імовірною.

8) Визначається найбільш імовірний стан захищеності. Для цього за допомогою нейрона $Cool_2$,, порівнюються величини вихідних сигналів нейронів Ka_s і Nm. Якщо $y_{Ka_s} \geq y_{Nm}$, то $y_{Cool_1} = Ka_s$ і вважається, що мережевий РІС піддається кібератаці. У цьому випадку $y_{Cool_1} = k$. У протилежному випадку $y_{Cool_1} = Nm$ і вважається, що стан мережевого РІС нормальний.

3.2 Модель глибокої нейронної мережі

Відповідно до [106] під час розроблення НСМ типу ГНС як базову архітектуру використано тришаровий персептрон, для переднавчання якого застосовано розріджений автокодувальник.

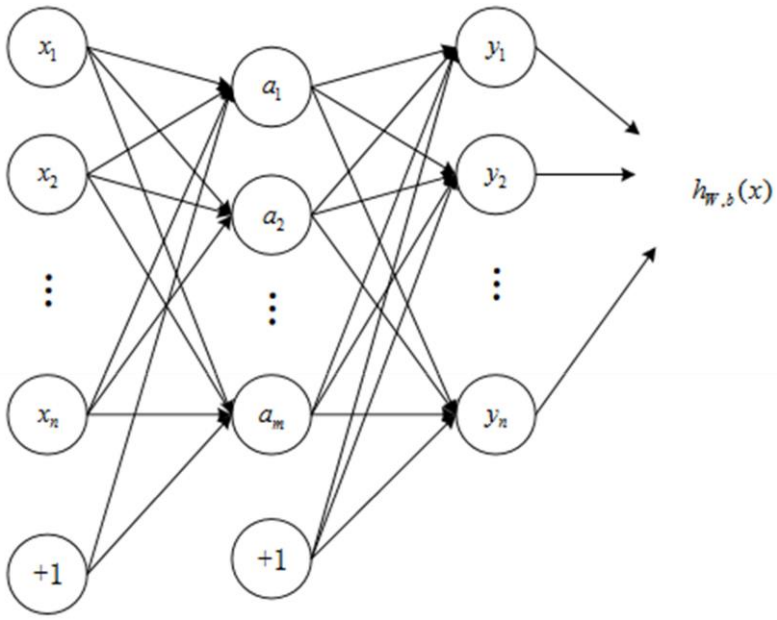

Рисунок 3.3 - Архітектура автокодувальника

Структура автокодувальника показана на рисунку 3.3. Зазначимо, що на рисунку 1 вихідні сигнали вхідних нейронів позначено міткою "x", прихованих нейронів - міткою "a", вихідних - "y", а блоків зміщення - міткою "+1".

Вхідними даними автокодувальника є нерозмічена навчальна вибірка $x = (x_1, x_2, \dots, x_i)$. У прихованих і вихідних нейронах використовується сигмоїдальна функція активації:

$$f(z_k) = \frac{1}{1+e^{=zk}}. \quad (3.14)$$

де $\boldsymbol{z_k}$ - вхідний сигнал *k*-го нейрона в прихованому або вихідному шарі. У свою чергу

$$z_k = \Sigma_{i=1}^{n}(W_{i,k}x_{i,k} + x_0 B_k), \quad (3.15)$$

де $W_{i,k}$ - вага зв'язку від і-го нейрона попереднього шару до *k*-го нейрона в прихованому або вихідному шарі,

$x_{i,k}$ - сигнал від *i*-го нейрона попереднього шару до *k*-го нейрону,

x_0=1 - вага зв'язку нейрона із самим собою,

b_k - зміщення *k*-го нейрона.

Вихід автокодувальника з кількістю нейронних шарів l дорівнює

$$h_{W,b}(x) = a^{(l)}, \quad (3.16)$$

де *W* - масив вагових коефіцієнтів, *b* - масив зміщень, $\boldsymbol{a^{(l)}}$- масив вихідних значень нейронів у шарі *l*

Стосовно малюнка 3.3.

$$a^{(l)} = y. \quad (3.17)$$

де *y* - масив вихідних значень нейронів останнього (*l*-го) шару.

Особливістю автокодувальника є застосування навчання без учителя при використанні алгоритму зворотного поширення помилки. Для цього цільова функція навчання автокодувальника визначається так:

$$h_{w,b}(x) \approx x \quad (3.18)$$

Використання цільової функції виду (3.18) передбачає рівність вихідного сигналу автокодувальника вхідному сигналу. Таким чином, навчання класичного автокодувальника зводиться до того, щоб за допомогою алгоритму зворотного поширення помилки знайти такі значення вагових коефіцієнтів, за яких вихідний сигнал дорівнюватиме вхідному [106, 107]. При цьому навчальні приклади можуть бути немаркованими, тобто не містити очікуваний вхідний сигнал.

Пошук оптимального значення вагових коефіцієнтів здійснюється за допомогою градієнтного спуску шляхом мінімізації функції втрат:

$$\mathrm{J(W,b)} = \left[\frac{1}{m}\sum_{i=1}^{m}\left(0{,}5\left\|h_{W,b}\left(x^{(i)}\right) - y^{(i)}\right\|^2\right)\right] + 0{,}5\lambda\sum_{l=1}^{m}\sum_{i=1}^{S_{l-1}}\sum_{j=1}^{S_l}\left(W_{j,i}^{(l-1)}\right)^2 \qquad (3.19)$$

m - кількість прихованих шарів,

s^l - кількість нейронів у шарі l,

$W_{j,i}^{(l-1)}$- вага

зв'язку між нейроном і у шарі l і нейроном j у шарі (l-1).

Перша частина функціонала - усереднена квадратична помилка за всіма навчальними прикладами, друга частина - регуляризація (або контроль згасання ваг), що контролює порядок ваг і не дає перенавчитися. Параметр λ, що контролює згасання ваг, регулює відносну важливість двох частин функціоналу.

Навчання проводиться доти, доки:

$$J(W,b) < \theta. \qquad (3.20)$$

де θ - заздалегідь визначений коефіцієнт (поріг).

Щодо класичного варіанта особливістю розрідженого автокодувальника є обмеження кількості одночасно активних нейронів у проміжних шарах. Вважається, що за рахунок цього розріджений автокодувальник автоматично

навчається виокремлювати із вхідних даних спільні ознаки, які відображаються у значеннях вагових коефіцієнтів. Для цього у функцію втрат вводиться додаткова компонента:

$$P = \sum_{j=1}^{h}(p \log\frac{p}{\hat{p}_j} + (1-p)\log\frac{(1-p)}{(1-\hat{p}_j)}) \quad (3.21)$$

де $\hat{p}_j$ - середнє значення функції активації нейрона j за всіма навчальними прикладами, $p \approx 0{,}05$- параметр розрідженості.

Зазначимо, що нейрон вважається активним, якщо його вихідний сигнал близький до 1, а неактивним - близький до 0.

З урахуванням (3.20) оптимізована функція втрат розрідженого автокодувальника має вигляд:

$$J_s(W,b) = J(W.b) + \beta P \quad (3.22)$$

де β - заданий коефіцієнт (у першому наближенні $\beta \approx 3$).

Попереднє навчання глибокої нейронної мережі, у якої кількість нейронних шарів дорівнює m, реалізується так:

1) Випадковим чином ініціалізуються вагові коефіцієнти всіх синаптичних зв'язків.

2) Виходячи з необхідної точності навчання встановлюється значення коефіцієнта θ.

3) Встановлюється номер шару, що навчається, 1). l = 2 (вхідний шар має номер

4) До l-го шару нейронів підключається новий додатковий шар.

5) На вхід l-го шару подається безліч навчальних прикладів.

6) За допомогою (3.13-3.22) розраховується значення матриці вагових коефіцієнтів зв'язків l-го шару нейронів.

7) Підключений на 4 етапі шар нейронів видаляється.

8) Якщо $l < m$, то $l = l + 1$ и здійснюється перехід на 5 етап. В іншому разі переднавчання закінчується.

Після етапу переднавчання два останні шари глибокої нейронної мережі навчаються на маркованих даних.

3.3 Метод створення навчальної вибірки для нейромережевої моделі протидії кібератакам

Відправною точкою розроблення методу створення навчальної вибірки послугували запропоновані в другому розділі принцип припустимості використання виду НСМ для розпізнавання кібератак на мережеві РІС, принцип визначення очікуваного вихідного сигналу НСМ для портретів кібератак, принцип використання експертних знань для формування навчальної вибірки, і розроблена на їхній основі модель формування параметрів навчальних прикладів.

Прийнято до уваги, що в деяких випадках БД мережевих кібератак можуть бути недоступними або малоінформативними. У цих випадках передбачено формувати безліч навчальних прикладів на основі експертної оцінки параметрів мережевого трафіку. У цьому разі завдання експертів полягатиме у визначенні, які параметри мережевого трафіку відповідатимуть тому чи іншому стану безпеки мережевого РІС. У першому наближенні передбачено, що вихідний сигнал НСМ буде реалізовано за допомогою одного вихідного нейрона. Також передбачено випадок, коли для формування навчальної вибірки будуть доступні тільки немарковані дані, що відповідають навчальним прикладам.

У загальному випадку перетворення інформації, що реалізується запропонованим методом, можливо представити за допомогою таких виразів:

$$\langle \Phi, \Omega_1, \Omega_2, D_1, D_2, D_3, t_d, N_x, N_y, Z_{\text{ов}}, k_{HCC}, W_n \rangle \rightarrow \langle Z_1, Z_2, Z_3, Z_4 \rangle \qquad (3.23)$$

$$Z_1 = \{z_1^{(\phi_k)}\}_{K_\phi} = \{(x^{(\phi_k)}, y^{(\phi_k)})\}_{K_\phi} \qquad (3.24)$$

$$Z_2 = \{z_2^{(\phi_k)}\}_{K_\phi} = \{r^{(\phi_k)}\}_{K_\phi} \quad (3.25)$$

$$Z_3 = \{z_3^{(\varphi_l)}\}_{L_\phi} = \{x^{(\varphi_l)}\}_{L_\phi} \quad (3.26)$$

$$Z_4 = \{z_4^{(\varphi_l)}\}_{L_\phi} = \{\{(x^{(\phi_k)}, y^{(\phi_k)})\}_{0,2K_\phi}, \{x^{(\varphi_l)}\}_{0,8L_\phi}\} \quad (3.27)$$

де Φ - множина (перелік) розпізнаваних мережевих кібератак, що розпізнаються, Ω_1 - множина портретів мережевих кібератак, отриманих із БД, Ω_2 - множина прикладів параметрів мережевого трафіку, кожен з яких відповідає окремому розпізнаваному стану безпеки (мережевій кібератаці), D_1 - множина експертних даних, які стосуються співвідношення очікуваного вихідного сигналу НСМ з еталоном кібератаки, D_2 - множина експертних даних, що стосуються продукційних правил розпізнавання кібератак, D_3 - множина експертних даних, що стосуються розпізнавання кібератак на основі аналізу параметрів мережевих запитів, td - допустимий термін формування навчальної вибірки, Z_1 - навчальна вибірка, приклади якої містять очікуваний вихідний сигнал, Z_2 - навчальна вибірка з прикладами у вигляді продукційних правил, Z_3 - навчальна вибірка, приклади якої не містять очікуваного вихідного сигналу, Z_4 - навчальна вибірка, у якій більша частина прикладів (≈80%) не містять очікуваного вихідного сигналу. сигналу, $Z_{ов}$- безліч обмежень на формування навчальної вибірки, W_n - обчислювальна потужність використовуваного АПО, $k_{нсс}$ - коефіцієнт використання НСР потужностей АПО, $z_1^{(\varphi_k)}, z_2^{(\varphi_k)}$- навчальні приклади виду Z_1 , Z_2 для кібератаки *k*-го виду, $z_3^{(\varphi_l)}$- навчальні приклади виду Z_3 для прикладу мережевого трафіку *l*-го виду, $x^{(\varphi_k)}$ - множина вхідних параметрів для кібератаки *k*-го виду, $y^{(\varphi_k)}$ - очікуваний вихідний сигнал НСМ для кібератаки *k*-го виду, $r^{(\varphi_k)}$ - множина продукційних правил виду (3.1, 3.2) для кібератаки *k*-го виду, K_φ - кількість кібератак, які мають бути розпізнані, $x^{(\varphi_l)}$- вхідні параметри для прикладу мережевого трафіку *l*-го виду, L_φ - кількість прикладів мережевих запитів.

Зазначимо, що основним джерелом даних для формування навчальної вибірки НСМ є Ω_1 і Ω_2 , що являють собою приклади мережевого трафіку, кожен з яких відповідає окремому мережевому запиту, відповідно стеку протоколів TCP/IP. Різниця між Ω_1 і Ω_2 полягає в тому, що кожному мережевому запиту (прикладу), який входить у множину Ω_1 , поставлено у відповідність певний вид стану захищеності (вид кібератаки), а в Ω_2 така відповідність відсутня. Φ являє собою впорядковану множину кібератак, які мають бути розпізнані. Упорядкування множини може бути реалізовано, наприклад, за принципами, що використовуються в БД KDD-99. Під час розроблення моделі формування параметрів навчальних прикладів визначено, що множина $x^{(\varphi_l)}$складається з 40 компонентів. Також, під час розроблення НСМ розпізнавання мережевих кібератак за допомогою експертних знань показано, що кількість параметрів у продукційних праивлах, які входять до складу $r^{(\varphi_k)}$, дорівнює 7.

Аналізуючи (3.1-3.4) визначено, що для їх реалізації необхідно шість етапів: розрахунок допустимого обсягу навчальної вибірки, визначення очікуваного вихідного сигналу НСМ для кожного з еталонів мережевих кібератак, формування очікуваного вихідного сигналу НСМ для кожного з еталонів мережевих кібератак, формування Z_1, Z_2, Z_3, Z_4. Також доцільно використовувати етап визначення можливості формування навчальної вибірки у вигляді множин Z_1, Z_2, Z_3 або Z_4 . Зазначимо, що наявність навчальної вибірки у вигляді $Z_1,$ надає можливість використання потужніших видів НСМ, однак її формування є складнішим і трудомісткішим. Тому прийнято вважати:

$$If Z_1 \in Z \rightarrow Z_1, Z_2, Z_3 \notin Z, \tag{3.28}$$

При цьому формування навчальної вибірки виду Z_2 може бути ускладненим за рахунок необхідної процедури експертного оцінювання, а

використання НСМ, адаптованих до Z_2 або Z_3 може бути обмежене у зв'язку з максимально допустимою помилкою розпізнавання.

Крім цього, виходячи із загальноприйнятої методології розроблення НСМ [17], сформульовано висновок щодо необхідності етапу масштабування вхідних і вихідних параметрів та етапу перевірки якості попереднього опрацювання навчальної вибірки.

Структурну схему методу створення навчальної вибірки показано на рисунку 3.4. Зазначені на рисунку 3.4 етапи методу деталізуються так.

Етап 1 - розрахунок обсягу навчальної вибірки. На цьому етапі розраховується мінімально і максимально допустима кількість навчальних прикладів. Вхідними даними етапу є - W_n, N_x та K_φ. Для розрахунку мінімально допустимої кількості навчальних прикладів використовується вираз:

$$L_\Sigma^{min} = \Sigma_{k=1}^{K_\varphi} L_{\varphi_k}^{min}, \tag{3.29}$$

Де L_Σ^{min} - загальна мінімально допустима кількість навчальних прикладів, $L_{\varphi_k}^{min}$ мінімально допустима кількість навчальних прикладів для кожного k-го виду кібератаки.

З огляду на розроблену модель формування параметрів навчальних прикладів, орієнтацію на використання БД KDD-99, NSL-KDD і [37], для навчальної вибірки виду Z_1, Z_3, Z_4 мінімально допустима кількість навчальних прикладів для кожного виду кібератаки дорівнює:

$$L_{\phi_k}^{min}(Z_1) = 10 \times N_x = 10 \times 40 = 400 \tag{3.30}$$

$$L_{\phi_k}^{min}(Z_3) = 30 \times N_x = 30 \times 40 = 1200 \tag{3.31}$$

$$L_{\phi_k}^{min}(Z_4) = 0{,}2 \times L_{\phi_k}^{min}(Z_1) + 0{,}8 \times L_{\phi_k}^{min}(Z_3) = 0{,}2 \times 400 + 0{,}8 \times 1200 = 1040 \tag{3.32}$$

де N_x - кількість вхідних параметрів НСМ.

Відповідно до розробленої НСМ виду PNN і результатів [6], для навчальної вибірки виду Z_2мінімально допустиму кількість навчальних прикладів для кожного виду кібератаки можливо розрахувати так:

$$L_{\phi_k}^{min}(Z_2) = 20 \times N_x = 20 \times 7 = 140. \quad (3.33)$$

Загальну мінімально допустиму кількість навчальних прикладів для кожного виду вибірки отримаємо, визначивши кількість атак, що розпізнаються, і підставивши (3.30-3.33) у (3.29).

Максимально припустимий обсяг навчальної вибірки визначають, виходячи з можливості забезпечення безперебійного навчання НСМ за її реалізації на загальнодоступному апаратно-програмному забезпеченні. У першому наближенні можна вважати, що така реалізація дає можливість безперебійного навчання впродовж доби (8640 с) [9, с. 27-30]. Використання зазначеної величини у виразах (2.17, 2.18), що отримано під час розроблення моделей правил визначення ефективних видів НСМ, дає змогу записати такі рівняння:

$$8640 \approx k_1 \tau\, e^{-\varepsilon} L_{\phi_k}^{max}(Z_2, Z_3)(N_x + N_y) \quad (3.34)$$

$$8640 \approx k_2 \tau\, e^{-\chi\varepsilon} L_{\phi_k}^{max}(Z_1)^2 (N_x + N_y)^2 \quad (3.35)$$

$$8640 \approx 0{,}2 k_2 \tau\, e^{-\chi\varepsilon} L_{\phi_k}^{max}(Z_4)^2 (N_x + N_y)^2 + 0{,}8 k_1 \tau\, e^{-\chi\varepsilon} L_{\phi_k}^{max}(Z_4)(N_x + N_y) \quad (3.36)$$

де $L_{\phi_k}^{max}(Z_1)$ - максимально допустима кількість прикладів виду Z_1,

$L_{\phi_k}^{max}(Z_2, Z_3)$ - максимально допустима кількість прикладів виду Z_2, Z_3 ,

$L_{\phi_k}^{max}(Z_2, Z_3)$ - максимально допустима кількість прикладів виду Z_4 ,

τ - тривалість однієї обчислювальної операції процесу навчання.

Після підстановки в (3.33-3.35) визначених у п. 2.3 величин $k_1 \approx 0{,}1$, $k_2 \approx 0{,}01$, $\chi \approx 1$, $\varepsilon \approx 0{,}01$ і тривіальних спрощень отримаємо:

$$L_{\phi_k}^{max}(Z_{2,}Z_3) \approx 86400/\tau(N_x + N_y) \tag{3.37}$$

$$L_{\phi_k}^{max}(Z_1) \approx 864000/\tau(N_x + N_y)^2 \tag{3.38}$$

$$L_{\phi_k}^{max}(Z_4) \approx 172800/\tau\left(N_x + N_y\right)^2 + 69120/\tau(N_x + N_y) \tag{3.39}$$

Враховуючи в (3.37-3.39), що для НСМ, які відповідають вибіркам Z_1, Z_3, Z_4 , $N_x + N_y = 41$, для НСМ, які відповідають Z_2 , $N_x + N_y \approx 10$ і орієнтуючись на максимізацію терміну навчання отримаємо:

$$L_{\phi_k}^{max}(Z_1) \approx 504\tau^{-1} \tag{3.40}$$

$$L_{\phi_k}^{max}(Z_1) \approx 8640\tau^{-1} \tag{3.41}$$

$$L_{\phi_k}^{max}(Z_1) \approx 2107\tau^{-1} \tag{3.42}$$

$$L_{\phi_k}^{max}(Z_1) \approx 1789\tau^{-1} \tag{3.43}$$

Зазначимо, що $\tau = f(W_n)$, а її величину слід визначити експериментальним шляхом, враховуючи можливість розпаралелювання процесу навчання. Таким чином, виходом першого етапу є $L_\Sigma^{min}, L_\phi^{min}(Z_1, Z_3), L_\phi^{min}(Z_2), L_\phi^{min}(Z_4), L_\phi^{max}(Z_1), L_\phi^{max}(Z_2), L_\phi^{max}(Z_3), L_\phi^{max}(Z_4)$

Етап 2 - визначення допустимих видів навчальної вибірки.

Вхідними даними етапу є $K_\phi, t_d, L_\phi^{min}(Z_1, Z_3), L_\phi^{min}(Z_2), \phi, \Omega_1, \Omega_2, D_2, D_3$. Виходом етапу є множина допустимих видів навчальної вибірки Z . Етап

поділено на чотири кроки, кожен із яких співвідноситься з перевіркою входження в Z кожного з видів навчальної вибірки Z_1, Z_2, Z_3 або Z_4 .

Крок 1 - перевірка допустимості Z_1 . Навчальна вибірка виду Z_1 вважається допустимою при виконанні будь-якої з двох умов.

Умова 1. Доступна БД, яка дає змогу сформувати $z_1^{(\phi_k)}$ достатню кількість елементів. Для цього в зазначених БД для кожного з видів кібератак має бути достатня кількість відповідних записів. Аналітичний вираз умови 1 має такий вигляд:

$$If\,\Omega_1 \notin \emptyset \wedge L_{\phi_k}^{\Omega_1} \geq 400, k = 1,..K_\Phi \rightarrow Z_1 \in Z \qquad (3.44)$$

де $L_{\phi_k}^{\Omega_1}$ - кількість елементів Ω_1 , що відповідають k-му виду кібератак.

Умова 2. За допомогою експертного оцінювання можна в прийнятний термін сформувати з доступних параметрів мережевого запиту множину $z_1^{(\phi_k)}$. В першому наближенні цю умову, можливо записати за допомогою такого виразу:

$$If\,\Omega_2 \notin \emptyset\; E_1(\phi, \Omega_2, D_3) = z_1^{(\phi_k)}, L_{\phi_k}^{z_1} \geq 400 \wedge t_{Z_1} \leq t_d \rightarrow Z_1 \in Z \qquad (3.45)$$

де E_1 - процедура формування $z_1^{(\phi_k)}$ з $\Omega_2, L_{\phi_k}^{z_1}$ - кількість елементів $z_1^{(\phi_k)}, t_d$ - допустимий термін формування навчальної вибірки, тривалість якого оцінюється за допомогою (2.33), t_{Z_1} - строк формування навчальної вибірки виду Z_1 , тривалість якого оцінюється за допомогою (2.27). Крок 2 - перевірка допустимості Z_2 . Навчальну вибірку виду Z_2 вважається допустимою при виконанні умови - за допомогою експертного оцінювання в прийнятний термін для кожного k-го виду кібератаки можна розробити безліч $r^{(\phi_k)}$ з кількістю елементів не меншою ніж 140:

$$If\ E_2(\Phi, D_2) = r^{(\Phi_k)}, L_{\phi_k}^{D_2} \geq 140 \wedge t_{Z_2} \leq \bar{t}_{\partial} \rightarrow Z_2 \in Z \quad (3.46)$$

де E_2 - процедура формування продукційних правил, t_{Z_2} - термін формування навчальної вибірки виду Z_2 , який можна оцінити за допомогою (2.28).

У (3.46) враховано, що мінімально допустиму кількість елементів визначено за допомогою виразу (3.24).

Крок 3 - перевірка допустимості Z_3 . Навчальна вибірка виду Z_3 вважається допустимою при виконанні умови:

$$If L_{\varphi} \geq k_{\varphi} L_{\Sigma}^{min} \rightarrow Z_3 \in Z \quad (3.47)$$

де k_{φ} - коефіцієнт очікуваного розподілу прикладів видів кібератак у доступній Ω_2 .

Базуючись на результатах [33] визначено, що при використанні як джерела даних Ω_2 мережевих сніферів $k_{\varphi} = 10^3$. Це дає змогу переписати (3.47) у вигляді:

$$If L_{\varphi} \geq 10^3 L_{\Sigma}^{min} \rightarrow Z_3 \in Z \quad (3.48)$$

Крок 4 - перевірка допустимості Z_4 . Навчальну вибірку виду Z_4 вважається допустимою при виконанні умови - можна в прийнятний термін сформувати вибірку, до складу якої входить як мінімум 20% прикладів виду $z_1^{(\phi_k)}$і не більше 80%, прикладів виду $z_1^{(\phi_l)}$. Аналітичний опис цієї умови є симбіозом умов (3.44, 3.45, 3.47, 3.48):

$$(If(\Omega_2 \notin \emptyset \wedge E_1(\Phi, \Omega_2, D_3) = z_1^{(\phi_k)}, L_{\phi_k}^{z_1} \geq 80 \wedge t_{Z_1} \leq t_d) \wedge If(L_{\varphi} k_{\varphi} L_{\Sigma}^{min})) \vee$$
$$(If(\Omega_2 \notin \emptyset \wedge L_{\phi_k}^{\Omega_1} \geq 80) \wedge If(L_{\varphi} \geq 0{,}8 k_{\varphi} L_{\Sigma}^{min})) \rightarrow Z_4 \in Z \quad (3.49)$$

Етап 3 - формування навчальних прикладів для вибірки виду Z_1 .

Базою етапу є розроблена модель формування параметрів навчальних прикладів. Враховано, що джерелом формування Z1 можуть бути або БД кібератак, або множини зафіксованих параметрів мережевих запитів. Для цього випадку передбачено використовувати процедуру експертного оцінювання відповідності параметрів мережевого запиту деякому виду кібератак. Вхідними даними етапу є $k_\phi, \phi, L_\phi^{min}(Z_1), L_\phi^{max}(Z_1), \Omega_1, \Omega_2, D_3, t_d$ а виходом - множина навчальних прикладів $Z_{1,a} = \{Z_{1,a}^{(\phi_k)}\}_{K_\phi} = \{(x_a^{(\phi_k)}, y_a^{(\phi_k)})\}_{K_\phi}$ параметри яких потребують масштабування. При цьому очікуваний вихідний сигнал подано в символьному вигляді. Етап поділено на три кроки.

Крок 1 - експертне оцінювання параметрів мережевого запиту. Цей крок виконується тільки в разі використання як джерела даних безлічі зафіксованих параметрів мережевих запитів. Результатом виконання є визначення виду стану захищеності (кібератака певного виду/безпечний стан), що відповідає кожному із зафіксованих запитів. Для цього пропонується використовувати процедуру експертного оцінювання, подібну до процедури експертного оцінювання близькості видів кібератак, що використовується в розробленій моделі формування параметрів навчальних прикладів, а математичний апарат якої визначено виразами (2.50-2.56). Відмінність зазначених процедур між собою полягає тільки в тому, що під час оцінювання окремих мережевих запитів експерт для кожного з них встановлює ймовірність приналежності до кожного з видів кібератак, що розпізнаються, які входять до множини *Ф*. Таким чином, у виразі (2.50) величина $x_{n,m}$ являє собою встановлену експертом імовірність того, що цей запит є кібератакою n-го виду. Відповідно у виразі (2.51) величина xn інтерпретується як середня колективна оцінка того, що даний запит є кібератакою *n*-го виду. Також у виразі (2.51) вважається

$$If\, x_n \le \Delta_\phi \to x_n = 0 \qquad (3.50)$$

де Δ_ϕ - емпіричний коефіцієнт (у першому наближенні $\Delta_\phi = 0{,}1$).

Крім того, запропонована процедура експертного оцінювання передбачає зіставлення мережевого запиту з кількома видами кібератак. Вхідні дані для експертного оцінювання зазвичай подаються у вигляді параметрів мережевого трафіку за стеком протоколів TCP/IP.

Крок 2 - визначення вихідного сигналу в символьному вигляді. Крок адаптовано до джерела навчальних прикладів. Якщо джерелом даних є Ω_1 , то значенням вихідного параметра навчального прикладу є комбінація символів:

$$y^{(\phi_k)} = 1 * \phi_k \tag{3.51}$$

де k - номер виду кібератаки в алфавіті, ϕ_k - назва k -го виду кібератаки.

Якщо джерелом даних є Ω_2 і в результаті виконання кроку 1 визначено, що є ненульова ймовірність приналежності мережевого запиту до кількох видів кібератак, то цей елемент використовується для формування кількох навчальних прикладів. Вихідний сигнал для кожного із зазначених прикладів визначається таким чином:

$$y^{(\phi_k)} = y_k * \phi_k \tag{3.52}$$

де k - номер виду кібератаки в алфавіті, $\boldsymbol{y_k}$ - середня колективна оцінка того, що цей мережевий запит є кібератакою k-го виду.

Крок 3 - визначення вхідних параметрів. Крок орієнтований на визначення значень вхідних параметрів навчальних прикладів. Прийнято, що номер параметра навчального прикладу дорівнює номеру параметра в БД KDD-99. При цьому параметри БД, що мають перелічуваний тип даних, підлягають цілочисельному кодуванню, а параметри, що мають числовий тип даних, масштабуються в інтервалі від 0 до 1.

Етап 3 виконують доти, доки обсяг навчальної вибірки не перевищить $L_{\phi_k}^{max}(Z_1)$, або доки термін її формування не перевищить $\bar{t}_d$.

Етап 4 - формування навчальних прикладів для вибірки виду Z_2 .

Етап базується на розробленій НСМ розпізнавання кібератак за допомогою експертних знань. Вхід етапу - Φ , D_2 і K_ϕ, вихід - навчальні приклади виду $Z_{2,a} = \{Z_{2,a}^{(\phi_k)}\}_{K_\phi} = \{r_a^{(\phi_k)}\}_{K_\phi}$. При цьому вихідний сигнал подано в символьному вигляді. Суть етапу полягає в тому, що для кожного виду кібератак із переліку Φ реалізується процедура експертного оцінювання даних, яка стосується формування продукційних правил розпізнавання кібератак на підставі аналізу семи параметрів мережевого запиту. Як і у випадку експертного оцінювання мережевих запитів, за базу обрано процедуру експертного оцінювання близькості видів кібератак, яку використано в моделі формування параметрів навчальних прикладів (2.50-2.55). Однак уважають, що на відміну від (2.50) експертні дані, які стосуються деякої кібератаки k-го виду, являють собою матрицю типу:

$$D_{2,k}=\begin{matrix}(X_{k,1,1}^{min}, X_{k,1,1}^{max}) & \dots & (X_{k,n,1}^{min}, X_{k,n,1}^{max}) & \dots & (X_{k,N,1}^{min}, X_{k,N,1}^{max}), y_{k,1} * \phi_k \\ \dots & \dots & \dots & \dots & \dots \\ (X_{k,1,m}^{min}, X_{k,1,m}^{max}) & \dots & (X_{k,n,m}^{min}, X_{k,n,m}^{max}) & \dots & (X_{k,N,m}^{min}, X_{k,N,m}^{max}), y_{k,m} * \phi_k \\ \dots & \dots & \dots & \dots & \dots \\ (X_{k,1,M}^{min}, X_{k,1,M}^{max}) & \dots & (X_{k,n,M}^{min}, X_{k,n,M}^{max}) & \dots & (X_{k,N,M}^{min}, X_{k,N,M}^{max}), y_{k,M} * \phi_k \end{matrix} \quad (3.53)$$

де N - кількість компонент у продукційному правилі для k-го виду кібератаки $(N = 7), X_{k,n,m}^{min}, X_{k,n,m}^{max}$- межі n-го діапазону продукційного правила виду (3.1, 3.2) для k-го виду кібератаки, визначені m-м експертом, $y_{k,m}$- визначена m-м експертом імовірність реалізації кібератаки k-го виду, що визначена передвизначеним продукційним правилом, M - кількість експертів.

З огляду на (3.31), множину D_2 можна представити так:

$$D_2 = \{D_{2,1}, \dots D_{2y_\phi,}\} \quad (3.54)$$

Процедура експертного оцінювання полягає в застосуванні виразів (2.50-2.55) до компонентів (3.53, 3.54). Виходом етапу є навчальні приклади, які входять до складу Z_2 і визначаються виразами виду:

$$z_2^{(\phi_k)} = \{(\left(X_{k,1}^{min}, X_{k,1}^{max}\right), \dots \left(X_{k,7}^{min}, X_{k,7}^{max}\right), y_k * \phi_k)_i\}_I \quad (3.55)$$

де I - кількість прикладів для кібератаки k-го виду.

Етап 4 виконується доки обсяг навчальної вибірки не перевищить $L_{\phi_k}^{max}(Z_2)$ або доки термін її формування не перевищить t_d.

Етап 5 - формування навчальних прикладів для вибірки виду Z_3 . Реалізація цього етапу схожа з реалізацією етапу 3 за винятком того, що вихідний сигнал у навчальних прикладах не розраховується. Вхідними даними є Ω_2 , $L_{\phi_k}^{max}(Z_3), t_d, K_\phi$ та L_ϕа виходом Z_{3a} . Етап виконується доки обсяг навчальної вибірки не перевищить її формування не перевищить $L_{\phi_k}^{max}(Z_3)$, або термін t_d.

Етап 6 - формування навчальних прикладів для вибірки виду Z_4 . Реалізація етапу є симбіозом етапів 3 і 5. Відмінністю є необхідна кількість маркованих і немаркованих навчальних прикладів. Вхід етапу - $K_\phi, \phi, L_\phi^{min}(Z_1), L_\phi^{max}(Z_1), L_{\phi_k}^{max}(Z_3), \Omega_1, \Omega_2, D_3, L_\phi$ а вихід - Z_4 . Виконання етапу розділено на 3 кроки:

Крок 1 - визначення вхідних параметрів. На цьому кроці здійснюється визначення значень вхідних параметрів навчальних прикладів виду Z_1 і Z_3. Процедура визначення аналогічна тій, яка застосовується на третьому кроці третього етапу цього методу.

Крок 2 - експертне оцінювання параметрів мережевого запиту. Цей крок ідентичний першому кроку третього етапу цього методу.

Крок 3 - визначення вихідного сигналу в символьному вигляді. Цей крок ідентичний другому кроку третього етапу цього методу.

Етап 6 виконується доти, доки обсяг навчальної вибірки не перевищить $L_{\phi_k}^{max}(Z_4)$, або доки термін її формування не перевищить t_d .

Етап 7 - визначення вихідного сигналу.

Етап орієнтований на визначення для кожного навчального прикладу виду Z_1 і Z_2 величини очікуваного вихідного сигналу НСМ, яка враховує схожість параметрів видів розпізнаваних кібератак. Вхідними даними етапу є $\Phi, D_1, K_\phi, Z_{1,a}$, і $Z_{2,a}$. Вихід - модифіковані множини $Z_{1,b}$ і $Z_{2,b}$. Етап базується на розробленій моделі формування параметрів навчальних прикладів і розділений на два кроки. Крок 1 - розрахунок міри схожості кібератак. Розрахунок полягає в експертному оцінюванні Φ і обробленні експертних даних за допомогою (2.50-2.55). Вихід кроку - безліч заходів схожості видів кібератак між собою:

$$O = \{O_k\}_{K_\Phi} \tag{3.56}$$

де O_k - оцінка ступеня схожості кібератаки *k*-го виду.

Крок 2 - врахування схожості видів кібератак. Для врахування оцінки ступеня схожості в очікуваному вихідному сигналі навчального прикладу слід у виразах (3.52, 3.56) компонент $y_k * \phi_k$ замінити на $y_k \times o_k$. У результаті виконання цього кроку і-ий навчальний приклад, що належить до Z_1, Z_2 або Z_4 і стосується *k*-го виду кібератаки, можна записати в такому вигляді:

$$z_{1,i}^{(\phi_k)} = (x_1, \dots x_{217})_i, y_{k,i} \times O_{k,i} \tag{3.57}$$

$$z_{2,i}^{(\phi_k)} = (\left(X_{k,1}^{min}, X_{k,1}^{max}\right), \dots \left(X_{k,7}^{min}, X_{k,7}^{max}\right), y_{k,i} \times O_{k,i} \tag{3.57}$$

Етап 8 - масштабування параметрів. Етап передбачає приведення величин параметрів навчальних прикладів до інтервалу значень допустимих для використання в НСМ [17]. Входом етапу є навчальні приклади з множин $Z_{1,b}, Z_{2,b}, Z_{3,a}$. У [17, 18] визначено, що масштабування числових параметрів навчальних прикладів виконується так:

$$\bar{a} = (a - a^{min})/(a^{max} - a^{min}) \tag{3.56}$$

де $a, \bar{a}$ - початкова і масштабована величина параметра, a^{max}, a^{min} - максимальна і мінімальна величина a у вибірці. Тому для кожного з параметрів етап розділено на два кроки.

Крок 1 - визначення екстремумів. На підставі аналізу всіх прикладів навчальної вибірки визначається значення a^{max}і a^{min}.

Крок 2 - реалізація масштабування.Величина параметра масштабується з використанням виразу (3.59).

Вихід етапу - Z_1, Z_2, Z_3. Якщо виходом етапу є Z_2, Z_3 , то на цьому виконання методу закінчується.

Етап 9 - перевірка якості попередньої обробки навчальних прикладів. Входом етапу є навчальна вибірка Z_1 .Для перевірки використовується константа Ліпшица виду:

$$Lp = \max_{i \neq j, x_i \neq x_j} (|y_i - y_j| / ||x_i - y_j||) \qquad (3.60)$$

де x_i, x_j, y_i, y_j - вхідні та вихідні параметри кібератак i, j-го видів. Якість обробки достатня, за умови $Lp \leq K_{Lp} (K_{Lp} \approx 50)$.

У протилежному випадку слід змінити методи масштабування, структуру та обсяг навчальної вибірки. Виходом етапу є сигнал Q, що вказує на завершення формування навчальної вибірки або на необхідність її модифікації.

ВИСНОВКИ

У магістерській роботі розв'язано актуальну науково-прикладну задачу розроблення ефективних нейромережевих моделей, методів і засобів розпізнавання кібератак, адаптованих до умов експлуатації та здатних оперативно розпізнавати нові види мережевих кібератак.

Проведені дослідження дають змогу сформулювати такі висновки:

1) У результаті аналізу науково-практичних праць, присвячених розробці та експлуатації систем розпізнавання кібератак на мережеві ресурси інформаційних систем загального призначення, показано, що одним з основних шляхів розвитку зазначених систем є впровадження методів аналізу мережевого трафіку, що базуються на сучасних рішеннях теорії штучних нейронних мереж. Для цього необхідно розвинути методологічну базу нейромережевого розпізнавання мережевих кібератак і розробити на цій базі метод створення навчальної вибірки та метод створення відповідних нейромережевих засобів. Для апробації запропонованих рішень доцільно розробити нейромережеву систему та провести дослідження її ефективності.

2) Набула подальшого розвитку методологічна база нейромережевого розпізнавання кібератак на мережеві ресурси інформаційних систем, яка за рахунок врахування умов створення таких засобів, забезпечила можливість створення ефективних нейромережевих моделей і методів розпізнавання.

3) Набули подальшого розвитку нейромережеві моделі розпізнавання, які за рахунок можливості навчання за допомогою експертних даних і використання комбінованої навчальної вибірки, дозволяють оперативно реагувати на нові типи мережевих кібератак.

4) Уперше розроблено метод створення навчальної вибірки для нейромережевого розпізнавання мережевих кібератак, який завдяки визначенню параметрів припустимих видів вибірки та врахуванню у вихідному сигналі близькості еталонів видів кібератак, дає змогу визначити коло припустимих видів нейромережевих моделей і забезпечити зменшення кількості навчальних ітерацій приблизно у 2,4 раза.

5) Уперше розроблено метод нейромережевого розпізнавання кібератак на мережеві ресурси інформаційних систем, який завдяки використанню розроблених нейромережевих моделей і розробленого методу створення навчальної вибірки дає змогу розширити функціональні можливості та забезпечити достатню точність розпізнавання.

6) З використанням запропонованих моделей і методів, розроблено та досліджено нейромережеву систему розпізнавання кібератак на мережеві ресурси інформаційних систем. На відміну від відомих нейромережевих засобів, у даній передбачено використання підсистем визначення умов створення нейромережевих засобів, формування адаптивної навчальної вибірки та розробки нейромережевих моделей, що забезпечує достатню точність розпізнавання й адаптацію до умов розроблення та застосування. Експериментальним шляхом показано, що ефективність запропонованої нейромережевої системи приблизно в 1,35 разів вища по відношенню до найкращих подібних систем, а за очікуваних умов застосування її застосування дасть змогу забезпечити похибку розпізнавання мережевих кібератак у межах 0,05, що достатньо для практичного використання. Також показано, що використання розробленого методу створення навчальної вибірки дає змогу приблизно у 2,4 раза зменшити кількість обчислювальних операцій нейромережевої моделі для досягнення припустимої помилки навчання.

СПИСОК ВИКОРИСТАНОЇ ДЖЕРЕЛ

1. 1. Іванов І. І. Застосування нейронних мереж для виявлення вторгнень в інформаційні системи. Проблеми програмування. 2021. No 2. С. 58–66.
2. Сидоренко В. В., Петренко А. П. Методи підвищення стійкості комп’ютерних мереж до атак типу „відмова в обслуговуванні”. Системи обробки інформації. Харків: ХУПС, 2020. Вип. 3(160). С. 51-59.
3. Коваленко А. А. Технології протидії несанкціонованому доступу до інформаційних ресурсів в мережах. Київ: НАУ, 2019. 169 с.
4. Ткаченко О.М. Захист інформації в інтернеті речей на основі блокчейн. Інформаційні технології та комп’ютерна інженерія. 2022. No 1. С. 32–40.
5. Шифрування даних мережевої infraструктури з використанням нейромереж : монографія / за ред. П. І. Рогатина. Львів : Видавництво Львівської політехніки, 2021. 240 с.
6. Білоус О. Інтелектуальний аналіз вразливостей програмного забезпечення на основі нечіткої логіки. Проблеми програмування. 2019. No 1. С. 51–60.
7. Гнатюк С. О. Методи та засоби протидії несанкціонованому доступу до інформаційних ресурсів комп’ютерних мереж. Київ: Каравела, 2020. 244 с.
8. Денисов А. А., Шелест М. Є. Кібербезпека: інтелектуальний аналіз загроз. Черкаси: ЧНУ, 2021. 205 с.
9. Журавель Д.П. Захист від DoS атак мережевого рівня на основі синергетичного підходу. Захист інформації. 2021. Т.23, No 2. С. 117-126.
10. Іванов С.М., Петренко А.І. Методи та моделі штучного інтелекту в системах виявлення кібератак. Сучасний захист інформації. 2022. No 1. С. 58-66.
11. Іскра Ю. Класифікація загроз інформаційній безпеці в корпоративних мережах передачі даних. Міжнародний науковий журнал "Інтернаука". Серія: "Економічні науки". 2020. No 5. С. 19–25
12. Коваль М. М. Методи захисту від DDoS-атак для клієнт-серверних додатків. Проблеми інформатизації та управління. 2021. No 3. С. 106-113.

13. Ковтун М., Субач І., Довбиш А. Мережева безпека. Львів: Новий Світ, 2019. 287 с.
14. Левін М. Атака типу "відмова в обслуговуванні": шляхи протидії. Захист інформації. 2020. Т. 22, No 3. С. 189-199.
15. Макаренко М. Аналіз загроз безпеці обчислювальної мережі на основі багатошарового персептрону. Захист інформації і кібербезпека. 2022. No 1. С. 51-60.
16. Мартинюк О.Б. Моделювання захисту інформаційних ресурсів корпоративних мереж на основі технологій штучного інтелекту. Прикладна математика та комп'ютинг. 2020. Т.2, No 18. С. 63-69.
17. Міночкін А.І., Романюк О.Н. Методи та моделі розпізнавання кібератак. Кібербезпека: освіта, наука, техніка. 2021. No 1. С. 36-45.
18. Міщенко А. В. Аналіз методів протидії DDoS-атакам на інформаційні ресурси. Захист інформації і кібербезпека. 2020. No 1(7). С. 36–43.
19. Мосов С.П., Кобзєва Т.А. Штучні нейронні мережі для виявлення вторгнень в інформаційно-телекомунікаційні системи. Проблеми інформатизації та управління. 2020. No 3. С. 21-31.
20. Орел А.С., Воргуль О.В., Сисоєнко В.М. Методи виявлення атак на веб-ресурси на основі нечіткої логіки. Захист інформації і кібербезпека. 2021. No 2(8). С. 27–35.
21. Пилипчук О. П., Дереза С. С. Моделі та методи захисту інформаційно-комунікаційних мереж. Рівне: НУВГП, 2020. 162 с.
22. Пушкар О.І., Бараннік В.В., Литвиненко О.Є. Застосування технологій штучного інтелекту для кіберзахисту обчислювальних систем та мереж. Вісник Хмельницького національного університету. 2020. No 5. С. 263-267.
23. Рогушина Ю.В., Пазізіна К.М., Передерій О.С. Інтелектуальні методи аналізу мережевого трафіку для виявлення DDOS-атак. Сучасна спеціальна техніка. 2021. No 2(58). С. 61-69.

24. Савченко С.В., Воробйов Ю.В. Нейромережевий підхід до захисту інформації від несанкціонованого доступу. Одеса: ОНАЗ, 2020. 140 с.
25. Сисоєнко В.П., Кузьміна Н.М. Методи машинного навчання для виявлення шкідливого програмного забезпечення в корпоративних мережах. Безпека інформації. 2021. Том 27. No 4. С. 303-310.
26. Складанний П.М. Аналіз DNS-трафіку як спосіб виявлення DDOS-атак на інформаційні ресурси. Захист інформації. 2022. Том 24. No1. С. 23-30.
27. Стрельцов Є.О. Моделі та методи оцінювання захищеності комп'ютерних мереж нейромережними технологіями : монографія. Житомир: ЖНАЕУ, 2021. 210 с.
28. Тесля Д. Ю. Застосування нейромереж для виявлення атак на веб-ресурси. Захист інформації і кібербезпека. 2021. No1. С. 30–36.
29. Ткаченко В.П. Методи та засоби протидії несанкціонованому доступу до інформації в корпоративних мережах. Київ: ДУІКТ, 2021. 203 с.
30. Трофимчук О.М. Аналіз загроз та моделювання захисту комп’ютерної мережі на основі теорії нечітких множин. Збірник наукових праць ЖВІ. 2020. Вип. 17. С. 32-40.
31. Фурашев В.М. Інформаційна безпека комп’ютерних мереж. Київ: НТУУ «КПІ», 2020. 280 с.
32. Харченко В.П., Юдін О.К., Богданович В.Ю. Перспективні моделі та методи захисту інформації від несанкціонованого доступу. Кібербезпека: освіта, наука, техніка. 2021. No 3. С. 50-58.
33. Цимбал В.П., Базова О.А. Моделі та методи захисту інформаційних ресурсів від DoS/DDoS-атак. Захист інформації. 2020. Том 22. No 2. С. 117–130.
34. Чередніченко О.Ю., Тесленко П.В. Захист веб-орієнтованих інформаційних систем на основі нечіткої логіки: монографія. Кривий Ріг: Вид. Р.А. Козлов, 2022. 190 с.

35. Швець Д.Ю., Романкевич В.О. Інтелектуальний аналіз мережевого трафіку для протидії несанкціонованому доступу. Сучасна спеціальна техніка. 2020. No 4 (58). С. 51-59.
36. Шелест М.Є., Максименко І.В. Нейромережевий підхід для виявлення DoS-атак в комп'ютерних мережах критичної інфраструктури. Захист інформації і кібербезпека. 2022. No 1. С. 4-12.
37. Шифрин Б.М. Основы кибербезопасности. Санкт-Петербург: БХВ-Петербург, 2021. 368 с.
38. Щеглюк О.Б. Моделі та методи захисту комп'ютерних мереж від несанкціонованого доступу : монографія. Тернопіль : Вектор, 2020. 311 с.
39. Яремчук Ю.Є., Павлиш В.А. Формалізація загроз інформаційній безпеці в мережах з використанням онтологічного підходу. Захист інформації і кібербезпека. 2021. No2. С. 41-50.
40. Batura O., Muravskyi Ye., Hlumiakova H. Advanced Persistent Threat: Detection Methods Review. 2021 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2021. С. 893-898.
41. Haykin S. Neural Networks and Learning Machines. New York: Pearson, 2009. 936 p.
42. Kumar P., Gurtov A., Iinatti J. et al. Security in Internet of Things: Challenges, Solutions and Future Directions. Helsinki University of Technology. 2019. No8. Pp. 159-184.
43. Lee I. The Internet of Things: A new era for cybercriminal opportunity // Computer Fraud & Security. 2014. No10. Pp. 5–7.
44. Sicari S., Rizzardi A., Miorandi D. Security risks and solutions in distributed IoT scenarios: A survey. arXiv preprint arXiv:2009.00748. 2020.
45. Skuratovskyi D. Protection of computer networks from unauthorized access using machine learning algorithms. Системні технології. 2022. No 2(137). С. 169-178.

46. Sokolowski J. AdaBoost Neural Network in Recognition of Network Attacks // Journal of Telecommunications and Information Technology. 2020. Vol. 2020. No. 2. P. 40–45.

Syer M.D., Shiva S., Bhatia R. Internet of Things to Smart IoT Through Semantic, Cognitive, and Perceptual Computing. Wiley-IEEE Press. 2021. 312 p.

47. Tang Y., Chen Z. Research of network attack and intrusion detection system based on neural network // Journal of Physics: Conference Series. 2021. Vol. 2030.

48. Wu M., Song H. Spatial temporal recurrent neural network for emotion recognition in video // Proceedings of the 2016 ACM on Multimedia Conference. New York, NY, USA. 2016. P. 494–498.