ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Підвищення ефективності системи інформаційної безпеки інформаційно-комунікаційної мережі на основі нейроструктурних технологій»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Володимир НЕТЬОСА

Виконав: здобувач вищої освіти групи СЗДМ 61
Володимир НЕТЬОСА

Керівник: _____ПОНОЧОВНИЙ Петро_____
доктор філософії (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Нетьосі Володимиру Ігоровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Підвищення ефективності системи інформаційної безпеки інформаційно-комунікаційної мережі на основі нейроструктурних технологій»
керівник кваліфікаційної роботи ПОНОЧОВНИЙ Петро, доктор філософії
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: телекомунікаційна мережа об'єкту інформаційної діяльності, система управління інформаційною безпекою, нейроструктурні технологій.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
4.1. Огляд системи оцінки якості функціонування інформаційно-комунікаційної мережі об'єкту інформаційної діяльності.
4.2. Дослідження напрямки удосконалення системи управління інформаційною безпекою інформаційно-комунікаційної мережі з використанням нейроструктурних технологій.
4.3. Розробка концептуальної моделі управління інформаційною безпекою інформаційно-комунікаційної мережі на основі нейроструктурних технологій.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах.

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Володимир НЕТЬОСА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Петро ПОНОЧОВНИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 78 сторінки, має 12 рисунків, 2 таблиці. Список використаних джерел містить 38 найменувань і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності системи інформаційної безпеки інформаційно-комунікаційної мережі на основі нейроструктурних технологій

В кваліфікаційній роботі проведено аналіз систем оцінки якості функціонування телекомунікаційних мереж. Досліджено напрямки удосконалення системи управління інформаційною безпекою інформаційно-комунікаційної мережі з використанням нейроструктурних технологій. Розроблено концептуальну модель управління інформаційною безпекою інформаційно-комунікаційної мережі на основі нейроструктурних технологій.

Апробація:

О.А. Турчин, В.І. Нетьоса, Є.О. Кравченко, Способи, методи та переваги функціонування системи захисту мережевих каналів передачі інформації на основі технологій штучного інтелекту. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.39-40. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, НЕСАНКЦІОНОВАНИЙ ДОСТУП ДО ІНФОРМАЦІЇ

ABSTRACT

The qualification work consists of an introduction, three sections, general conclusions, a list of sources used, the total volume of the work is 81 pages, has 12 figures, 2 tables. The list of sources used contains 38 items and takes up 3 pages.

The purpose of the qualification work is to increase the efficiency of the information security system of the information and communication network based on neurostructural technologies

The qualification work analyzes the systems for assessing the quality of functioning of telecommunication networks. The directions of improving the information security management system of the telecommunication network using neurostructural technologies are investigated. A conceptual model of information security management of the telecommunication network based on neurostructural technologies is developed.

Approbation:

O.A. Turchyn, V.I. Netyosa, E.O. Kravchenko, Methods, methods and advantages of functioning of the system for protecting network channels of information transmission based on artificial intelligence technologies. All-Ukrainian Scientific and Practical Conference: Current Problems of Security of Information and Telecommunications Systems. Kyiv, November 5, 2025, Kyiv: DUIKT Research Center. – 2025. P.41-42. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: TELECOMMUNICATION NETWORK, INFORMATION SECURITY MANAGEMENT SYSTEM, UNAUTHORIZED ACCESS TO INFORMATION

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІзОД	–	Інформація з обмеженим доступом
ОКІ	–	Об’єкт критичної інфраструктури
СТЗІ	–	Система технічного захисту інформації
ТКВІ	–	Технічний канал витоку інформації
ОТЗС	–	Основні технічні засоби і системи
ТЗПІ	–	Технічний засіб перетворення інформації
ДТЗС	–	Допоміжні технічні засоби системи
ПЕМВ	–	Побічні електромагнітні випромінювання
ТЗОС	–	Технічні засоби охоронної сигналізації

ВСТУП

В умовах глобалізації та сучасного розвитку інформаційних технологій і розвитку мереж передачі даних зв'язку, однією з найважливіших відповідальностей є управління безпекою телекомунікаційних даних під час передачі важливої інформації. Попит на надійні, високоякісні системи, які можна використовувати для управління інформаційною безпекою телекомунікаційних мереж, надихає людей на пошук нових ефективних рішень. Нещодавно нейромережеві технології продемонстрували свою ефективність, виходячи з концепції, що нервові клітини в живому організмі функціонують подібно до мозку. Це призвело до ситуацій, коли додаткові вдосконалення системи інформаційної безпеки можуть бути досягнуті за допомогою нейромережевих технологій.

Метою кваліфікаційної роботи є удосконалення системи управління інформаційною безпекою інформаційно-комунікаційної мережі на основі нейроструктурних технологій.

У процесі підготовки кваліфікаційної роботи були вирішено наступні задачі:

– проведено аналіз систем оцінки якості функціонування інформаційно-комунікаційної мережі;

– досліджено напрямки удосконалення системи управління інформаційною безпекою інформаційно-комунікаційної мережі з використанням нейроструктурних технологій;

– розроблено концептуальну модель управління інформаційною безпекою інформаційно-комунікаційної мережі на основі нейроструктурних технологій.

Об’єкт дослідження. Система інформаційною безпеки інформаційно-комунікаційної мережі.

Предмет дослідження. Система управління інформаційною безпекою інформаційно-комунікаційної мережі.

Розділ 1

РОЗДІЛ 1 АНАЛІЗ СИСТЕМ ОЦІНКИ ЯКОСТІ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1. Огляд стану, перспектив і тенденцій розвитку телекомунікаційних мереж

На сучасному етапі розвитку інформаційних технологій телекомунікаційна мережа вважається сукупністю технічних засобів та споруд, призначених для зв'язку, комутації, передачі та прийому будь-якого виду сигналу, включаючи письмові слова, зображення та звуки або повідомлення. Ці системи призначені для використання в комунікації з іншими комп'ютерами, телефонами та персональними комп'ютерами. Обладнання використовується для обробки, концентрації, зберігання інформації та перетворення інформації в цифрові дані та навпаки. Сучасні телекомунікаційні мережі та технології для загального зв'язку загалом швидко розвиваються: з'являються нові рішення, збільшується база технологічних елементів, вносяться різні модифікації тощо. Як правило, телекомунікаційні мережі класифікуються за кількома різними ознаками. Найчастіше використовуються такі типи категоризації [1]:

За площею:

• Локальна обчислювальна мережа (LAN) - зазвичай розташована в будівлі.

• Широкомасштабна мережа (WAN) - охоплює географічну область (країну або континент).

• Метропольна мережа (MAN) - використовується для об'єднання мереж у місті в єдину велику мережу.

Інтернет складається з окремих комп'ютерів, підключених до інших мереж у світі через загальнодоступну мережу (загальнодоступну мережу).

• Інтранет – персональні комп'ютери підключені до інших мереж через приватну мережу.

• Віртуальна приватна мережа (VPN) – окремі комп'ютери підключені до інших мереж через частину загальнодоступної мережі.

За способом підключення (топологія):

Точка-точка (просторово явний або логічний).

• Кільцевий (фактичний або потенційний).

• Шина (хімічна).

• Пропускна здатність (інтуїтивна).

• Сітчастий (просторовий або логічний).

• Переданий або підключений через концентратори (реальний або логічний).

За засобами зв'язку:

• режим точка-точка: кожна пара вузлів має пряме з'єднання; це з'єднання не використовується іншими вузлами;

• комутований режим: у прямій мережі кількість необхідних з'єднань зменшується за допомогою комутаторів;

• багатоточковий (широкомовний) режим: усіма учасниками мережі використовується спільний протокол зв'язку.

Пропускна здатність:

Низька швидкість: швидкості від кбіт/с до Мбіт/с.

• швидкий: зі швидкістю до Гбіт/с.

Усі комунікаційні мережі складаються з п'яти основних компонентів, які присутні в кожному мережевому середовищі, незалежно від призначення чи типу. Ці складові компоненти включають: термінали, комунікаційні процесори, комунікаційні канали, комп'ютери та програмне забезпечення для керування комунікаціями. Термінали є початковою та кінцевою точкою будь-якої інформаційно-комунікаційної мережі. Будь-який пристрій, який передає або приймає дані, можна вважати термінальним компонентом. Телекомунікаційні процесори сприяють передачі та прийому інформації між комп'ютерами та терміналами, забезпечуючи різні елементи керування та додаткові функції (наприклад, перетворення цифрового сигналу в аналоговий і навпаки).

Комунікаційні канали є протокою для передачі та прийому даних. Формуються канали зв'язку через телекомунікаційні середовища, найпоширенішими з яких є мідні труби та коаксіальний кабель (СК). Оптоволоконний кабель стає все більш популярним завдяки своїм швидшим та надійнішим комунікаційним властивостям, як для бізнесу, так і для особистого використання. У телекомунікаційному середовищі комп'ютери з'єднуються через фізичні носії для виконання своїх комунікаційних обов'язків. Програмне забезпечення для керування комунікаціями є спільним для всіх комп'ютерів у мережі та відповідає за регулювання активності та функціональності мережі. Зазвичай кожна ідея комунікаційної мережі має три компоненти, або площини (різних рівнів, оскільки їх можна вважати частиною складнішої мережі) [1]:

Площина керування містить інформацію, яка використовується для керування транспортним засобом (також називається сигналізацією).

Площина даних, площина користувача або площина носія відповідає за передачу мережевого трафіку між користувачами.

• Управління трафіком здійснюється на операційній площині.

Нещодавня спостережувана тенденція конвергенції в різних типах мереж є специфічною не лише для локальних та глобальних комп'ютерних мереж, але й для телекомунікаційних мереж інших типів.

Найпопулярнішими телекомунікаційними мережами сьогодні є:

• телекомунікаційні мережі;

Радіомережа складається з:

• кабельного телебачення;

• комп'ютерних мереж

У всіх цих мережах ресурсом, що надається клієнтам, є інформація.

Табл.1.1

Початковий розподіл виду послуг і форми подання інформації в мережах різного типу.

Вид телекомунікаційної мережі	Вид послуг	Вид представленої інформації
Телефонні мережі	Інтерактивні послуги	Тільки голосова
Радіомережі	Широкомовні послуги	Тільки голосова
Телевізійні мережі	Широкомовні послуги	Голос і зображення
Комп'ютерні мережі		Алфавітно-цифрова інформація

Телефонні мережі сприяють взаємодії, оскільки два учасники розмови (або кілька учасників, якщо це конференція) по черзі займаються діяльністю. Радіомережі та телевізійні мережі надають телевізійні послуги, тоді як інформація передається лише в одному напрямку – від мережі до абонентів, дотримуючись протоколу «один до багатьох» (точка-багатоточка). Сьогодні в багатьох випадках відбувається зустріч різних різновидів телекомунікаційних мереж.

Незважаючи на визнані відмінності між комп'ютерами, телефонами, телевізорами та первинними мережами, всі ці мережі мають подібний склад на високому рівні абстракції. Комунікаційна мережа, що базується на телекомунікаціях (рис. 1.1), зазвичай складається з таких компонентів:

Мережа доступу – призначена для фокусування інформаційних потоків від користувацького обладнання на кількох шляхах зв'язку в обмеженій кількості вузлів магістральної мережі;

Основна мережа відповідає за з'єднання окремих мереж доступу, вона забезпечує передачу трафіку з однієї мережі до іншої через швидкі канали.

Інформаційні центри або центри управління послугами (центри обробки даних або пункти обслуговування) – це власні інформаційні активи мережі, на яких базуються користувацькі послуги.

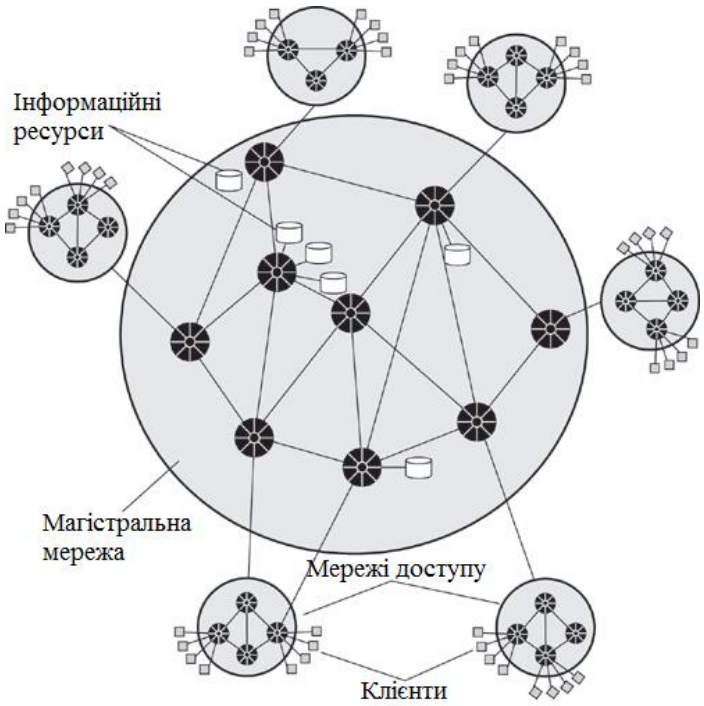


Рис. 1.1 Структура інформаційно-комунікаційної мережі

Мережа, що забезпечує доступ, і магістральна мережа побудовані навколо комутаторів. Кожен комутатор має певну кількість каналів зв'язку, які з ним пов'язані, і ці канали використовуються для зв'язку з іншими комутаторами.

Мережа, що забезпечує доступ, є нижчою частиною ієрархії інформаційно-комунікаційної мережі. Кінцеві (термінальні) вузли пов'язані з цією мережею - пристрої встановлені у користувачів (абонентів, клієнтів) мережі. У випадку комп'ютерної мережі термінальними вузлами є комп'ютери, телефони та телевізійні або радіомережі, відповідні теле- та радіоприймачі. Основною метою мережі доступу є централізація інформаційних потоків від кількох джерел зв'язку в невеликій кількості вузлів магістральної мережі. Мережа, що отримує доступ до інформації, як і телекомунікаційна мережа в цілому, може мати кілька рівнів (на рисунку показано два). Комутатори, розташовані в каналах нижчого рівня, мультиплексують інформацію, яка надходить по кількох абонентських каналах (часто їх називають абонентськими завершеннями, локальним контуром), і передають її комутаторам вищого рівня, щоб потім інформація передавалась до магістральних комутаторів. Кількість шарів мережі доступу залежить від її розміру; Мала мережа доступу може мати лише один рівень, тоді

як велика може мати два або три рівні. Наступні рівні зосереджені на додатковій концентрації трафіку, його зборі та об'єднанні в швидші канали. Через магістральну мережу окремі мережі доступу об'єднуються, що дозволяє передавати трафік між ними на високих швидкостях по каналах. Магістральні комутатори також можуть використовуватися для керування інформаційними потоками між кількома особами, а також потоками, які агрегуються, і дані передаються з великої кількості окремих з'єднань. Таким чином, інформація транспортується через магістральну мережу до мережі приймача, там розділяється, а потім передається на вхідний порт обладнання користувача.

У випадку, якщо абонент-отримувач підключений до того ж комутатора доступу, що й абонент-відправник (безпосередньо або через комутатори, що знаходяться нижче ієрархії з'єднань), останній незалежний від першого та самостійно виконує необхідну операцію переходу [1].

Інформаційні центри / центри управління послугами – це інформаційні ресурси мережі, з яких надаються послуги користувачам. Ці центри можуть зберігати як загальну, так і специфічну інформацію.

• специфічна інформація, що стосується користувача, тобто дані, що безпосередньо цікавлять окремих користувачів мережі.

• додаткова сервісна інформація, яка дозволяє користувачам брати участь у певних заходах.

Прикладом інформаційних ресурсів першого типу є веб-портали, які містять різні короткі повідомлення, інформацію з електронних магазинів тощо. У телефонних мережах роль цих центрів делегується службам екстреної допомоги (наприклад, поліції, швидкій допомозі) та іншим довідковим службам, пов'язаним з різними організаціями та підприємствами – станціями, аеропортами, магазинами тощо. У телевізійних мережах ці студії присвячені наданню телевізійних програм, що відображають «живий» досвід роботи центру. До ресурсів другого типу належать, наприклад, різні системи автентифікації та авторизації, які використовуються організацією для перевірки легітимності облікових записів користувачів, ці системи також допомагають організації у

перевірці правильності мережевої інформації. Крім того, білінгові системи, які розраховують вартість послуг у комерційній мережі, а також інформація про користувачів, яка зберігається в базі даних, обидві ці системи допомагають організації у перевірці легітимності користувачів. У телефонних мережах існують сервісні центри, що контролюють послуги (Services Control Point, SCP). Ці центри – комп'ютери, що зберігають програми, нестандартні для обробки дзвінків користувачів, наприклад, дзвінки до безкоштовних довідкових служб бізнес- чи розважальних компаній (так звані служби 800) або дзвінки під час телевізійних програм. Іншим поширеним типом допоміжних інформаційних центрів є централізована система управління мережею, яка являє собою програмний додаток, що працює на одному або кількох комп'ютерах.

Кожен тип мережі має кілька атрибутів, але їх загальна структура зазвичай описана вище. Крім того, залежно від призначення та розміру мережі, деякі частини узагальненої структури можуть бути відсутніми або мати незначне значення. Наприклад, у невеликій локальній комп'ютерній мережі мережі доступу та магістральні мережі чітко не визначені, вони натомість зливаються в загальну, просту структуру. У корпоративній мережі типова ситуація – відсутність системи виставлення рахунків, оскільки послуги співробітникам надаються на нефінансовій основі. У деяких телефонних мережах інформаційних центрів може не існувати, а в телевізійних мережах мережа доступу є розподільчою мережею, оскільки інформація в ній поширюється лише в один напрямок – від мережі до абонентів.

Як наслідок, сучасний стан телекомунікаційних мереж можна охарактеризувати як такий, що рухається до досконалості. Незрозуміло, як вони виглядатимуть у майбутньому, скільки поколінь технологій та мережевого проектування потрібно буде передати. Однак перші кроки до цих розробок вже очевидні: потужні пакети передачі та універсальні мережі, що є високошвидкісними, технології оптичного зв'язку, характерні для наступного покоління телекомунікаційних мереж.

1.2. Проблема оцінювання параметрів якості функціонування телекомунікаційних мереж.

Сьогодні інформація передається в сучасних мережах через різні сигнальні системи, що використовують різні протоколи "носіїв". Основна функція кожного типу сигналу полягає в забезпеченні необхідної якості роботи, основні компоненти якої описані наступним чином:

Показники здатності мережі передавати інформацію.

Показники надійності системи передачі даних;

Враховуються часові показники доставки інформації, а також показники ступеня точності інформації.

Показники ефективності мережі;

Показники вартості розповсюдження інформації.

Цей список не є повним, але він відображає основні показники якості передачі даних. Сьогодні стали очевидними значні проблеми щодо основних показників якості для різних послуг та мереж передачі даних. Для того, щоб користувач міг користуватися якісними послугами, такими як голосовий зв'язок, текстові повідомлення, електронна пошта та соціальні мережі, сигнал повинен проходити мережу певним чином. Найважливішими показниками є час, необхідний для встановлення з'єднання, надіслане повідомлення, кількість завершених з'єднань, максимальна швидкість передачі даних тощо. Ще одним критичним елементом є структура мережі, яка постійно розвивається та вдосконалюється. Як наслідок, важливо визначати показники якості як з точки зору системи та мережі, так і з точки зору користувача. Для стільникових мереж швидкість передачі даних зменшується зі збільшенням кількості користувачів. Співвідношення сигнал/шум на вході мобільного телефону має велике значення. Наприклад, обговоримо послугу передачі даних мережі UMTS. Найбільш вразливим місцем щодо якості мережі є «радіочастоти» системи UMTS – система UTRAN (через обмежений характер її ресурсів). Якість послуг, що пропонуються в мережі UMTS, залежить від вищезазначених характеристик,

включаючи потужність випромінювання, навантаження мережі тощо. Для забезпечення високої якості роботи мережі необхідно визначити параметри радіоресурсу, наприклад, запас стійкості до перешкод або реакцію на швидке згасання. У мережах IMT-MC-450 важливими показниками є максимальна та середня швидкість передачі даних, час затримки або доставки інформації, відсоток втрачених або пошкоджених пакетів, помилки в каналі передачі або перевантаження. На цей момент створено обидва основні показники якості обслуговування дзвінків, а також стандарти для цих показників (нормативний документ, що описує галузь зв'язку України КНД 45-067-97) [5]. Розглянувши документ та вищезазначену інформацію, можна зробити висновок, що ідентифікація 15 різних часових властивостей мережі має вирішальне значення для оцінки якості обслуговування та якості функціонування телекомунікаційних мереж. На основі цієї інформації можна зробити висновок, що необхідною умовою успішної роботи мережі зв'язку є забезпечення її ефективного та надійного управління. Для передачі керуючої інформації в сучасному зв'язку використовується кілька різних систем сигналізації. Для забезпечення певного ступеня якості мережі розглядаються основні показники, що описують якість роботи мережі та причини цих наслідків.

1.3. Принципи побудови системи характеристик якості телекомунікаційних мереж

Процес визначення якості телекомунікаційних послуг (QoS) та продуктивності мереж (NP) повинен враховувати кореляцію між якістю інформаційно-комунікаційної послуги та властивостями мережі. Для цього визначаються місця вимірювання якості телекомунікаційних послуг та властивостей мережі [6].

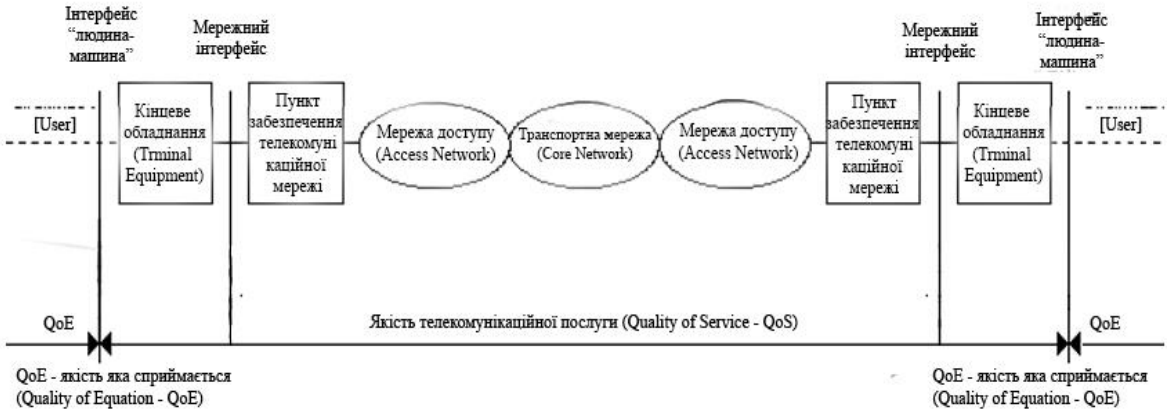


Рис. 1.2 Точки вимірювання параметрів якості телекомунікаційної послуги і характеристик мережі

Визначення показників якості інформаційно-комунікаційної послуги на основі отриманих значень параметрів рекомендується проводити в точках доступу до інформаційно-комунікаційної послуги, а не на інтерфейсі «людина-машина» будь-яких мережевих процесів, що надають послугу.

Телекомунікаційні мережі слугують засобом розповсюдження інформації споживачам. Розповсюдження інформації та надання послуг зв'язку забезпечується певним набором типів з'єднань, що реалізуються мережею. Атрибути типів з'єднань впливають на властивості інформаційно-комунікаційної мережі. Як результат, кожну телекомунікаційну послугу можна охарактеризувати набором показників якості на основі атрибутів, що описують специфіку інформаційно-комунікаційної мережі.

Процес визначення властивостей мережі рекомендується, оскільки він передбачає ідентифікацію подій та станів, які можна спостерігати на інтерфейсі технічних телекомунікацій або на межі з'єднання між технічними та звичайними засобами.

Для визначення ефективності послуг споживачам важливо розуміти існуючі взаємозв'язки між показниками якості телекомунікаційних послуг та атрибутами мережі, враховуючи різні підходи до цього.

Табл. 1.2

Основні відмінності в підходах до визначення показників якості телекомунікаційних послуг

Якість, яка сприймається (QoE)	Якість телекомунікаційної послуги (QoS)	Характеристики мережі (NP)
Орієнтовані на споживача телекомунікаційної послуги	Орієнтовані на оператора телекомунікацій	
Описується параметрами (атрибутами) ставлення споживача	Описується параметрами (атрибутами) послуги	Описуються параметрами (атрибутами) елементу з'єднання
Орієнтовано на ефект, що очікується споживачем	Орієнтовано на ефект, що сприймається споживачем	Орієнтовані на розробку, проектування, експлуатацію і технічне обслуговування
Визначається споживачем	Вимірюється між точками (у точках) доступу до послуги	Описують можливості елементів з'єднання або наскрізних з'єднань

Щоб визначити, які показники та стандарти якості необхідні для телекомунікаційних послуг, слід використовувати системний підхід відповідно до документа ETSI ETR 003 [9].

Основні принципи системного підходу вимагають, щоб усі аспекти якості телекомунікаційних послуг оцінювалися з точки зору як споживача, так і виробника (оператора телекомунікацій), а також наявності механізму координації суб'єктивних оцінок споживачів з оцінками оператора для досягнення якості послуг, яка задовольняє споживачів.

Спільний (базовий) рівень необхідності показників якості телекомунікаційних послуг такий:

Вимоги та вимоги споживача щодо якості телекомунікаційних послуг.

Якість телекомунікаційних послуг, що надаються оператором, постачальником або виробником, визначається типом послуги.

Рівень телекомунікаційних послуг, який може надаватися оператором телекомунікацій або визначається типом інформаційно-комунікаційної послуги (оцінка «зверху»).

Якість телекомунікаційних послуг, за яку споживач готовий платити.

Зв'язок між різними методами визначення якості телекомунікаційних послуг з боку споживача, постачальника послуг (провайдера) та оператора телекомунікацій, а також спосіб взаємодії учасників під час процесу оцінювання, все це враховується для створення більш точної картини якості послуги.

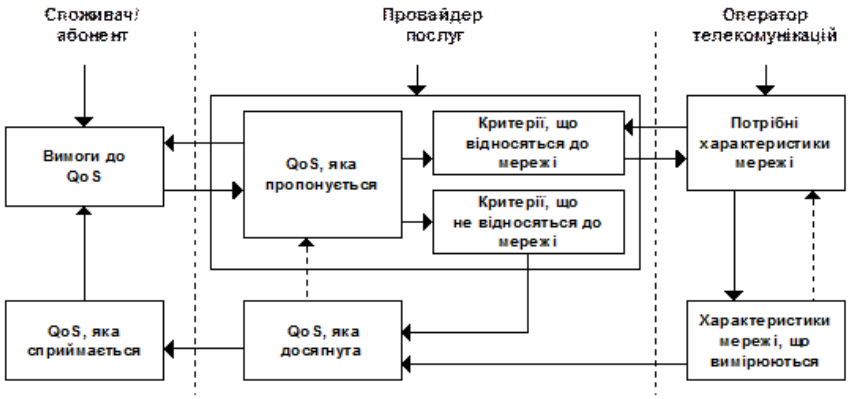


Рис. 1.3 Схема взаємодії при забезпеченні якості телекомунікаційних послуг

Згідно зі схемою, особами, залученими до процесу визначення необхідних характеристик якості телекомунікаційних послуг, є споживачі та виробники цих послуг: постачальники та оператори телекомунікацій. Для покращення якості обслуговування споживачів протягом усього процесу надання телекомунікаційних послуг відповідно до вимог рекомендується дотримуватися підходу за схемою, зображеною на рисунку 1.4.

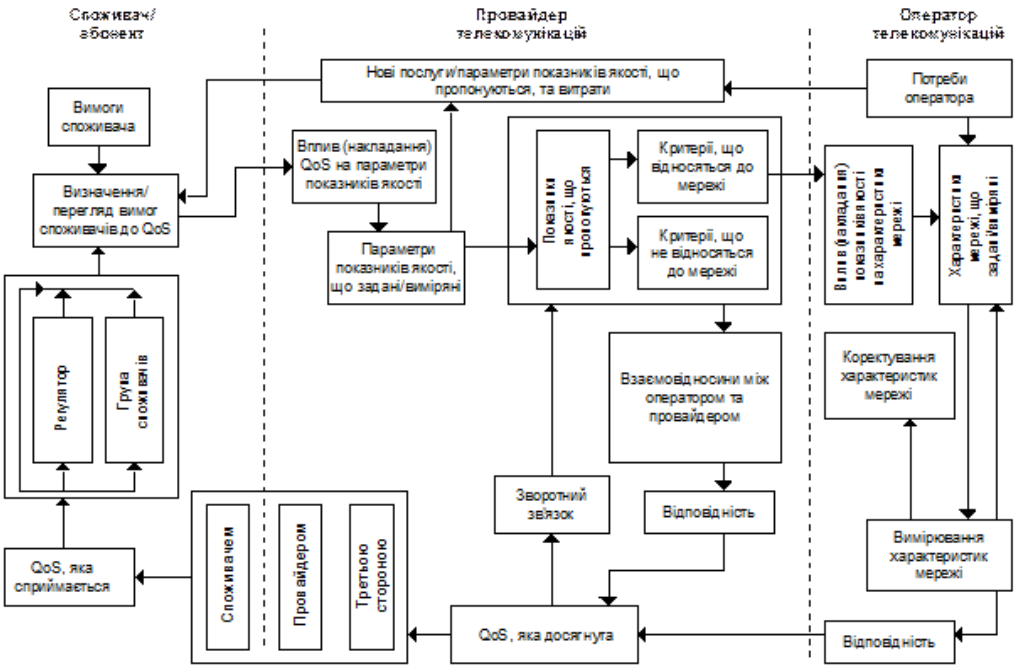


Рис. 1.4 Схема реалізація підходу при управлінні якістю обслуговування споживачів на всіх етапах надання телекомунікаційних послуг

Згідно зі схемою, першим кроком у розробці системи показників та визначенні необхідних характеристик якості телекомунікаційних послуг є: збір, вивчення та систематизація запитів споживачів. Споживач, як правило, бере участь у визначенні вимог до окремих послуг зв'язку та оцінює ефективність результатів. З точки зору споживача, якість інформаційно-комунікаційної послуги визначається, перш за все, її характеристиками:

Вони більше стурбовані споживачем, ніж функціонуванням мережі.

Не залежать від специфіки технології мережі.

– розглядають усі можливі телекомунікаційні послуги з точки зору споживача;

Можуть бути гарантовані споживачам операторами та постачальниками телекомунікаційних послуг, які мають з ними договір. Ці постачальники несуть відповідальність за надання послуг та підтримку рівня якості (SLA).

Параметри якості послуг зв'язку, пов'язані з властивостями мережі зв'язку, слід розуміти як характеристики якості роботи мережі, її компонентів та визначати відповідно до вимог щодо забезпечення бажаної якості послуг зв'язку.

Вони не обов'язково повинні бути зрозумілими споживачем і не потребують детального опису як способів визначення якості телекомунікаційних послуг. Однак, при описі характеристик інформаційно-комунікаційної послуги враховуються значення, пов'язані з усією телекомунікаційною мережею в цілому (наприклад, втрата зв'язку в мережі від початку до кінця).

1.5. Висновки по розділу

Створення успішної системи інформаційної безпеки для телекомунікаційних систем можливе лише за наявності інформаційно-комунікаційної мережі з високими властивостями якості та надійності. І навпаки, необхідною умовою успішної комунікаційної мережі є ефективне та надійне управління. Тобто, ці процеси пов'язані один з одним.

Для забезпечення певного рівня якості мережі розглядаються основні показники, що описують якість роботи мережі та причини цих наслідків. Однак існує складність в оцінці якісних характеристик інформаційно-комунікаційної мережі. Це питання вирішується шляхом використання різних протоколів зв'язку з різними «носійськими» системами.

Основна функція кожного типу сигналу полягає в забезпеченні відповідного рівня якості. Оскільки комунікаційні системи в телекомунікаційних мережах використовують сигнальні системи, які фактично складаються з взаємопов'язаних датчиків, для підвищення якості роботи цих мереж і, як наслідок, створення ефективної системи інформаційної безпеки, як засіб передачі сигналу слід використовувати бездротову мережу датчиків. Це створить комунікаційну мережу з широким спектром проектування, підвищить її ефективність та надійність.

Розділ 2
ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ НЕЙРОСТРУКТУРНИХ ТЕХНОЛОГІЙ

2.1. Особливості застосування інтелектуальних технологій при управлінні кібербезпекою телекомунікаційних мережа

Інтелектуальні інформаційні технології (ІІТ) – це інформаційні технології, що сприяють швидкому аналізу політичних, економічних, соціальних та технічних питань, а також прийняттю бізнес-рішень. Використання ІІТ у реальному житті передбачає врахування специфіки досліджуваної сфери, яка характеризується такими ознаками:

Якість та ефективність прийняття рішень;

• невизначений характер цілей та меж інституцій.

• Різноманітність тем, що стосуються вирішення проблеми;

• Хаотична, нестабільна та стандартизована поведінка середовища;

• різноманітність факторів, що впливають один на одного;

• недостатня формалізація, сингулярність ситуацій;

• латентність, приховування та неявний характер інформації;

• Важливість малих дій та способів їх реалізації є одночасно значними та різноманітними.

• нетрадиційна логіка міркувань тощо.

ІІТ є результатом створення інформаційних систем та інформаційних технологій для підвищення ефективності управління знаннями, прийняття рішень та вирішення проблем. У цьому випадку будь-яка описана життєва чи ділова ситуація вважається такою, що відповідає типу когнітивної моделі (когнітивна схема, архетип, фрейм тощо), яка потім використовується як

платформа для створення та проведення експериментів, включаючи комп'ютерні експерименти.

Інтелектуальна система (ІС) – це технологічна або комп'ютерна система, яка вирішує проблеми, що традиційно вважаються креативними, що належать до певної галузі знань і мають пам'ять, яка зберігає знання про предмет. Склад інтелектуальної системи складається з трьох основних компонентів – бази знань, розв'язувача та інтелектуального інтерфейсу.

Інженерія знань є невід'ємною частиною всього процесу розробки інтелектуальних інформаційних систем в цілому та, зокрема, інформаційних систем (ІС). Це підхід до ІС, який включає методи вилучення, вивчення та вираження знань, що стосуються правил, у формі бази правил. Розвиток ІС призвів до створення інженерії знань, яка є процесом створення інтелектуальних систем. Це сукупність моделей, методів та технік, призначених для створення систем, які можуть вирішувати проблеми з використанням знань. Фундаментальними компонентами інженерії знань є використання таких операцій, як узагальнення, генерування гіпотез, які можна використовувати для висновку, створення нових програм, що базуються на вже існуючих комп'ютерних програмах тощо. Слово «інженерія», що походить з англійської мови, стосується процесу «кваліфікованої» обробки об'єктів, створення чогось. Як наслідок, процес надання спеціальних експертних знань у досліджуваній галузі, який здійснюється людиною або комп'ютером (програмою), також можна розглядати як інженерію знань.

Інтелектуальні системи різних типів:

1. Логічна система для обчислень

Системи на основі обчислень включають логіку, здатну вирішувати питання проектування та управління декларативними описами умов. У цьому випадку користувач може контролювати всі частини обчислювального процесу в режимі розмови. Ці системи можуть автоматично створювати математичне представлення проблеми та генерувати автоматичні обчислювальні алгоритми,

що відповідають формалізованим вимогам. Ці властивості пояснюються наявністю бази знань у вигляді функціональної семантичної мережі та компонентів дедуктивного мислення та планування.

2. Дайте відповідь на запитання за допомогою інтелектуальної системи, яка є рефлексивною.

Рефлексивна система – це система, яка розробляє спеціальні алгоритми, що реагуватимуть на різні комбінації вхідних ефектів. Алгоритм дозволяє вибрати найімовірнішу реакцію інтелектуальної системи на набір вхідних тригерів, з відомою ймовірністю вибору певної реакції на кожен вхідний тригер, а також на комбінації вхідних тригерів. Ця функція подібна до функції перцептрона. Перцептрон, або перцептрон, – це комп'ютеризована модель сприйняття інформації мозком (кібернетична модель мозку), запропонована Френком Розенблаттом у 1957 році та реалізована як частина електронної машини Mark-1 у 1960 році. Перцептрон став популярною моделлю нейронної мережі, а Mark-1 був першим комп'ютером з неврологічною системою. Незважаючи на відсутність складності, перцептрон здатний легко навчатися та вирішувати складні проблеми. Програмне забезпечення Reflex використовується в таких сферах: доступ до баз даних природною мовою; оцінка інвестиційних пропозицій; оцінка та прогнозування впливу шкідливих речовин на здоров'я населення; прогнозування спортивних результатів. 3. Інтелектуальна інформаційна система

Інтелектуальна інформаційна система (ІС) – це система, що базується на знаннях.

4. Інтелектуальна система, яка поєднує їх обидва

Гібридна інтелектуальна система зазвичай вважається системою, яка використовує більше одного методу імітації людського інтелекту для вирішення проблеми. Як результат, ГІС складається з:

Аналітичних моделей

• складних систем

• комп'ютерно-реалізованих нейронних мереж

Нечітких систем

• Генетичних алгоритмів

• моделювання статистичних моделей

Міждисциплінарний характер «гібридних інтелектуальних систем» приваблює вчених та спеціалістів, які вивчають ефективність кількох, зазвичай різних, підходів до вирішення проблем проектування та управління.

Інтелектуальні інформаційні системи (ІІС) складаються з п'яти основних компонентів, які взаємодіють один з одним: мовна підсистема, яка забезпечує зв'язок між користувачем та іншими компонентами ІСП, інформаційна підсистема, яка зберігає дані та обробляє їх, підсистема управління знаннями, яка зберігає знання про об'єкт, такі як процедури, евристики та правила, а також методи обробки знань, підсистема управління моделями та підсистема вирішення та вирішення завдань, яка взаємодіє з чотирма іншими підсистемами.

Класифікація завдань, що виконуються ІІС, така:

Інтерпретація даних. Це одна з найпоширеніших обов'язків експертних систем. Інтерпретація – це процес розуміння значущості даних, результати якого повинні бути точними та узгодженими. Як правило, використовується кілька методів аналізу даних.

Діагностика. Діагностика – це процедура пов'язування об'єкта з певним класом об'єктів та/або розпізнавання проблеми в певній системі. Несправність – це відхилення від очікуваної норми. Це розуміння дозволяє нам розглядати як відмови обладнання в технічних системах, так і захворювання живих організмів, і всі вони розглядаються з єдиної теоретичної точки зору. Одним із конкретних аспектів цього є вимога розуміння функціональної структури («анатомії») діагностичної системи.

Опитування. Основна функція моніторингу полягає в постійній інтерпретації даних у режимі реального часу та сигналізації про перевищення параметрами допустимих меж. Найбільші проблеми викликають «пропуск» ситуації сповіщення та проблема «хибної» активації. Складність цих питань

пояснюється неоднозначним характером симптомів кризових ситуацій та необхідністю врахування часового контексту.

Проектування. Проектування – це процес створення специфікацій, які спрямовують створення об'єктів із певною властивістю. Опис стосується всього набору необхідних документів – ілюстрацій, додаткових приміток тощо. Найбільше занепокоєння викликають отримання вичерпного структурного опису знань про об'єкт та проблем, пов'язаних зі слідом. Для планування ефективного проектування та, більшою мірою, для перепроектування, важливо формувати не лише рішення щодо проектування, але й обґрунтування їх прийняття. Як результат, два основні процеси, що є частиною екологічної системи проектувальника, нерозривно пов'язані в процесі проектування: процес виведення рішень та процес пояснення.

Прогнозування. Прогнозування – це процес прогнозування наслідків певних подій або явищ на основі аналізу раніше записаних даних. Системи прогнозування є логічними у своєму виведенні ймовірних наслідків із заданих сценаріїв. Динамічна параметрична модель зазвичай служить основою для системи прогнозування, значення параметрів змінюються відповідно до конкретної ситуації. Результати цієї моделі є основою для прогнозів, які мають ймовірний висновок.

Планування. Планування вважається процесом пошуку планів дій, пов'язаних з об'єктами, які можуть виконувати певну функцію. У цьому стилі навчання (ES) використовуються моделі поведінки реальних об'єктів для логічного виведення результатів запланованої діяльності.

Освіта. Визначення навчання полягає в тому, що це використання комп'ютера для навчання предмету чи дисципліні. Навчальні системи розпізнають помилки у вивченні будь-якої галузі за допомогою комп'ютера та пропонують відповідні рішення. Вони отримують знання про характеристики гіпотетичного студента, а потім у своїй практиці визнають брак знань студентів та знаходять способи їх виправлення, коригуючи слабкі сторони студентів. Крім

того, вони стратегічно планують спілкування зі студентом на основі його успіхів, що призведе до передачі знань.

Управління. Управління вважається відповідальністю структурованої системи, яка сприяє певному режиму діяльності. Цей стиль ES регулює поведінку складних систем відповідно до конкретних вимог.

Підтримка прийняття рішень. Підтримка рішень - це набір процедур, які надають особі, яка приймає рішення, інформацію та рекомендації, що допомагають їй приймати рішення. Ці ES сприяють вибору бажаної альтернативи серед кількох. потенційні варіанти під час прийняття відповідальних рішень.

Як правило, всі системи, засновані на знаннях, можна розділити на системи, що вирішують проблеми аналізу, та системи, що вирішують проблеми синтезу. Основна відмінність між завданнями аналізу та завданнями синтезу полягає в тому, що в завданнях аналізу можна скласти список можливих рішень, які потім включаються в систему. На відміну від цього, в завданнях синтезу потенційна кількість рішень необмежена та складається з рішень проблем або компонентів. Обов'язки аналізу: інтерпретація даних, діагностика та підтримка рішень. Обов'язки синтезу включають проектування, планування та управління. Поєднані: інструкції, нагляд, прогнозування [17].

Серед цієї групи інтелектуальних інформаційних технологій найбільш актуальною та значною як основа для бездротової сенсорної системи є нейротехнологія, головним чином через її зосередженість на завданнях аналізу та здатність до самонавчання. Нейронні мережі зазвичай не програмуються з певною метою, натомість вони набувають. Здатність до навчання є однією з основних переваг нейронних мереж над традиційними методами. Технічно, навчання - це процес пошуку зв'язків між коефіцієнтами нейронів. Під час процесу навчання нейронна мережа здатна розпізнавати складні асоціації між вхідними та вихідними даними, а також виконувати узагальнення. Це означає, що якщо навчання пройде успішно, мережа зможе повернути відповідний результат на основі даних, яких бракувало в навчальному наборі. Це

найефективніше для аналізу та організації вхідних даних від датчиків бездротової мережі.

2.3. Модель забезпечення ефективності нейромережевого оцінювання якості інформаційної безпеки телекомунікаційних мереж

Штучна нейронна мережа (ШНМ) – це обчислювальна модель, що базується як на програмному, так і на апаратному забезпеченні. Вона побудована на принципі функціонування біологічних нейронних мереж, або нервових клітин, у живому організмі. Ця ідея виникла в результаті дослідження функціонування мозку та спроби відобразити це функціонування. Першу спробу, що включала нейронні мережі, зробили В. Маккалох та В. Піттс. Після створення алгоритмів навчання отримані моделі були використані для практичних цілей. До них належали прогнозування, розпізнавання образів та управління.

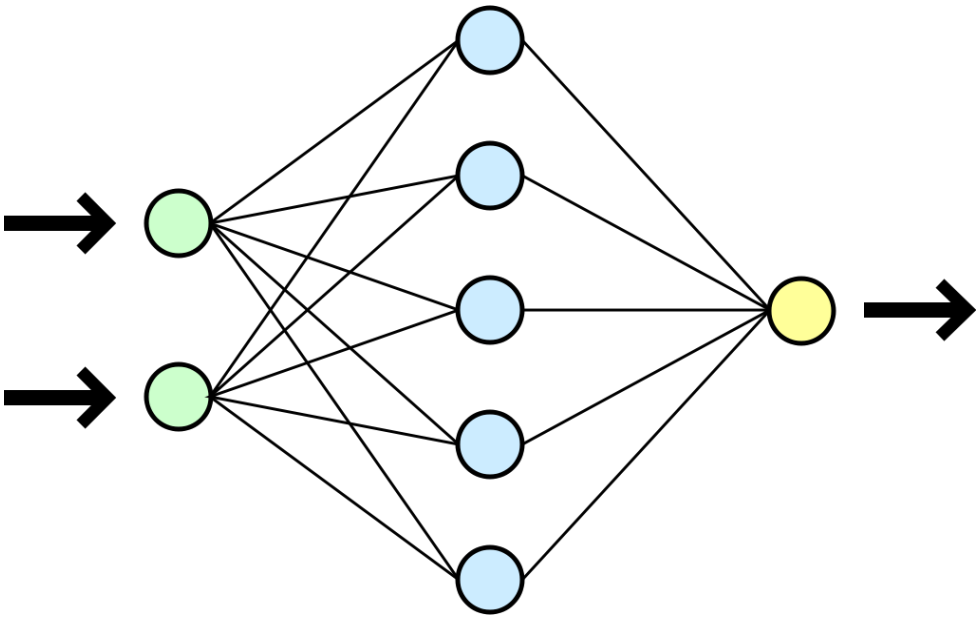


Рис. 3.1 Схема простої нейромережі: зеленим кольором позначені вхідні нейрони, блакитним - приховані нейрони, жовтим - вихідний нейрон

ШНМ – це сукупність простих процесорів, які з'єднані та взаємодіють один з одним. Ці процесори зазвичай прості (порівняно з процесорами персональних комп'ютерів). Кожен процесор у цій мережі обробляє лише сигнали, які він отримує кожного періоду, та сигнали, які він надсилає іншим процесорам кожного періоду. Однак, будучи підключеними до великої мережі з контрольованою взаємодією, ці прості процесори здатні виконувати складні завдання.

З точки зору машинного навчання, нейронна мережа є окремим екземпляром системи розпізнавання образів, а саме, дискримінаційного аналізу, кластерного аналізу тощо.

З математичної точки зору, навчання нейронних мереж – це складна проблема, яка включає кілька параметрів.

З точки зору кібернетики, нейронна мережа використовується в розробці адаптивних стратегій керування та як засіб роботи роботів.

З точки зору обчислювальної розробки та програмування, нейронна мережа є рішенням проблеми ефективного паралелізму.

З точки зору штучного інтелекту, ШНМ є основоположним принципом коннективістської філософії та основним напрямком у структурному підході до дослідження потенціалу комп'ютерів для моделювання (або конструювання) природного інтелекту.

Нейронні мережі не призначені для програмування з використанням традиційного визначення цього слова, натомість вони навчаються. Здатність до навчання є однією з основних переваг нейронних мереж над традиційними методами. Технічно, навчання - це процес знаходження зв'язків між коефіцієнтами нейронів. Під час процесу навчання нейронна мережа здатна розпізнавати складні асоціації між вхідними та вихідними даними, а також виконувати узагальнення. Це означає, що якщо навчання успішне, мережа зможе повернути правильну відповідь на основі даних, які були відсутні у навчальній вибірці, а також неповних та/або "шумних", часткових спотворень даних. Різні об'єкти можуть функціонувати як зображення: текстові символи, зображення,

звукові зразки тощо. Під час налаштування мережі представлені різні зображення, які супроводжуються описом їхнього класу. Вибірка зазвичай представлена вектором значень атрибутів. У цьому випадку повний набір ознак має бути унікальним для визначення класу вибірки. Якщо ознак недостатньо, мережа може пов'язати один і той самий зразок з кількома класами, що неправильно. Після навчання мережі, вона може бути піддана раніше ненавченим зображенням та отримати відповідь, яка описує її приналежність до класу. Структура цієї мережі характеризується спільністю нейронів у вихідному шарі з кількістю класів, визначених користувачем. У цьому випадку встановлюється пряма відповідність між виходом нейронної мережі та класом, до якого вона належить. Коли зображення вводиться в мережу, один з її виходів повинен вказувати, що зображення належить до цього типу. Інші виходи повинні вказувати, що зображення не належить до відповідного класу. Якщо два або більше виходів вказують на те, що зображення є частиною класу, вважається, що мережа не має уявлення про свою відповідь [17].

Конструкції нейронних мереж:

• Полегшене навчання:

Перцептрон

Адаптивні резонансні екосистеми

Комбінаційне навчання:

Радіальна базисна функція

Здатність нейронних мереж розпізнавати зв'язки між різними параметрами дозволяє їм більш лаконічно виражати багатовимірні дані, якщо дані тісно пов'язані. Зворотний процес - отримання вихідного набору даних з частини інформації - називається (автоматичною) асоціативною пам'яттю. Асоціативна пам'ять також сприяє відновленню оригінального сигналу/піктограми з пошкоджених вхідних даних. Подолання гетероасоціативної проблеми запам'ятовування контенту дозволяє використовувати адресовану за контентом пам'ять. Визнаються такі кроки вирішення проблем:

Дані збираються з метою навчання.

Підготовка даних та їх нормалізація;

Вибір топології мережі;

Експериментальне дослідження вибору властивостей мережі;

Експериментальне дослідження вибору параметрів навчання;

Фактичне навчання;

Необхідність забезпечення адекватності навчання;

Зміна параметрів, заключна інструкція;

Усне пояснення функцій мережі для більш детального розуміння.

Під час навчання мережа спостерігається у певному порядку вибірковими тренерами. Порядок, у якому глядач може спостерігати за нею, може бути обраний як послідовний, випадковий або інші типи. Деякі мережі, які навчаються без вчителя (наприклад, мережі Хопфілда), спостерігають вибірку лише один раз. Інші мережі (такі як Кохонена), а також мережі, які навчає вчитель, мають вибірку, яку вони переглядають кілька разів, кожен повний прохід через вибірку називається епохою навчання. Під час навчання з вчителем початковий набір даних розділяється на два компоненти - навчальна вибірка, яка фактично виникає, та тестові дані, які розділені принципом, що не є довільним. Дані навчання та тестування подаються в мережу для навчання, а тестові дані використовуються для обчислення помилки мережі (тестові дані ніколи не використовуються для навчання мережі). Як результат, якщо помилка, пов'язана з тестовими даними, зменшується, кажуть, що мережа узагальнює. Якщо розбіжність між навчальними та тестовими даними продовжує зменшуватися, а розбіжність між навчальними та тестовими даними збільшується, то мережа перестала розширюватися і просто «запам'ятовує» навчальні дані. Це явище відоме як перенавчання мережі або перенавчання. У цьому випадку навчання зазвичай припиняється. Під час процесу навчання можуть виникнути інші проблеми, такі як параліч або положення мережі поблизу локального мінімуму поверхні помилки. Неможливо передбачити появу конкретної проблеми, а також рекомендувати одне її рішення [18]. Все вищесказане стосується ітераційних методів пошуку рішень для нейронних мереж. Для них неможливо реально щось

гарантувати, і навчання нейронних мереж не є повністю автоматизованим. Однак, поряд з ітеративними методами навчання, існують також неітеративні методи, які мають високий ступінь стабільності та дозволяють повністю автоматизувати процес навчання.

Навіть якщо навчання спочатку проходить успішно, мережа може не вивчити те, що задумав автор. Відомим випадком був випадок, коли мережу спочатку навчили розрізняти зображення танків від їхніх відповідних фотографій, але пізніше було виявлено, що всі танки були сфотографовані на одному фоні. Таким чином, мережа навчилася розпізнавати цей тип ландшафту, а не навпаки, або розпізнавати танки. В результаті мережа дізнається про мінімальні вимоги, які необхідно виконати для успішного навчання, але які є найбільш узагальнюваними. Якість навчання нейронної мережі слід оцінювати на прикладах, які не брали участі в її створенні. У цьому контексті кількість експериментальних прикладів має бути більшою, чим вражаюча якість навчання. Якщо помилки нейронної мережі становлять приблизно 1 на 1 000 000, то для перевірки цієї ймовірності необхідно протестувати 1 000 000 прикладів. Було очевидно, що оцінка та тестування добре переносимих нейронних мереж є складним завданням. У цьому контексті виникає питання щодо застосування моделі оцінки нейронної мережі, яка є достатньо ефективною, враховуючи ефективність інформаційно-комунікаційної мережі.

2.3. Модель забезпечення ефективності нейромережевого оцінювання якості функціонування телекомунікаційних мереж

Інформація щодо системи, її атрибутів, входів, виходів та стану може бути неточною, узагальненою та погано написаною. У цьому випадку використовуються нечіткі моделі або, загалом, нейронні моделі неструктурованих даних.

Нечіткі продукційні моделі (нечіткі моделі/системи на основі правил) є найпопулярнішим типом нечітких моделей, що використовуються для опису,

дослідження та моделювання складних, недосконалих систем і процесів. Найпоширенішими процедурами нечіткої логіки наразі є Мамдані, Ларсен, Цукамото та Такагі-Сугено.

Під нечіткою продукційною моделлю ми розуміємо узгоджений набір окремих нечітких продукційних правил виду «ЯКЩО А, то В» (де А та В – це передумови (антецеденти) та висновок (наслідок) цього правила у формі нечітких тверджень), призначених для визначення ступеня точності висновків правил, виходячи з передумов та відомої істинності відповідних правил.

Для створення простих плавних тверджень у передумовах та висновках плавних продукційних правил (наприклад, «a є A», «b є B» у правилах, що мають вигляд «якщо a є A, то b є B»), необхідно вказати тип функцій належності, пов'язаних з відповідними плавними множинами.

Для оцінки ступеня інформаційної безпеки життєздатними є нечіткі продукційні моделі та алгоритми нечіткого виведення на їх основі. Експерт з інформаційної безпеки, можливо, вже створив набір попередньо розроблених функцій належності, які охоплюють основний діапазон вхідних та вихідних змінних, або йому потрібно буде створити ці функції самостійно. Інформація, що представлена через мовлення, може бути озвученою (мовленнєва інформація), обробленою (інформація, що циркулює в ІТС) та збереженою на носіях інформації (паперових, магнітних та інших матеріалах).

Для оцінки безпеки інформації експерт повинен врахувати всі можливі технічні шляхи витоку інформації, стан пов'язаного каналу відповідатиме стану інформаційної безпеки щодо певного типу загрози.

Незважаючи на визнані переваги нечіткого виробництва, є й негативні аспекти:

Вхідний набір нечітких правил складається експертом і може мати частковий або суперечливий характер;

Суб'єктивність у виборі типу та значень функцій належності в операторах нечітких правил;

Відсутність можливості автоматичного отримання знань.

Формально, нечіткі виробничі моделі можуть бути представлені за допомогою нечіткої виробничої мережі, яка за структурою ідентична багатошаровій нейронній мережі, елементи якої реалізують окремий етап нечіткого виводу в виробничій моделі. Щоб усунути вищезгадані недоліки, у кількох дослідженнях висловлювалася ідея створення нечітких моделей для виробництва, які є адаптивними (з уточненням під час процесу та на основі результатів їх роботи), а також реалізації специфічних компонентів цих моделей за допомогою нейромережевої технології.

Склад нейронної мережевої системи (НСС) для вимірювання ступеня інформаційної безпеки, який проілюстровано на рис. 3.2, включає m-нейронні кластери (шари), які визначаються кількістю станів інформаційної безпеки у відповідь на певний тип загрози. Стан безпеки дорівнює нейронному шару, а кількість класів визначається параметрами, які визначаються (вимірюються) та порівнюються з нормами з метою визначення стану інформаційної безпеки для кожного з конкретних технічних каналів витоку, згідно з розробленою моделлю небезпек для інформації.

За результатами опитування та першої прямої (розрахункової) оцінки безпеки щодо безпеки кожного потенційного технічного каналу маємо матриці розміром $n \times Ml$, де Ml – загальна кількість небезпек, пов’язаних з l-м технічним каналом.

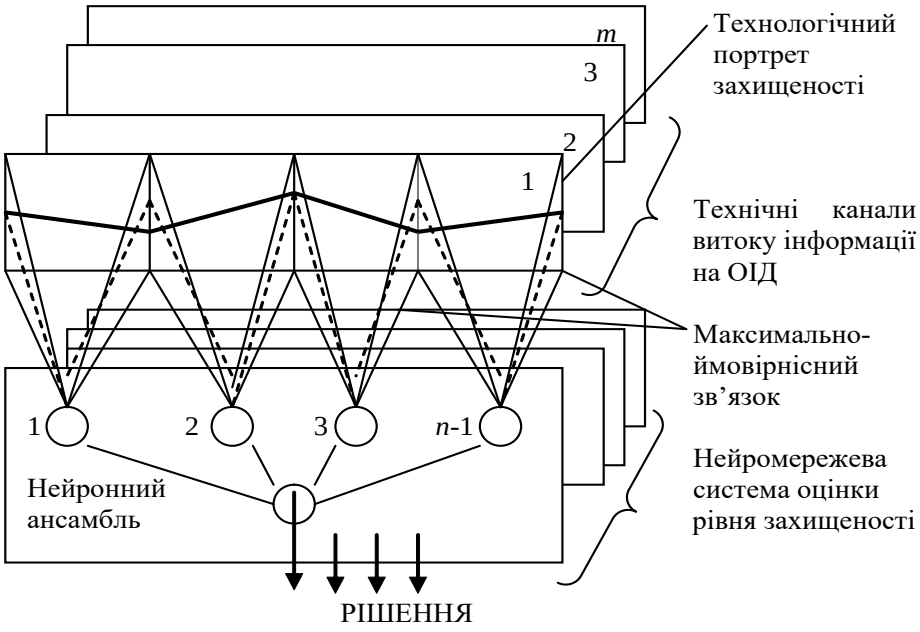


Рис. 2.2 Структура нейромережевої системи

Таким чином, ми маємо набір матриць, які фактично описують формальні атрибути OID.

Вкрай важливо проводити інструментальний нагляд та визначати остаточний список потенційних каналів витоку технічної інформації на об'єкті. Таким чином, ми маємо колекцію {ml}TKVI.

Набір станів безпеки, що відповідають технічним каналам втрати інформації на OID у певний момент часу, можна описати як динамічну систему. Ці стани називаються подіями та зображуються за допомогою технологічних образів безпеки. Цей термін, який описує відповідні ідеї фізичного, інформаційного та безпекового характеру, вважається практикою динамічної мережі, розподіленої в певному технологічному стані або конфігурації станів. Еволюційні зміни, що відбуваються між подіями, не враховуються, і передбачається, що динаміка системи безперервно розвивається від події до події. Цей тип системи називається дискретно-подійною.

Контекст середовища нейронної мережевої системи (NMS), яка оцінює ступінь інформаційної безпеки, можна описати як набір дискретно-подійних систем, пов'язаних з дискретними технологічними станами безпеки.

Після отримання необхідної кількості інструментальних вимірювань та спеціальних досліджень для кожного з каналів витоку технічної інформації, отриманих на OID, необхідно розробити процедуру вимірювання інформації про стан технологічної безпеки кожного з каналів відповідно до затвердженої моделі загрози.

Результати інструментальних вимірювань та спеціальних досліджень, що стосуються кожного з каналів витоку технічної інформації, сприймаються матрицею датчиків як набір спостережень: , та = 1,2,...,n. В окремому каналі інформації простір вибірки зменшується, в результаті чого маємо послідовність дискретних змінних Uk, k = 0,1,...,n-1, які приймають значення Z1, Z2,...,Zr.

Вкрай важливо створити структуру нейронного приймача рішень, який приймає меншу підмножину простору.

Послідовність дискретних змінних Ur, k = 0,1,...,n-1, які приймають значення za, a = 1,2,...,r, можна приблизно представити векторами , Φ(0) та , Φ(k) відповідно.

Склад найпростішої нейроподібної системи для вимірювання безпеки являє собою набір з M+1 колекцій нейронних мереж у першому шарі. Ансамбль складається з n нейронів, їхній потенціал збудження описується як

$$Y_{\mu}(k) = \sum_{a=1}^{n} \Xi a(k) \Phi_{a}(k)_{\mu} \qquad (2.1)$$

де Ξ , $\Phi(0)_{\mu}$ та Ξ , $\Phi(k)_{\mu}$. – вектори, якими можна апроксимувати послідовність дискретних змінних U_r, k = 0,1,...,n-1, що приймають значення z_a, a = 1,2,...,r .

Кожен нейрон пов'язаний з процедурою, яка визначається методом позначених ліній. У цьому методі певні значення призначаються певним

(позначеним) лініям Z1, Z2,..., Za,..., Zk, що призводить до того, що певне значення параметра процесу пов'язується з найбільш збудженим синаптичним зв'язком.

На відміну від типового нейрона, синаптичні зв'язки якого ідентичні, нейрон, який використовує метод позначених ліній, має пріоритет над ними. Синаптичний вхід великої кількості має більший вплив на параметри процесу. Ще одна відмінність полягає в тому, що протягом k-го моменту часу стимулюється лише один синаптичний зв'язок, таким чином завдання входу та контролю порогу спрощується за допомогою вагової функції w.

Дійсно

$$Y_{\mu}(k) = \sum_{a=1}^{r} \Xi a(k) \Phi_a(k)_{\mu} - \Theta_a(k)_{\mu}$$

Для кожного технічного каналу в множині {ml}TKVI необхідно визначити його значення. Незважаючи на різну кількість небезпек, пов'язаних з кожним можливим технічним маршрутом, ця кількість не становить загрози для самого технічного маршруту. Як наслідок, важливість кожного каналу слід визначати співвідношенням загальної кількості загроз, пов'язаних з певним каналом, до загальної кількості загроз, які експертне опитування вважало «однією».

Тоді формула для розрахунку важливості кожного технічного каналу у списку виглядає наступним чином:

$$\lambda_l = \frac{M_l^1}{M_l}, \quad l = \overline{1, L},$$

де M_l^1 - кількість загроз *l*-го технічного каналу, які прийняли значення “1” за результатами експертного опитування; M_l – загальна кількість загроз, що характеризують *l*-й технічний канал.

В результаті створюється набір значень важливості кожного потенційного витоку технічної інформації - {λl}TKVI, . Вхідний синапс має більший обсяг, коли параметр технічного каналу вищий.

Важливо ранжувати технічні канали за їхньою важливістю, а потім створити остаточний список потенційних каналів витоку технічної інформації на OID.:

$$\{m_l\}^*_{\text{ТКВІ}},\ l = \overline{1, L},\ \text{де}\ L \le 8. \qquad (1)$$

При спробі вирішення проблем, пов'язаних з вимірюванням ступеня інформаційної безпеки, насамперед необхідно оцінити ступінь відповідності отриманих сигналів (портретів технологічної безпеки – результатів інструментальних вимірювань та спеціалізованих досліджень щодо кожного з технічних каналів витоку інформації) опорним сигналам, що має визначити критерії для прийняття рішення. Методика вимірювання відповідності різна залежно від характеру проведених розслідувань. В результаті рішення щодо інформаційної безпеки приймається після вивчення норм, встановлених у нормативних документах системи технічного захисту в Україні.

2.4. Нейромережева модель оцінювання якості функціонування системи управління інформаційної безпекою за допомогою нейронних мереж радіально-базисного типу

Один із підходів до вирішення питань, поставлених у висновку другого розділу цього проєкту, полягає у використанні математичних моделей, що базуються на використанні апарату штучних нейронних мереж (ШНМ) з радіальними базисними функціями (РБФ). Цей апарат ШНМ з РБФ має добре розроблену методологію структурного моделювання та навчання, що походить від добре розробленої теорії програмування. Дослідження в галузі ШНМ з РБФ присвячені зусиллям відомих вчених, таких як Є.В. Бодянський, О.Г. Руденко,

А.І. Галушкін, В.І. Литвиненко, А.О. Фефелов, О.О. Д. Ідик, Є. Горшков, В. Колодяжний та інших. Штучні нейронні мережі з радіальними базисними функціями мають необхідні властивості для моделювання складних систем, що мають глибокий вплив, створення моделей поведінки нестаціонарних об'єктів та прогнозування випадкових подій. Зазвичай прогнози неточні, але похибка залежить від використаної методології прогнозування. Чим більше ресурсів виділяється на прогноз, тим кращим і точнішим слід передбачити прогноз і тим меншою буде шкода, спричинена невизначеністю. ШНМ з RBF мають низку переваг порівняно з іншими математичними методами прогнозування. ШНМ з RBF мають більш гнучку архітектуру, ніж штучні нейрони перцептронного типу.

Штучні нейронні мережі з радіальними базисними функціями є універсальними пристроями апроксимації, єдиним додатковим компонентом є один нелінійний шар нейронів, параметри цього шару регулюються, і можна використовувати стандартні процедури навчання. Завдяки своєму єдиному нелінійному шару нейронів ці пристрої мають високу швидкість і фільтр, який дуже важливий для обробки "шумних даних". У визначених рамках ШНМ з RBF зміна структури проста, достатньо визначити кількість нейронів у прихованому шарі. Ще однією перевагою є можливість змінювати функцію активації. Лише кілька незначних перетворень дозволяють повністю переформувати структуру ШНМ з RBF, що дозволяє найефективніше змінювати архітектуру, що використовується, та мінімізувати помилку, пов'язану з навчанням (підвищити точність і якість прогнозу). Ще однією значною перевагою ШНМ з RBF є те, що експерту не потрібно вибирати математичну модель для поведінки часового ряду. Створення моделі ШНМ з RBF є адаптивним, під час навчання, без участі експерта. ШНМ з RBF отримує конкретні приклади з бази даних, що стосуються розглянутої проблеми, і вона адаптується до цих даних. Структура ШНМ з RBF проілюстрована на рисунку, це демонструє, що мережа має вхідний шар, лише один прихований шар, який базується на радіальних обертах, та вихідний шар, який є лінійним.

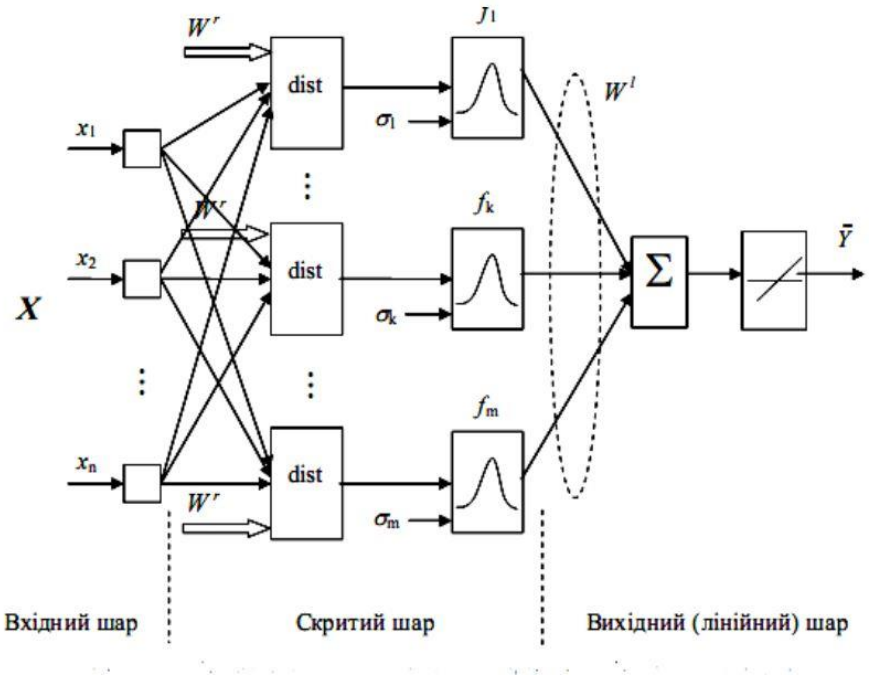


Рис. 2.3 Узагальнена архітектура штучної нейронної мережі з радіально-базисними функціями

Навчання штучних нейронних мереж (ШНМ) за допомогою RBF зазвичай здійснюється однокроковим або багатокроковим методом. Для навчання мережі та створення її дизайну типове середовище використовує програму швидкої обробки даних та має велику різноманітність програм і функцій, призначених для проектування та дослідження штучних нейронних мереж цього типу. Однокроковий алгоритм навчання дає ШНМ, яка має точність до нуля на навчальному наборі. Мережа будується автоматично під час процесу навчання; структура вивчається за один крок. Цей алгоритм створює фіктивну нейронну мережу з радіальним базисом, яка має бажаний вихідний результат, а структура фіктивної мережі ідентична складу навчальної вибірки. Єдина вимога - вибрати достатньо велике значення параметра впливу, але не настільки велике, щоб значення вхідних даних були ідентичними. Навчання мережі за цим алгоритмом відбувається швидко, але структура моделі є складною та неінтуїтивно зрозумілою, оскільки кількість нейронів у прихованому шарі ідентична кількості елементів у навчальному наборі. Як наслідок, вищезгадана структура ШНМ з RBF призводить до неможливості створення високоякісного прогнозу для

великих розмірів вибірки, що типово для реальних задач. Під час навчання ШНМ з RBF за допомогою багатокрокового алгоритму навчання структура штучної нейронної мережі радіального типу формується за допомогою повторюваної процедури, яка додає один нейрон до кожного кроку. Формується дворівнева система [19]. Перший рівень складається з нейронів, які обчислюють зважену відстань між своїми входами, використовуючи евклідову функцію dist, а також специфічні входи. Другий рівень складається з простих лінійних нейронів (y = f(x) = x) та обчислює зважений вхід, використовуючи пов'язану функцію, а також її окремі входи. Обидва мають різницю. Функція dist базується на формулі

$$d_i = \sqrt{\sum_f (x_j - w_{i,j})^2}, i = \overline{1, S}$$

де $w_{i,j}$ – елемент матриці ваг W; W – матриця ваг, що має розмірність (S x R); x_j – значення j-го входу, R = 1.

На початку дослідження, стратегія радіально-базисного рівня не містить нейронів. Нейрони додаються до прихованого шару, доки сума квадратичних помилок мережі не стане меншою за певне значення або не буде використана максимальна кількість нейронів. Спочатку визначається розрахункова тривалість роботи штучної нейронної мережі радіального типу. Далі вибирається вхідний вектор з найбільшим значенням середньоквадратичної помилки. Після цього додається нейрон з радіальним базисом, ваги якого ідентичні цьому вектору. Просте лінійне зважування реорганізується для мінімізації середньоквадратичної помилки. Під час навчання ШНМ з RBF (роботоподібною базою) сприятлива структура нейронної мережі (з оптимальною кількістю прихованих нейронів) досягається за допомогою багатокрокового алгоритму, який забезпечить точніший прогноз з мінімальною помилкою, коли обсяг навчального набору значно великий. Архітектура моделі спрощується за рахунок максимальної точності вхідних даних.

В результаті аналіз показує, що найефективнішим методом кількісного

прогнозування є використання ШНМ з RBF. Сучасні реальні проблеми мають велику кількість факторів впливу, дослідження показало, що саме багатокроковий алгоритм навчання доцільний для використання з ШНМ на основі RBF, яка має здатність обробляти велику кількість даних та в процесі навчання формувати структуру штучної нейронної мережі радіального типу, що має властивості, що є прогностичними.

2.5. Висновки по розділу

На основі висновків першої частини розділу про характеристики інтелектуальних інформаційних технологій було зазначено, що нейроструктурна технологія майже ідеально підходить для створення бездротової мережі датчиків, оскільки ця технологія має глибокий аналіз статистичних даних, що дозволить ефективно приймати рішення, а також здатність до самостійного навчання.

Оскільки процес мережевого моделювання є складним та обширним, він вимагає обов'язкового тестування якості. Це тестування нейронної мережі має відбуватися на прикладах, які не брали участі в її навчанні, кількість тестових прикладів залежатиме від необхідного ступеня якості навчання. Якщо помилки нейронної мережі становлять приблизно 1 на 1 000 000, то для перевірки цієї ймовірності необхідно протестувати 1 000 000 прикладів. Було очевидно, що оцінка та тестування добре переносимих нейронних мереж є складним завданням. У цьому контексті постає питання про те, як використовувати модель оцінки нейронної мережі, яка є ефективною з огляду на ефективність комунікаційної мережі. На основі отриманої інформації було створено модель оцінки якості роботи телекомунікаційних систем, яка базується на радіальних нейронних мережах, реалізація яких вирішить проблему необхідності реалізації процесу навчання. Оскільки питання реалізації бездротового мережевого датчика на основі нейронної технології вирішено, необхідно перейти безпосередньо до реалізації власної концептуальної моделі забезпечення ефективності ТКМ щодо інформаційної безпеки, яка слугуватиме прототипом високоякісної системи інформаційної безпеки для телекомунікаційних мереж різного застосування.

Розділ 3
КОНЦЕПТУАЛЬНА МОДЕЛЬ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТЕЛЕКОМІНІКАЦІЙНОЇЇ МЕРЕЖІ НА ОСНОВІ НЕЙРОСТРУКТУРНИХ ТЕХНОЛОГІЙ

3.1. Системи управління інформаційною безпекою телекомунікаційних мереж: призначення та функціональні завдання

З огляду на те, що метою цього проекту є опис та створення прототипу високоефективної системи інформаційної безпеки для телекомунікаційних мереж, характеристики якої згадані в першому абзаці цього розділу, очевидно, що необхідно зосередитися та описати призначення та функціональні аспекти таких систем. Цей розділ присвячений більш детальному розгляду атрибутів цих систем. Як результат, система управління інформаційною безпекою (СУІБ) є частиною більшої загальної системи управління, яка враховує ризик інформаційної безпеки як бізнес-активу, ця система призначена для розробки, впровадження, управління, перевірки та підтримки інформаційної безпеки.

Модель PDCA (Plan-Do-Check-Act, PDCA) використовується для процесів, пов'язаних з СУІБ [3]:

• Планування (planning) - процес створення СУІБ, створення переліку активів, оцінк ризиків та вжиття заходів;

• Виконання (actions) - процес впровадження та реалізації відповідних дій;

• Перевірка (verification) - процес перевірки ефективності та продуктивності СУІБ. Зазвичай проводиться внутрішніми аудиторами.

• Дія (покращення) – впровадження превентивних та коригувальних заходів.

Це базується на п'яти групах функцій системи управління, які вирізняються стандартами ISO/ITU-T.

Група 1: конфігурація мережі та управління іменем – ці обов'язки включають налаштування параметрів окремих мереж та інформаційно-

комунікаційної мережі в цілому. Для компонентів мережі ця сукупність завдань визначає адреси, ідентифікатори (імена) та місця розташування, пов'язані з мережею. Для всієї мережі управління конфігурацією зазвичай включає створення карти мережі або відображення фактичних зв'язків між компонентами мережі та змін у зв'язку між ними. Статистичні результати роботи інформаційно-комунікаційної мережі можуть служити основою для прийняття рішень у рамках групи управлінських обов'язків.

Група 2: Обробка помилок – ця група обов'язків включає виявлення, визначення та усунення наслідків помилок та несправностей мережі, включаючи статистичну інформацію про те, як працює мережа.

Група 3: Аналіз продуктивності та надійності – обов'язки цієї групи пов'язані з оцінкою, на основі всієї вже накопиченої статистичної інформації, параметрів, пов'язаних з часом відгуку системи, пропускною здатністю віртуального або реального каналу зв'язку, обсягом трафіку в кожному сегменті мережі та каналі, ймовірністю пошкодження даних під час передачі по мережі, а також коефіцієнтом доступності мережі. Можливості оцінки продуктивності та надійності мережі необхідні як для операційного управління мережею, так і для планування нових мереж.

Група 4: Управління безпекою – обов'язки цієї групи включають регулювання доступу до даних під час їх зберігання або передачі через Інтернет. Фундаментальними компонентами управління безпекою є процес автентифікації користувачів, процес перевірки та підтвердження прав доступу до мережевих ресурсів, процес управління повноваженнями тощо.

Під час вирішення завдань безпеки цієї групи слід враховувати статистику щодо атак на мережу та спроб обійти безпеку її ресурсів.

Облік роботи мережі – обов'язки цієї групи полягають у записі тривалості використання різних мережевих ресурсів – пристроїв, каналів та транспортних послуг, включаючи статистичну інформацію щодо інформаційно-комунікаційної мережі.

Виходячи з вищезазначеної інформації, ми робимо висновок, що основними обов'язками системи управління інформаційною безпекою є управління конфігурацією інформаційно-комунікаційної мережі, виявлення помилок, аналіз продуктивності та надійності, і, як наслідок, управління безпекою ТСМ, включаючи облік її використання. Для покращення самої системи інформаційної безпеки, тобто для підвищення ефективності процесу досягнення її функціональних цілей, необхідно покращити якість інформаційно-комунікаційної мережі.

В результаті, практичні обов'язки цієї роботи безпосередньо пов'язані з обов'язками управління комунікаційними мережами з метою підвищення якості їхньої роботи.

3.2. Поняття, структура та характеристики моделі забезпечення ефективності функціонування телекомунікаційних мереж

Відправною точкою для розробки концептуальної моделі, яка б забезпечила ефективність традиційної конвенційної моделі (ТКМ), стали принципи, запропоновані в третьому розділі цього дослідження. Ці принципи були використані для визначення очікуваного вихідного сигналу та формування навчальної вибірки на основі експертних знань, на основі цих принципів була створена модель для створення навчальних прикладів. Очікувалося, що вхідна база статистичних даних буде недоступною. Як результат, можливо створювати навчальні приклади на основі оцінки даних експертом. Завдання експертів полягає в тому, щоб з'ясувати, які з вхідних даних відповідають обраній нечіткій концепції. У першому припущенні робиться висновок, що вихід НММ досягається за допомогою лише одного нейрона. Крім того, задокументовано випадок, коли цільовий вихідний сигнал відсутній у навчальній вибірці. Як правило, перетворення інформації, яке відбувається за допомогою цього методу, представлено такими формулами:

$$\left\langle A, \mathbf{\Omega}_1, \mathbf{\Omega}_2, \mathbf{D}_1, \mathbf{D}_2, \mathbf{D}_3, N_x, N_y, \mathbf{Z}_{\text{нв}}, W_{\text{п}} \right\rangle \to \left\langle \mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3 \right\rangle, \quad (3.1)$$

$$\boldsymbol{Z}_1 = \left\{ \boldsymbol{z}_1^{(\phi_k)} \right\}_{K_\phi} = \left\{ \left(\boldsymbol{x}^{(\phi_k)}, y^{(\phi_k)} \right) \right\}_{K\phi}, \quad (3.2)$$

$$\boldsymbol{Z}_2 = \left\{ \boldsymbol{z}_2^{(\phi_k)} \right\}_{K\phi} = \left\{ \boldsymbol{r}^{(\phi_k)} \right\}_{K_\phi}, \quad (3.3)$$

$$\boldsymbol{Z}_3 = \left\{ \boldsymbol{z}_3^{(\varphi_l)} \right\}_{L_\phi} = \left\{ \boldsymbol{x}^{(\varphi_l)} \right\}_{L_\phi}, \quad (3.4)$$

де A – алфавіт неструктурованих даних, що мають бути розпізнані,

$\boldsymbol{\Omega}_1$ – множина даних, отриманих із БД,

$\boldsymbol{\Omega}_2$ – множина нечітких елементів,

$\boldsymbol{D}_1$ – множина експертних даних, що стосуються співвідношення очікуваного вихідного сигналу НМ з вибраним еталоном,

$\boldsymbol{D}_2$ – множина експертних даних, що стосуються продукційних правил розпізнавання нечітких даних,

$\boldsymbol{D}_3$ – множина експертних даних, що стосуються розпізнавання нечітких даних серед відповідних елементів,

$\boldsymbol{Z}_1$ – навчальна вибірка, приклади якої містять очікуваний вихідний сигнал,

$\boldsymbol{Z}_2$ – навчальна вибірка з прикладами у вигляді продукційних правил,

$\boldsymbol{Z}_3$ – навчальна вибірка, приклади якої не мають очікуваного вихідного сигналу,

$\boldsymbol{Z}_{нв}$ – множина обмежень на формування навчальної вибірки,

W_n – обчислювальна потужність апаратних засобів, що використовуються НМС розпізнавання нечітких даних,

$\boldsymbol{z}_1^{(\phi_k)}$, $\boldsymbol{z}_2^{(\phi_k)}$ – навчальні приклади виду $\boldsymbol{Z}_1$, $\boldsymbol{Z}_2$ для k-ої пари вхідних сигналів,

$\boldsymbol{z}_3^{(\varphi_l)}$ – навчальні приклади виду $\boldsymbol{Z}_3$ для *l*-го нечіткого елементу,

$\boldsymbol{x}^{(\phi_k)}$ – множина вхідних параметрів *k*-ої пари даних,

$y^{(\phi_k)}$ – очікуваний вихідний сигнал HMM для *k*-ої пари даних,

$\boldsymbol{r}^{(\phi_k)}$ – множина продукційних правил для *k*-ої пари даних,

K_ϕ – кількість нечітких даних, які мають бути розпізнані,

$\boldsymbol{x}^{(\varphi_l)}$ – вхідні параметри для *l*-го нечіткого елементу,

L_φ – кількість нечітких елементів.

Основним джерелом інформації для створення навчальної вибірки є та , що є набором вхідних статистичних даних. Різниця між та полягає в тому, що вхідні дані, пов'язані з ним, об'єднуються певним нечітким елементом, результатом є збіг між ними, і між ними немає відповідності. — це набір даних, який не є структурованим і має певний порядок, заснований на певному принципі (в алфавітному порядку). Під час створення моделі, яка формує параметри навчальних прикладів, було виявлено, що набір має 217 компонентів. Крім того, під час розробки LMM для забезпечення ефективності комунікаційних мереж було помічено, що кількість параметрів у продукційних правилах, що входять до складу, становила 7.

За допомогою (3.1-3.4) було виявлено, що для їх реалізації необхідно виконати п'ять кроків: дозволений обсяг навчальної вибірки, очікуваний вихідний сигнал LMM для кожного зі стандартів нечітких елементів, створення LMM та . Також рекомендується використовувати етап визначення потенціалу для формування навчальної вибірки у вигляді колекцій або наборів. Важливо визнати, що наявність навчальної вибірки у формі дозволяє використовувати потужніші типи LMM, проте її створення є найскладнішим. Як результат, можна очікувати:

$$\textit{Якщо } \boldsymbol{Z}_1 \in \boldsymbol{Z} \to \boldsymbol{Z}_2, \boldsymbol{Z}_3 \notin \boldsymbol{Z}. \tag{3.5}$$

Крім того, створення навчальної вибірки відповідного типу може бути ускладнене оцінкою експерта, а використання пов'язаних з нею нейронних моделей (НММ) може бути обмежене максимально допустимою похибкою розпізнавання. Крім того, на основі загальновизнаного методу розробки НММ [23] було виявлено, що необхідні етап нормалізації вхідних та вихідних параметрів та етап контролю якості попередньої обробки навчальної вибірки. Крім того, очікувалося, що ГС забезпечить механізм створення навчальної вибірки, який відповідав би мінімальним вимогам стандарту GSM та вже був відфільтрований. Формальна структура методу створення навчальної вибірки проілюстрована на рис. 3.1.

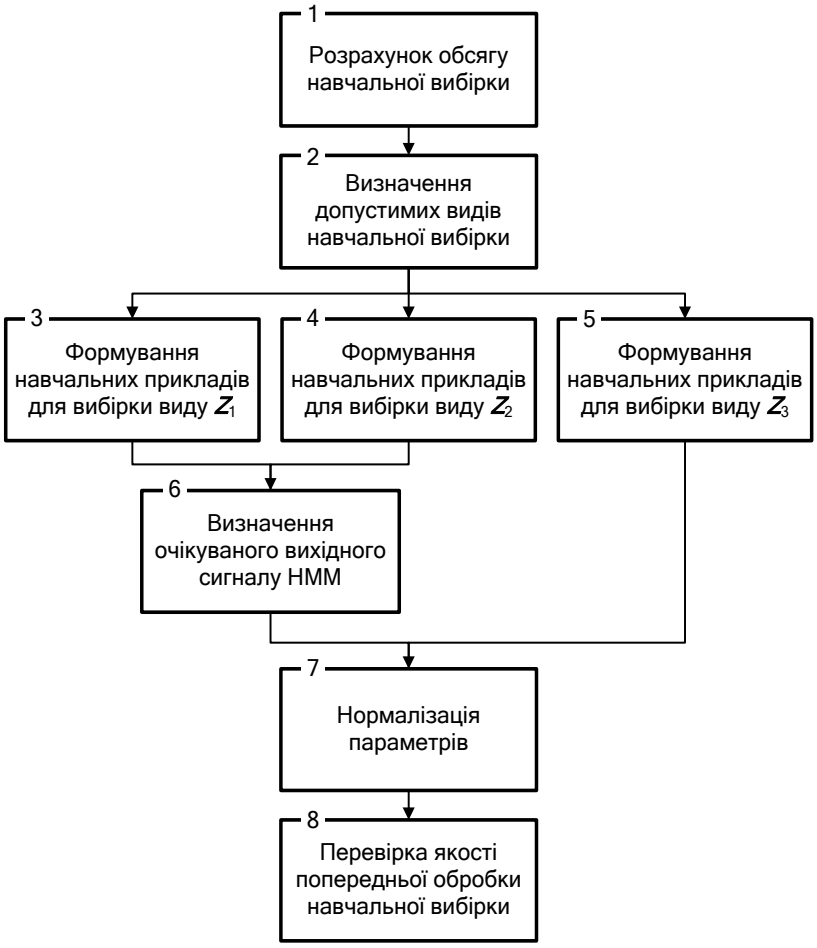


Рис. 4.1. Структурна схема методу створення навчальної вибірки

Етап 1 – Виконується розрахунок розміру навчальної вибірки. На цьому етапі визначається мінімальна та максимальна кількість навчальних прикладів, які можна вмістити. Дані, що вводяться на етапі: Wn, Nx та Kf. Для визначення мінімальної кількості прикладів, які можна врахувати, використовується вираз

$$L_{\Sigma}^{min} = \sum_{k=1}^{K_{\phi}} L_{\phi_k}^{min}, \tag{3.6}$$

де L_{Σ}^{min} – загальна мінімально допустима кількість прикладів,

$L_{\phi_k}^{min}$ – мінімально допустима кількість навчальних прикладів для кожної *k*-ої пари вхідних даних, що має бути розпізнана.

Беручи розроблену модель для створення навчальних прикладів та [23], мінімальна кількість навчальних прикладів, необхідних для кожної пари, дорівнює:

$$L_{\phi_k}^{min}(\boldsymbol{Z}_1, \boldsymbol{Z}_3) = 10 \times N_x = 10 \times (55...217) = 550...2170, \tag{3.7}$$

де N_x – кількість вхідних параметрів HMM.

Згідно з розробленим LMM типу MPNN та результатами [20], для навчальної вибірки типу мінімальна кількість прикладів, які можна навчити на пару, розраховується наступним чином:

$$L_{\phi_k}^{min}(\boldsymbol{Z}_2) = 20 \times N_x = 20 \times 7 = 140. \tag{3.8}$$

Загальна мінімальна кількість навчальних прикладів, які можна використовувати для кожного типу вибірки, виводиться з (4.7, 4.8) у (4.5). Максимальний обсяг навчальної вибірки, який можна безпечно реалізувати, базується на потенціалі підтримки навчання LMM без перерв на загальнодоступному апаратному та програмному забезпеченні. Спочатку

очікувалося, що така реалізація дозволить повне навчання відбуватися протягом 1 дня (8640 секунд) [19]. Використовуючи питоме значення з виразів, отриманих у розробленій моделі правил, що визначають ефективні типи LMM, можна записати такі рівняння:

$$8640 \approx k_1 \tau e^{-\varepsilon} L_{\phi_k}^{max}(\boldsymbol{Z}_2, \boldsymbol{Z}_3)(N_x + N_y), \tag{3.9}$$

$$8640 \approx k_2 \tau e^{-\chi\varepsilon} L_{\phi_k}^{max}(\boldsymbol{Z}_1)^2 (N_x + N_y)^2, \tag{3.10}$$

де $L_{\phi_k}^{max}(\boldsymbol{Z}_1)$ – максимально допустима кількість прикладів виду $\boldsymbol{Z}_1$,

$L_{\phi_k}^{max}(\boldsymbol{Z}_2, \boldsymbol{Z}_3)$ – максимально допустима кількість прикладів виду $\boldsymbol{Z}_2$, $\boldsymbol{Z}_3$,

τ – тривалість однієї обчислювальної операції процесу навчання.

Після підстановки у (4.9, 4.10) визначених у п. 2.3 величин $k_1 \approx 0{,}1$, $k_2 \approx 0{,}001$, $\chi \approx 1$, $\varepsilon \approx 0{,}01$ та тривіальних спрощень отримаємо:

$$L_{\phi_k}^{max}(\boldsymbol{Z}_2, \boldsymbol{Z}_3) \approx 86400 / \tau(N_x + N_y), \tag{3.11}$$

$$L_{\phi_k}^{max}(\boldsymbol{Z}_1) \approx 8640000 / \tau(N_x + N_y)^2 . \tag{3.12}$$

Враховуючи в (3.11, 3.12), що для HMM, які відповідають вибіркам $\boldsymbol{Z}_1$, $\boldsymbol{Z}_3$, $N_x + N_y \approx (60...220)$, для HMM, що відповідають $\boldsymbol{Z}_2$, $N_x + N_y \approx 10$ та орієнтуючись на максимізацію терміну навчання отримаємо:

$$L_{\phi_k}^{max}(\boldsymbol{Z}_1) \approx 2400\, \tau^{-1}, \tag{3.13}$$

$$L_{\phi_k}^{max}(\boldsymbol{Z}_2) \approx 8640\, \tau^{-1}, \tag{3.14}$$

$$L_{\phi_k}^{max}(\boldsymbol{Z}_3) \approx 1440\,\tau^{-1}. \quad (3.15)$$

Зазначимо, що $\tau = f(W_n)$, а її величину слід визначити експериментальним шляхом. Таким чином, виходом першого етапу являється L_{Σ}^{min} та $L_{\phi}^{min}(\boldsymbol{Z}_1, \boldsymbol{Z}_3)$, $L_{\phi}^{min}(\boldsymbol{Z}_2)$, $L_{\phi}^{max}(\boldsymbol{Z}_1)$, $L_{\phi}^{max}(\boldsymbol{Z}_2)$, $L_{\phi}^{max}(\boldsymbol{Z}_3)$.

Етап 2 – визначення типів навчання, що допускаються. Дані, що вводяться на етап, це Kϕ, , , , , , , , , . Виходом етапу є множина всіх можливих типів навчальних вибірок, що допускаються. Процес поділено на три кроки, кожен з яких відповідає перевірці легітимності входження окремого елемента в один із трьох типів навчальної вибірки, або.

Крок 1 – перевірка легітимності. Вибірка навчального типу вважається прийнятною, коли виконується будь-яка з двох вимог.

Умова 1. Наявність бази даних, яка дозволяє створювати з достатньою кількістю компонентів. Для цього у зазначеній базі даних вхідної статистичної інформації має бути присутня достатня кількість відповідних нечітких сегментів. Аналітичний вираз умови 1 має наступний вигляд:

$$\textit{Якщо } \boldsymbol{\Omega}_1 \notin \varnothing \wedge L_{\phi_k}^{\boldsymbol{\Omega}_1} \geq 550, k = 1,..K_{\phi} \rightarrow \boldsymbol{Z}_1 \in \boldsymbol{Z} \quad (3.16)$$

де $L_{\phi_k}^{\Omega_1}$ – кількість елементів $\boldsymbol{\Omega}_1$, що стосуються *k*-ої пари даних.

Умова 2. Використовуючи експертну оцінку, набір прийнятних нечітких коефіцієнтів може бути сформований у відповідний час. У першому припущенні цю умову можна виразити наступним чином:

$$\textit{Якщо } \boldsymbol{\Omega}_2 \notin \varnothing \wedge \mathrm{E}_1(\boldsymbol{\Phi}, \boldsymbol{\Omega}_2, \boldsymbol{D}_3) = \boldsymbol{z}_1^{(\phi_k)}, L_{\phi_k}^{z_1} \geq 550 \wedge t_{Z_1} \leq t_d \rightarrow \boldsymbol{Z}_1 \in \boldsymbol{Z}\,, \quad (3.17)$$

де E_1 – процедура формування $\boldsymbol{z}_1^{(\phi_k)}$ із $\boldsymbol{\Omega}_2$,

$L_{\phi_k}^{z_1}$ – кількість елементів $\boldsymbol{z}_1^{(\phi_k)}$,

t_d – допустимий термін формування навчальної вибірки

$t_{\boldsymbol{Z}_1}$ – термін формування навчальної вибірки виду $\boldsymbol{Z}_1$

Крок 2 – Оцінка допустимості. Вибірковий навчальний набір певного типу вважається допустимим, якщо виконується умова – за допомогою експертної оцінки для кожної k-тої пари даних за відповідний час можна створити набір з кількістю елементів не менше 140.

$$\textit{Якщо } \mathrm{E}_2\left(\boldsymbol{\Phi}, \boldsymbol{D}_2\right) = \boldsymbol{r}^{(\phi_k)}, L_{\phi_k}^{D_2} \geq 140 \wedge t_{Z_2} \leq \bar{t}_{\partial} \rightarrow \boldsymbol{Z}_2 \in \boldsymbol{Z}, \tag{3.18}$$

де E_2 – процедура формування продукційних правил,

$t_{\boldsymbol{Z}_2}$ – термін формування навчальної вибірки виду $\boldsymbol{Z}_2$

Крок 3 – перевірка допустимості $\boldsymbol{Z}_3$. Навчальна вибірка виду $\boldsymbol{Z}_3$ вважається допустимою при виконанні умови:

$$\textit{Якщо } L_{\varphi} \geq k_{\varphi} L_{\Sigma}^{min} \rightarrow \boldsymbol{Z}_3 \in \boldsymbol{Z}, \tag{3.19}$$

де k_{φ} – коефіцієнт очікуваного розподілу фонем в доступній $\boldsymbol{\Omega}_2$.

Використавши [23] визначено, що при використанні, в якості джерела даних для формування $\boldsymbol{\Omega}_2$, наприклад, загальнодоступних телевізійних записів $k_{\varphi} = 10$. Це дозволить записати (3.19) так:

$$\textit{Якщо } L_{\varphi} \geq 10 L_{\Sigma}^{min} \rightarrow \boldsymbol{Z}_3 \in \boldsymbol{Z} \tag{3.20}$$

Етап 3 – створення прикладів, що навчають тип. Основою етапу є змодельований процес формування параметрів навчальних прикладів.

Вважається, що джерелом формування може бути база даних вхідної статистичної інформації або набір нечітких атрибутів речей. Для цього запропонована процедура полягає в оцінці подібності нечіткого числа до певної пари даних за допомогою експерта. Вхідними даними етапу є K, , , , , , а виходом є набір прикладів, що потребують нормалізації своїх параметрів, вони називаються навчальними прикладами. У цьому випадку вихідний сигнал виражається у вигляді символічного рядка. Процес складається з шести кроків.

Крок 1 – визначення стаціонарних фрагментів, які є квазістаціонарними. Для оцінки використовуються вирази, що були сформовані під час розробки параметрів моделі. Виходом кроку є від 1 до 5 стаціонарних фрагментів, що представляють 128 етапів організації даних.

Крок 2 – обробка стаціонарних фрагментів, які є квазістаціонарними. Результатом обробки є значення коефіцієнта, пов'язаного з кожним зі стаціонарних фрагментів, які є квазістаціонарними. Етап полягає у застосуванні віконної функції Хеммінга (4.21) до витвору мистецтва, застосуванні дискретного перетворення Фур'є та обчисленні коефіцієнтів.

$$w(n) = 0{,}53836 - 0{,}46164 \times cos(2\pi n/(N-1)) \times s(n), \qquad (3.21)$$

де n – номер відліку деякого фрагменту даних,

N – кількість відліків у фрагменті,

$s(n)$ – початкова величина вхідних даних n-ній стадії ,

$w(n)$ – величина нечітких елементів у n-мій стадії після обробки віконною функцією Хемінга.

$$x_k = \sum_{n=0}^{N-1} w(n) \times cos(2\pi nk / N), 0 \le k < N, \qquad (3.22)$$

де x_k – структурованість відносно пар вхідних даних *k*.

$$m = 1127,01048 \times ln\left(1 + \frac{f}{700}\right), \tag{3.23}$$

де *m* – завантаженість даними відносно частоти їх подачі *f*.

Крок 3 – оцінка нечітких ознак експертом. Ця процедура застосовується лише при використанні набору нечітких значень як джерела даних. Результатом цієї процедури є очікувані дані, що описують кожен з нечітких компонентів. Для цього пропонується процедура, подібна до процедури експертної оцінки. Ця процедура подібна до процедури розробленої моделі для створення навчальних прикладів. Різниця між переліченими процедурами ґрунтується виключно на тому, що під час оцінки неоднозначної інформації експерт визначає ймовірність асоціації з кожною з пар даних в алфавіті для кожної з них. Тобто значення – це ймовірність, призначена експертом цьому нечіткому поняттю як n-тій фонемі. В результаті значення вважається середнім колективним значенням цього нечіткого поняття на n-му рівні. Також вважається, що

$$\textit{Якщо } x_n \le \Delta_\phi \to x_n = 0, \tag{3.24}$$

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

Запропонований метод експертної оцінки передбачає асоціювання подібного звуку з кількома різними звуками.

Крок 4 – обчислення вихідного сигналу в символічній формі. Процедура підходить для типу навчальних прикладів. Якщо джерелом даних є , то вихідне значення прикладу є сумішшю знаків:

$$y^{(\phi_k)} = 1 * \phi_k. \tag{3.25}$$

де *k*– номер неструктурованої пари даних в алфавіті.

Якщо джерело даних є , і в результаті кроку 4 виявлено, що існує ймовірність пов'язати нечітке поняття з кількома парами даних, цей елемент є основою для створення кількох навчальних прикладів. Вихідний сигнал для цих прикладів має наступний вигляд:

$$y^{(\phi_k)} = y_k * \phi_k . \tag{3.26}$$

де k – номер неструктурованої пари даних в алфавіті.,

ϕ_k – k -та пара,

y_k – середня колективна оцінка того, що даний нечіткий елемент є *k*-ою парою.

Крок 5 – підвищення рівня. На цьому кроці дотримується розробленої моделі для створення навчальних прикладів, визначається масштабний коефіцієнт і набір випадкових даних перетворюється на структурований набір даних.

Крок 6 – визначення вхідних параметрів. Крок включає обчислення значень вхідних параметрів для навчальних прикладів. Значення першого вхідного параметра ідентичне масштабному коефіцієнту. k_ϕ:

$$x_1 = k_\phi . \tag{3.27}$$

Значення інших вхідних параметрів ідентичні відповідним значенням коефіцієнтів, отриманих за допомогою процедури масштабування:

$$x_q = c_q , q = i + 24(j-1) + 1, \tag{3.28}$$

де j – номер квазістаціонарного інтервалу нечіткого
елементу після масштабування,
i – номер коефіцієнту в j-му фрагменті.

Етап 3 виконується, доки обсяг навчальної вибірки не перевищить $L_{\phi_k}^{max}(\boldsymbol{Z}_1)$ (4.13) або доки термін її формування не перевищить $\bar{t}_d$.

Етап 4 – створення навчальних сценаріїв для вибору типу.

Дані, що вводяться на етапі, це , а також Кϕ. Виходом є набір навчальних прикладів відповідного типу, параметри яких необхідно нормалізувати. У цьому випадку вихідний сигнал виражається у вигляді символьного рядка. Метою етапу є визначення ступеня розпізнавання кожної пари алфавітних даних процедурою експертної оцінки даних, пов'язаної з правилами виробництва їх розпізнавання. Це досягається шляхом аналізу перших семи формант (незалежно від типу даних, отриманих сенсорною мережею). Подібно до процесу експертної оцінки нечіткого поняття, який є частиною третього кроку другого етапу цього методу, процедура експертної оцінки близькості пар даних використовується як основа для розробленої концепції створення навчальних прикладів.

Спочатку передбачається, що дані про деяку k-ту пару літер алфавіту представляють собою матрицю виду

$$D_{2,k} = \begin{vmatrix} \left(X_{k,1,1}^{min}, X_{k,1,1}^{max}\right), & \dots & \left(X_{k,n,1}^{min}, X_{k,n,1}^{max}\right), & \dots & \left(X_{k,N,1}^{min}, X_{k,N,1}^{max}\right), y_{k,1} * \phi_k \\ \dots & \dots & \dots & \dots & \dots \\ \left(X_{k,1,m}^{min}, X_{k,1,m}^{max}\right), & \dots & \left(X_{k,n,m}^{min}, X_{k,n,m}^{max}\right), & \dots & \left(X_{k,N,m}^{min}, X_{k,N,m}^{max}\right), y_{k,m} * \phi_k \\ \dots & \dots & \dots & \dots & \dots \\ \left(X_{k,1,M}^{min}, X_{k,1,M}^{max}\right), & \dots & \left(X_{k,n,M}^{min}, X_{k,n,M}^{max}\right), & \dots & \left(X_{k,N,M}^{min}, X_{k,N,M}^{max}\right), y_{k,M} * \phi_k \end{vmatrix}, \quad (3.29)$$

де N – кількість компонент в продукційному правилі для k-ої пари,

$X^{min}_{k,n,m}, X^{max}_{k,n,m}$ – нижня та верхня межа *n*-го діапазону продукційного правила виду (2.93) для *k*-ої пари, визначені *m*-им експертом,

$y_{k,m}$ – визначена *m*-им експертом ймовірність того, що при виконанні продукційного правила нечіткий елемент є *k*-ою парою,

M – кількість експертів.

Згідно з моделлю MPNN, для всіх літер алфавіту n-та компонента продукційного правила пов'язана з n-тою формантою, а кількість цих компонентів дорівнює . З урахуванням можна представити це так:

$$\boldsymbol{D}_2 = \left\{D_{2,1},...D_{2,K_\phi}\right\}. \tag{3.30}$$

Фактичний процес експертної оцінки передбачає використання цих виразів для опису компонентів. Результатом цього етапу є приклади навчання, які включаються до композиції та виражаються у вигляді:

$$\boldsymbol{z}_2^{(\phi_k)} = \left\{\left(\left(X^{min}_{k,1}, X^{max}_{k,1}\right),...\left(X^{min}_{k,7}, X^{max}_{k,7}\right), y_k * \phi_k\right)_i\right\}_I, \tag{3.31}$$

де I – кількість навчальних прикладів для *k*-ої пари.

Етап 4 вважається завершеним, коли обсяг навчальної вибірки перевищує (4.14) або коли термін її формування перевищує .

Етап 5 – створення навчальних вибірок, що відповідають типу прикладу. Реалізація цього етапу аналогічна реалізації етапу 3, проте нечіткий елемент не пов'язаний з жодною літерою алфавіту, відповідно, початкові вихідні сигнали не обчислюються. Вхідні дані цього етапу – , , , Кϕ та , а вихідні – . Неможливість пов'язати нечітке поняття зі стандартним числом призводить до відсутності можливості визначити масштабний коефіцієнт. Як наслідок, пропонується

зробити масштаб фонемоподібного компонента однаковим для всіх значень масштабного коефіцієнта від 0,2 до 5. Згідно із запропонованою моделлю формування параметрів навчальних прикладів, якщо . У випадку , крок переходу. В результаті один нечіткий компонент слугуватиме джерелом даних для 9 прикладів.

Таким чином, процес реалізації етапу включає три дії.

Крок 1 – визначення стаціонарних фрагментів, що є квазістаціонарними. Цей крок аналогічний першому кроку третього етапу цього методу.

Крок 2 – обробка стаціонарних фрагментів, що є квазістаціонарними. Ця процедура ідентична другому кроку третього етапу цього методу.

Крок 3 – визначення вхідних параметрів для прикладів. На цьому етапі для кожного з можливих значень визначаються значення компонентів множини, які виводяться з навчальних прикладів відповідного виду. Для розрахунку використовуються вирази (4.30, 4.31).

Етап 5 завершується, коли обсяг навчальної вибірки перевищує (4.15) або коли термін її формування перевищує .

Етап 6 – визначення вихідного сигналу. Етап передбачає надання кожному навчальному прикладу типу та величини очікуваного вихідного сигналу від LMM, це визначається подібністю акустичних властивостей фонем. Вхідними даними етапу є K*, а також навчальні набори, що входять до складу та . Виходом етапу є змінений набір навчальних прикладів, що складають вибірку. Основою етапу є запропонована ідея визначення очікуваного результату LMM для пар даних та метод формування параметрів навчальних прикладів на основі запропонованої ідеї. Зазначена модель включає обчислення вихідного сигналу LMM з використанням міри подібності, яка показує, наскільки кожна фонема

схожа на цільовий звук. Це враховується у вихідному сигналі LMM на третьому та четвертому етапах методу. В результаті процес складається з двох кроків.

Крок 1 – обчислення подібності нечіткої інформації. Процедура включає проведення професійної оцінки неструктурованих пар даних, що складають набір, а також обробку професійних даних математичними засобами. Виходом кроку є набір метрик, що оцінюють подібність пар документів:

$$\boldsymbol{O} = \{o_k\}_{K_\phi}, \tag{3.32}$$

де o_k – оцінка міри схожості *k*-ої фонеми із алфавіту $\boldsymbol{\Phi}$.

Крок 2 – врахування подібності нечіткої інформації. Щоб врахувати оцінку вимірювання подібності у виході навчального прикладу, компонент змінюється на . Таким чином, і-й навчальний приклад, що стосується k-тої пари типу або , матиме наступний склад:

$$z_{1,i}^{(\phi_k)} = (x_1, \ldots x_{217})_i, y_{k,i} \times o_{k,i}, \tag{3.33}$$

$$\boldsymbol{z}_{2,i}^{(\phi_k)} = \left(\left(X_{k,1}^{min}, X_{k,1}^{max}\right), \ldots \left(X_{k,7}^{min}, X_{k,7}^{max}\right)\right)_i, y_{k,i} \times o_{k,i}. \tag{3.34}$$

Етап 7 – Нормалізація параметрів. Цей етап призначений для забезпечення того, щоб вхідні та вихідні значення навчальних прикладів знаходилися в межах допустимого діапазону значень. Вхідними даними для етапу є приклади з навчального набору, що містяться в , . Параметри навчальних прикладів стандартизовані за такою формулою:

$$\bar{a} = \frac{a - a^{min}}{a^{max} - a^{min}}, \tag{3.35}$$

де a – початкова величина параметру,

$\bar{a}$ – нормалізована величина вхідного параметру a,

a^{max}, a^{min} – максимальна та мінімальна величина a у вибірці.

В результаті, кожен з параметрів складається з двох кроків.

Крок 1 – визначення екстремумів. На основі аналізу всіх прикладів навчальної вибірки визначається середній час на кожен навчальний приклад.

Крок 2 – нормалізація. Значення параметра виражається у відсотках від (4.35).

В результаті, вихід етапу становить , , , на якому параметри навчальних прикладів змінюються для використання з LMM. Якщо результуючий вихід становить , то процес завершено.

Етап 9 – оцінюється якість попередньої обробки навчальних прикладів. Цей етап реалізується лише для вибірки навчальної вибірки, яка є її вхідними даними. Для перевірки використовується константа Ліпшица виду.

$$Lp = \max_{i \neq j, x_i \neq x_j} \frac{\left| y_i - y_j \right|}{\left\| \boldsymbol{x}_i - \boldsymbol{x}_j \right\|}, \tag{3.36}$$

де $\boldsymbol{x}_i, \boldsymbol{x}_j$ – вектори вхідних параметрів для *i*-ої та *j*-ої пар,

y_i, y_j – вихідні параметри для *i*-ої та *j*-ої пар.

Якість препроцесора вважається адекватною, якщо . В іншому випадку, відповідною процедурою є зміна методу нормалізації, структури та обсягу навчальної вибірки. Спочатку передбачається, що . Виходом етапу є сигнал, який вказує на завершення формування навчальної вибірки або необхідність її зміни.

Структурний та аналітичний опис процесу створення навчальної вибірки зображено на рис. 3.2.

Рис. 3.2. Структурно-аналітична схема методу створення навчальної вибірки

3.3. Нейромережева модель забезпечення ефективності функціонування системи управління кібербезпекою на основі розпізнавання неструктурованих даних

Якість препроцесора вважається адекватною, якщо . В іншому випадку, відповідною процедурою є зміна методу нормалізації, структури та обсягу навчальної вибірки. Спочатку передбачається, що . Виходом етапу є сигнал, який вказує на завершення формування навчальної вибірки або необхідність її зміни.

Структурний та аналітичний опис процесу створення навчальної вибірки зображено на рис. 3.2.

$$Якщо\ x_1 \in \left[X_1^{min}, X_1^{max}\right]_l \wedge \ldots \wedge x_7 \in \left[X_7^{min}, X_7^{max}\right]_l \rightarrow Y_l, \qquad (3.37)$$

де $x_1,...x_7$ – характеристики перших семи формант,

$\left[X_1^{min}, X_1^{max}\right],\ldots,\left[X_7^{min}, X_7^{max}\right]$ – задані діапазони $x_1,...x_7$,

l – номер продукційного правила,

Y_l – результат продукційного правила (очікувана пара).

У разі встановлення продукційних правил за допомогою виразу (4.37), завданням експертів є визначення меж діапазонів. У [24] зазначено, що кожна з формант має один пов'язаний з нею коефіцієнт. Крім того, аналіз [22] показав, що стиль MPNN для LMM найбільш повно розвинений для навчання з використанням продукційних правил. Конструкція MPNN, яка призначена для категоризації неструктурованих пар даних, продемонстрована на рис. 4.3.

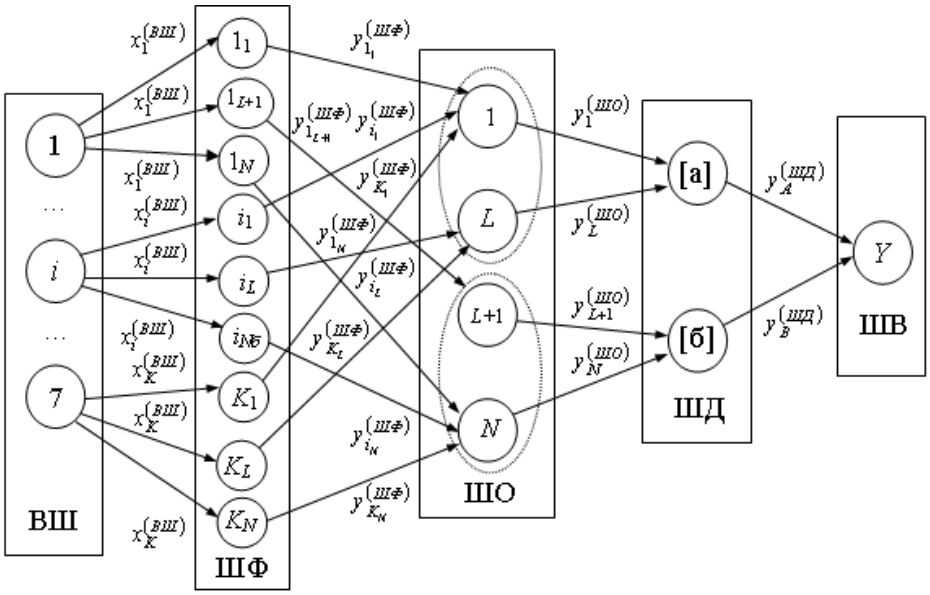


Рис. 3.3. Структура MPNN

Структурна композиція MPNN складається з п'яти шарів: вхідного (VS), фільтрації (SF), зображень (SHO), додавання (SHD) та виходу (SHV). Нейрони VS пов'язані з нейронами, що ідентифікують атрибути. Завданням il-го нейрона в SF є оцінка i-го вхідного параметра ai відповідно до l-го правила продукування. Для цього використовується функція, яка активує форму.

$$\exists x_i^{(ВШ)} \in \left[X^{min}, X^{max}\right]_l \rightarrow y_{j_l}^{(ШФ)} = x_i^{(ВШ)}, \exists x_i^{(ВШ)} \notin \left[X^{min}, X^{max}\right] \rightarrow y_{j_l}^{(ШФ)} = 0, \quad (3.38)$$

де $x_i^{(ВШ)}$ – значення амплітудної характеристики *i*-ої форманти,

$y_{j_l}^{(ШФ)}$ – вихідний сигнал j_l нейрону ШФ.

Вихідний сигнал *l*-го нейрону ШО розраховується так:

$$y_l^{(ШО)} = \sum_{k=1}^{K} exp\left(-\left(w_{k_l,l} - y_{k_l}^{(ШФ)}\right)^2 \Big/ 2\sigma^2\right), \quad (3.39)$$

де $w_{k_l,l}$ – вага зв'язку між k_l-им нейроном ШФ та *l*-им нейроном ШО,

K=7 – кількість вхідних параметрів,

σ – радіус функції Гауса.

В нейронах ШД використовується лінійна функція активації. Вихідний сигнал *j*-го нейрону ШД ($y_j^{(ШД)}$) розраховується так:

$$y_j^{(ШД)} = \sum_{i=1}^{N} y_i^{(ШО)}, \tag{3.40}$$

де N – кількість нейронів ШО, пов'язаних з *j*-им нейроном ШД,

$y_i^{(ШО)}$ – активність *i*-ого нейрону ШО, пов'язаного з *j*-им нейроном ШД.

Завдання окремого нейрона SHV полягає у виборі найбільшого сигналу, який можуть створити нейрони SD. Щоб перетворити знання про те, як класифікувати неструктуровані дані, у MPNN (4.40), необхідно:

- додати новий нейрон до SH;

- додати додаткові нейрони до SH, що відповідають правилу продукування, та пов'язати вагові параметри вхідних з'єднань зі значеннями ідентифікаційних параметрів, що відповідають заданому звуку;

- з'єднати нові нейрони SH та SH;

- з'єднати новий нейрон SH з відповідним нейроном SH A або B.

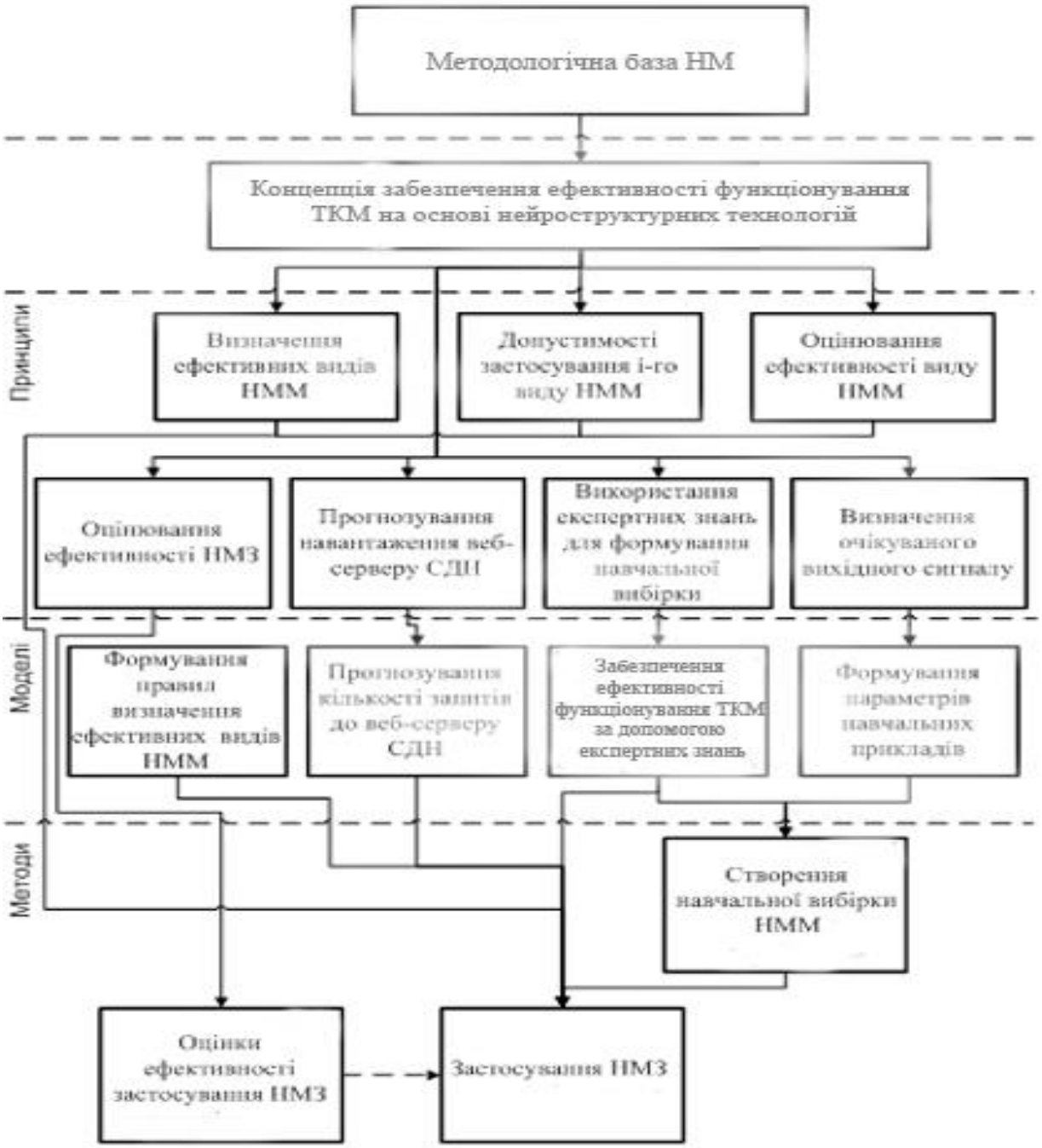


Рис. 3.4. Інфологічна схема методології нейромережевого розпізнавання

3.4 Висновки по розділу

Запропоновані принципи та моделі є основою для розробки методологічного підходу до забезпечення ефективності телекомунікаційних мереж на основі розпізнавання випадкових, неструктурованих даних за допомогою експертних знань (рис. 4.4). На основі NMM також були розроблені інші методи: створення вибіркового навчального набору, що включає обидва компоненти NMM для розпізнавання неоднозначних пар даних, використання нейронної мережі для розпізнавання даних та оцінка ефективності методу.

Необхідність розвитку пояснюється висновками третього розділу, які демонструють, що за допомогою запропонованих принципів і моделей ефективність традиційної китайської медицини (ТКМ) може бути підвищена, зберігаючи при цьому її безпеку.

ВИСНОВКИ

У процесі підготовки кваліфікаційного завдання було виконано такі дії:

- проведено дослідження різних систем, що використовуються для оцінки якості мережевого зв'язку.

- вивчено методи вдосконалення системи інформаційної безпеки інформаційно-комунікаційної мережі за допомогою нейротехнологій.

- Створено концептуальну основу управління інформаційною безпекою в телекомунікаційних мережах на основі нейротехнологій.

1. Перша частина кваліфікаційного завдання містить висновки Огляду стану, можливостей та тенденцій розвитку телекомунікаційних мереж. Визначено проблеми з оцінкою якості функціональності мережі. Описано основи принципів системи.

2. Друга частина кваліфікації зосереджена на напрямках вдосконалення системи інформаційної безпеки інформаційно-комунікаційної мережі за допомогою нейротехнологій. Визначено особливості застосування інтелектуальних технологій у кібербезпеці телекомунікаційних мереж. Описано принципи нейронних мереж, що використовуються для обробки статистичної інформації щодо якості мереж зв'язку. Обговорено моделі, призначені для забезпечення ефективності оцінки нейронною мережею якості інформаційної безпеки в телекомунікаційних мережах.

3. У третій частині кваліфікаційного завдання створюється концептуальна модель управління кібербезпекою інформаційно-комунікаційної мережі, натхненна нейротехнологіями. Обговорюється система управління інформаційною безпекою. Описуються ідеї та організація моделі, що використовується для забезпечення ефективності системи інформаційної безпеки. Створюється нейронна мережа, призначена для забезпечення ефективності системи інформаційної безпеки на основі неструктурованих даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

3. www.ik.3dscorpion.com.ua

4. www.factor-ltd.by

5. Інформаційно-психологічна протидія в Національній гвардії України (психологічний аспект) [Текст] : монографія / І. В. Воробйова, Я. В. Мацегора, І. І. Приходько та ін.; за заг. ред. проф. І.І. Приходька; 2-ге вид. – Х.: Національна акад. НГУ, 2016. – 265 с.

6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. –К.: Кондор, 2004. – 384 с.

7. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

9. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013. – [Second edition 2013-10-01]. – Geneva, 2013. – P. 23.

10. Information technology. Security techniques. Information security risk management: ISO/IEC 27005:2011. – [Second edition 2011-06-01]. – Geneva, 2011. – P. 68.

11. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. Том I. Несанкционированное получение информации – К.: Арий, 2008. - 464 с.

12. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г Защита информации в телекоммуникационных системах.. — К.: МК-Пресс, 2005. — 288 с, ил.

19. Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2013) /

В. В. Мохор, А. М. Богданов, А. С. Килевой. К.: ООО «Три-К», 2013. — 129 с.

20. Домарєв В.В. Організація захисту інформації на об’єктах державної та підприємницької діяльності /Домарєв В.В., Скворцов С.О./ Навч. Посібник. – К.: Вид-во Європейського університету, 2006. – 102с.

22. https://worldvision.com.ua/ua/datchiki-dvizheniya-tekhnologicheskie-osobennosti/

23. http://www.sirius.kiev.ua/images/documents/instrukcii

25. https://secur.ua/kombinirovannyj-datchik-dvizhenija-i-razbitija-satel-navy.html

26. ДСТУ EN 54-1:2003 Системи пожежної сигналізації. Частина 1. Вступ (EN 54-1:1996, IDT)

27. https://secur.ua/ua/articles/ua_ogljad-zasobiv-ohoroni-i-bezpeki.html

28. Горніцька Д. А. Система социотехнических атак в информационной среде / Д. А. Горніцька, О. Г. Корченко, В. П. Харченко // Проблемы экономики и управления на железнодорожном транспорте. Материалы второй международной научно-практической конференции. − .: ЭКУЖТ, 2007. − С. 137-138.

29. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - К., 2000. - С 50-52.

30. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. – К. : Кондор, 2004. – 384 с. – (Юридична книга).

31. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 2000, 37 с.

32. Гинце А. А. Особенности СКУД систем доступа крупных распределенных объектов / А. А. Гинце. ААМ Систем, 2005.

34. О. К. Юдін, О. М. Весельська. Аналіз та класифікація систем контролю

та управління доступом на підприємстві. Наукоємні технології, 2(38), 2018. С. 220-225

35. https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review.

36. https://tzi.com.ua/zagalnij-oglyad-sistem-vbroakustichnogo-zashumlennya.html.

37. https://plenka.market/ua/ultra_vision_r_silver_20_1524_m/

38. https://ecosound.kiev.ua/akucticheckie-paneli

Додаток А

ДЯКУЮ ЗА УВАГУ !

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кваліфікаційна робота здобувача освітнього ступеня «Магістр»

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ НЕЙРОСТРУКТУРНИХ ТЕХНОЛОГІЙ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Володимир НЕТЬОСА

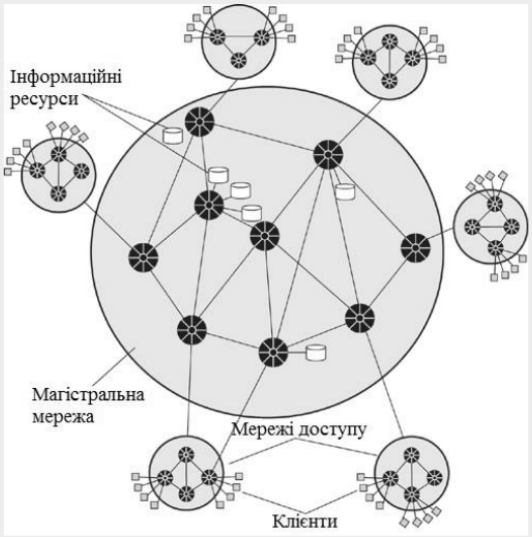
Керівник: доктор філософії Петро ПОНОЧОВНИЙ

Київ - 2026

АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність роботи зумовлена потребою підвищення захищеності інформаційно-комунікаційних мереж під час передавання важливої та конфіденційної інформації.
- Мета роботи - удосконалення системи управління інформаційною безпекою інформаційно-комунікаційної мережі на основі нейроструктурних технологій.
- Об’єкт дослідження - система інформаційної безпеки інформаційно-комунікаційної мережі.
- Предмет дослідження - система управління інформаційною безпекою інформаційно-комунікаційної мережі.
- Основні завдання: аналіз якості функціонування ІКМ, дослідження нейроструктурних технологій та розроблення концептуальної моделі управління кібербезпекою.

СТРУКТУРА ТА ОСОБЛИВОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ



- ІКМ включає мережі доступу, магістральну мережу та інформаційні ресурси, які забезпечують надання сервісів користувачам.
- Ключовими елементами є термінальні вузли, комутатори, канали зв’язку, інформаційні центри та системи управління послугами.
- Багаторівнева структура мережі створює додаткові вимоги до моніторингу, оцінювання якості та захисту інформаційних потоків.

ОЦІНЮВАННЯ ЯКОСТІ ФУНКЦІОНУВАННЯ ІКМ

- Якість телекомунікаційних послуг оцінюється через точки доступу до послуги та характеристики мережі.
- До основних параметрів належать пропускна здатність, затримка, точність передавання, надійність та ефективність доставки інформації.
- Оцінювання QoS і NP є базою для виявлення слабких місць, планування ресурсів і підвищення стійкості системи інформаційної безпеки.

СИСТЕМНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПОСЛУГ

- Системний підхід враховує вимоги споживача, можливості оператора та фактичний рівень якості послуг.
- Взаємозв’язок між QoS та характеристиками мережі дозволяє визначити критичні параметри для управління безпекою.
- Показники якості доцільно використовувати як вхідні дані для інтелектуального аналізу стану мережі.

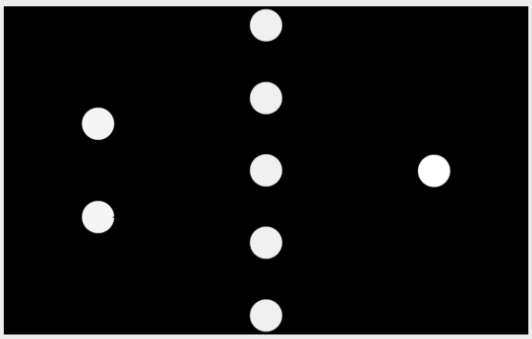
Основні відмінності в підходах до визначення показників якості телекомунікаційних послуг

Якість, яка сприймається (QoE)	Якість телекомунікаційної послуги (QoS)	Характеристики мережі (NP)
Орієнтовані на споживача телекомунікаційної послуги	Орієнтовані на оператора телекомунікацій	
Описується параметрами (атрибутами) ставлення споживача	Описується параметрами (атрибутами) послуги	Описуються параметрами (атрибутами) елементу з’єднання
Орієнтовано на ефект, що очікується споживачем	Орієнтовано на ефект, що сприймається споживачем	Орієнтовані на розробку, проектування, експлуатацію і технічне обслуговування
Визначається споживачем	Вимірюється між точками (у точках) доступу до послуги	Описують можливості елементів з’єднання або наскрізних з’єднань

НАПРЯМКИ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

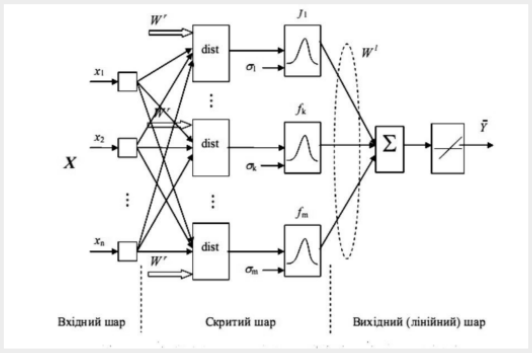
- Удосконалення СУІБ передбачає перехід від статичного контролю до адаптивного управління станом захищеності мережі.
- Нейроструктурні технології дозволяють виявляти приховані закономірності у великих масивах статистичної та неструктурованої інформації.
- Інтелектуальна обробка даних забезпечує прогнозування відхилень, класифікацію інцидентів і підтримку прийняття рішень.
- Ключовий результат - підвищення оперативності реагування на загрози та зниження ризику несанкціонованого доступу.

НЕЙРОМЕРЕЖЕВІ ПРИНЦИПИ ОБРОБКИ СТАТИСТИЧНОЇ ІНФОРМАЦІЇ



- Нейронна мережа приймає вхідні параметри стану ІКМ, формує приховані представлення та генерує оцінку якості або рівня загрози.
- Навчання моделі дає можливість підвищити точність розпізнавання нестандартних режимів роботи мережі.
- Отримані результати використовуються для підтримки рішень щодо посилення захисту та керування мережевими ресурсами.

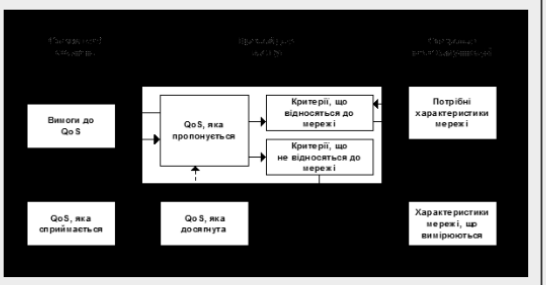
МОДЕЛЬ ОЦІНЮВАННЯ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ РАДІАЛЬНО-БАЗИСНОГО ТИПУ



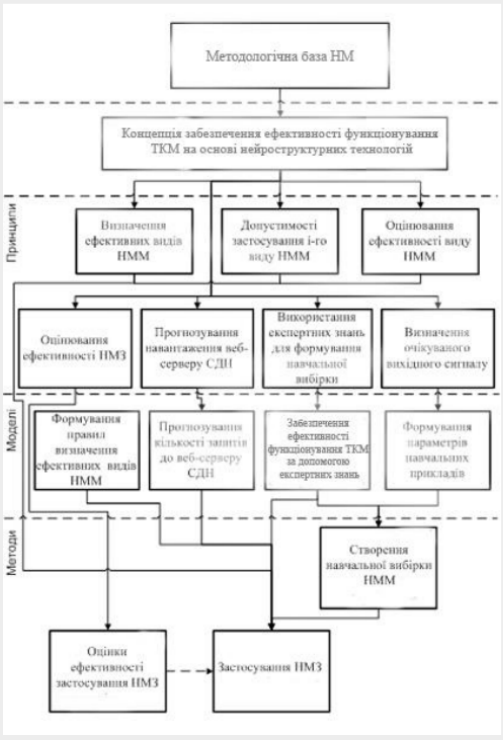
- Радіально-базисна нейронна мережа використовується для апроксимації складних залежностей між параметрами якості ІКМ і станом інформаційної безпеки.
- Модель містить вхідний шар, прихований шар радіально-базисних функцій та вихідний шар з інтегральною оцінкою.
- Перевагою підходу є можливість швидкої класифікації станів і адаптації до зміни мережевого середовища.

АЛГОРИТМІЧНА ОСНОВА ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ БЕЗПЕКОЮ

- Алгоритмічна структура передбачає послідовне збирання даних, попередню обробку, нейромережеве оцінювання та формування керуючих дій.
- На основі результатів аналізу визначаються відхилення від нормального режиму та можливі ознаки загроз.
- Система підтримує прийняття рішень щодо зміни політик безпеки, обмеження доступу або підвищення рівня моніторингу.

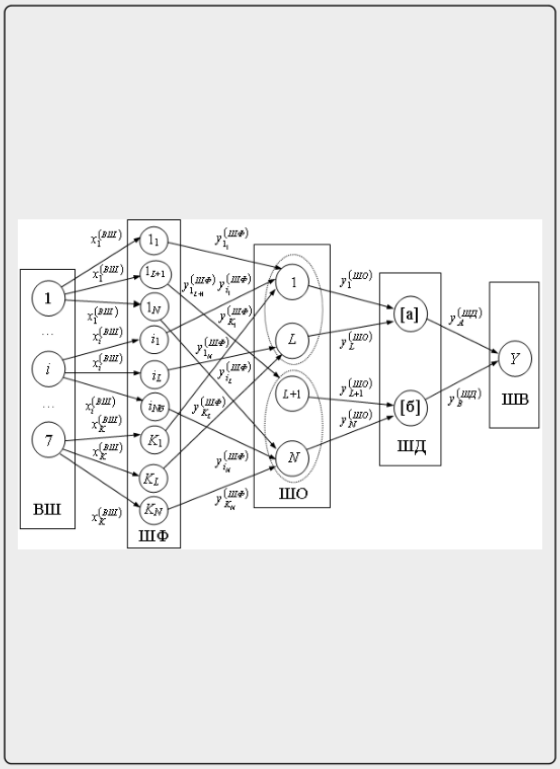


КОНЦЕПТУАЛЬНА МОДЕЛЬ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ІКМ



- Концептуальна модель поєднує моніторинг параметрів мережі, аналіз загроз, нейромережеве оцінювання та механізм управлінського впливу.
- Функціонування моделі орієнтоване на забезпечення конфіденційності, цілісності та доступності інформації.
- Запропонований підхід формує основу для адаптивної СУІБ інформаційно-комунікаційної мережі.

РОЗПІЗНАВАННЯ НЕСТРУКТУРОВАНИХ ДАНИХ У СИСТЕМІ КІБЕРБЕЗПЕКИ



- Неструктуровані дані можуть містити журнали подій, текстові повідомлення, сигнатури інцидентів та інші ознаки порушення безпеки.
- Нейромережева модель дозволяє класифікувати такі дані та виявляти нетипові патерни поведінки.
- Результати розпізнавання використовуються для формування інтегральної оцінки захищеності ІКМ.

ФУНКЦІОНАЛЬНІ ЗАВДАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

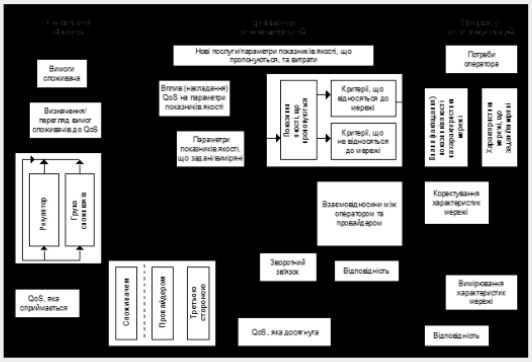
- Постійний моніторинг показників якості функціонування інформаційно-комунікаційної мережі.
- Виявлення відхилень, аномалій і потенційних ознак несанкціонованого доступу.
- Класифікація рівня небезпеки подій та формування пріоритетів реагування.
- Підтримка вибору управлінських рішень на основі інтегральної оцінки стану безпеки.
- Адаптація політик захисту відповідно до зміни стану мережі та характеристик загроз.

ПРАКТИЧНА ЦІННІСТЬ ЗАПРОПОНОВАНОГО ПІДХОДУ

- Застосування нейроструктурних технологій підвищує точність оцінювання стану інформаційної безпеки ІКМ.
- Модель дозволяє швидше виявляти проблемні зони та прогнозувати погіршення якості функціонування мережі.
- Інтелектуальна підтримка рішень знижує залежність від ручного аналізу великого обсягу мережевих даних.
- Запропонований підхід може бути використаний для розвитку адаптивних систем кіберзахисту об’єктів інформаційної діяльності.

ОЧІКУВАНІ РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ НЕЙРОСТРУКТУРНОЇ МОДЕЛІ

- Підвищення ефективності СУІБ досягається за рахунок поєднання моніторингу, аналізу, прогнозування та керуючого впливу.
- Модель забезпечує системне узгодження показників якості мережі з показниками інформаційної безпеки.
- Результатом є більш стійке функціонування ІКМ в умовах зміни навантаження та кіберзагроз.



ЗАГАЛЬНІ ВИСНОВКИ

- Проведено аналіз систем оцінювання якості функціонування інформаційно-комунікаційних мереж та визначено ключові показники їх роботи.
- Досліджено напрями удосконалення системи управління інформаційною безпекою з використанням нейроструктурних технологій.
- Обґрунтовано доцільність застосування нейронних мереж для обробки статистичної та неструктурованої інформації про стан ІКМ.
- Розроблено концептуальну модель управління кібербезпекою інформаційно-комунікаційної мережі на основі нейроструктурного підходу.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Володимир НЕТЬОСА

ема: система інформаційної безпеки ІКМ на основі нейроструктурних технолог

Київ - 2026