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 магістра

студента *Трубки Дениса Андрійовича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Нейро-нечітке прогнозування трафіку інформаційно-комунікаційних мереж для систем виявлення атак*

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				
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 магістра

студенту ***Трубки Денису Андрійовичу*** **академічної групи** ***125м-21-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

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

на тему ***Нейро-нечітке прогнозування трафіку інформаційно-комунікаційних мереж для систем виявлення атак***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів побудови сучасних систем виявлення та запобігання атак, а також методів інтелектуального аналізу даних.	03.09.2022 – 10.10.2022
Розділ 2	Розробка підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму та оцінка його ефективності.	11.10.2022 – 24.11.2022
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	25.11.2022 – 04.12.2022

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

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Трубка Д.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 88 с., 15 рис., 2 табл., 4 додатки, 45 джерел.

Об’єкт дослідження – телекомунікаційний трафік.

Предмет дослідження – підхід до прогнозування мережевого самоподібного трафіку із використанням нейро-нечітких мереж.

Мета кваліфікаційної роботи – дослідження та обґрунтування нейро-нечітких адаптивних фільтрів-апроксиматорів для прогнозування мережевого трафіку для виявлення його аномалій при використанні в системах виявлення та запобігання атак.

Наукова новизна результатів полягає у тому, що було запропоновано проводити прогнозування мережевого трафіку із використанням нейро-нечітких адаптивних фільтрів-апроксиматорів Anfis, параметри яких було оптимізовано за допомогою генетичного алгоритму.

У першому розділі досліджено принципи побудови сучасних систем виявлення та запобігання атак, а також проаналізовано методи інтелектуального аналізу даних – гібридні нейро-нечіткі мережі та генетичні алгоритми.

У спеціальній частині роботи запропоновано підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму та оцінено його ефективність. 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.

ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ, АДАПТИВНА МЕРЕЖА НЕЧІТКОГО ВИСНОВКУ, ТЕЛЕКОМУНІКАЦІЙНИЙ ТРАФІК, ГЛОБАЛЬНА ОПТИМІЗАЦІЯ, СИСТЕМИ ВИЯВЛЕННЯ АТАК, ГЕНЕТИЧНИЙ АЛГОРИТМ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

ABSTRACT

Explanatory note: p. 88, fig. 15, tab. 2, 4 additions, 45 sources.

The object of research is telecommunication traffic.

The subject of the study is an approach to predicting network self-similar traffic using neuro-fuzzy networks.

The purpose of the qualification work is research and substantiation of neuro-fuzzy adaptive approximator filters for predicting network traffic to detect its anomalies when used in attack detection and prevention systems.

The scientific novelty of the results lies in the fact that it was proposed to forecast network traffic using Anfis neuro-fuzzy adaptive filters-approximators, the parameters of which were optimized using a genetic algorithm.

The first chapter examines the principles of building modern systems for detecting and preventing attacks, and also analyzes the methods of intelligent data analysis – hybrid neuro-fuzzy networks and genetic algorithms.

In a special part of the work, an approach to forecasting network traffic using adaptive networks of fuzzy inference and a genetic algorithm is proposed and its effectiveness is evaluated. Based on the results of the research, conclusions were made regarding the solution to the problem.

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

NETWORK ANOMALIES DETECTION, ADAPTIVE FUZZY INFERENCE NETWORK, TELECOMMUNICATION TRAFFIC, GLOBAL OPTIMIZATION, ATTACK DETECTION SYSTEMS, GENETIC ALGORITHM, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АФА – Адаптивний фільтр-апроксиматор;

ГА – Генетичний алгоритм;

ЕА – Еволюційний алгоритм;

ІАД – Інтелектуальний аналіз даних;

ІКМ – Інформаційно-комунікаційна мережа;

МНК – Метод найменших квадратів;

НМ – Нейронна мережа;

ПЗ – Програмне забезпечення;

СВА – Системи виявлення атак;

СВВ – Системи виявлення вторгнень;

ADS – Anomaly Detection System – Система виявлення аномалій;

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

IDS – Intrusion Detection System – Система виявлення вторгнень;

MDS – Misuse Detection Systems – Системи виявлення зловживань.

ЗМІСТ

ВСТУП

З розвитком інформаційних технологій збільшується кількість уразливостей та загроз різноманітним системам обробки даних і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки, а перспективним напрямком, який активно розвивається у сфері інформаційної та кібербезпеки є виявлення кібератак і запобігання вторгнень в інформаційних системах з боку неавторизованої сторони [1-13].

Отже, розвиток інформаційно-комунікаційних систем і мереж (ІКМ) та інформаційних технологій супроводжується проблемами безпеки мережевих ресурсів.

Одним із рішень актуальної задачі захисту ІКМ від кібератак є розробка та вдосконалення систем виявлення та запобігання атак (СВА), головне завдання яких полягає у виявленні мережевих атак, спроб несанкціонованого доступу і використання ресурсів мережі.

Мета функціонування СВА зводиться до оперативного виявлення вторгнень в ІКМ та запровадження ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів та сервісів.

Для виявлення мережевих вторгнень використовуються сучасні методи, моделі, засоби і комплексні технічні рішення для систем виявлення та запобігання вторгнень (СВВ), які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Загалом при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому системи виявлення вторгнень та атак повинні постійно удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні [12].

Наразі сформувались два напрямки протидії вторгнень: виявлення зловживань та виявлення аномалій [4, 5]. При виявленні мережевих аномалій даними для аналізу є мережевий трафік, представлений як інтенстівность (швидкість) передачі даних або набір мережевих пакетів, в загальному випадку фрагментованих на рівні IP. Дані можуть бути агреговані за певний часовий інтервал і нормалізовані, по ним оцінюються характеристики (набір ознак) трафіку. Створений набір ознак порівнюється з набором характеристик нормальної діяльності об'єкта (користувача або системи) – шаблоном нормальної поведінки. Якщо спостерігається суттєва розбіжність порівнюваних наборів, то фіксується мережева аномалія. В іншому випадку відбувається уточнення шаблону нормального трафіку за допомогою зміни параметрів його настройки з урахуванням поточного спостережуваного профілю мережевої активності. При цьому рішення о стані ІКМ приймається, зазвичай, за статистичними правилами (критеріями) [1-13].

Наразі для визначення шаблону нормальної поведінки перспективним є використання моделей захисту на основі розпізнавання аномалій в ІКМ [8-10], оскільки поточний трафік є реалізацією випадкового процесу, а його адекватна модель – статистично стійка закономірність цього процесу.

Мережевий трафік є нелінійним стохастичним процесом з властивостями самоподоби та з хаотичною і фрактальною динамікою. Крім того, встановлено, що агрегований трафік від різних джерел на малих часових масштабах проявляє мультифрактальний характер [15].

Оцінка характеристик трафіку ІКМ необхідна для побудови його адекватної моделі, що дозволяє сформувати еталонну модель (шаблон) «нормального» трафіку і за нею виявляти аномалії трафіку в СВА. При цьому прогнозування мережевого трафіку дозволяє підвищити оперативність виявлення атак.

Для вирішення задачі прогнозування мережевого трафіку найбільш актуальним є використання методів систем штучного інтелекту: нейронних мереж (НМ) та систем з нечіткою логікою, які є універсальними ефективними

апроксиматорами, а побудовані на їх основі фільтри ефективні для прогнозування та апроксимації нелінійних, стохастичних процесів [14-15].

Таким чином, актуальною задачею є побудова інтелектуальних адаптивних фільтрів-апроксиматорів (АФА) для прогнозування мережевого самоподібного трафіку, які б дозволяли їх використання в СВА для виявлення мережевих аномалій в реальному масштабі часу з достатньою ефективністю відносно похибок і достовірності та підвищеною оперативністю.

Метою роботи є дослідження та обґрунтування нейро-нечітких адаптивних фільтрів-апроксиматорів для прогнозування мережевого трафіку для виявлення його аномалій при використанні в системах виявлення та запобігання атак.

Постановка задачі:

• проаналізувати принципи побудови сучасних систем виявлення та запобігання атак;

• провести аналіз методів інтелектуального аналізу даних (гібридних нейро-нечітких мереж та генетичних алгоритмів);

• запропонувати підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Сучасні виклики кібербезпеки

Наразі все більше організацій ставлять кібербезпеку корпоративного середовища одним із пріоритетних завдань для успішної діяльності. Забезпечення захисту від атак – серйозний виклик, який залежить від багатьох факторів. Згідно звіту спеціалістів ESET наразі існують основні виклики, які постають перед кібербезпекою вже зараз та виникнуть у найближчому майбутньому [16].

1. Збільшення кількості кібератак.

Відповідно до звіту Cybersecurity Ventures [17], очікується, що глобальні збитки, спричинені кіберзлочинною діяльністю зростатимуть на 15% на рік з 2021 до 2025 року та можуть досягти 10,5 трильйонів доларів щорічно (рис. 1.1). Причинами такого зростання є значний ріст активності груп кіберзлочинців та зловмисників, діяльність яких спонсорується державою. У той же час кількість атак зростає внаслідок процесів цифрової трансформації.

Рисунок 1.1 – Глобальні витрати від кіберзлочинності у 2021 р. [17]

Оцінка вартості збитків базується на історичних показниках кіберзлочинності, включно з нещодавнім зростанням у порівнянні з минулим роком, різким збільшенням хакерської діяльності ворожих національних держав та організованих злочинних угруповань, а також площею кібератак, яка буде на порядок більшою у 2025 році, ніж це сьогодні.

Витрати, пов'язані з кіберзлочинністю, включають пошкодження та знищення даних, викрадені гроші, втрату продуктивності, крадіжку інтелектуальної власності, крадіжку особистих і фінансових даних, розкрадання, шахрайство, порушення нормального ходу діяльності після атаки, судове розслідування, відновлення та видалення зламаних даних і систем, а також шкоди репутації.

2. Дефіцит кваліфікованих спеціалістів з кібербезпеки.

Згідно з дослідженням $(ISC)^2$ Cybersecurity Workforce Study кількість кадрів у сфері кібербезпеки у 2022 році зросла на 4,7 мільйона, що на 11,1% більше, ніж у минулому році, тобто на 464 000 нових робочих місць [18]. Таке зростання спостерігається в усіх регіонах, при цьому Азіатсько-Тихоокеанський регіон (APAC – Asia-Pacific) зареєстрував найбільше зростання (15,6%), а Північна Америка – найменше (6,2%) (рис. 1.2). Тут EMEA – Europe, the Middle East and Africa – Європа, Близький Схід та Африка, LATAM – Південна Америка.

В умовах підвищеного попиту на професіоналів у галузі кібербезпеки продовжує зростати дефіцит кваліфікованих кадрів. Згідно з дослідженням $(ISC)^2$ Cybersecurity Workforce Study, глобальна нестача кадрів у сфері кібербезпеки становить 3,4 мільйона, при цьому 70% організацій мають незакриті вакансії (рис. 1.3). Багато держав працюють над зменшенням цього дефіциту, а великі компанії, такі як Google, Microsoft або IBM, запроваджують різні ініціативи, спрямовані на навчання та підвищення кваліфікації людей у сфері кібербезпеки.

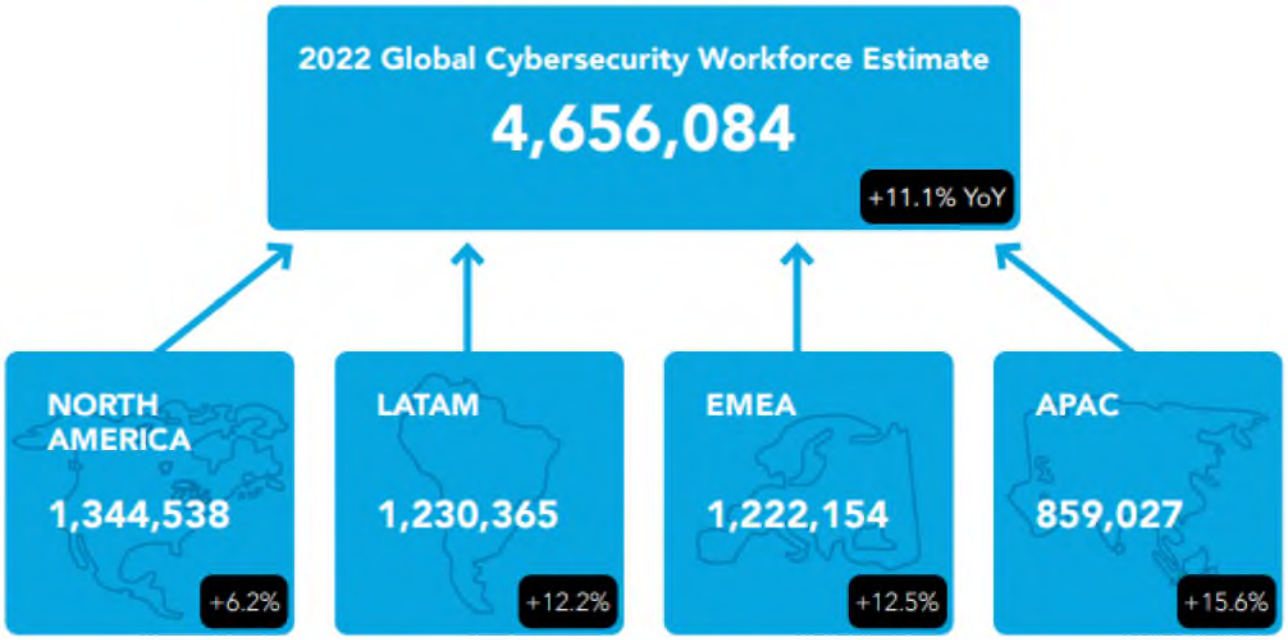


Рисунок 1.2 – Глобальна оцінка робочої сили з кібербезпеки у 2022 р. [18]

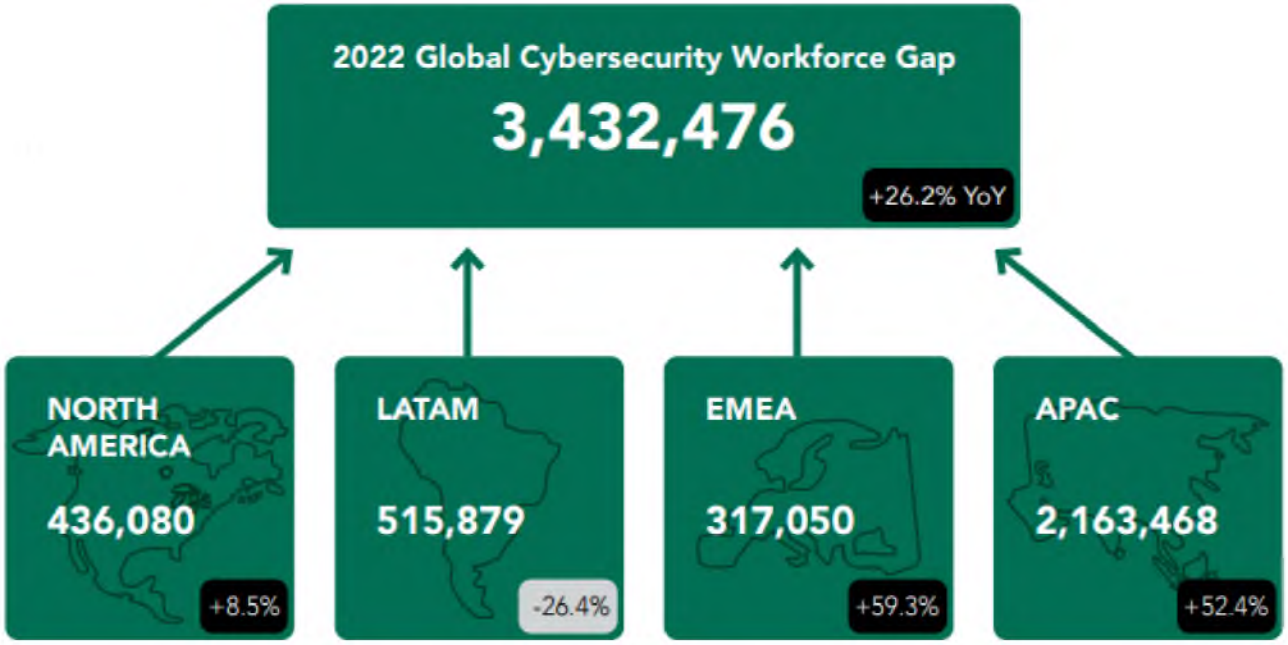


Рисунок 1.3 – Глобальна нестача кадрів у сфері кібербезпеки у 2022 р. [18]

Тим часом Всесвітній економічний форум спільно з кількома компаніями запустив освітню онлайн-платформу для окремих осіб та організацій під назвою Cybersecurity Learning Hub. Метою цього проекту є навчання та

вдосконалення навичок спеціалістів із кібербезпеки для забезпечення якісної роботи в цій галузі.

3. Недостатня підтримка інклюзивного персоналу.

На додаток до дефіциту кадрів з'являється інший виклик для кібербезпеки – це підтримка різноманітності та інклюзивності під час вибору персоналу на роботу. Для залучення менш захищених груп суспільства, наприклад, людей з інвалідністю необхідно розробити спеціальні ініціативи та політику.

Це не лише питання цінностей, а й виклик для інновацій та продуктивності, які є ключовими факторами успіху будь-якої організації. Крім цього, залучення таких груп людей допоможе скоротити дефіцит кваліфікованих спеціалістів з кібербезпеки.

4. Перехід на дистанційну та гібридну роботу.

У зв'язку із цифровою трансформацією бізнесів, спричиненою пандемією, багато компаній зіткнулися із проблемами у безпеці корпоративного середовища. Тоді кількість спроб атак на протокол віддаленого робочого столу (RDP) зросла на рекордні 768% протягом 2020 року, що виявилось одним із найуразливіших місць в інфраструктурі підприємств.

Тому зараз компаніям варто продовжувати належну підготовку та забезпечення можливостей співробітникам, які працюють віддалено, щоб уникнути потенційних ризиків та захиститися від нових атак кіберзлочинців, які постійно шукають нові недоліки кібербезпеки у корпоративних мережах.

5. Зростання активності у даркнеті.

Величезне зростання кримінальної активності у даркнеті за останні роки, особливо після початку пандемії, є серйозною проблемою, яка ще раз показує важливість досліджень у цих мережах Інтернету.

Моніторинг даркнету допомагає спеціалістам з кібербезпеки запобігати атакам, розуміти, як думають шахраї та кіберзлочинці, які шкідливі інструменти використовують зловмисники для доступу до систем організацій

або для обману користувачів, а також які корпоративні дані поширюються на чорних ринках.

6. Поява нових витончених тактик кібератак.

Одним із різновидів фішингу, який останнім часом активізувався, є гібридний фішинг, який поєднує традиційний метод на основі електронної пошти з вішингом. Цей вид використовується для отримання доступу до систем організації та розгортання шкідливих програм, таких як програми-вимагачі.

Під час нещодавньої атаки потенційна жертва спочатку отримала електронний лист, наприклад, про продовження підписки на послугу. При цьому у разі бажання скасувати підписку користувач може зателефонувати до служби підтримки за номером телефону, вказаним у повідомленні. Під час дзвінка жертву обманом заманюють встановити шкідливе програмне забезпечення (ПЗ), яке часто може поширюватися на інші пристрої.

Тим часом можливості машинного навчання створювати несправжні голоси швидко розвиваються. Серйозною загрозою є кількість атак, під час яких шахраї використовують інструменти на основі машинного навчання. Зокрема для імітації голосу директора певної компанії в режимі реального часу, щоб переконати співробітника переказати гроші на рахунок, який насправді належить зловмисникам.

7. Інтерес до криптовалюти зростає.

Не тільки користувачі, компанії та державні установи знаходять нові способи використання криптовалюти, а й кіберзлочинці. Збільшення кількості схем шахрайства з криптовалютою підтвердило інтерес хакерів до цієї галузі. Не дивно, що виклики, пов'язані з безпекою у світі криптовалют, також часто стають заголовками новин.

Використовуючи платформи у галузі криптовалют, NFT та ігор, зловмисники часто створюють нові фішингові сайти для викрадення облікових даних користувачів, зокрема для входу у криптовалютні гаманці. Тоді як криптовалютні біржі потрапляють під приціл APT-груп. Наприклад, нещодавно

було викрадено криптовалюту на суму 625 мільйонів доларів США з відеогри Axie Infinity, що пов'язують із кіберзлочинцями Lazarus.

8. Активність програм-вимагачів все ще висока.

Програми-вимагачі все ще залишаються серйозною проблемою, яка вимагає від організацій максимального захисту. Зокрема їм необхідно подбати про інструменти для протидії атакам програм-вимагачів, організацію комплексних навчальних програм з безпеки для співробітників та готовність до відновлення, якщо атака все ж таки трапиться. З 2020 по 2021 рік кількість атак програм-вимагачів зросла удвічі, залишаючись найбільш руйнівною загрозою для підприємств.

9. Вплив віртуального світу.

Прогнози щодо розвитку метавсесвіту показують, що до 2026 року 25% населення світу проводитиме принаймні 1 годину на день у цьому віртуальному світі. Тому безпека в метавсесвіті є викликом на майбутнє.

Ці спільні віртуальні світи для спілкування та ігор безсумнівно призведуть до великої кількості атак та шахрайства. Крім того, технологічні інновації не завжди розробляються з урахуванням правил безпеки та конфіденційності, оскільки пріоритетом є швидший вихід на ринок.

10. Недостатня обізнаність користувачів.

Базова проблема, з якою кібербезпека завжди стикатиметься, це недостатня цифрова обізнаність працівників щодо векторів атак та способів їх розпізнання. Тому співробітники є найслабшою ланкою захисту будь-якої організації. Однак завдяки підвищенню обізнаності сучасним загрозам персонал може стати першою лінією кіберзахисту.

1.2 Аналіз сучасних систем виявлення вторгнень та комп'ютерних атак

Як відомо, навіть найнадійніші системи захисту не здатні захистити від атак комп'ютерні системи державних та відомчих установ. Одна з причин – у тому, що в більшості систем безпеки застосовують стандартні механізми

захисту: ідентифікацію та аутентифікацію, механізми обмеження доступу до інформації згідно з правами суб'єкта і криптографічні механізми. Це традиційний підхід із своїми недоліками, як-то: незахищеність від власних користувачів – зловмисників, розмитість поділу суб'єктів системи на «своїх» і «чужих» через глобалізацію інформаційних ресурсів, порівняна легкість підбору паролів внаслідок використання їхнього змістового різновиду, зниження продуктивності і ускладнення інформаційних комунікацій внаслідок обмеження доступу до ресурсів організації. Важливо, щоб такі системи могли протистояти атакам, навіть якщо зловмисник уже був аутентифікований та авторизований і з формальної точки зору додержання прав доступу мав необхідні повноваження на свої дії [19-25].

Ці функції і виконують системи виявлення вторгнень (Intrusion Detection Systems, IDS). Оскільки передбачити всі сценарії розгортання подій в системі з активним «чужим» суб'єктом неможливо, слід або якомога детальніше описати можливі «зловмисні» сценарії або ж, навпаки, – «нормальні» і постулювати, що всяка активність, яка не підпадає під прийняте розуміння «нормальності», є небезпечною.

Сучасні системи виявлення вторгнень (СВВ) і системи виявлення та запобігання атак (СВА) 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 і СВА стали необхідним компонентом інфраструктури безпеки більшості організацій.

1.2.1 Технології і методи виявлення мережевих атак

IDS поділяються на системи, що реагують на відомі атаки – системи виявлення зловживань (Misuse Detection Systems, MDS) і системи виявлення

аномалій (Anomaly Detection Systems, ADS), які реєструють відхилення еволюції системи від нормального перебігу [19-28].

Моделі виявлення і запобігання мережевих атак діляться на два типу:

1. Хостова (host-based) модель виявлення мережевих атак передбачає аналіз даних, одержуваних і переданих в інформаційно-комунікаційну мережу (ІКМ), і аналіз різних журналів реєстрації, наявних на конкретному вузлі (хості) шляхом застосування відповідних методик і алгоритмів.

2. Мережева (network-based) модель виявлення мережевих атак передбачає аналіз мережевого трафіку безпосередньо в мережі, тобто аналізуються дані, взяті з технічних каналів зв'язку, з використанням середовища передачі даних і каналоутворюючого обладнання обчислювальної мережі, шляхом застосування відповідних методик і алгоритмів мережевого аналізу даних.

Засобами технології виявлення мережевих атак є програмні та апаратні системи виявлення атак, які функціонують переважно в TCP/IP мережах і базуються на сигнатурних та статистичних методиках виявлення на основі хостових і мережевих моделей.

Виявлення атак вимагає виконання однієї з двох умов: або розуміння очікуваного поведінки контрольованого об'єкта системи, або знання всіх можливих атак і їх модифікацій. У першому випадку використовується технологія виявлення аномальної поведінки (anomaly detection), а в другому – технологія виявлення зловмисної поведінки або зловживань (misuse detection).

Класифікація сучасних методів виявлення атак/вторгнень наведена на рис. 1.4.

Серед відомих методів виділяються наступні:

• статистичний метод;

• приховані марківські моделі;

• нечітка логіка;

• експертні системи;

• використання прогнозованих шаблонів;

• генетичні алгоритми;

• штучні нейронні мережі;

• аналіз переходів зі стану в стан;

• Data mining-методи.

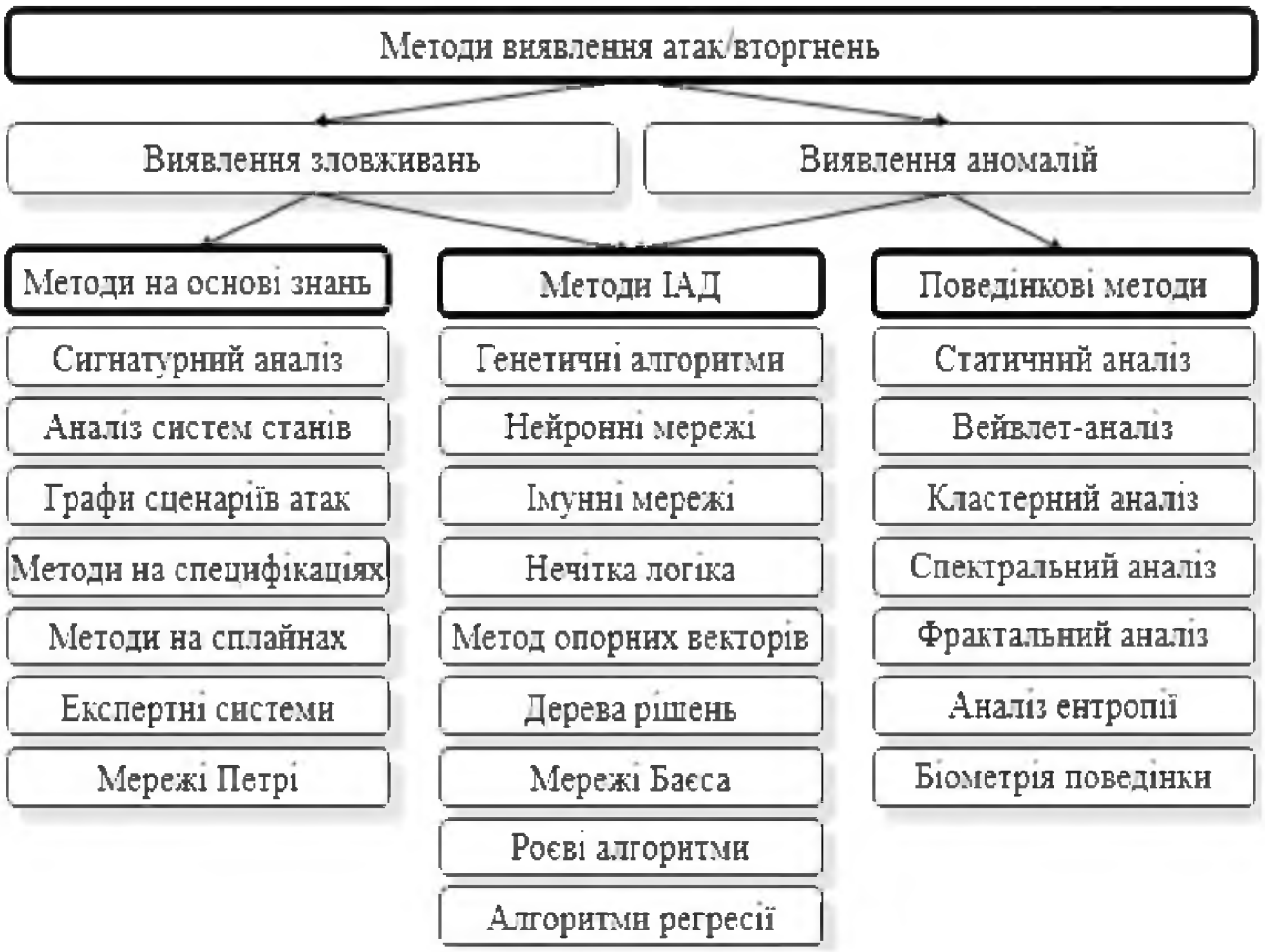


Рисунок 1.4 – Класифікація сучасних методів виявлення атак/вторгнень

Наразі актуальним є виявлення атак за допомогою методів інтелектуального аналізу даних (ІАД), зокрема нейронних мереж та систем нечіткої логіки, які є універсальними ефективними апроксиматорами. Встановлено, що протидіяти вторгненням і атакам основуючись тільки на одному з методів ІАД малоефективно, тому рекомендовано підходити до цього питання комплексно і будувати інтелектуальну систему протидії вторгненням, засновану на декількох методах ІАД.

Застосовувані при виявленні та запобіганні мережевих атак методи і моделі зводяться до мережевого і хостового аналізу сигнатурних і статистичних даних мережевого трафіку з подальшим виведенням засобів виявлення атак про здійснення атаки. До таких висновків відносяться повідомлення на консоль або в журнали засобів виявлення атак про час виявлення і проведення, назві та типу атаки. Результатами роботи засобів виявлення атак є дані про номери пакетів, що містяться в сеансі атаки.

Сигнатурний аналіз і контроль профілів при виявленні атак в ІКМ включає в себе аналіз заданих заздалегідь послідовностей, як самих аналізованих даних, так і послідовностей дій. Сучасні методики виявлення мережевих атак досить різнорідні і не зведені до єдиного критерію, за яким можливо оцінювати ефективність їх застосування. Таким критерієм може служити повнота охоплення всіх аналізованих параметрів, необхідних для точного і найбільш ймовірного виявлення атаки з мінімально хибним спрацьовуванням.

Для того, щоб система прийняття рішень могла узагальнювати дані, отримані від різних підсистем СВВ, необхідно стандартизувати формат повідомлень про атаки, що посилаються цими аналізаторами. Підсистема системи виявлення вторгнень повинна передавати в систему прийняття рішень вектор виду:

$$S = \left(A, C, G, T, M, P, P_н, P_в\right), \tag{1.1}$$

де А – системний ідентифікатор виявника атаки, С – ідентифікатор виявленої атаки, G – вид атаки, Т – системний час атаки, М – ідентифікатор методу, яким виявлена атака, Р – вірогідність проведення атаки, $P_н$ – нижня межа ймовірності атаки, $P_в$ – верхня межа ймовірності атаки.

Подальша обробка проводиться роздільно для кожного з видів атак. Часова вісь t розбивається на інтервали аналізу Δt. Довжина інтервалу Δt визначається виходячи з типу атаки і швидкості її виявлення підсистемами СВВ. У кожному інтервалі проводиться аналіз повідомлень з метою оцінки узагальненої ймовірності атаки. У ряді робіт, виконаних у суміжних областях,

показано, що вироблення оптимального методу об'єднання статистичних гіпотез про виявлення різнорідних об'єктів в практичній ситуації неможлива. Для систем виявлення атак це пояснюється відсутністю даних про апріорні ймовірності атак різних видів, різною природою проаналізованих ознак, неможливістю оцінки спільних рис розподілу значень цих ознак, рознесенням в часі моментів повідомлень про атаки.

Збільшення ймовірності виявлення атаки веде до зростання ймовірності «помилкової тривоги». Для того щоб ймовірність «помилкової тривоги» залишалася в допустимих межах, пропонується використовувати мажоритарний критерій для прийняття рішень. Якщо в системі присутні кілька виявників атак, які виявлятимуть заданий вид атаки, то рішення про наявність атаки приймається в випадку, якщо вона виявлена більш ніж половиною СВА.

Розвитком мажоритарного підходу є вимоги трудомісткої експертної роботи та застосування при обчисленні ймовірності атаки апріорної інформації про властивості підсистем, які реалізуються на основі обчислення зваженої суми значень P_i, де в якості ваги застосовується ступінь довіри до того чи іншого виявника (підсистемі СВВ) при розгляді даної конкретної атаки. Тоді ймовірність виявлення атаки (класу або групи атак) k може бути представлена виразом:

$$P_{КОБ}(\Delta t_i) = \sum_{j=1}^{m} W_{kj} \cdot P_{kj}, \tag{1.2}$$

де m – число аналізаторів, що використовуються в СВВ, P_{kj} – ймовірність атаки k, передана j-м аналізатором на інтервалі Δt_i,, W_{kj} – ступінь довіри результатам роботи аналізатора j при виявленні атаки k, причому $\sum_{j=1}^{m} W_{kj} = 1$. Якщо повідомлень про атаки в інтервалі аналізу Δt_i не зафіксовано, $P_{КОБ}(\Delta t_i) = 0$.

Сучасні СВВ можна розділити за характеристиками, що представлені на рис. 1.5.

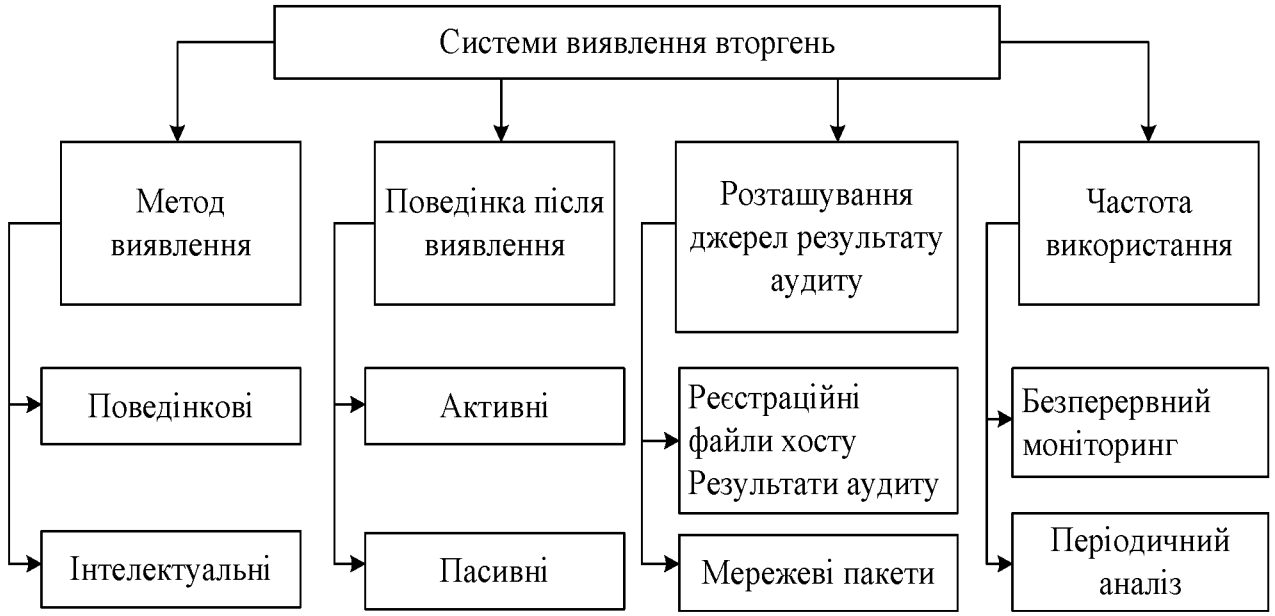


Рисунок 1.5 – Характеристики систем виявлення вторгнень

1.2.2 Аналіз програмних засобів систем виявлення вторгнень

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережевих вторгнень використовуються сучасні методи, моделі, засоби, програмне забезпечення і комплексні технічні рішення для систем виявлення та запобігання вторгнень, які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому СВВ повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні [12].

Серед таких систем є спеціалізовані програмні засоби, які направлені на виявлення підозрілої активності або втручання в ІКМ і прийняття адекватних заходів щодо запобігання кібератакам. Ці системи та засоби, як правило,

достатньо дорогі, мають закритий код та вимагають періодичної підтримки розробників (висококваліфікованих фахівців) щодо їх удосконалення і відповідного налаштування до умов конкретних організацій.

Як вже зазначалось вище, методи виявлення атак розділяють на методи виявлення зловживань і аномалій 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:

– 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.

Це також пов’язане з інтенсивним розвитком програмно-апаратних засобів і глобалізації ІКМ та їх повсякденного використання у всіх сферах діяльності суспільства.

В роботі [12] було проведено аналіз сучасних СВВ відносно базових характеристик «Клас кібератак», «Адаптивність», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження»,

«Реакція на кібератаку», «Захищеність» та «Підтримка операційної системи (ОС)» (табл. 1.1).

Таблиця 1.1 – Зведені дані результатів аналізу СВВ [12]

№	СВВ	Класи кібератак		Адаптивність	Методи виявлення											Управління системою		Масштабованість	Рівень спостереження		Реакція на кібератаку	Захищеність	Підтримка ОС			
		Зловживання	Аномалії		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Класерний	Аналітичний	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Централізоване	Розподілене		Системний	Мережевий			Unix	Linux	Windows	MacOS
1	Shadow	+	+	-	-	-	-	-	+	-	-	-	-	-	-	-	+	+	-	+	-	+	+	+	-	-
2	Cisco IPS	+	+	+	-	+	+	-	-	+	-	-	-	-	-	+	+	+	+	+	+	+	+	+	+	-
3	Arbor Networks Spectrum	+	+	+	-	+	+	-	-	-	+	-	-	-	-	+	-	+	+	+	+	-	+	+	+	-
4	InfoWatch ASAP	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	+	-	-	+	+	+	+
5	Symantec DeepSight Threat Management System	+	+	+	+	+	+	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+
6	IPS	+	+	+	-	+	+	-	-	-	+	-	+	-	-	+	-	+	+	+	+	+	-	-	+	-
7	Tipping Poing NGIPS	+	+	+	-	-	+	-	-	-	+	+	-	-	-	-	+	+	+	+	+	+	-	-	+	+
8	Axoft invGUARD	+	+	-	-	+	+	-	-	-	+	-	+	+	-	+	-	+	+	+	-	-	+	+	-	-
9	DefensePro	+	+	+	-	+	+	-	-	-	-	-	+	-	-	+	-	+	-	+	+	+	+	+	+	+
10	KATA Platform	+	+	+	-	+	+	-	-	-	+	-	+	-	-	-	+	+	+	+	+	+	+	+	+	+

«Клас кібератак» – визначає здатність системи виявляти аномалії та зловживання на різних рівнях ІКМ. Більшість сучасних засобів мають здатність виявляти обидва класи атак (аномалії та зловживання).

«Адаптивність» – дозволяє системі ефективно адаптуватись до нових атак (відсутніх у базі даних сигнатур), наприклад, 0-day та виявляти кібератаки з незначними модифікаціями.

«Методи виявлення» – множини методів, що використовуються для виявлення атак і складають математичну основу системи. Найбільш поширеними є методи статистичного і кластерного аналізу, контролю зміни подій, графів атак, сигнатурні, динамічні, машинного навчання, поведінкові, евристичні, експертні, нечітких множин тощо.

«Управління системою» – визначає схему управління і його рівень. Управління може здійснюватися централізовано із одного хоста або розподілено із окремих хостів, пов'язаних однією системою. Найбільш оптимальною є організація управління за централізованою схемою з певною множиною центрів, кожний з яких може бути задіяний для управління всією структурою.

Централізовані системи реалізують управління всіма засобами (модулями) виявлення аномалій та зловживань з однієї станції, а розподілені реалізують управління окремо, де кожний модуль відповідає за свою функцію.

«Масштабованість» – можливість розширення системи, її адаптивність до різних мережевих структур та долучення нових аналізованих ресурсів мережі.

«Рівень спостереження» – визначає, на якому рівні системи отримуються дані для виявлення кібератак. Застосовуються два рівні отримання даних – мережевий та системний. Сучасні системи, як правило, підтримують обидва рівні спостереження, оскільки саме їх взаємодія дозволяє краще забезпечити захист. Від цієї характеристики залежить швидкість формування первинних даних, їх правильна обробка та отримання точної інформації про поточний стан ІКМ.

Аналіз трафіку мережі здійснюється за допомогою спеціальних сенсорів (мережевих і системних), що застосовуються у системах виявлення атак та аномалій. Мережеві сенсори аналізують дані на мережевому рівні (зазвичай на основі сигнатурного аналізу) і генерують повідомлення про виявлення кібератак та відправляють їх до модулів управління. Системні сенсори аналізують журнали реєстрації операційної системи, додатки та програмні

застосунки на можливі аномалії чи загрози і генерують відповідні повідомлення, які надходять до модулів управління.

«Реакція на кібератаку» – визначає наявність у системі компонентів чи модулів протидії. Тобто, після реєстрації атаки ініціюються дії для редукування подальшого негативного впливу.

«Захищеність» – характеризує наявність власних компонентів системи, які відповідають за її захист від кібератак та зовнішнього негативного інформаційного впливу, а також за стійкість до виходу з ладу та зменшення кількості уразливостей розробки в цілому.

«Підтримка ОС» – характеризує тип ОС (наприклад, Unix, Linux, Windows, MacOS тощо), що підтримує відповідне ПЗ системи.

1.3 Гібридні нейро-нечіткі мережі

Наразі характерним є широке застосування методів систем штучного інтелекту (нейронних мереж, систем нечіткого висновку тощо) для вирішення різних завдань кібербезпеки, у тому числі прогнозування мережевого трафіку для СВА. Для побудови систем штучного інтелекту використовують різні підходи. Найбільш популярними наразі, і вже «класичними» є структурний та логічний підхід [14, 15, 29-43].

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 (НМ)». 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 нейро-нечіткі 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 нейро-нечітка мережа – 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.

1.3.1 Адаптивна мережа нечіткого висновку на основі алгоритму Сугено-Такагі

Алгоритм Сугено-Такагі використовує наступну модель нечіткого правила [15, 31]:

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

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,

$$y_i^* = p_{10} + \sum_{i=1}^{n} p_{ij} x_j \ , \tag{1.3}$$

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

$$y(x_1, x_2, \ldots, x_n) = \frac{\sum_{i=1}^{m} \min_j \left(\mu_{ij}(x_j)\right) p_{i0}}{\sum_{i=1}^{m} \min_j \left(\mu_{ij}(x_j)\right)} \ . \tag{1.4}$$

Структура нейро-нечіткої мережі Anfis на основі алгоритму Сугено-Такаги, представлена на рис. 1.6.

Мережа Anfis на основі алгоритму Сугено-Такаги 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.

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.

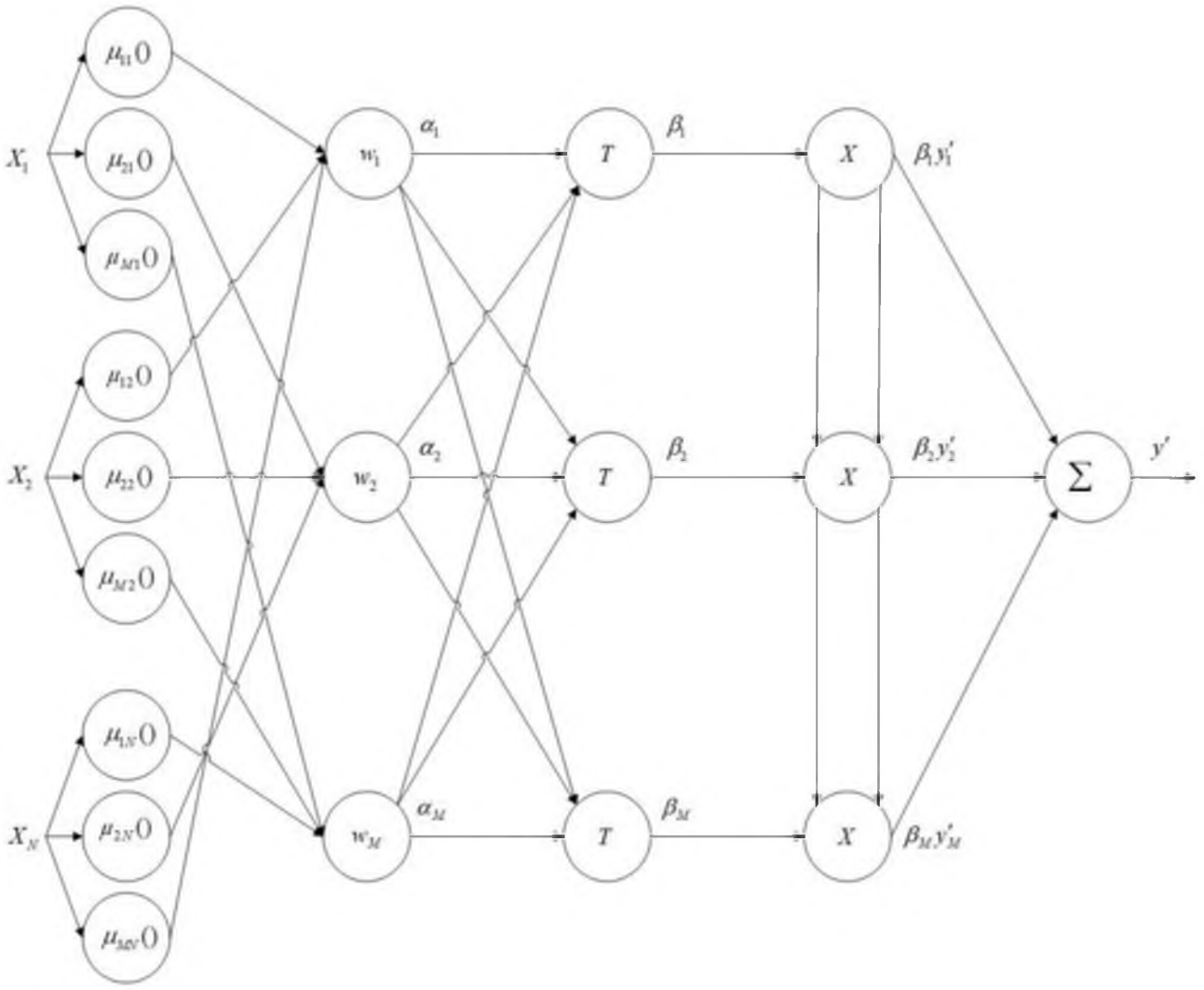


Рисунок 1.6 – Структура адаптивної мережі нечіткого висновку на основі алгоритму Сугено-Такагі

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

$$\tau_r^* = \frac{\tau_r}{\sum_{j=1}^{m} \tau_j}. \tag{1.5}$$

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:

$$y_r = \tau_r^* \left(b_{0,r} + b_{1,r} x_1 + \ldots + b_{n,r} x_n \right). \tag{1.6}$$

5. Єдиний вузол цього шару підсумовує вклади всіх правил:

$$y = \sum_{j=1}^{m} y_j. \tag{1.7}$$

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.

1.3.2 Адаптивна мережа нечіткого висновку на основі алгоритму Такагі-Сугено-Канга

В мережі Anfis із застосуванням алгоритму Такагі-Сугено-Канга процес навчання розбитий на два етапи та процес обчислень по етапах виконується паралельно і одночасно.

Відмінність алгоритмів Такагі-Сугено-Канга від алгоритму Сугено-Такагі полягає у реалізації нечіткої продукційної моделі, що базується на правилах типу [32]:

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

$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j \ , j = 1,\dots n. \tag{1.8}$$

Ця нечітка адаптивна мережа базується на таких положеннях:

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

$$\mu_{A_{ij}}(x_j) = \exp\left(-0{,}5\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right), \tag{1.9}$$

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:

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

$$= \frac{\sum_{i}^{n}\left(\left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j\right)\right)\prod_{j=1}^{m} \exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}}\right)^2\right]}{\sum_{i=1}^{n}\prod_{j}^{m}\exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}}\right)^2\right]}. \quad (1.10)$$

На рис. 1.7 представлена структура нейро-нечіткої мережі Anfis на основі алгоритму Такагі-Сугено-Канга.

Наведений аналітичний вираз (1.10) 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.

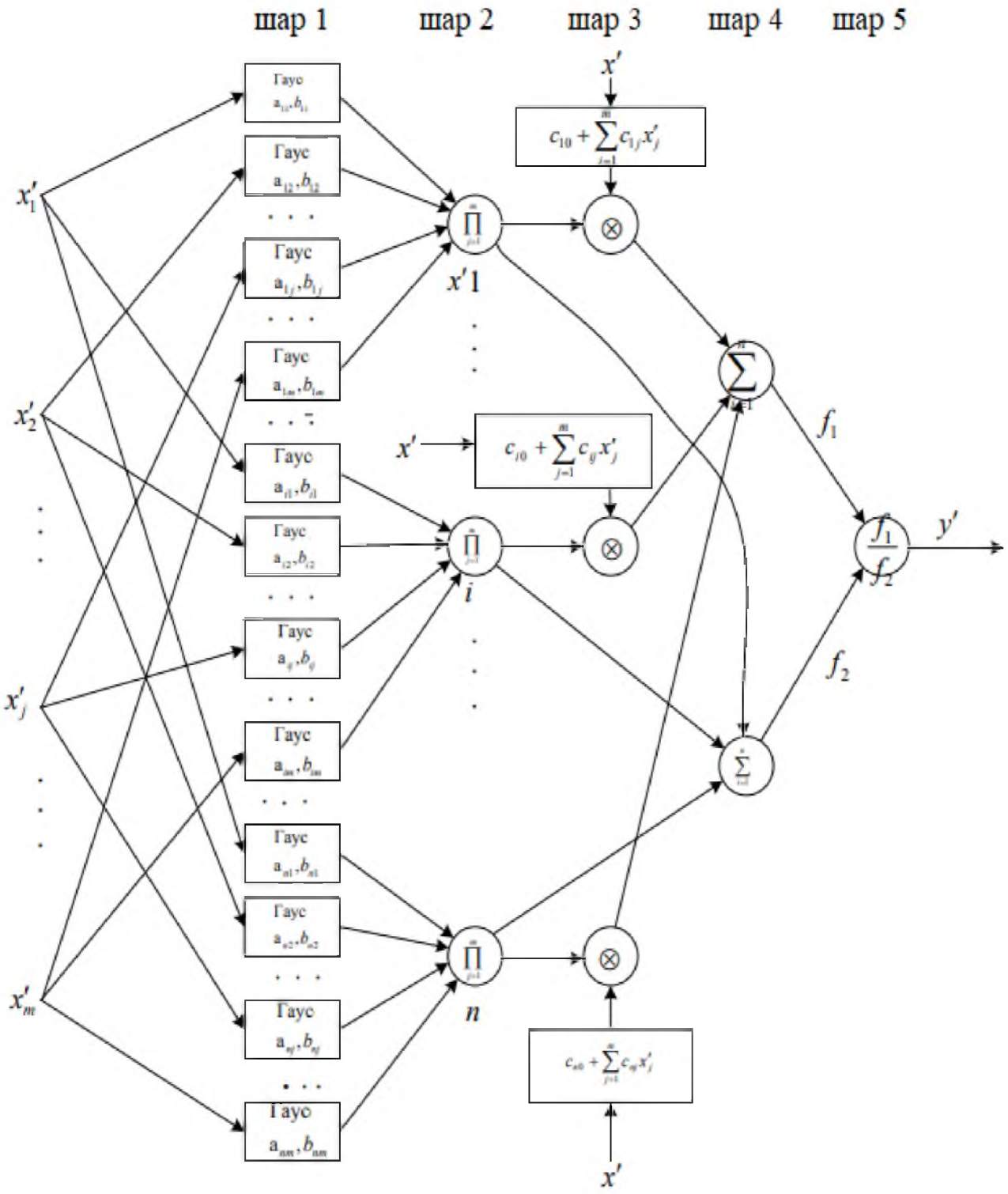


Рисунок 1.7 – Структура адаптивної мережі нечіткого висновку на основі алгоритму Такагі-Сугено-Канга

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 (1.10) у наступному вигляді:

$$y' = \sum_{i=1}^{n} w'_i \left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j \right), \tag{1.11}$$

де

$$w'_i = \frac{\prod_{j=1}^{m} \mu_{A_{ij}}(x'_j)}{\sum_{i=1}^{n} \prod_{j}^{mj} \mu_{A_{ij}}(x'_j)} = \frac{\prod_{j}^{m} \exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}} \right)^2 \right]}{\sum_{i=1}^{n} \prod_{j}^{m} \exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}} \right)^2 \right]} = \text{const} \tag{1.12}$$

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:

$$\begin{bmatrix} w_1'^{(1)} & w_1'^{(1)}x_1^{(1)} & \dots & w_1'^{(1)}x_m^{(1)} & \dots & w_n'^{(1)} & w_n'^{(1)}x_1^{(1)} & \dots & w_n'^{(1)}x_m^{(1)} \\ w_1'^{(2)} & w_1'^{(2)}x_1^{(2)} & \dots & w_1'^{(2)}x_m^{(2)} & \dots & w_n'^{(2)} & w_n'^{(2)}x_1^{(2)} & \dots & w_n'^{(2)}x_m^{(2)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ w_1'^{(k)} & w_1'^{(k)}x_1^{(k)} & \dots & w_1'^{(k)}x_m^{(k)} & \dots & w_n'^{(k)} & w_n'^{(k)}x_1^{(k)} & \dots & w_n'^{(k)}x_m^{(k)} \end{bmatrix}' \times \begin{bmatrix} c_{10} \\ \dots \\ c_{1m} \\ \dots \\ c_{n0} \\ \dots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix}, \tag{1.13}$$

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

Запишемо (2-13) у скороченому матричному вигляді

$$\boldsymbol{W} \times \mathbf{c} = \boldsymbol{y}. \tag{1.14}$$

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**:

$$c = W^{+} y = \left(W^{\mathrm{T}} \cdot W\right)^{-1} W^{\mathrm{T}} y. \tag{1.15}$$

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

$$y' = \begin{bmatrix} y'^{(1)} \\ y'^{(2)} \\ \dots \\ y'^{(k)} \end{bmatrix} = W \cdot c\,. \tag{1.16}$$

Визначаємо вектор похибок:

$$e = y' - y. \tag{1.17}$$

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

$$a_{ij}^{(k)}(t+1) = a_{ij}^{(k)}(t) - C\frac{dE^{(k)}(t)}{da_{ij}^{(k)}}; \tag{1.18}$$

$$b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) - C\frac{dE^{(\kappa)}(t)}{db_{ij}^{(k)}}. \quad (1.19)$$

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.

1.3.3 Адаптивна мережа нечіткого висновку на основі алгоритму Ванга-Менделя

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 мережа Anfis на основі алгоритму Ванга-Менделя є окремим випадком мережі Anfis на основі алгоритму Такагі-Сугено-Канга.

Мережа Anfis із застосуванням алгоритму Ванга-Менделя заснована на нечітких правилах [33]:

$П_i$: 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:

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

$$=\sup_{x\in X}\{\mu_{A_i'}(x)\,\mu_{A_{ij}}(x)\,\mu_{B_i}(y)\}=\sup_{x_1\ldots x_m\in X}\left\{\mu_{B_i}(y)\prod_{j=1}^{m}(\mu_{A_{ij}'}(x_j)\mu_{A_{ij}}(x_j))\right\}. \qquad (1.20)$$

Враховуючи, що вхідні змінні $x_j,\ldots,x_m$ є чіткими, то (1.20) набуває наступного вигляду

$$\mu_{B_i'}(y)=\mu_{B_i}[y]\prod_{j=1}^{m}\mu_{Aij}(x_i'). \qquad (1.21)$$

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

$$y'=\frac{\sum_{i=1}^{n}(\operatorname{argmax}_y\mu_{B_i'}(y)\;\mu_{B_i'}(y))}{\sum_{i=1}^{n}\mu_{B_i'}(y)}=\frac{\sum_{i=1}^{n}(\operatorname{argmax}_y\mu_{B_i'}(y)\;\mu_{B_i}(y)\prod_{j=1}^{m}\mu_{A_{ij}}(x_j'))}{\sum_{i=1}^{n}(\mu_{B_i'}(y)\prod_{j=1}^{m}\mu_{A_{ij}}(x_j'))}. \qquad (1.22)$$

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

$$y'=\frac{\sum_{i=1}^{n}(\operatorname{argmax}_y\mu_{B_i'}(y)\prod_{j=1}^{m}\mu_{A_{ij}}(x_j'))}{\sum_{i=1}^{n}\prod_{j=1}^{m}\mu_{A_{ij}}(x_j')}. \qquad (1.23)$$

У разі функції належності всіх нечітких множин вида функції Гауса, вираз (1.23) набуде вигляду

$$y'=\frac{\sum_{i=1}^{n}(\operatorname{argmax}_y(\exp\left[-\frac{y-c_i}{d_i}\right]))\prod_{j=1}^{m}\exp\left[-\frac{x_j'-a_{ij}}{b_{ij}}\right]}{\sum_{i=1}^{n}\prod_{j=1}^{m}\exp\left[-\frac{x_j'-a_{ij}}{b_{ij}}\right]} \qquad (1.24)$$

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.

Отже, в остаточному вигляді рівняння (1.24) перетворюється на наступний вираз:

$$y' = \frac{\sum_{i=1}^{n} c_i \prod_{j=1}^{m} \exp\left[-\frac{x'_j - a_{ij}}{b_{ij}}\right]}{\sum_{i=1}^{n} \prod_{j=1}^{m} \exp\left[-\frac{x'_j - a_{ij}}{b_{ij}}\right]}. \quad (1.25)$$

На рис. 1.8 представлена структура нечіткої продукційної мережі Anfis з алгоритмом Ванга-Менделя, елементи шарів якої реалізують відповідні компоненти виразу (1.25).

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 $\left(x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}, y^{(k)}\right)$, де $k=1,\ldots,K$ розраховується значення вихідної змінної $y'^{(k)}$.

Етап 2. Обчислюється функція похибки всім прикладів навчальної вибірки:

$$E^{(k)} = 0{,}5\left(y'^{(k)} - y^{(k)}\right)^2, \; k = 1,\ldots, K. \quad (1.26)$$

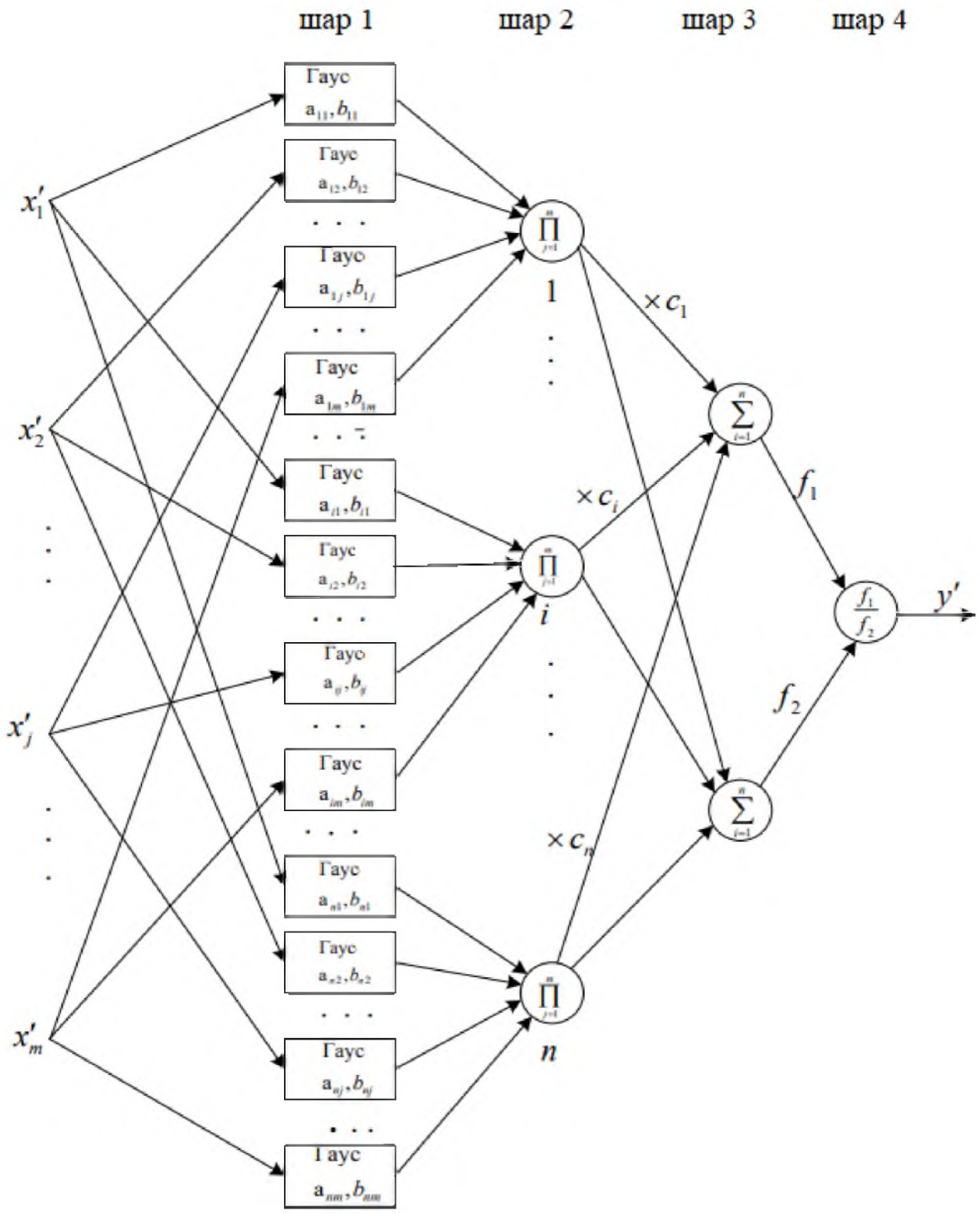


Рисунок 1.8 – Структура адаптивної мережі нечіткого висновку на основі алгоритму Ванга-Менделя

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

$$c_i(t+1) := c_i(t) - C\frac{dE^{(k)}(t)}{dc_i(t)},\ i = 1,\ldots,\ n,\quad k = 1,\ldots,\ K; \tag{1.27}$$

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:

$$E^{(k)} \prec \varepsilon,\ k = 1,\ldots,\ K; \tag{1.28}$$

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

$$E = \frac{1}{K}\sum_{k=1}^{K}\left(y'^{(k)} - y^{(k)}\right)^2 \prec \varepsilon; \tag{1.29}$$

- 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

$$a_{ij}(t+1) := a_{ij}(t) - C\frac{dE^{(k)}(t)}{da_i(t)} = a_{ij}(t) - C\frac{2\left(x_j'^{(k)} - a_{ij}\right)\left(y'^{(k)} - y^{[k]}\right)\left(c_i - y'^{(k)}\right)\prod_{j=1}^{m}\exp\left[-\left(\frac{x_j'^{(k)} - a_{ij}}{b_{ij}}\right)^2\right]}{b_{ij}^2\sum_{i=1}^{n}\prod_{j=1}^{m}\exp\left[-\left(\frac{x_j'^{(k)} - a_{ij}}{b_{ij}}\right)^2\right]} \tag{1.30}$$

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 Генетичні алгоритми

Для розв'язання задач оптимізації складних систем різного походження широко використовують еволюційні алгоритми (ЕА). Суть парадигми ЕА полягає у використанні базових принципів теорії біологічної еволюції – відбору, мутації і відтворення осіб. ЕА є частиною більш широкої технології так званих м'яких обчислень (Soft Computing), що включають в себе ще НМ, нечітку логіку, ймовірнісні міркування і мережі довіри. Дані технології доповнюють одна одну та використовуються у різних комбінаціях або самостійно для створення інтелектуальних систем [15].

Найбільш розвинений клас еволюційних алгоритмів – генетичні алгоритми (ГА).

Перевагами ЕА є:

- широка область застосування;
- можливість проблемно-орієнтованого кодування рішень;
- підбір початкової популяції, комбінування еволюційних обчислень з не еволюційними алгоритмами, продовження процесу еволюції до тих пір, поки є необхідні ресурси;
- придатність для пошуку в складному просторі рішень великої розмірності;
- відсутність обмежень на вид цільової функції;
- ясність схеми та базових принципів еволюційних обчислень;
- інтегрованість еволюційних обчислень з іншими некласичними парадигмами ШІ, такими як НМ і нечітка логіка.

До недоліків ЕА слід віднести наступні:

- евристичний характер еволюційних обчислень не гарантує оптимальності отриманого рішення (правда, на практиці, найчастіше, важливо

за заданий час отримати одне або кілька субоптимальних альтернативних рішень, тим більше що початкові дані в завданні можуть динамічно змінюватися, бути неточними або неповними);

- відносно висока обчислювальна трудомісткість, яка проте долається за рахунок розпаралелювання на рівні організації еволюційних обчислень і на рівні їх безпосередньої реалізації в обчислювальній системі;

- відносно невисока ефективність на заключних фазах моделювання еволюції (оператори пошуку в ЕА не орієнтовані на швидке потрапляння в локальний оптимум);

- невирішеність питань само адаптації.

ГА запропонував професор Мічиганського університету Холланд (J. Holland) в 60 рр. XX століття. Елементи цих алгоритмів досліджені раніше в роботах інших авторів. ГА отримали загальне визнання після виходу у 1975 р. в світ книги Холланда, що стала класикою в цій області «Адаптація в природних і штучних системах». Холланд відзначав, що розробку ним теорії ГА стимулювало читання біологічної літератури по дарвінівській теорії природного відбору і селекції сільськогосподарських культур.

Поряд з моделлю еволюції Дарвіна, покладеної в основу канонічного і сучасних ЕА, відомо також значне число інших моделей еволюції – модель Ламарка, модель Фріза, модель Гаулда і Елдріджа, тощо. На основі принципів, закладених в цих моделях, побудовані відповідні варіанти ЕА. Деякі ідеї зазначених моделей можуть бути використані і використовуються також для модифікації класичних ГА.

Чарльз Дарвін в його знаменитій праці «Походження видів» (1859 р.) показав, що еволюційний розвиток земної флори і фауни відбувається під впливом навколишнього середовища на основі наступних принципів: спадковість (нащадки зберігають властивості батьків), мінливість (нащадки майже завжди неідентичні), природний відбір (виживають найбільш пристосовані нащадки).

У 1944 р. Евері (O. Avery), Маклауд (C. MacLeod) і Маккарті (M. McCarty) довели, що дезоксирибонуклеїнова кислота (ДНК) є речовиною, що визначає спадкові процеси. У 1953 р. Крик (F. Crick) і Уотсон (J. D. Watson) розшифрували структуру ДНК у вигляді подвійної спіралі. Таким чином, на початку 60-х рр. XX століття стали відомі молекулярно-біологічні основи спадковості і мінливості видів, які й лягли в основу теорії ГА.

Мета при оптимізації за допомогою ГА полягає у тому, щоб знайти найкраще можливе рішення або рішення задачі по одному або декільком критеріям. Щоб реалізувати ГА, потрібно спочатку вибрати відповідну структуру для представлення цих рішень. У постановці задачі пошуку об'єкт цієї структури даних представляє точку в просторі пошуку усіх можливих рішень. Властивості об'єктів представлені значеннями параметрів, що об'єднуються в хромосоми. У генетичних методах оперують хромосомами, що відносяться до множини об'єктів популяції. Імітація генетичних принципів веде до еволюційного поліпшення значень цільової функції (функції пристосованості) від покоління до покоління.

Найчастіше хромосома – це бітовий рядок. Однак ГА не обмежені бінарним представленням даних. Деякі реалізації використовують цілочисельне або дійсне кодування. Незважаючи на те, що для багатьох реальних задач, мабуть, більше підходять рядки змінної довжини, в даний час структури фіксованої довжини найбільш поширені й вивчені. Тому далі розглядаються лише структури, які є поодинокими рядками по n біт.

Кожна хромосома (рядок) є конкатенацією ряду підкомпонентів, званих генами. Як було вже сказано раніше, гени розташовуються в різних позиціях або локусах хромосоми й приймають значення, звані алелями. В уявленнях з бінарними рядками ген – це біт, локус – його позиція в рядку і алель – його значення (0 або 1). Генотип відноситься до повної генетичної моделі особи і відповідає структурі в ГА, а фенотип відноситься до зовнішніх спостережуваних ознак і відповідає вектору в просторі параметрів.

Приклад використання ГА – задача максимізації наступної функції двох змінних: $f(x_1, x_2)=x_1x_2$, де $0\leq x_1\leq 1$ і $0\leq x_2\leq 1$.

Зазвичай методика кодування реальних змінних x_1 і x_2 полягає в їх перетворенні в двійкові цілочисельні рядки достатньої довжини (достатньої для забезпечення бажаної точності). Якщо припустити, що 10-розрядне кодування достатньо й для x_1, й для x_2, то встановити відповідність між генотипом і фенотипом закодованих осіб можна, розділивши відповідне бінарному представленню ціле число на значення 2^{10}-1. Наприклад, код [0000000000] відповідає дійсному значенню 0/1023 або 0, тоді як код [1111111111] відповідає 1023/1023 або 1. Структура даних, яка оптимізується – 20-бітний рядок, що представляє конкатенацію кодувань x_1 і x_2. Змінна x_1 розміщується в крайніх лівих 10-розрядах, тоді як x_2 розміщується у правій частині генотипу особи (20-бітовому рядку). При цьому, генотип – точка в 20-вимірному бінарному просторі, який досліджується ГА. Фенотип – точка в двовимірному просторі параметрів.

Кодування рішень.

Після того як обрані параметри, їх число і розрядність, необхідно вирішити, як безпосередньо записувати дані. Можна використовувати звичайне кодування, коли, наприклад, $1011_2=11_{10}$, або коди Грея, коли $1011_G=1110_2=14_{10}$. Незважаючи на те, що використання кодів Грея тягнуть неминуче кодування/декодування даних, вони дозволяють уникнути деяких проблем, які є нормальним результатом кодування. Перевага коду Грея у тому, що якщо два числа є послідовними при кодуванні, то і їх двійкові коди розрізняються тільки на один розряд, а в двійкових кодах це не так. Слід зазначити, що кодувати й декодувати в коди Грея можна таким чином: спочатку копіюється найстарший розряд, потім:

- з двійкового коду в код Грея: G[i] = XOR(B[i+1], B[i]);
- з коду Грея в двійковий код: B[i] = XOR(B[i+1], G[i]).

Тут G[i] і-й розряд коду Грея, а B[i] – і-й розряд бінарного коду. Наприклад, послідовність чисел від 0 до 7 в двійковому коді: {000, 001, 010, 011, 100, 101, 110, 111}, а в кодах Грея: {000, 001, 011, 010, 110, 111, 101, 100}.

1.4.1 Етапи генетичного алгоритму

Стандартний ГА починає свою роботу з формування початкової популяції I_0 – кінцевого набору допустимих рішень задачі. Ці рішення можуть бути обрані випадковим чином або отримані за допомогою простих наближених алгоритмів. Вибір початкової популяції не має значення для збіжності процесу в асимптотиці, проте формування «гарної» початкової популяції (наприклад, із множини локальних оптимумів) може помітно скоротити час досягнення глобального оптимуму. Якщо відсутні припущення про місцезнаходження глобального оптимуму, то індивіди з початкової популяції бажано розподілити рівномірно по всьому простору пошуку рішення.

Щоб оптимізувати будь-яку структуру з використанням ГА, потрібно задати міру якості для кожного індивіда в просторі пошуку. Для цієї мети використовується функція пристосованості. У задачах максимізації цільова функція часто сама виступає як функція пристосованості; для задач мінімізації цільову функцію слід інвертувати. Якщо задача, яку необхідно вирішити, має обмеження, виконання яких неможливо контролювати алгоритмічно, то функція пристосованості, як правило, включає також штрафи за невиконання обмежень (вони зменшують її значення).

На кожному кроці еволюції за допомогою ймовірнісного оператора селекції (відбору) обираються два рішення-батька для їх подальшого схрещування. Серед операторів селекції найбільш поширеними є два ймовірнісних оператора пропорційної і турнірній селекції. У деяких випадках також застосовується відбір урізанням.

Найпростіший пропорційний відбір – рулетка – відбирає осіб за допомогою n «запусків» рулетки. Колесо рулетки містить по одному сектору

для кожного і-го члена популяції. Розмір і-го сектора пропорційний відповідній величині P(i). При такому відборі члени популяції з більш високою пристосованістю з більшою ймовірністю будуть частіше вибиратися, ніж особи з низькою пристосованістю.

Турнірний відбір може бути описаний таким чином: з популяції, що містить m рядків (осіб), вибирається випадковим чином t рядків й найкращий рядок записується в проміжний масив (між обраними рядками проводиться турнір). Ця операція повторюється m раз. Рядки в отриманому проміжному масиві потім використовуються для схрещування (також випадковим чином). Розмір групи рядків, що відбираються для турніру, часто дорівнює 2. У цьому випадку говорять про двійковий/парний турнір. Взагалі ж t – чисельність турніру.

Стратегія відбору урізанням використовує відсортовану по спадаючій популяцію. Число осіб для схрещування вибирається відповідно до порогу $T \in [0; 1]$. Поріг визначає, яка частка осіб, починаючи з найпершої (самої пристосованої), братиме участь у відборі. В принципі, поріг можна задати й рівним 1, тоді все особи поточної популяції будуть допущені до відбору. Серед осіб, допущених до схрещування випадковим чином m/2 раз вибираються батьківські пари, нащадки яких утворюють нову популяцію.

Як тільки два рішення-батька обрані, до них застосовується ймовірнісний оператор схрещування (Crossover), який будує на їх основі нові (1 або 2) рішення-нащадка. Відібрані особи піддаються кросоверу (іноді званого рекомбінацією) із заданою вірогідністю P_c. Якщо кожна пара батьків породжує двох нащадків, для відтворення популяції необхідно схрестити m/2 пари. Для кожної пари з ймовірністю P_c застосовується кросовер. Відповідно, з ймовірністю $1-P_c$ кросовер не відбувається і тоді незмінені особи переходять на наступну стадію (мутації).

Існує велика кількість різновидів оператора схрещування. Найпростіший одноточковий кросовер працює наступним чином (рис. 1.9). Спочатку випадковим чином вибирається одна з можливих точок розриву (точка розриву

– ділянка між сусідніми бітами в рядку.) Обидві батьківські структури розриваються на два сегменти по цій точці. Далі відповідні сегменти різних батьків склеюються і виходять два генотипу нащадків.

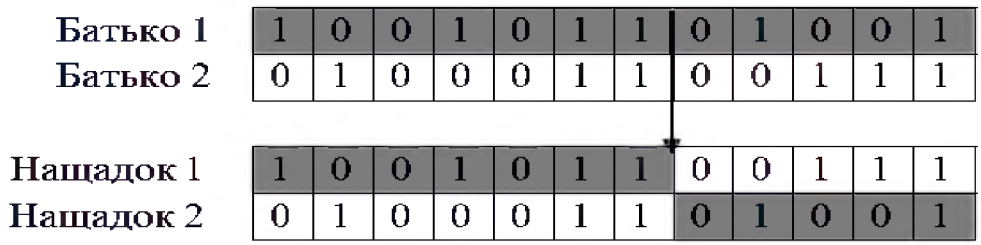


Рисунок 1.9 – Приклад роботи одноточкового кросовера

Наразі дослідники ГА пропонують багато інших операторів схрещування. Двоточковий і рівномірний кросовер цілком гідні альтернативи одноточковому. У двоточковому кросовері обираються дві точки розриву, й батьківські хромосоми обмінюються сегментом, який знаходиться між двома цими точками. У рівномірному кросовері кожен біт першого нащадка випадковим чином успадковується від одного з батьків; другому нащадку дістається біт другого з батьків.

Після того як закінчиться стадія кросовера, нащадки можуть піддаватися випадковим модифікаціям, званим мутаціями. У найпростішому випадку в кожній хромосомі, яка піддається мутації, кожен біт з ймовірністю P_m змінюється на протилежний – це так звана одноточкова мутація (рис. 1.10).

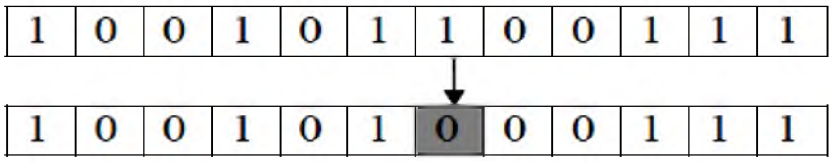


Рисунок 1.10 – Приклад виконання одноточкової мутації

Складнішою різновидом мутації є оператори інверсії і транслокації. Інверсія це перестановка генів у зворотному порядку всередині навмання вибраної ділянки хромосоми (рис. 1.11).

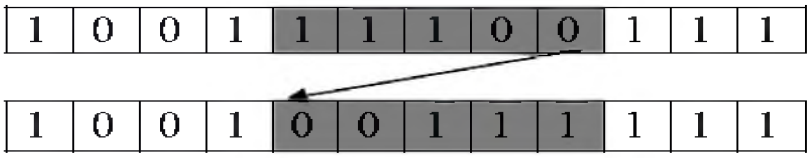


Рисунок 1.11 – Приклад виконання інверсії

Транслокація – це перенесення будь-якої ділянки хромосоми, в інший сегмент цієї ж хромосоми (рис. 1.12).

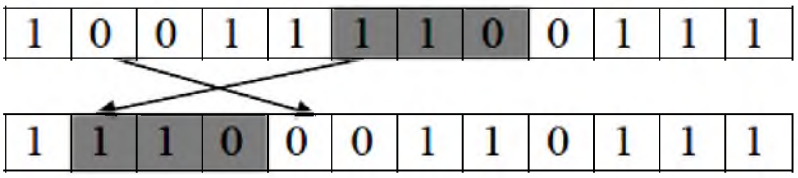


Рисунок 1.12 – Приклад виконання транслокації

Слід зазначити, що всі розглянуті вище генетичні оператори (одноточковий і багатоточковий кросовер, одноточкова мутація, інверсія, транслокація) мають схожі біологічні аналоги.

У деяких роботах пропонується використовувати стратегію інцесту як механізму само адаптації оператора мутації. Вона полягає у тому, що ймовірність мутації кожного гена P_m визначається для кожного нащадка на підставі генетичної близькості його батьків. Наприклад, це може бути відношення числа співпадаючих генів батьків до загальної кількості генів хромосоми. Це призводить до цікавого ефекту – при високій різноманітності генофонду популяції наслідки мутації будуть мінімальними, що дозволяє оператору схрещування працювати без стороннього втручання. У разі ж

зниження різноманітності, що виникає в основному при «застряганні» ГА в локальному оптимумі, наслідки мутації стають більш відчутними, а при повному стиску популяції ГА просто стає стохастичним, що збільшує ймовірність виходу популяції з локального оптимуму.

Іноді (з метою підвищення середньої пристосованості популяції) допустимо здійснювати спрямовані мутації, тобто після кожної зміни хромосоми перевіряти, чи підвищилася в результаті цієї мутації її пристосованість і, якщо ні, повертати хромосому до початкового стану.

Після схрещування і мутації осіб необхідно вирішити проблему про те, які з нових осіб увійдуть в наступне покоління, а які ні, а також що робити з їхніми батьками. Є два найпоширеніші способи.

1. Нові особи (нащадки) займають місця своїх батьків. Після чого настає наступний етап, у якому нащадки оцінюються, відбираються, дають потомство і поступаються місцем своїм «дітям».

2. Наступна популяція включає в себе як батьків, так і їх нащадків.

У другому випадку необхідно додатково визначити, які з осіб батьків і нащадків потраплять в нове покоління. У найпростішому випадку, в нього після кожного схрещування включаються дві кращі особи з четвірки батьків та їхніх нащадків.

Більш ефективним є механізм витиснення, який реалізується таким чином, що прагне видаляти «схожі» хромосоми із популяції та залишати такі, що відрізняються.

При розгляданні питання формування нового покоління слід виділити окремо принцип «елітизму». Суть цього принципу полягає у тому, що в нове покоління завжди включаються кращі батьківські особи. Їх число може бути від 1 і більше. Використання цього принципу дозволяє не втратити гарне проміжне рішення, але із-за цього алгоритм може «застрягти» у локальному екстремумі. У більшості випадків «елітизм» не шкодить пошуку рішення, і головне – надає алгоритму можливість аналізувати різні хромосоми з простору пошуку.

Робота ГА являє собою ітераційний процес, який триває до тих пір, поки не пройде задане число поколінь або не виконається будь-який інший критерій зупинки. В оптимізаційних задачах традиційними критеріями зупинки алгоритму є, наприклад, тривала відсутність прогресу в сенсі поліпшення значення середньої (або кращої) пристосованості популяції, мала різниця між кращим і гіршим значенням пристосованості для поточної популяції і тому подібне.

1.4.2 Канонічний генетичний алгоритм

Канонічний (Canonical) ГА є класичним алгоритмом. Ця еволюційна модель була запропонована Дж. Холландом в його знаменитій праці «Адаптація в природних і штучних середовищах» (1975). Часто можна зустріти опис простого ГА (Simple GA) Голдберга (D. Goldberg), він відрізняється від канонічного тим, що використовує замість рулеточного, турнірний відбір.

Модель канонічного ГА має наступні характеристики.

• фіксований розмір популяції;

• фіксовану розрядність генів;

• пропорційний відбір;

• одноточковий кросовер і одноточкову мутацію;

• формування наступного покоління з нащадків поточного покоління без «елітизму».

Алгоритм роботи ГА (репродуктивний план Холланда) складається в даному випадку з наступних етапів.

Етап 1. Ініціалізація початкової популяції. Покласти номер епохи t=0. Ініціалізувати випадковим чином m генотипів осіб і сформувати з них випадкову популяцію. Обчислити пристосованість осіб популяції $F(0)=(f_1(0), .., f_m(0))$, а потім середню пристосованість популяції

$$f_{\text{ñð}}(0) = \sum_{i=1}^{m} f_i(0) / m . \qquad (1.31)$$

Етап 2. Вибір батьків для схрещування. Збільшити номер епохи на одиницю: t=t+1. Визначити випадковим чином номер першого з батьків $l \in \{1...m\}$, призначивши ймовірність випадання будь-якого номера h пропорційною величині $f_h(t)/f_{ср}(t)$. Повторним випробуванням визначити номер другого з батьків k.

Етап 3. Формування генотипу нащадків. З заданою вірогідністю p_c провести над генотипами обраних батьків одноточковий кросовер. Далі до кожного з отриманих нащадків з імовірністю p_M застосувати оператор мутації.

Етап 4. Оновлення популяції. Помістити нащадків в популяцію, попередньо видаливши з неї батьків. Обчислити пристосованості нащадків й оновити значення середньої пристосованості популяції $f_{ср}(t)$.

Якщо формування популяції не завершено, перейти до етапу 2.

Слід зауважити, що у деяких модифікаціях класичного (канонічного) алгоритму нащадки заміняють в популяції не своїх батьків, а дві випадково вибрані особи.

1.5 Висновок. Постановка задачі

Встановлено, що одним із рішень актуальної задачі захисту ІКМ від кібератак є розробка та вдосконалення СВА, головне завдання яких полягає у виявленні мережевих атак, спроб несанкціонованого доступу і використання ресурсів мережі.

Одним із напрямків протидії вторгнень є виявлення аномалій. При виявленні мережевих аномалій даними для аналізу є мережевий трафік, представлений як інтенсивность (швидкість) передачі даних або набір мережевих пакетів, в загальному випадку фрагментованих на рівні IP.

Для визначення шаблону нормальної поведінки перспективним є використання моделей захисту на основі розпізнавання аномалій в ІКМ, оскільки поточний трафік є реалізацією випадкового процесу, а його адекватна модель – статистично стійка закономірність цього процесу.

Оцінка характеристик мережевого трафіку необхідна для побудови його адекватної моделі, що дозволяє сформувати еталонну модель (шаблон) «нормального» трафіку і за нею виявляти аномалії трафіку в СВА. При цьому прогнозування трафіку дозволяє підвищити оперативність виявлення атак.

Таким чином, невирішеною задачею є побудова адаптивних фільтрів-апроксиматорів для прогнозування мережевого самоподібного трафіку, які б дозволяли їх використання в СВА для виявлення мережевих аномалій в реальному масштабі часу з достатньою ефективністю відносно похибок і достовірності та підвищеною оперативністю.

З розвитком інформаційних технологій особливо актуальною стала проблема обробки великих даних. Безліч параметрів для виявлення мережевих атак становить значний обсяг даних, що визначає можливість їх обробки саме методами ІАД. Встановлено, що протидіяти вторгненням і атакам основуючись тільки на одному з методів ІАД малоефективно, тому рекомендовано підходити до цього питання комплексно і будувати СВВ, яка була б заснована на декількох методах ІАД.

Для вирішення задачі прогнозування мережевого трафіку найбільш актуальним є використання методів систем штучного інтелекту: нейронних мереж (НМ) та систем з нечіткою логікою, які є універсальними ефективними апроксиматорами, а побудовані на їх основі фільтри ефективні для прогнозування та апроксимації нелінійних, стохастичних процесів [14-15].

Для усунення недоліків НМ і систем з нечіткою логікою запропоновані гібридні нейро-нечіткі мережі Anfis. Такі мережі можуть бути побудовані на основі алгоритмів Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя.

Найбільш популярними методами глобальної оптимізації є генетичні алгоритми.

Отже, висновки, які отримані в цьому розділі, визначають подальші цілі і завдання, та підтверджують актуальність роботи.

Таким чином, для виконання мети кваліфікаційної роботи необхідно:

• запропонувати підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму

В адаптивних фільтрах-апроксиматорах процес адаптації полягає в оцінюванні шуканого виходу фільтра та коригування його параметрів залежно від значення вихідної похибки.

АФА на основі нечіткої логіки ґрунтуються на твердженні, що функція належності елемента множині може набувати значення в інтервалі [0, 1]. Чим це значення ближче до 1, тим більша відповідність елемента універсальної множини властивостям нечіткої множини.

Переваги таких АФА – прозорість процесу одержання висновків на основі словесного опису експертних знань про процес, а також стійкість до шумів. Недоліки – відсутність автоматичного набуття знань; обмежена кількість вхідних змінних.

Для усунення недоліка щодо відсутності автоматичного набуття знань запропоновано будувати АФА на основі гібридних нейро-нечітких мереж Anfis (див. розділ 1.3).

Рівняння АФА на основі адаптивної мережі нечіткого висновку пропонується наводити у вигляді:

$$\hat{Y}[m+n]=\sum_{\tau\in P}\sum_{k\in Q}\beta_k[\tau]\cdot\alpha_k[m-\tau], \qquad (2.1)$$

де $\beta_k[\tau]=U_k^{-1}(\alpha_k[\tau]/\sum_k\alpha_k[\tau])$, $U=U(a_U)$, $\alpha_k[m-\tau]=T_{\underset{l,k\in Q}{norm}}\{L_{l,k}(y_k[m-\tau])\}$, $L=L(a_L)$.

Тут m – поточний такт часу; n – глибина прогнозу; P – множина глибин пам'яті відповідних входів; Q – множина входів нейронів; U_k^{-1} – функція, зворотна функції належності проміжного виходу k мережі з параметрами a_U; α_k – значення проміжного виходу; T_{norm} – довільна t-норма моделювання

логічної операції «І»; y_k – значення вхідного сигналу на вході мережі k; $L_{l,k}$ – функція належності нечіткого правила l входу k із параметрами a_L. Параметри налаштування такого АФА – $\{a_U, a_L\} \subset a$.

Зазвичай для налаштування параметрів адаптивної мережі нечіткого висновку використовують або алгоритм зворотного поширення похибки або .

Слід зазначити, що знаходження (налаштування) оптимальних (для конкретної задачі) параметрів АФА є актуальною задачею, зокрема, й при прогнозуванні мережевого трафіку. Оскільки ця задача є полімодальною, то це вимагає використання методів глобальної оптимізації, серед яких найбільш ефективними є пошукові методи. У них алгоритм пошуку оптимального рішення пов'язує наступні один за одним рішення $\Psi_s(j+1) = F[\Psi_s(j)]$, де F – алгоритм пошуку, який показує які операції слід зробити на кроці j при рішенні $\Psi_s(j)$, щоб отримати нове рішення $\Psi_s(j+1) \succ \Psi_s(j)$. Тут знак переваги $\succ$ при мінімізації функціоналу має сенс:

$$C[\Psi_s(j+1)] < C[\Psi_s(j)]. \tag{2.2}$$

Розвитком пошукових методів є ЕА, серед яких найбільш поширені ГА, які моделюють розвиток біологічної популяції на рівні геномів: мутації структури і параметрів $\delta\Psi_s$, їх схрещування (розмноження):

$$\Psi_s(j+1) = \Psi_s(j) + \delta\Psi_s(j), \tag{2.3}$$

і правило відбору, що дозволяє виявляти їх сприятливі варіації, за допомогою яких будується послідовність поліпшених рішень.

Як критерій параметричної оптимізації використовують критерій регулярності, що заснований на поділі даних на навчальну А і перевірочну В вибірки [44]:

$$C_{рег} = \frac{\left\| Y_B^*[m+n] - \hat{Y}_B[m+n] \right\|}{\left\| Y_B^*[m+n] \right\|}, \tag{2.4}$$

де m – глибина пам'яті, n – глибина прогнозу.

Як критерій структурної (глобальної) оптимізації використовують комбінований критерій [44]:

$$C_{комб} = 0{,}2 \cdot C_{рег} + 0{,}8 \cdot C_{зм}, \tag{2.5}$$

де $C_{см}$ – критерій незміщенності (мінімуму зсуву), що заснований на аналізі рішень.

Критерій $C_{см}$ не чутливий до рівня шуму у вхідних даних і при збільшенні завад їх мінімум не зміщується в область простіших моделей [44]:

$$C_{см} = \frac{\left\| \hat{Y}_A[m+n] - \hat{Y}_B[m+n] \right\|}{\left\| Y^*[m+n] \right\|}, \tag{2.6}$$

де $\hat{Y}_A[m+n]$ і $\hat{Y}_B[m+n]$ – виходи моделей, які навчені на вибірках А і В, відповідно.

Таким чином, запропонований підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму полягає у використанні глобальної оптимізації (ГА) для вибору параметрів нейро-нечітких АФА Anfis (на основі алгоритму Сугено-Такагі, алгоритму Такагі-Сугено-Канга та Ванга-Менделя).

Узагальнена структура алгоритму прогнозування мережевого трафіку згідно запропонованого підходу із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму зображена на рис. 2.1.

2.2 Оцінка ефективності запропонованого підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму

Оцінка ефективності запропонованого підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму виконувалась в середовищі Matlab за допомогою стандартних і розроблених програм.

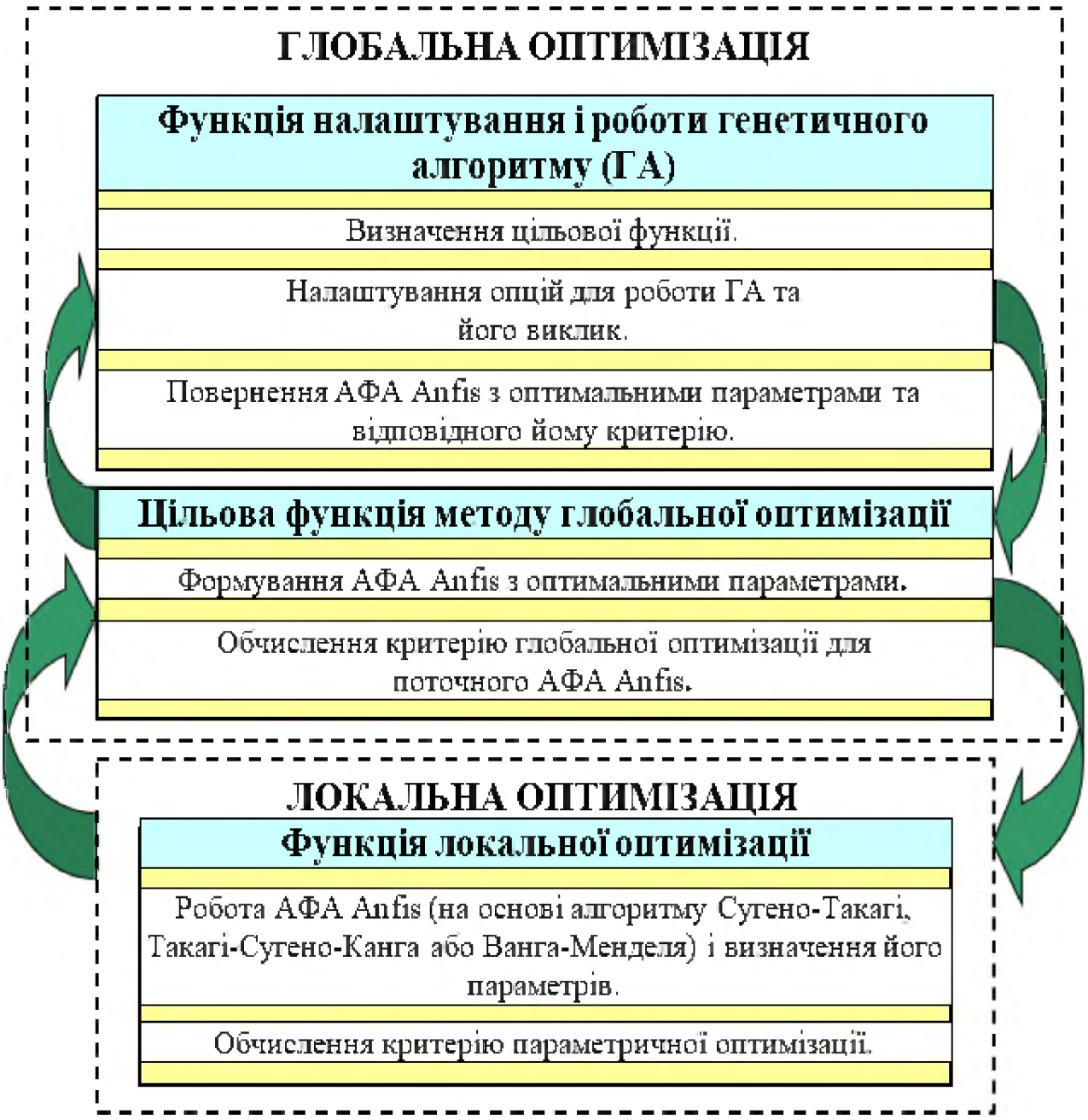


Рисунок 2.1 – Узагальнена структура алгоритму прогнозування мережевого трафіку згідно запропонованого підходу із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму

Моделювання розв'язання задачі прогнозування мережевого трафіку виконувалося на основі експериментальних даних – трафіку, що передається через мережу Інтернет [45]. Дані являють собою залежність розміру Ethernet

кадрів в байтах від часу. Для їх нормування по часової осі була проведена процедура агрегації з кроком 5 с.

Глибина прогнозу була прийнята 1 такт (5 с), а глибина пам'яті за різними входами від 1 до 4.

В якості критерію глобальної (структурної) оптимізації було обрано критерій (2.5).

Як глобальний метод оптимізації використовувався ГА, який мав одноточкове схрещування, селективний вибір батьків, формування нової популяції із витісненням. Кількість поколінь обмежувалось на рівні 100, а розмір популяції – 30.

Як АФА використовувались адаптивні мережі нечіткого висновку Anfis:

• на основі алгоритму Сугено-Такагі (див. розділ 1.3.1);

• на основі алгоритму Такагі-Сугено-Канга (див. розділ 1.3.2);

• на основі алгоритму Ванга-Менделя (див. розділ 1.3.2).

При глобальній оптимізації варіювались наступні параметри кожного АФА:

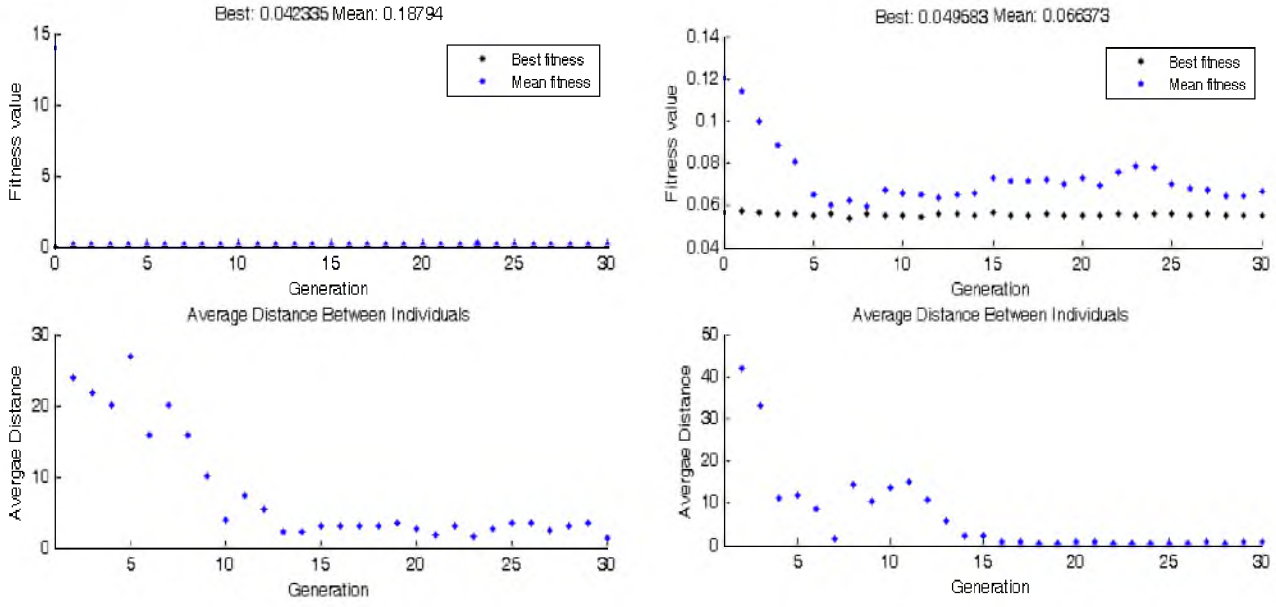
• $L_{l,k}$ – функція належності нечіткого правила l входу k;

• M_{po} – метод параметричної оптимізації (функція навчання адаптивної мережі нечіткого висновку Anfis).

Результати глобальної оптимізації параметрів нейро-нечітких АФА Anfis наведено на рис. 2.2.

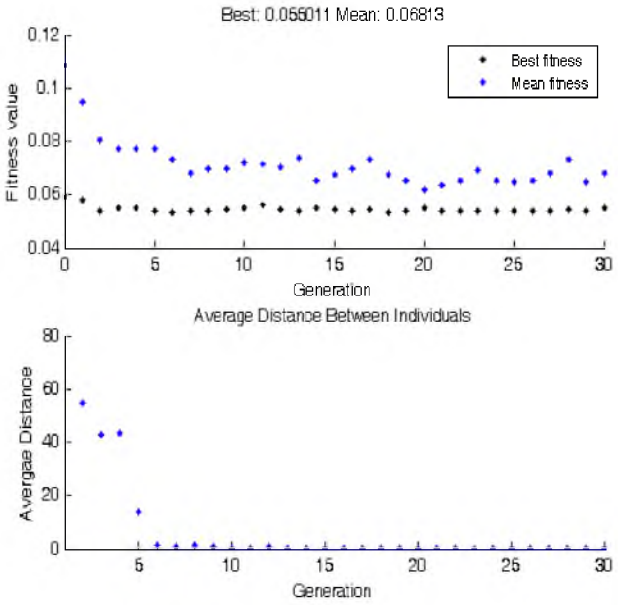
Встановлено, що для нейро-нечіткого АФА Anfis на основі алгоритму Сугено-Такагі мінімуму критерію (2.5) ($C_{комб}$=0,042) відповідає нейро-нечітка мережа Anfis з функцією належності – різниця двох сигмоїдальних функцій, і яка навчена алгоритмом зворотного поширення похибки.

Встановлено, що для нейро-нечіткого АФА Anfis на основі алгоритму Такагі-Сугено-Канга мінімуму критерію (2.5) ($C_{комб}$=0,05) відповідає нейро-нечітка мережа Anfis з Гаусовою функцією належності, і яка навчена гібридним алгоритмом (комбінація градієнтного спуску і МНК).



а

б



в

Рисунок 2.2 – Результати оптимізації параметрів АФА на основі адаптивних мереж нечіткого висновку Anfis з використанням алгоритму Сугено-Такагі (а), Такагі-Сугено-Канга (б) та Ванга-Менделя (в) для прогнозування мережевого трафіку за допомогою ГА

Встановлено, що для нейро-нечіткого АФА Anfis на основі алгоритму Ванга-Менделя мінімуму критерію (2.5) ($C_{комб}$=0,055) відповідає нейро-нечітка мережа Anfis з Гаусовою функцією належності, і яка навчена гібридним алгоритмом (комбінація градієнтного спуску і МНК).

В результаті моделювання (див. рис. 2.2) встановлено, що ГА виходить в область оптимальних рішень у середньому протягом перших п'яти поколінь. Його швидкодія склала у середньому 16 с на покоління.

Результати прогнозування мережевого трафіку для кожного АФА на основі адаптивних мереж нечіткого висновку Anfis з налаштованими параметрами наведено на рис. 2.3 та в табл. 2.1.

Таблиця 2.1 – Похибки прогнозування (2.4) мережевого трафіку

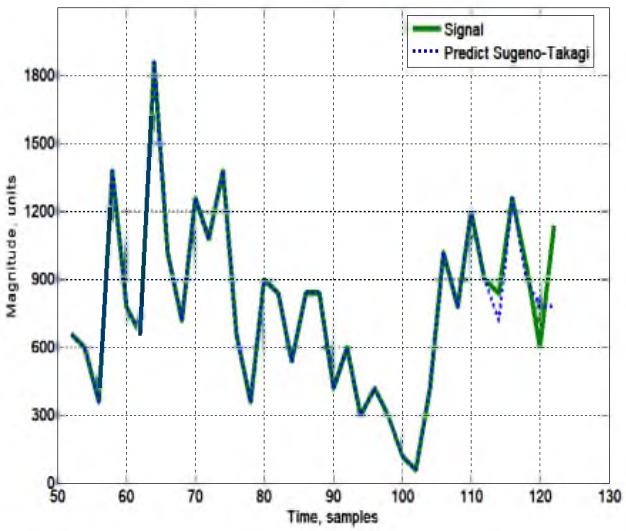
Нейро-нечіткий АФА Anfis		
на основі алгоритму Сугено-Такагі	на основі алгоритму Такагі-Сугено-Канга	на основі алгоритму Ванга-Менделя
0,0432	0,0485	0,0496

Як похибки прогнозування використовувався критерій регулярності (2.4), значення якого для нейро-нечіткого АФА Anfis на основі алгоритму Сугено-Такагі склало – 0,0432, для АФА Anfis на основі алгоритму Такагі-Сугено-Канга склало – 0,0485, для АФА Anfis на основі алгоритму Ванга-Менделя – 0,0496.

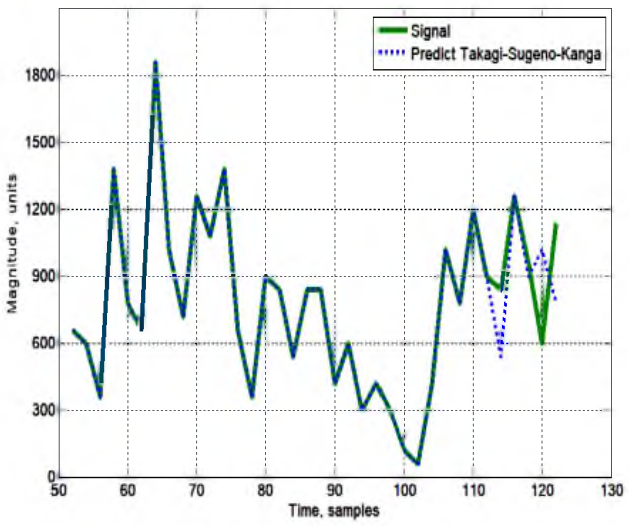
Таким чином, найкращі результати з прогнозування мережевого трафіку (в сенсі критерію регулярності (2.4)) показав нейро-нечіткий АФА Anfis на основі алгоритму Сугено-Такагі, АФА Anfis на основі алгоритму Такагі-Сугено-Канга та алгоритму Ванга-Менделя показали приблизно однакові результати.

Адекватність отриманих нейро-нечітких АФА перевірялась за непараметричним критерієм знаків. Було встановлено, що для рівня значущості

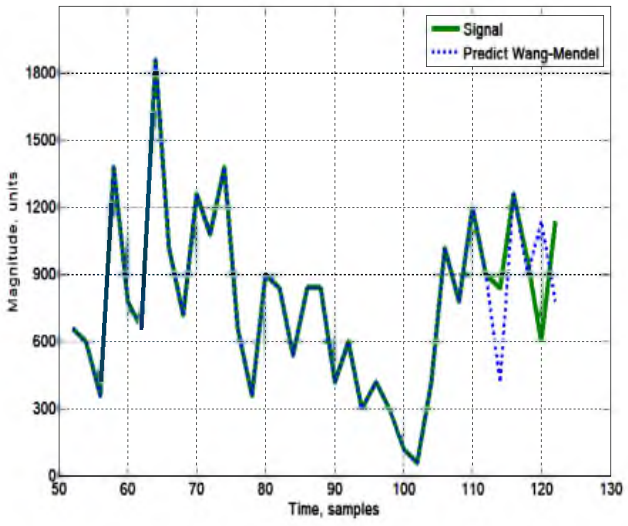
0,01 досліджені нейро-нечіткі АФА з обґрунтованими параметрами адекватні експериментальним реалізаціям.



а



б



в

Рисунок 2.3 – Результат прогнозування мережевого трафіку нейро-нечітким АФА Anfis на основі алгоритму: а – Сугено-Такагі; б – Такагі-Сугено-Канга; в – Ванга-Менделя

Практична цінність кваліфікаційної роботи полягає в тому, що отримані нейро-нечіткі адаптивні фільтри-апроксиматори Anfis на основі алгоритмів

Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя можуть бути використані в засобах моніторингу, здатних аналізувати трафік мережі в режимі реального часу.

2.3 Висновки

В розділі запропоновано підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму полягає у використанні глобальної оптимізації (ГА) для вибору параметрів нейро-нечітких АФА Anfis (на основі алгоритму Сугено-Такагі, алгоритму Такагі-Сугено-Канга та Ванга-Менделя).

Оцінка ефективності запропонованого підходу виконувалась в середовищі Matlab за допомогою стандартних і розроблених програм на основі експериментальних даних – трафіку, що передається через мережу Інтернет. Дані являють собою залежність розміру Ethernet кадрів в байтах від часу.

Як глобальний метод оптимізації використовувався ГА, який мав одноточкове схрещування, селективний вибір батьків, формування нової популяції із витісненням. Кількість поколінь обмежувалось на рівні 100, а розмір популяції – 30.

Як АФА використовувались адаптивні мережі нечіткого висновку Anfis на основі алгоритму Сугено-Такагі, алгоритму Такагі-Сугено-Канга та Ванга-Менделя. При глобальній оптимізації варіювались наступні параметри кожного АФА: $L_{l,k}$ – функція належності нечіткого правила l входу k; M_{po} – метод параметричної оптимізації (функція навчання адаптивної мережі нечіткого висновку Anfis).

Як критерій глобальної оптимізації використовувався комбінований критерій.

Встановлено, що для нейро-нечіткого АФА Anfis на основі алгоритму Сугено-Такагі мінімуму цього критерію ($C_{комб}$=0,042) відповідає мережа Anfis з функцією належності – різниця двох сигмоїдальних функцій, і яка навчена

алгоритмом зворотного поширення похибки. Для АФА Anfis на основі алгоритму Такагі-Сугено-Канга мінімуму комбінованого критерію ($C_{комб}$=0,05) відповідає мережа Anfis з Гаусовою функцією належності, і яка навчена гібридним алгоритмом (комбінація градієнтного спуску і МНК). Для нейро-нечіткого АФА Anfis на основі алгоритму Ванга-Менделя мінімуму комбінованого критерію ($C_{комб}$=0,055) відповідає мережа Anfis з Гаусовою функцією належності, і яка навчена гібридним алгоритмом (комбінація градієнтного спуску і МНК).

В результаті моделювання встановлено, що ГА виходить в область оптимальних рішень у середньому протягом перших п’яти поколінь. Його швидкодія склала у середньому 16 с на покоління.

Як похибки прогнозування використовувався критерій регулярності, значення якого для нейро-нечіткого АФА Anfis на основі алгоритму Сугено-Такагі склало – 0,0432, для АФА Anfis на основі алгоритму Такагі-Сугено-Канга – 0,0485, для АФА Anfis на основі алгоритму Ванга-Менделя – 0,0496.

Таким чином, найкращі результати з прогнозування мережевого трафіку (в сенсі критерію регулярності (2.4)) показав нейро-нечіткий АФА Anfis на основі алгоритму Сугено-Такагі, АФА Anfis на основі алгоритму Такагі-Сугено-Канга та алгоритму Ванга-Менделя показали приблизно однакові результати.

Адекватність отриманих нейро-нечітких АФА перевірялась за непараметричним критерієм знаків. Було встановлено, що для рівня значущості 0,01 досліджені нейро-нечіткі АФА з обґрунтованими параметрами адекватні експериментальним реалізаціям.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Запропоновано підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму. Отримані інтелектуальні прогнозуючі моделі можуть бути використані в засобах моніторингу, здатних аналізувати трафік мережі в режимі реального часу.

Метою даного розділу є обґрунтування економічної доцільності прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму. Досягнення цієї мети потребує виконання таких розрахунків, як:

– капітальні витрати 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 капітальних (фіксованих) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на прогнозування мережевого трафіку із використанням композиції адаптивних мереж нечіткого висновку та генетичного алгоритму визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму

Трудомісткість розробки підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму, $t_{тз}=17$;

$t_в$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо, $t_в=25$;

$t_м$ – тривалість моделювання розробленого підходу щодо прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму, $t_м=30$;

$t_р$ – тривалість розробки підходу щодо прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму, $t_м=60$;

$t_д$ – тривалість підготовки технічної документації, $t_д=10$.

Отже,

$$t = t_{тз}+ t_в+ t_м+ t_р+ t_д = 17+25+30+60+10= 142 \text{ години.}$$

Розрахунок витрат на розробку підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму

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 $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 26412+1089,14 = 27501,14 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 142*186 = 26412 \text{ грн.}$$

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:

$$З_{мч} = t*С_{мч}=142*7,67=1089,14 \text{ грн.}$$

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:

$$С_{мч} = 0,8 \cdot 4 \cdot 1,68 + \frac{9100 \cdot 0,3}{1920} + \frac{8400 \cdot 0,2}{1920} = 7,67 \text{ грн.}$$

Для реалізації запропонованого підходу може бути використано стандартне апаратне забезпечення, яке вже наявне на підприємстві, тому капітальні витрати не виникають.

Оцінка ефективності запропонованого підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму проведена шляхом моделювання в середовищі Matlab / Simulink. При цьому використовувалась безкоштовна навчальна версія пакета прикладних програм Matlab&Simulink, тому додаткові капітальні витрати не виникають.

Витрати на налагодження системи інформаційної безпеки становитимуть 1500 грн.

Вирішення певних технічних завдань із прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму потребує залучення аутсорсингових організації, вартість послуг котрих складає 12000 грн.

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

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

$$= 27501{,}14+12000+1500 = 41001{,}14 \text{ грн.}$$

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.

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

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

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 ($С_{ак} = 0$ грн.).

Середовище Matlab/Simulink, яке застосовується для оцінки ефективності запропонованого підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму, вже використовується на підприємстві, тому додаткові витрати щодо відновлення й модернізації системи не виникають.

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 16500 грн. Додаткова заробітна плата – 5% від основної заробітної плати.

Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,2 ставки.

Отже,

$$С_з = (16500*12 + 16500*12*0,05)*0,2= 41580 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2022 р. складає 22%.

$$С_{св} = 41580*0,22 = 9147,6 \text{ грн.}$$

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:

$$С_{ел} = 0,9*1920*1,68 = 2903,04 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 41001,14*0,02 = 820,02 грн).

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

$$С_к = 8000+41580+9147,6+2903,04 +820,02 = 62450,66 \text{ грн.}$$

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 26%. Тому, отримуємо:

$$С_{ак}= 41001,14*0,26=10660,30 \text{ грн.}$$

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

$$С = 62450,66 + 10660,30 = 73110,96 \text{ грн.}$$

3.3 Оцінка можливого збитку

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

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 16200 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15100 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 13 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 240 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 2000 грн.;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 25.

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:

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{15100 \cdot 13}{176} \cdot 4 = 4461{,}36 \text{ грн},$$

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 $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{15100 \cdot 13}{176} \cdot 6 = 6692{,}05 \text{ грн.}$$

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

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_в = \frac{16200 \cdot 1}{176} \cdot 2 = 184{,}09 \text{ грн.}$$

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

$$П_в = 6692{,}05+184{,}09+2000 = 8876{,}14 \text{ грн.}$$

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

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{240000}{2080} \cdot (4+2+6) = 1384{,}62 \text{ грн.}$$

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.

$$U = 4461{,}36+8876{,}14+1384{,}62 = 14722{,}12 \text{ грн.}$$

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

$$B = \sum_i \sum_п U = \sum_1 \sum_{25} 14722{,}12 = 368053 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації загрози (25%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки, отже було розраховано:

$$E = 368053*0,25 - 73110,96 = 18902,29 \text{ грн.}$$

3.5 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:

$$ROSI=18902,29 / 41001,14 = 0,46 \text{ частки одиниці}$$

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, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,46 > (6 – 5)/100 = 0,46 > 0,01.$$

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI}$$

$$T_0 = 1 / 0,23 = 2,17 \text{ років.}$$

3.6 Висновок

Отже, згідно з наведеними розрахунками можливо зробити висновок, що обґрунтування підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму є економічно доцільним.

Капітальні витрати, які складають 41001,14 грн, дозволяють отримати ефект величиною 18902,29 грн. Відповідно до отриманих значень показників економічної ефективності можна зазначити, що такий підхід дозволить отримувати 0,46 економічного ефекту на 1 грн. капітальних витрат (коефіцієнт повернення інвестицій ROSI складає 0,46 грн.). Термін окупності при цьому складатиме 2,17 років.

Величина економічного ефекту визначатиметься також розміром компанії, величиною вартості нематеріальних активів (об’єктів прав

інтелектуальної власності) та кількістю об’єктів прав інтелектуальної власності, право на авторство яких може бути порушеним.

ВИСНОВКИ

Основні результати кваліфікаційної роботи полягають у наступному:

1. Встановлено, що одним із рішень актуальної задачі захисту ІКМ від кібератак є розробка та вдосконалення СВА, головне завдання яких полягає у виявленні мережевих атак, спроб несанкціонованого доступу і використання ресурсів мережі. Одним із напрямків протидії вторгнень є виявлення аномалій; при цьому даними для аналізу є мережевий трафік, представлений як інтенсивність (швидкість) передачі даних або набір мережевих пакетів, в загальному випадку фрагментованих на рівні IP. Для визначення шаблону нормальної поведінки перспективним є використання моделей захисту на основі розпізнавання аномалій в ІКМ, оскільки поточний трафік є реалізацією випадкового процесу, а його адекватна модель – статистично стійка закономірність цього процесу. Оцінка характеристик мережевого трафіку необхідна для побудови його адекватної моделі, що дозволяє сформувати еталонну модель (шаблон) «нормального» трафіку і за нею виявляти аномалії трафіку в СВА. При цьому прогнозування трафіку дозволяє підвищити оперативність виявлення атак.

2. З розвитком інформаційних технологій особливо актуальною стала проблема обробки великих даних. Безліч параметрів для виявлення мережевих атак становить значний обсяг даних, що визначає можливість їх обробки саме методами ІАД. Встановлено, що протидіяти вторгненням і атакам основуючись тільки на одному з таких методів малоефективно, тому рекомендовано будувати систему протидії вторгненням, засновану на декількох методах штучного інтелекту.

Для вирішення задачі прогнозування мережевого трафіку найбільш актуальним є використання нейронних мереж та систем з нечіткою логікою, які є універсальними ефективними апроксиматорами, а побудовані на їх основі фільтри ефективні для прогнозування та апроксимації нелінійних, стохастичних

процесів. Для усунення недоліків НМ і систем з нечіткою логікою запропоновані гібридні нейро-нечіткі мережі Anfis.

3. Запропоновано підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму, який полягає у використанні глобальної оптимізації (ГА) для вибору параметрів нейро-нечітких АФА Anfis (на основі алгоритму Сугено-Такагі, алгоритму Такагі-Сугено-Канга та Ванга-Менделя). Параметри АФА, які налаштовувались ГА: функція належності нечіткого правила l входу k; та метод параметричної оптимізації (функція навчання мережі Anfis).

4. Оцінка ефективності запропонованого підходу до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму виконувалась в середовищі Matlab за допомогою стандартних і розроблених програм. На прикладі експериментальних даних – трафіку, що передається через мережу Інтернет оцінено ефективність та адекватність отриманих нейро-нечітких адаптивних фільтрів-апроксиматорів.

ПЕРЕЛІК ПОСИЛАНЬ

1. 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.

2. Павлов І.М. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем / І.М. Павлов, С.В. Толюпа, В.І. Ніщенко // Сучасний захист інформації. – №4. – 2014. – С. 44-52.

3. 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.

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. Толюпа С.В. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. / С.В. Толюпа, С.С. Штаненко, Г. Берестовенко // Збірник наукових праць Військового інституту телекомунікацій та інформатизації ім. Героїв Крут. – № 3. – 2018. – С. 56-66.

7. 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.

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

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

10. Бекетова Г., Ахметов Б., Корченко А., Лахно В. Разработка модели интеллектуального распознавания аномалій и кибератак с использованием логических процедур, базирующихся на покрытиях матриц признаков // Ukrainian Scientific Journal of Information Security. – 2016. – Vol. 22, issue 3. – P. 242-254.

11. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах / Т.І. Зоріна // Вісник східноукраїнського національного університету ім. В. Даля. – № 15 (204), ч.1. – 2013. – С. 48-54.

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

13. 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.

14. Nelles O. Nonlinear System Identification: From Classical Approaches to Neural and Fuzzy Models / O. Nelles. – Berlin: Springer, 2001. – 785 pp.

15. 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.

16. 10 викликів кібербезпеки: до чого готуватися користувачам та компаніям. [Електронний ресурс]. – Режим доступу: https://eset.ua/ua/news/view/993/10-vyzovov-kiberbezopasnosti-k-chemu-gotovitsya-polzovatelyam-i-kompaniyam.

17. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [Електронний ресурс]. – Режим доступу: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

18. (ISC)^2 CYBERSECURITY WORKFORCE STUDY [Електронний ресурс]. – Режим доступу: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.

19. Радченко М.М. Аналіз системи виявлення вторгнень та комп'ютерних атак / М.М. Радченко, О.І. Іванов, С.І. Прохорський, К.К. Мужеський // Міждисциплінарні дослідження в науці та освіті, 2013. – 379 с.

20. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко / Підручник МОН України. – К.: Видавництво DIRECTLINE, 2009. – 714 с.

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.

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. Ghorbani A.A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention: Concepts and Techniques // Springer Science & Business Media. – 2009. – 212 p.

27. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. – 2014. – Vol. 5. no. 4. – P. 29–64.

28. Gyanchandani M., Rana J.L., Yadav R.N. Taxonomy of Anomaly Based Intrusion Detection System: A Review // International Journal of Scientific and Research Publications. – 2012. – Vol. 2. Issue 12. – P. 1-13.

29. Нейрокомпьютеры и интеллектуальные роботы / Под ред. Н. М. Амосова. – Киев.: Наукова думка, 1991. – 412 с.

30. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А. П. Ротштейн. – Винница: «УНІВЕРСУМ-Вінниця», 1999. – 320 с.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. Levonevskiy D.K. Network attacks detection using fuzzy logic / D.K. Levonevskiy, R.R. Fatkieva, S.R. Ryzhkov. Global Journal of Computer Science and Information Technology Research. Framingham : Global Journals Inc. – 2015. – P. 243-244.

38. 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.

39. Zitzler E. Evolutionary Multiobjective Optimization / E. Zitzler // Handbook of Natural Computing. – Springer-Verlag Berlin Heidelberg, 2012. – P. 871-904.

40. 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.

41. 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.

42. 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.

43. 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.

44. Ivakhnenko A.G. Inductive learning algorithms for complex systems modeling / A.G. Ivakhnenko, H.R. Madala – London, Tokyo: CRC Press, 1994. – 384 p.

45. Архів трафіку. [Електронний ресурс]. – Режим доступу: http://ita.ee.lbl.gov.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	44	
6	А4	Спеціальна частина	10	
7	А4	Економічний розділ	11	
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 Трубка.ppt

2 Диплом Трубка.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 студента групи 125м-21-1 Трубки Д.А.

на тему: «Нейро-нечітке прогнозування трафіку інформаційно-комунікаційних мереж для систем виявлення атак»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 88 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на дослідження та обґрунтування нейро-нечітких адаптивних фільтрів-апроксиматорів для прогнозування мережевого трафіку для виявлення його аномалій при використанні в системах виявлення та запобігання атак.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів побудови сучасних систем виявлення та запобігання атак, а також методів інтелектуального аналізу даних (гібридних нейро-нечітких мереж та генетичних алгоритмів) в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до прогнозування мережевого трафіку із використанням адаптивних мереж нечіткого висновку та генетичного алгоритму та шляхом моделювання оцінено його ефективність.

Наукова новизна результатів полягає у тому, що було запропоновано проводити прогнозування мережевого трафіку із використанням нейро-нечітких адаптивних фільтрів-апроксиматорів Anfis, параметри яких було оптимізовано за допомогою генетичного алгоритму.

Практична цінність роботи полягає в тому, що отримані нейро-нечіткі адаптивні фільтри-апроксиматори Anfis на основі алгоритмів Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя можуть бути використані в засобах моніторингу, здатних аналізувати трафік мережі в режимі реального часу.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Трубка Д.А. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

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