КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій
(факультет)

інформаційних технологій проектування та прикладної математики
(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

на тему: «Побудова нейромережевих засобів оцінки параметрів безпеки інтернет-ресурсів інформаційних систем»

Булава Роман Юрійович
(прізвище, ім’я та по батькові студента повністю)

Київ 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій
(факультет)

інформаційних технологій проектування та прикладної математики
(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТППМ
д.т.н., професор Терентьєв О.О.
_____

„___” _____2023 року

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

на тему: «Побудова нейромережевих засобів оцінки параметрів безпеки інтернет-ресурсів інформаційних систем»

Виконав: студент ІІ-го курсу, групи ІСТм-І1 .

Спеціальності: 126 «Інформаційні системи та технології»
(шифр і назва напряму підготовки, спеціальності)

Булава Р.Ю. .
(прізвище та ініціали)

Керівники к.ф-м.н., доц. Доля О.В. .
(прізвище та ініціали)
Рецензент к.т.н., доц. Шабала Є.Є. .
(прізвище та ініціали)

Київ, 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій .
Кафедра: інформаційних технологій проектування та прикладної математики.
Освітній рівень: «магістр за ОПП» .
Спеціальність: 126 «Інформаційні системи та технології» .

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТППМ
д.т.н., професор Терентьєв О.О.
_____

„___” __ ___2023 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

Булава Роман Юрійович
1. Тема роботи: Побудова нейромережевих засобів оцінки параметрів безпеки інтернет-ресурсів інформаційних систем .
затверджена наказом ректора КНУБА № ___ від «__» _червень 2023 р.
2. Керівник роботи: Доля Олена Вікторівна, к.ф-м.н, доцент кафедри інформаційних технологій проектування і прикладної математики .
3. Строк подання студентом роботи до захисту: грудень 2023 року .
4. Зміст пояснювальної записки за розділами:
Р.1. Аналіз предметної області та постановка задачі .
Р.2. Побудова нейромережевих методів оцінки параметрів безпеки інтернет-орієнтованих інформаційних систем .
Р.3. Нейромережева система оцінки параметрів безпеки інтернет орієнтованих інформаційних систем .
Р.4. Ергономіка інформаційних технологій .
5. Інформаційні слайди:
С.1. Програмні засоби захисту, в яких оцінюються параметри безпеки .
С.2. Структура моделі MPNN
С.3. Оцінка можливості застосування нейромережевих методів для виявлення кібератак .

С.4. Структура системи розпізнавання мережевих кібератак .
С.5. Склад нейромережевої системи розпізнавання мережевих кібератак .

6. Календарний план виконання атестаційної випускової роботи

Види робіт та їх зміст	Дата виконання
Р. 1. Аналіз предметної області та постановка задачі	Вересень 2023 р.
Р. 2. Побудова нейромережевих методів оцінки параметрів безпеки інтернет-орієнтованих інформаційних систем	Жовтень 2023 р.
Р. 3. Нейромережева система оцінки параметрів безпеки інтернет-орієнтованих інформаційних систем	Листопад 2023 р.
Р. 4. Ергономіка інформаційних технологій	Грудень 2023 р.
Остаточне оформлення роботи	Грудень 2023 р.
Попередній захист роботи на кафедрі	Грудень 2023 р.

7. Консультанти розділів атестаційної випускової роботи

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	дата	підпис
Ергономіка інформаційних технологій	д.т.н. проф. Терентьєв О.О.		
Експериментальні дослідження	к.т.н. доц. Шабала Є.Є.		

8. Дата видачі завдання: 05 вересня 2023 року

Керівник _____ Доля О.В.
(підпис) (прізвище та ініціали)

Магістр _____ Булава Р.Ю.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Булава Р.Ю. «Побудова нейромережевих засобів оцінки параметрів безпеки інтернет-ресурсів інформаційних систем».

Атестаційна випускова робота бакалавра за спеціальністю: 126 «Інформаційні системи та технології», спеціалізація: «Інформаційні системи та технології». – Київський національний університет будівництва та архітектури. – Київ, 2023.

Отримані результати дозволяють визначити недоліки сучасних нейромережевих засобів виявлення кібератак та засобів виявлення вразливостей і окреслити перспективні шляхи їх вдосконалення.

Ключові слова: моделі, методи, нейромережа, безпека інтернет-ресурсів інформаційних систем.

SUMMARY

Bulava R.Yu "Construction of neural network tools for evaluating security parameters of Internet resources of information systems".

Attestation work of a bachelor's degree on a specialty: 126 "Information systems and technologies", specialization: "Information systems and technologies". - Kyiv National University of Construction and Architecture. - Kyiv, 2023.

The obtained results allow to determine the disadvantages of modern neural network means of detecting cyber attacks and means of identifying vulnerabilities and outlining promising ways of their improvement.

Keywords: models, methods, neural network, security of Internet resources of information systems.

ЗМІСТ

ВСТУП

Одною із основних перешкод широкому впровадженню нейромережевих методів та моделей в системах виявлення кібератак та в системах виявлення вразливостей ресурсів інформаційних систем є відсутність параметрів на основі яких можливо оцінити їх ефективності. Також відсутні і методи оцінки ефективності такого впровадження. Для вирішення цієї проблеми був проаналізований широкий спектр сучасних нейромережевих методів та моделей, що застосовуються у зазначених системах виявлення. Визначено перелік параметрів і розроблено метод їх використання для оцінки ефективності розробки та вибору вказаних методів та моделей при побудові означених систем виявлення. Отримані результати дозволяють визначити недоліки сучасних нейромережевих засобів виявлення кібератак та засобів виявлення вразливостей і окреслити перспективні шляхи їх вдосконалення.

В теперішній час створення перспективних систем забезпечення інформаційної безпеки (ІБ) ресурсів інформаційних систем (РІС) асоціюється з використанням інтелектуальних засобів, що функціонують з використанням методів та моделей теорії нейронних мереж (НМ). Відповідно до результатів нейромережеві методи та моделі в основному використовуються для виявлення (розпізнавання) кібератак та вразливостей РІС. Крім того, НМ використовуються для управління параметрами захисту. Перспективність використання нейромережевих методів та моделей підтверджується окремими вдалими застосуваннями НМ в системах виявлення кібератак (СВК) (продукція компанії Cisco) та великою кількістю відповідних теоретико-практичних робіт. Разом з тим велика кількість хибних спрацювань, довготривалий термін та нестабільність навчання, недостатня адаптація до багатьох особливостей сучасного стану РІС значно обмежують їх практичну цінність. Тому в сучасних умовах гостро стоїть проблема обґрунтованої оцінки ефективності застосування нейромережевих методів та моделей в СВК

та в системах виявлення вразливостей (СВВ). Проблема ускладнюється тим, що аналіз вказує на відсутність в теперішній час базового набору параметрів, використання яких дозволило б хоча б в першому наближенні визначити ефективність застосування нейромережевого інструментарію в СВК та СВВ.

Результати дозволяють стверджувати, що виявлення (розпізнавання) кібератак та вразливостей РІС за допомогою НМ в основному зводиться до оцінок величин параметрів безпеки РІС. Якщо виставлена за допомогою НМ оцінка перевищує певне граничне значення, то вважається, що кібератака (вразливість) виявлені. В протилежному випадку вважається, що рівень безпеки знаходиться в допустимих межах. При цьому, по аналогії з загальновідомим терміном діагностичний параметр, під терміном параметр безпеки РІС будемо розуміти фізичну величину, що характеризує стан забезпечення конфіденційності, цілісності та доступності інформації РІС, а під терміном кібератаки (кібернетичної атаки) на РІС будемо розуміти реалізацію у кібернетичному просторі загроз безпеці його компонентів (а саме конфіденційності, цілісності та доступності) з урахуванням їх вразливостей. Зазначимо, що відповідно кібернетичний простір – це віртуальний простір, отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій для підтримки та управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства.

Таким чином, посилення вимог до ефективності систем розпізнавання кібератак на ресурси інтернет-орієнтованих ІС, перспективність використання нейромережевих методів оцінки параметрів безпеки для розпізнавання кібератак, невідповідність їх характеристик до змін умов застосування нових видів кібератак і можливості роботи при обмежених розрахункових ресурсів зумовлюють актуальність даної теми, яка за рахунок вибраних характеристик дозволить швидко розпізнавати нові види кібератак при обмежених розрахункових можливостях.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БШП – багатошаровий персептрон

ІС – інформаційна система

ЛМ – ланцюг Маркова

НМ – нейронна мережа

НМЗ – нейромережеві засоби

НММ – нейромережева модель

НМС – нейромережева система

ПБ – параметри безпеки

РБФ – нейронна мережа з радіальними базисними функціями

СВА – система виявлення атак

СД – слой додавання

СЗІ – система захисту інформації

СО – слой образів

СРА – система розпізнавання атак

СФ – слой фільтрації

ТК – топографічна карта Кохонена

ША – шаблон атаки

ШНМ – штучна нейронна мережа

ШНП – шаблон нормальної поведінки

ШП – шаблон поведінки

ШПО – шкідливе програмне забезпечення

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Загальна характеристика нейронних мереж

Штучні нейронні мережі (англ. artificial neural networks, ANN), або конективістські системи (англ. connectionist systems) — це обчислювальні системи, за основу в яких взяті біологічні нейронні мережі, які складають мозок тварин. Такі системи навчаються задач (поступально покращують свою продуктивність на них), розглядаючи приклади, загалом без спеціального програмування під задачу. Наприклад, у розпізнаванні зображень вони можуть навчатися ідентифікувати зображення, які містять котів, аналізуючи приклади зображень, мічені як «кіт» і «не кіт», і використовуючи результати для ідентифікування котів в інших зображеннях. Вони роблять це без жодного апріорного знання про котів, наприклад, що вони мають хутро, хвости, вуса та котоподібні писки. Натомість, вони розвивають свій власний набір доречних характеристик з навчального матеріалу, який вони оброблюють.

Штучні нейронні мережі (надалі ШНМ) є зручним і природним базисом для подання інформаційних моделей. Нейромережа може бути досить формально визначена, як сукупність простих процесорних елементів (часто званих нейронами), що володіють повністю локальним функціонуванням, і об'єднаних односпрямованими зв'язками (званими синапсами). Мережа приймає деякий вхідний сигнал із зовнішнього світу, і пропускає його крізь себе з перетвореннями в кожному процесорному елементі. Таким чином, в процесі проходження сигналу по зв'язках мережі відбувається його обробка, результатом якої є певний вихідний сигнал. У збільшеному вигляді ШНМ виконує функціональну відповідність між входом і виходом, і може служити інформаційною моделлю G системи F.

ШНМ ґрунтується на сукупності з'єднаних вузлів, що називають штучними нейронами (аналогічно до біологічних нейронів у головному мозку тварин). Кожне з'єднання між штучними нейронами може передавати сигнал

від одного до іншого. Штучний нейрон, що отримує сигнал, може обробляти його, й потім сигналізувати штучним нейронам, приєднаним до нього.

В поширених реалізаціях ШНМ сигнал на з'єднанні між штучними нейронами є дійсним числом, а вихід кожного штучного нейрону обчислюється нелінійною функцією суми його входів. Штучні нейрони та з'єднання зазвичай мають вагу, яка підлаштовується в перебігу навчання. Вага збільшує або зменшує силу сигналу на з'єднанні. Штучні нейрони можуть мати такий поріг, що сигнал надсилається лише якщо сукупний сигнал перетинає цей поріг. Штучні нейрони зазвичай організовано в шари. Різні шари можуть виконувати різні види перетворень своїх входів. Сигнали проходять від першого (входового) до останнього (виходового) шару, можливо, після проходження шарами декілька разів.

Первинною метою підходу ШНМ було розв'язання задач таким же способом, як це робив би людський мозок. З часом увага зосередилася на відповідності певним розумовим здібностям, ведучи до відхилень від біології. ШНМ використовували в ряді різноманітних задач, включно з комп'ютерним баченням, розпізнаванням мовлення, машинним перекладом, соціально-мережевим фільтруванням, грою в настільні та відеоігри, та медичним діагностуванням.

Нейромережа – це система, яка має здатність до навчання. Вона діє не тільки відповідно до заданого алгоритма та формул, але і на підставі минулого досвіду. Така собі дитина, яка з кожним разом складає пазл, роблячи все менше помилок.

Отже, ШНМ – це мережа простих елементів, так званих нейронів, які отримують вхід, змінюють свій внутрішній стан (збудження) відповідно до цього входу, і виробляють вихід, залежний від входу та збудження. Мережа утворюється з'єднанням виходів певних нейронів зі входами інших нейронів з утворенням орієнтованого зваженого графу. Ваги, як і функції, що

обчислюють збудження, можуть змінюватися процесом, званим навчанням, який керується правилом навчання.

1.1.1 Основні складові штучних нейронних мереж

Основними складовими ШНИ є: нейрони, синапс(вага), функція поширення, тренувальний сет, ітерація, епоха, помилка.

Нейрон – це обчислювальна одиниця, яка отримує інформацію, виробляє над нею прості обчислення і передає її далі. Вони діляться на три основних типи (рис.1.1): вхідний (синій), прихований (червоний) і вихідний (зелений). Також існують такі типи нейронів – зміщення і контекстний.

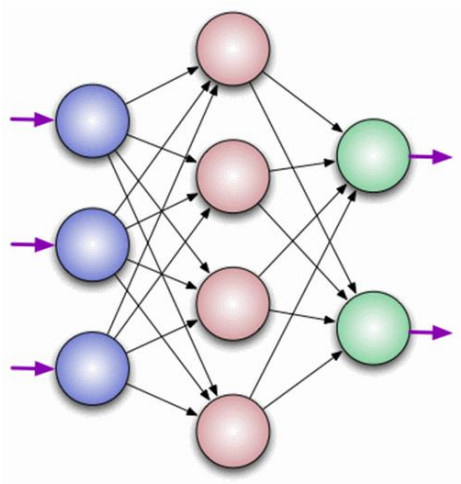

Рисунок 1.1 Графічне зображення нейрону в ШНМ

У тому випадку, коли нейромережа складається з великої кількості нейронів, вводять термін шару. Відповідно, є вхідний шар, який отримує інформацію, n прихованих шарів, які її обробляють і вихідний шар, який виводить результат. У кожного з нейронів є 2 основні параметри: вхідні дані (input data) і вихідні дані (output data). У разі вхідного нейрона: input = output. В інших, в поле input потрапляє сумарна інформація всіх нейронів з попереднього шару, після чого, вона нормалізується, за допомогою функції активації і потрапляє в поле output.

Нейрон входу (input neuron) не має попередників, а слугує інтерфейсом входу для всієї мережі. Аналогічно, нейрон виходу (output neuron) не має наступників, і відтак слугує інтерфейсом виходу для всієї мережі.

Важливо пам'ятати, що нейрони оперують числами в діапазоні [0,1] або [-1,1].

Мережа складається зі з'єднань, кожне з яких передає вихід нейрону i до входу нейрону j. В цьому сенсі i є попередником, а j є наступником i. Тому кожному з'єднанню призначено вагу (weight) ω_{ij}.

Синапс це зв'язок між двома нейронами. У синапсів є 1 параметр - вага. Завдяки йому, вхідна інформація змінюється, коли передається від одного нейрона до іншого. Припустимо, є 3 нейрона (Рис.1.2), які передають інформацію з наступних підстав. Тоді у нас є 3 ваги, відповідні кожному з цих нейронів. У того нейрона, у якого вага буде більше, та інформація і буде домінуючою в наступному нейроні.

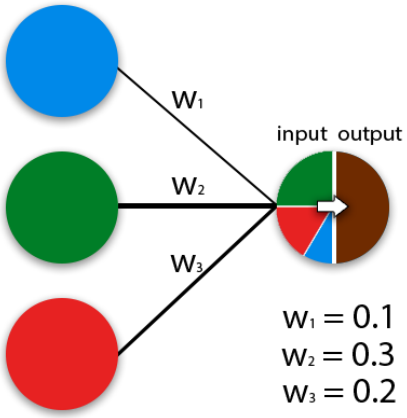

Рисунок 1.2 Графічне пояснення ваги у нейроні

Сукупність ваг нейронної мережі або матриця ваг – це своєрідний мозок всієї системи. Саме завдяки цим вагам, вхідна інформація обробляється і перетворюється в результат. Під час ініціалізації нейронної мережі, ваги розставляються в випадковому порядку.

Функція активації – це спосіб нормалізації вхідних даних. Тобто, якщо на вході у нас буде велике число, то пропустивши його через функцію

активації, ми отримаємо вихід в потрібному вам діапазоні. Функцій активації досить багато тому ми розглянемо найосновніші: лінійна, сигмоїдна (логістична) і гіперболічний тангенс. Головні їх відмінності - це діапазон значень.

Лінійна функція $f(x) = x$ ця функція майже ніколи не використовується, за винятком випадків, коли потрібно протестувати нейронну мережу або передати значення без перетворень.

Сигмоїдна функція $f(x) = \frac{1}{1+e^{-x}}$ це найпоширеніша функція активації, її діапазон значень [0,1] її іноді називають логістичною функцією.

Гіперболічний тангенс $f(x) = \frac{e^{2x}-1}{e^{2x}+1}$ маємо сенс використовувати гіперболічний тангенс, тільки тоді, коли наші значення можуть бути і негативними, і позитивними, так як діапазон функції [-1,1]. Використовувати цю функцію тільки з позитивними значеннями недоцільно так як це значно погіршить результати нейромережі.

Тренувальний сет – це послідовність даних, якими оперує нейронна мережа.

Ітерація – це загальна кількість тренувальних сетів пройдених нейронною мережею.

Епоха при ініціалізації нейронної мережі ця величина встановлюється в 0, що задається вручну. Чим більше епоха, тим краще натренована мережу і відповідно, її результат. Епоха збільшується кожного разу, коли ми проходимо весь набір тренувальних сетів.

Важливо не плутати ітерацію з епохою і розуміти послідовність їх інкременти, спочатку *n* раз збільшується ітерація, а потім вже епоха і ніяк не навпаки. Іншими словами, не можна спочатку тренувати нейромережу тільки на одному сеті, потім на іншому. Потрібно тренувати кожен сет один раз за добу. Так, ви зможете уникнути помилок в обчисленнях.

Помилка – це процентна величина, що відображає розбіжність між очікуваним і отриманими відповідями. Помилка формується кожну епоху і повинна йти на спад. Помилку можна обчислити різними шляхами, але тут буде розглянуто лише три основних способи: Mean Squared Error (MSE), Root MSE і Arctan. Тут немає якогось обмеження на використання, як у функції активації, і ви вільні вибрати будь-який метод, який буде приносити найкращий результат. Варто лише враховувати, що кожен метод вважає помилки по різному. У Arctan, помилка, майже завжди, буде більше, так як він працює за принципом: чим більша різниця, тим більше помилка. У Root MSE буде найменша помилка, тому, найчастіше, використовують MSE, яка зберігає баланс в обчисленні помилки.

MSE:

$$\frac{(i_1-a_1)^2+(i_2-a_2)^2+\cdots+(i_n-a_n)^2}{n};$$

Root MSE:

$$\sqrt{\frac{(i_1-a_1)^2+(i_2-a_2)^2+\cdots+(i_n-a_n)^2}{n}};$$

Arctan:

$$\frac{arctan^2(i_1-a_1)+\cdots+arctan^2(i_n-a_n)}{n};$$

Принцип підрахунку помилки у всіх випадках однаковий. За кожен сет, ми рахуємо помилку, віднявши від ідеальної відповіді, отриманий результат. Далі, або зводимо до квадрата, або обчислюємо квадратний тангенс з цієї різниці, після чого отримане число ділимо на кількість сетів.

1.2 Аналіз нейромережевих засобів оцінки параметрів безпеки інтернет-орієнтованих інформаційних систем (ІС)

Одним з основних ознак розвитку сучасного суспільства є подальше зростання залежності від якості і надійності комп'ютеризованих ІС, застосовуваних у різних областях людської діяльності. Відповідне посилення стратегічної спрямованості інформаційних ресурсів обумовлює необхідність

підвищення вимог до рівня їх інформаційної безпеки. Проблема загострюється тим, що особливості найбільшої глобальної мережі Інтернет, з якої інтегровано більшість ІС, і використання загальнодоступного програмного забезпечення призводять до значних обсягів випадкових і непередбачених негативних впливів на зазначені системи. Відзначимо, що Інтернет-орієнтація ІС розглядається в ракурсі необхідності захисту ресурсів таких систем від кібератак в процесі реалізації базових технологічних процесів отримання, зберігання, транспортування, обробки та подання інформації. При цьому під поняттям кібератак будемо розуміти реалізацію в кібернетичному просторі загроз безпеки його компонентів (зокрема конфіденційності, цілісності і доступності) з урахуванням їх вразливостей. У той же час кіберпростір – це віртуальний простір, отримане в результаті взаємодії користувачів, програмного і апаратного забезпечення, мережевих технологій для підтримки та управління процесами перетворення інформації з метою забезпечення інформаційних потреб суспільства.

У загальному випадку під поняттям інформаційна безпека розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноти, несвоєчасні і недостовірності використовуваної інформації; негативного інформаційного впливу; негативних наслідків застосування інформаційних технологій; несанкціонованого поширення, використання, порушення цілісності, конфіденційності та доступності інформації. У той же час під поняттям безпеки інформації (information security) розуміють стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. При цьому під поняттям захисту інформації в інформаційних системах розуміють діяльність, яка спрямована на забезпечення безпеки оброблюваної в ІС інформації та ІС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків в результаті реалізації загроз.

З позицій джерел виникнення недоліків і деструктивних впливів від інформаційної безпеки відокремлюють функціональну. При цьому у визначенні функціональної безпеки акцент ставиться на правильності функціонування і вважається, що вона в основному пов'язана з ненавмисно реалізованими деструктивними факторами, помилки носять випадковий характер, а еталонний стан об'єкта, відхилення від якого вказує на помилку, відомо. Однак складність і багатофакторність процесів функціонування ресурсів сучасних Інтернет-орієнтованих ІС в більшості випадків вказує на неможливість окремого оцінювання параметрів функціональної та інформаційної безпеки.

Підтверджується висновок про недоцільність виділення параметрів оцінки стверджується, що рівень функціональної безпеки системного засобу визначається тим, наскільки адекватно співвідноситься набір механізмів захисту умов конкретного використання і тим, наскільки коректні дані механізми реалізовані. При цьому вказується, що недостатність механізмів захисту, так і некоректність їх реалізації визначають уразливість системних засобів. Поділ дестабілізуючих чинників на умисні й випадкові не передбачено. Тому, можна вважати, що процедура оцінки ПБ ІС зводиться до визначення величин параметрів безпеки, які свідчать про наявність / відсутність кібератак. При цьому під поняттям безлічі параметрів безпеки будемо розуміти безліч параметрів, які відображають стан безпеки об'єктів захисту ІС. У загальному випадку множина ПБ Інтерент-орієнтованих ІС формуються на основі аналізу:

- Параметрів вхідних і вихідних мережевих з'єднань з використанням різних протоколів.

- Потенційно небезпечного програмного коду, який передається в ІС.

- Параметрів, що відображають функціонування системного та прикладного програмного забезпечення ІС.

- Функціональні параметри апаратного забезпечення ІС;

- Параметри, що характеризують зміст інформації, яка передається в ІС.

Джерелом статистичних даних для формування такої безлічі ПБ є системні журнали операційних систем робочих станцій і серверів ІС, бази даних засобів захисту інформації (мережевих журналів, антивірусів, систем захисту від спаму, DLP-систем), а також бази даних параметрів кібератак (КДД- 99).

Проведемо декомпозицію проблеми оцінки ПБ Інтернет- орієнтованих ІС для розпізнавання кібератак. Відзначимо, що акцент ставиться па ІС загального призначення, які в основному використовуються в сферах організаційного управління, промисловості і економіці. Згідно з характерними властивостями Інтернет-орієнтованими ІС є:

- Підтримка типових Інтернет-сервісів (веб-сайту, електронної пошти);

- Складність опису (досить велика кількість функцій, процесів, елементів даних і складні взаємозв'язки між ними).

- Різнорідність методів і моделей, використаних при побудові її компонентів.

- Наявність сукупності тісно взаємодіючих компонентів (підсистем), що мають свої локальні завдання і цілі функціонування (наприклад, традиційних додатків, пов'язаних з обробкою транзакцій і рішенням регламентних задач і додатків аналітичної обробки підтримки прийняття рішень), що використовують нерегламентовані запити до даних великого обсягу.

- Функціонування в неоднорідному середовищі на декількох апаратно-програмних платформах.

- Необхідність постійної інтеграції в ІС існуючого і нового програмного забезпечення.

- Використання програмного забезпечення, створеного роз’єднаними і різнорідними групами розробників з різним рівнем кваліфікації та традиціями використання тих чи інших інструментальних засобів.

- Використання програмного забезпечення, яке в багатьох випадках не має офіційної підтримки і несе в собі потенційну загрозу безпеці за рахунок помилок і люків, які можуть проявлятися тільки в певних умовах експлуатації.

- Широке використання в програмному забезпеченні архітектури розподілених об'єктів.

- Складнощі адміністрування як в штатних умовах експлуатації, так і при модифікації програмного забезпечення.

- Формування управлінських рекомендацій на основі обробки великих обсягів різнорідної інформації.

- Необхідність постійної актуалізації інформаційних ресурсів.

- Тісна інтеграція з іншими інтернет-орієнтованими ІС, частина з яких несуть в собі потенційні загрози як навмисного, так і не навмисного характеру.

- Тісна взаємодія з зовнішнім інтернет-середовищем, яке включає в себе велику кількість інформаційно-програмних деструктивних засобів.

- Стандартизація та уніфікація процедур взаємодії між різними функціональними блоками ІС.

- Інтелектуалізація процедур обробки даних, що значно ускладнює оцінки керуючих сигналів ІС.

- Адаптованість до користувачів з різною кваліфікацією, що значно зменшує ефективність захисту від деструктивних впливів.

- Взаємодія з віддаленими користувачами.

- Децентралізація управління як системою захисту, так і всієї ІС в цілому, що в багатьох випадках визначає запізнення і зменшення ефективності управлінських впливів.

Простір зазначених властивостей показано на рис. 1.3, а їх аналіз дозволяє стверджувати, що основними факторами, що визначають особливості оцінки ПБ вітчизняних Інтернет-орієнтованих ІС, є:

- Складність розпізнавання кібератак внаслідок складності встановлення явного зв'язку між порушенням інформаційної безпеки і певним видом

кібератак, складністю визначення вразливостей програмного забезпечення та наслідків реалізації кібератак, можливістю виникнення порушення інформаційної безпеки без явно вираженої кібератаки, високою варіативністю кібератак.

- Виникнення нових видів кібератак через постійне вдосконалення методів і засобів здійснення кібератак, використання нових інтернет-сервісів.

- Необхідність функціонування при обмежених обчислювальних ресурсах, викликаних використанням бюджетного апаратного забезпечення і розташування на одній апаратній платформі інтернет-серверів разом з СЗІ.

- Варіативність умов застосування, що обумовлюється реконфігурацією ІС, зміною програмно-апаратного забезпечення об'єктів ІС, модифікацією інтернет-сервісів, кваліфікацією адміністративного персоналу та ін.

При цьому результати вказують на те, що типові порушення захищеності Інтернет-орієнтованих ІС виникають унаслідок деструктивного впливу:

- ШПО, розміщеного на веб-сторінках.

- ШПО, яке поширюється за допомогою електронної пошти.

- Витоків текстової інформації з використанням засобів електронної пошти.

- Нецільових електронних листів (спаму).

- Видалених мережевих кібератак на Інтернет-сервери.

Наслідками деструктивних впливів може бути як порушення інформаційної безпеки типових Інтернет-сервісів, так і порушення інформаційної безпеки всіх інших функціональних блоків ІС.

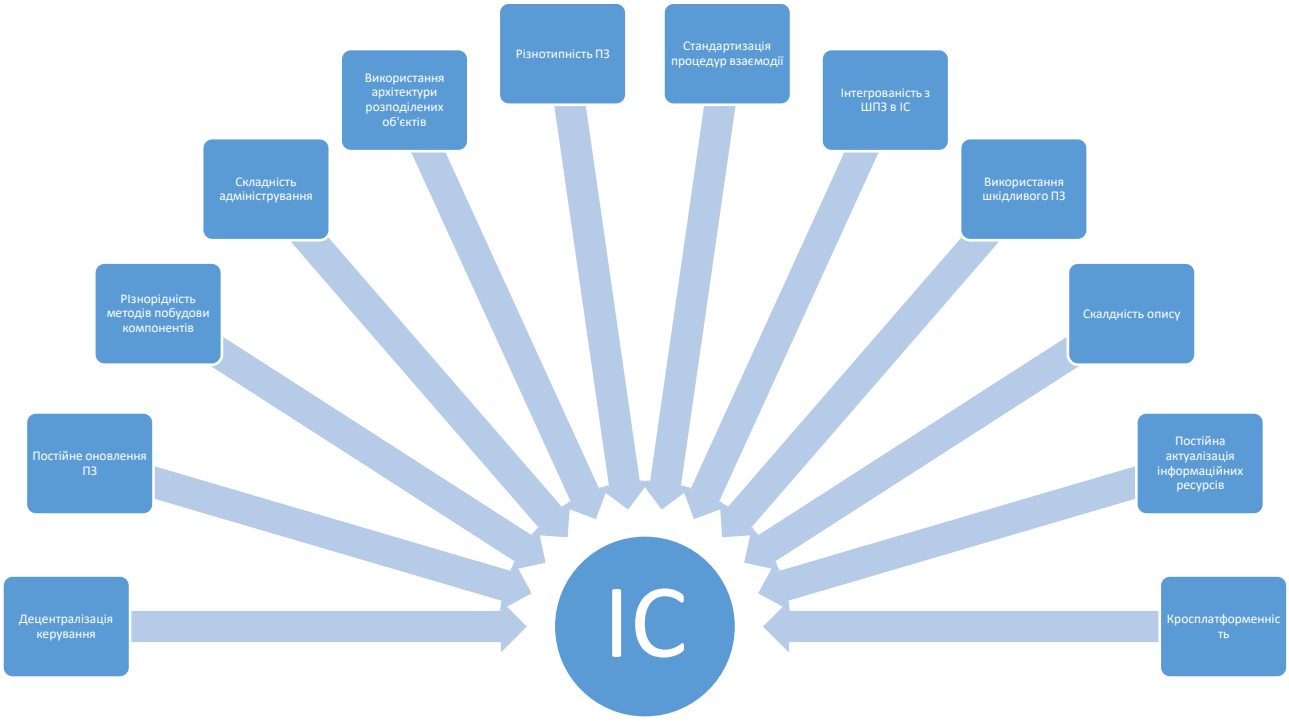

Рисунок 1.3 Властивість Інтернет-орієнтованих ІС

Також потрібно вказати на необхідність захисту від деструктивних впливів за допомогою спеціалізованих програмних засобів захисту, функціонування яких вимагає оцінки ПБ. Перелік найбільш важливих для Інтернет-орієнтованих ІС засобів захисту показаний на рис. 1.4.

Перелік основних причин порушення захисту ІС добре співставляються з переліком найбільш актуальних, невирішених завдань оцінки ПБ – розпізнавання віддалених мережевих кібератак на ІС, розпізнавання ШПО і класифікації електронних листів для розпізнавання спаму і витоків інформації.

Рисунок 1.4 Програмні засоби захисту,
в яких оцінюються параметри безпеки

1.3 Актуальність задачі оцінки параметрів безпеки ІС

Розпізнавання мережевих кібератак. Відповідно, під поняттям мережевих кібератак будемо розуміти кібератаку, реалізація якої пов'язана з деструктивним впливом, яке здійснюється за допомогою мережевих каналів зв'язку. Для розпізнавання мережних кібератак використовуються СРА, які представляють комплекс засобів, призначених для моніторингу відбуваються в ІС подій для подальшого аналізу з метою визначення ознак порушення безпеки об'єкта моніторингу. Для прийняття рішень в СРА використовуються два основні методи: визначення аномалій і визначення зловживань. Робота аналізатора при визначенні аномалії базується на припущенні, що ознакою атаки є відхилення поточних величин ПБ від ШНП. Для визначення ШНП застосовуються статистичні моделі. У деяких СРА формується комплексний показник аномалій. При формуванні даного показника для визначення взаємозв'язків між показниками використовуються варіаційні матриці. Також використовується підхід до визначення аномалій з використанням методу

прогнозу подій, який дозволяє виявити кібератаку на ранніх етапах її здійснення. Суть методу полягає в прогнозуванні кібератаки на основі аналізу попередніх подій, пов'язаних з об'єктом захисту. До недоліків відносять високий рівень помилкових спрацьовувань, в основному за рахунок недосконалості моделей ШНП, які не дозволяють досить точно визначити прогнозовані величини ПБ. СРА, що використовують метод визначення зловживання, аналізують послідовність подій, пов’язаних з діяльністю об'єкта захисту і порівнюють їх зі зразками відомих атак. Такі зразки називають ША, а сам метод – визначення атак на основі сигнатур. За якої причини неповноти інформації та наявності шумів при реєстрації ПБ труднощі викликає завдання розрахунку відповідності подій, що стосуються об'єкта захисту. Для вирішення цієї задачі застосовуються різні методи – експертний, аналізу переходів, моделювання атак.

При застосуванні експертного методу відомі кібератаки описуються у вигляді деякого набору правил, виконання яких сигналізує про їх реалізації. Метод аналізу переходів передбачає очіпку мережевий кібератаки в вигляді послідовності переходів об’єктів з одного стану в інший. При застосуванні методу моделювання кібератак попередньо сформовані послідовності подій, характерні для реалізації кібератаки, порівнюються як з поточними показниками. В результаті порівняння формується висновок про ймовірність здійснення кібератаки. Часто використовуються статистичні моделі зміни ПБ ІС при кібератаці. В цілому, метод визначення зловживань дозволяє досить ефективно виявляти кібератаки відомих типів при низькому показнику помилкових спрацьовувань, але не дозволяє виявити кібератаку, зразок якої невідомий. Важливим і на сьогодні невирішеним завданням є формування ША. Загалом ШНП і ША називають ШП. Хоча розробці ШП присвячено досить багато робіт, але практичний досвід і результати вказують на те, що ці шаблони недостатньо адаптовані до типової динаміки ПБ Інтернет-орієнтованих ІС, яка в більшості випадків не може бути про адекватно описана

за допомогою однорідних моделей. Так, на рис. 1.5, 1.6 показано наведені в графіки зміни кількості TCP / IP пакетів, отриманих веб-сервером.

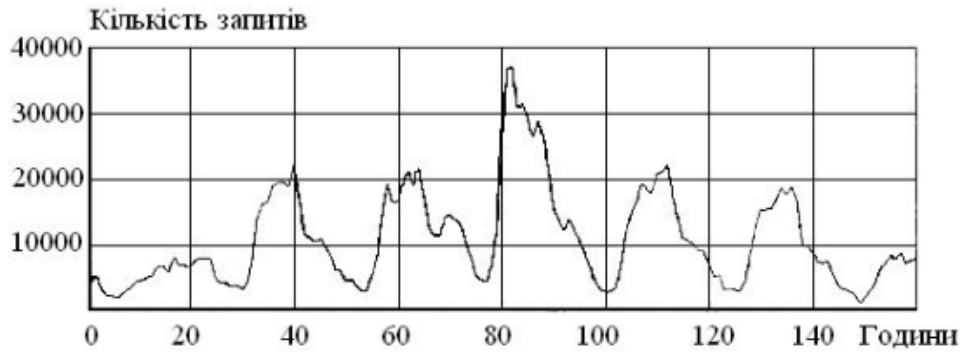

Рисунок 1.5 Зміна кількості TCP / IP пакетів при вікні спостережень в n-годин

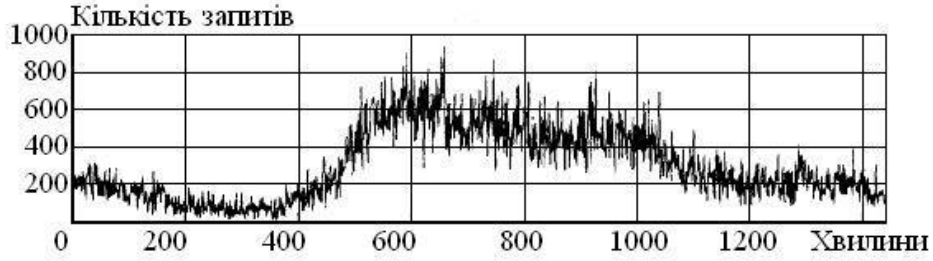

Рисунок 1.6 Зміна кількості TCP / IP пакетів при вікні спостережень в n-хвилин

Аналіз графіків рис. 1.5, 1.6 показує, що при нормальних умовах експлуатації екстремальні величини кількості запитів, що надходять до веб-сервера, значно відрізняються від середніх значень. У загальному випадку максимальні значення в 5-10 разів перевищують середні. Крім того, простежується певна циклічність процесу зміни кількості запитів. Ще однією особливістю процесу є те, що циклічність процесу зміни кількості запитів відбувається в декількох масштабах часу. Також, проаналізувавши рис. 1.6, можна зробити висновок про наявність флуктації трафіку при невеликих вікнах спостережень (1-60 с.), в межах яких кількість переглядів сторінок і кількість відвідувачів сайту не змінюється. Цей факт обумовлений тим, що

типова веб-сторінка значно більше максимального розміру мережевого пакету. Тому одиночний запит до веб-сторінки призводить до стрімкого зростання кількості мережевих пакетів. В цій роботі наведені зміна обсягу вхідного і вихідного мережевого трафіку комп'ютера-сервера корпоративної ІС, який забезпечував не тільки функціонування веб-сервера, але і сервера баз даних, файлового сервера і сервера друку. Даний підхід доцільний при застосуванні в експериментальних цілях, але не завжди прийнятний на практиці внаслідок організаційних обмежень і використання обчислювальних ресурсів комп'ютера-сервера. Крім того, в статистиці відсутня інформація про багатьох параметрах, які широко використовуються в ШП, наприклад, кількість звернень до веб-сервера з однієї IP-адреси (хоста).

Розпізнавання шкідливих програм. Шкідливим будемо називати будь-яке ПЗ, яке може завдати шкоди ІС. За останні кілька років саме ШПО стало однією з основних причин порушень захищеності ІС. При цьому для більшості Інтернет-орієнтованих ІС характерна організація електронного документообігу при адміністративному обмеженні повноважень користувачів на установку програмного забезпечення і доступу до файлів. В цьому випадку ймовірними шляхами зараження є використання електронної пошти, офісних документів і перегляд веб-сайтів. Для зазначених ресурсів ШПО, як правило, розробляється за допомогою скриптових мов програмування. Таким чином, ШПО, створене за допомогою скриптових мов програмування, є однією з основних загроз інформаційної безпеки ІС. Відзначимо, що до скриптових ШПО також відносяться шкідливі макроси, які використовують можливості макромов, вбудованих в системи обробки даних. Найбільш поширені макровіруси і макротрояни, написані на мові VBA і пристосовані для функціонування в середовищах MS Office, AutoCAD, 1С "Підприємство" і 1С "Бухгалтерія". Крім того, в сучасних версіях ОС Windows вбудований скриптова інтерпретатор Windows Scripting Host, який дозволяє виконувати скрипти (макроси), написані на мовах VBScript і JScript. Запуск макросу може

бути здійснений користувачем при відкритті файлу. Ця особливість використовується для активізації скриптових вірусів і троянів, які поширюються в вигляді файлів, прикріплених до листів електронної пошти. Результати вказують, що більшість поштових вірусів і троянів функціонують в середовищі інтерпретатора WScript і написані на мові програмування VBScript. Тому більшість поштових вірусів і троянів не відрізняються від макровірусів MS Office. ШПО, призначене для нанесення шкоди при перегляді веб-сайтів, має певні відмінності. Воно вбудовано в веб-сторінку і виконується в середовищі браузера. Для створення такого ШПО використовуються мови програмування Java, C ++, VBA, JavaScript, JScript, VBScript і ActiveScript.

В основному для захисту від скриптового ПО використовуються антивірусні сканери і поведінкові аналізатори. Найчастіше для виявлення ВПО використовується метод пошуку сигнатур. Особливістю пошуку сигнатур скриптового ШПО є те, що сканер може аналізувати програмний код скрипта в текстовому вигляді. У порівнянні зі стандартними файловими вірусами, дана особливість значно спрощує роботу сканера і дозволяє проводити аналіз функціональності макросу. Однак найбільш поширений метод пошуку сигнатур дозволяє розпізнавати тільки відоме ШПО і відкриває шлях для обходу антивірусного захисту поліморфний і зашифрованого ШПО. Іншими важливими недоліками методу сигнатур є відносно низька швидкість пошуку всіх видів ШПО і необхідність постійного оновлення бази сигнатур. Крім того, в більшості антивірусних сканерів задекларовано використання евристичних методів пошуку ШПО, реалізація яких практично не документується. Однак аналіз вказує на те, що в більшості випадків базою цих методів є статистичний аналіз послідовності виконання програмного коду об'єкта, що перевіряється. Що стосується поведінкових аналізаторів, то вони досить вузько застосовуються на практиці, так як більшість дій, характерних для ШПО, можуть виконуватися і звичайними програмами. Ще одним засобом захисту від скриптів ШПО є модулі блокування скриптів (макросів), що входять до

складу СЗІ офісних пакетів і браузерів. Однак їх широкому застосуванню заважає складність їх оперативного налаштування і значне обмеження функціональних можливостей використання офісних документів і веб-сторінок. Наприклад, блокування браузером спливаючих вікон сильно спотворює інформацію веб-сторінки, а дозвіл їх перегляду є прогалиною в захисті. Отже, завдання розпізнавання скриптового ШПО далека від свого рішення, що підтверджується незалежним тестуванням антивірусних засобів.

1.4 Постановка задачі оцінки параметрів безпеки інтернет-орієнтованих ІС

Метою даної дипломної роботи є рішення актуальної проблеми, створення комплексної методології розробки нейромережевих методів оцінки безпеки інтернет-орієнтованих ІС. Для досягнення поставленої мети необхідно провести аналіз типових методів оцінки безпеки ІС, базових методів побудови нейронних мереж а також визначити вимоги до безпеки інформації в голобальній мережі Інтернет. Крім того необхідно дослідити типи атак на ІС та проаналізувати ефективні способи захисту від них. В даній роботі необхідно спланувати структуру та компоненти нейромережевих методів оцінки безпеки інтренет-орієнтованих систем. Для ефективного функціонування даної системи в дипломній роботі необхідно:

- Провести аналіз предметної області.
- Проаналізувати параметри безпеки інтернет-орієнтованих ІС.
- Оцінити основні фактори ПБ інтернет-орієнтованих ІС.
- Розібрати основні причини порушення захисту ІС.
- Забезпечити зрозумілість і зручність роботи для розробника.
- Провести швидке розпізнавання шкідливого ПЗ.

2. ПОБУДОВА НЕЙРОМРЕЖЕВИХ МЕТОДІВ ОЦІНКИ ПАРАМЕТРІВ БЕЗПЕКИ ІНТЕРНЕТ-ОРІЄНТОВАНИХ ІС

2.1 Метод застосування продукційних правил для представлення експертних знань

За відправну точку розробки є метод застосування продукційних правил для представлення експертних знань орієнтований на розроблену MPNN, що відрізняється від PNN наявністю фільтруючого слою (СФ), то узагальнений метод дещо модифікується (рис. 2.1).

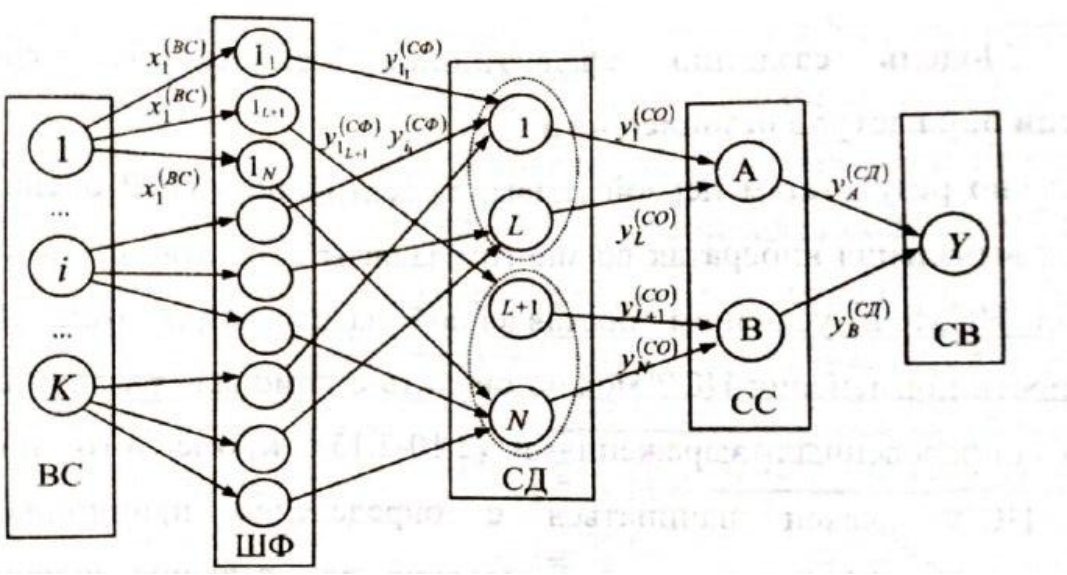

Рисунок 2.1 Структура моделі MPNN

Для подання в MPNN нового продукційного прикладу правила необхідно:

- Додати до слою образів (СО) новий нейрон, який буде відповідати новому навчальному прикладу продукційного правила.

- Залежно від класифікації навчального прикладу встановити для нового нейрона вихідний зв'язок з відповідним нейроном слою додавання (СД).

- Додати в СФ нейрони, які будуть у відповідності з виразом перетворювати сигнали, що передаються від вхідних нейронів до нового нейрона СО.

- Встановити зв'язки між новими нейронами СО і СФ.

- Встановити зв'язки між новими нейронами СФ і відповідними вхідними нейронами.

- Встановити для нових нейронів СФ вагові коефіцієнти вхідних зв'язків рівними величинам параметрів нового навчального прикладу.

Для підвищення універсальності пропонованих рішень передбачено використання методу представлення продукційних правил не тільки в складі комплексної методології розробки нейромережевої системи (НМС), а й самостійно. Тому процес створення методу базувався на розробленій моделі створення ефективних нейромережевих засобів (НМЗ) оцінки ПБ. Крім того, для визначення безлічі ПБ і кібератак, на основі яких формуються вхідні параметри нейромережевих моделей (НММ) і продукційні правила, використовують розроблену модель процесу інтеграції ПБ ІС. Це дозволило використовувати в якості вхідних даних методу безліч характеристик об'єкта захисту ІС. Процес формування продукційних правил розпізнавання кібератак реалізується за допомогою розробленого підходу до визначення статистично подібних кібератак. У підсумку метод застосування продукційних правил для представлення експертних знань в MPNN, яка призначена для розпізнавання кібератак на ІС, складається з наступних етапів:

1. Формування множини можливих кібератак. Етап передбачає аналіз безлічі характеристик об'єкта захисту ІС, в результаті якого визначається множина кібератак, яке повинна розпізнавати НМ.

$$Ka = \{Ka_1, Ka_2, \dots, Ka_j\}, \tag{2.1}$$

де j – кількість атак, Ka – j-та кібератака.

2. Визначення ПБ для розпізнавання довільної кібератаки. На цьому етапі, використовуючи розроблену модель інтеграції ПБ, визначається множина ПБ, які будуть використані в якості вхідних параметрів НМЗ оцінювання:

$$Ka_j \to \{Xj\}_{Nj}, \tag{2.2}$$

де *Nj* – кількість ПБ для розпізнавання *j*-ої кібератаки.

3. Визначення подібних кібератак. Етап орієнтований на виділення з статистично подібних між собою кібератак:

$$\left\{Ka_1^{(p)}, \dots, Ka_j^{(p)}\right\}, \forall Ka_1^{(p)} \subset Ka, \dots, Ka_j^{(p)} \subset Ka, Ka_1^{(p)} \cup Ka_2^{(p)} \dots \cup Ka_j^{(p)} = Ka, \quad (2.3)$$

де $Ka_1^{(p)}$ – *i*-а множина подібних кібератак.

Згідно розробленого підходу, схожість похідної *k*-ої та *j*-ої кібератак визначається кортежем:

$$\langle T_{(k,j)}\left(Ka_k, Ka_j\right), R_{(k,j)}(\{X_k\}_{N_k}, \{X_j\}_{N_j})\rangle, \quad (2.4)$$

де $T_{(k,j)}\left(Ka_k, Ka_j\right)$ – функція подібності типу *k*-ої та *j*-ої кібератак, $R_{(k,j)}(\{X_k\}_{N_k}, \{X_j\}_{N_j})$ – функція подіності множин ПБ, які використовуються для розпізнавання *k*-ої і *j*-ої кібератак.

Розрахунок подібності *k*-ої і *j*-ої кібератак виконується за допомогою п'яти кроків.

3.1 Визначення типу кібератак. На цьому етапі визначається тип *k*-ої і *j*-ої кібератак:

$$Ka_k \to Ks_k \vee Kq_k, Ka_j \to Ks_j \vee Kq_j, \quad (2.5)$$

3.2 Розрахунок функції подібності типу кібератак. Для розрахунку порівнюються типи *k*-ої і *j*-ої кібератак. Використовується функціонал:

$$\left(Ks_k \wedge Ks_j\right) \vee \left(Kq_k \wedge Kq_j\right) \to T_{(k,j)} = 0 \neg T_{(k,j)} \neq 0 \quad (2.6)$$

3.3 Визначення множини спільних ПБ. Даний крок спрямований на визначення, безлічі ПБ, які використовуються для розпізнавання *k*-ої і *j*-ої кібератак:

$$\left\{X_{(k,j)}\right\}_{N_{(k,j)}} = \{X_k\}_{N_k} \cap \left\{X_j\right\}_{N_j}, \quad (2.7)$$

де $N_{(k,j)}$ – кількість загальних ПБ.

3.4 Розрахунок коефіцієнта подібності множин ПБ. Для розрахунку коефіцієнта подібності використовується вираз:

$$R_{(k,j)} = N_{(k,j)}/N_{(k,j)}^{max}\text{, де } N_{(k,j)}^{max} = N_k \exists N_k > N_j \neg N_{(k,j)}^{max} = N_j. \quad (2.8)$$

3.5 Визначення подібності кібератак. Приймається остаточне рішення про подібність *k*-ої і *j*-ої кібератак. Кібератаки вважаються подібними, якщо справедливий вираз:

$$T_{(k,j)} = 0 \wedge R_{(k,j)} \leq R_{max}, \quad (2.9)$$

4. Визначення ПБ для розпізнавання подібних кібератак. Етап орієнтований на визначення множини ПБ, використовуваних як вхідні параметри НМ для розпізнавання подібних кібератак:

$$\left\{X_1^{(p)}, \dots, X_j^{(p)}\right\} \rightarrow Ka_j^{(p)}, \quad (2.10)$$

де $X_j^{(p)}$ – множина ПБ, відповідних *j*-ій множині подібних кібератак, $Ka_j^{(p)} = \left\{Ka_{1,j}, \dots, Ka_{M_j,i}\right\}$, M_j – кількість елементів $Ka_j^{(p)}$.

Для визначення $X_j^{(p)}$ використовується вираз:

$$X_j^{(p)} = X_{1,j} \cup \dots \cup X_{M,j}, \quad (2.11)$$

де $X_{M,j}$ – множина ПБ для розпізнавання.

5. Отримання експертних даних. Даний етап спрямований на формування множин подібних кібератак $\overline{Ka}^{(p)}$, для яких можна розробити продукційні правила розпізнавання. Якщо для деякого *j*-ї множини $Ka_j^{(p)} \in Ka$ отримати представницькі експертні дані для розробки продукційних правил на основі аналізу $X_j^{(p)}$ досить складно, то

$$Ka_j^{(p)} \not\subset \overline{Ka}^{(p)}. \quad (2.12)$$

В іншому випадку

$$Ka_j^{(p)} \subset \overline{Ka}^{(p)}. \quad (2.13)$$

6. Розробка множини нейромережевих моделей. Даний етап спрямований на формування множини НМ типу MPNN, кожна з яких призначена для розпізнавання окремих множин подібних кібератак:

$$Net = \{net_1, net_2, \dots net_M\}, \quad (2.14)$$

де net_j – j-та НМ, призначена для розпізнавання j-ої множини $Ka_j^{(p)}$.

7. Розробка структури вхідного слою. В результаті виконання даного етапу для кожної $net_j \in Net$ визначається кількість нейронів у вхідного слою (ВС) MPNN. Використовується вираз:

$$N_{x,j} = N_j^{max} \tag{2.15}$$

Також встановлюється відповідність між i-им входом НМ і i-им ПБ з множини $X_j^{(p)}$.

8. Розробка продукційних правил. На цьому етапі для кожної множини $Ka_j^{(p)} \in Ka$ на основі експертних даних розробляється множина продукційних правил:

$$Pr_j = \left\{pr_{1,j}, \dots pr_{L_j j}\right\} \tag{2.16}$$

де $pr_{i,j}$ – i-е продукційне правило для розпізнавання $Ka_{i,j} \in Ka_j^{(p)}$, L_j – кількість продукційних правил для розпізнавання $Ka_j^{(p)}$.

Продукційні правила задаються виразами виду:

$$x_1 \in \left[x_1^{min}, x_1^{max}\right] \wedge x_2 \in \left[x_2^{min}, x_2^{max}\right] \dots \wedge X_{N^{max}} \in \left[X_{N^{max}}^{min}, X_{N^{max}}^{max}\right] \longrightarrow Ka_{i,j}, \tag{2.17}$$

де x_1, x_2 ... – інтегровані ПБ, $\left[x_1^{min}, x_1^{max}\right], \left[x_2^{min}, x_2^{max}\right]$, ... – задані діапазони величин інтегрованих ПБ.

9. Розробка СД. На цьому етапі для кожної $net_j \in Net$ СД визначається стільки нейронів, скільки подібних кібератак повинна розпізнавати НМ:

$$N_{\text{ШД},j} = M_j \tag{2.18}$$

Також встановлюється відповідність між кожним n-им нейроном СД і n-ою кібератакою:

$$n_{\text{ШД},j} \rightarrow Ka_{n,j}. \tag{2.19}$$

10. Визначення структури СО і СФ. Для кожного $net_j \in Net$ виконання етапу є пристосуванням структури СО і СФ MPNN до заданих продукційних правил:

$$\langle N_{\text{ШФ}}, N_{\text{ШО}}, L_{\text{ШФ}}, L_{\text{ШО}}, L_{\text{ШД}} \rangle = f\left(Pr_j\right), \quad (2.20)$$

де $N_{\text{ШФ}}$ – множина нейронів СФ, $N_{\text{ШО}}$ –множина нейронів СО, $L_{\text{ШФ}}, L_{\text{ШО}}, L_{\text{ШД}}$ – множина вихідних СФ, СО і СД.

Визначення довільного *n*-го продукційного правила виконується п'ятьма кроками:

10.1 Визначення нейрона СО. На цьому етапі до СО додається *n*-ий нейрон, який буде відповідати *n*-ому продукційному правилу:

$$n_{\text{ШО},j} \rightarrow Pr_{n,j}. \quad (2.21)$$

10.2 Модифікація $L_{\text{ШД}}$. Модифікація полягає у встановленні для *n*-го нейрона СО зв'язку з нейроном СД, що відповідає *n*-ій кібератаці.

10.3 Визначення нейронів СФ. На даному етапі в СФ додається множина нейронів $N_{n,\text{ШФ}} \in N_{\text{ШФ}}$, що, згідно з *n*-ому продукційному правилу, перетворять сигнали від вхідних нейронів до n-го нейрона СО. Перетворення задається виразом

$$\exists x_i^{(\text{ВШ})} \in \left[P^{min}, P^{max}\right]_l \rightarrow y_{jl}^{(\text{ШФ})} = x_i^{(\text{ВШ})}, \quad \exists x_i^{(\text{ВШ})} \notin \left[P^{min}, P^{max}\right]_l \rightarrow y_{jl}^{(\text{ШФ})} = 0 \quad (2.22)$$

де $x_i^{(\text{ВШ})}$ – значення *i*-го ПБ, $y_{jl}^{(\text{ШФ})}$ – вихідний сигнал j_l нейрона СФ.

10.4 Модифікація зв'язків $L_{\text{ШО}}$. Реалізація кроку полягає у встановленні зв'язків між $n_{\text{ШО},j}$ і $N_{n,\text{ШФ}}$.

10.5 Модифікація зв'язків $L_{\text{ШФ}}$.. На цьому етапі встановлюються зв'язки між N_x і $N_{n,\text{ШФ}}$.

Кроки 1-5 виконуються для всіх заданих продукційних правил.

11. Верифікація розроблених MPNN. Верифікація кожної $net_j \in Net$ полягає в порівнянні її похибки розпізнавання і обчислювальної складності з

максимально допустимими значеннями цих параметрів. Для кожної net_j похибка розпізнавання і обчислювальна складність розраховуються на прикладах тестової вибірки. Мережа net_j вважається здатною для практичного використання, якщо для всіх прикладів тестової вибірки справедливий вираз:

$$\varepsilon_j \leq \varepsilon_{max} \wedge \xi_j \leq \xi_{max}. \quad (2.23)$$

де ε_j – похибка розпізнавання net_j, ξ_j – обчислювальна складність, ε_{max} – максимально допустима похибка розпізнавання, ξ_{max} – максимально допустима обчислювальна складність.

Для перевірки ефективності запропонованого методу проведено експериментальні дослідження, в яких MPNN застосовувалася для виявлення мережевих атак. Як джерело статистичних даних для формування навчальної і тестової множини НМ використана база даних KDD-99, яка містить близько 5000000 записів – образів мережевих з'єднань. Кожен запис складається з 42 полів. У полях від 1 до 41 записані такі параметри мережевого з'єднання як тривалість, тип протоколу, мережевий сервіс, кількість отриманих байтів, кількість переданих байтів, статус з'єднання. У 42 поле записана інформація, що характеризує стан захищеності ІС – або відсутність атаки (normal), або її тип. У базі представлені 22 види атаки, які поділяються на 4 основні класи – відмова в обслуговуванні (DoS), несанкціоноване отримання прав доступу незареєстрованим користувачем (R2L), несанкціоноване підвищення привілеїв (U2R) зареєстрованим користувачем і сканування портів (Probe). Кількість записів, які відповідають відсутності кібератак, так само 972 781.

Оскільки передумовою застосування експертних знань в НМ є недостатня повнота навчальних даних, то основна увага була зосереджена на розпізнаванні кібератак U2R, для яких кількість записів в KDD-99 найменша. в області захисту інформації розроблено 4 продукційних правила для розпізнавання кібератак buffer_overflow, що відносяться до U2R.

Основні параметри мережі наступні: кількість вхідних параметрів мережі К = 41, кількість нейронів СД дорівнює 2 (нейрон А відповідає атаці,

нейрон В - нормальному стану), кількість нейронів СО дорівнює 18, а кількість нейронів СФ дорівнює 738, ці дані складають основу математичного забезпечення виразів. Структура розробленої MPNN приведена на рис. 2.1 з урахуванням наведених величин.

Апробація розробленої моделі на даних KDD-99 показала абсолютну точність розпізнавання всіх видів кібератак buffer_overflow. Для порівняння отриманих результатів використана робота, в якій наведено результати розпізнавання цього ж типу кібератак з використанням сигнатур, які представлені в базі KDD-99. Для розпізнавання використані багатошаровий персептрону (БШП) і топографічна карта Кохонена (ТК). Точність розпізнавання атак типу buffer_overflow ТК становить 0,0458. При цьому БШП, через малий обсяг навчальних даних, взагалі не вдалося навчити розпізнавати кібератаки типу buffer_overflow. В роботі для розпізнавання buffer_overflow застосована спеціальна адаптивна модель, точність розпізнавання якої не перевищує 0,5.

Тому можна вважати, що запропонований метод дозволяє підвищити точність розпізнавання кібератак, сигнатури яких недостатньо представлені в базі даних. Також проведене порівняння вказує на те, що застосування запропонованого методу дозволяє підвищити точність розпізнавання кібератак класу U2R, сигнатури яких представлені в базі даних KDD-99, як мінімум в 2 рази.

Незважаючи на можливості представлення експертних знань, широкого застосування модифікованої мережі PNN в області захисту інформації заважає один недолік – низька здатність узагальнювати навчальну інформацію. Відзначимо, що здатність НМ до узагальнення загальноприйнято оцінювати ставленням кількості синаптичних зв'язків до кількості навчальних прикладів, яку вона може безпомилково або з певною похибкою запам'ятати.

Для мережі PNN одному навчальному прикладу відповідає один нейрон СО з кількістю синаптичних зв'язків, яке на одиницю перевищує кількість

вхідних параметрів. У той же час в БШП з одним вихідним нейроном і такою ж кількістю синаптичних зв'язків співвідноситься 10-100 навчальних прикладів. Тому при розпізнаванні кібератак узагальнюючі можливості БШП в 10-100 вище, ніж в MPNN. Разом з тим MPNN і БШП мають досить схожі структурні схеми і відносяться до одного класу НМ з прямим поширенням сигналу. Крім того, аналіз вказує на те, що за допомогою конструктивних алгоритмів можливо створити БШП, базою якого є мережа PNN. Тому перспективною є розробка методу використання експертних знань в БШП, який призначений для розпізнавання мережних кібератак.

Ще одним важливим напрямком удосконалення запропонованого методу повинна бути його адаптація до використання поданих за допомогою апарату нечіткої логіки експертних знань про мережеві кібератаки.

2.2 Метод визначення тимчасових характеристик використання нейромережевих засобів.

Основою розробки методу є підхід до визначення принципової доцільності застосування НМЗ оцінювання ПБ, метод застосування продукційних правил для представлення експертних знань в НМЗ оцінювання ПБ і модель створення ефективних НМЗ оцінювання ПБ. Крім того, передбачається можливість застосування методу визначення доцільності як в складі комплексної методології, так і самостійно. Тому в методі застосована модель процесів інтеграції ПБ, використовуваних НМЗ розпізнавання кібератак. Реалізація методу полягає у виконанні наведених нижче етапів.

Етап 1 – формування безлічі вхідних і вихідних параметрів НМ. Етап передбачає використання розробленої моделі інтеграції ПБ, що дозволяє на основі аналізу характеристик об'єкта захисту $O = \{o_1, \dots o_5\}$ і характеристик кібератаки $\Phi = \{\phi_1, \dots \phi_\phi\}$ визначити безліч ПБ, які будуть використані в якості вхідних параметрів НМ:

$$X = \{x_1, \dots x_{N_x}\}, \tag{2.24}$$

де N_x – кількість вхідних параметрів НММ.

Також визначається множина вихідних параметрів НММ, які будуть свідчити про наявність або відсутність кібератак певного типу:

$$Y = \{y_1, \dots y_{N_y}\}, \tag{2.25}$$

де N_y – кількість вихідних параметрів.

Етап 2 – отримання статистичних даних. В результаті аналізу характеристик об'єкта захисту, умов завдання оцінювання ПБ і множини доступних НМЗ $M = \{m_1, \dots m_K\}$ оцінюється можливість реєстрації ПБ, використовуваних для визначення X і Y. Якщо оцінка негативна, то НМЗ, крім MPNN, використовувати недоцільно. Тобто

$$M = \{m_{MPNN}\} \tag{2.26}$$

Етап 3 – представлення експертних знань. Використовуючи розроблений метод застосування продукційних правил для представлення експертних знань в НМС, оцінюється можливість розробки моделі MPNN. Якщо оцінка негативна, то модель MPNN виключається з подальшого розгляду:

$$m_{MPNN} \notin M. \tag{2.27}$$

В іншому випадку

$$m_{MPNN} \in M. \tag{2.28}$$

Етап 4 – перевірка множини допустимих видів НМ. Етап орієнтований на перевірку того, чи пуста множина допустимих НМЗ. Якщо справедливий вираз (2.27), то НМЗ використовувати недоцільно:

$$M = \emptyset. \tag{2.29}$$

Етап 5 – визначення допустимої помилки навчання НМ. На даному етапі в результаті аналізу характеристик об'єкта захисту визначаються мінімально допустимі величини пропуску кібератаки і помилкового розпізнавання кібератаки. Менша з величин використовується як мінімально допустима помилка навчання НМ. Таким чином, для визначення ε використовується правило:

$$\delta_1 \leq \delta_2 \rightarrow \varepsilon = \delta_1 \quad \varepsilon = \delta_2. \tag{2.30}$$

де δ_1 – мінімально допустима величина пропуску кібератаки, δ_2 – мінімально допустима величина хибного розпізнавання кібератаки, ε – мінімально допустима помилка навчання НММ.

В першому наближенні $\varepsilon = 0{,}05$.

Етап 6 – визначення часових обмежень процесу розробки НМ. На даному етапі визначається допустима тривалість розробки (T_f) і допустимий термін навчання НМ (t_d). (T_f) визначається на основі експертної оцінки. Для визначення використовується залежність

$$P(t_d) \geq P_n, \tag{2.31}$$

де $P(t_d)$ – ймовірність безвідмовної роботи апаратно-програмних засобів, що забезпечують навчання НМ протягом t_d, P_n – допустима ймовірність безвідмовної роботи НМЗ.

У першому наближенні $P_n = 10^{-5}$ відповідно до (2.29), $t_d \approx 10^5 c$. Тобто допустимий термін навчання НМЗ приблизно дорівнює одній епосі.

Етап 7 – визначення мінімального обсягу навчальної вибірки. Даний етап спрямований на визначення мінімально допустимої кількості навчальних прикладів для НМ:

$$P_{min} = 20N_x, \tag{2.32}$$

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

Етап 8 – розрахунок терміну навчання. На цьому етапі розраховується термін навчання НММ на мінімально допустимій кількості навчальних прикладів. Для топографічної карти Кохонена (ТК), нейромережі з радіальними базисними функціями (РБФ), PNN і MPNN:

$$t_{min} \approx 0{,}1\tau e^{-\varepsilon} P_{min}\left(N_x + N_y\right), \tag{2.33}$$

де τ – тривалість однієї обчислювальної операції процесу навчання.

Для БШП:

$$t_{min} \approx 0{,}001\tau e^{-\varepsilon} P_{min}^{2} \left(N_x + N_y\right)^2, \quad (2.34)$$

Етап 9 – перевірка терміну навчання. Етап передбачає для всіх НМЗ, що входять в *M*, порівняння допустимого терміну навчання з терміном навчання на мінімально допустимому кількості навчальних прикладів. Входження *j*-го НМЗ в множину ефективних НМЗ з допустимим терміном навчання визначається за допомогою наступного правила:

$$t_{min}\left(m_j\right) \geq t_d \rightarrow m_j \notin M^{(m)}, \quad (2.35)$$

де $M^{(m)}$ – множина ефективних НМЗ із допустимим терміном навчання, m_j - *j*-ий НМЗ.

В іншому випадку $m_j \in M^{(m)}$. Якщо, $M^{(m)} = \emptyset$, то НМЗ взагалі використовувати недоцільно.

Етап 10 – розрахунок максимально допустимої тривалості формування навчальної вибірки. На даному етапі для кожної $m_j^{(m)} \in M^{(m)}$ розраховується максимально допустима тривалість формування навчальної вибірки ($T_{j,max}$). Відзначимо, що оскільки в MPNN в якості навчальних прикладів використовуються експертні дані, то для НМЗ на базі цієї НММ тривалість формування навчальної вибірки дорівнює тривалості розробки продукційних правил. Для розрахунку $T_{j,max}$ використовується вираз

$$T_{j,max} = T_f - t_j, \quad (2.36)$$

де t_j – термін навчання *j*-ої НММ $m_j^{(m)} \in M^{(m)}$.

Результатом виконання етапу є сформована множина:

$$\left\{T_{1,max}, \dots T_{L,max}\right\}, \quad (2.37)$$

де *L* – кількість елементів $M^{(m)}$.

Етап 11 – визначення терміну формування навчальної вибірки. Етап орієнтований на аналіз характеристик об'єкта захисту і умов задачі оцінювання для визначення терміну формування навчальної вибірки з мінімально допустимою кількістю навчальних прикладів:

$$T_d = f(O, Y), \tag{2.38}$$

де T_d – термін формування навчальної вибірки.

Етап 12 – перевірка терміну формування навчальної вибірки. На даному етапі для кожного $m_j^{(m)} \in M^{(m)}$ проводиться порівняння $T_{j,max}$ і T_d. Множина НМЗ, які доцільно використовувати для оцінки ПБ, формується за допомогою виразів (2.39,2.40):

$$T_{j,max} > T_d \rightarrow m_j^{(m)} \notin Mz, \tag{2.39}$$

$$T_{j,max} < T_d \rightarrow m_j^{(m)} \in Mz, \tag{2.40}$$

де Mz – множина НМЗ, які доцільно використовувати для оцінки ПБ.

В результаті реалізації методу формується безліч НМЗ, які доцільно використовувати для оцінки ПБ з метою розпізнавання кібератак.

Відзначимо, що використання запропонованого методу багато в чому ускладнюється необхідністю залучення висококваліфікованих експертів, знання яких необхідні для оцінки можливості формування в прийнятний термін мінімально допустимої навчальної вибірки (9 і 11 етапи). Разом з тим, достатньо відомих БД, в яких представлені образи кібератак і які можуть бути використані в якості навчальних прикладів нейромережевих засобів розпізнавання. Очевидно, якщо кількість таких образів більше, ніж мінімально допустима кількість навчальних прикладів, то 9 і 10 етапи виконувати не потрібно, а оцінка 11 пункту позитивна.

Тому в спрощеному варіанті методу замість етапів 10-12 слід оцінити можливість формування мінімальної навчальної вибірки на основі доступних баз даних образів кібератак.

Розглянемо використання методу на конкретному прикладі розпізнавання кібератак типу IP-спуфінг.

Етап 1. Для виявлення атак даного типу необхідна статистика, що стосується наступних функціональних параметрів: кількість одночасних підключень, швидкість обробки запитів, затримка між запитами, кількість

пакетів з однаковими адресами відправника і одержувача, вік віртуального каналу і кількість віртуальних каналів . Номенклатура вхідних параметрів НМ буде відповідати зазначеним функціональним параметрам. Кількість вхідних параметрів $N_x = 5$. Для виявлення кібератаки даного типу можливо обмежитися одним вихідним параметром, величина якого буде вказувати на впевненість системі виявлення атак (СВА) в наявності чи відсутності атаки типу IP-спуфінг. Тобто $N_Y = 1$.

Етап 2. Реєстрацію наведених ПБ можливо здійснити мережевими екранами і СВА. При цьому в якості доступної бази даних можливо використовувати KDD-99.

Етап 3. У першому наближенні мережу MPNN виключена з розгляду. Через це $m_{MPNN} \notin M$.

Етап 4. Оскільки результат другого етапу позитивний, то $M \neq \emptyset$.

Етап 5. Ґрунтуючись на отриманих результатах, визначено, що допустима помилка навчання НМ $\varepsilon = 0{,}05$.

Етап 6. На основі експертної оцінки визначено, що термін, протягом якого ризик від реалізації кібератаки не перевищує встановлену межу, становить $T_a = 30$ діб. Таким чином, максимально допустима тривалість розробки НМ становить 30 діб. Відповідно, допустимий термін навчання НМ становить $t_d \approx 10^5\ c$ (24 години).

Етап 7. Підставивши $N_x = 5$ у вираз (2.32), отримаємо:

$$P_{min} \geq (10 \ldots 20) \times N_x = 20 \times 5 = 100. \qquad (2.41)$$

Таким чином, мінімальна кількість навчальних прикладів рівна $P_{min} = 100$.

Етап 8. Для розрахунку терміну навчання НММ виду ТК, РБФ, PNN на мінімально допустимій навчальної вибірці у вираз (2.33) підставлено $P_{min} = 100, N_X = 5, N_Y = 1, \chi = 1, \tau = 10^{-2}$. Отримано:

$$t_{min} \approx 0{,}1\tau e^{-\varepsilon} P_{min}(N_X + N_Y) = 0{,}1 \times 10^{-2} \times e^{-1\times 0{,}05} \times 100 \times (5+1) = 5{,}71. \qquad (2.42)$$

Таким чином, термін навчання ТК, РБФ, PNN на мінімально допустимій навчальної вибірці становить 5,71 с.

Для розрахунку терміну навчання БШП ці ж дані підставлено до виразу (2.33). Отримано:

$$t_{min} \approx \mu_2 \tau e^{-\chi\varepsilon} P^2 (N_X + N_Y)^2 = 0{,}001 \times 10^{-2} \times e^{-1\times 0{,}05} \times 100^2 \times (5+1)^2 = 34{,}24. \quad (2.43)$$

Тому термін навчання БШП на мінімально допустимій навчальної вибірці становить 34,24 с.

Етап 9. Підстановка термінів навчання БШП, ТК, РБФ, PNN в вираз (2.35) вказує на входження зазначених НММ у множині $M^{(m)}$. Відповідно, допустимий термін навчання НММ становить $t_d \approx 10^5\ c$ (24 години).

Етап 10. У якості доступної бази даних зареєстрованих ПБ можливо використовувати KDD-99. Відповідно, $Mz = M^{(m)}$. Таким чином, в першому наближенні для розпізнавання кібератак типу IP-спуфінг можливо використовувати НМС на базі НММ виду БШП, ТК, РБФ і PNN.

При використанні спрощеного варіанту запропонованого методу проведено визначення доцільності застосування НМС для виявлення типової кібератаки на ІС. У сучасних умовах в якості доступних джерел статистичних даних ПБ, призначених для формування навчальної вибірки НМ, доцільно використовувати параметри, які реєструються операційними системами, мережевими серверами і такими СЗІ, як міжмережеві екрани, антивіруси, системи захисту від спаму і DLP-системи.

Для кожної ІС ведуться відповідні бази даних, куди записуються зареєстровані величини зазначених ПБ. Крім того, бази даних СЗІ містять величини ПБ, які сигналізують про відсутність або наявність атаки на ІС. Тому, використовуючи наведену в класифікацію, в першому наближені визначено, що номенклатура і обсяг зареєстрованих статистичних параметрів дозволяють сформувати навчальну вибірку НМ, яка призначена для виявлення таких видів кібератак:

- Мережеві кібератаки, що реалізуються на транспортному і прикладному рівнях стека протоколів TCP/IP.

- ШПЗ - комп'ютерних вірусів і троянів.

- Спама.

- Витоків текстової інформації за допомогою листів електронної пошти.

Очевидно, що певний перелік кібератак вимагає подальшої деталізації, реалізувати яку в повному обсязі заважає велика кількість відомих підтипів атак, постійна поява, нових підтипів атак і необхідність використання експертних даних при визначенні максимально допустимої тривалості розробки НМС. Тому реалізована тільки часткова деталізація. Застосувавши спрощений варіант методу, розглянуто доцільність використання НММ для виявлення кібератак наступних типів: СП, Dos-атак, веб-орієнтованих скриптових вірусів і троянів (ВСВ) і несанкціонованого отримання прав доступу незареєстрованим користувачем (R2L). Розглядалися такі підтипи R2L, як phf і multihop. В якості вхідних параметрів НМ використані:

- СП, Dos-атаки типу neptune і типу smurf – кількість одночасних підключень, швидкість обробки запитів, кількість пакетів з однаковими адресами відправника і адресата, кількість віртуальних каналів;

- ВСВ – назва потенційно небезпечних операторів мови програмування JavaScript;

- R2L – параметри мережевих з'єднань (тривалість, тип протоколу, мережевий сервіс, кількість отриманих байтів, кількість переданих байтів, статус з'єднання).

Результати розрахунків наведені в табл. 2.1. і на рис. 2.2.

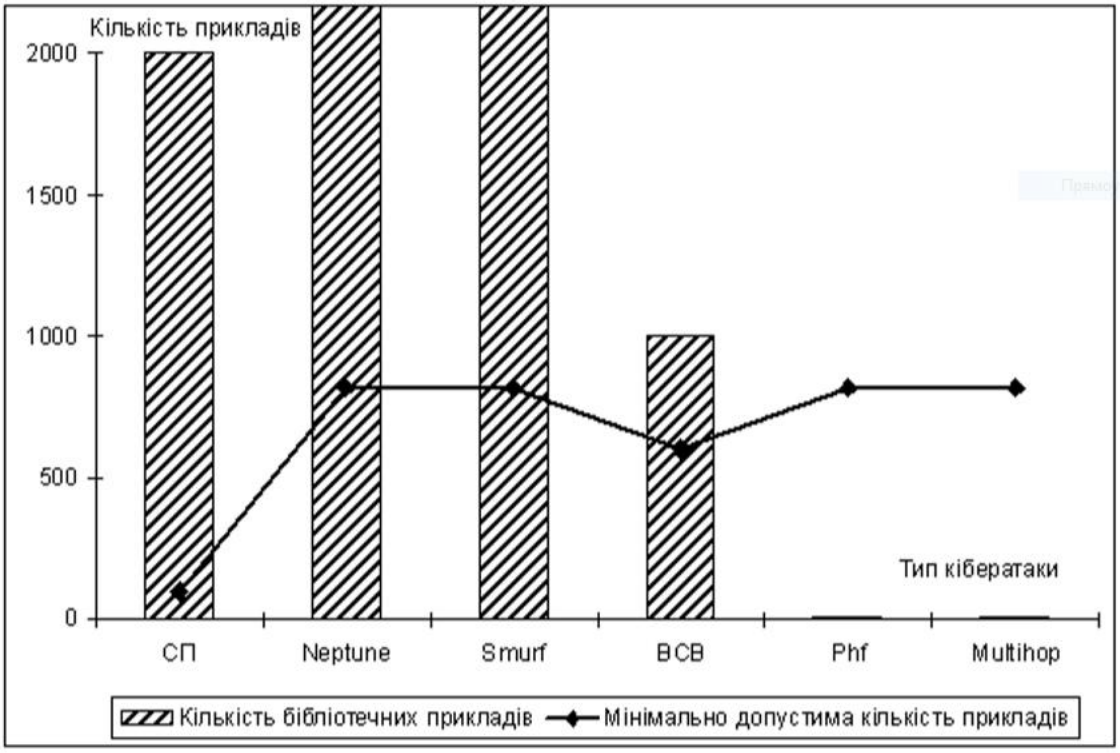

Рисунок 2.2 Оцінка можливості застосування нейромережевих методів для виявлення кібератак

Аналіз даних табл. 2.1 дозволяє позитивно оцінити можливість навчання НММ при мінімально допустимій кількості навчальних прикладів, допустимого терміну навчання і можливості формування мінімальної навчальної вибірки на основі існуючих баз даних. Тому, згідно з спрощеним варіантом запропонованого методу, НМС на основі БШП, ТК, РБФ і PNN доцільно використовувати для розпізнавання кібератак типу СП, Neptune, Smurf і BCB, а недоцільно – для розпізнавання атак типу phf і multihop.

Таблиця 2.1 Проміжні результати оцінок

Етап оцінки	Вид кібератаки					
	СП	Dos-атак		BCB	R2L	
		Neptune	Smurf		Phf	Multihop
Кількість вхідних параметрів	5	41		30	41	

Допустима похибка при навчанні	0,05					
Тип НМ	БШП					
Мінімальна кількість навчальних прикладів	100	820		600	820	
Допустимий період навчання, с	$\approx 10^5$					
Тривалість ітерації, с	$\approx 10^{-2}$					
Термін навчання, с	3,5	112,8		32,9	112,8	
Оцінка можливості навчання за допустимий термін	Позитивна					
Приблизна кількість прикладів кібератак в БД	2000	10^6	3×10^6	10^3	4	7
Оцінка можливості формування навчальної вибірки на основі БД	Позитивна				Негативна	

3. НЕЙРОМЕРЕЖЕВА СИСТЕМА ОЦІНКИ ПАРАМЕТРІВ БЕЗПЕКИ ІНТЕРНЕН-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

3.1 Система розпізнавання мережевих кібератак

Проектування системи розпізнавання мережевих кібератак проведено за допомогою комплексної методології оцінки ПБ ІС із застосуванням структурних рішень системи оцінювання ПБ для розпізнавання кібератак на ресурси Інтернет-орієнтованих ІС. Відповідно до результатів п. 1.3 та доступними статистичними даними, розглянуті кібератаки типу шторм запитів (Ka_z), спрямовані викликати відмову в обслуговуванні веб-сервера і кібератаки типу U2R, спрямовані на несанкціоноване підвищення привілеїв користувачів. У свою чергу, згідно з механізмом реалізації, з кібератак типу U2R виділено наступні підтипи кібератак: buffer_overflow (Ka_b) loadmodule (Ka_l), perl (Ka_p), rootkit (Ka_r).

Таким чином, безліч кібератак визначається виразом:

$$Ka = \{Ka_z, Ka_b, Ka_l, Ka_p, Ka_r\}. \quad (3.1)$$

Формування множини ПБ. Згідно з комплексною методології, на першому етапі проектування системи проведено формування множини ПБ, оцінка яких дозволить розпізнати очікувану множину кібератак. Оскільки Xs_z залежить від терміну експлуатації веб-сервера, то Ka_s відноситься до ПК, що дозволяє створити марківську модель ШНП. Для розпізнавання $\{Ka_b, Ka_l, Ka_p, Ka_r\}$ в якості ПБ використано безліч параметрів мережевого з'єднання (Xq_{U2R}), представлене в базі даних KDD-99.

Відзначимо, що механізм реалізації $\{Ka_b, Ka_l, Ka_p, Ka_r\}$ і характер Xq_{U2R} не залежить від терміну функціонування ІС. Тому ці кібератаки відносяться до НК, що не передбачає створення для їх розпізнавання марківської моделі ШП.

Визначення вхідних і вихідних параметрів НММ. Оскільки при розпізнаванні Ka_s можна використовувати ШНП, то в якості першого вхідного

параметра НММ застосовується наведена різниця між реальною кількістю звернень до веб-сервера (Rr) і кількість звернень, розрахованих відповідно до ШНП (Rm):

$$n_1 = (R_r - R_m)/R_m. \quad (3.2)$$

Другий вхідний параметр призначений для синхронізації ШНП з реальною кількістю звернень і розраховується як наведений час звернення до веб-сервера:

$$n_2 = t - Round\left(\frac{t}{24}\right), \quad (3.3)$$

де *t* – момент звернення.

При розпізнаванні мережевих кібератак типу U2R, як і в разі розпізнавання ШПО, для встановлення співвідношення між ПБ і вхідним параметром НММ проведена їх нумерація для кожного з очікуваних видів кібератак. Номер ПБ дорівнює номеру відповідного вхідного параметра НММ. Таким чином, в НММ, призначених для розпізнавання Ka_s, кількість вхідних параметрів дорівнює 2, а в НММ, призначених для розпізнавання $\{Ka_b, Ka_l, Ka_p, Ka_r\}$ кількість вхідних параметрів дорівнює 41. Відзначимо, що при розпізнаванні Ka_s тип вхідних даних числовий. При розпізнаванні U2R параметри №1 і №5-41 також мають числовий тип, а параметр №2-№4 – символьний. Також за аналогією з системою розпізнавання ШПО і класифікації електронної пошти, до складу ВШ НММ входить тільки один нейрон. При цьому вихід НММ (Y) при класифікації кібератак дорівнює 1, а при класифікації безпечного стану дорівнює -1. В інших випадках класифікацію слід проводити відповідно до вираження.

Визначення оптимального виду НММ. Особливістю статистики, що стосується прикладів функціонування веб-сервера, є відсутність в ній даних, які відповідають моментам реалізації мережевих кібератак типу Ka_s. Тобто статистичні дані для формування навчальної вибірки НММ відсутні, хоча і є достатніми для розробки ШП.

Також відзначимо, що при розпізнаванні кібератак, що входять до складу $\{Ka_b, Ka_l, Ka_p, Ka_r\}$, необхідну кількість навчальних прикладів визначається виразом:

$$P \geq 20 * N_{\text{вх}} = 20 * 41 = 82 \quad (3.4)$$

При цьому кількість записів бази даних KDD-99, які відповідають очікуваним кібератак, наступне: buffer_overflow - 33, loadmodule - 9, perl - 3, rootkit - 10. Таким чином, відповідно до розробленого методом, визначення тимчасових обмежень, кількість навчальних даних недостатня для побудови всіх HMM, крім MPNN. Тому для розпізнавання всієї множини Ka використана HMM типу MPNN, пристосована до навчання за допомогою експертних даних у вигляді продукційних правил. Мережа $MPNN_{\text{шт}}$ застосовується для розпізнавання Ka_s, а мережа $MPNN_{U2R}$ – для розпізнавання $\{Ka_b, Ka_l, Ka_p, Ka_r\}$.

Застосування експертних даних для розпізнавання мережних кібератак типу шторм запитів розроблено 10 продукційних правил. Із них 5 правил відповідає безпечному стану, а 5 – реалізації атаки. Приклади правил наступні.

Приклад 1.

Опис правила: Якщо в будь-який момент часу реальна кількість звернень перевищує ШНП більш, ніж в 1,5 рази, то відбувається кібератака.

Формалізований запис: Якщо $n_1 > 1{,}5 \wedge n_2 \in [0{,}24] \Longrightarrow Y = 1$.

Приклад 2.

Опис правила: Якщо в будь-який момент часу реальна кількість звернень знаходиться в межах від 1,25 до 1,4 від ШНП, то ймовірність кібератаки 0,7.

Формалізований запис: Якщо $n_1 \in [1.25{,}1.4] \wedge n_2 \in [0{,}24] \Longrightarrow Y = 0.7$.

Приклад 3.

Опис правила: Якщо в момент часу, кратному інтервалу [4,8], реальна кількість звернень знаходиться в межах від 1,2 до 1,3 від ШНП, то ймовірність кібератаки 0,8.

Формалізований запис: Якщо $n_1 \in [1.1{,}1.3] \wedge n_2 \in [4{,}8] \Longrightarrow Y = 0.8$.

Приклад 4.

Опис правила: Якщо в будь-який момент часу реальна кількість звернень знаходиться в межах від 0,8 до 1,1 від ШНП, то ймовірність кібератаки 0,1.

Формалізований запис: Якщо $n_1 \in [0.8,1.1] \wedge n_2 \in [0,24] \Longrightarrow Y = 0.1$.

Для розпізнавання кібератак типу U2R розроблені 28 продукційних правил. 14 правил відповідають відсутності кібератак, 4 правила стосуються розпізнавання buffer_overflow, 4 правила - loadmodule, 3 правила - perl і 3 правила - rootkit.

Приклад правила визначення нормального функціонування:

Якщо тривалість з'єднання (duration) = 0 ∧ протокол (protocol_type) – tcp ∧ сервіс (service) – http ∧ flag – SF ∧ кількість отриманих байтів (src_bytes) – від 0 до 400 ∧ кількість переданих байтів (dst_bytes) – від 100 до 5000 ∧ land - 0 ∧ wrong_fragment - 0 і urgent – 0 і hot – 0 ∧ num_failed_logins – 0 ∧ logged_in = 1 ∧ num_compromised = 0 ∧ root_shell – від 0 до 1 ∧ su_attempted = 0 ∧ num_root = від 0 до 1 ∧ num_file_creations – 0 ∧ і num_shells = 0 ∧ num_access_files = 0 ∧ num_outbound_cmds – 0 ∧ is_host_login = 0 ∧ is_guest_login = від 1 до 3 ∧ count = від 1 до 3 ∧ srv_count = 0 ∧ serror_rate = 0 ∧ srv_serror_rate = 0 ∧ rerror_rate = 0 ∧ srv_rerror_rate = 1.00 ∧ same_srv_rate = 0 ∧ diff_srv_rate = 0 ∧ srv_diff_host_rate від 1 до 4 ∧ dst_host_count = від 1 до 84 ∧ dst_host_srv_count = 1.00 ∧ dst_host_same_srv_rate = 0.00 і dst_host_diff_srv_rate = 0.00 ∧ dst_host_same_src_port_rate = 1.00 ∧ dst_host_srv_diff_host_rate = 0.02 ∧ dst_host_serror_rate = 0 ∧ dst_host_srv_serror_rate = 0 ∧ dst_host_rerror_rate = 0 ∧ dst_host_srv_rerror_rate = 0.

Приклад правил розпізнавання loadmodule.

Якщо тривалість з'єднання (duration) = від 70 до 110 ∧ протокол (protocol_type) – tcp ∧ сервіс (service) – telnet ∧ flag – SF ∧ кількість отриманих байтів (src_bytes) – від 1000 до 9000 ∧ land – 0 ∧ wrong_fragment – 0 ∧ urgent – 0 ∧ hot – 2 ∧ num_file_creations – від 2 до 4 ∧ num_shells = від 0 до 2 ∧

num_access_files = від 0 до 1 ∧ num_outbound_cmds – 0 ∧ is_host_login = 0 ∧ is_guest_login = 1 ∧ count = 0 ∧ srv_count = 0 ∧ serror_rate = 1 ∧ srv_serror_rate = 10 ∧ rerror_rate = 1 ∧ srv_rerror_rate = 0 ∧ same_srv_rate = 0.3 ∧ diff_srv_rate = 0 ∧ srv_diff_host_rate = 0 ∧ dst_host_count від 1 до 84 ∧ dst_host_srv_count = 10 ∧ dst_host_same_srv_rate = 1 ∧ dst_host_diff_srv_rate = 0.00 ∧ dst_host_same_src_port_rate = 1 ∧ dst_host_srv_diff_host_rate = від 0 до 0.3 ∧ dst_host_serror_rate = 0 ∧ dst_host_srv_serror_rate = 0 ∧ dst_host_rerror_rate = 0 ∧ dst_host_srv_rerror_rate = від 0 до 0.1.

3.2 Структура системи розпізнавання мережевих кібератак

Розробка НМС. Проведені дослідження дозволили розробити показану на рис. 3.1 структуру НМС розпізнавання мережних кібератак.

Основними частинами структури є:

- ПАВД – підсистема аналізу вхідних даних, за рахунок якої формується множина вхідних параметрів НММ і проводиться накопичення статистичних даних.
- ПЕО – підсистема експертної оцінки, в якій на основі експертних даних формуються продукційні правила, що характеризують стан захищеності.
- ПРС – підсистема розпізнавання і сигналізації, за рахунок якої реалізується розпізнавання кібератак і відбувається сигналізація про стан захищеності.
- МУС – модуль управління системою, яка служить для переведення системи в наступні два режими функціонування: РН (навчання НММ), РРК (розпізнавання кібератак).

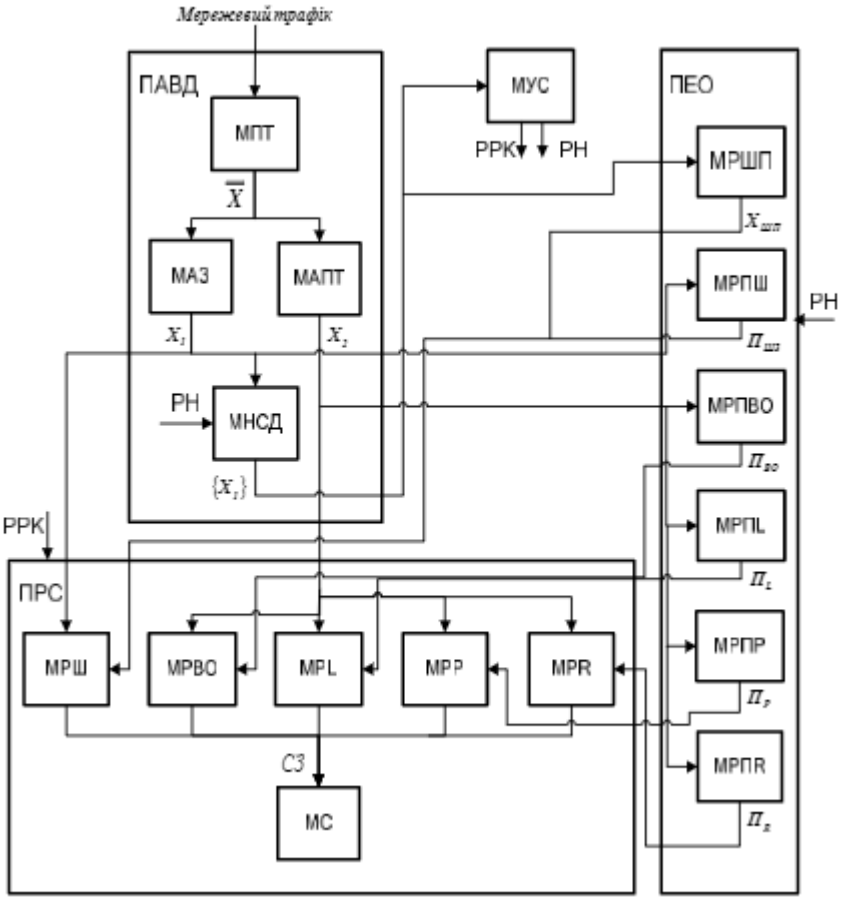

Рисунок 3.1 Структура системи розпізнавання мережевих кібератак

Призначення окремих модулей розробленої НМС, які входять до вказаних підсистем, приведено в табл. 3.1.

Таблиця 3.1 Склад нейромережевої системи розпізнавання мережевих кібератак

Назва підсистеми	Назва модуля	Призначення модуля
ПАВД	МПТ	Перехоплення вхідного тарифу веб-сервера
	МАЗ	Аналіз трафіку для визначення кількості запитів за одну секунду (X_1)
	МАПТ	Аналіз трафіку для визначення множини параметрів мережевих запитів (X_2)

	МНСД	Накопичення множин статистичних даних для формування ШНП ($\{X_1\}$)
ПЕО	МРШП	Розробка ШНП ($X_{ШП}$)
	МРПШ, МРПВО, МРПL, МРПР, МРПR	Розробка продукційних правил для розпізнавання кібератак виду шторм запитів ($П_{ШТ}$), buffer-overflow ($П_{ВО}$), loadmodule ($П_L$), perl ($П_Р$), rootkit ($П_R$).
ПРС	МРШ, МРВО, МРL, МРР, МРR	Розпізнавання кібератак виду шторм запитів, buffer_overflow, loadmodule, perl, rootkit.
	МС	Сигналізація

Експериментальні дослідження. На першому етапі була розроблена марківська модель ШНП кількості звернень до веб-сервера за 1с. Статистичні дані зібрані протягом 2012 р. в процесі експлуатації веб-сервера одного з комерційних установ країн СНД. Зі статистики відфільтровані дані, відповідні атакам, зафіксованим системою визначення атак.

Проведений аналіз показав відсутність тренда і наявність періодичних складових. Побудована періодограма кількості звернень до веб-сервера показана на рис. 3.2.

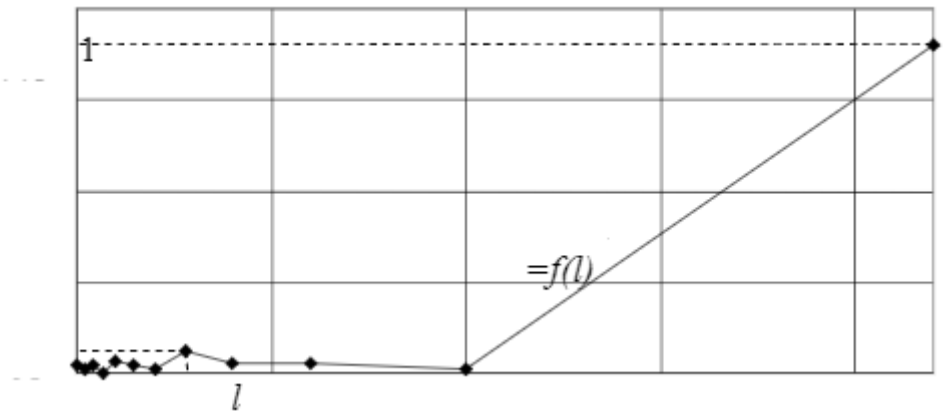

Рисунок 3.2. Періодограма кількості звернень до веб-сервера

На періодограмі простежується два максимума $I_1 = 102$ і $I_2 = 1442$, яким відповідають періоди $l_1 = 4{,}8$ год. і $l_2 = 24$ год. Тому статистичні дані розглядалися як два періодичні ряди даних з періодами 4,8 год. і 24 години.

Для моделювання двох періодичних рядів створена марківська модель, яка складається з двох модулів (марківських моделей) M_1 і M_2.

Модуль M_1 призначений для моделювання процесу з періодом l_1 = 24 год., а модуль M_2 – для моделювання процесу з періодом l_2 = 4,8 год. В межах періоду l_1 визначені дві нестаціонарні точки: максимуму $A^{(24)} = 12$ год. і мінімуму $B^{(24)} = 0$ год. У зв'язку з тривалим терміном ($l_1/2 = 12$ год.) і різкими змінами ПБ моделювання на напівперіоді проводилося за допомогою чотирьох ЛМ. Для цього кожен напівперіод був розділений на два однакових відрізка, кожному з яких відповідала своя ЛМ. Таким чином M_1 складався з чотирьох ергодичної стаціонарних ЛМ – $L_{1,1}^{(1)}$, $L_{1,2}^{(1)}$, $L_{2,1}^{(1)}$ і $L_{2,2}^{(1)}, L_{1,1}^{(1)}, L_{1,1}^{(1)}$, призначених для моделювання на інтервалах, кратних [0, 6], $L_{1,2}^{(1)}$ – на інтервалах, кратних [6, 12], $L_{2,1}^{(2)}$ – на інтервалах кратних [12, 18], а $L_{2,2}^{(2)}$ – на інтервалах, кратних [18,24].

Також при побудові ЛМ прийнято, що можливі переходи тільки між трьома сусідніми станами. Результати моделювання ШП за допомогою M_1 показані на рис. 3.3 у вигляді графіків математичного очікування і розподілу ймовірності.

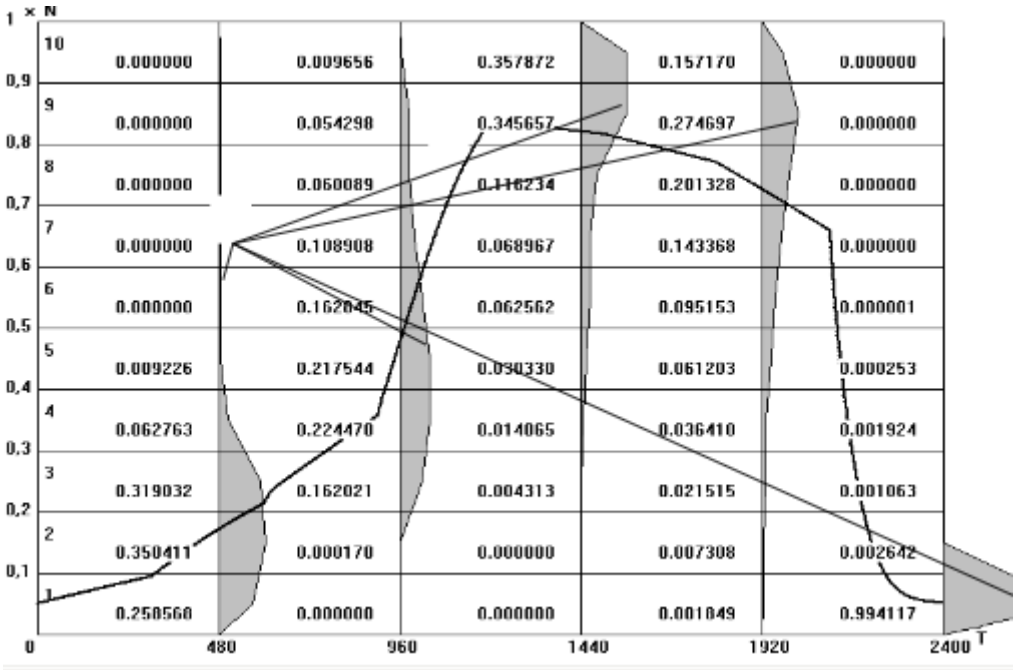

Рисунок 3.3. Параметри марківської моделі M_1 із періодом 24 год.

На рис. 3.3 символом *A* позначений графік математичного очікування, а символом *B* – графіки ймовірності розподілу по станах ЛМ.

Модель M_2 складається з двох ергодичних стаціонарних ЛМ – $L_1^{(2)}$ і $L_2^{(2)}$. ЛМ $L_1^{(2)}$ призначена для моделювання на інтервалах, кратних [0, 2.4], а $L_2^{(2)}$ – на інтервалах, кратних [2.4, 4.8]. При цьому середня відносна похибка математичного очікування становить ≈ 7 %, що в 1,5-2 рази менше, ніж похибка поширених моделей ШП веб-сервера.

4. ЕРГОНОМІКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

4.1 Розрахунок часу евакуації людей при пожежі в приміщенні

Підприємство є одноповерховою будівлею, що відображена на рис. 4.1 розмірами 10 м. на 20м.; кількість робочих кімнат 8; кількість працюючих 13; кількість виходів 1.

Для розрахунку загального часу евакуації необхідно розрахувати час на кожній ділянці руху людей, починаючи від максимально віддаленої точки.

Рух людей під час процесу евакуації є вимушеним, тобто пов’язаним із необхідністю покинути приміщення чи будівлю через виниклу небезпеку. Вимушений рух людей має свої специфічні особливості, вже на початковій стадії, людині погрожує небезпека в результаті того, що пожежа супроводжується виділенням теплоти, продуктів повного й неповного згорання, токсичних речовин, обвалення конструкцій, що так чи інакше погрожує людині. Із цього слід зробити висновок, що при плануванні будівлі і устрої приміщень в них необхідно прийняти заходи, щоб процес евакуації міг закінчитися безпечно і в необхідний час.

Друга особливість полягає у тому, що в силу погрожуючої людині небезпеки рух інстинктивно починається одночасно в один і той же напрям – у сторону виходів. Це призводить до того, що проходи швидко заповнюються людьми при визначеній щільності потоків. Із збільшенням щільності потоків швидкість руху зменшується, що створює певний визначений ритм руху. В цій ситуації з’являється погроза утворення затору, і дуже важко запобігти їй.

Показником ефективності процесу вимушеної евакуації є час, на протязі якого люди можуть при необхідності покинути окремі приміщення і будівлю в цілому. Безпечність, досягнута тоді, коли цей час менший, ніж тривалість пожежі. Короткочасність процесу евакуації повинна досягатися не тільки конструктивно-планувальними рішеннями, на які звертали увагу раніше, але й організаційними рішеннями.

Процес евакуації людей можна поділити на три етапи :

- рух людей від найбільш віддаленої точки приміщення до евакуаційних виходів;
- рух людей від евакуаційних виходів до виходів на зовні;
- рух людей від виходів із будівлі та їх розсіювання.

При евакуації основними параметрами, які характеризують процес руху людей є :

1) щільність людського потоку – *D*, люд/м2;

2) швидкість руху людського потоку – *v*, м/хв;

3) пропускна спроможність шляху (виходів) - *Q* ;

4) інтенсивність руху людського потоку - *q* ;

1) Щільність людського потоку *D*, яка складається з *N* людей, дорівнює:

$$D_1 = \frac{N_1 f}{A}, \text{ м}^2/\text{м}^2 \qquad (4.1)$$

де $A = g \cdot l$ – площа шляху евакуаційної ділянки [м²];

l – довжина ділянки; *g*- ширина ділянки;

f – площа горизонтальної проекції людини.

Якщо $D < 0.05$ людина має повну свободу пересування;

Якщо $0.05<D<0.15$ людина не може вільно змінювати напрямок свого руху;

Якщо $0.15<D<=0.92$ люди рухаються вкупі. Величина 0.92 є верхньою межею, коли люди рухаються вкупі, та нею обмежується щільність при проектуванні евакуаційних шляхів.

2) Швидкість руху людського потоку *v* залежить від його щільності *D* та виду шляху (горизонтальні чи похилі). Значення швидкості v, а також інтенсивності руху людського потоку q в залежності від його цільності D приведено в табл. 4.1.

Таблиця 4.1 Значення швидкості *v* і інтенсивності *q* руху людського потоку залежно від його щільності D

Щільність потоку $м^2/м^2$, Д	Горизонтальний шлях		Дверний пройом	Сходи вниз		Сходи вверх	
	Швидкість м/хв. *v*	Інтенсив-ність, *q* м/хв.	Інтенсив-ність, *q* м/хв.	Швидкість м/хв. *v*	Інтенсив-ність, *q* м/хв.	Швидкість м/хв. *v*	Інтенсив-ність, *q* м/хв.
0,01	100	1	1	100	1	60	0,6
0,05	100	5	5	100	5	60	3
0,1	80	8	8,7	95	9,5	53	5,3
0,2	60	12	13,4	68	13,6	40	8
0,4	40	16	18,4	40	16	26	10,4
0,6	27	16,2	19	24	14,4	18	10,8
0,8	19	15,2	17,3	13	10,4	13	10,4
0,9 и більше	15	13,5	8,5	8	7,2	11	9,9

3) Пропускна спроможність шляху *Q* (м/хв чи люд/хв)

$$Q = D \cdot v \cdot \delta \text{ , м}^2\text{/хв.} \quad (4.2)$$

4) Інтенсивністю руху людського потоку *q* (м/хв чи люд/хв)

$$q = D \cdot v \quad (4.3)$$

Інтенсивність руху не залежить від ширини шляху і являється характеристикою потоку. Інтенсивністю руху людського потоку на кожному відрізку дорівнює:

$$q_i = \frac{q_{i-1}\delta_{i-1}}{\delta_i} \text{ , м/хв.} \quad (4.4)$$

де: δ_I, δ_{i-1} – ширина розглядаючого і-го і перед ним (і – 1) відрізків шляху, м;

q_i, q_{i-1} – значення інтенсивності руху потоку на розглядаючому і-му і перед ним (і - 1) відрізках шляху, м/хв.

Якщо q_i менше чи рівно q_{max}, то час руху на відрізку можні визначити по формулі:

$$t_1 = \frac{l_1}{v_1}, \qquad (4.5)$$

при цьому значение q_{max} треба приниймати рівним, м/хв.:

- для горизонтальних шляхів 16,5
- для дверних проємів 19,6
- для сходів вниз 16
- для сходів вверх 11

Розрахунковий час евакуації людей із приміщення й будівлі *tp* встановлюється по розрахунку часу руху людських потоків від найбільш віддалених місць розташування. При розрахунку весь шлях руху людського потоку поділяється на ділянки (прохід, коридор, сходинковий марш, дверний проріз, тамбур) довжиною l_i і шириною g_i.

Початковими ділянками являються проходи між робочими місцями.

Розрахунковий час евакуації дорівнює :

$$t_p = t_1 + t_2 + t_3 + \ldots + t_i = t \text{ [хв]}, \qquad t_i = l_i / v_i \text{ [хв]}.$$

де t_i – час руху людського потоку на кожній окремій ділянці.

Умова безпечної евакуації характеризується виразом $t_p <= t_{нб}$, тобто розрахункова тривалість вимушеної евакуації на різноманітних ділянках при розрахункових швидкостях людей і розрахунковій пропускній спроможності евакуаційних дверей повинна бути рівна або менша необхідного часу тривалості евакуації. Необхідний час евакуації $t_{нб}$ визначається по таблиці.

Використовуючи вище зазначений опис, за винятком таких ділянок як дверний проріз та тамбур (не передбачена у будівлі), проведемо розрахунок часу евакуації людей для прийнятого приміщення.

Маршрут евакуації розбивається на дев'ять етапів (ділянок). Для проведення розрахунку задамося планом евакуації людей (рис. 4.1).

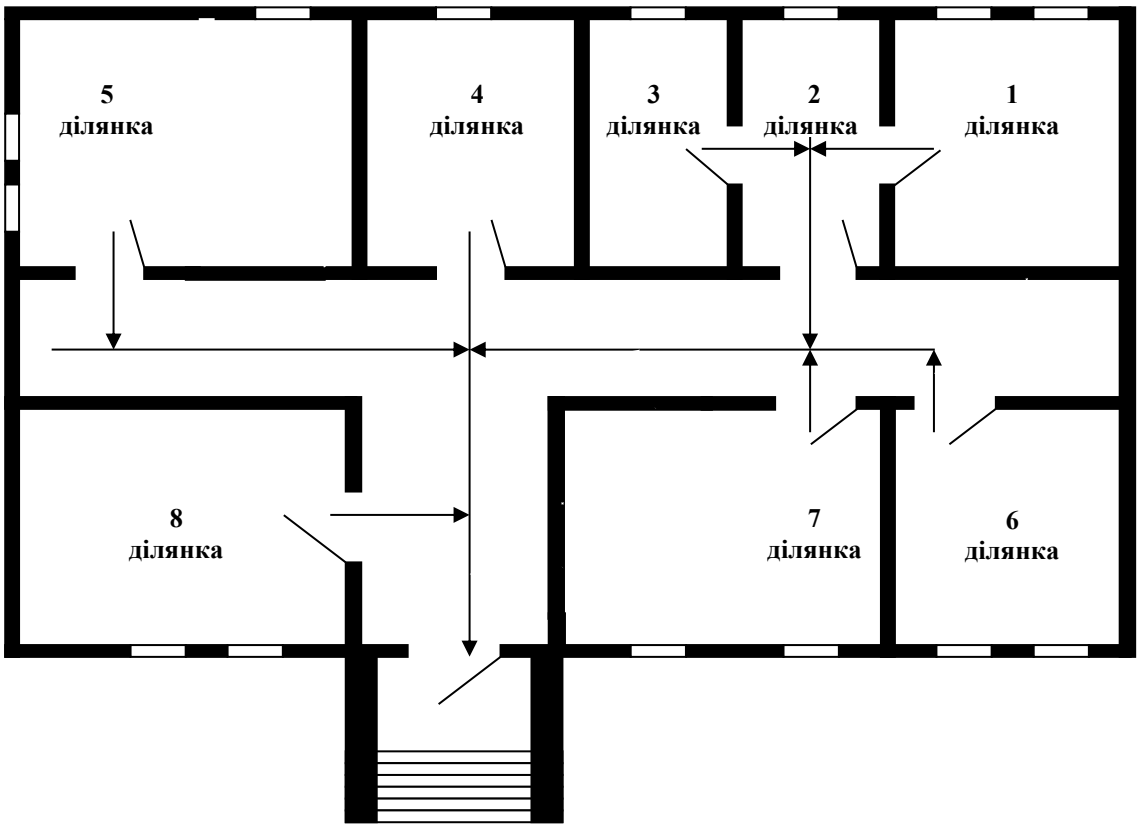

Рисунок 4.1 План евакуації людей

Перша ділянка

Час руху людського потоку – вихід людей з кімнати № 1:

де l= 13 м – довжина ділянки ; v – швидкість руху на ділянці.

f = 0.113 м^2 – середня площа горизонтальної проекції людини ;

N = 2 – кількість людей ; S= 3 м – ширина ділянки .

$$D_1 = 2\left(\frac{0.113}{3 \cdot 13}\right) = 0.006 \text{ [м}^2\text{/м}^2\text{]}$$, тоді v_1 = 100 м/хв ; q_1= 1 м/хв.

t_1 = 13/100 =0,13 хв.

Друга ділянка

Час руху людського потоку – вихід людей з кімнати № 2:

$$D = 3\left(\frac{0.113}{11 \cdot 3}\right) = 0.01 \text{ [м}^2\text{/м}^2\text{]}$$, тоді v_3 = 100 м/хв ; q_3= 1 м/хв.

t_2 = 11/100 =0,11 хв.

де l= 11 м; f= 0.113 м^2; N= 3; S= 3 м.

Третя ділянка

Час руху людського потоку – вихід людей з кімнати № 3:

$D = 1\left(\frac{0.113}{12 \cdot 3}\right) = 0.003$ [м^2/м^2], тоді v_2 = 100 м/хв; q_2= 1 м/хв.

t = 12/100 =0,12 хв.

де l= 12 м; f= 0.113 м^2; N= 1; S= 3 м.

Четверта ділянка

Час руху людського потоку – вихід людей з кімнати № 4:

$D = 2\left(\frac{0.113}{5 \cdot 3}\right) = 0.01$ [м^2/м^2], тоді v_4= 100 м/хв; q_4= 1 м/хв.

t = 5/100 =0,05 хв.

де l= 5 м; f= 0.113 м^2; N= 2; S= 3 м.

П'ята ділянка

Час руху людського потоку – вихід людей з кімнати № 5:

$D = 2\left(\frac{0.113}{12 \cdot 3}\right) = 0.007$ [м^2/м^2], тоді v_5= 100 м/хв ; q_5= 1 м/хв.

t = 12/100 =0,12 хв.

де l= 12 м; f= 0.113 м^2; N= 2; S= 3 м.

Шоста ділянка

Час руху людського потоку – вихід людей з кімнати № 6:

$D = 2\left(\frac{0.113}{12 \cdot 3}\right) = 0.007$ [м^2/м^2], тоді v_6= 100 м/хв; q_6= 1 м/хв.

t = 12/100 =0,12 хв.

де l= 12 м; f= 0.113 м^2; N= 2; S= 3 м.

Сьома ділянка

Час руху людського потоку – вихід людей з кімнати № 7:

$D = 2\left(\frac{0.113}{9 \cdot 3}\right) = 0.008$ [м^2/м^2], тоді v_7= 100 м/хв; q_7= 1 м/60в..

Т = 9/100 =0,09 хв.

Де l= 9 м; f= 0.113 м^2; N= 2; S= 3 м.

Восьма ділянка

Час руху людського потоку – вихід людей з кімнати № 8:

$D = 2\left(\frac{0.113}{3 \cdot 3}\right) = 0.02$ [м^2/м^2], тоді v_8 = 100 м/хв; q_8 = 1 м/хв.

t = 3/100 =0,03 хв.

де l = 3 м; f = 0.113 м^2; N = 2; S = 3 м.

Дев'ята ділянка

Час руху людського потоку – вихід людей з кімнати № 9:

$D = 7\left(\frac{0.113}{9 \cdot 3}\right) = 0.03$ [м^2/м^2], тоді v_9 = 100 м/хв; q_9 = 1 м/хв.

t = 9/100 =0,09 хв.

де l = 9 м; f = 0.113 м^2; N = 7; S = 3 м.

Десята ділянка

Час руху людського потоку – вихід людей з кімнати № 10:

$D = 11\left(\frac{0.113}{5 \cdot 3}\right) = 0.08$ [м^2/м^2], тоді v_{10} = 100 м/хв; q_{10} = 1 м/61в..

T = 5/100 =0,05 хв.

Де l = 5 м; f = 0.113 м^2 ; N = 11; S = 3 м.

Одинадцята ділянка

Час руху людського потоку – вихід людей з кімнати № 11:

$D = 13\left(\frac{0.113}{3 \cdot 3}\right) = 0.1632$ [м^2/м^2], тоді v_{11} = 60 м/хв; q_{11} = 12 м/хв.

t = 3/60 =0,05 хв.

де l = 3 м; f = 0.113 м^2 ; N = 13; S = 3 м.

Загальний час евакуації : $t = t1 + t2 + ... + t18$ = 1,01 [хв].

$t_{нб}$ = 2,5 хвилин для одноповерхового будинку (з СНиП 2.01.02-85, табл. 12)

t = 1,01 < $tнб$ = 2,5 хв, тобто вимоги пожежної безпеки виконуються.

В зв’язку з можливістю виникнення пожежі на території будівлі внаслідок несправної роботи комп’ютернрї техніки, яка підключена до електромережі, я вирішив вибрати вуглекислотні вогнегасники моделі ОУ-8 та порошкові – моделі ОП-8Б. Розмістити їх необхідно на пожежних щитах в вестибюлі та біля пожежного, по одному екземпляру кожного типу.

За допомогою вогнегасника ОУ-8 можна гасити різні речовини, крім тих, які можуть горіти без доступу повітря. Також їм можна тушити пожежу в пристроях під напругою до 1000V, при умові приближення по струмопровідних частин не ближче одного метру.

Механізм припинення горіння за допомогою використання вуглекислого газу базується на його властивостях шляхом розбавлення знижувати концентрацію реагуючих речовин до рівня, при якому горіння становиться неможливим.

За допомогою вогнегасника ОП-8Б можна тушити палаюче електрообладнання під напругою до 1000V, легкозаймисті рідини, тліючі матеріали (навіть ті що горять без доступу повітря) праці в робочому приміщенні.

4.2 Ергономічні вимоги до організації і обладнання робочих місць з комп`ютерною технікою

Оператор обробки інформації при виконанні своєї роботи майже весь робочий час знаходиться в сидячому положенні за робочим столом, на якому розташоване його робоче обладнання. Для запобігання виникнення, пов`язаних з таким видом робіт, хвороб (скаліоз, хвороби очей та ін.), а також для усунення загального дискомфорту, зменшення втомлюваності працівника, підвищенню його продуктивності необхілно правильно організувати робоче місце.

Організація робочого місця передбачає:

- правильне розміщення робочого місця у виробничому приміщенні;
- вибір ергономічного обгрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини;
- раціональну компановку обладнання на робочих місцях;
- урахування характеру та особливостей трудової діяльності;
- ДНАОП 0.00-1.31-99, ГОСТ 12.2.032-78, ДСанПІН 3.3.2.007-98 регламентує такі вимоги до організації робочого місця користувача ВДТ (візуальний дисплейний термінал):

1) Конструкція робочого столу має відповідати сучасним вимогам ергономіки і забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів. Рекомендовані розміри столу: висота – 725 мм, ширина – 600-1400 мм, глибина – 80-1000 мм. Робочий стіл повинен мати простір для ніг висотою не менше ніж 450 мм, на рівні витягнутої ноги не менше 650 мм.

Робоче місце має бути обладнане підставкою для ніг шириною не менше ніж 300 мм, глибиною не менше ніж 400 мм, з можливістю регулювання по висоті в межах 150 мм та кута нахилу опорної поверхні – в межах 20°. Підставка повина мати рифлену поверхню і бортик по передньому краю заввишки 10 мм.

2) Робочий стілець користувача ВДТ повинен мати такі основні елементи: сидіння, спинку та стаціонарні або знімні підлокітники. Робочий стілець має бути підйомно – поворотним, регульованим за висотою, за кутом нахилу сидіння та спинки і за відстанню від спинки до попереднього краю сидіння. Поверхня сидіння має бути плоскою, передній край заокругленим.

Висота поверхні сидіння має регулюватися в межах 400…500 мм, а ширина і глибина становити не менше ніж 400 мм. Кут нахилу сидіння – до 15° вперед і до 5° назад.

Висота спинки має становити (300 ± 20) мм, ширина – не менше ніж 380 мм, радіус кривизни горизонтальної площини – 400 мм. Кут нахилу спинки має регулюватися в межах 0…30° від вертикального положення. Відстань від спинки до переднього краю сидіння має регулюватися в межах 260…400 мм.

Для зниження статичного навантаження м`язів верхніх кінцівок слід використовувати стаціонарні або знімні підлокітники довжиною не менше ніж 250 мм, шириною не менше ніж 50…70 мм. Що регулюються за висотою над сидінням у межах 230…260 мм і відстанню між підлокітниками в межах 350…500 мм.

Поверхня сидіння і спинки стільця має бути напівм`якою з нековзним, повітронепроникненим покриттям, що легко чиститься і не електризується.

Конструкція виробничих меблів для користувача ВДТ має бути такою, щоб забезпечувати йому підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг – на підлозі або на підставці для ніг; стегна – в горизонтальній площині; верхні частини рук – вертикальні; кут ліктьового суглоба (між плечем та передпліччям) – 70 - 90°; зап`ястки зігнуті під кутом не більше 20° відносно горизонтальної площини, нахил голови вперед в межах 15-20° до вертикалі.

3) Дисплей має розташуватися на столі на відстані від очей користувача не більше 700 мм (оптиальна відстань 450 – 500 мм). Розташування екрану має забезпечувати зручність зорового спостереження у вертикальній площині під кутом + 30° до нормальної лінії погляду працюючого. В горизонтальній площині кут спостереження екрану не повинен перевищувати 60°.

4) Клавіатуру слід розташувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого. У конструкції клавіатури має передбачитися опорний пристрій, який дає змогу зиінювати кут нахилу поверхні клавіатури у межах 5…10°. Висота середнього рядка клавіш має не перевищувати 30 мм. Поверхня клавіатури має бути матовою з коефіцієнтом відбиття 0,4.

5) Документ для вводу даних розташовується на відстані 450…500 мм від очей працівника, переважно зліва, кут між екраном дисплея та документом в горизонтальній площині має бути 30 - 40°.

6) Розміщення принтера або іншого пристрою введення – виведення інформації на робочому місці має забезпечувати добру видимість екрана ВДТ, зручність ручного керування пристроєм введення – виведення інформації в зоні досяжності: по висоті 900 – 1300 мм, по глибині 400 – 500 мм. Під принтери ударної дії потрібно підкладати вібраційні килимки для гасіння вібрації та шуму. На рис. 4.2 зображено вид робочого місця з ВДТ: А-принтер. В-монітор. С-системний блок. D-клавіатура. Е-папка для документів.

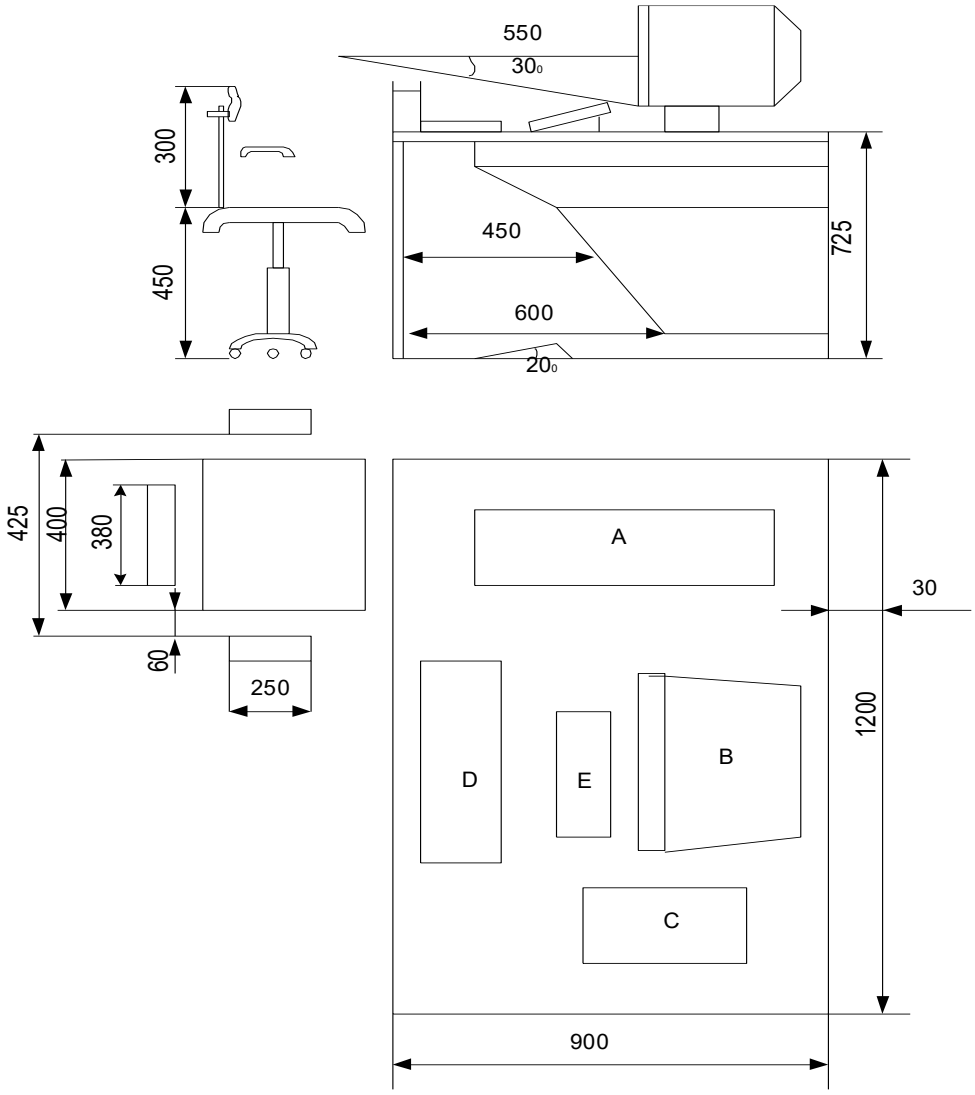

Рисунок 4.2 Вид робочого місця з ВДТ

ВИСНОВКИ

Дана робота присвячена для вирішення актуальної научно-прикладної проблеми, створення комплексної методології розробки широкодоступних ефективних нейромережевих методів оцінки параметрів безпеки інтернет-орієнтованих інформаційних систем, які дозволяють швидко розпізнати нові види кібератак при обмежених розрахункових можливостях і варіативності умов застосування.

Для реалізації поставленої задачі було виконано наступні завдання:

- аналіз предметної області.
- вивчено будову нейромережевих методів оцінки параметрів безпеки інтернет-орієнтованих інформаційних систем.
- проведений аналіз типових загроз в інтернет-орієнтованих інформаційних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. WiFiver.com - український Wi-Fi портал

2. http://wifi.nau.edu.ua/- WI-FIмережа НАУ

3. Шахнович І. «Сучасні Технології бездротового зв'язку» - М.: Техносфера, 2004

4. Джим Гейер. «Бездротові Мережі. Перший крок »- М.: Видавництво: Вільямс, 2005

5. "Основы построения беспроводных локальных сетей стандарта 802.11", Рошан, Издательский дом "Вильямс", Москва, 2004

6. В. Г. Олифер, Н. А. Олифер Компьютерные сети. Принципы, технологии, протоколы.4-е изд.-2008, СПб, Издательский дом "Питер", 958 стр.

7. Гордейчик С. В., Дубровин В. В. Безопасность беспроводных сетей.- М.: Горячая линия- Телеком, 2008.- 288 с.:.

8. Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видатничій Центр, 2002. – 520 с.

9. Рослякв А.В., Ваняшин С.В., Самсонов М.Ю. и др. Сети следующего поколения NGN / Под ред. А.В. Рослякова. – М.: Эко-Трендз, 2008. – 424 с.

10. Величко В.В., Катунин Г.П., Шувалов В.П. Оснолвы инфокоммуникационных технологий. Учебное пособие для вузов/Под ред. В.П. Шувалова. – М.: Горячая линия – Телеком, 2009. – 712 с.

11. Иртегов Д.В. Введение в сетевые иехнологии. – СПБ.: БХВ-Петербург, 2004. – 560 с.

12. Autonomic Systems: Concept for Self-Managing IT Infrastructure White Paper. Fujitsu Siemens Computers, March 2003.

13. Brassard G. Modern Cryptology. - N.Y.: Springer-Verlag, 1988. - 107 p.

14. Cisco Systems, Designing a Campus Network for High Availability. – 2006 – 60с.

15. Cisco Systems, Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design. – 2006. – 91с.

16. Cisco Systems, Understanding Rapid Spanning Tree Protocol (802.1w) (Document ID: 24062). - 2006. – 14с.

17. Cisco Systems, Understanding Multiple Spanning Tree Protocol (802.1s) (Document ID: 24248). – 2005. – 14с.

18. David Hucaby. CCNP Self-Study: CCNP BCMSN Exam Certification Guide, Third Edition. – Cisco Press, 2005. – 624с.

19. Dave Hucaby, Steve McQuerry. Cisco Field Manual: Catalyst Switch Configuration. – Cisco Press, 2002. – 560с.

20. Eric Ouellet, Robert Padjen, Arthur Pfund, Ron Fuller, Tim Blankenship ―Building a Cisco Wireless LAN‖ - Syngress Publishing, Inc, 2002.

21. Глибовець М. М. Штучний інтелект / М. М. Глибовець, О. В. Олецький. – К. : Києво-Могилн. Акад., 2002. – 366 с.

22. Богуш В. М. Інформаційна безпека: термінологічний навчальний довідник / В. М. Богуш, В. Г. Кривуца, А. М. Кудін. – К. : ДВК, 2004. – 508 с.

23. Фленов М. Е. PHP глазами хакера / М. Е. Фленов. – СПб. : БХВ-Петербург, 2005. – 304 с.

24. Ткаченко Р. О. Нейронні мережі прямого поширення з неітераційним навчанням : автореф. дис. на здобуття наук. Ступеня д-ра техн. наук : спец 05.13.06 “Автоматизовані системи управління та прогресивні інформаційні технології” / Р. О. Ткаченко. – Л., 2000. – 32 с.

25. Джерри Х. Реестр Microsoft Windows XP / Джерри Х. ; пер. з. англ. – М. : Еком, 2006. – 656 с.

26. Менаске Д. Производительность Web-служб. Аналіз, оцінка і планування / Менаске Д., Виргило А. ; пер. з англ. – СПб : ДиаСофтЮп, 2003. – 480 с.

27. Яциковська У. О. Моделювання мережного трафіку комп'ютерної мережі під час реалізації атак типу Dos/DDoS / У. О. Яциковська, М. П. Карпінський // Інформаційна безпека. – 2011. - № 1(5). – С. 142-146.

28. Bezobrazov S., Glovko V. Neural Networks for Artificial Immune Systems: LVQ for Detectors Construction // International Workshop on Intelligent Data Acquisition and Advanced Computing System: Technology and Applications. – Dortmund, 2007. – P. 180-184.

29. Абрамов Е. С. Разработка и исследование методов построения систем обнаружения атак: дис. канд. техн. наук: 05.13.19 / Абрамов Е. С. – Таганрог, 2005. – 199 с.

30. Айвенс К. Комп'ютерні мережі / Айве К. ; пер. з англ. – СПб. : Питер, 2006. – 304 с.

31. Дьяконов М. Ю. Нейросетевая система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем: автореф. Дисс. На соискание научн. Степени канд. техн. наук : спец. 05.13.19 – Методы и системы защиты информации, информационная безопасность / М. Ю. Дьяконов – Уфа, 2010. – 28 с.

32. Васильев В. И. Нейронные сети при обнаружении атак в сети Internet (на примере атаки SYNFLOOD) / В. И. Васильев, А. Ф. Хафизов // Нейрокомпьютеры в информационных и экспертных системах. – М.: Радиотехника, 2007. – №6. – С. 34-38.

33. Емельянова Ю. Г. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы / Ю. Г. Емельянова, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко // Программные системы: теория и приложения. – 2011. – №3(7). – С. 3-15.

34. Закер К. Компьютерные сети / Закер К.; : пер. с англ. – СПб. : БХВ-Петербург, 2000. – 1008 с.

35. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – СПб. : БХВ-Петербург, 2000. – 450 с.

36. Карпінський М. П. Аналітичний метод дослідження величини зміни параметрів сигналів у бездротових сенсорних мережах / М. П. Карпінський, В. М. Чиж, С. М. Балабан // Вісник Національного університету “Львівська політехніка”. Серія : Комп’ютерні системи та мережі. – 2014. – №806. – С. 93.

37. Gurney, Kevin (1997). An introduction to neural networks. UCL Press. ISBN 1857286731. OCLC 37875698.

38. Штучна нейронна мережа [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki.

39. Kruse, Rudolf,; Borgelt, Christian; Klawonn, F.; Moewes, Christian; Steinbrecher, Matthias; Held,, Pascal (2013). Computational intelligence : a methodological introduction. Springer. ISBN 9781447150121. OCLC 837524179.

ДОДАТКИ

Додаток А

Графічні матеріали

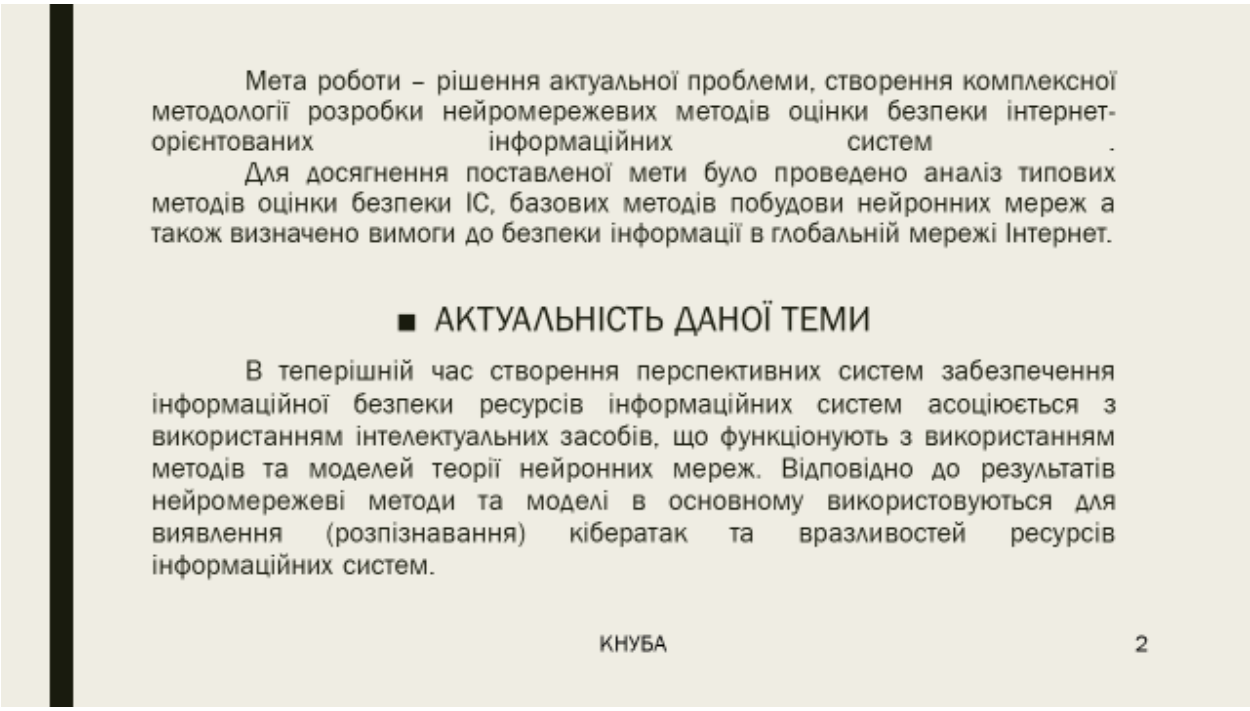

Рисунок 5.2 Мета та актуальність роботи

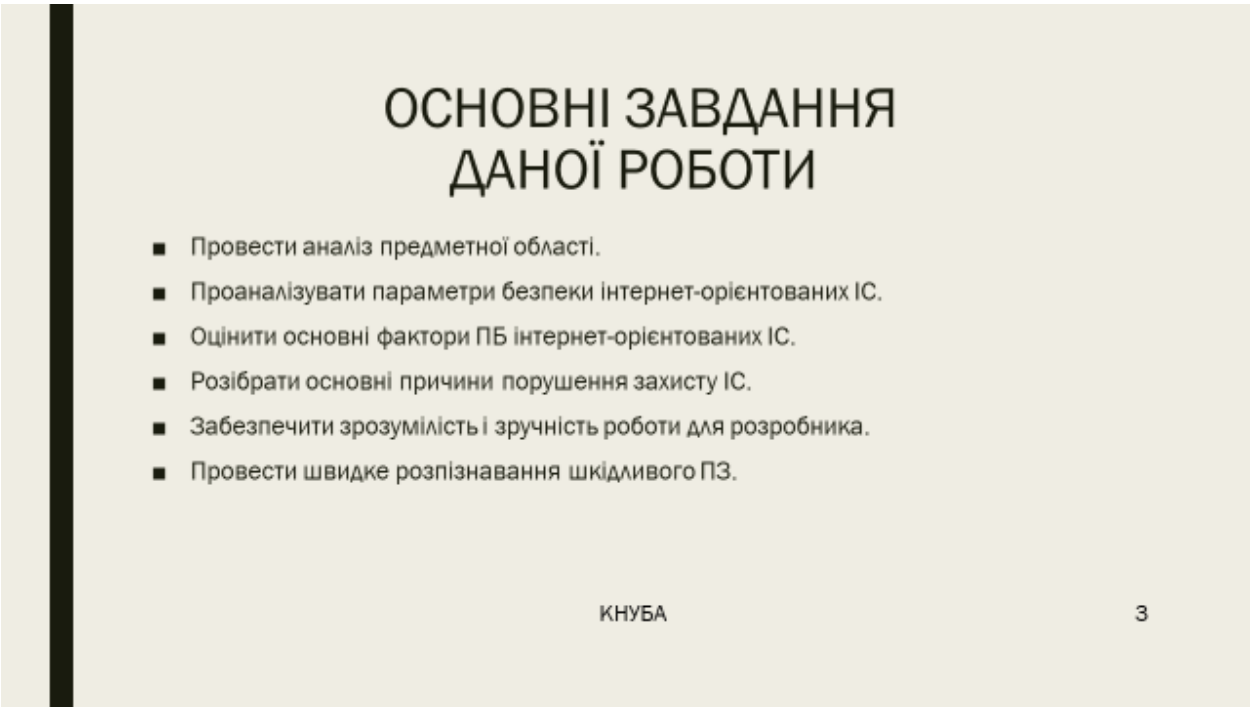

Рисунок 5.3 Основні завдання бакалаврської роботи

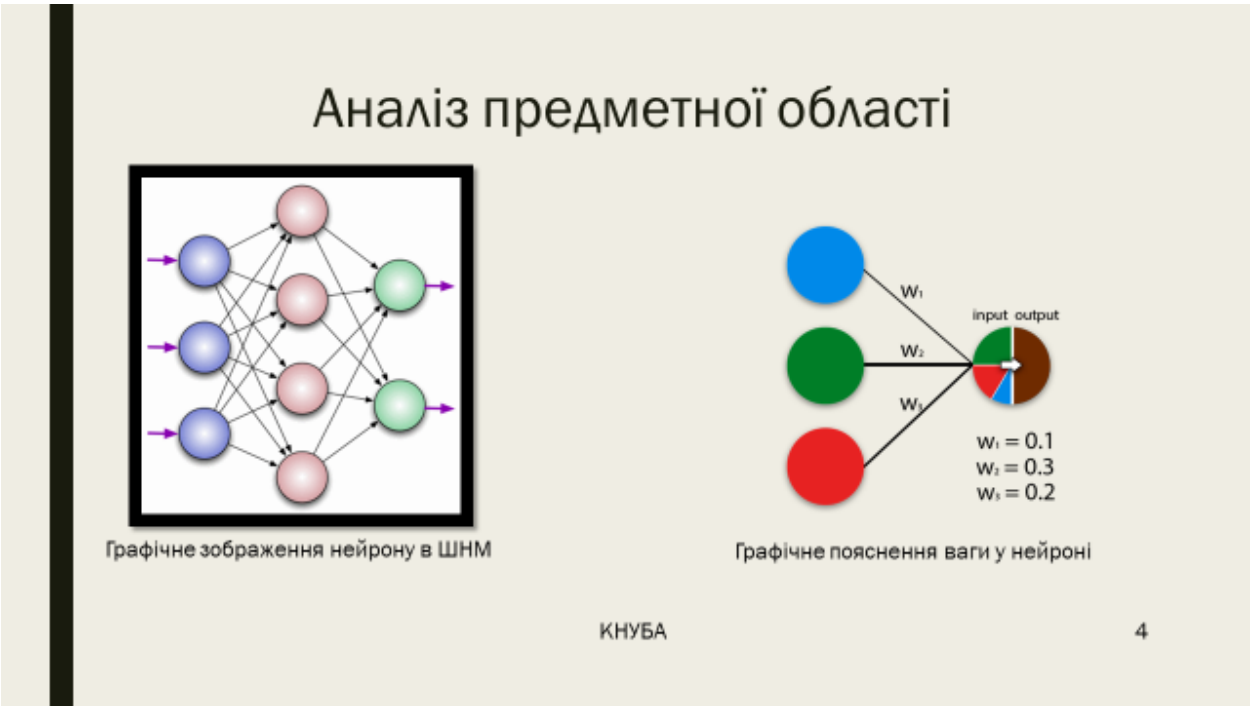

Рисунок 5.4 Аналіз предметної області

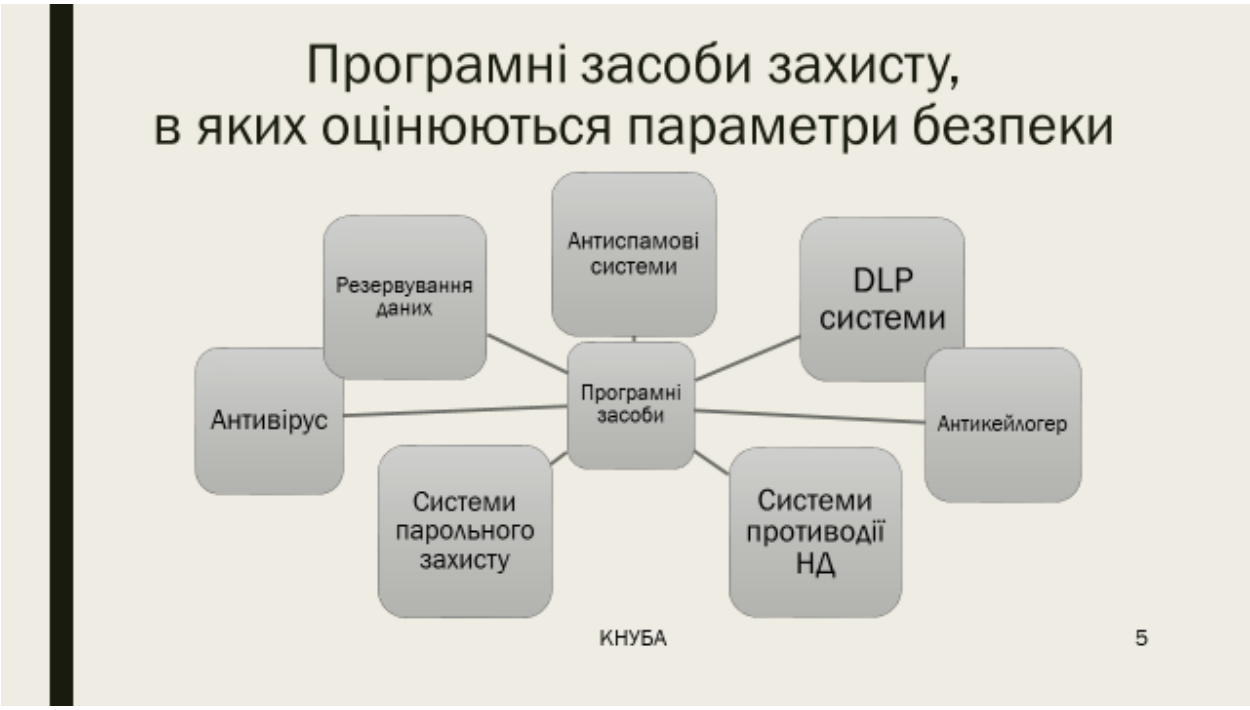

Рисунок 5.5 Засоби оцінок параметрів безпеки інтернет-ресурсів інформаційних систем

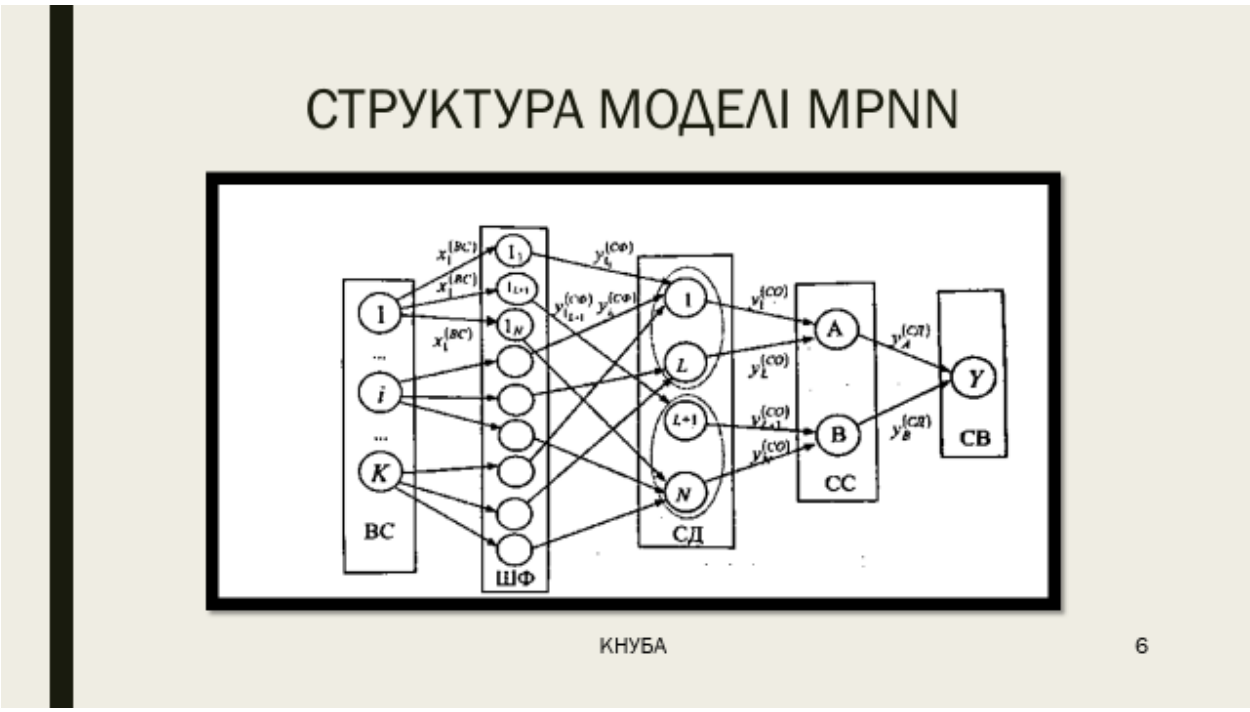

Рисунок 5.6 Структура моделі MPNN

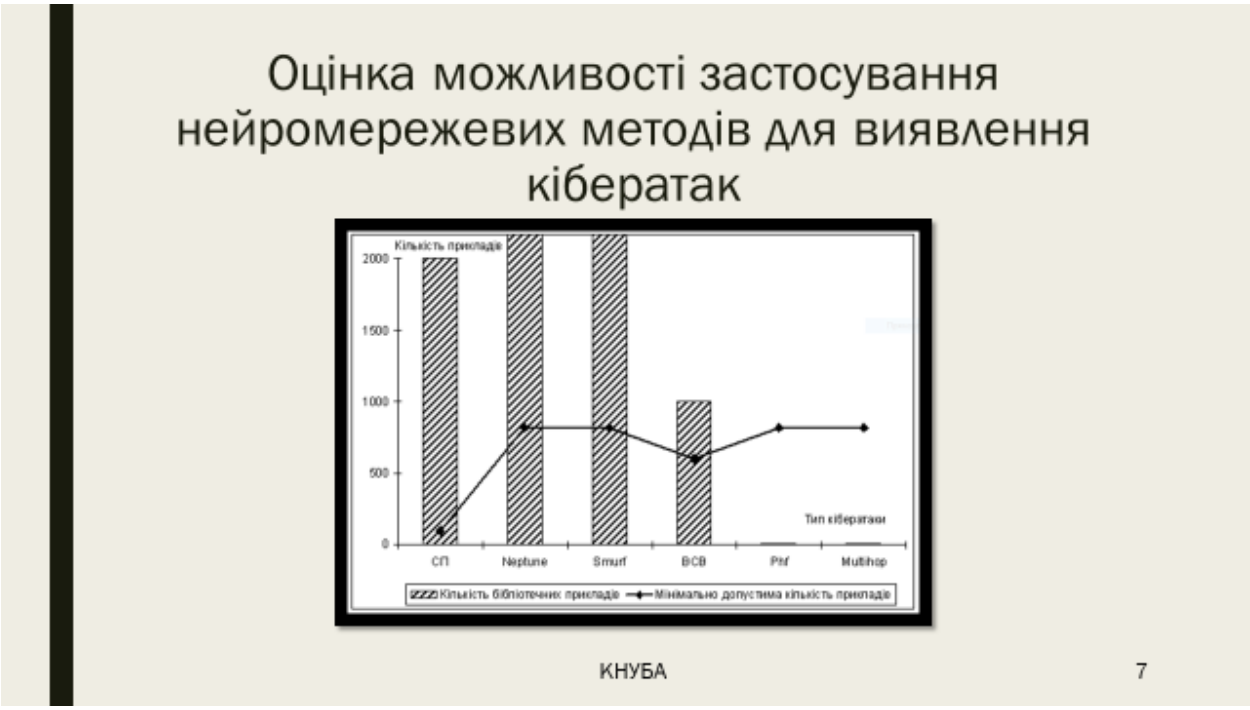

Рисунок 5.7 Оцінка можливості застосування нейромережевих методів для виявлення кібератак

Рисунок 5.8 Структура системи розпізнавання мережевих кібератак

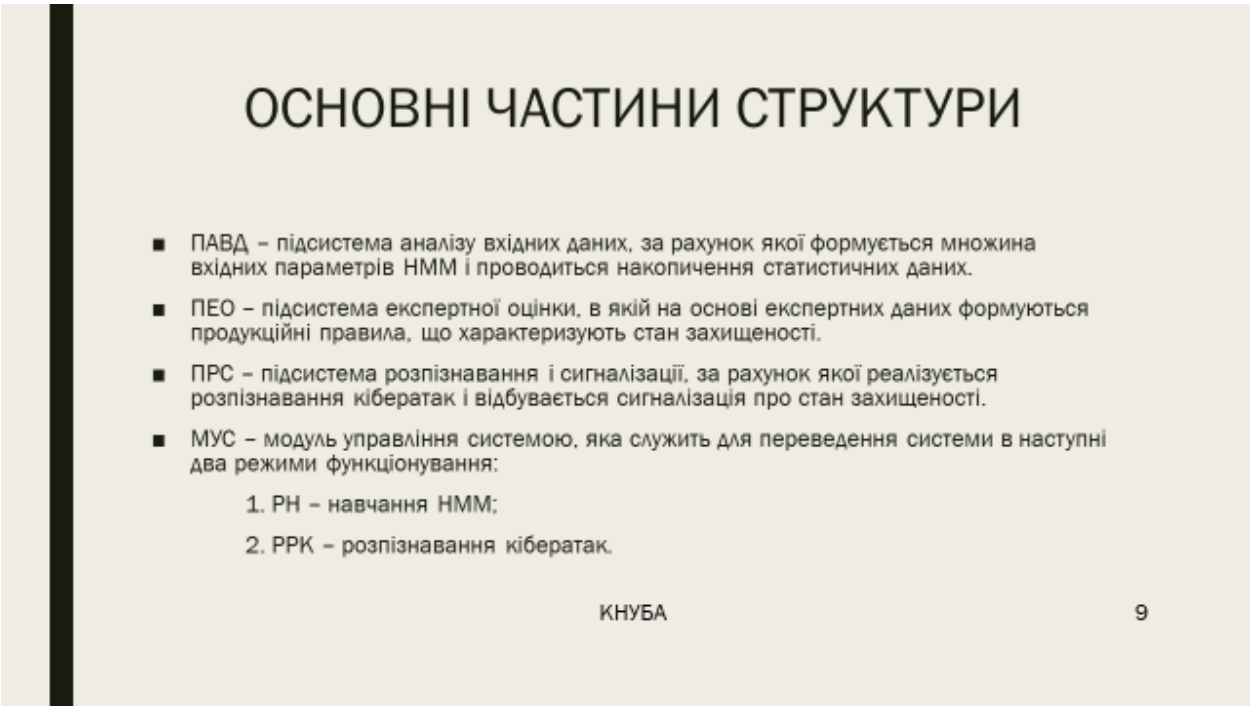

Рисунок 5.9 Основні складові частини структури розпізнавання мережевих кібератак

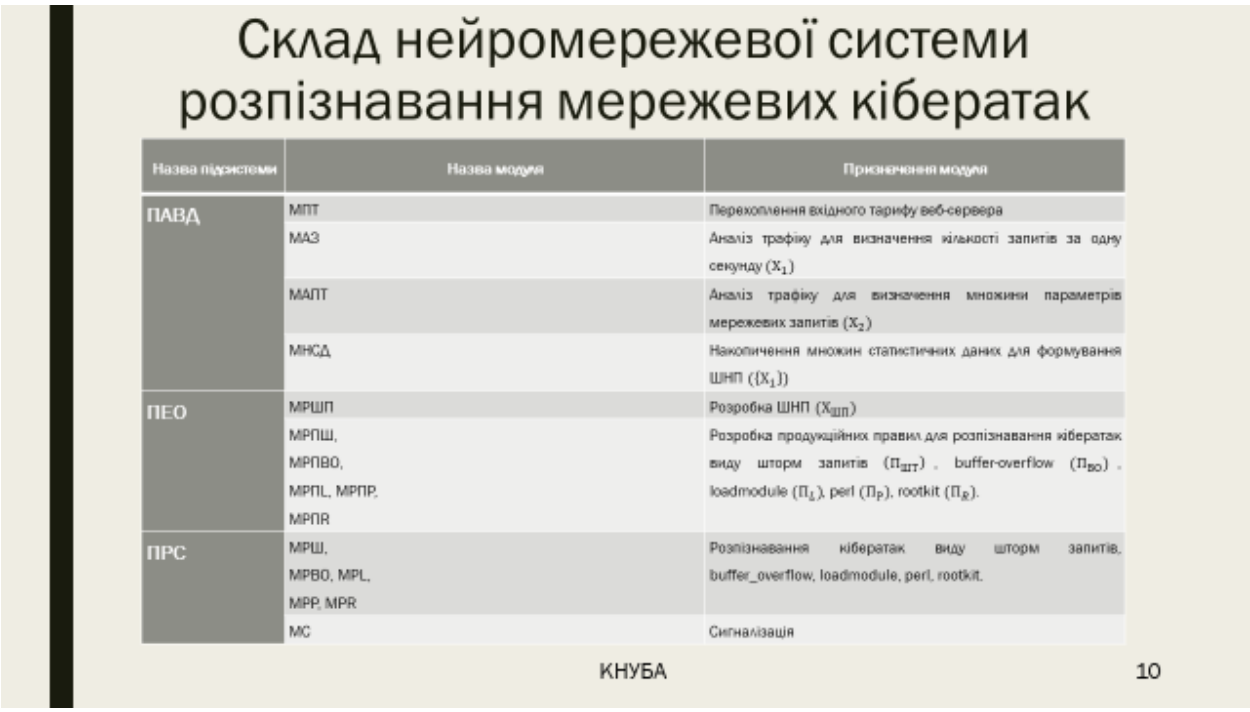

Рисунок 5.10 Склад нейромережевої системи розпізнавання мережевих кібератак

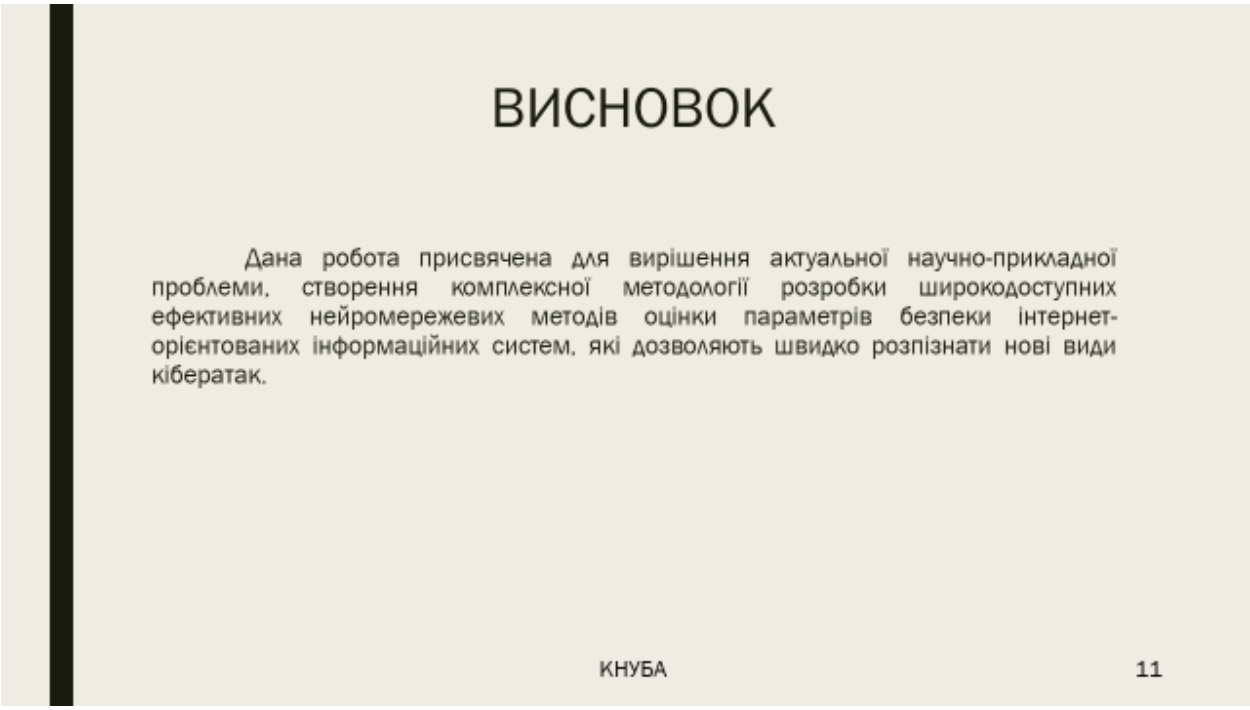

Рисунок 5.11 Висновок

Рисунок 5.12 Фінальний слайд презентації