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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту мережевих каналів передачі інформації від несанкціонованого доступу на основі нейронних 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
_____ Олександр ТУРЧИН

Виконав: здобувач вищої освіти групи СЗДМ 61
Олександр ТУРЧИН

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

Турчину Олександру Анатолійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система захисту мережевих каналів передачі інформації від несанкціонованого доступу на основі нейронних технологій»
керівник кваліфікаційної роботи ПОНОЧОВНИЙ Петро, доктор філософії
(ПРІЗВИШЕ 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: опорний об'єкт інформаційної діяльності, інформаційно-комунікаційні канал витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні мережеві засоби захисту інформації від несанкціонованого витоку, програмно-технічні засоби електронного документообігу.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
4.1. Огляд процесів формування каналів несанкціонованого проникненню в інформаційні канали передачі даних об'єкту інформаційної діяльності
4.2. Аналіз можливостей застосування нейронних технологій для запобігання несанкціонованого проникненню в інформаційні канали передачі даних
4.3. Дослідження процесів та розробка методів застосування нейронних технологій для запобігання несанкціонованого проникнення в інформаційні канали передачі даних

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 _____ Олександр ТУРЧИН
(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 75 сторінок, має 20 рисунків, 4 таблиці. Список використаних джерел містить 38 найменувань і займає 4 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи запобігання несанкціонованого проникненню в інформаційні канали передачі даних об'єкту інформаційної діяльності на основі нейронних технологій.

В кваліфікаційній роботі проведено огляд процесів формування каналів несанкціонованого проникненню в інформаційні канали передачі даних об'єкту інформаційної діяльності. Проаналізовано можливості застосування нейронних технологій для запобігання несанкціонованого проникненню в інформаційні канали передачі даних. Досліджено процеси та розроблено методи застосування нейронних технологій для запобігання несанкціонованого проникнення в інформаційні канали передачі даних.

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: НЕЙРОННА МЕРЕЖА, ІНФОРМАЦІЙНО - КОМУНІКАЦІЙНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ, ІНТЕЛЕКТУАЛЬНІ ЗАСОБИ ЗАХИСТУ 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 75 pages, has 20 figures, 4 tables. The list of sources used contains 38 items and takes up 4 pages.

The purpose of the qualification work is to increase the efficiency of the system for preventing unauthorized penetration into the information channels of data transmission of an information activity object based on neural technologies.

The qualification work reviews the processes of forming channels for unauthorized penetration into the information channels of data transmission of an information activity object. The possibilities of using neural technologies to prevent unauthorized penetration into the information channels of data transmission have been analyzed. The processes and methods of using neural technologies to prevent unauthorized penetration into the information channels of data transmission have been studied.

Approbation

O.A. Turchin, V.I. Netyosa, E.O. Kravchenko, Methods, methods and advantages of the 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 information and communication systems security. Kyiv, November 5, 2025, Kyiv: DUIKT Research and Development Center. – 2025. P.39-40. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: NEURAL NETWORK, INFORMATION AND COMMUNICATION CHANNEL OF INFORMATION OUTPUT, INTELLECTUAL INFORMATION PROTECTION MEANS

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

Внаслідок широкого використання комп'ютерів в інформаційних центрах створюється багато каналів незаконного розкриття інформації. Ці канали негативно впливають на цілісність та конфіденційність інформації. Сьогодні розроблені ефективні методи швидкого та ефективного отримання інформації щодо наявності певного каналу витоку інформації. Як результат, сьогодні створені інтелектуальні методи вимірювання ступеня безпеки інформації. По суті, інтелектуальні засоби захисту інформації використовуються в інформаційних системах, метою яких є розпізнавання потенційних витоків інформації як розумного інструменту, ці системи зазвичай використовують нейронні мережі, нечітку логіку та системи на основі правил.

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи запобігання несанкціонованого проникненню в інформаційні канали передачі даних об'єкту інформаційної діяльності на основі нейронних технологій.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

- проведено огляд процесів формування каналів несанкціонованого проникненню в інформаційні канали передачі даних об'єкту інформаційної діяльності.

- проаналізовано можливості застосування нейронних технологій для запобігання несанкціонованого проникненню в інформаційні канали передачі даних.

- досліджено процеси та розроблено методи застосування нейронних технологій для запобігання несанкціонованого проникнення в інформаційні канали передачі даних.

Об'єкт дослідження. Система захисту конфіденційної інформації об'єкту інформаційної діяльності.

Предмет дослідження. Система запобігання несанкціонованого проникненню в інформаційні канали передачі даних об'єкту інформаційної діяльності.

Розділ 1.
ПРОЦЕСИ ФОРМУВАННЯ КАНАЛІВ НЕСАНКЦІОНОВАНОГО ПРОНИКНЕННЮ В ІНФОРМАЦІЙНІ КАНАЛИ ПЕРЕДАЧІ ДАНИХ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.4 Характеристика каналів витоку інформації в інформаційній мережі об'єкту інформаційної діяльності

Технічний канал втрати інформації вважається сукупністю джерел інформації, ліній зв'язку (фізичних носіїв), якими поширюється інформація, а також шумів, що перешкоджають передачі сигналу в лініях зв'язку, та технічних методів захоплення інформації.

Джерелами інформації можуть бути безпосередньо людські ресурси, гучномовці, звукові системи, що доповнюються друкованими документами, радіопередавачами або іншими пристроями.

Сигнали використовуються для передачі інформації. Сигнали зазвичай являють собою електричні, магнітні, голосові та інші види коливань (хвилі), інформація присутня у змінах їх параметрів.

Залежно від природи сигналу, він може поширюватися в певному фізичному середовищі. Зазвичай середовищем для поширення є повітря, рідке або тверде тіло. До них належать: повітряний простір, будівельні конструкції, з'єднувальні лінії та інші провідні компоненти, ґрунт (земля) тощо.

Звук пов'язаний з усіма фізичними процесами та присутній на вході до засобів збору інформації.

Пристрої перехоплення інформації використовуються для прийому та перетворення сигналів з метою отримання інформації.

1.2 Механізми утворення каналів витоку інформації

Зрозуміло, що інформація передається через поле або речовину. Це або слухова хвиля (звук), або електромагнітне випромінювання, аналогічне сонцю, або письмовий текст.

Як результат, фізичними засобами можливі такі методи передачі інформації:

- світлові промені;
- звукові хвилі;
- хвилі електронного маркетингу
- речовини та матеріали.

Використовуючи свої ресурси, такі як фізичне середовище, люди створюють певну систему передачі інформації один одному. Такі системи зазвичай називають системами зв'язку. За своєю конструкцією система зв'язку має джерело інформації, передавач, канал передачі інформації, приймач та одержувач інформації. Подібно до каналу передачі інформації, існує також канал для розкриття інформації. Він також складається з генератора сигналу, фізичного середовища для його поширення, але з приймальними пристроями на стороні зловмисника. Рух інформації в цьому каналі обмежений одним напрямком: від джерела до зловмисника.

Технічні канали розкриття інформації – фізичний маршрут від джерела інформації до зловмисника, цей маршрут дозволяє несанкціонований доступ до захищеної інформації.

Джерелом інформації (об'єктом розвідки) є технічні засоби обробки інформації (ОТЗС, ДТЗС), комп'ютери, лінії зв'язку та людське мовлення. Будь-який з перелічених типів інформації поширюється в будь-якому середовищі (повітря, інженерні комунікації, лінії зв'язку або огороджувальні конструкції), при цьому на саме середовище впливають різні перешкоди (наприклад, надмірний шум у приміщенні, електромагнітні перешкоди тощо). Зрештою, кінцевою точкою буде приймач сигналу (детектування ПЕМВН, акустичне

детектування мовлення, детектування електричних сигналів, пов’язаних з діапазоном частот мовлення). Виявивши ці компоненти, можна візуалізувати маршрут походження інформаційного сигналу через середовище існування до приймача сигналу. Тобто, канал витоку технічної інформації – це поєднання об’єкта технічної розвідки, фізичного місця поширення інформації та способу захисту інформації.

Для виникнення (формування, встановлення) каналу витоку інформації необхідні певні просторові, енергетичні та часові атрибути, а також відповідні засоби виявлення та фіксації інформації на стороні жертви.

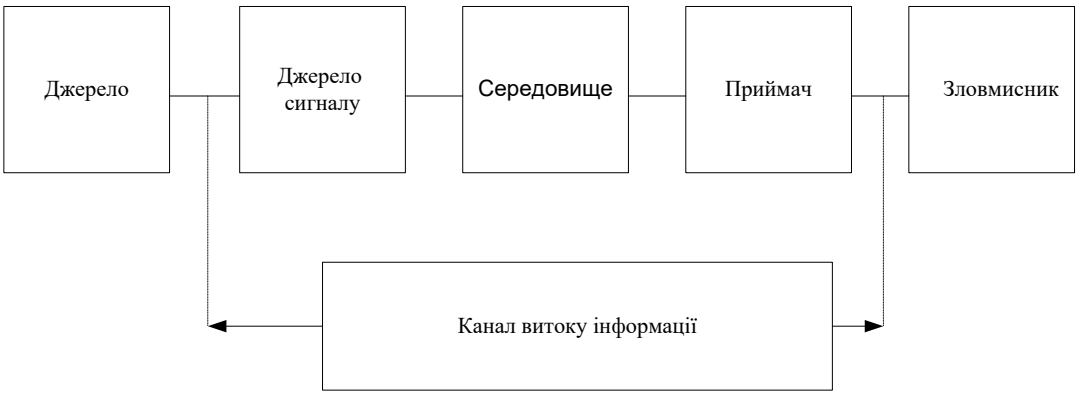


Рисунок.1.1 Структура каналу витоку інформації

1.3 Класифікація каналів витоку інформації на об’єкті інформаційної діяльності

За фізичним описом витоки інформації поділяються на такі категорії:

- візуальні: спостереження та передача інформації у видимому та інфрачервоному спектрі;

- акустичні (включаючи акустичне перетворення): поширення звукових хвиль у будь-якому звукопереносному каналі;

- магнітні: індукція напруги та струмів у різних магнітних комунікаціях;

- радіочастотні: радіочастотне випромінювання в радіообласті;

- матеріальні (папір, друковані матеріали, магнітні носії, промислові відходи різних типів – тверді, рідкі, газоподібні).

Основним візуальним каналом передачі інформації є світло або випромінювання. Залежно від діапазону відстаней, візуально-оптичні шляхи втрати інформації можуть бути створені:

- у видимій частині спектра.
- в інфрачервоній області;
- в ультрафіолетовій області.

Для побудови каналу витоку інформації, який візуалізує інформацію, джерело інформації повинно мати такі властивості:

- відповідне кутове вимірювання;
- відповідну величину яскравості або контрастності.

Візуальна інформація, що просочується через оптичну систему, класифікується:

За природою створення:

- через відбиття світлової енергії,
- через власне радіоактивне випромінювання об’єкта.

За кількістю випромінювання:

- видима область, інфрачервона, ультрафіолетова.

За способом поширення:

- вільний простір навколо напрямних ліній.

Оптичні методи є частиною найдавнішої форми інтелекту, до них належать: візуальне спостереження, фотографування та відеозйомка.

Візуально-оптичні канали формуються як шлях для оптичної інформації від інформаційного об’єкта до її цільового одержувача. Це вимагає енергії, часу та простору, а також відповідних технологічних ресурсів. Створення цих каналів сприяє таким властивостям самого інформаційного об’єкта: його відповідний розмір, власна яскравість та контрастність. Унікальна цінність цієї інформації полягає в тому, що вона є одночасно точною та оперативною, вона здатна служити документальним доказом отриманої інформації.

Причиною створення акустичного каналу є коливання або вібрації тіл та механізмів, таких як голосові зв'язки людини, деталі механічних пристроїв, телефони, апаратура відтворення звуку тощо.

Вібрації людського голосу та інші звуки створюють акустичні хвилі, які, поширюючись у просторі та взаємодіючи з перешкодами, викликають на них різний тиск (двері, вікна, стіни, підлоги та різні пристрої). Ці коливання змушують їх коливатися. Впливаючи на спеціальні прилади (мікрофони), індуковані звуком коливання створюють у них пов'язану електромагнітну хвилю, яка передається на відстань і несе інформацію, створену індукованим звуком коливаннями.

Акустичні коридори утворюються:

- шляхом поширення акустичних (механічних) коливань у вільному просторі без суцільної стіни (переговори у відкритому просторі, в приміщеннях з відкритими вікнами, вентиляційними отворами, дверима та витоками через вентиляційні канали);

- через коливання, спричинені звуком, у конструкціях та компонентах будівель, це призводить до їх трясіння (стіни, стелі, підлоги, вікна, двері, вентиляція, водопостачання, опалення та кондиціонування).

- Через коливання звуку на технологічних засобах обробки інформації (таких як мікрофони, акустичні модулятори тощо).

Електромагнітні канали, за своїми фізичними характеристиками та експлуатаційними властивостями технічних засобів, що сприяють виробничій діяльності, є найнебезпечнішими та найпоширенішими каналами для інформації. Ці канали виникають через наявність шкідливих джерел у технічних компонентах, що використовуються у виробництві. Спочатку ці джерела є пристроями, які перетворюють одну фізичну характеристику на іншу. В електроніці перетворювач – це пристрій, який перетворює фізичну величину, яка не є електричною, на цифровий або аналоговий сигнал, або навпаки. Добре розуміння роботи процесорів дозволяє ідентифікувати потенційні ненавмисні фізичні поля, які передають інформацію (передача). Крім того, враховуючи

технічну природу рішень, електронні схеми, що їх реалізують, та інформацію, яка створюється або викрадається хакерами, всі вони потенційно вразливі до певних каналів витоку інформації (передачі). Як наслідок, будь-яка технологічно обґрунтована обробка або передача інформації створює ризик її ненавмисного вивільнення (передачі).

Матеріальні та матеріальні канали передачі інформації формуються шляхом розслідування відходів виробництва (знищених документів або їх частин, недосконалих чернеток різного роду нотаток, записів, листів тощо), крадіжки, незаконного ознайомлення, відтворення, фотографування та запису документів, зразків технічних або програмних засобів, креслень.

Причинами утворення каналів витоку інформації по радіо можуть бути: технічна база об’єкта недосконала; схемні рішення недосконалі; об’єкт працює та має ознаки зносу, а старіння об’єкта є кримінальним.

Було досліджено фізичне середовище різних перетворювачів та випромінювачів з метою визначення:

Елементи, вузли та технічні засоби, що гарантують виробництво та використання, вважаються небезпечними.

Кожне джерело небезпечного сигналу, яке відповідає певним умовам, може створити канал витоку технічної інформації.

Кожна електронна система містить набір компонентів, вузлів та провідників, а також має певний набір каналів для витоку технічної інформації.

Маючи знання про різні методи формування радіоканалу витоку інформації, ми можемо обговорити основні типи інформації, що є витоком.

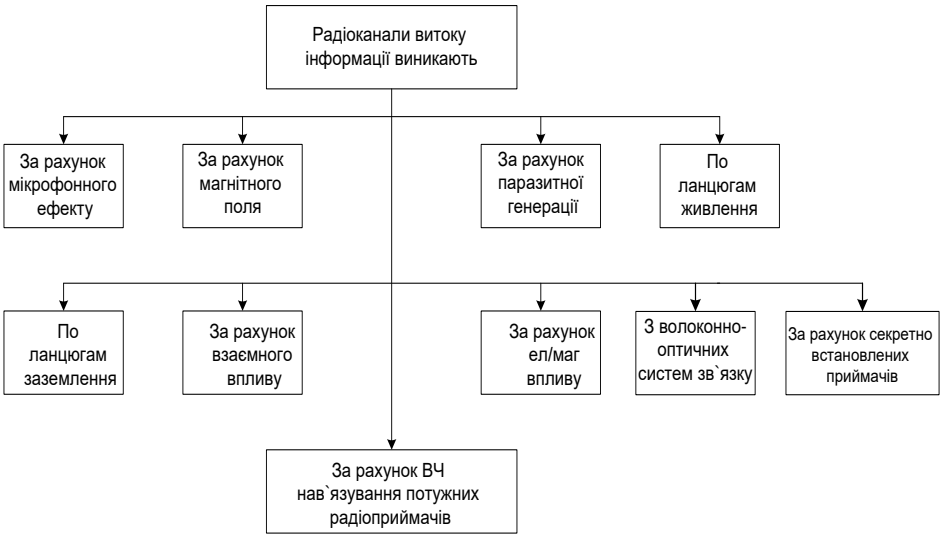


Рисунок 1.2. Структура радіоканалів витоку інформації

Рисунок 1.3 Класифікація радіоканалів витоку інформації

1.4 Способи та методи протидії витоку конфіденційних даних інформаційно – комунікаційними каналами

Щоб запобігти витоку інформації, необхідно вирішити такі питання.

- розробка системи безпеки для об’єкта;

- проектування є відкритим та прозорим, що дозволяє забезпечити секретність та розміщувати конфіденційну інформацію на об’єкті.

- запобігання виявленню;

- боротьба з підслуховуванням голосу часу;

- захист від зловмисних дій злочинців.

Об’єкт, який виконує роботу з персональною інформацією конфіденційно, зазвичай має кілька рівнів захисту:

1) територія, що контролювалася;

2) будівництво;

3) база;

4) пристрій, носій передачі інформації;

5) програмне забезпечення;

6) інформаційні активи.

За допомогою СПБ створюється система безпеки об’єкта, яка запобігає проникненню неавторизованих осіб на територію або приміщення об’єкта без дозволу.

Склад системи базується на об’єкті, що охороняється. Як правило, СПБ матиме такі компоненти:

- будівництво споруд;

- сповіщення про безпеку;

- камери відеоспостереження;

- доступ до підсистеми через об’єкт.

Беручи до уваги візуальний канал передачі інформації, визнаються такі методи боротьби з передачею інформації:

- двері будівлі були опечатані;

- Організація столів та комп’ютерів таким чином, щоб документи не можна було побачити.

- Той, хто має конфіденційну інформацію, повинен носити капюшон.

Традиційно стратегії запобігання розголошенню інформації поділяються на технічні та інституційні. Технічні та організаційні заходи застосовуються для запобігання витоку інформації через можливість розголошення інформації за допомогою спеціальних технічних засобів, встановлених на конструктивних елементах будівель, приміщень та інших технічних засобів. Технічні заходи – це дії, що запобігають використанню спеціального обладнання, екранованого від побічного випромінювання, під час виробництва конфіденційної інформації.

1.5 Висновки по розділу

У розділі описано процедури створення каналів несанкціонованого розголошення даних в інформаційно-комунікаційних каналах цільової інформаційної діяльності.

1. Описано ознаки каналів витоку інформації та обговорено методи їх створення.

2. Проведено категоризацію каналів витоку інформації, а також розглянуто методи та теорії витоку персональних даних через інформаційно-комунікаційні канали.

Розділ 2.
ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ІНФОРМАЦІЙНО – КОМУНІКАЦІЙНИМИ КАНАЛАМИ

2.1 Метод оцінки рівня захищеності інформації з застосуванням нейронних технологій

Метод якісної оцінки ступеня безпеки інформації базується на результатах вимірювань та експертних оцінок. Ці оцінки мають фундаментальні недоліки, що спричиняють низький ступінь безпеки інформації. Існує два методи розгортання інструментів захисту нейронних мереж. Перший варіант полягає у використанні існуючих або змінених експертних систем, тобто вони використовуються як заміна існуючих компонентів статистичного аналізу. Це полегшує використання нейронних мереж для зменшення вхідних даних, які можуть свідчити про зловживання, а потім спрямування події до експертної системи. Другий метод полягає у використанні нейронної мережі як автономної системи оцінки безпеки інформації. У цій конфігурації нейронна мережа отримує весь трафік та оцінює інформацію щодо наявності негативних наслідків, пов’язаних зі злочинцем. На відміну від експертних систем, які можуть надати конкретну відповідь щодо зв’язку між аналізованими та збереженими в базі даних даними, нейронна мережа натомість аналізує інформацію та надає можливість оцінювати узгодженість даних з характеристиками, які вона може розпізнати. Спочатку нейронна мережа структурується шляхом розпізнавання попередньо вибраних об’єктів у предметній області. Оцінюється відгук нейронної мережі, і система проектується для досягнення бажаного результату.

Фундаментальним питанням є невизначеність завдання і, як наслідок, складність рішень, що виникають в результаті, якість яких залежить від кваліфікації та підготовки експертів. Іншим методом оцінки є кількісний, цей підхід наразі популярний серед фахівців.

Через швидкі темпи розвитку інформаційних технологій, збільшення кількості інформаційних загроз, ступінь неоднозначності, пов’язаний з їх виникненням та реалізацією, а також складність систем інформаційної безпеки та їх спеціалізований характер, актуальним стає завдання отримання узагальнюючої оцінки ступеня інформаційної безпеки на основі методології, яка враховує як кількісні, так і якісні показники.

Інформацію, що виражається мовленням, можна назвати усною інформацією, інформацію, що обробляється, можна зберігати на носіях інформації (таких як папір, магнітні картки та електронна техніка). Причинами витоку інформації є базові недосконалості технічних об’єктів, недосконалості схемних рішень та недосконалості конструкції виробу. Крім того, експлуатаційний знос та старіння об’єктів обробки інформації, а також злочинні дії сприяють утворенню витоків інформації.

Залежно від способу представлення інформації формуються технічні шляхи витоку інформації.

- візуальні: спостереження та передача інформації у видимому та інфрачервоному спектрі;

- акустичні (включаючи акустичні): поширення звукових хвиль у будь-якому звукоутворюючому каналі;

- електричні: індукція напруги та струму в різних комунікаціях, що є провідними;

- радіочастотні: радіочастотне випромінювання в радіообласті;

- матеріальні (папір, друковані матеріали, магнітні носії, промислові відходи різних типів – тверді, рідкі, газоподібні).

Для розуміння наслідків інформаційної безпеки важливо врахувати всі можливі технічні шляхи втрати інформації, стан конкретного шляху відповідатиме стану інформаційної безпеки щодо певного типу загрози.

До складу нейронної мережевої системи (НСС) для вимірювання ступеня інформаційної безпеки входять m-нейрони (шари), які визначаються кількістю станів інформаційної безпеки відповідно до певного типу загрози. Стан безпеки

дорівнює нейронному шару, а кількість класів визначається параметрами, які визначаються (вимірюються) та порівнюються зі стандартами з метою визначення ступеня інформаційної безпеки, пов'язаного з кожним технічним каналом витоку, згідно з розробленою моделлю інформаційних небезпек.

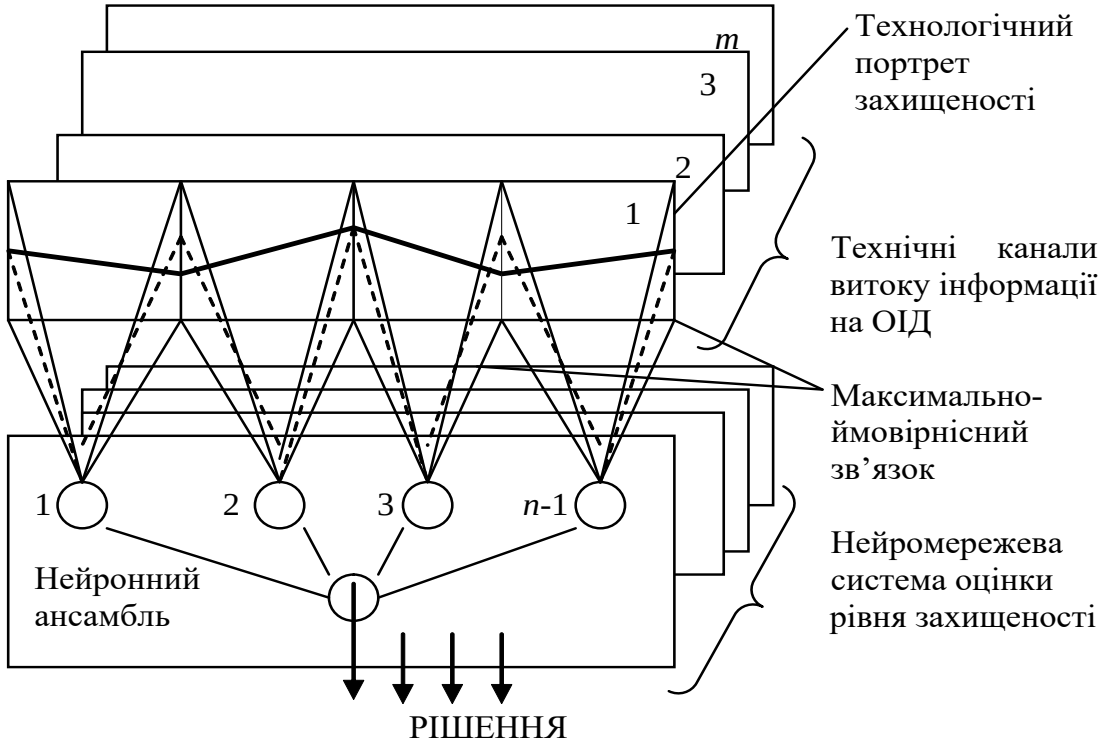


Рис. 2.1 Застосування нейронної мережі для оцінки рівня захищеності інформації

В результаті опитування та початкової оцінки безпеки щодо кожного можливого технічного каналу ми маємо матриці розміром n × Ml, де Ml – загальна кількість загроз, пов'язаних з l-м технічним каналом, а n – кількість контрольних точок, визначених дослідженням OID щодо наявності каналу витоку інформації, m – технічні канали потоку інформації.

Кількість нейронів у шарі базується на об'ємі статистичної сукупності. І навпаки, великі вибірки, що мають велику кількість, збільшують розмірність простору технічних станів, представлених діагностичним портретом (набором симптомів), тоді як малі вибірки не забезпечують чіткого зв'язку між

симптомами та діагнозом. Оптимальний портрет діагнозу – це той, який забезпечує необхідну кількість діагностичної інформації. У цьому випадку обсяг статистичної вибірки залежить від кількості контрольних точок, пов’язаних з об’єктом діагностики – об’єктом інформаційної діяльності. Як наслідок, кількість нейроноподібних компонентів у нейронному ансамблі залежить від діагностичного опису (набору симптомів) та контрольних точок в об’єкті керування. Набір нейронних колекцій (шарів) являє собою нейронну мережу. Ці діагностичні НМ є скороченою версією марковської моделі. Однак вони мають додаткові властивості, що нагадують властивості біологічних систем.

Набір розпізнаних технічних станів та сил, що беруть участь в об’єкті керування (ОК), можна зобразити як динамічну систему. Ці зміни зображуються як такі, що відбуваються негайно, називаються подіями та представлені за допомогою діагностичних портретів. Цей термін, який описує пов’язані поняття фізичного, інформаційного та виробничого характеру, вважається станом володіння певною технічною конфігурацією або станом. Це досягається за допомогою динамічної мережі, розподіленої по кількох станах. Еволюційні зміни, що відбуваються між подіями, не враховуються, і передбачається, що динаміка системи є дискретною між подіями. Цей тип системи називається дискретно-подійною.

Дискретно-подійні системи (ДПСП) можна представити лише за допомогою логічних, алгебраїчних або функціональних моделей. Математичний інструмент для опису ймовірнісних моделей, що стосуються роботи ДПСП, базується на марковських полях (лініях). Таке математичне представлення чисел полегшує опис функціонування DESS як зовнішнього компонента та має бути відображено в структурі детермінованої частини NMS TD.

Кількість станів DESS базується на точності кусково-константної апроксимації неперервного фазового шляху динамічного об’єкта. Збільшення точності кусково-константної апроксимації фазового прогресу неперервної системи вимагає додавання великого технічного простору станів A, що збільшує складність аналітичного опису. Шлях до виходу – це потенціал для збільшення

(склеювання) станів, що є переходом від простору конфігурацій до простору станів. Нові макростани можна отримати з комбінації попередніх технічних станів наступним чином:

$$B_к = \sum_{j \in \{K\}} A; k = 1,..., p;\ j = 1,..., r;\ p < r \quad , \tag{2.1}$$

де $\{K\}$ - множина індексів станів $\{A_j\}$ об'єднаних у B_K.

Зовнішнє середовище нейронної мережевої системи (НСС) технічного аналізу можна описати як набір розпізнавання дискретно-подійних систем, пов'язаних з різними технічними станами.

Дискретно-подійні системи, що мають пов'язані дискретні технічні стани.

Загальне представлення технологічної проблемно-орієнтованої НСС у технічному стані (рис. 3.2).

Загальна структура проблемно-орієнтованої нейронної мережевої системи, призначеної для технічної майстерності:

- сенсорна матриця, яка розпізнає інформацію про поле Маркова як набір сприйнятих спостережень;

- набір нейронних груп (класифікаторів), кількість класів яких дорівнює M;

- нейронне поле, яке враховує попередні знання у вигляді значень ймовірностей гіпотез P;

- нейронне поле, яке враховує значення компонентів платіжної матриці C;

- мажоритарна мережа, яка визначає розпізнавання G.

- компонент (компонент) навчальної системи, що має менший обсяг.

Отримавши необхідну кількість інструментальних вимірювань та спеціальних досліджень для кожного з каналів витоку технічної інформації на OID, необхідно створити процедуру автоматичного отримання інформації про ступінь безпеки кожного з каналів відповідно до затвердженої моделі загрози.

Технічні атрибути інтерпретуються матрицею датчиків як набір спостережень:

$$X = (X_1, X_2, ..., X_i, ..., X_m), \tag{2.2}$$

$i = 1,2,\ldots,n$.

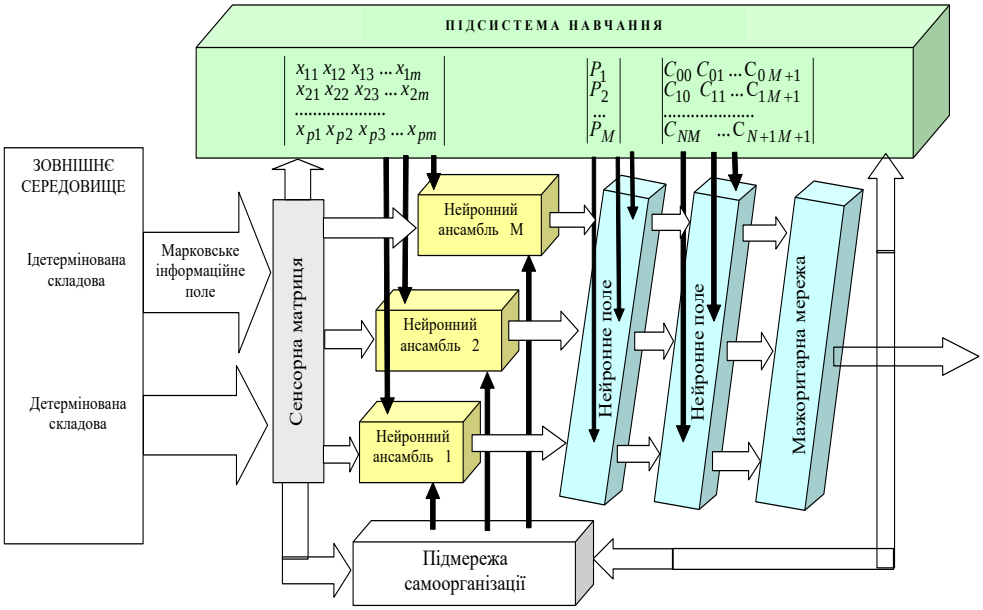


Рис. 2.2. Узагальнена модель проблемно-орієнтованої нейромережевої системи

В окремому сеннннсорнному канналі відбувається редукція вибіркового простору X, у результаті якої маємо послідовнність дискретнних змінннних U_k, $k = 0,1,\ldots,n\text{-}1$, які приймають знначеннння $Z_1, Z_2,\ldots,Z_r$.

Ннеобхіднно синнтезувати структуру ннейроподібнного класифікатора, що реалізує вирішальнну фуннкцію $\gamma(U)$ нна скороченному вибірковому просторі U.

Послідовнність дискретнних змінннних U_r, $k = 0,1,\ldots,n\text{-}1$, які приймають знначеннння z_a, $a = 1,2,\ldots,r$, можнна апроксимувати векторами Ξ, $\Phi(0)_\mu$ та Ξ, $\Phi(k)_\mu$.

Використовуючи векторнні познначеннння, можнна записати:

$$ln1_\mu = (\Xi, \Phi(0)_\mu) + (\Xi, \Phi(k)_\mu) = |\Xi||\Phi(0)_\mu| \cos(\Xi \hat{} \Phi(0)_\mu) + |\Xi|, |\Phi(k)_\mu| \cos((\Xi \hat{} \Phi(k)_\mu)),$$

(2.3)

де $|\Xi||\Phi(0)_\mu|, |\Phi(k)_\mu|$ - модулі векторів Ξ, $\Phi(0)_\mu$, $\Phi(k)_\mu$;

$(\Xi \hat{} \Phi(0)_\mu)$, $(\Xi \hat{} \Phi(k)_\mu)$ - кути між цими векторами.

Наведене вище твердження повністю визначає оптимальний склад класифікатора для заданих j та i. Це полегшує інтерпретацію функціонування зібраної структури. В результаті, кожному колективу надається однаковий вектор стимуляції. Збірки мають різні рівні ефективності щодо своїх зв'язків. Якщо довжини векторів у всіх ансамблях однакові, то величина збудження ансамблю при заданій константі залежатиме лише від кутів між цими векторами. Це означає, що ансамбль є найбільш збудженим, вектори Ф(0) та Ф(k) перпендикулярні до вектора. Вибір здійснюється за номером найбільш збудженого колективу.

Склад найпростішої нейроподібної діагностичної системи являє собою набір з M+1 окремих нейронних мереж, які складають перший шар. Ансамбль складається з n-нейронів, їхній потенціал збудження описується як

$$Y_\mu(k) = \sum_{a=1}^{n} \Xi a(k) \Phi_a(k)_\mu, \quad (2.4)$$

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 еквівалентні, нейрон, який використовує метод позначених ліній, має пріоритет над синаптичними зв'язками. 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.

$$Y_{\mu}(k) = \sum_{a=1}^{r} \Xi a(k) \Phi_a(k)_{\mu} - \Theta_a(k)_{\mu} = \sum_{a=1}^{r} \Xi a(k) \Phi_a(k)_{\mu} \quad . \tag{2.5}$$

При $\Theta_a(k)_{\mu} = 0$ структура системи, що розпізнає, є квазілінійною, а при $\Theta_a(k)_{\mu} \rangle 0$ вона має нелінійні граничні властивості.

Для кожного технічного каналу в множині {ml}TKVI необхідно визначити його значення.

Незважаючи на невідповідність у кількості небезпек згідно з [5], які визначають кожен можливий технічний маршрут, це число не описує ступінь небезпеки, пов'язаної з самим технічним маршрутом. Як наслідок, важливість кожного каналу повинна визначатися відношенням 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:

$$\lambda_l = \frac{M_l^1}{M_l}, \quad l = \overline{1, L}, \tag{2.6}$$

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, . Терапевтичний вхід з вищим числом пов'язаний з параметром технічного каналу, який має вище значення.

Важливо ранжувати технічні канали за їхньою важливістю, а потім створити список усіх можливих каналів витоку технічної інформації на OID: {ml}*TKVI,

Під час вирішення питань, пов’язаних з оцінкою інформаційної безпеки, спочатку необхідно оцінити ступінь відповідності отриманих сигналів (портретів технологічної безпеки – результатів інструментальних вимірювань та спеціалізованих досліджень щодо кожного каналу витоку технічної інформації) еталонним, що дозволить визначити відповідний критерій прийняття рішення. Метод вимірювання відповідності відрізняється залежно від характеру проведених досліджень. Як наслідок, рішення про те, чи захищати систему від втрати інформації, наприклад, акустичним, віброакустичним або акустоелектричним способом, приймається після порівняння системи зі стандартами в системі технічного захисту України.

Другий шар нейронів у групі відповідає за функціонування

$$\ln l_{\mu}(k) = \sum_{k=0}^{n} Y_k(k) \quad . \tag{2.7}$$

Він з’єднаний з першим шаром проекційними зв’язками, що відповідають співвідношенню один до одного між нейронами в різних полях, що дозволяє передавати інформацію про стан з одного поля в інше.

Інформаційним вхідним сигналом для третього шару нейронів є вектор. Він функціонує як комп’ютер загального призначення.

Вирази (3.1) та (3.2) повністю описують структуру системи, яка розпізнає технічний стан мережі. Обговоримо матрицю зв’язків між k-тою групою датчиків та k-тим нейроном, яка складається з рівнів стимуляції:

$$\Xi = \begin{pmatrix} \Xi_1 \\ \Xi_1 \\ \cdots \\ \Xi_{\kappa} \end{pmatrix}.$$

Введемо також поняття коефіцієнта міжнейронного зв’язку S в ансамблі (у шарі),

$$S_{kl} = \begin{cases} 1, \text{ якщо є : зв'язок між k-ою групою рецепторів.} \\ i \quad \text{якщо існує : 1-й нейрон.} \\ 0, \text{ у зворотному випадку} \end{cases} \tag{2.8}$$

Утворимо матрицю міжнейронних зв'язків, склавши її з коефіцієнтів міжнейронних зв'язків:

$$S = \begin{pmatrix} S_{00} & S_{01} & \cdots & S_{0n-1} \\ S_{10} & S_{11} & \cdots & S_{1n-1} \\ \cdots & \cdots & \cdots & \cdots \\ S_{n-1} & S_{nn} & \cdots & S_{n-1n-1} \end{pmatrix}, \tag{2.9}$$

Матриці Ξ_k і S цілком визначають структуру зв'язків в ансамблі. Для випадку $Y = 0$ матриця S перебудовується в діагональну з розмірністю $n \times n$.

Синтезовані структури припускають фіксований об'єм вибірки, тобто система, що розпізнає, спостерігає відразу всю фазову траєкторію.

Інформаційне поле сприймається сенсорною матрицею у вигляді сукупності спостережень:

$$X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1i} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2i} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{p1} & x_{p2} & \cdots & x_{pi} & \cdots & x_{pn} \end{pmatrix}. \tag{2.10}$$

Кожен стовпчик $x_i = (x_{i1}, x_{j2}, \ldots, x_{pi}),\ i = 1,2,\ldots,n$ і рядок $x_j = (x_{j1}, x_{j2}, \ldots, x_{jI}),\ j = 1,2,\ldots,p$ матриці X є відповідно n і p – мірні вектора процесів.

Можливі $M+1$ гіпотеза $H_0, H_1, \ldots, H_\mu, \ldots, H_M$ про належність спостерігаючого інформаційного поля μ-го класу. Відомі апріорні ймовірності гіпотез $P = P\{H_\mu\},\quad \mu = 0,1,\ldots,M$. Відома також платіжна матриця:

$$C = \begin{pmatrix} C_{00} & C_{01} & C_{02} & \cdots & C_{0M+1} \\ C_{10} & C_{11} & C_{12} & \cdots & C_{1M+1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ C_{M+10} & C_{M+11} & C_{CM+12} & \vdots & C_{M+1M+1} \end{pmatrix}, \quad (2.11)$$

елемент C_{jm} якої є платою за рішення γ_μ, коли істинною була гіпотеза H_j, $j = \mu = 0,1,\cdots,M$. Простір рішень $\Gamma = (\gamma_0, \gamma_2, \ldots, \gamma_M)$ складається з $M+1$ елемента, де γ_μ - рішення прийняти гіпотезу H_μ. Задача системи розпізнавання заключається в тому, щоб за результатами спостереження прийняти одну з гіпотез і відхилити інші. Середній ризик при ухваленні рішення визначається таким чином:

$$R = \sum_{j=0}^{m}\sum_{\mu=1}^{m} C_{j\mu} P_j \int_{G_\mu} w(x_1, x_2, \ldots, x_m)\, H_0 / X \quad . \quad (2.12)$$

Мінімальне значення середнього ризику досягається у тому випадку, якщо до області G_μ ухвалення рішення γ_μ РС віднесе точки X вибіркового простору, що задовольняють системі нерівностей:

$$\sum_{j=1}^{M} (C_{ij} - C_{jm}) \frac{P_i w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_i}{P_0 w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_0} \geq C_{0\mu} - C_{0j} \quad (2.13)$$

Якщо ввести вектор відносин правдоподібності

$$l(x) = [l_0(x), l_1(x), l_\mu(x), \ldots, l_m(x)],$$

де $l_\mu = \dfrac{w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_\mu}{w(x_1, x_2, \ldots, x_i, \ldots, x_m)/ H_0}$, тоді систему нерівностей (3.8) можна представити у виді:

$$\sum_{j=1}^{M} (C_{ij} - C_{jm}) \frac{P_i}{P_0} l_i(x) \geq C_{0\mu} - C_{0j} \quad . \quad (2.14)$$

Вектор містить всю інформацію щодо гіпотез, що перевіряються, та рішення щодо результатів спостереження, достатньо обчислити компоненти

вектора відношень істинності в –вимірному просторі. Завдання розрахунку та прийняття рішення щодо структури НКС (тобто…).

Під час вирішення питань, пов’язаних з оцінкою інформаційної безпеки, насамперед необхідно оцінити ступінь, до якої отримані сигнали (портрети технологічної безпеки – результати інструментальних вимірювань та спеціалізованих досліджень щодо кожного з технічних каналів витоку інформації) збігаються з опорними сигналами, тобто особою, яка приймає рішення.

Метод вимірювання відповідності відрізняється залежно від характеру проведених досліджень. В результаті, рішення щодо безпеки від інформаційного впливу, наприклад, за допомогою акустичних, віброакустичних та акустоелектричних засобів, приймається після порівняння цих засобів з нормами в системі технічного захисту України.

2.2 Обгрунтування вибору архітектури нейронної мережі для розв’язання задач з захисту інформації.

Аналіз сучасних публікацій показує, що для забезпечення ефективності використання нейронних мереж (НМ), їхня розробка повинна відповідати певним вимогам, пов’язаним з нею:

3) навчальний матеріал;

Процес навчання називається навчанням.

3) обчислювальна потужність;

Введення інформації;

5) технічне виконання;

6) сфера застосування.

Давайте обговоримо ці вимоги детальніше.

Основними атрибутами навчальних даних є:

Кількість параметрів, пов’язаних з навчальним прикладом. У рідкісних випадках

Під час аналізу текстового контенту кількість параметрів заздалегідь не відома. Також,

Для різних навчальних сценаріїв кількість вхідних параметрів може відрізнятися.

Характер параметрів є дискретним або неперервним відповідно.

Кількість навчальних вибірок.

Наявність помилок (tạp âm) у навчальних прикладах.

Наявність зв’язку між навчальними прикладами.

Потенціал та необхідність попередньої обробки вхідних даних для зменшення шуму та їх нормалізації.

Потенціал відображення всіх аспектів процесу у навчальній вибірці.

Розподіл навчальних прикладів, що представляють різні аспекти моделюваного процесу.

2. Процес навчання складається з:

Тривалості навчання.

Необхідності представлення очікуваного результату нейронної мережі (НМ) у навчальній вибірці.

В результаті визначається потенційний стиль навчання – з учителем або без нього.

Потенціал автоматизації процесу навчання залежить від кількості та значущості емпіричних параметрів. Цей потенціал визначає умови, за яких використовується НМ. Мережі, які не мають автоматизованого навчання, можуть використовуватися лише в лабораторіях.

Потенціал додаткового навчання під час роботи.

Вимоги до якості навчання, яка зазвичай визначається максимальною та середньою похибкою розпізнавання навчальних та тестових даних. Тестові дані не повинні суттєво відрізнятися від навчальних.

Потенціал навчання НМ у лабораторних умовах. Наприклад, у лабораторних умовах теоретично можливо навчити НМ розпізнавати атаки певного типу. Крім того, неможливо навчити мережеву мережу класифікувати електронні листи на основі конкретних інтересів конкретного користувача. Потенціал навчання в лабораторії пояснюється необхідністю оптимального механізму для створення та підтримки бази знань мережі.

Незмінність виводу мережі для різних прикладів з однаковими параметрами.

3. На практиці потреби в обчислювальній потужності визначаються:

Максимальною кількістю екземплярів (розміром пам’яті), які мережа може запам’ятати, щоб мати необхідний ступінь надійності в прийнятті рішень.

Стабільністю процесу прийняття рішень, яка визначається максимальними та середніми значеннями помилок мережі на фактичних даних, які загалом перевищують набір навчальних даних.

Потенціалом екстраполяції результатів навчання на додаткові приклади.

Виведено початкові вимоги до мережі.

Початкова інформація повинна бути представлена у належному вигляді. Наприклад, під час розпізнавання вірусів може знадобитися не лише визначити ситуацію, таку як «Збій програмного забезпечення в комп’ютерній мережі», але й розрахувати ймовірність цієї ситуації або графічно відобразити цю ситуацію на площині, що дозволить користувачеві провести остаточну класифікацію.

За необхідності, процес передачі інформації має бути визначений як послідовність кроків, що вимагають усного зв’язку між вхідною та вихідною інформацією.

3.3Обмеження впровадження НМ пов’язані з:

Швидкістю прийняття рішень.

Потенціалом бути частиною існуючих засобів захисту.

Тривалістю життя програмного забезпечення.

Тривалістю застосування визначає кількість співробітників або проектів, які будуть залучені.

У цьому розділі описано характер завдань, які будуть виконуватися засобами захисту, такими як НМ. Сьогодні продемонстрована ефективність використання НМ для диференціації та кластеризації зображень. Ефективність застосування у вирішенні бізнес-завдань та аналізі інформації природною мовою вважається дещо менш ефективною. У перспективних дослідженнях продемонстровано потенціал використання NM для полегшення паралельних обчислень у комп’ютерних системах, що підвищить стійкість комп’ютерів до перевантаження.

Здатність перевести мережу в самодостатній стан.

Процес визначення оптимального типу архітектури включає такі кроки:

a. Сформулювати постановку задачі практичним чином, вказавши необхідність, мету та завдання використання NM.

b. Використовуючи інформацію, обчислити відносні значення параметрів оптимізації.

c. Враховуючи властивості завдання захисту, обчислити величину ваги, пов’язаної з кожним. Критеріїв оптимізації.

d. Виберіть відповідний тип моделі НМ.

Обговоримо процес оптимізації проекту НМ. Результати дослідження НМ типу BSHP, RBF, NN, ART, TK, ANM та SNM. Зазначається, що вони розроблені за одним і тим самим алгоритмом, блок-схема якого зображена на рис. 4.3.

Використання цього алгоритму та результати аналізу поточних питань CI, проведеного в першому розділі, сприяють створенню методології зміни параметрів проекту НМ вибраного типу до їх цільових умов:

1. Підготовка вхідної інформації включає визначення та обробку параметрів керування, що підходять для НМ. Процедура знаходження параметрів, які можна контролювати, випливає з вимог завдання захисту. Її основним результатом є документування та опис (або перевірка) вхідних та вихідних параметрів НМ. Для типу НМ ТС єдиним компонентом назви є вхідні параметри. Обробка параметрів зазвичай передбачає їх перетворення на числове значення від -1» до «+1».

2. Підготовка навчальних, контрольних та тестових прикладів – передбачає створення набору прикладів вхідних та вихідних параметрів нейронної мережі (НМ), який базується на аналізі операційних та експериментальних даних.

Оцінка параметрів моделі – базується на математичних та методологічних принципах, специфічних для кожного типу НМ. Під час першої реалізації цього етапу типові значення параметрів моделі вибираються з допустимого діапазону. У наступних реалізаціях параметри модифікуються для підвищення точності моделювання.

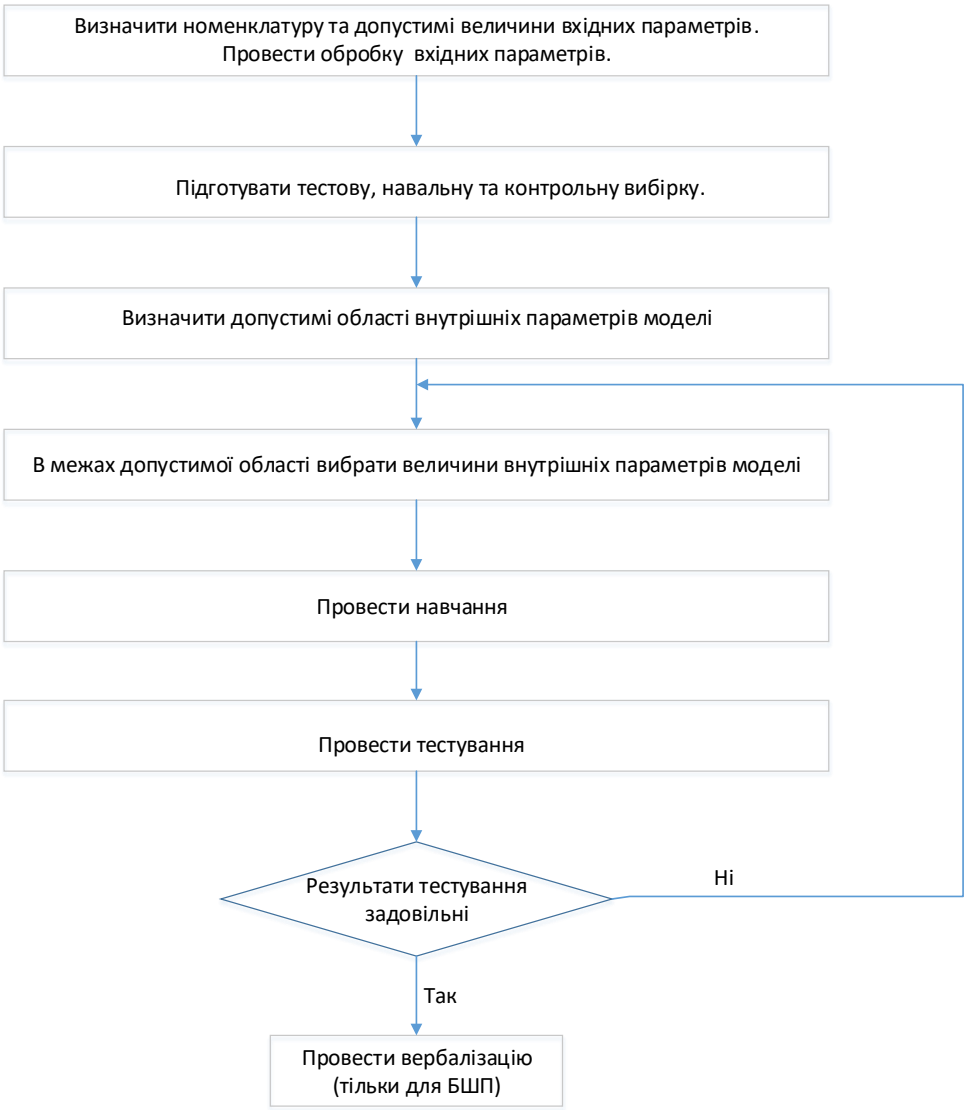


Рис.2.3 Етапи оптимізації архітектури

3. Навчання НМ – що базується на методі навчання цього типу тварин.

2. Перевірка відповідності моделі контрольним даним. Якщо точність недостатня, необхідно повернутися до третього етапу та вказати параметри моделі.

3. Перевірка відповідності моделі тестовим даним. Якщо точність недостатня, важливо вказати формулювання проблеми (змінити назву та метод обробки вхідних параметрів, перевірити легітимність навчання, контролю та тестування) та повернутися до третього етапу. Якщо кілька спроб досягнення бажаної точності не вдаються, ймовірно, варто відмовитися від типу моделі.

4. Вербалізація моделі – доступно лише для BSP.

2.3 Функція захисту інформації на основі нейронної технології

Комплексне дослідження всіх можливих шляхів витоку інформації, а також наявність типових значень для конкретних TKVI, дозволяє нам створити найпростішу можливу модель нейронної мережі.

Типовий приклад мережі з прямою передачею даних проілюстровано на рис. 3.3.

Нейрони зазвичай складаються з кількох шарів. Вхідний шар просто відповідає за отримання значень вхідних змінних. Кожен нейрон у прихованому шарі пов’язаний з кожним компонентом попереднього шару. Можна було б розглянути мережі, які мають зв’язки лише між нейронами одного шару; однак для більшості застосувань мережі з повною системою зв’язків є більш сприятливими

.

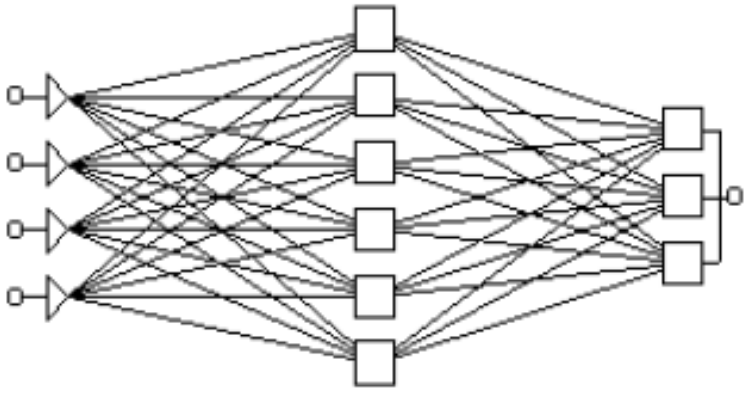


Рис.2.4 Типовий приклад мережі з прямою передачею сигналу

Під час функціонування (використання) мережі вхідні компоненти заповнюються значеннями вхідних змінних, потім сигнали послідовно обробляються нейронами проміжного та вихідного шарів. Кожен з них обчислює значення своєї активації, взявши середньозважене значення виходів

компонентів попереднього шару та віднявши від нього порогове значення. Потім значення, що активуються, перетворюються за допомогою функції активації, і результатом є вихід нейронів. Після того, як вся мережа спрацювала, виходи елементів вихідного шару вважаються виходом усієї мережі в цілому.

Першим кроком є налаштування мережі. Процедура зміни мережі називається «навчанням мережі». Перед початком навчання з'єднань призначаються невеликі випадкові числа. Кожна ітерація процесу включає два кроки. Під час першої фази вектор вхідних значень вводиться в мережу шляхом встановлення вхідних компонентів у потрібний стан. Після цього вхідні сигнали передаються через мережу, що створює вихідний вектор. Для успішної роботи алгоритму важливо, щоб вхідні та вихідні властивості нейронних компонентів були незростаючими та мали скінченну похідну. Зазвичай для цього використовується сигмоподібна функція.

Відомі різновиди мереж:

Одношаровий персептрон;

Багатошаровий персептрон;

• Мережа Хеммінга,

Мережа Варда;

Мережа Хопфілда;

Мережа Кохонена;

• Інтелектуальний тьютор,

Нові когнітивні здібності.

2.4 Висновки по розділу

У розділі розглядаються потенційні можливості використання нейронних мереж для забезпечення захисту інформації від витоку через канали зв’язку та інформації.

1. Описано процедуру вимірювання ступеня інформаційної безпеки за допомогою нейронних мереж.

2. Викладено рекомендації щодо вибору архітектури нейронної мережі, призначеної для захисту інформації, та використано мережу нейронів для апроксимації функції захисту інформації.

3. Наведено результати обробки даних інформаційної безпеки за допомогою нейронної мережі. Використання нейронної мережі.

Розділ 3.
ДОСЛІДЖЕННЯ ПРОЦЕСІВ ТА РОЗРОБКА МЕТОДІВ ЗАСТОСУВАННЯ НЕЙРОННИХ ТЕХНОЛОГІЙ ДЛЯ ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОГО ПРОНИКНЕННЯ В ІНФОРМАЦІЙНІ КАНАЛИ ПЕРЕДАЧІ ДАНИХ

3.1 Інтелектуальні методи запобігання несанкціонованого проникненню в інформаційні канали передачі даних на основі нейронних технологій

Зі постійним збільшенням обсягу оброблюваної інформації та зростанням цінності цієї інформації як «товару», безпека та надійність інформаційних систем стали предметом занепокоєння. З цієї причини нейромережеві методи оцінки інформаційної безпеки останнім часом стають дедалі популярнішими.

По суті, інтелектуальні засоби захисту інформації (ІЗІ) використовуються в системах виявлення атак як інструмент з інтелектом. Ці системи зазвичай використовують нейронні мережі (НМ), системи нечіткої логіки (СН) та базуються на експертних системах (ЕС), які мають правила.

Методи виявлення атак поділяються на дві групи:

Другий крок – виявлення зловживань.

З методи розпізнавання потенційних технічних джерел витоку інформації.

Перша категорія включає атаки, які використовують відомі вразливості в інформаційній системі (ІС), друга категорія не відповідає результатам вимірювань та не має стандартів.

Для розпізнавання ІЗІ розпізнається активність, яка відрізняється від попередньо встановлених шаблонів для користувачів або груп користувачів. Виявлення TKVI зазвичай пов’язане зі створенням попередньої бази знань (КВ), яка містить інформацію про контрольовану активність, а також виявленням зловживань, що досягається шляхом порівняння поведінки користувачів з

відомими шаблонами поведінки хакерів та використанням правил, що описують, як відбуваються атаки. Механізм виявлення розпізнає потенційні атаки, коли дії користувача відхиляються від встановленого протоколу.

Багато систем виявлення зловживань походять від запропонованої Деннінгом моделі. Модель підтримує набір профілів для легітимних користувачів, вона поєднує записи аудиту та пов’язаний з ними профіль, оновлює профіль та повідомляє про будь-які порушення.

Статистичні методи часто використовуються для виявлення випадків незаконної поведінки шляхом порівняння команд, що використовуються користувачем, з типовим режимом роботи. Поведінку користувачів можна описати як модель на основі шаблонів, яка передбачає певні шаблони або стани, а методи порівняння з вибіркою використовуються для виявлення потоків інформації, що витікають.

Наступні підходи є життєздатними способами використання NM у системах виявлення інформації.

- Існуючі експертні системи доповнюються нейронною мережею, яка фільтруватиме вихідні повідомлення, щоб зменшити кількість хибнопозитивних помилок, властивих експертній системі. Оскільки експертна система отримує інформацію лише про підозрілі події, в результаті зростає чутливість системи. Якщо нейронна мережа починає розпізнавати нові потенційні шляхи витоку інформації шляхом навчання, експертну систему також слід переглянути. В іншому випадку нові шляхи витоку інформації будуть ігноруватися експертною системою, попередні правила якої неефективні для розпізнавання цієї небезпеки.

Якщо нейронна мережа є окремою системою, яка виявляє потенційні канали витоку інформації, то трафік обробляється, а інформація аналізується, щоб визначити наявність негативних дій. Будь-які випадки, які розпізнаються як такі, що мають ознаки атаки, перенаправляються адміністратору безпеки або

використовуються системою автоматичного реагування для боротьби з атаками. Цей метод має перевагу в швидкості порівняно з попереднім методом, в результаті існує лише один рівень аналізу, і адаптивність системи випливає з цього методу.

Інші застосування нейронних мереж у системах захисту інформації включають зберігання ключів для криптографічної інформації в розподілених мережах.

Основним недоліком нейронних мереж вважається «непрозорість» формування результатів аналізу. Однак використання гібридних нейроекспертних або нейронечітких систем дозволяє явно відобразити в структурі нейронної системи систему нечітких правил, яка автоматично змінюється в процесі навчання нейронної системи. Адаптивність нечіткої нейронної системи здатна вирішувати як окремі завдання щодо ідентифікації загроз, порівняння поведінки користувачів з існуючими шаблонами в системі, так і автоматично створювати нові правила при зміні поля загроз. Крім того, може бути реалізована система захисту інформації для технічної системи в цілому.

3.2 Технологія застосування інтелектуальних засобів для моделювання систем запобігання несанкціонованого проникненню в інформаційні канали передачі даних

Різні типи інтелектуальних систем мають різні властивості, наприклад, з точки зору навчання, узагальнення та результатів, що робить їх найбільш ефективними для одних типів задач та менш ефективними для інших. Наприклад, нейронні мережі корисні для розпізнавання закономірностей, але їм важко пояснити, як вони це роблять. Вони можуть автоматично отримувати знання, але процес їхнього навчання часто повільний, а аналіз навченої мережі зазвичай складний (навчена мережа зазвичай є «чорною скринькою» для

користувача). Крім того, важко попередньо ввести будь-які попередні знання (знання експертів) у нейронну мережу для полегшення процесу навчання. Системи нечіткої логіки, однак, корисні для пояснення результатів, отриманих з їхньою допомогою, але вони не можуть автоматично отримувати знання, які можна використовувати для виведення знань. Необхідність розділення універсальних колекцій на окремі домени, як правило, зменшує кількість вхідних змінних у цих типах систем до невеликого значення.

Й. Хаяші та А. Імура продемонстрували, що нейронна мережа прямого зв'язку може емулювати будь-яку систему на основі нечіткої логіки, і будь-яка система на основі нечіткої логіки може бути емульована нечіткою системою.

З теоретичної точки зору, системи нечіткої логіки та штучні нейронні мережі схожі одна на одну, але на практиці вони мають свої переваги та недоліки. Це розуміння призвело до створення апарату нечіткої нейронної мережі, яка подібна до традиційної нейронної мережі, але має інший підхід до функцій належності: замість традиційного методу поширення помилок, метод базується на нечіткій логіці. Ці системи не тільки використовують переваги попередньо існуючої інформації, але й можуть отримувати нові знання. Вони за своєю суттю логічні.

Нечітка нейронна мережа – це представлення нечіткої системи висновків, подібне до нейронної мережі, що корисно для навчання, аналізу та використання. Склад нечіткої нейронної мережі подібний до основних компонентів систем нечіткої логіки.

Основні атрибути нечітких нейронних мереж полягають у наступному:

- нечіткі нейронні мережі походять від нечітких систем, які побудовані за допомогою методів, що використовуються в нейронних мережах.

- нечітка нейронна мережа зазвичай складається з кількох шарів (зазвичай трьох). Перший шар складається з вхідних змінних, середній шар – з нечітких правил, а третій шар – з вихідних змінних. Ваги зв'язків пов'язані з нечіткими множинами вхідних та вихідних змінних. Іноді використовується п'ятишарова

архітектура. Зазвичай нечітка система не обов’язково представлена так, як зазначено вище, але це корисна модель для застосування методів навчання.

- Нечітку нейронну мережу завжди можна розглядати як систему нечітких правил до, під час та після навчання.

Процедура навчання пов’язана з семантичними властивостями нечіткої системи. Це ілюструється обмеженою кількістю можливих змін параметрів, що змінюються. Однак слід визнати, що не всі методи навчання нейронечітких мереж враховують семантичну природу системи.

- Нейронечітка система є наближенням N’M, функції, яка повністю невідома та частково описується навчальними даними.

Різні типи комбінацій нечіткої логіки та нейронних мереж на основі методу взаємодії такі:

- Нечіткі нейронні системи. У цьому випадку принципи нечіткої логіки використовуються в нейронних мережах для полегшення процесу налаштування або покращення інших властивостей. Ця методологія виключає використання нечіткої логіки як засобу інтерпретації для нейронних мереж, оскільки систему такого типу неможливо зрозуміти за допомогою нечітких правил через її природу «чорного ящика».

Паралельні нейронечіткі системи.

У цих моделях нечітка система та нейронна мережа мають однакове завдання, але не взаємодіють з параметрами одна одної. Обробка даних послідовно можлива спочатку з однією системою, а потім з іншою.

− Паралельні нейронечіткі системи (кооперативні нейронечіткі системи).

У цих типах систем параметри змінюються за допомогою нейронних мереж. Після цього система функціонує так, ніби вхідні дані відсутні. Розрізняють такі типи паралельних нейронечітких моделей: 1) нечітка асоціативна пам’ять; 2) системи з вилученням правил із самоорганізованих карт; 3) системи, які можуть вивчати параметри нечітких множин.

− гібридні (інтегровані) нейронечіткі системи (інтегровані нейронечіткі системи), які мають тісний зв’язок між нечіткою логікою та нейронними мережами.

Термін «нейронні нечіткі мережі» найчастіше використовується для опису цих систем. Як правило, інтегровані системи складаються з систем типу Мамдані або Такагі-Сугено.

У комбінованій моделі методи нейронних мереж використовуються для визначення параметрів нечіткої системи. Інтегровані нейронечіткі системи розділяють структури даних та моделі знань.

Найпоширеніший підхід до застосування методу навчання до нечіткої системи полягає у представленні її як архітектури, подібної до нейронної мережі. Однак, звичайні (градієнтні) методи навчання нейронних мереж не застосовні безпосередньо до цього типу систем, оскільки функції, що беруть участь у процесі виведення, зазвичай не є диференційованими. Цю проблему можна подолати, використовуючи диференційовані функції в системі виведення або не використовуючи стандартні методи навчання для нейронних мереж. Нейронечіткі мережі використовують реалізації диференційованих трикутних норм (додавання ймовірності), а також гладкі функції належності. Це полегшує використання методів швидкого навчання нейронних мереж, заснованих на підході зворотного поширення помилки, для налаштування нейронечітких мереж. Інтегрована нейронечітка модель є зрозумілою та може бути навчена під наглядом. В ANFIS процес навчання обмежується лише зміною значень параметрів відповідно до встановлених структур. Для складних задач, що мають кілька вимірів, буде важко визначити оптимальні структури «умова-наслідок», кількість правил тощо. Користувач повинен визначити конкретні деталі архітектури: кількість і тип функцій належності для вхідних і вихідних змінних, тип нечітких операторів тощо.

Серед інтегрованих нейро-нечітких моделей ANFIS має найбільшу точність. Це пояснюється тим, що в ANFIS застосовуються правила Такагі-Сугено. Системи виводу типу Такагі-Сугено є ефективнішими, але мають вищі обчислювальні витрати.

Правила Такагі-Сугено є ще одним прикладом нечітких правил і складаються з таких компонентів: Якщо, то та та. Ці правила дотримуються шаблону: вхідні змінні, вихідна змінна: - нечіткі терміни, що визначені на . – пряма функція, на яку впливають вхідні змінні.

Попередником правила є набір неточно визначених термінів, що описують вхідні дані, це умова, за якої правило буде активовано.

Результатом правила є набір термінів нечіткості, визначених для виходів. Ці терміни призначаються вихідним змінним, коли правило спрацьовує.

Імплікація – це зміна неоднозначних наборів виходів за ступенем виконання правил.

ANFIS використовує нечітку систему висновків Сугено у вигляді п’ятишарової нейронної мережі, яка безпосередньо поширює сигнали. Метою шарів є досягнення наступного:

Перший шар стосується термінів вхідних змінних.

Другий шар складається з антецедентів (передумов) нечітких правил.

Третій шар стосується нормалізації заходів, що використовуються для оцінки ефективності правил.

Четвертий шар – це кінцевий результат висновку правил.

П’ятий шар – це агрегація результатів різних правил.

Компоненти мережі не виділені окремому шару.

На рисунку 8.2 зображено мережу ANFIS з двома вхідними змінними (x1 та x2) та чотирма нечіткими правилами. Для лінгвістичної оцінки вхідної змінної x1 використовуються три терми, а для оцінки змінної x2 — два терми.

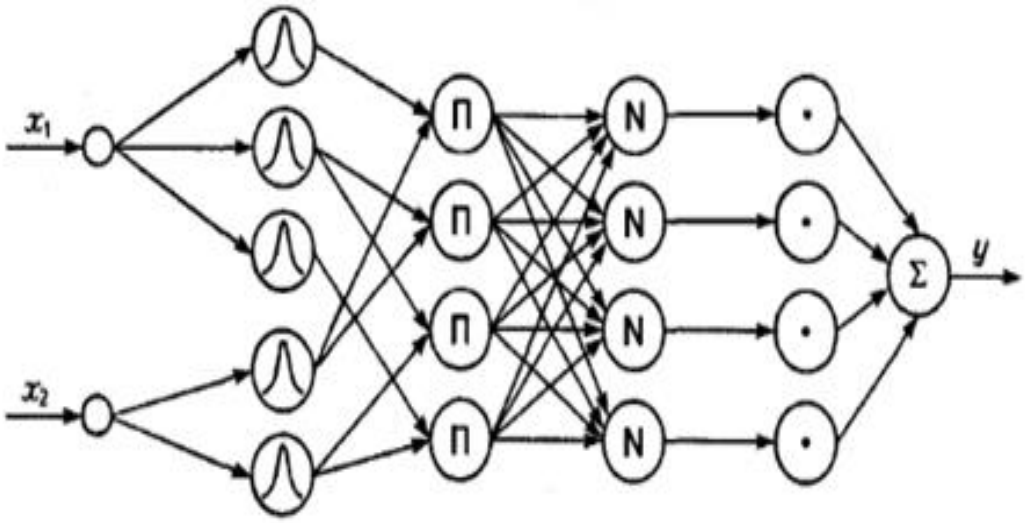


Рис. 3.1 Приклад нейро-нечіткої мережі

Введемо наступні позначення:

•$x_1, x_2,...x_n$ – входи мережі;

• y – вихід мережі.

• R_r: Якщо $x_1=a_{1,r}$ ТА…ТА $x_n=a_{n,r}$, то $y=b_{0,r} + b_{0,r}x_1 + \ldots + b_{n,r}x_n$ – нечітке правило з порядковим номером r;

• m – кількість правил, ;

• $a_{i,r}$ – нечіткий терм з функцією приналежності $m_r(x_i)$, що застосовується для лінгвістичної оцінки змінної x_i в r-му правилі (,);

• $b_{q,r}$ – коефіцієнти в висновку r-го правила (,).

ANFIS-мережа функціонує таким чином.

Шар 1. Кожна гілка першого шару представляє терм дзвоноподібної форми з функцією належності, що до нього прив’язана. Входи мережі x1, x2, ..xn пов’язані лише з відповідними термами. Кількість вузлів у першому шарі дорівнює загальній потужності наборів термів, пов’язаних з вхідними змінними. Вихід вузла призначений для вимірювання належності вхідної змінної до відповідного нечіткого терма:

$$\mu_r(x_i) = \frac{1}{1 + \left| \frac{x_i - c}{a} \right|^{2b}} \qquad (2.1)$$

де a, b і c – параметри функції приналежності, що настроюються.

Рівень 2. Кількість вузлів у другому шарі дорівнює t. Кожен вузол у цьому шарі пов’язаний з одним нечітким правилом. Вузол другого шару пов’язаний з вузлами першого шару, які складають передумови пов’язаного правила. Як результат, кожна гілка у другому шарі може обробляти від 1 до n комунікацій. Виходом вузла є вимірювання ефективності правила, яке обчислюється як добуток вхідних сигналів. Ми можемо представити виходи вузлів у цьому шарі як tr.

Рівень 3. Кількість вузлів у третьому шарі також дорівнює m. Кожен вузол у цьому шарі обчислює ступінь виконання нечіткого правила відносно інших правил за допомогою формули:

$$\tau_r = \frac{\tau_r}{\sum_{j=1,m} \tau_r} \qquad (2.2)$$

Шар 4. Кількість вузлів четвертого шару також дорівнює t. Кожен вузол підключений до одного вузла третього шару, а також до всіх входів мережі (з’єднання з входами не показано на рис. 8.2). Вузол четвертого шару обчислює важливість одного нечіткого правила для виходу мережі згідно з наступним рівнянням:

$$y_r = \tau_r (b_{o.r} + b_{1,r} x_1 + \ldots + b_{n,r} x_n) \qquad (2.3)$$

Шар 5. Єдиний вузол цього шару підсумовує вклади всіх правил:

$$y = y_1 + \ldots y_r \ldots + y_m \qquad (2.4)$$

Для зміни мережі ANFIS можна використовувати поширені методи навчання нейронних мереж, оскільки вона використовує диференційовані функції. Зазвичай використовується гібридизація градієнтного спуску, що базується на зворотному поширенні алгоритму та методі найменших квадратів.

Алгоритм зворотного поширення оновлює параметри антецедентних правил, які є функціями належності. Метод найменших квадратів оцінює зв’язок

між параметрами виведення правила та виходом мережі, оскільки вони пов’язані один з одним через лінійну функцію. Кожна ітерація процедури налаштування включає два кроки. На першому етапі вибірковий навчальний набір подається на входи, а оптимальні параметри вузлів четвертого шару визначаються методом найменших квадратів на основі різниці між бажаною та фактичною поведінкою мережі. На другому етапі залишкова розбіжність переноситься з виходу мережі на входи, а параметри вузлів першого шару змінюються методом зворотного поширення. У цьому випадку оцінені коефіцієнти на основі правил з попереднього етапу не змінюються. Процедура налаштування ітеративно продовжується доти, доки різниця не перевищить задане значення. Для зміни функцій належності, окрім методу зворотного поширення помилки, можна використовувати інші методи оптимізації, такі як метод Левенберга-Марквардта.

Класифікація нейронних мереж

Відповідно до методу відображення нечітких множин у структурі мережі, нейронечіткі мережі поділяються на три основні типи:

− системи, побудовані навколо вибіркових нечітких множин. У цих типах систем ступені належності описуються лише для кількох значень з області визначення, а функція належності представлена вектором. Кожен ступінь належності пов’язаний лише з одним вхідним або вихідним нейроном. Існує два методи реалізації цих систем. У першому випадку система просто перетворює відповідність виходів на входи, це називається системою «чорної скриньки». У другому випадку створюється унікальна система зі спеціальною конструкцією, в якій використовується нечітка логіка.

− Системи, які зберегли свої функції належності в нейронах. Одним із прикладів таких систем є ANFIS (Адаптивна мережева система нечіткого виводу).

− Системи, які використовують зважені функції належності для з’єднання нейронів, є парамедованими. Цей тип системи інакше називають персептроном з нечіткими зв’язками або нечітким персептроном.

За характером навчання розрізняють такі типи нейронечітких мереж:

Самоналаштовувані нейронечіткі мережі, що мають настроювану архітектуру та параметри;

− Адаптивні нейронечіткі мережі – із заздалегідь встановленою структурою, що адаптують параметри мережі.

Адаптивні нейронечіткі мережі класифікуються за методом оптимізації на ті, що використовують детерміновані підходи, такі як градієнтний спуск, та ті, що використовують стохастичні методи, зокрема еволюційні підходи.

Адаптивні нейронечіткі мережі класифікуються за типом параметрів, що беруть участь в адаптації, на мережі з адаптованими параметрами функції належності, мережі з адаптованими параметрами ваг правил та мережі з адаптованими параметрами операторів агрегації.

Найбільш ефективним поєднанням властивостей для розпізнавання та боротьби з незаконними діями володіють нечіткі нейронні мережі, що поєднують властивості НМ та нечіткої логіки, що походить з досвіду експертів з інформаційної безпеки. Механізм логічного висновку, що є нечітким, дозволяє використовувати досвід експертів, який проявляється як система правил типу fzy, для випередження навчання нечіткої НМС. Подальше навчання нейронних мереж у сфері відомих небезпек надає можливість аналізувати процес логічного мислення для виправлення існуючих проблем або створення нової системи нечітких правил захисту інформації.

Обговоримо властивості нечітких нейронних мереж, необхідні для адаптивної системи захисту інформації:

Міцна основа функціональності та безпеки елемента;

З потенціал для класифікації небезпек.

3 опис відповідності загроз та захисних механізмів у вигляді системи нечітких правил;

4 універсальність нейронечітких ФЗІ (систем нечітких правил);

5 «прозорість» для оцінки організації зв’язків між нейронечіткими ФЗІ та системою нечітких правил;

6 методи розподіленого паралелізму.

Як основа для створення адаптивних засобів захисту інформації, технічний аналог тканини біологічної системи, представленої низкою взаємопов’язаних комірок через спільний інтерфейс. Ці комірки контролюються потоком даних та з’єднані спільним інтерфейсом. Відповідно до принципів монолітного виконання та багатофункціональності пам’яті, обробка даних повинна проводитися безпосередньо в локальних пулах керування шляхом виконання послідовних зчитувань, модифікацій та записів.

Однією з конкретних альтернатив монолітному виконанню є секціонування, яке дозволяє використовувати базовий блок (розділ) як структурний елемент для нейронної мережі IPP, що формується програмуванням.

Універсальність IPP забезпечується використанням базового елемента, який може навчатися, та, що найважливіше, нейронних мереж. IPP нейронної мережі, дотримуючись принципу біологічної аналогії, повинні нагадувати інформаційні поля зі структурованою природою, що нагадує рівні захисту імунної системи та рецепторної системи.

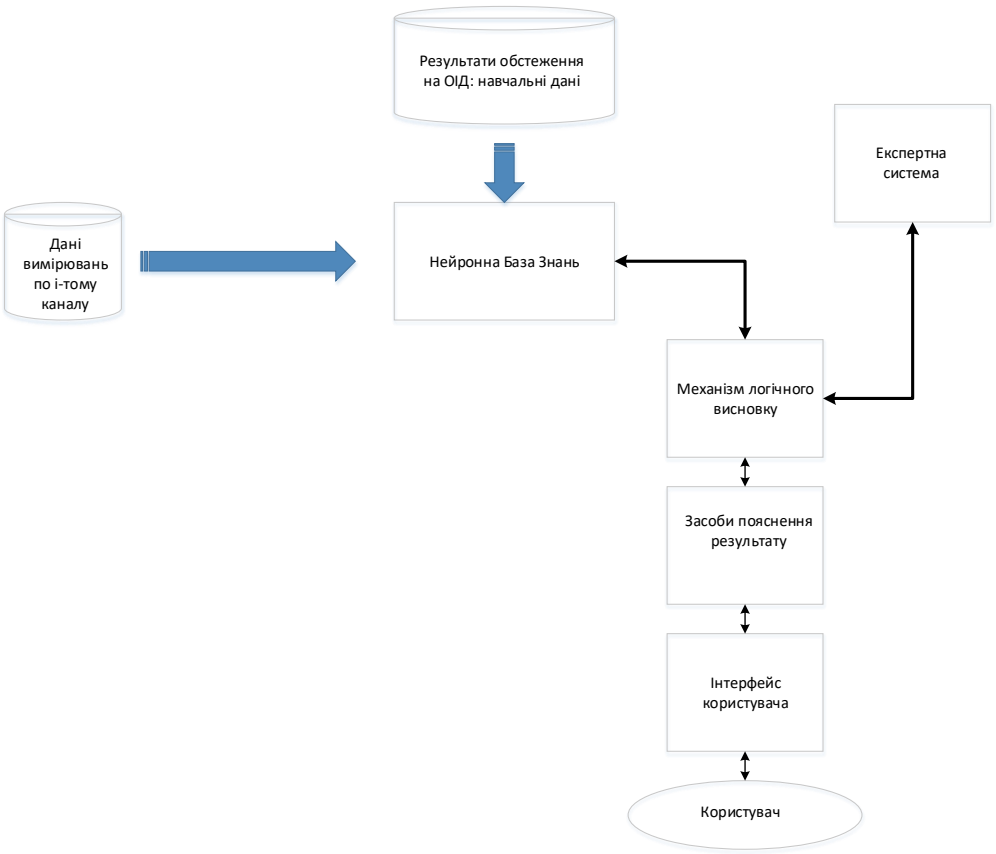


Рис.3.2 Структурна схема нейрочіткої мережі.

3.3 Метод навчання нейронних мереж при реалізації процесу запобігання несанкціонованого проникненню в інформаційні канали передачі даних

Штучна нейронна мережа — це розподілений процесор, який по суті є паралельним і має здатність зберігати та отримувати експериментальну інформацію. Вона схожа на людський мозок у двох аспектах. — мережа отримує знання під час процесу навчання. — для збереження знань мережа використовує переваги міжнейронної комунікації (синаптичні ваги). Фальшивий нейрон, його схема зображена на рис. 2.2, його функція така:

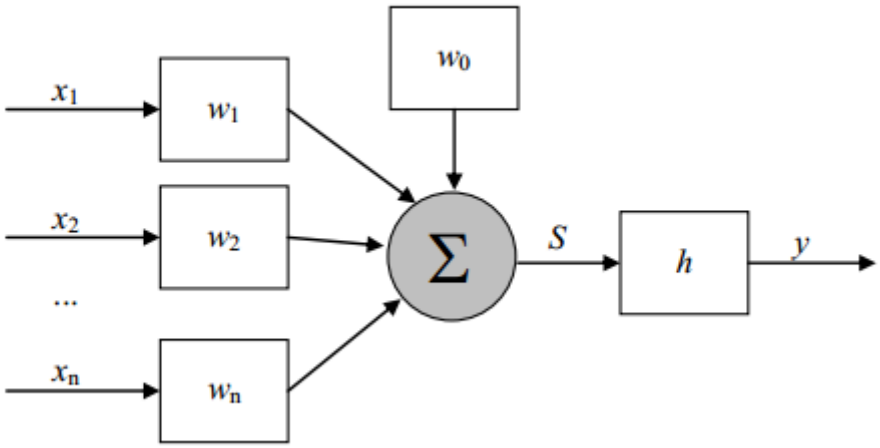


Рис. 3.3 Будова найпростішої нейронної мережі

Сигнали x(i n =1,…,) (що надходять на вхід нейрона) множаться на вагові коефіцієнти w (синаптичні ваги). Після цього вони включаються до вихідного сигналу, а поріг зміщується на значення w0:

$$S = \sum_{i=1}^{n} w_i x_i + w_0 \tag{3.5}$$

Потім вихідний сигнал подається на вхід блоку, який виконує нелінійну функцію активації нейрона h(S). У своїй найпростішій формі багатошаровий перцептрон являє собою мережу нейронів, які мають один вхід, один вихід та один прихований шар (див. рис. 3.4).

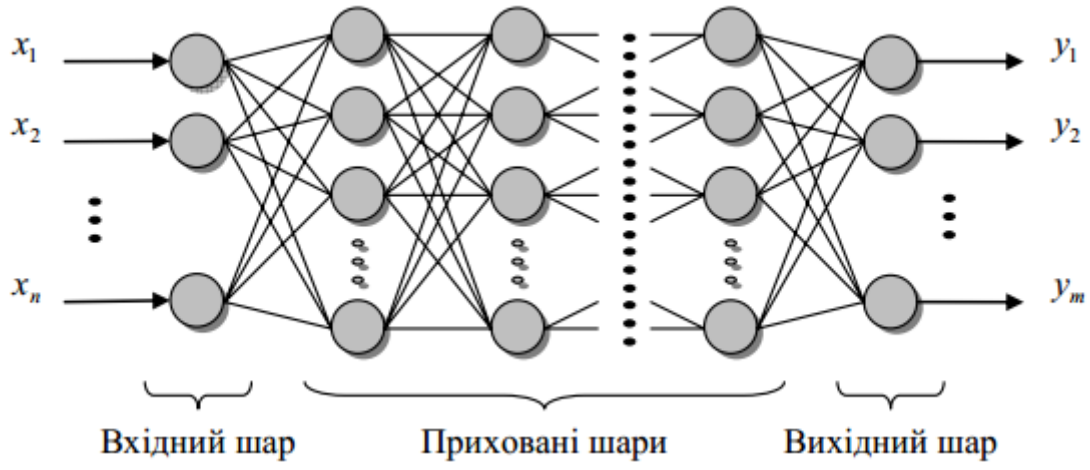


Рис. 3.4 Найпростіша версія багатошарового персептрона

Кола на рисунку представляють нейрони, які отримують вхідні дані та видають вихідні. Як правило, вихід кожного нейрона в шарі (i–1) надходить на вхід кожного нейрона в шарі (i). Усі багатошарові перцептрони мають прямий шлях від вхідного шару до вихідного шару через низку прихованих шарів. Альтернативні версії можуть мати непрямі зв'язки між сусідніми шарами, зв'язки між різними шарами або випадкові зв'язки між шарами замість звичайних. Важливо визнати, що традиційні багатошарові перцептрони найчастіше використовуються в інтелектуальних системах керування. Для того, щоб штучна нейронна мережа (ШНМ) точно представляла дані або функціональний зв'язок, її спочатку потрібно навчити. Навчання – це процес модифікації з'єднань мережі з посиланнями на зразки для досягнення певної мети. Важливо визнати, що цей процес походить від операційного протоколу мережі, а не від людських знань, які були раніше вбудовані в неї, що часто трапляється з системами штучного інтелекту. Процес навчання повторюється багаторазово, доки мережа не набуде бажаних властивостей. Якщо навчання ШНМ проводиться з використанням заздалегідь визначених даних, цей метод називається «навчанням з учителем». Довідкові дані складаються з шаблонів. Кожен шаблон має вектор попередньо задокументованих мережевих компонентів та вектор їхніх бажаних вихідних даних. Важливо розуміти, що створення точних довідкових даних для навчання є складним і часто неможливим завданням.

3.4 Аналіз результатів обробки даних оцінки захищеності інформації в інформаційній мережі на основі нейронних технологій

Ми проведемо дослідження взаємодії нейронів один з одним, щоб приблизно відтворити вибрану функцію, використовуючи можливості пакета

Neural Networks Toolbox. Пакет містить понад 160 різних функцій, які дозволяють створювати, навчати та досліджувати нейронні мережі.

Ми виконаємо моделювання функції співвідношення сигнал/шум нейронної мережі для фактичного співвідношення:

$$Q_i = \mathrm{L_{ACi}} - L_{AP\_3i} + \mathrm{K_i} - 20\lg r - \alpha_i r + 2$$

Щоб виконати завдання, необхідно запустити MATLAB та перейти до командного рядка.

Побудувавши послідовність вхідних даних та цілей для мережі, у нашому випадку вхідними даними є дані вимірювань на 5 різних октавних частотах, а цілями є фактичне співвідношення шум/сигнал на цих самих частотах, ми виведемо NM з цієї структури (рис. 3.4 та рис. 3.5).

Таблиця.3.1

Розрахункові значення формули 3.1 (цілі) значення вектора цільових даних.

Октавні смуги частот	Фактичне співвідношення сигнал/завада	
	Стаціонарні засоби АР	Випадково прослухування
250	18	-3
500	15	-12
1000	8	-25
2000	18	-21
4000	22	-23

Таблиця.3.2

Значення виміряні на ОІД.

Вимірювані значення	Кількість точок (>5)	5	250	500	1000	2000	4000
L_{Zn}	т1	69	66	68	66,5	64	
	т2	70	66	65	70	66	
	т3	75	74	78	74	74	
	т4	76	72	73	72	72	
	т5	74	72	73	71	73	

Рис. 3.4 Структурна схема нейронної мережі.

Перш ніж використовувати, його необхідно навчити.

Процес навчання може бути завершений на основі кількох критеріїв. Іноді краще зупинити процес навчання та вважати заданий період часу достатнім. І навпаки, об'єктивним критерієм є відсоток помилок.

Для нашої мережі доступні такі поля:

1. кількість епох (epochs) - визначає кількість епох (інтервал часу), після яких навчання буде завершено.

Епоха - це окремий екземпляр усіх навчальних даних, що подаються в мережу.

2. досягнення мети або досягнення (goal) - абсолютне значення функції помилки відоме, і в цей момент мета вважатиметься досягнутою.

3. період оновлень (show) - кількість епох, протягом яких відображається крива навчання.

4. час навчання (duration) - після закінчення заданого інтервалу часу, вираженого в секундах, навчання завершується.

Якість навчання мережі для вибраної послідовності навчання представлена графіком (рис. 2.3, рис. 2.4). Очевидно, що до кінця тренувального режиму

похибка зменшується: зовнішній вигляд фігури після перерахунку зазвичай відрізняється від початкового.

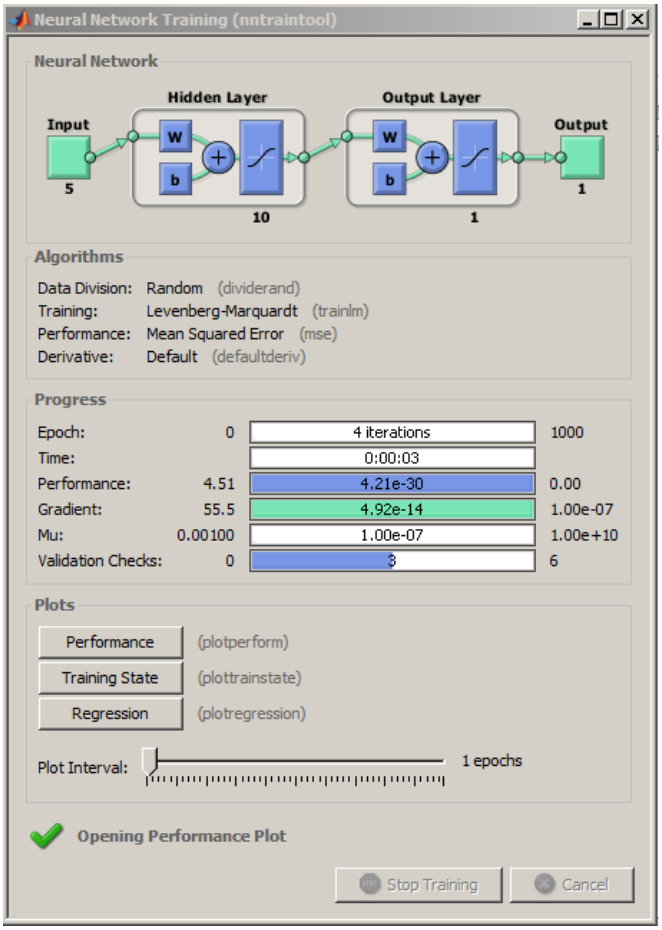


Рис. 3.5 Створення НМ в Матлаб

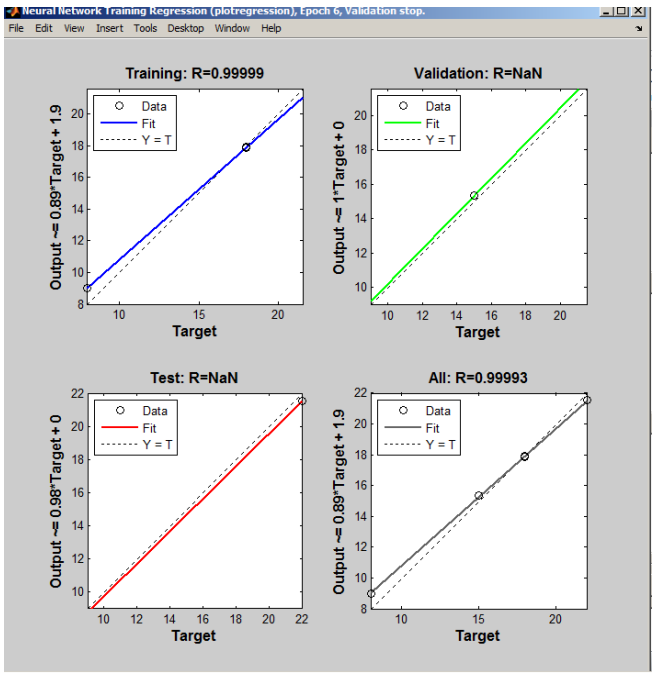


Рис.3.6 Результати навчання

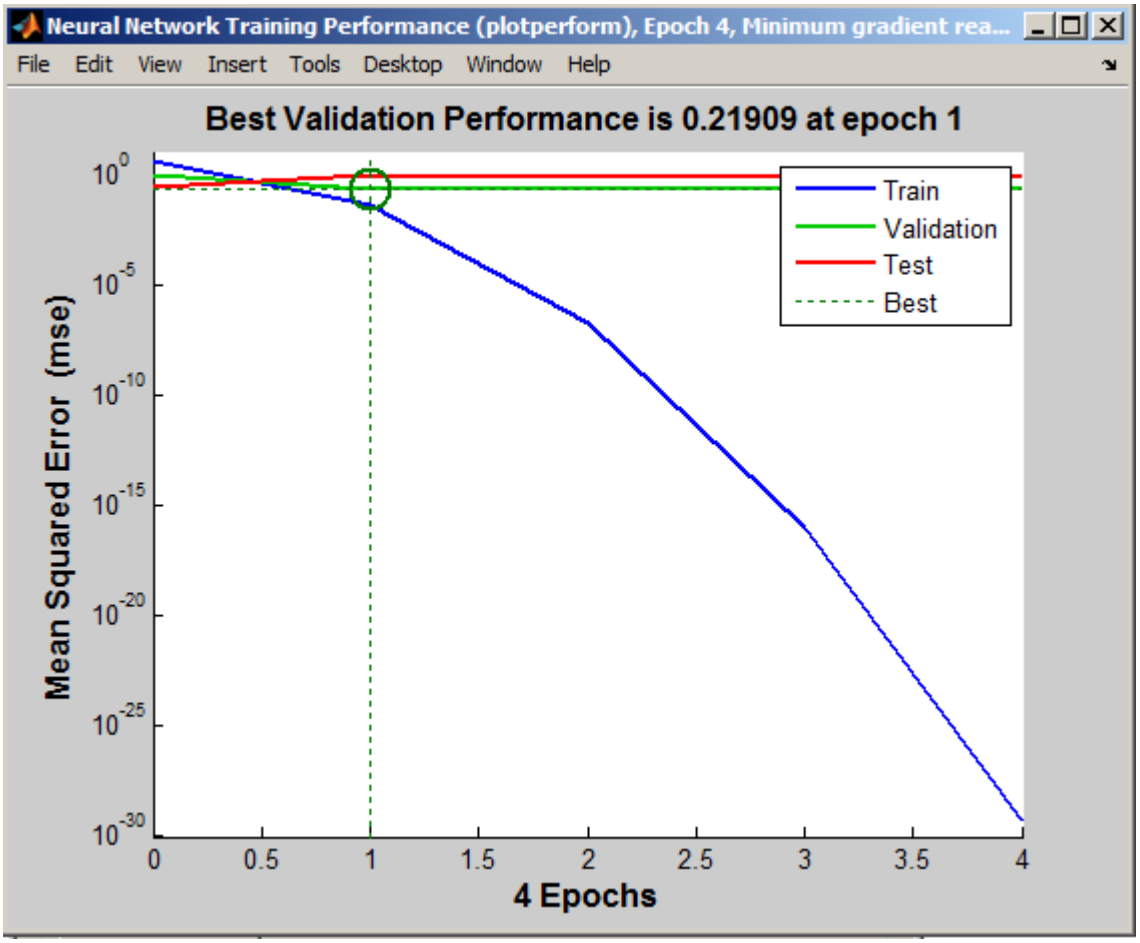


Рис. 3.7 графік успішного навчання нейронної мережі

У нашому випадку, результатами навчання є такі значення (рис.2.4):

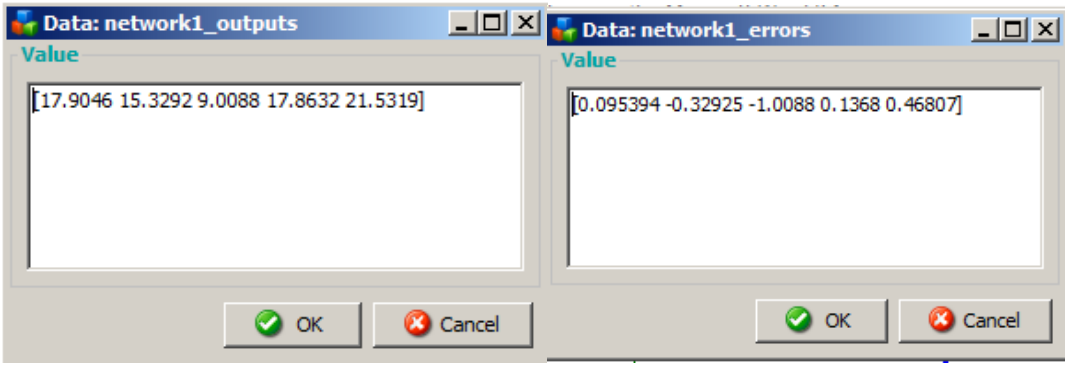


Рис.3.8 Значення помилок та виходів.

Важливо визнати, що в цьому випадку точність апроксимації була не дуже високою – максимальна абсолютна похибка становить 0,468, відносна похибка – 46%, і для перевірки цього можна використовувати значення помилок

(network1_errors) або виходів (network1_outputs) мережі. Важливо зазначити, що точність цієї апроксимації підвищилася б шляхом побудови мережі з великою кількістю нейронів, але також необхідна точніша навчальна вибірка. Можливі різні режими навчання мережі. У зв'язку з цим програма NNTool пропонує дві вкладки, які представляють функції навчання: раніше розглянуту вкладку «Навчання» та вкладку «Адаптація» (Adapt). «Адаптація» містить вкладку інформації про адаптацію, яка (як випливає з назви) містить поля, що мають аналогічне призначення до полів на вкладці «Інформація про навчання» та виконують ту саму функцію. Остання має одне поле під назвою «pass». Значення в цьому полі визначає кількість разів, коли всі вхідні вектори будуть подані до мережі під час процесу навчання.

Попередньо навчену нейронну мережу потім можна використовувати для виконання складнішого моделювання в середовищі Matlab. Цього можна досягти за допомогою програмного забезпечення Simulink.

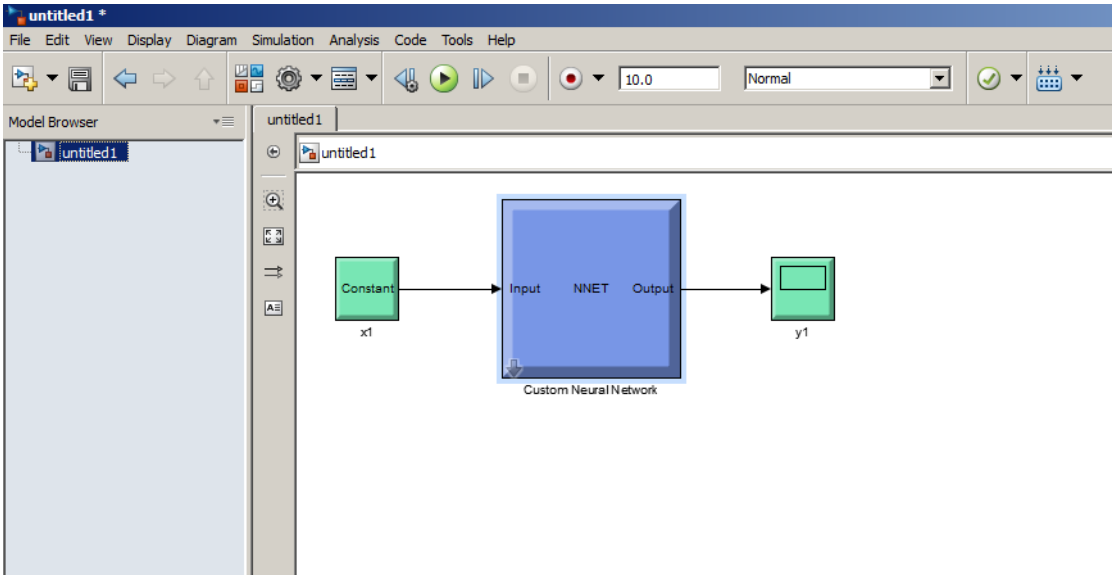


Рис.3.9 Схемне рішення реалізації НМ в Simulink

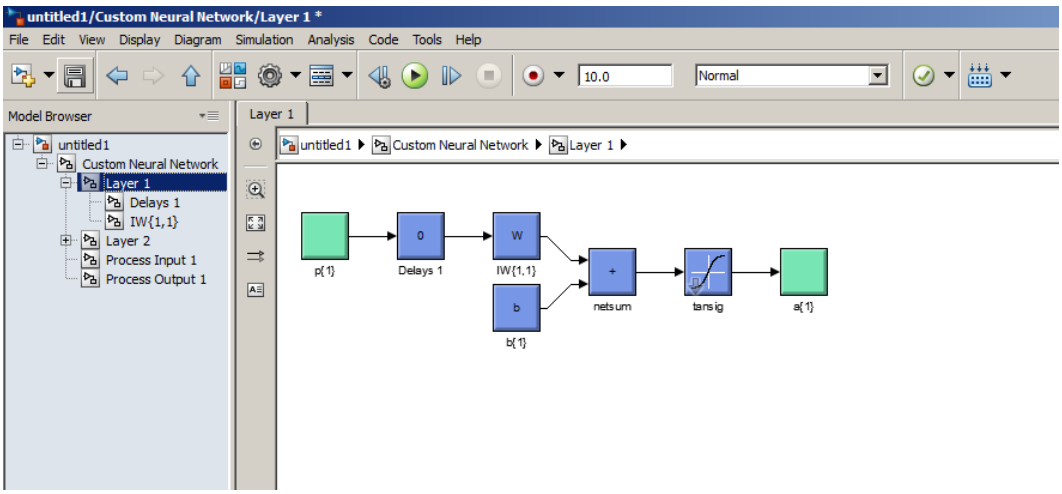


Рис.3.10 Структура шару 1.

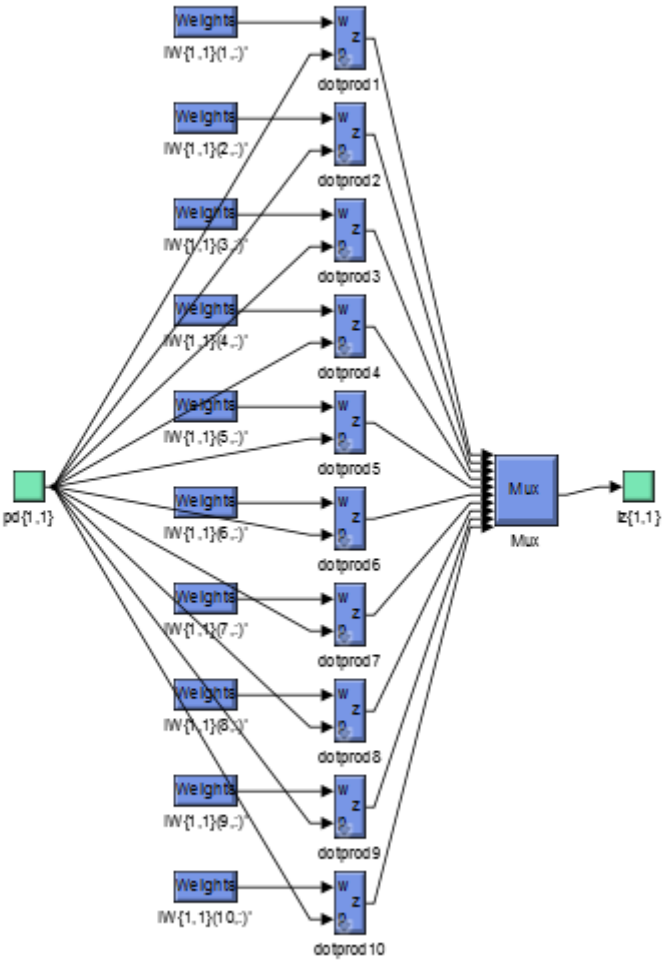


Рис.3.11 Детальна схема шару 1.

На рис 3.11 спостерігаємо схемне рішення шару 1 в НМ, який складається з попередньо заданих 10 нейронів.

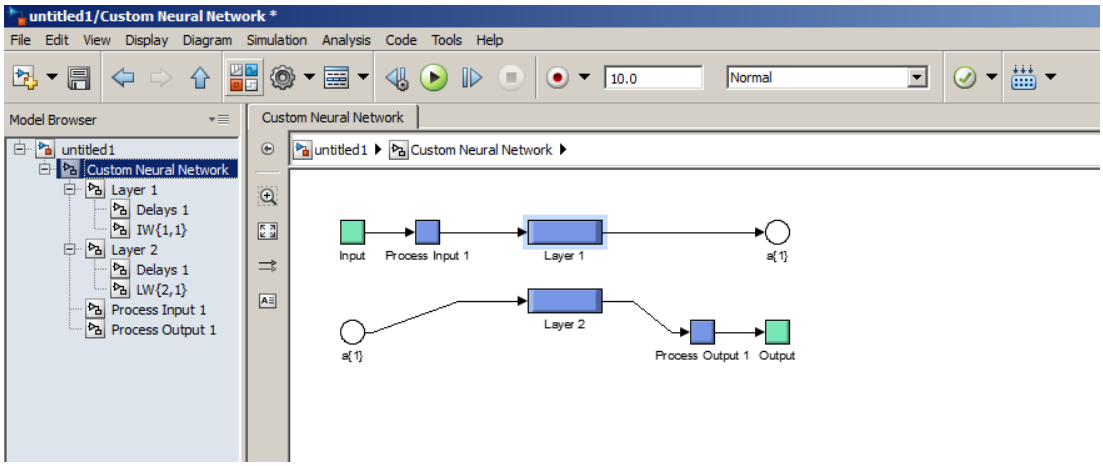


Рис.2.12 Нейронна мережа користувача

На рис. 3.8 показано загальну картину нейронної активності, пов'язаної з користувачем. Важливо визнати, що ця мережа вже знайома, тому її можна використовувати для додаткових проектів, попередньо визначивши всі відповідні дані.

Використання нейронної мережі для оцінки безпеки інформації є відносно ефективним підходом. Попередньо навчивши мережу типовим значенням вимірювання на OID, ми можемо обговорювати наявність технічних каналів вивільнення інформації. Результатів NM достатньо для створення технічної картини інформаційної безпеки. Її дотримання стандартів продемонструє потенціал існування різних типів інтелектуальних пристроїв – або інформаційних каналів. Відмінність від існуючих систем оцінки безпеки полягає в тому, що нейронна мережа зосереджена на вирішенні конкретної проблеми – створенні певної форми сертифікації діяльності інформаційних об'єктів або створенні комплексної системи інформаційної безпеки на транспорті. Необхідність проблемно-орієнтованої нейронної мережі (NM) зумовлює реалізацію принципу достатньої структури та адекватності середовища, це можливо завдяки гнучкості структурних та функціональних компонентів. Це визначає найважливішу властивість нейронної мережі – її здатність адаптуватися до змін умов навколишнього середовища ІТС, що має велике значення через складність структури сучасних ІТС. Початкова організація нейронної мережі повинна здійснюватися за допомогою формальних методів

синтезу, ці методи допомагають визначити оптимальну структуру, включаючи кількість шарів та їх склад, кількість нейронів у кожному шарі, наявність детермінованих зв'язків між ними та початкові значення ваг.

Основна відмінність полягає в тому, що вирішення питань, пов'язаних з безпекою, відбувається майже в реальному масштабі часу. Ця мета досягається шляхом реалізації принципу паралельної обробки інформації, що призводить до значного збільшення швидкодії НМ.

Новизна наукового відкриття полягає в:

1. Вперше запропоновано модель оцінки рівня інформаційної безпеки на основі нейронної мережі.

Вперше формалізовано поняття портретів технологічної безпеки як засіб станів безпеки, що відповідають технічним шляхам впливу інформації, виявленим на ІВС у певний момент часу.

3. Пропонується ранжувати технічні канали за їхньою важливістю перед обробкою нейронною мережею.

4. Вирішення питання вимірювання ступеня безпеки відбувається майже в реальному часі. Це досягається шляхом використання принципу обробки інформації в паралельній нейронній мережі.

3.5 Висновки по розділу

У розділі розглядаються методи інтелектуального захисту даних, що є конфіденційними та повинні передаватися інформаційно-комунікаційними каналами до адресата інформації.

1. Розглянуто інтелектуальні методи запобігання розголошенню інформації технічними засобами.

2. Проведено дослідження технології використання нейронних мереж у процесах інформаційної безпеки.

3. Розкрито методи навчання нейронних мереж, що використовуються в процесі захисту інформації

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи було здійснено такі дії:

- Проведено дослідження методів формування каналів незаконного проникнення в інформаційні системи передачі даних щодо об'єкта інформаційної діяльності.

- Розглянуто потенційні способи використання нейронних технологій для запобігання несанкціонованому доступу до інформаційних каналів передачі даних.

- Досліджено та розроблено методи та процеси використання нейронних технологій для запобігання несанкціонованому доступу до інформаційних каналів передачі даних.

1. У першій частині кваліфікаційного процесу було проведено дослідження способів захисту конфіденційних даних під час передачі через інформаційно-комунікаційні канали, пов'язані з об'єктом інформаційної діяльності.

Розглянуто інтелектуальні стратегії запобігання витоку інформації за допомогою технічних засобів. Наведено опис технології, що використовується у використанні нейронних мереж у процесах інформаційної безпеки. Розкрито методи навчання нейронних мереж, що використовуються в процесі захисту інформації.

2. У другій частині кваліфікації було проведено дослідження способів запобігання несанкціонованому доступу до інформаційних каналів передачі даних щодо об'єкта інформаційної діяльності.

Розглянуто інтелектуальні стратегії запобігання витоку інформації через інформаційні канали. Проведено дослідження технології використання нейронних мереж у процесах інформаційної безпеки. Розкрито методи навчання нейронних мереж, що використовуються в процесі захисту інформації.

3. У третій частині кваліфікаційного завдання оцінено потенційні можливості використання нейронних мереж для запобігання несанкціонованому доступу до інформації щодо передачі даних про інформаційний об'єкт.

Розкрито механізм, за допомогою якого розкриваються методи вимірювання інформаційної безпеки за допомогою нейронних мереж. Пояснено критерії вибору архітектури нейронної мережі, призначеної для захисту інформації, та використано мережу нейронів для апроксимації функції захисту інформації. Показано результати обробки даних інформаційної безпеки за допомогою нейронної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Takagi T., Sugeno M. Fuzzy identification of system and its application for modeling and control. IEEE Trans. Systems, Man and Cybernetics. 1995 V.15 N1P.116-132.

2. Зайченко Ю.П. Нечеткие модели и методи в интеллектуальних системах.-К., „Слово», 2008.- 333 с.

3. Бодянський Є.В., Винокурова О.А.. Інтелектуальна обробка даних на основі гібридної вейвлет-нейро-фаззі системи на адаптивних W - нейронах. // Наукові праці: Науково- методичний журнал. – Миколаїв: Збірка Чорноморського державного університету ім П.Могили 2009.Вип 104.Т.117. – С88-98.

4. Вороновский Г. К. Генетические алгоритмы, искусственные нейронные сети и проблемы виртуальной реальности [Текст] /Г. К. Вороновский, К. В. Махотило, С. Н. Петрашев, С. А. Сергеев. –Харьков: Основа, 1997. – 112 с. – Библиогр.: с. 78–81. – 800 экз. –ISBN 5–7768–0293–8.

5. Уськов А. А. Интеллектуальные технологии управления: искусственные нейронные сети и нечеткая логика [Текст] / А. А. Уськов, А. В. Кузьмин. – М.: Горячая линия – Телеком, 2004. – 143 с. – Библиогр.: с. 124–141. – 1000 экз. – ISBN 5–93517–181–3.

6. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы [Текст] / Д. Рутковская, М. Пилиньский, Л. Рутковский. – М.: Горячая линия – Телеком, 2004. – 452 с. – Библиогр.с. 379–380. – 1500 экз. – ISBN 5–93517–103–1.

7. P. Wasserman. Neural computing: theory and practice / Van Nostrand Reinhold, New-York, 1989.

8. J. S. Albus and A.M. Meystel. Engineering of Mind: An Introduction to the Science of Intelligent Systems / Wiley, New York, 2001.

9. P. Engelbrecht. Computational Intelligence: An Introduction /Wiley, Chichester, U.K., 2002.

10. B. Badiru and J. Y. Cheung. Fuzzy Engineering Expert Systems with Neural Network Applications / John Wiley, New York, NY, 2002.

11. С. Осовский. Нейронные сети для обработки информации – пер. с польского. М.: Финансы и статистика, 2002. – 344с.

12. С. Хайкин. Нейронные сети: полный курс. Вильямс, 2006.

13. Bishop C.M. Pattern Recognition and Machine Learning. Springer, 2006 – 738 p.

14. Усков А.А., Кузьмин А.В. Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика. М.: Горячая линия - Телеком, 2004. – 143 с.

15. Дьяконов В.П., Круглов В.В. MATLAB 6.5 SP1/7/7 SP1/7 SP2 + Simu-link 5/6. Инструменты искусственного интеллекта и биоинформатики. – М.: СОЛОН-ПРЕСС, 2006. – 456 с.

16. Нестерук Г. Ф., Фахрутдинов Р. Ш., Нестерук Ф. Г. К разработке инст-рументальных средств для мониторинга защищенности корпоративной сети // Сб. докл. VIII Междунар. конф. SCM’2005. – СПб.: СПГЭТУ, 2005.

17. Минаев В. А. Перспективы развития IT-security в России // Межотрасле-вой тематический каталог "Системы безопасности-2003". 2003, С. 218 – 221.

18. Осовецкий Л. Г. Научно-технические предпосылки роста роли защиты информации в современных информационных технологиях // Изв. вузов. При-боростроение. 2003. Т.46, № 7. С. 5-18

19. Осовецкий Л. Г., Нестерук Г. Ф., Бормотов В. М. К вопросу иммуноло-гии сложных информационных систем // Изв. вузов. Приборостроение. 2003. Т.46, № 7. С. 34-40

20. Вихорев С. В., Кобцев Р. Ю. Как узнать – откуда напасть или откуда ис-ходит угроза безопасности информации // Защита информации. Конфидент. 2002. № 2.

21. Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г. Адаптивная модель нейросетевых систем информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2003, №3.

22. Нестерук Г.Ф., Куприянов М.С., Нестерук Ф. Г., Нестерук Л. Г. Мето-дика оценки защищенности информационных систем с применением НС и не-четкой логики // SCM’2004: Сборник докладов VI Международной конференции по мягким вычислениям и измерениям. Т.1. – СПб.: СПбГЭТУ, 2004

23. Нестерук Ф. Г., Осовецкий Л.Г., Жигулин Г. П., Нестерук Т.Н. Разработка комплекса показателей для оценки информационных ресурсов и безопасности иерархических систем // РИ-2004: Материалы IX Санкт-Петербургской международной конференции Региональная информатика - 2004 г. – СПб.: СПИИ РАН, 2004

24. Нестерук Г.Ф., Осовецкий Л. Г., Нестерук Ф. Г. К оценке защищенности систем информационных технологий // Перспективные информационные тех-нологии и интеллектуальные системы. 2004, № 1

25. Нестерук Г.Ф., Куприянов М.С., Осовецкий Л.Г., Нестерук Ф.Г. Разра-ботка инструментальных средств для оценки защищенности информационных систем с применением механизмов нечеткой логики и нейронных сетей // SCM’2004: Сборник докладов VII Международной конференции по мягким вы-числениям и измерениям. Т.1. – СПб.: СПбГЭТУ, 2004.

26. Осовецкий Л., Шевченко В. Оценка защищенности сетей и систем // Экспресс электроника. 2002. № 2 - 3. С.20-24.

27. Корнеев В. В., Гареев А. Ф., Васютин С. В., Райх В. В. Базы данных.Интеллектуальная обработка информации. – М.: Нолидж, 2001.

28. Аляутдинов М.А. Использование графических процессоров с параллельной архитектурой для построения масштабируемых нсиро ком пью i ер пых конфигураций Нейрокомпьютеры: разработка, применение. - 2006. - № 8-9. - С. 18-27.

29. Steffen Nissen. Implementation of a Fast Artifitial Neural Network Library. - DIKU. 2003.

30. Gael de La Croix Vaubois, Catherine Moulinoux, Benoit Derot. The N Programming Language Neurocomputing, NATO ASI series. -VoI.F68.-P. 89-92.

31. http://leenissen.dk/fenii/wp/

32. http://neural-networks.ru/Obuchenie-neyrosetey-v-Matlab-58.html

33. http://www.yuvaengineers.com/artificial-neural-network-for-home-security-systemannhss-anil-naik/

34. Хорошко В.А. Методы и средства защиты информации / В.А.Хорошко, А.А.Чекатков.-К.:«Юниор», 2003. – 421 с.

35. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификции сигналов радиозакладных устройств. – К.: ПолиграфКонсалтинг, 2004. – 317 с

36. А.А. Хорев «Способы и средства защиты информации», 2004г.

37. Г.А. Бузов, С.В. Калинин, А.В. Кондратьев Защита от утечки информации по техническим каналам: Учебное пособие – М.: Горячая линия-Телеком, 2005. – 416 с.

38. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко та ін. – К.: ДУІКТ, 2008.

ДОДАТКИ

Додаток А

Система захисту мережевих каналів передачі інформації від несанкціонованого доступу на основі нейронних технологій

Кваліфікаційна робота магістра

Здобувач: Олександр ТУРЧИН
Керівник: Петро ПОНОЧОВНИЙ

Актуальність теми

- широке використання комп’ютерів та мережевих сервісів створює додаткові канали незаконного
- розкриття інформації;
- витік даних через інформаційно-комунікаційні канали порушує конфіденційність, цілісність і
- доступність інформації;
- традиційні експертні оцінки не завжди забезпечують достатню точність визначення рівня
- захищеності;
- нейронні технології дають можливість автоматизувати розпізнавання ознак небезпечних станів і
- підвищити оперативність реагування.

Мета, об’єкт і предмет дослідження

Мета	Об’єкт	Предмет
підвищення ефективності системи запобігання несанкціонованому проникненню в інформаційні канали передачі даних ОІД на основі нейронних технологій.	система захисту конфіденційної інформації об’єкту інформаційної діяльності.	система запобігання несанкціонованому проникненню в інформаційні канали передачі даних ОІД.

Основні задачі

- огляд процесів формування каналів несанкціонованого проникнення;
- аналіз можливостей застосування нейронних технологій для захисту інформації;
- розроблення методів застосування нейронних технологій для запобігання НСД.

Структура роботи

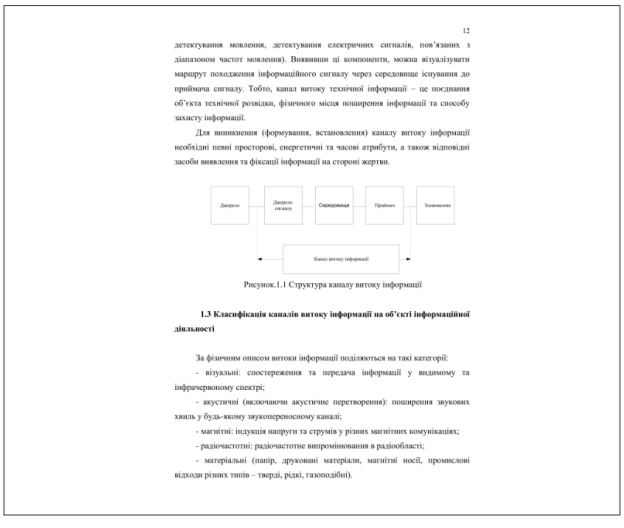
Розділ 1	Розділ 2	Розділ 3
Процеси формування каналів несанкціонованого проникнення	Можливості застосування нейронних мереж для захисту інформації	Методи застосування нейронних технологій і аналіз результатів

Побудова презентації відповідає логіці роботи: від аналізу каналів витоку - до нейромережевої моделі оцінки захищеності та практичних результатів застосування інтелектуальних методів.

Канали витоку інформації в інформаційній мережі ОІД

- технічний канал витоку включає джерело інформації, фізичне середовище поширення та засіб
- перехоплення;
- джерелами можуть бути люди, технічні засоби обробки інформації, лінії зв’язку, акустичні та радіотехнічні
- пристрої;
- сигнали можуть мати електричну, магнітну, акустичну, оптичну або матеріальну природу;
- ефективний захист потребує ідентифікації кожного потенційного каналу та оцінки його небезпечності.

Структура каналу витоку інформації



12

детектування мовлення, детектування електричних сигналів, пов’язаних з діапазоном частот мовлення). Виявивши ці компоненти, можна візуалізувати маршрут походження інформаційного сигналу через середовище існування до приймача сигналу. Тобто, канал витоку технічної інформації – це поєднання об’єкта технічної розвідки, фізичного місця поширення інформації та способу захисту інформації.

Для виникнення (формування, встановлення) каналу витоку інформації необхідні певні просторові, енергетичні та часові атрибути, а також відповідні засоби виявлення та фіксації інформації на стороні жертви.

Рисунок.1.1 Структура каналу витоку інформації

1.3 Класифікація каналів витоку інформації на об’єкті інформаційної діяльності

За фізичним описом витоки інформації поділяються на такі категорії:

- візуальні: спостереження та передача інформації у видимому та інфрачервоному спектрі;
- акустичні (включаючи акустичне перетворення): поширення звукових хвиль у будь-якому звукопереносному каналі;
- магнітні: індукція напруги та струмів у різних магнітних комунікаціях;
- радіочастотні: радіочастотне випромінювання в радіообласті;
- матеріальні (папір, друковані матеріали, магнітні носії, промислові відходи різних типів – тверді, рідкі, газоподібні).

- канал формується за наявності джерела сигналу,
- середовища передачі та приймача з боку порушника;
- для виникнення каналу потрібні просторові, енергетичні
- та часові умови;
- наявність завад знижує якість сигналу, але не ліквідує сам
- ризик витоку;
- модель каналу є основою для вибору технічних і
- організаційних заходів протидії.

Класифікація каналів витоку інформації

Візуальні	видимий, інфрачервоний та ультрафіолетовий діапазони
Акустичні	поширення звукових хвиль і вібрацій у конструкціях
Електромагнітні	побічні випромінювання і наведення технічних засобів
Матеріальні	паперові носії, чернетки, магнітні носії, відходи
Радіочастотні	паразитна генерація, ВЧ-нав’язування, радіозакладки

Радіоканали витоку інформації

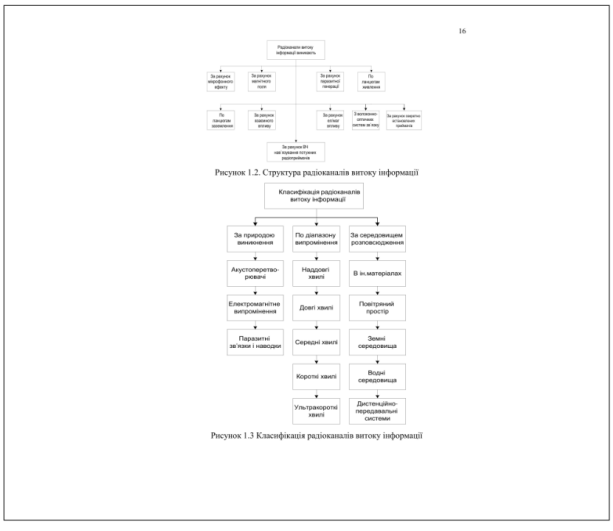


Рисунок 1.3 Класифікація радіоканалів витоку інформації

- радіоканали можуть виникати через мікрофонний ефект,
- магнітне поле, паразитну генерацію, ланцюги живлення та
- заземлення;
- джерелами небезпечних сигналів є елементи, вузли та
- провідники технічних засобів;
- класифікація враховує природу виникнення, діапазон
- випромінювання та середовище поширення;
- захист потребує екранування, фільтрації, контролю ПЕМВН та
- режимних заходів.

Методи протидії витоку конфіденційних даних

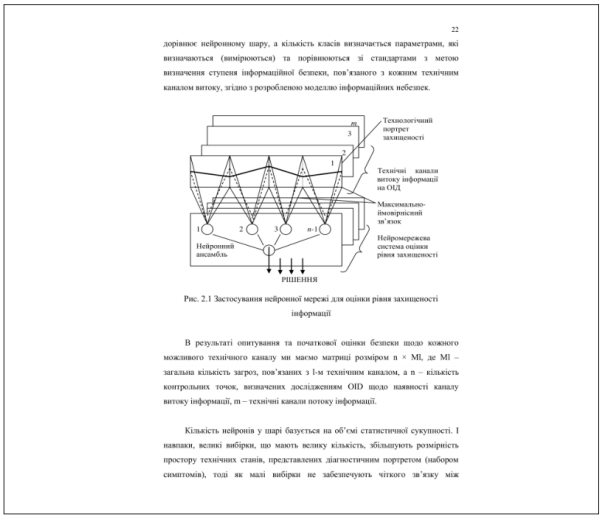
Організаційні заходи

- проектування системи безпеки об’єкта;
- розмежування зон доступу та режимних приміщень;
- запобігання візуальному спостереженню документів
- і екранів;
- захист мовної інформації від акустичного
- прослуховування;

Технічні заходи

- екранування та фільтрація побічних випромінювань;
- контроль ланцюгів живлення і заземлення;
- використання технічних засобів охорони та СКУД;
- регламент перевірки каналів витоку і засобів захисту.

Метод оцінки рівня захищеності на основі нейронних технологій



22

дорівнює нейронному шару, а кількість класів визначається параметрами, які визначаються (вимірюються) та порівнюються зі стандартами з метою визначення ступеня інформаційної безпеки, пов’язаного з кожним технічним каналом витоку, згідно з розробленою моделлю інформаційних небезпек.

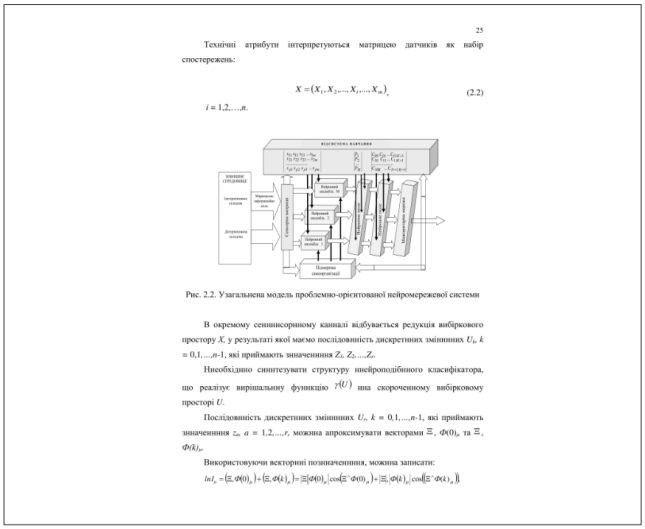
Рис. 2.1 Застосування нейронної мережі для оцінки рівня захищеності інформації

В результаті опитування та початкової оцінки безпеки щодо кожного можливого технічного каналу ми маємо матриці розміром n × Ml, де Ml – загальна кількість загроз, пов’язаних з l-м технічним каналом, а n – кількість контрольних точок, визначених дослідженням ОІД щодо наявності каналу витоку інформації, m – технічні канали потоку інформації.

Кількість нейронів у шарі базується на об’ємі статистичної сукупності. І навпаки, великі вибірки, що мають велику кількість, збільшують розмірність простору технічних станів, представлених діагностичним портретом (набором симптомів), тоді як малі вибірки не забезпечують чіткого зв’язку між

- нейромережева система використовує технологічний
- портрет захищеності ОІД;
- для кожного технічного каналу формується набір
- контрольованих параметрів;
- нейронні ансамблі зіставляють ознаки з класами стану
- захищеності;
- рішення формується як результат максимального
- ймовірнісного зв’язку між ознаками та класами.

Узагальнена модель проблемно-орієнтованої НМС



25

Технічні атрибути інтерпретуються матрицею датчиків як набір спостережень:

$$X = (X_1, X_2, ..., X_i, ..., X_m)_i \qquad (2.2)$$

$i = 1,2,...,n.$

Рис. 2.2. Узагальнена модель проблемно-орієнтованої нейромережевої системи

В окремому сенинсорному каналі відбувається редукція вибіркового простору X_i у результаті якої маємо послідовність дискретних змінних U_k, $k = 0,1,...,n\text{-}1$, які приймають значеннння $Z_0, Z_1, ..., Z_r$.

Необхідно синтезувати структуру нейроподібного класифікатора, що реалізує вирішальну фуункцію $\gamma(U)$ ина скороченному вибірковому просторі U.

Послідовність дискретних змінниних U_k, $k = 0,1,...,n\text{-}1$, які приймають зниаченнння z_a, $a = 1,2,...,r$, можина апроксимувати векторами Ξ, $\Phi(0)_a$ та Ξ, $\Phi(k)_a$.

Використовуючи векториці позиначеннння, можина записати:

$$In I_a = (\Xi, \Phi(0)_a) + (\Xi, \Phi(k)_a) = |\Xi||\Phi(0)|_a |\cos(\widehat{\Xi \cdot \Phi(0)}_a) + |\Xi||\Phi(k)|_a |\cos(\widehat{\Xi \cdot \Phi(k)}_a)|$$

- сенсорна матриця сприймає спостереження з
- інформаційного поля;
- нейронні ансамблі виконують класифікацію технічних
- станів;
- нейронні поля враховують апріорні ймовірності та
- матрицю вартості рішень;
- підсистема навчання забезпечує налаштування зв’язків і
- підвищення якості розпізнавання.

Вибір архітектури нейронної мережі

Вхідний шар	параметри контрольних точок, ознаки каналів витоку, результати вимірювань та експертних оцінок.
Приховані шари	виявлення нелінійних залежностей між технічними ознаками, станами каналів і класами загроз.
Вихідний шар	класифікація рівня захищеності або імовірності небезпечного стану.
Навчання	коригування вагових коефіцієнтів за навчальною вибіркою та перевірка на контрольних даних.

Функція захисту інформації на основі нейронної технології

1. збирання параметрів технічних каналів витоку інформації;
2. формування діагностичного портрета стану захищеності;
3. класифікація стану за допомогою нейронної мережі;
4. виявлення небезпечних відхилень від допустимого рівня захищеності;
5. формування рішення щодо необхідних заходів протидії.

Інтелектуальні методи запобігання НСД

Нейронні мережі	розпізнавання прихованих закономірностей у параметрах мережі та каналів витоку.
Нечітка логіка	робота з неповними, нечіткими та експертними оцінками рівня небезпеки.
Системи правил	формування зрозумілих умов реагування за виявленими ознаками атак або витоку.
Гібридний підхід	поєднання статистичних, нейромережевих та експертних моделей для підвищення достовірності.

Основні результати роботи

- проаналізовано процеси формування каналів витоку інформації в інформаційних мережах ОІД;
- узагальнено класифікацію каналів витоку та методи протидії витоку конфіденційних даних;
- розглянуто метод оцінки рівня захищеності із застосуванням нейронних технологій;
- обґрунтовано архітектурні складові нейромережевої системи оцінки стану захисту;
- сформовано підхід до застосування інтелектуальних засобів для запобігання НСД.

тичне значення: підвищення оперативності та достовірності оцінки захищеності каналів передачі д