Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Короткової Наталії Романівни*

академічної групи *125-18-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Класифікація атак в інформаційно-комунікаційних мережах з використанням гібридних нейронечітких мереж*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н., доц. Герасіна О.В.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Коротковій Наталії Романівні*** **академічної групи** ***125-18-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Класифікація атак в інформаційно-комунікаційних мережах з використанням гібридних нейронечітких мереж***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів функціонування систем виявлення вторгнень, класифікаційних ознак систем виявлення вторгнень і атак та напрямів їх побудови, а також гібридних Anfis з різними алгоритмами нечітких перетворень.	25.02.2022 – 31.03.2022
Розділ 2	Аналіз існуючих підходів до ідентифікації мережевих атак з використанням систем нечіткого висновку, формулювання задачі ідентифікації та дослідження мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак.	01.04.2022 – 12.05.2022
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	13.05.2022 – 09.06.2022

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Короткова Н.Р.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 12 рис., 1 табл., 4 додатки, 44 джерела.

Об’єкт розробки – мережевий трафік.

Предмет розробки – підхід до ідентифікації мережевих атак з використанням систем нечіткого висновку.

Мета кваліфікаційної роботи – розробка та дослідження алгоритмів адаптивних нейронечітких мереж Anfis на базі різних уявлень нечітких правил, що дозволяють виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки.

Наукова новизна результатів полягає у тому, що використання гібридних мереж Anfis на базі різних алгоритмів нечітких перетворень дозволяють виконувати ідентифікацію мережевих атак.

У першому розділі проаналізовано принципи функціонування систем виявлення вторгнень, класифікаційні ознаки систем виявлення вторгнень і атак та напрями їх побудови, а також нейронечіткі мережі Anfis з різними алгоритмами нечітких перетворень.

У спеціальній частині роботи проаналізовано існуючі підходи до ідентифікації мережевих атак з використанням систем нечіткого висновку, сформульовано задачу ідентифікації мережевих атак та досліджено алгоритми нейронечітких мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.

НЕЙРОНЕЧІТКА МЕРЕЖА, ІДЕНТИФІКАЦІЯ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, БАЗИ ЗНАНЬ, НЕЧІТКІ ПРАВИЛА, МЕРЕЖЕВІ АТАКИ, КЛАСИФІКАЦІЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

РЕФЕРАТ

Пояснительная записка: 73 с., 12 рис., 1 табл., 4 приложения, 35 источников.

Объект разработки – сетевой трафик.

Предмет разработки – подход к идентификации сетевых атак с использованием систем нечеткого вывода.

Цель квалификационной работы – разработка и исследование алгоритмов адаптивных нейронечетких сетей Anfis на основе различных представлений нечетких правил, позволяющих выполнять классификацию входящего трафика сети для идентификации различных инцидентов кибербезопасности.

Научная новизна результатов заключается в том, что использование гибридных сетей Anfis на базе различных алгоритмов нечетких преобразований позволяет идентифицировать сетевые атаки.

В первой главе проанализированы принципы функционирования систем обнаружения вторжений, классификационные признаки систем обнаружения вторжений и атак, и направления их построения, а также нейронечеткие сети Anfis с разными алгоритмами нечетких преобразований.

В специальной части работы проанализированы существующие подходы к идентификации сетевых атак с использованием систем нечеткого вывода, сформулирована задача идентификации сетевых атак и исследованы алгоритмы нейронечетких сетей Anfis на основе различных представлений нечетких правил для идентификации сетевых атак. По результатам исследований сделаны выводы о решении поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, экономического эффекта и срока окупаемости капитальных инвестиций по применению предложенных решений.

НЕЙРОНЕЧЕТКАЯ СЕТЬ, ИДЕНТИФИКАЦИЯ, СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, БАЗЫ ЗНАНИЙ, НЕЧЕТКИЕ ПРАВИЛА, СЕТЕВЫЕ АТАКИ, КЛАССИФИКАЦИЯ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ABSTRACT

Explanatory note: p. 73, fig. 12, tab. 1, 4 additions, 44 sources.

The object of development is network traffic.

The subject of development is an approach to the identification of network attacks using fuzzy inference systems.

The purpose of the qualification work is to develop and study the algorithms of adaptive fuzzy Anfis networks based on different representations of fuzzy rules that allow the classification of incoming network traffic to identify various cybersecurity incidents.

The scientific novelty of the results is that the use of Anfis hybrid networks based on various fuzzy transformation algorithms allows the identification of network attacks.

The first section analyzes the principles of operation of intrusion detection systems, classification features of intrusion and attack detection systems and directions of their construction, as well as fuzzy Anfis networks with different algorithms for fuzzy transformations.

The special part of the paper analyzes the existing approaches to network attack identification using fuzzy inference systems, formulates the problem of network attack identification and investigates algorithms of fuzzy Anfis networks based on different representations of fuzzy rules for network attack identification. Based on the results of research, conclusions were made on the solution of the problem.

In the economic section, calculations of capital costs, economic effect and payback period of capital investments are performed using the proposed solutions.

NEURO-FUZZY NETWORK, IDENTIFICATION, INVASION DETECTION SYSTEMS, KNOWLEDGE BASES, FUZZY RULES, NETWORK ATTACKS, CLASSIFICATION, SOFTWARE

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІКМ – Інформаційно-комунікаційна мережа;

ІАД – Інтелектуальний аналіз даних;

ІТ – Інформаційні технології;

МНК – Метод найменших квадратів;

НМ – Нейронна мережа;

ПЗ – Програмне забезпечення;

СВА – Системи виявлення атак;

СВВ – Система виявлення вторгнень;

ШІ – Штучний інтелект;

Anfis – Adaptive Neuro Fuzzy Inference System – Адаптивна мережа нечіткого висновку.

ЗМІСТ

ВСТУП

Розвиток інформаційних технологій (ІТ) відбувається настільки швидко, що класичні механізми захисту, не здатні залишатися ефективними та забезпечувати відповідну безпеку ресурсам інформаційно-комунікаційних систем і мереж (ІКМ), а шкідливе програмне забезпечення (ПЗ) та інші кіберзагрози стають все більш поширеними [1-12].

Також, в останні роки, проходить значне збільшення обсягів інформації, яка накопичується, зберігається та обробляється за допомогою різних ІКМ. При цьому, концентрування в єдиних базах даних інформації різного призначення, а також швидке розширення кола користувачів, що мають безпосередній доступ до ресурсів ІКМ, утворюють проблему забезпечення їх захисту від різного роду вторгнень. Зростання складності апаратно-програмних засобів та існуючі недоліки сучасних ІТ призводять до удосконалення кібератак. Необхідно зазначити, що несанкціоновані дії на ресурси ІКМ здійснюють впив і на середовище оточення, породжуючи в ньому, як наслідок, певні аномалії. Таке середовище зазвичай гетерогенне, нечітко визначене, а для вирішення задач виявлення кібератак, які утворили аномалії в цьому середовищі, необхідні відповідні засоби. Такі засоби повинні надавати можливість виявлення вторгнень за множиною різних характерних ознак, включаючи їх динамічну складову, яка контролюється в реальному режимі часу.

У зв'язку з цим, необхідні спеціальні засоби, що дозволяють оперативно виявляти та попереджувати порушення безпеки. Для цього застосовуються системи виявлення вторгнень (СВВ), які є невід'ємною частиною будь-якої сучасної системи безпеки, а світова тенденція свідчить про те, що виявлення вторгнень, стане обов'язковою функцією операційної системи та вже застосовується в різному ПЗ. Особливо необхідні СВВ, які орієнтовані на виявлення аномальних станів. Вони, як правило, формують (містять) профіль нормальної (ненормальної) активності в ІКМ та детектують відхилення від нього [11-12].

Наразі питання забезпечення необхідного рівня мережевої безпеки та захисту від кібератак активно вивчаються різними дослідниками у галузі машинного навчання та аналізу даних. Пов'язано це з тим, що існуючі інтелектуальні алгоритми аналізу дозволяють вирішувати завдання пошуку аномалій та виявлення всіляких взаємозв'язків усередині даних тощо [13-15]. Однак, у будь-якій з представлених систем формування інтелектуальних рішень, результат, як правило, залежить як від інструментів і алгоритмів навчання, що використовуються, так і від якості даних, на яких будується деяка модель.

Зниження якості даних відбувається як під дією об'єктивної невизначеності, що виявляється в шумах, аномаліях, викидах тощо, так і під дією лінгвістичної невизначеності, що виявляється через суб'єктивність оцінки експертів [13]. Наразі для підвищення якості даних через об'єктивну невизначеність розроблено комплекс методів та алгоритмів обробки та фільтрації, при цьому вплив суб'єктивності експертів є найскладнішим завданням, ефективність у вирішенні якого показали системи нейронечіткого висновку.

Проблема формування бази нечітких правил полягає у розробці оптимальних функцій належності та створенні терм-множин, що дозволяють створити систему нечіткого висновку, яка не залежить від суб'єктивних оцінок фахівців у тій чи іншій галузі. Одним з методів, покликаних вирішити цю проблему, є побудова нейронечіткої мережі Anfis (Adaptive Neuro Fuzzy Inference System – адаптивна мережа нечіткого висновку) [14, 16-18].

Таким чином, дослідження, розробка і вдосконалення підходів до ідентифікації мережевих атак з використанням нечіткої логіки наразі є актуальною задачею.

Метою роботи є розробка та дослідження алгоритмів адаптивних нейронечітких мереж ANFIS на базі різних уявлень нечітких правил, що дозволяють виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки.

Постановка задачі:

• проаналізувати принципи функціонування систем виявлення вторгнень, а також класифікаційні ознаки систем виявлення вторгнень і атак та напрями їх побудови;

• провести аналіз нейронечітких мереж Anfis з різними алгоритмами нечітких перетворень;

• провести аналіз існуючих підходів до ідентифікації мережевих атак з використанням систем нечіткого висновку;

• сформулювати задачу ідентифікації мережевих атак з використанням нейронечітких мереж Anfis;

• дослідити алгоритми адаптивних нейронечітких мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Принципи функціонування систем виявлення вторгнень

Наразі системи виявлення вторгнень і атак, зазвичай, являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, СВВ стали необхідним компонентом інфраструктури безпеки більшості організацій.

Сучасні мережеві СВВ зазвичай складаються з п'яти функціональних компонентів, а саме:

1. Модуль збору даних – призначений для реєстрації параметрів мережевого трафіку, що передається відповідно до різних протоколів.

2. Модуль зберігання даних – у якому накопичуються первинні статистичні дані та результати аналізу.

3. Модуль аналізу – приймає інформацію з модулів збору та зберігання даних та аналізує дані на наявність ознак мережевої кібератаки. Результат спрацьовування модуля – розпізнаний стан захищеності мережевого ресурсу. У найпростішому випадку (системи виявлення атак (СВА)) розпізнаються лише два стани – нормальний або стан реалізації мережевої кібератаки. У сучасних мережевих СВА додатково розпізнаються відомі види мережевих кібератак. Крім цього, може розраховуватись ймовірність (достовірність) кожного із заздалегідь визначених станів захищеності. Це збільшує гнучкість реалізації захисних заходів.

4. Модуль реагування – активується у тому випадку, коли аналізуючий механізм визначив наявність кібератаки. Якщо СВА діє автономно, результатом спрацьовування даного модуля є сигналізація про параметри кібератаки. У разі

інтеграції СВА із системою реагування на кібератаку реалізується певний набір захисних заходів.

5. Консоль управління, призначена для налаштування інших модулів та системи в цілому.

Типова послідовність функціонування сучасної мережевої СВВ показана на рис. 1.1.

Рисунок 1.1 – Типова послідовність функціонування сучасної мережевої СВВ

Як показує практика та результати досліджень у цій галузі, основним напрямком удосконалення сучасних СВВ є підвищення ефективності аналізу мережевого трафіку.

Як правило, методи виявлення атак розділяють на методи виявлення зловживань і методи виявлення аномалій [1-10]. Зловживання засновані на використанні існуючих недоліків ІКМ. Основною відмінністю між аномалією і

зловживанням є те, що аномалія – це процес, який виникає перед можливим вторгненням в систему або вказує на наявність вже існуючої атаки. Фактично, аномалія – це відхилення від нормального стану системи, незвичайна активність в ній, що може свідчити про певні атакуючі дії. Слід зазначити, що аномалія може виникнути і за інших причин, наприклад, внаслідок неправильної роботи системи.

Саме тому за допомогою ефективного аналізу аномалій, що виникають у системі, можна попередити кібератаки певних типів і вчасно вжити необхідних заходів щодо їх блокування та захисту ІКМ.

Варто сказати, що широке використання сучасних засобів захисту від кібератак не гарантує безпеки на належному рівні, оскільки останнім часом [19-23]:

- зростають атаки, спрямовані на корпоративні системи, публічні, конфіденційні та державні інформаційні ресурси;
- кібератаки, постійно модифікуються, удосконалюються і стають більш регулярними;
- виявлення кібератак класичними засобами захисту не завжди є ефективним;
- частішають випадки здійснення складних атак на ІКМ.

Все вищевказане також пов’язане з інтенсивним розвитком програмно-апаратних засобів і глобалізації інформаційних мереж та їх повсякденного використання у всіх сферах діяльності суспільства.

1.2 Класифікаційні ознаки систем виявлення вторгнень і атак та напрями їх побудови

Більшість існуючих класифікацій СВВ дуже абстрактні, не є повними, і у них значні важливі характеристики (елементи) потребують доповнень та узагальнень [24].

Один з варіантів класифікаційних ознак систем виявлення і запобігання атак представлений на рис. 1.2.

Рисунок 1.2 – Класифікаційні ознаки систем виявлення і запобігання атакам

Першою класифікаційною ознакою систем виявлення атак є класифікація за середовищем моніторингу, тобто в залежності від того де здійснюється збір інформації: в мережі, на конкретному комп'ютері чи на певних додатках, що працюють на комп'ютері

Більшість класифікацій розділяють СВА за даною ознакою на два типи: СВА на рівні мережі та СВА на рівні вузла. Проте сьогодні наявність одного типу зменшує свою ефективність через відсутність іншого, тому досить популярною стає розробка гібридних або комбінованих систем які успішно функціонують як на рівні мережі так і на рівні вузла. А зі збільшенням спектра надання додаткових послуг та появою такого поняття як додаток (application) виникла необхідність моніторингу безпеки на рівні додатків. Тому доцільно

класифікувати системи виявлення атак за середовищем моніторингу таким чином: на рівні мережі, на рівні вузла, гібридні (комбіновані) та на рівні додатків.

Другою ознакою класифікації СВА є поділ за методом виявлення загроз. Прийнято розділяти системи виявлення атак на ті, що засновані на використанні методу виявлення сигнатур, і ті, що базуються на використанні методу виявлення аномалій. Наразі методи виявлення аномалій являються пріоритетними у побудові СВВ. Найпопулярнішими серед них можна виділити чотири підгрупи, а саме:

- статичне виявлення аномалій;
- виявлення засноване на інтелектуальному аналізі даних (ІАД);
- виявлення засноване на існуючих знаннях;
- виявлення на основі машинного навчання.

Також в більшості класифікацій відсутні гібридні методи, які стрімко досліджуються сьогодні і являють собою синтез сигнатурного методу і методу виявлення аномалій.

Наступною класифікаційною ознакою є поділ за архітектурою. В залежності від архітектури СВА виділяють системи, на якій виконується програмне забезпечення (host) і системи, за якими спостерігають (target). Раніше СВА, переважно, виконувалися на тих же системах, які вони захищали, проте з появою робочих станцій і персональних комп'ютерів у більшості архітектур СВА передбачається виконання СВА на окремій системі, тим самим розділяючи системи host і target. Це поліпшує безпеку функціонування СВА.

За характером відповіді системи виявлення атак поділяють на активні та пасивні. СВА може реагувати на вторгнення в пасивній чи активній формі. Пасивні заходи частіше всього являють собою звіт СВА, зроблений для людей, які потім виконують деякі дії на основі даного звіту. Коли система виявлення атак активно реагує на вторгнення вона може додатково змінити стан об'єкта, що піддався атаці, або, в рідкісних випадках, змінити стан зловмисника. Активні заходи над об'єктом, що піддався атаці, мають на увазі автоматичне

втручання в деяку іншу систему (наприклад, керування комутатором або мережним екраном).

Ще однією ознакою класифікації систем виявлення атак є розподіл за принципом роботи на статичні та динамічні. Не кожна сучасна класифікація систем виявлення атак має подібну класифікаційну ознаку, а все через те, що більшість науковців вважають статичні СВА морально застарілими. Проте, існують інформаційні системи які не несуть в собі безліч важливої інформації та не підлягають постійному нападу зі сторони зловмисників, тому й не потребують складних механізмів реалізації динамічних СВА.

Статичні системи роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе програмне забезпечення, помилки в конфігураціях, перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів.

Динамічні СВА здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні СВВ реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

Наступною ознакою класифікації є розподіл за часом реакції. Багато ранніх систем виявлення атак були пакетного типу, тобто вони цілком залежали від накопичення записів аудиту в операційній системі. СВА пакетного режиму не виконують ніяких активних дій у відповідь на виявлені атаки. Даний тип деякий час розглядався як єдиний можливий, але наразі були додані СВА у реальному часі.

Також доцільно класифікувати системи виявлення атак за джерелом аудиту. СВА виявляють вторгнення на основі аналізу даних, зібраних з використанням різних джерел аудиту. Зібрані дані представляють систему, додатки і поведінку мережі. Успішне виявлення вторгнень залежить від повноти даних зібраних з джерел аудиту, швидкості збору та обробки даних.

Дані з журналів аудиту комп'ютерних систем несуть в собі інформацію про користувальницьку діяльність на даній машині. У разі успішної атаки, вони уразливі для змін, тому вони актуальні лише до моменту здійснення атаки.

Ще однією важливою ознакою класифікації систем виявлення атак є розподіл за технологіями побудови. При розгортанні СВА важливо знати, які технології використовуються в побудові інформаційної системи. Адже дротові мережі, порівняно з бездротовими, використовують різні і специфічні методи безпечної передачі, наприклад, шифрування. Тому фізична мережа передачі даних відіграє важливу роль у проектуванні систем виявлення атак.

Провідні мережі, як правило, швидші і дешевші, ніж бездротові. Деякі з мережевих функцій, таких як, поведінка трафіка і топології мережі, можуть бути використані для виявлення вторгнень у провідних мережах зв'язку. Мобільні бездротові мережі являють собою набір мобільних вузлів, що автоматично самонастроюються без допомоги фіксованої інфраструктури або централізованого управління. Вони бувають: ієрархічні, мобільні агенти, автономні та розділенні і кооперативні. Ієрархічні СВА призначені для багатошарових мережевих інфраструктур, де мережа ділиться на кластери.

За парадигмою виявлення СВА поділяються на ті що оцінюють стан і ті що оцінюють переходи між станами. Парадигма виявлення описує, як СВА оцінює вторгнення і може бути двох типів. Перший тип оцінює стан щоб дізнатись чи є він безпечним чи вразливим. Другий тип оцінює переходи міг станами, а саме переміщення з безпечного стану в незахищений.

Ще однією з класифікаційних ознак систем виявлення атак є розподіл за режимом збору даних. Дані аудиту можуть бути зібрані в розподіленому режимі з декількох різних місць або джерел, або вони можуть бути зібрані централізовано від одного джерела.

Окремо необхідно відмітити СВА основаних на методах Data Mining. Проаналізуємо їх. Виявлення атаки з допомогою скритої марковської моделі. Скрита марковська модель представляє собою статистичну модель, де система моделюється як процес Маркова з невідомими параметрами. Задача методу

полягає в оцінці скритих параметрів, що базуються на параметрах, які спостерігаються. Послідовності подій, зібрані з нормальних операційних систем, використовуються в якості навчальної вибірки для оцінки параметрів прихованої марковської моделі. Після навчання скритої марковської моделі ймовірнісні оцінки використовуються в якості порогових значень для ідентифікації мережевих аномалій в тестових даних.

Виявлення атак за допомогою байєсовських мереж. Байєсовська мережа являє собою модель, яка кодує імовірнісні взаємозв'язки між змінними. Основний метод застосування баєсовських мереж передбачає незалежність серед атрибутів. Кілька варіантів застосування байєсовських мереж були запропоновані для виявлення мережевих аномалій. Більшість методів направлено на формування умовних залежностей між атрибутами з використанням складних мереж Байєса. Байєсовські методи часто використовуються в процедурі класифікації і локалізації помилкових спрацьовувань. Для виявлення вторгнень або прогнозування поведінки порушника байєсовські мережі можуть бути ефективними в деяких випадках, але в загальному випадку точність цього методу залежить від припущень, пов'язаних з поведінкою моделі цільової системи. Таким чином, будь-яке значне відхилення від припущень призведе до зменшення точності виявлення.

Виявлення атак за допомогою методів кластеризації. Методи кластеризації групують дані в кластери на підставі схожості об'єктів. Більшість методів кластеризації починається з вибору центральної точки для кожного кластера, а множина елементів розподіляється по кластерам. Після цього центри коригуються, а елементи перерозподіляються. Кластеризація дозволяє вивчити і виявити аномалії, не вимагаючи множини класів або типів аномалій, тобто для виявлення аномалій за допомогою методів кластеризації не виникає потреби в навчальній множині. Кластеризація досить широко застосовується для виявлення мережевих аномалій.

Виявлення невідомих мережевих атак найчастіше будується саме на методах кластеризації. Однорідні групи зі схожими характеристиками або

кластери формуються шляхом розбиття набору елементів без будь-яких позначок. В системі вкрай важливо правильно визначити кластери, щоб максимально віддалити їх від викидів. Кінцева мета даних методів полягає у визначенні ступеня відхилення викидів від кластерів. За допомогою простого порівняння з пороговим значенням викиди з високим ступенем відхилення від кластерів позначаються як аномалії.

Виявлення атак за допомогою методу опорних векторів. Даний метод є одним з найбільш популярних методів класифікації. Метод будує оптимальну гіперплощину в просторі характеристик: $w \times x - b = 0$, що розділяє нормальні і аномальні елементи. Характерною особливістю методу опорних векторів є постійне скорочення емпіричної помилки класифікації і збільшення зазору між класами. Тому даний метод часто називають методом класифікатора з максимальним зазором. Метод відшукує елементи, що знаходяться на кордонах між двома класами, які і називаються опорними векторами.

Виявлення атак за допомогою нейронних мереж (НМ) [14]. Інтерес до штучних НМ викликаний тим фактом, що людський мозок виробляє обчислювальні операції принципово іншим чином, ніж звичайна цифрова обчислювальна машина. НМ представляють множину інструментів для самих різних застосувань: кластеризація даних, витяг ознак, скорочення розмірності тощо.

Виявлення атак за допомогою генетичних алгоритмів [14]. Генетичні алгоритми являють собою обчислювальну модель, засновану на принципах еволюції і природного відбору. При такому підході завдання, яке необхідно вирішити, перетворюється в середовище, яка використовує хромосомну структуру даних. Хромосоми розвивалися протягом багатьох поколінь, використовуючи такі операції, як вибір, рекомбінація і мутація. У задачі виявлення мережевих аномалій, хромосома для записів містить гени, що відповідають таким атрибутам, як сервіси, прапори, кількість звернень і т.д.

Виявлення атак за допомогою правил нечіткої логіки [14]. Нечіткі системи виявлення мережевих вторгнень використовують множину нечітких

правил для визначення ймовірності конкретних або загальних мережевих атак. Нечітка множина може бути сформована для опису трафіка в конкретній мережі. В роботі [25] описується метод для побудови класифікаторів, що використовують нечіткі асоціативні правила, які застосовуються для виявлення вторгнення в мережу. Нечіткі набори правил асоціації використовуються для опису нормальних і аномальних класів. Належність запису певному класу визначається за допомогою відповідної метрики. Нечіткі асоціативні правила формуються на основі звичайних навчальних вибірок. Тестований зразок класифікується як нормальний, якщо згенерований сукупністю правил показник буде вище певного порогового значення. Зразки з більш низьким показником вважаються аномальними.

Отже, узагальнений вигляд класифікації систем виявлення загроз представлений на рис. 1.3.

Взагалі кажучи, сучасні системи виявлення вторгнень і атак ще далекі від ергономічних і ефективних, з точки зору безпеки рішень. Підвищення ефективності ж слід ввести не тільки в області виявлення зловмисних дій на інфраструктуру захищених об'єктів інформатизації, але і з точки зору повсякденної експлуатації цих засобів, а також економії обчислювальних та інформаційних ресурсів власника даної системи захисту.

Якщо говорити безпосередньо про модулі обробки даних, то, кожна сигнатура атаки в системі обробки інформації про атаку є базовим елементом для розпізнавання більш загальних дій – розпізнавання фази атаки (етапи її реалізації). Саме поняття сигнатури узагальнюється до деякого вирішального правила. А кожна атака навпаки розбивається на набір етапів її проведення. Чим простіша атака, тим простіше її виявити і більше з'являється можливостей щодо її аналізу. Сценарій атаки представляє собою граф переходів, в аналогічний графу кінцевого детермінованого автомата. А фази атак можна описати, наприклад, наступним чином: випробування портів; ідентифікація програмних і апаратних засобів; збір банерів; застосування експлойтів; дезорганізація функціоналу мережі з допомогою атак на відмову в

обслуговуванні; управління через бекдори; пошук встановлених троянів; пошук проксі-серверів; видалення слідів присутності тощо.

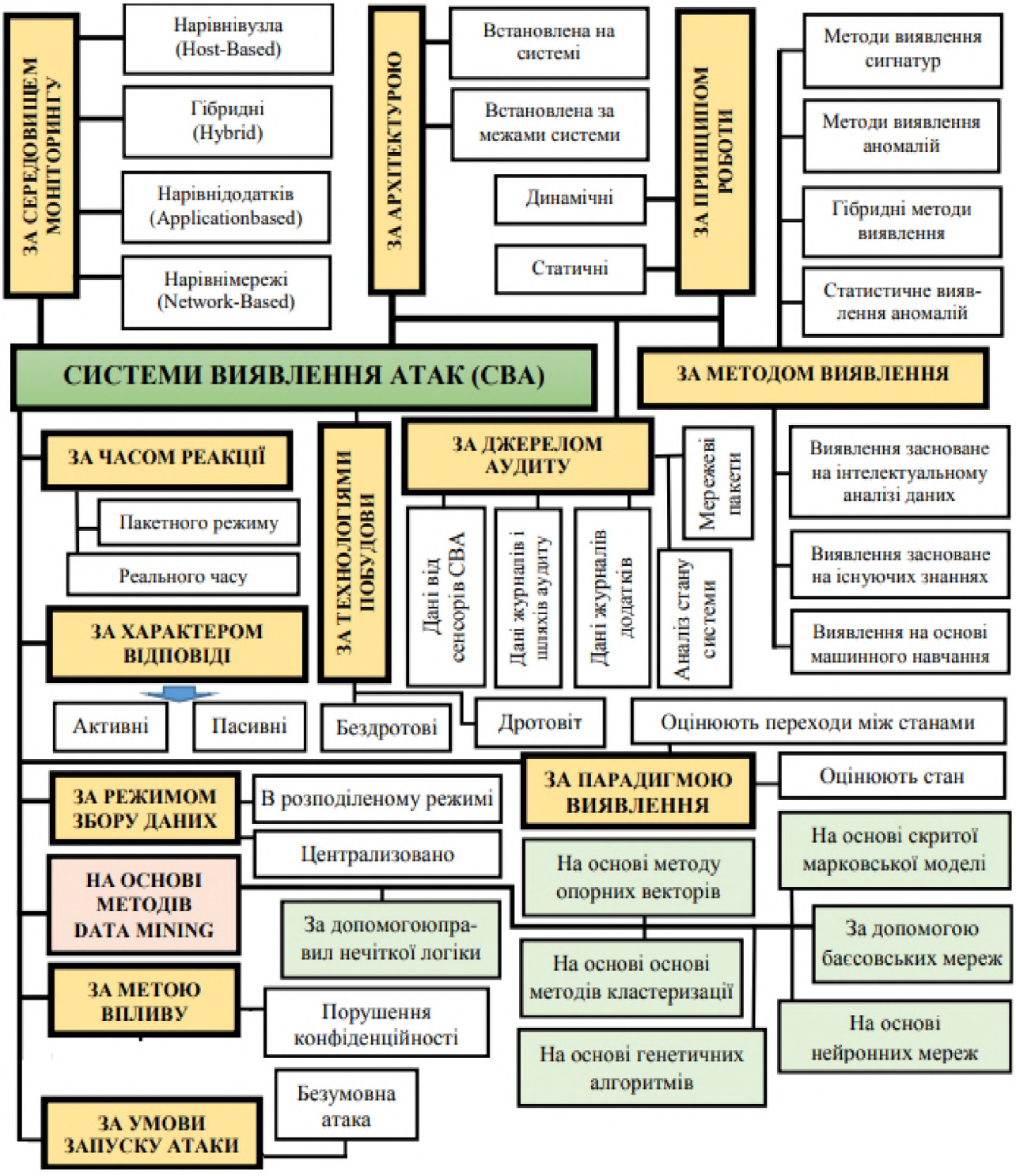

Рисунок 1.3 – Узагальнений вигляд класифікації систем виявлення вторгнень та атак

Переваги такого підходу очевидні – у разі роздільної обробки різних етапів атаки з’являється можливість розпізнавати загрозу ще в процесі її підготовки і формування, а не на стадії її реалізації, як це відбувається в існуючих системах. При цьому, елементною базою для розпізнавання може бути як сигнатурний пошук, так і виявлення аномалій, використання експертних методів та систем, довірчих стосунків та інших інформаційних, вже відомих і реалізованих, мережевих і локальних примітивів оцінки того, що відбувається в інформаційному середовищі потоку подій.

Узагальнюючий підхід до аналізу дозволяє визначати відповідно й розподілені загрози, як у логічному так і фізичному просторі. Загальна схема обробки вступників подій також дозволяє здійснювати пошук розподілених атак – шляхом подальшої агрегації даних з різних джерел і конструювання мета-даних про відомі інциденти.

1.3 Нейронечіткі мережі

Наразі характерним є широке застосування методів систем штучного інтелекту (нейронних мереж, систем нечіткого висновку тощо) для моделювання складних процесів в системах кібербезпеки. Для побудови систем штучного інтелекту використовують різні підходи. Найбільш популярними наразі, і вже «класичними» є структурний та логічний підхід [14].

При структурному підході здійснюють спроби систем штучного інтелекту (ШІ) шляхом моделювання структури людського мозку. Однією з перших таких спроб був перцептрон Ф. Розенблатта. Пізніше виникли й інші моделі, які наразі відомі під терміном «нейронні мережі». Ці моделі розрізняються за будовою окремих нейронів, за топологією зв'язків між ними і за алгоритмами навчання. Для нейронних моделей характерна більша виразність, легке розпаралелювання алгоритмів, а також пов'язана з цим висока продуктивність паралельно реалізованих НМ.

Основою для логічного підходу служить булева алгебра, яка має свій подальший розвиток у вигляді числення предикатів, в якому вона розширена за рахунок введення предметних символів, відносин між ними, кванторів існування та загальності. Домогтися більшої виразності логічного підходу дозволяє такий напрям, як нечітка логіка.

Теорію нечітких множин запропонував в 1965 р. професор Лотфі Заде, який розширив класичне поняття множини, допустивши, що характеристична функція (функція належності елемента множині) може приймати будь-які значення в інтервалі [0; 1], а не тільки значення 0 або 1. Подальші роботи Л. Заде і його послідовників заклали міцний фундамент нової теорії і створили передумови для впровадження методів нечіткого висновку в інженерну практику.

Для більшості логічних методів характерна велика трудомісткість, оскільки під час пошуку доказу можливий повний перебір варіантів. Тому даний підхід вимагає ефективної реалізації обчислювального процесу, і його працездатність, зазвичай, гарантується при порівняно невеликому розмірі бази даних.

Кожна з систем ШІ має свої особливості, що робить їх найбільш придатними для вирішення одних задач і менш придатними – для інших. Взагалі, системи з нечіткою логікою і штучні НМ еквівалентні один одному, проте, на практиці у них є свої власні переваги і недоліки.

Так, НМ ефективні для задач розпізнавання образів, але дуже незручні для з'ясування питання, як вони таке розпізнавання здійснюють. Вони можуть автоматично здобувати знання, але процес їх навчання може відбуватися досить повільно, а аналіз навченої мережі досить складний (навчена мережа зазвичай – «чорний ящик» для користувача). При цьому будь-яку апріорну інформацію (знання експерта) для прискорення процесу її навчання в НМ ввести неможливо.

Системи ж з нечіткою логікою, навпаки, ефективні для пояснення отриманих з їх допомогою висновків, але вони не можуть автоматично

здобувати знання для використання їх в механізмах висновків. Необхідність розбивки універсальних множин на окремі області, зазвичай, обмежує кількість вхідних змінних в таких системах невеликим значенням.

Для усунення недоліків НМ і систем з нечіткою логікою запропоновані гібридні мережі, в яких висновки робляться на основі апарату нечіткої логіки, але відповідні функції належності підлаштовуються із використанням алгоритмів навчання НМ, наприклад, алгоритму зворотного поширення похибки. Такі системи не тільки використовують апріорну інформацію, але й можуть набувати нових знань, а для користувача є логічно прозорими.

Отже, гібридна НМ – це мережа з чіткими сигналами, вагами і активаційною функцією, але з об'єднанням сигналів і ваг з використанням *t*-норми, *t*-конорми або деяких інших безперервних операцій. Входи, виходи і ваги гібридної мережі – речові числа, що належать відрізку [0,1].

Одним з перших варіантів гібридних мереж є Anfis (Adaptive Neuro Fuzzy Inference System) – адаптивна мережа нечіткого висновку.

Нейронечіткі мережі Anfis дозволяють вхідним сигналам за допомогою нечітких перетворень (алгоритмів Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя) та апроксимації зіставити вихідний сигнал. Ці методи дозволяють апроксимувати довільні безперервні функції, залежні від багатьох змінних, сумою функцій, залежних від однієї змінної, із заданою точністю. Розглянемо основні ідеї побудови нейронечітких мереж Anfis із застосуванням даних алгоритмів, а також представимо підходи до формування нейронечіткого висновку.

1.3.1 Нейронечітка мережа Anfis із застосуванням алгоритму Сугено-Такагі

Алгоритм Сугено-Такагі використовує наступну модель нечіткого правила [14, 26]:

R_i: ЯКЩО x_1 це A_{i1}, … І x_n це A_{in}, ТО $y=f(X)$,

де $X=(x_1,x_2,\ldots,x_n)$; $f(X)$ – деяка чітка функція, наприклад, поліном першого порядку.

Визначаються рівні «відсікання» a_i для лівої частини кожного з правил відповідно до виразу $a_i = \min_j\left(A_{ij}(x_j)\right)$, $i=1,\ldots m$, $j=1,\ldots n$ та розраховуються «індивідуальні» виходи правил R_i,

$$y_i^* = p_{10} + \sum_{i=1}^{n} p_{ij} x_j \ , \tag{1.1}$$

де p_{i0}, p_{ij} – коефіцієнти полінома або цифрові ваги, які уточнюються в процесі аналізу даних.

Блок дефазифікації здійснює перехід від нечіткого значення лінгвістичної змінної (управління) до числового значення. У разі спрощеного алгоритму нечіткого виведення (алгоритм Сугено нульового порядку), коли $y_i = f(X) = p_{i0}$, слідує

$$y(x_1, x_2, \ldots, x_n) = \frac{\sum_{i=1}^{m} \min_j\left(\mu_{ij}(x_j)\right) p_{i0}}{\sum_{i=1}^{m} \min_j\left(\mu_{ij}(x_j)\right)} \ . \tag{1.2}$$

Нейронечітка мережа Anfis, відповідна моделі нечіткого висновку Сугено-Такаги, представлена на рис. 1.4.

Мережа Anfis є п'ятишаровою штучною НМ прямого розповсюдження сигналу, алгоритм реалізації наступний:

- перший шар – терми вхідних змінних;
- другий шар – посилки (антецеденти) нечітких правил;
- третій шар – нормалізація ступенів виконання правил;
- четвертий шар - укладання правил;
- п'ятий шар – агрегування (композиція) результату, отриманого за різними правилами.

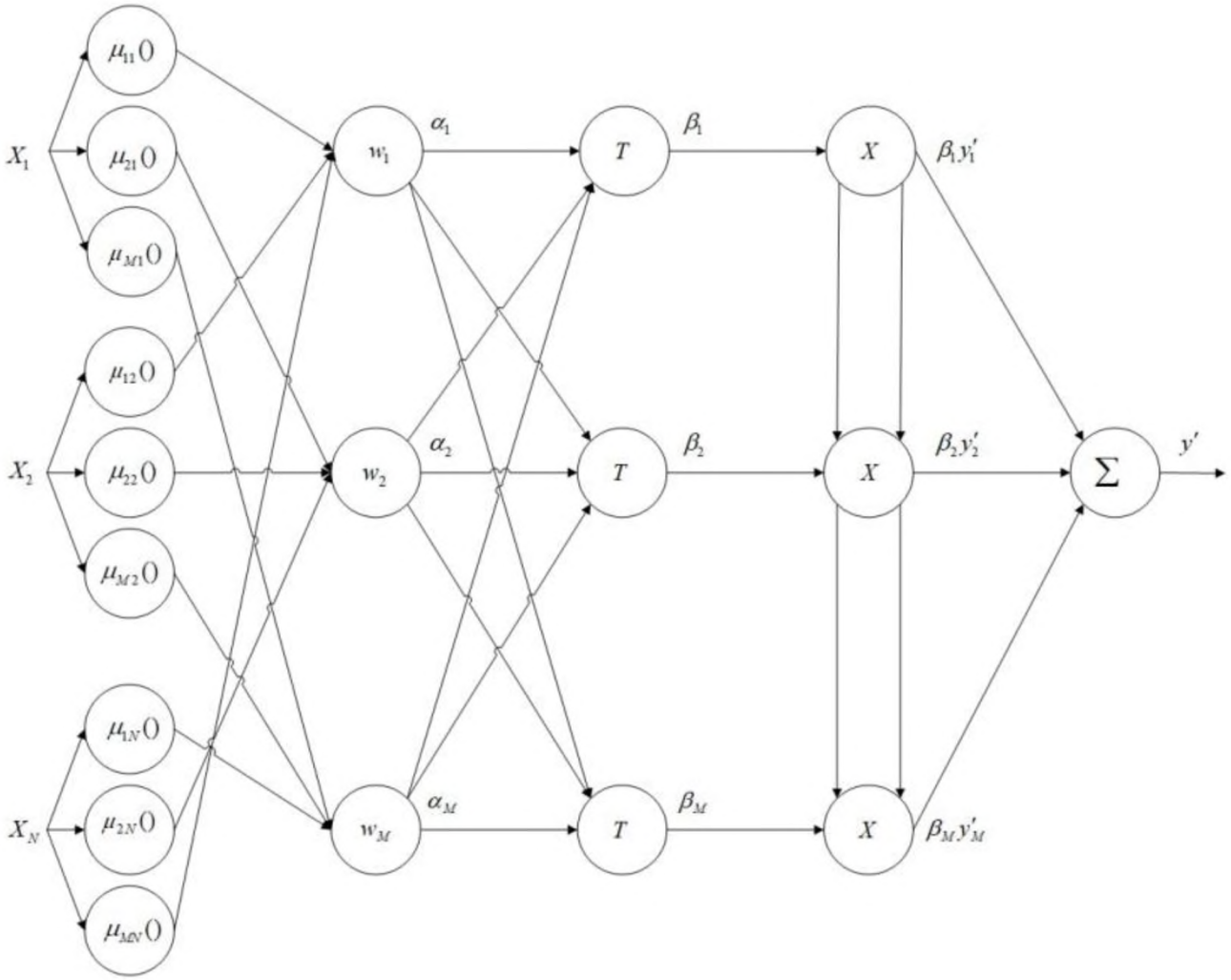

Рисунок 1.4 – Нейронечітка мережа Anfis з використанням висновку Сугено-Такагі

Шар 1. Входи мережі з'єднані лише з термами. Кількість вузлів першого шару дорівнює сумі потужностей терм-множин вхідних змінних, де операція фазифікації виконана на синглетонній базі.

Шар 2. Кількість вузлів другого шару *m*. Кожен вузол цього шару відповідає одному нечіткому предиктивному правилу.

Вузол другого шару з'єднаний із тими вузлами першого шару, які формує посилки відповідного правила. Отже, кожен вузол другого шару може приймати від 1 до *n* сигналів. Виходом вузла є ступінь виконання правила, яка розраховується як добуток вхідних сигналів (по Ларсену). Позначимо виходи вузлів цього шару τ_r, r=1,…, $\overline{m}$, де $\overline{m}$ – кількість нечітких правил.

Шар 3. Кількість вузлів третього шару дорівнює $\overline{m}$. Кожен вузол цього шару розраховує відносний рівень виконання нечіткого правила (нормалізація) за формулою

$$\tau_r^* = \frac{\tau_r}{\sum_{j=1}^{m} \tau_j}. \tag{1.3}$$

Шар 4. Кількість вузлів шару також дорівнює *m*. Кожен вузол з'єднаний з одним із вузлів третього шару, а також з усіма входами мережі. Вузол четвертого шару розраховує внесок одного нечіткого правила у вихід мережі за формулою:

$$y_r = \tau_r^* \left(b_{0,r} + b_{1,r} x_1 + \ldots + b_{n,\text{r}} x_n \right). \tag{1.4}$$

5. Єдиний вузол цього шару підсумовує вклади всіх правил:

$$y = \sum_{j=1}^{m} y_{\text{j}}. \tag{1.5}$$

Налаштування мережі ANFIS з двома вхідними лінгвістичними змінними x_1, x_2 і чотирма нечіткими правилами виконується комбінацією градієнтного спуску у вигляді алгоритмів зворотного поширення похибки і методу найменших квадратів (МНК).

Алгоритм зворотного поширення похибки налаштовує параметри антецедентів (передумов), тобто. функцій належності фазифікатора. МНК оцінює коефіцієнти укладання правил, оскільки вони лінійно пов'язані з виходом мережі. Кожна ітерація процедури налаштування виконується у два етапи.

У першому етапі на входи подається навчальна вибірка і по нев'язці між бажаною і дійсною поведінкою мережі МНК знаходяться оптимальні параметри вузлів четвертого шару. На другому етапі залишкова нев'язка передається з виходу мережі на входи та методом зворотного поширення похибки модифікуються параметри вузлів першого шару. При цьому знайдені на попередньому етапі коефіцієнти укладання правил не змінюються.

Ітераційна процедура налаштування продовжується, поки нев'язка перевищує заздалегідь встановлене значення. Для налаштування функцій належності фазифікатора, крім методу зворотного поширення похибки, можуть використовуватись інші алгоритми оптимізації.

Далі було розглянуто мережу Anfis із застосуванням алгоритму Такагі-Сугено-Канга, який реалізований нечіткою НМ, де процес навчання розбитий на два етапи та процес обчислень по етапах виконується паралельно і одночасно.

1.3.2 Нейронечітка мережа Anfis із застосуванням алгоритму Такагі-Сугено-Канга

Відмінність алгоритмів Такагі-Сугено-Канга від алгоритму Сугено-Такагі полягає у реалізації нечіткої продукційної моделі, що базується на правилах типу [27]:

$П_i$: ЯКЩО x_1 це A_{i1}, І… І x_j це A_{ij}, ТО

$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j \ , j = 1,... n. \tag{1.6}$$

Ця нечітка адаптивна мережа базується на таких положеннях:

- вхідні змінні є чіткими;
- функції належності всіх перелічених множин визначені функцією Гауса;

$$\mu_{A_{ij}}(x_j) = \exp\left(-0{,}5 \left(\frac{x_j - a_{ij}}{b_{ij}} \right)^2 \right), \tag{1.7}$$

де x_j – входи мережі; a_{ij}, b_{ij} – параметри функції належності, що налаштовуються.

- нечітка імплікація Ларсена – нечіткий добуток;
- Т-норма – нечітке добуток;
- композиція не здійснюється;
- метод дефазифікації – метод центроїду.

Виходячи з цих положень функціональна залежність для отримання вихідної змінної величини після дефазифікації набуде вигляду:

$$y' = \frac{\sum_{i}^{n}\left(\left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j\right)\prod_{j}^{m} \mu_{A_{ij}}\left(x'_j\right)\right)}{\sum_{i=1}^{n}\prod_{j}^{m}\mu_{A_{ij}}\left(x'_j\right)} =$$

$$= \frac{\sum_{i}^{n}\left(\left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j\right)\right)\prod_{j=1}^{m} \exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}}\right)^2\right]}{\sum_{i=1}^{n}\prod_{j}^{m}\exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}}\right)^2\right]}. \quad (1.8)$$

На рис. 1.5 представлена мережа Anfis із застосуванням алгоритму Такагі-Сугено-Канга.

Наведений аналітичний вираз (1.8) лежить в основі мережі Anfis із застосуванням алгоритму Такагі-Сугено-Канга, яка включає п'ять шарів.

Шар 1 складається з елементів, які виконують фазифікацію вхідних чітких змінних x'_j (j=1,…,n). Елементи цього шару обчислюють значення ступенів належності функцій належності $\mu_{A_{ij}}\left[x'_j\right]$, заданих гаусівськими функціями з параметрами a_{ij} і b_{ij}.

Шар 2, число елементів якого дорівнює кількості правил в базі, виконує нечітку імплікацію ступенів належності відповідних правил.

Шар 3 генерує значення функцій $\left(c_{j0} + \sum_{j=1}^{m} c_{ij} x'_j\right)$, які множаться на результати обчислень елементами попереднього шару.

У шарі 4 перший елемент (суматор) служить для активізації висновків правил відповідно до значень агрегованих у попередньому шарі ступенів належності передумов правил. Другий елемент (суматор) проводить допоміжні обчислення для подальшої дефазифікації результату.

Шар 5 складається з одного нормалізуючого елемента та виконує дефазифікацію результату.

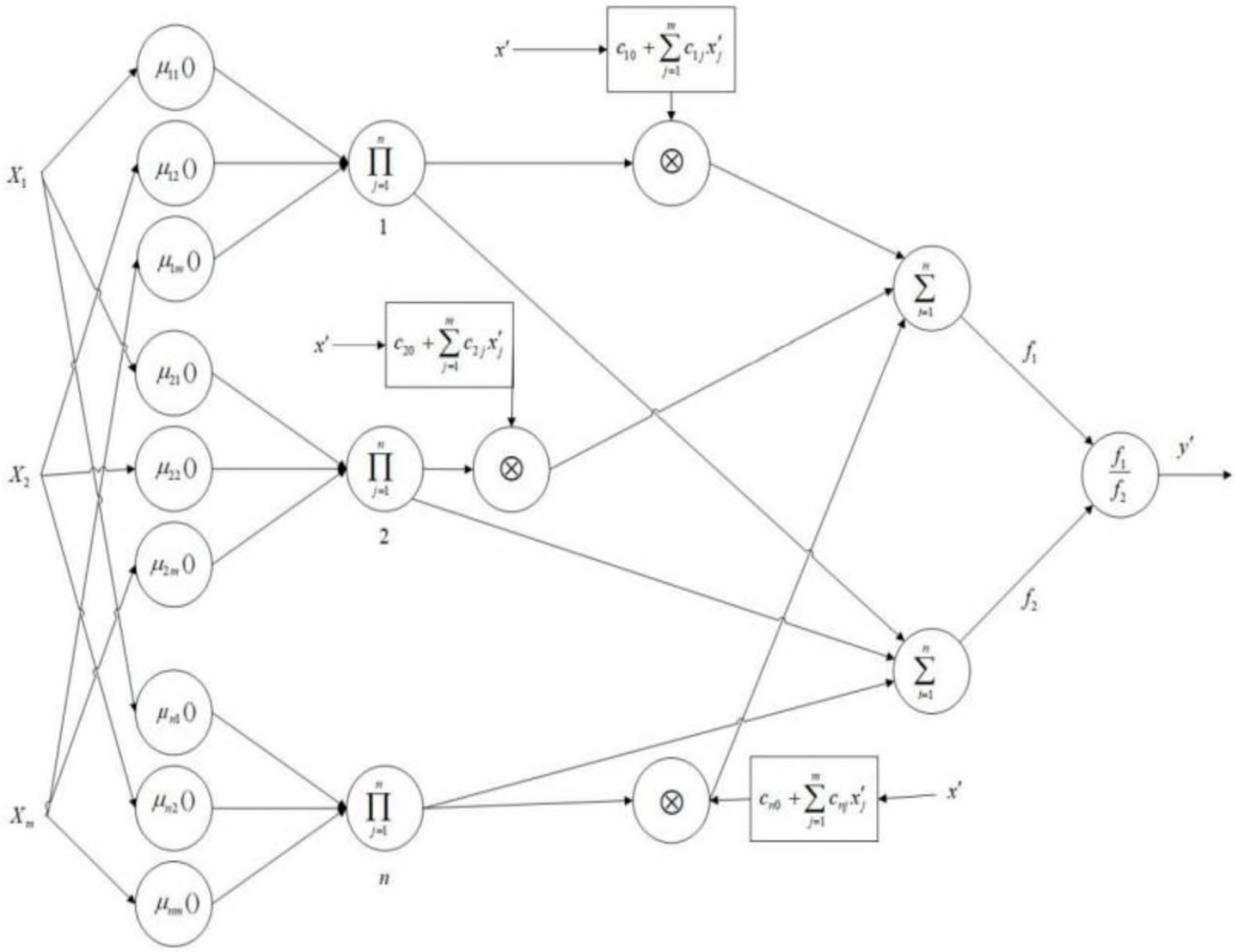

Рисунок 1.5 – Нейронечітка мережа Anfis з використанням висновку Такагі-Сугено-Канга

З наведеного опису випливає, що мережа Такагі-Сугено-Канга містить два параметричних шарів (шар 1 і 3). Параметрами, що налаштовуються в процесі навчання, є:

- у шарі 1 – нелінійні параметри a_{ij} і b_{ij} гаусівських функцій належності фазифікатора;
- у шарі 3 – параметри c_{i0} та c_{ij} лінійних функцій $\left(c_{j0}+\sum_{j=1}^{m}c_{ij}x'_j\right)$ із висновків правил.

За наявності n правил і m вхідних змінних число параметрів першого шару дорівнює $2nm$, а другого – $n(m+1)$. Таким чином, сумарна кількість налаштовуваних параметрів дорівнює $n(3m+1)$.

Спочатку розраховуються параметри c_{i0} та c_{ij} лінійних функцій за умови фіксованих значень параметрів a_{ij} та b_{ij}. Параметри c_{i0} та c_{ij} знаходяться шляхом розв'язання системи лінійних рівнянь.

Представимо вихідну змінну з виразу (1.9) у наступному вигляді:

$$y' = \sum_{i=1}^{n} w_i' \left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j \right), \tag{1.9}$$

де

$$w_i' = \frac{\prod_{j=1}^{m} \mu_{A_{ij}}(x_j')}{\sum_{i=1}^{n} \prod_{j}^{mj} \mu_{A_{ij}}(x_j')} = \frac{\prod_{j}^{m} \exp\left[-\left(\frac{x_j' - a_{ij}}{b_{ij}} \right)^2 \right]}{\sum_{i=1}^{n} \prod_{j}^{m} \exp\left[-\left(\frac{x_j' - a_{ij}}{b_{ij}} \right)^2 \right]} = \text{const} \tag{1.10}$$

Алгоритм навчання мережі Anfis із застосуванням алгоритму Такагі-Сугено-Канга здійснюється наступним чином.

При K навчальних прикладах $\left(x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}, y^{(k)}\right)$, та заміні значень вихідних змінних $y'^{(k)}$ значеннями еталонних змінних $y^{(k)}$, отримаємо систему з K лінійних рівнянь виду:

$$\begin{bmatrix} w_1'^{(1)} & w_1'^{(1)}x_1^{(1)} & \ldots & w_1'^{(1)}x_m^{(1)} & \ldots & w_n'^{(1)} & w_n'^{(1)}x_1^{(1)} & \ldots & w_n'^{(1)}x_m^{(1)} \\ w_1'^{(2)} & w_1'^{(2)}x_1^{(2)} & \ldots & w_1'^{(2)}x_m^{(2)} & \ldots & w_n'^{(2)} & w_n'^{(2)}x_1^{(2)} & \ldots & w_n'^{(2)}x_m^{(2)} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ w_1'^{(k)} & w_1'^{(k)}x_1^{(k)} & \ldots & w_1'^{(k)}x_m^{(k)} & \ldots & w_n'^{(k)} & w_n'^{(k)}x_1^{(k)} & \ldots & w_n'^{(k)}x_m^{(k)} \end{bmatrix}' \times \begin{bmatrix} c_{10} \\ \ldots \\ c_{1m} \\ \ldots \\ c_{n0} \\ \ldots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \ldots \\ y^{(k)} \end{bmatrix}, \tag{1.11}$$

де $w_i'^{(k)}$ – агрегована ступінь істинності передумов за i-м правилом при пред'явленні k-го вхідного вектора $\left(x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}\right)$.

Запишемо (2-13) у скороченому матричному вигляді

$$\boldsymbol{W}\times \mathbf{c} = \boldsymbol{y}. \tag{1.12}$$

Розмірність матриці **W** дорівнює $K\times(m+1)n$, при цьому зазвичай кількість рядків K значно більша за кількість стовпців: $K\times(m+1)n$. Вирішення цієї системи рівнянь можна провести за один крок за допомогою псевдоінверсії матриці **W**:

$$c = W^{+} y = \left(W^{\mathrm{T}} \cdot W\right)^{-1} W^{\mathrm{T}} y. \tag{1.13}$$

Потім після визначення лінійних параметрів c_{ij} їх фіксують та розраховують фактичні вихідні сигнали мережі для всіх прикладів, для чого використовується лінійна залежність

$$y' = \begin{bmatrix} y'^{(1)} \\ y'^{(2)} \\ \dots \\ y'^{(k)} \end{bmatrix} = W \cdot c\ . \tag{1.14}$$

Визначаємо вектор похибок:

$$e = y' - y\ . \tag{1.15}$$

Після чого, наприклад, за алгоритмом Уідроу-Хоффа уточнюємо параметри:

$$a_{ij}^{(k)}(t+1) = a_{ij}^{(k)}(t) - C\frac{dE^{(\kappa)}(t)}{da_{ij}^{(k)}}; \tag{1.16}$$

$$b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) - C\frac{dE^{(\kappa)}(t)}{db_{ij}^{(k)}}. \tag{1.17}$$

Після уточнення нелінійних параметрів процес адаптації параметрів запускається знову доти, доки настане повторюваність результатів. Цей алгоритм називають гібридним. Його особливість полягає у розподілі етапів процесу навчання. Гібридний алгоритм ефективніший, ніж метод Уідроу-Хоффа, у якого уточнення всіх параметрів проводиться паралельно та одночасно.

У мережі Такагі-Сугено-Канга результатом є поліном $c_{i0} + \sum_{j=1}^{m} c_{ij} x_j$, тоді як у мережі Ванга-Менделя вихідна змінна є константною c_i, яку можна розглядати як поліном нульового порядку. Тому далі було розглянуто нечітку нейронну продукційну мережу Ванга-Менделя як окремий випадок мережі Такагі-Сугено-Канга.

1.3.3 Нейронечітка мережа Anfis із застосуванням алгоритму Ванга-Менделя

Мережа Anfis із застосуванням алгоритму Ванга-Менделя заснована на нечітких правилах [28]:

$П_i$: ЯКЩО x_1 це A_{i1}, І… І x_j це A_{ij}, І… І x_{im} це A_{im}, ТО y=$B_{i/}$, j=1,…,n.

Ця нечітка адаптивна мережа базується на наступних положеннях:

- вхідні змінні є чіткими;
- функції належності всіх перелічених множин визначені функцією Гауса;
- нечітка імплікація Ларсена – нечіткий добуток;
- Т-норма – нечіткий добуток;
- композиція не здійснюється;
- метод дефазифікації – середній центр.

Виходячи з цих передумов нечіткий висновок для даної моделі має такий вигляд:

$$\mu_{B_i'}(y) = \sup_{x \in X} \left\{ \mu_{A_i'}(x) \, \mathrm{T} \, \mu_{A_i \to B_i}(x, y) \right\} = \sup_{x \in X} \left\{ \mu_{A_i'}(x) \cdot \mu_{A_i \to B_i}(x, y) \right\} =$$

$$= \sup_{x \in X} \left\{ \mu_{A_i'}(x) \, \mu_{A_{ij}}(x) \, \mu_{B_i}(y) \right\} = \sup_{x_1 \ldots x_m \in X} \left\{ \mu_{B_i}(y) \prod_{j=1}^{m} \left(\mu_{A_{ij}'}(x_j) \mu_{A_{ij}}(x_j) \right) \right\}. \quad (1.18)$$

Враховуючи, що вхідні змінні $x_j,\ldots,x_m$ є чіткими, то (1.18) набуває наступного вигляду

$$\mu_{B_i'}(y) = \mu_{B_i}[y] \prod_{j=1}^{m} \mu_{Aij}(x_j'). \quad (1.19)$$

Так акумулювання активізованих висновків правил не проводиться, а методом дефазифікації є метод середнього центру, то вихідна змінна визначається:

$$y' = \frac{\sum_{i=1}^{n}(\arg\max_{y} \mu_{B_i'}(y)\ \mu_{B_i'}(y))}{\sum_{i=1}^{n}\mu_{B_i'}(y)} = \frac{\sum_{i=1}^{n}(\arg\max_{y} \mu_{B_i'}(y)\ \mu_{B_i}(y)\prod_{j=1}^{m}\mu_{A_{ij}}(x_j'))}{\sum_{i=1}^{n}(\mu_{B_i'}(y)\prod_{j=1}^{m}\mu_{A_{ij}}(x_j'))}. \quad (1.20)$$

З урахуванням того, що максимальне значення, яке $\mu_{B_i}(y)$ може прийняти в точці $\arg\max_{y} \mu_{B_i'}(y)$ дорівнює одиниці, (1.20) набуде вигляду:

$$y' = \frac{\sum_{i=1}^{n}(\arg\max_{y} \mu_{B_i'}(y)\prod_{j=1}^{m}\mu_{A_{ij}}(x_j'))}{\sum_{i=1}^{n}\prod_{j=1}^{m}\mu_{A_{ij}}(x_j')}. \quad (1.21)$$

У разі функції належності всіх нечітких множин вида функції Гауса, вираз (1.21) набуде вигляду

$$y' = \frac{\sum_{i=1}^{n}(\arg\max_{y}(\exp\left[-\frac{y-c_i}{d_i}\right]))\prod_{j=1}^{m}\exp\left[-\frac{x_j'-a_{ij}}{b_{ij}}\right]}{\sum_{i=1}^{n}\prod_{j=1}^{m}\exp\left[-\frac{x_j'-a_{ij}}{b_{ij}}\right]} \quad (1.22)$$

де c_i, d_i – відповідно, центри та ширина гаусівських функцій, що представляють функції належності нечітких множин B_i висновків правил; a_{ij}, b_{ij} – відповідно центри і ширина гаусівських функцій, що є функціями належності нечітких множин A_{ij} предпосилок правил.

В остаточному вигляді (1.22) перетворюється на:

$$y' = \frac{\sum_{i=1}^{n}c_i\prod_{j=1}^{m}\exp\left[-\frac{x_j'-a_{ij}}{b_{ij}}\right]}{\sum_{i=1}^{n}\prod_{j-1}^{m}\exp\left[-\frac{x_j'-a_{ij}}{b_{ij}}\right]}. \quad (1.23)$$

На рис. 1.6 представлена структура нечіткої продукційної мережі Anfis з алгоритмом Ванга-Менделя, елементи шарів якої реалізують відповідні компоненти виразу (1.23).

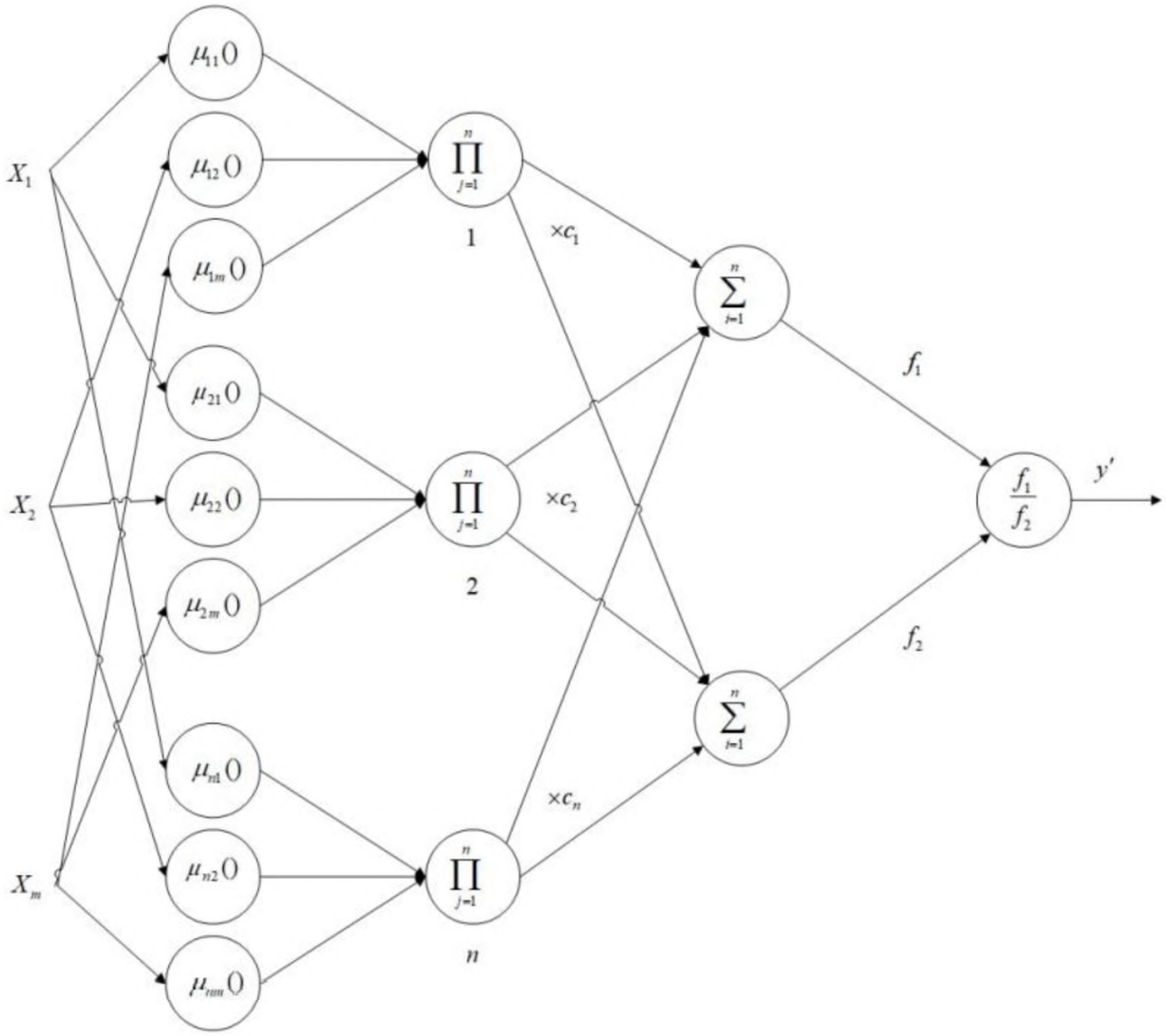

Рисунок 1.6 – Нейронечітка мережа Anfis з використанням висновку Ванга-Менделя

У шарі 2, число елементів якого дорівнює кількості правил в базі, здійснюється агрегування ступенів належності передумов відповідних правил.

У шарі 3 перший елемент служить для активізації висновків правил (c_i) відповідно до значень агрегованих у попередньому шарі ступенів належності

передумов правил. Другий елемент шару проводить допоміжні обчислення для подальшої дефазифікації результату.

Шар 4, що складається з одного елемента, виконує дефазифікацію вихідної змінної.

Алгоритм навчання поділяється на дві процедури. Спочатку налаштовуються лінійні параметри елементів третього шару c_i, а потім – параметри нелінійної функції належності в елементах першого шару a_{ij} та b_{ij}, де $i=1,...,n$; $j=1,...,m$.

Етап 1. Для кожного прикладу з навчальної вибірки $\left(x_1^{(k)},, x_2^{(k)},..., x_m^{(k)}, y^{(k)}\right)$, де $k=1,\ldots,K$ розраховується значення вихідної змінної $y'^{(k)}$.

Етап 2. Обчислюється функція похибки всім прикладів навчальної вибірки:

$$E^{(k)} = 0{,}5\left(y'^{(k)} - y^{(k)}\right)^2,\ k = 1,..., K. \tag{1.24}$$

Етап 3. Коригуються значення c_i для кожного i-го правила по кожному k-му прикладу навчальної вибірки, виходячи із співвідношення

$$c_i(t+1) := c_i(t) - C\frac{dE^{(k)}(t)}{dc_i(t)},\ i = 1,...,\ n,\ \ k = 1,...,\ K; \tag{1.25}$$

Процедура коригування значень c_i (етапи 1-3) ітераційно повторюється і вважається завершеною у разі, якщо:

• або значення функції похибки за кожним прикладом навчальної вибірки не перебільшує деякого встановленого порога:

$$E^{(k)} \prec \varepsilon,\ k = 1,...,\ K; \tag{1.26}$$

• або оцінка середньої сумарної похибки нечіткої продукційної моделі з урахуванням усіх прикладів навчальної вибірки не перевищує деякого встановленого порога:

$$E = \frac{1}{K}\sum_{k=1}^{K}\left(y'^{(k)} - y^{(k)}\right)^2 \prec \varepsilon; \tag{1.27}$$

• або похибка стабілізувалася на певному значенні $\succ \varepsilon$.

При виконанні процедури коригування значень a_{ij} і b_{ij} в елементах першого шару етапи 1 і 2 виконуються аналогічно етапам процедури коригування c_i. На заключному етапі цієї процедури значення a_{ij} і b_{ij} змінюються відповідно до таких виразів

$$a_{ij}(t+1) := a_{ij}(t) - C\frac{dE^{(k)}(t)}{da_i(t)} = a_{ij}(t) - C\frac{2\left(x_j'^{(k)} - a_{ij}\right)\left(y'^{(k)} - y^{[k]}\right)\left(c_i - y'^{(k)}\right)\prod_{j=1}^{m}\exp\left[-\left(\frac{x_j'^{(k)} - a_{ij}}{b_{ij}}\right)^2\right]}{b_{ij}^2\sum_{i=1}^{n}\prod_{j=1}^{m}\exp\left[-\left(\frac{x_j'^{(k)} - a_{ij}}{b_{ij}}\right)^2\right]} \quad (1.28)$$

Умови завершення коригування значень a_{ij} і b_{ij} подібні c_i.

У разі невиконання першої чи другої умови процес ітераційно повторюється, починаючи з коригування c_i до тих пір, поки мережа Anfis не буде коректно навчена.

Мережа Anfis з алгоритмом Ванга-Менделя, відрізняючись простотою обчислювальної точки зору і великою чутливістю до змін вхідних змінних, де реалізовано градієнтний метод оптимізації фронтального типу, водночас не є ефективною з точки зору швидкодії.

1.4 Висновок. Постановка задачі

В розділі проаналізовано принципи функціонування систем виявлення вторгнень, а також класифікаційні ознаки систем виявлення вторгнень і атак та напрями їх побудови. Встановлено, що СВВ є невід'ємною частиною будь-якої сучасної системи безпеки. Особливо необхідні СВВ, які орієнтовані на виявлення аномальних станів. Вони, як правило, формують (містять) профіль нормальної (ненормальної) активності в ІКМ та детектують відхилення від нього.

Наразі питання забезпечення необхідного рівня мережевої безпеки та захисту від кібератак активно вивчаються різними дослідниками у галузі

машинного навчання та аналізу даних. Це пов'язано з тим, що існуючі інтелектуальні алгоритми аналізу дозволяють вирішувати завдання пошуку аномалій та виявлення всіляких взаємозв'язків усередині даних тощо. Однак, у будь-якій з представлених систем формування інтелектуальних рішень, результат, як правило, залежить як від інструментів і алгоритмів навчання, що використовуються, так і від якості даних, на яких будується деяка модель.

Зниження якості даних відбувається як під дією об'єктивної невизначеності, що виявляється в шумах, аномаліях, викидах тощо, так і під дією лінгвістичної невизначеності, що виявляється через суб'єктивність оцінки експертів. Наразі для підвищення якості даних через об'єктивну невизначеність розроблено комплекс методів та алгоритмів обробки та фільтрації, при цьому вплив суб'єктивності експертів є найскладнішим завданням, ефективність у вирішенні якого показали системи нейронечіткого висновку.

В розділі проаналізовано нейронечіткі мережі Anfis з різними алгоритмами нечітких перетворень (Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя). Встановлено, що побудова мережі Anfis – один з методів, покликаних вирішити проблему формування системи нечіткого виведення, яка б не залежила від суб'єктивних оцінок фахівців у тій чи іншій галузі.

Таким чином, для виконання мети кваліфікаційної роботи необхідно:

• провести аналіз існуючих підходів до ідентифікації мережевих атак з використанням систем нечіткого висновку;

• сформулювати задачу ідентифікації мережевих атак з використанням нейронечітких мереж Anfis;

• дослідити алгоритми адаптивних нейронечітких мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Існуючі підходи до ідентифікації мережевих атак з використанням систем нечіткого висновку

Існує досить велика кількість технологій забезпечення безпеки в мережах, у тому числі на нечіткому висновку. Розглянемо основні технології, що використовуються наразі для ідентифікації мережевих атак.

Дослідження бінарної класифікації мережевих атак з використанням методів нечіткої логіки проведено в роботі [29], де описано процес нечіткого висновку Такагі-Суґено на обмеженому наборі ознак мережевого трафіку. Результати розробленого підходу показали високу точність визначення підозрілої активності.

Найбільш складна система виявлення мережевих атак була запропонована в роботі [30] і ґрунтувалася на комплексуванні нейронних та нейронечітких класифікаторів. Запропонований підхід використовувався для обробки даних, отриманих від сенсорів системи управління інформацією та подіями безпеки, та показав високу ефективність виявлення нових типів атак при мінімальній кількості помилкових спрацьовувань.

У зв'язку з високою ефективність, яку продемонстрували методи на основі штучних НМ спільно з алгоритмами нечіткого висновку, у роботі [31] автори представили метод нечіткої кластеризації для генерації різних навчальних підмножин, а для агрегування отриманих результатів запропонували мета-навчальний модуль. Цей підхід дозволив зменшити помилкові спрацьовування та отримати більш стабільні результати при ідентифікації атак.

Вперше ідентифікацію мережевих атак на прикладі різних шаблонів DDoS, розглянули як динамічний процес підбору найбільш ефективного алгоритму класифікації за допомогою нечіткої логіки в роботі [32]. Результати експериментів показали, що побудована система нечіткої логіки ефективно

обирає алгоритм класифікації на основі статусу трафіку і дозволяє вибудовувати певний компроміс між точністю та затримками алгоритмів ідентифікації.

Підвищення точності виявлення мережевих атак за допомогою нечіткої логіки розглянуто в дослідженні [33] і засноване на мережевому моніторингу характеристик, таких як час відгуку, розміри вхідних та вихідних пакетів, пропускну здатність і т.д. У рамках цієї роботи побудований інтегральний показник наявності певного типу загрози, з використанням бази нечітких правил відповідності характеристик типу загроз.

Застосування інструментів нечіткої логіки для виявлення вторгнень у мережі продемонстровано також у статті [34], в якій описано проведення лавинної атаки із синхронізацією за протоколом управління передачею. Запропонований підхід показав порівняні за продуктивністю результати з методом дерев рішень, що є найпоширенішим методом машинного навчання.

Дослідження [35] присвячено виявленню шкідливих вузлів у мобільній adhoc-мережі MANET під час проведення різних типів атак. Пропонована система нечіткого висновку дозволяє також запобігати подібним атакам за допомогою ефективного методу блокування вузлів та забезпечувати необхідний рівень безпеки.

Модифіковану гібридну систему виявлення мережевих атак у бездротових сенсорних мережах на основі нечіткої логіки представили автори у роботі [36]. Результати експериментів показали, що збудована система виявлення вторгнень має високу точність та низьку частоту помилкових спрацьовувань, а також підтверджує ефективність застосування даної системи по аналізу пропускної спроможності та кількості втрачених пакетів.

Таким чином, огляд існуючих методів, алгоритмів і систем нечіткого висновку для аналізу мережевого трафіку в умовах невизначеності показав, що сучасні системи не дозволяють враховувати всі актуальні типи атак, а також залишають місце для модифікації та покращення точності результатів

ідентифікації, оскільки залежать від експертної оцінки та алгоритмів оптимізації.

2.2 Постановка задачі ідентифікації мережевих атак з використанням нейронечітких мереж Anfis

Проведені дослідження в галузі нейронечіткої класифікації [37-42] показали, що застосування різних систем нечіткого висновку для ідентифікації мережевих атак різного типу підтверджує ефективність розгляду всіх розглянутих у розділі 1.3 типів нейронечітких мереж Anfis та більш докладного вивчення їх переваг та недоліків при класифікації інцидентів кібербезпеки на реальному мережевому трафіку.

Розглянемо завдання побудови системи нейронечіткої класифікації мережевих атак з погляду прогнозного моделювання, вирішення якої можна отримати методами машинного навчання із вчителем. У зв'язку з тим, що множина ідентифікованих атак обмежена тільки з практичної точки зору і представлена найбільш поширеними типами атак, це завдання є багатокласовою класифікацією. Слід зазначити, що нейронечітка система дозволяє перетворювати на терм-множини як безперервні, так і категоріальні дані, що значно розширює множину можливих для використання змінних характеристик.

Опишемо формальну математичну постановку задачі класифікації мережевих атак. Припустимо, що інформація про події в мережі фіксується з деяким досить малим інтервалом часу. При цьому, крім даних про сам пристрій та його технічні характеристики, також фіксується інформація про дії вчинених кінцевими користувачами через пристрої, що розглядаються.

Нехай множина X містить інформацію про стани всіх об'єктів мережі $x_i \in X, i = 1,..,m$, із якими зіставляються деякі записи журналу подій, тобто $x_i = \{x_{i1}, x_{i2}, ..., x_{ik}\}$. Задача багатокласової класифікації мережевих атак

складається у тому, щоб об'єктам мережі зіставити множину типів атак $Y = \{1,...,K\}$.

Таким чином, завдання ідентифікації мережевих атак полягає у тому, що необхідно побудувати відображення

$$f_c(X): X \to Y, \tag{2.1}$$

яке дозволяє описати залежність між фіксованими характеристиками мережевого трафіку та порівняти поведінку об'єктів мережі з характеристиками та вибрати найбільш ймовірну при відсутності атак і при конкретному типі атаки.

2.3 Дослідження алгоритмів нейронечітких мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак

В рамках даної кваліфікаційної роботи було проведено аналіз класифікації мережевих атак на наборі даних UNSW-NB151 [43], який містить відомості про трафік з п'ятьма різними типами мережевих атак і множина Y (2.1) має вигляд {Normal, Fuzzers, Generic, Reconnaissance, Exploits, DoS}. Слід зазначити, що представлені дані про мережевий трафік зібрані більш ніж за 40 характеристиками і мають понад 2,5 млн. записів. Крім того, даними зіставлені збалансовані набори для навчання та для тестування при аналізі точності отриманих моделей класифікації.

Отже, у основі UNSW-NB151 кожен запис містить 47 ознак мережевого трафіку п'яти типів: номінальні, цілі, числові, часові, бінарні. Для кожного запису міститься інформація про те, до якого з десяти класів відноситься з'єднання: нормальні з'єднання (Normal) або один із дев'яти різних видів атак.

У табл. 2.1 перераховані види з'єднань, що зберігаються в зазначеній базі, кількість представлених записів про них, а також короткий опис.

Як видно з табл. 2.1, вибірка стандартів в основі UNSW-NB151 нерівномірна за видами з'єднань: для типу атаки Worms представлено досить

невелику кількість прикладів для навчання. Для подальшого моделювання було взято перші 6 видів з’єднань.

Таблиця 2.1 – Види атак, що представлені в базі UNSW-NB151

Вид з'єднання	**Кількість**	**Опис**
Normal	2218761	Нормальні транзакції даних
Exploits	44525	Зловмисник знає про проблеми безпеки в системі та використовує дані вразливості у своїх цілях
Fuzzers	24246	Спроба викликати зупинення програми або мережі шляхом подання на її вхід великого обсягу випадково згенерованих даних
Reconnaissance	13987	Містить всі типи атак, які збирають інформацію про мережу (з метою розвідки)
Generic	215481	Техніка працює проти всіх блокових шифрів (із заданим блоком та розміром ключа), незалежно від структури блокового шифру
DoS	16353	Шкідлива спроба зробити сервер або мережевий ресурс недоступним для користувачів, зазвичай це тимчасове переривання або припинення послуг хоста, підключеного до Інтернету
Analysis	2677	Містить різні атаки шляхом сканування портів, відправки спаму та проникнення html-файлів
Backdoors	2329	Техніка, в якій механізм безпеки системи обходиться непомітно для доступу до комп'ютера або його даних
Shellcode	1511	Невеликий фрагмент коду, що використовується як корисне навантаження під час експлуатації

Вид з'єднання	Кількість	Опис
		вразливостей програмного забезпечення
Worms	174	Атакуючий реплікує себе, щоб поширитися на інші комп'ютери. Часто він використовує комп'ютерну мережу для поширення, покладаючись на збої безпеки на цільовому комп'ютері для доступу до нього

Для проведення моделювання з ідентифікації атакуючих впливів представлені алгоритми нейронечіткої класифікації Anfis були реалізовані у вигляді самостійних модулів мовою Python.

Результати класифікації представлені у вигляді матриць похибок для алгоритму нечіткого висновку Сугено-Такагі (рис. 2.1), алгоритму Такагі-Сугено-Канга (рис. 2.2) та алгоритму Ванга-Менделя (рис. 2.3).

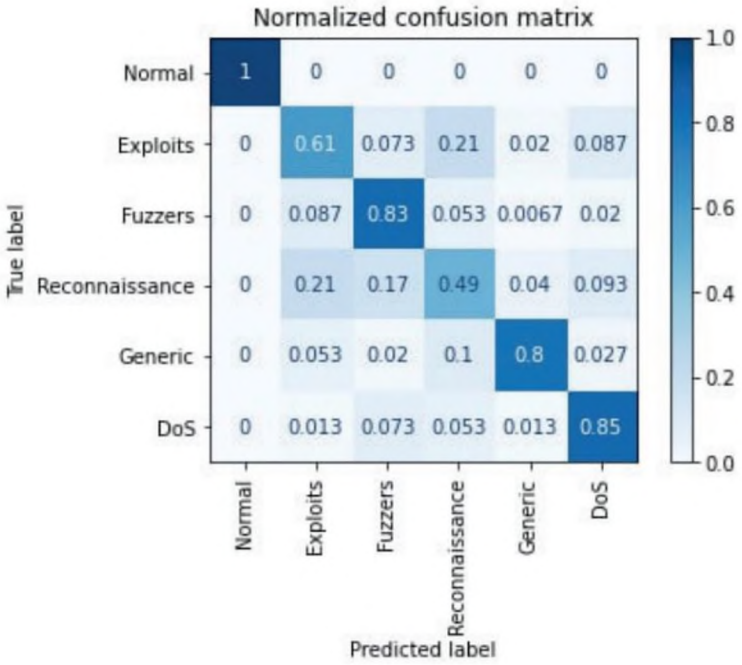

Рисунок 2.1 – Матриця помилок Anfis із використанням алгоритму Сугено-Такагі

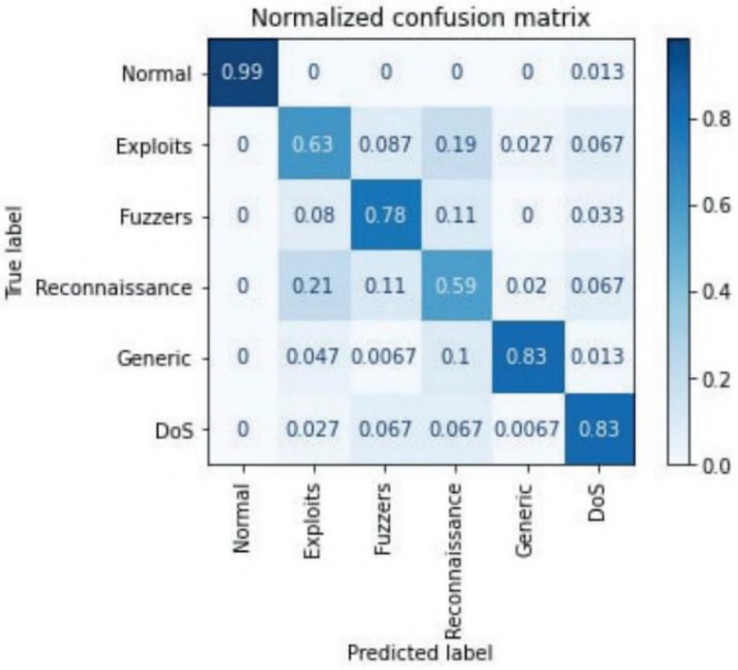

Рисунок 2.2 – Матриця помилок Anfis із використанням алгоритму Такагі-Сугено-Канга

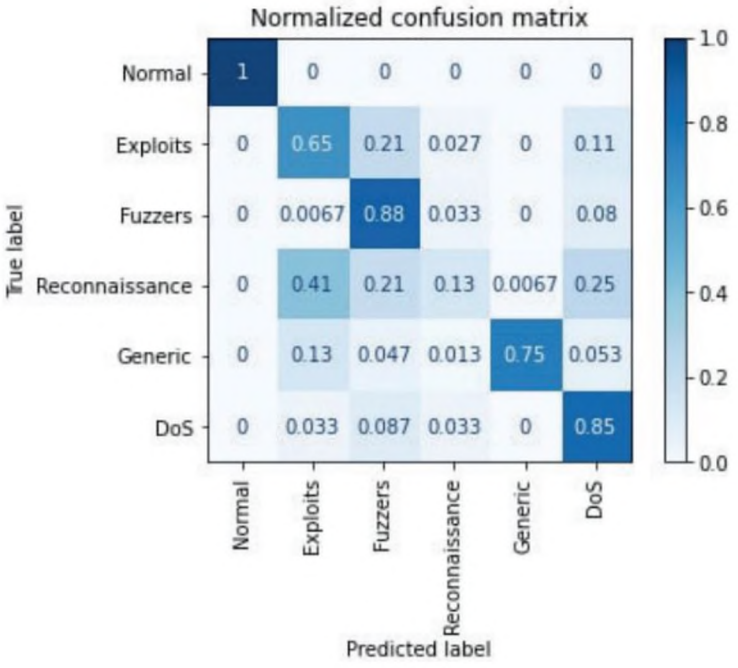

Рисунок 2.3 – Матриця помилок Anfis із використанням алгоритму Ванга-Менделя

Отримані результати також представлені загальною оцінкою ефективності ідентифікації мережевих атак за допомогою мір точності, повноти, F-мір та кількістю істинно позитивних результатів класифікації (рис. 2.4), згідно з якою найбільш оптимальним нейронечітким класифікатором з точки зору різних заходів точності є мережа Anfis з використанням нечіткого висновку Такагі-Сугено-Канга (TSK). При цьому найменш ефективні результати ідентифікації різних типів мережевих атак показала нейронечітка мережа Anfis з використанням нечіткого висновку Ванга-Менделя (VM).

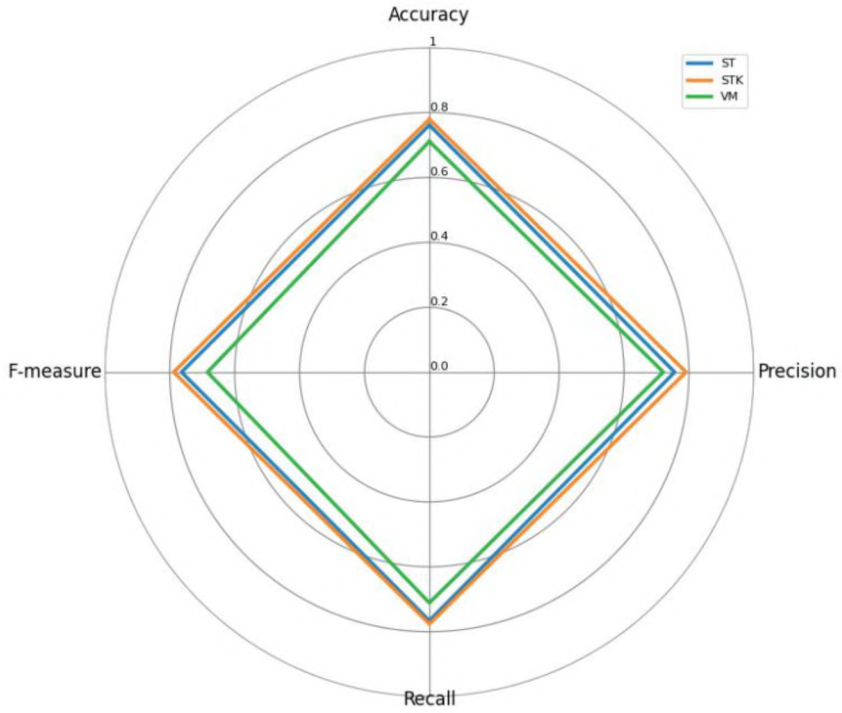

Рисунок 2.4 – Оцінка точності результатів класифікації атак різними алгоритмами

Для того, щоб оцінити ефективність застосування досліджуваних нейронечітких алгоритмів для ідентифікації мережевих атак не тільки з точки зору точності одержуваних результатів навчених моделей, було проведено оцінку продуктивності запропонованого рішення відносно часу, що витрачається на ідентифікацію в мережевому трафіку кожного з розглянутих типів атак (рис. 2.5).

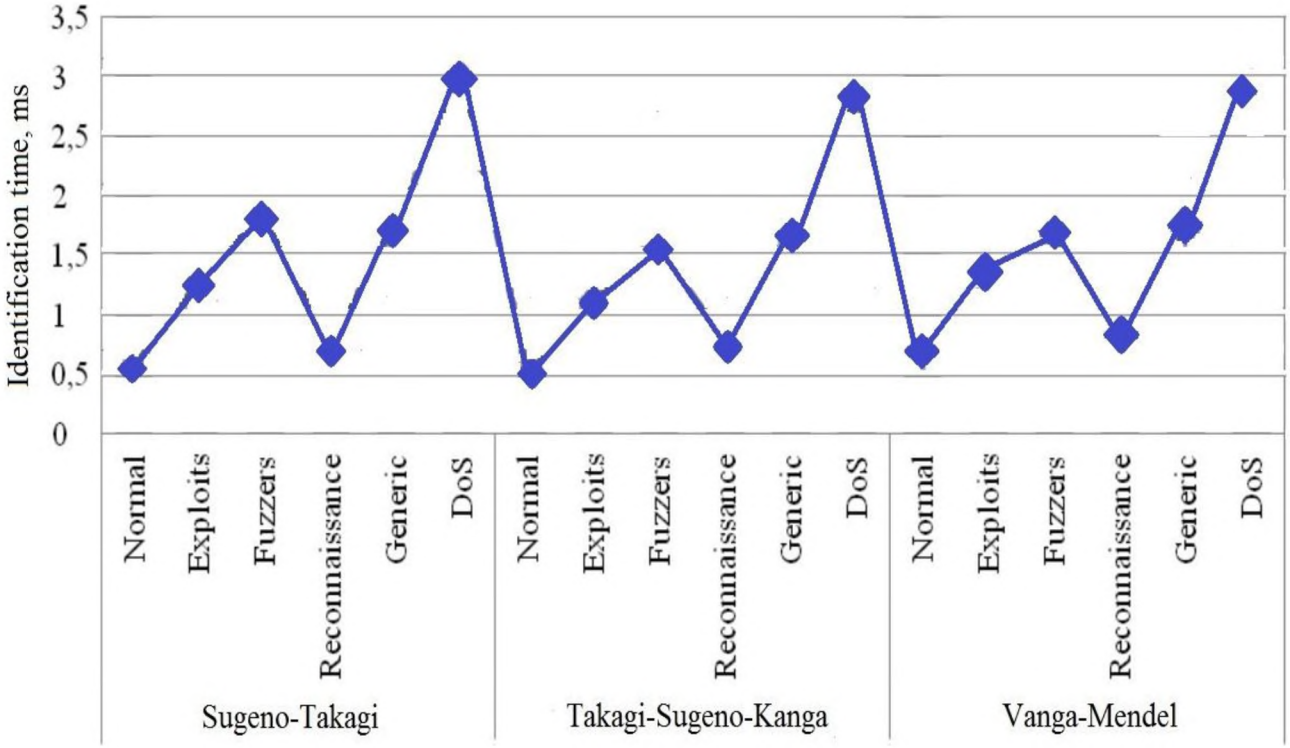

Рисунок 2.5 – Продуктивність алгоритмів нейронечіткої класифікації мережевих атак

Для кожного алгоритму нечіткого виведення на рис. 2.6 також представлено значення отриманої точності моделі класифікації.

Проведене моделювання, спрямоване на аналіз продуктивності та точності алгоритмів нейронечіткої класифікації мережевого трафіку, показало, що на кожному з представлених типів атак всі методи ідентифікації вимагали незначних обчислювальних ресурсів і показували у середньому порівняні за точністю результати. Проте, підхід заснований на нечіткому висновку Такагі-Сугено-Канга здебільшого показав кращу точність.

Таким чином, у рамках даної кваліфікаційної роботи було проведено дослідження алгоритмів адаптивних нейронечітких мереж Anfis на основі різних уявлень нечітких правил, що дозволяють виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки. Результати аналізу швидкостей атак та точності алгоритмів нейронечіткої

класифікації показали, що на кожному з представлених типів атак усі методи ідентифікації вимагали незначних обчислювальних ресурсів.

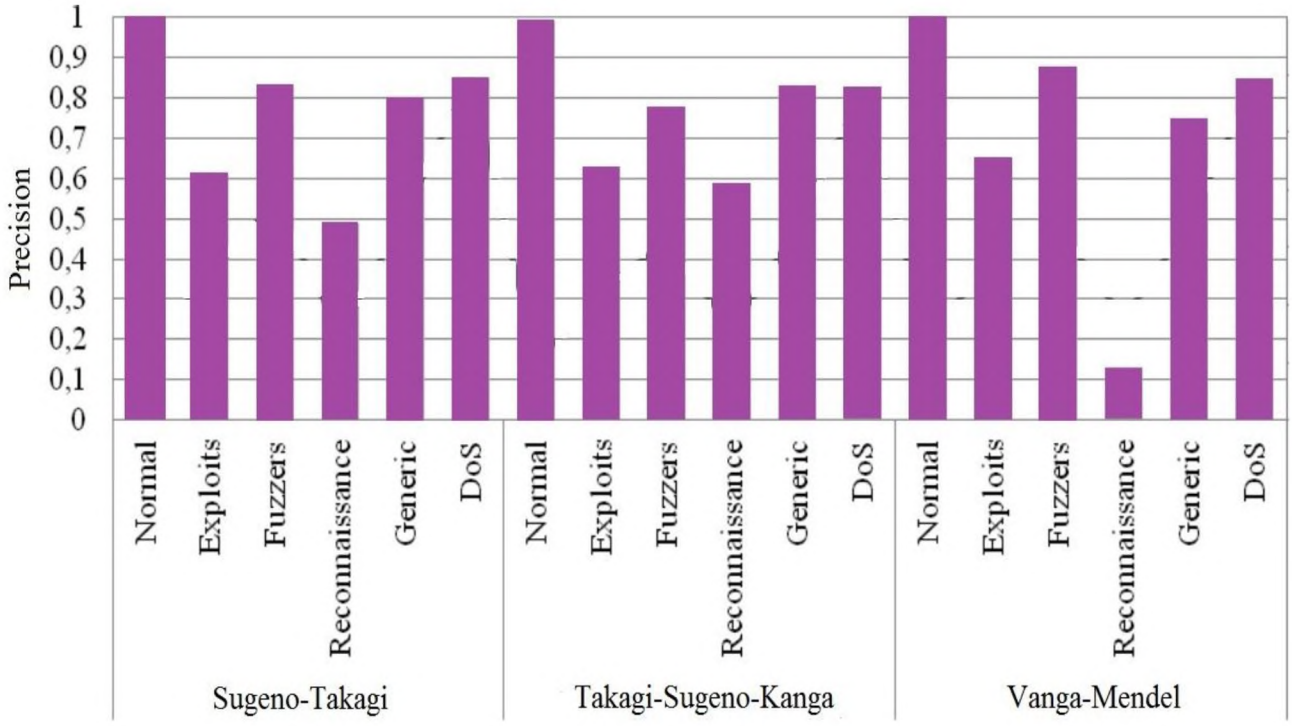

Рисунок 2.6 – Точність алгоритмів нейронечіткої класифікації мережевих атак

Отримані результати загальної оцінки ефективності ідентифікації мережевих атак за допомогою різних заходів точності показали, що найбільш оптимальним нейронечітким класифікатором є мережа Anfis із використанням нечіткого висновку Такагі-Сугено-Канга. При цьому найменш ефективні результати ідентифікації різних типів мережевих атак показало застосування нечіткого висновку Ванга-Менделя. Розроблене програмне забезпечення може бути використане для обробки даних, отриманих з датчиків системи управління інформацією та подіями безпеки.

2.4 Висновки

Огляд існуючих методів, алгоритмів і систем нечіткого висновку для аналізу мережевого трафіку в умовах невизначеності показав, що сучасні

системи не дозволяють враховувати всі актуальні типи атак, а також залишають місце для модифікації та покращення точності результатів ідентифікації, оскільки залежать від експертної оцінки та алгоритмів оптимізації.

Проведені дослідження в галузі нейронечіткої класифікації показали, що застосування різних систем нечіткого висновку для ідентифікації мережевих атак різного типу підтверджує ефективність розгляду всіх типів нейронечітких мереж Anfis (Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя) та більш докладного вивчення їх переваг та недоліків при класифікації інцидентів кібербезпеки на реальному мережевому трафіку.

Було сформульовано задачу ідентифікації мережевих атак з використанням нейронечітких мереж Anfis.

Для проведення моделювання з ідентифікації атакуючих впливів алгоритми нейронечіткої класифікації Anfis були реалізовані у вигляді самостійних модулів мовою Python.

Було проведено дослідження алгоритмів адаптивних нейронечітких мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак. Результати аналізу швидкостей атак та точності алгоритмів нейронечіткої класифікації показали, що на кожному з представлених типів атак усі методи ідентифікації вимагали незначних обчислювальних ресурсів. Отримані результати загальної оцінки ефективності ідентифікації мережевих атак за допомогою різних заходів точності показали, що найбільш оптимальним нейронечітким класифікатором є мережа Anfis із використанням нечіткого висновку Такагі-Сугено-Канга. При цьому найменш ефективні результати ідентифікації різних типів мережевих атак показало застосування нечіткого висновку Ванга-Менделя.

Розроблене програмне забезпечення може бути використане для обробки даних, отриманих з датчиків системи управління інформацією та подіями безпеки.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Запропоновано підхід до ідентифікації мережевих атак з використанням нейронечітких мереж Anfis, який може бути використаний як один із методів нечіткого висновку для аналізу мережевого трафіку в умовах невизначеності.

Метою даного розділу є обґрунтування економічної доцільності ідентифікації мережевих атак з використанням гібридних нейронечітких мереж. Досягнення цієї мети потребує виконання таких розрахунків, як: капітальні витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування; річний економічний ефект від впровадження запропонованих заходів; показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальними витрати називаються тому, що робляться, як правило, один раз, на початкових етапах створення ІС. До капітальних слід відносити наступні витрати: вартість розробки і впровадження проекту; залучення зовнішніх консультантів; первинні закупівлі основного ПЗ; первинні закупівлі додаткового ПЗ; первинні закупівлі апаратного забезпечення тощо.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу щодо ідентифікації мережевих атак з використанням гібридних нейронечітких мереж

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо ідентифікації мережевих атак з використанням гібридних нейронечітких мереж, $t_{тз}$=25;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в$=50;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=40;

$t_р$ – тривалість розробки підходу, $t_м$=90;

$t_д$ – тривалість підготовки технічної документації, $t_д$=18.

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 25+50+40+90+18 = 223 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо ідентифікації мережевих атак з використанням гібридних нейронечітких мереж.

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = З_{зп} + З_{мч} = 51736 + 2334{,}8 = 54070{,}8 \text{ грн.}$$

$$З_{зп} = t^* З_{іб} = 223*232 = 51736 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t^* С_{мч} = 223*10{,}47 = 2334{,}8 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}9 \cdot 5 \cdot 1{,}68 + \frac{590 \cdot 0{,}3}{1920} + \frac{640 \cdot 0{,}6}{1920} = 10{,}47 \text{ грн.}$$

В роботі запропоновано підхід до ідентифікації мережевих атак з використанням нейронечітких мереж Anfis, що дозволить виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки та проведена розробка програмного забезпечення на основі цього підходу.

Витрати на впровадження розробку програмного забезпечення для ідентифікації мережевих атак з використанням нейронечітких мереж Anfis здійснюється, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки програмного забезпечення для ідентифікації мережевих атак з використанням нейронечітких мереж Anfis.

Трудомісткість розробки програмного забезпечення для ідентифікації мережевих атак з використанням нейронечітких мереж Anfis визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку програмного забезпечення, $t_{тз}=15$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=25$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=25$;

$t_р$ – тривалість формування правил аналізу мереживого трафіку, $t_м=20$;

$t_с$ – тривалість отримання інформації про стани всіх об'єктів мережі та записів журналу подій, перетворення їх на терм-множин $t_м=15$;

$t_к$ – тривалість ідентифікайії мережевих атак із використанням нейронечітких мереж Anfis, $t_м=15$;

$t_д$ – тривалість підготовки технічної документації, $t_д=14$.

Отже,

$$t = t_{тз}+ t_в+ t_а+ t_р+ t_с + t_к + t_д =15+ 25+25+20+15+15+14= 129 \text{ години.}$$

Розрахунок витрат на розробку програмного забезпечення для ідентифікації мережевих атак з використанням нейронечітких мереж Anfis

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = З_{зп} + З_{мч} = 27735 + 1359{,}63 = 29094{,}63 \text{ грн.}$$

$$З_{зп} = t * З_{іб} = 129 * 215 = 27735 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t * С_{мч} = 129 * 10{,}47 = 1359{,}63 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}9 \cdot 5 \cdot 1{,}68 + \frac{590 \cdot 0{,}3}{1920} + \frac{640 \cdot 0{,}6}{1920} = 10{,}47 \text{ грн.}$$

Додаткові витрати виникають у разі залучення зовнішніх консультантів і складають 6000 грн,

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$$= 6000 + 54070{,}8 + 29094{,}63 = 89165{,}43 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки.

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 8000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$$С_{з} = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 17000 грн. Додаткова заробітна плата – 5% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,1 ставки. Отже,

$$С_з = (17000*12 + 17000*12*0,05)*0,1= 21420 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 21420*0,22 = 4712,4 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,9 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,9*5*1920*1,68 = 14512,2 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 89165,43*0,01=891,7 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 8000+21420 +4712,4 +14512,2+891,7 = 49536,3 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів. За статистичними даними активність користувачів складає 16%. Тому:

$$С_{ак} = 89165,43*0,16=14266,47 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 49536,3 + 14266,47 = 63802,77 \text{грн.}$$

3.2 Оцінка можливого збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Оцінка можливого збитку від атаки на вузол або сегмент мережі

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 3 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 1 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 2 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 21000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 18000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 5 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 460 тис. грн. на рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 0 грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 60.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с}{F} t_п = \frac{18000*5}{176} * 3 = 1534{,}09 \text{ грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} t_{ви} = \frac{18000*5}{176} * 2 = 1022{,}73 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} t_в = \frac{21000*1}{176} * 1 = 119{,}32 \text{ грн.}$$

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 1022{,}73+119{,}32 = 1142{,}02 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{F_Г} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{46000_0}{208_0} \cdot (3 + 1 + 2) = 1326,9_2 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

U = 1534,09+1142,02 +1326,92 = 4003,03 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_{1} \sum_{60} 4003,03 = 240181,8 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = В \cdot R - C \text{ грн.},$$

де В – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації загрози (42%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

E = 240181,8*0,42– 62842,3= 38034,06 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

ROSI = 38034,06/89165,43 = 0,43 частки одиниці,

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (9%);

$N_{інф}$ – річний рівень інфляції, (8%).

Розрахункове значення коефіцієнта повернення інвестицій:

0,43 > (9 – 8)/100 = 0,43 > 0,01.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

T_o= K/E = 1/ROSI = 1/0,43 = 2,3 роки.

3.4 Висновок

Таким чином, запропонований підхід щодо ідентифікації мережевих атак з використанням гібридних нейронечітких мереж може вважатися економічно доцільним, оскільки отримане значення коефіцієнту повернення інвестицій перевищує рівень дохідності від альтернативного вкладення коштів (ROSI=0,43). Капітальні витрати складатимуть 89165,43 грн. Період окупності складатиме 2,3 роки.

ВИСНОВКИ

1. В результаті аналізу принципів функціонування систем виявлення вторгнень, а також класифікаційних ознак систем виявлення вторгнень і атак та напрямів їх побудови встановлено, що СВВ є невід'ємною частиною будь-якої сучасної системи безпеки. Особливо необхідні СВВ, які орієнтовані на виявлення аномальних станів. Вони, як правило, формують (містять) профіль нормальної (ненормальної) активності в ІКМ та детектують відхилення від нього.

Наразі питання забезпечення необхідного рівня мережевої безпеки та захисту від кібератак активно вивчаються різними дослідниками у галузі машинного навчання та аналізу даних. Це пов'язано з тим, що існуючі інтелектуальні алгоритми аналізу дозволяють вирішувати завдання пошуку аномалій та виявлення всіляких взаємозв'язків усередині даних тощо. Однак, у будь-якій з представлених систем формування інтелектуальних рішень, результат, як правило, залежить як від інструментів і алгоритмів навчання, що використовуються, так і від якості даних, на яких будується деяка модель.

Зниження якості даних відбувається як під дією об'єктивної невизначеності, що виявляється в шумах, аномаліях, викидах тощо, так і під дією лінгвістичної невизначеності, що виявляється через суб'єктивність оцінки експертів. Наразі для підвищення якості даних через об'єктивну невизначеність розроблено комплекс методів та алгоритмів обробки та фільтрації, при цьому вплив суб'єктивності експертів є найскладнішим завданням, ефективність у вирішенні якого показали системи нейронечіткого висновку.

2. В результаті аналізу нейронечітких мереж Anfis з різними алгоритмами нечітких перетворень (Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя) встановлено, що побудова мережі Anfis – один з методів, покликаних вирішити проблему формування системи нечіткого виведення, яка б не залежила від суб'єктивних оцінок фахівців у тій чи іншій галузі.

3. В результаті аналізу існуючих підходів до ідентифікації мережевих атак з використанням систем нечіткого висновку в умовах невизначеності встановлено, що сучасні системи не дозволяють враховувати всі актуальні типи атак, а також залишають місце для модифікації та покращення точності результатів ідентифікації, оскільки залежать від експертної оцінки та алгоритмів оптимізації.

Встановлено, що застосування різних систем нечіткого висновку для ідентифікації мережевих атак різного типу підтверджує ефективність розгляду всіх типів нейронечітких мереж Anfis (Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя) та більш докладного вивчення їх переваг та недоліків при класифікації інцидентів кібербезпеки на реальному мережевому трафіку.

4. Сформульовано задачу ідентифікації мережевих атак з використанням гібридних нейронечітких мереж Anfis.

5. Проведено дослідження алгоритмів адаптивних нейронечітких мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак. Результати аналізу швидкостей атак та точності алгоритмів нейронечіткої класифікації показали, що на кожному з представлених типів атак усі методи ідентифікації вимагали незначних обчислювальних ресурсів. Отримані результати загальної оцінки ефективності ідентифікації мережевих атак за допомогою різних заходів точності показали, що найбільш оптимальним нейронечітким класифікатором є мережа Anfis із використанням нечіткого висновку Такагі-Сугено-Канга. При цьому найменш ефективні результати ідентифікації різних типів мережевих атак показало застосування нечіткого висновку Ванга-Менделя.

ПЕРЕЛІК ПОСИЛАНЬ

1. Лукова-Чуйко Н., Наконечний В., Толюпа С., Зюбіна Р. Проблеми захисту критично важливих об'єктів інфраструктури // Безпека інформаційних систем і технологій. – 2020. – № 1(2). – С. 31-39.

2. Браницкий А.А. Анализ и классификация методов обнаружения сетевых атак / А.А. Браницкий, И.В. Котенко // Труды СПИИРАН. – 2016. – Вып. 2(45). – С. 207-244.

3. Носенко К.М. Огляд систем виявлення атак в мережевому трафіку / К.М. Носенко, О.І. Півторак, Т.А. Ліхоузова // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління». – 2014. – № 1(24). – С. 67-75.

4. Довбешко С.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак / С.В. Довбешко, С.В. Толюпа, Я.В. Шестак // Сучасний захист інформації. – 2019. – №1(37). – С. 6-15.

5. Лазаренко С.В. Особливості функціонування систем виявлення атак на автоматизовані системи / С.В. Лазаренко // Сучасний захист інформації. – 2015. – №1. – С. 33-40.

6. Смирнов А. Имитационная модель NIPDS для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А. Смирнов, Ю. Дрейс, Д. Даниленко // Ukrainian Scientific Journal of Information Security. – 2014. – Vol. 20, issue 1. – P. 29-35.

7. Гулак Г.М. Модель системи виявлення вторгнень з використанням двоступеневого критерію виявлення мережевих аномалій / Г.М. Гулак, В.В. Семко, П.М. Складанний // Сучасний захист інформації. – 2015. – №4. – С. 81-85.

8. Разработка модели интеллектуального распознавания аномалий и кибератак с использованием логических процедур, базирующихся на покрытиях матриц признаков / Г. Бекетова, Б. Ахметов, А. Корченко, В. Лахно

// Ukrainian Scientific Journal of Information Security. – 2016. – Vol. 22, issue 3. – P. 242-254.

9. Петров О. Метод та модель інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту / О. Петров, О. Корченко, В. Лахно // Ukrainian Scientific Journal of Information Security, 2015. – Vol. 21, issue 1. – P. 26-34.

10. Карачанская Е.В. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре / Е.В. Карачанская, Н.И. Соседова // Безопасность информационных технологий. – 2019. – С. 98-110.

11. Корченко А. Модели систем выявления аномалий, порожденных кибератаками. Эвристические алгоритмы и распределенные вычисления в прикладных задачах: Коллективная монография. / А. Корченко. – Выпуск 2. – Под ред. Б.Ф. Мельникова. – Ульяновск. – 2013. – С. 56-86.

12. Казмірчук С. Аналіз систем виявлення вторгнень / С. Казмірчук, А. Корченко, Т. Паращук // Захист інформації. – 2018. – Т.20. – №4. – С. 259-276.

13. Jin S. Intrusion Detection System Enhanced by Hierarchical Bidirectional Fuzzy Rule Interpolation / S. Jin, Y. Jiang, J. Peng. // 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC). – Miyazaki, Japan, 2018. – Pp. 6-10. – DOI 10.1109/SMC.2018.00010.

14. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с. – ISBN 978-966-350-735-4.

15. Субач І.Ю. Модель виявлення аномалій в інформаційно-телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу / І.Ю. Субач, В.В. Фесьоха // Збірник наукових праць ВІТІ. – 2017. – № 3.

16. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский // пер. с польск. И.Д. Рудинского. – М.: Горячая линия-Телеком, 2006. – 452 с.

17. Штовба С.Д. Проектирование нечетких систем средствами Matlab / С.Д. Штовба. – М.: Горячая линия-Телеком, 2007. – 288 с.

18. Круглов В.В. Нечеткая логика и искусственные нейронные сети / В.В. Круглов, М.И. Дли, Р.Ю. Голунов. – М.: Физматлит, 2001. – 224 с.

19. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі / В. В. Литвинов [та ін.] // Математичні машини і системи. К : ІПММС НАН України, 2018. – № 1. – С. 31-40.

20. Хакерська атака на Україну: подробиці // «РБК-Україна» укр. інформ. портал. [Електронний ресурс]. – Режим доступу: https://www.rbc.ua/ukr/news/hakerskaya-ataka-ukrainu-podrobnosti-14 98566985.html.

21. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А.А. Завада, О.В. Самчишин, В.В. Охрімчук // Інформаційні системи. Житомир : Збірник наукових праць ЖВІ НАУ, 2012. – Т. 6, № 12. – С. 97-10.

22. A Review of Intrusion Detection Systems / Neyole Misiko Jacob, Muchelule Yusuf Wanjala // Global Journal of Computer Science and Information Technology Research. Framingham : Global Journals Inc. – 2017. – Vol. 5, No. 4. – P. 1-5.

23. Грайворонський М.В. Безпека інформаційно-комунікаційних систем : навч. посіб. / М.В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.

24. Толюпа С.В. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови / С.В. Толюпа, С.С. Штаненко, Г.В. Берестовенко // Збірник наукових праць ВІТІ. – 2018. – № 3. – Р. 112-122.

25. Tajbakhsh A. Intrusion detection using fuzzy association rules / A. Tajbakhsh, M. Rahmati, A. Mirzaei // Applied Soft Computing. – 2009. – Vol. 9. – No. 2. – P. 462-469.

26. Chiang T.-S. Learning convergence analysis for Takagi-Sugeno Fuzzy Neural Networks / T.-S. Chiang, P. Liu, C-E. Yang. // 2012 IEEE International Conference on Fuzzy Systems. – Brisbane, QLD, Australia, 2012. – P. 1-6.

27. Субботин С.А. Метод синтеза нейро-нечетких моделей количественных зависимостей для решения задач диагностики и прогнозирования / С.А. Субботин. // Радиоэлектроника, информатика, управление. – 2010. – № 1. – С. 121- 127.

28. Ketata R. Fuzzy Approach for 802.11 Wireless Intrusion Detection. i-manager's / R. Ketata, H. Bellaaj. // Journal on Software Engineering. – 2007. – Vol. 2, issue 2. – P. 49-55.

29. Груздев С.П. Бинарная классификация компьютерных атак на информационные ресурсы при помощи нечёткой логики / С.П. Груздев, О.И. Шелухин // Телекоммуникации и информационные технологии. – 2019. – Т. 6, № 2. – С. 115-122.

30. Браницкий А.А. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов / А.А. Браницкий, И.В. Котенко // Информационно-управляющие системы. – 2015. – № 4. – С. 69-77.

31. Wang G. A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering / G. Wang, J. Hao, J. Ma, L. Huang. // Expert Systems with Applications. – 2010. – Vol. 37, issue 9. – P. 6225-6232.

32. Alsirhani A. DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark / A. Alsirhani, S. Sampalli, P. Bodorik. // IEEE Transactions on Network and Service Management. – 2019. – Vol. 16, no. 3. – P. 936-949.

33. Levonevskiy D.K. Network attacks detection using fuzzy logic / D.K. Levonevskiy, R.R. Fatkieva, S.R. Ryzhkov. // 2015 XVIII International Conference on Soft Computing and Measurements (SCM). – St. Petersburg, Russia, 2015. – P. 243-244.

34. A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack / N.P. Mkuzangwe, F.V. Nelwamondo. // Intelligent Information and Database Systems. ACIIDS 2017. Lecture Notes in Computer Science; N. Nguyen, S. Tojo, L. Nguyen, B. Trawiński (ed.). Springer, Cham. – 2017. – Vol. 10192. – P. 14-22.

35. Balan E.V. Fuzzy Based Intrusion Detection Systems in MANET / E.V. Balan, M.K. Priyan, C. Gokulnath, G.U. Devi. // Procedia Computer Science. – 2015. – Vol. 50. – P. 109-114.

36. Singh R. Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks / R. Singh, J. Singh, R. Singh. // Wireless Communications and Mobile Computing. – 2017. – Vol. 2017. – Article 3548607.

37. ViswaBharathy A.M. Fixed Neuro Fuzzy Classification Technique For Intrusion Detection Systems / A.M. ViswaBharathy, R. Bhavani // International Journal of Scientific & Technology Research. – 2019. – Vol. 8, issue 10. – P. 450-455.

38. Belej Ol. Development of a Network Attack Detection System Based on Hybrid Neuro-Fuzzy Algorithms / Ol. Belej, L. Halkiv // CEUR Workshop Proceedings. Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020). – Zaporizhzhia, Ukraine, April 27-May 1, 2020. – 2020. – Vol. 2608. – P. 926-938.

39. Upasani N.A modified neuro-fuzzy classifier and its parallel implementation on modern GPUs for real time intrusion detection / N. Upasani, H. Om. // Applied Soft Computing. – 2019. – Vol. 82. – Article 105595.

40. Pradeepthi K.V. Detection of Botnet traffic by using Neuro-fuzzy based Intrusion Detection / K.V. Pradeepthi, A. Kannan. // 2018 Tenth International Conference on Advanced Computing (ICoAC). – Chennai, India, 2018. – P. 118-123.

41. Mangrulkar N.S. Network Attacks and Their Detection Mechanisms: A Review / N.S. Mangrulkar, A R. Bhagat Patil, A.S. Pande. // International Journal of Computer Applications. – 2014. – Vol. 90, no. 9. – P. 37-39.

42. Munz G. Real-time Analysis of Flow Data for Network Attack Detection / G. Munz, G. Carle. // 2007 10th IFIP/IEEE International Symposium on Integrated Network Management. – Munich, Germany, 2007. – P. 100-108.

43. Moustafa N. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) / N. Moustafa, J. Slay. // 2015 Military Communications and Information Systems Conference (MilCIS). – Canberra, ACT, Australia. – 2015. – P. 1-6.

44. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	28	
6	А4	Спеціальна частина	11	
7	А4	Економічний розділ	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	6	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Короткова.ppt

2 Диплом Короткова.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-18-2 Короткової Н.Р. на тему: «Класифікація атак в інформаційно-комунікаційних мережах з використанням гібридних нейронечітких мереж»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 73 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на розробку та дослідження алгоритмів адаптивних нейронечітких мереж Anfis на базі різних уявлень нечітких правил, що дозволяють виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки.

При виконанні роботи авторка продемонструвала добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів функціонування систем виявлення вторгнень, класифікаційних ознак систем виявлення вторгнень і атак та напрямів їх побудови, а також нейронечітких мереж Anfis з різними алгоритмами нечітких перетворень в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ.

У ньому було проаналізовано існуючі підходи до ідентифікації мережевих атак з використанням систем нечіткого висновку, сформульовано задачу ідентифікації мережевих атак та досліджено алгоритми нейронечітких мереж Anfis на основі різних уявлень нечітких правил для ідентифікації мережевих атак.

Практична цінність роботи полягає у тому, що розроблене програмне забезпечення може використовуватись для обробки даних, отриманих з датчиків системи управління інформацією та подіями безпеки.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її авторка Короткова Н.Р. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**