МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

І.А. Терейковський,
А.О. Корченко

ІНТЕЛЕКТУАЛІЗОВАНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ: НЕЙРОННІ МЕРЕЖІ В ЗАХИСТІ ІНФОРМАЦІЇ

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавр
за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи»
спеціальності 123 Комп'ютерна інженерія

Електронне мережне навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2022

Рецензент *Толюпа С. В.* доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київський національний університет імені Тараса Шевченка

Відповідальний редактор *Тарасенко В.П.,* доктор технічних наук, професор

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 1 від 01.09.2022 р.)
за поданням Вченої ради факультету прикладної математики
(протокол № 1 від 01.09.2022 р.)

Навчальний посібник містить матеріали для самостійної роботи здобувачів ступеня бакалавр за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи» спеціальності 123 «Комп'ютерна інженерія» при вивченні розділу «Застосування нейронних мереж в області захисту інформації» з дисципліни «Інтелектуалізовані методи захисту інформації». Також стане у нагоді розробникам програмного забезпечення, аспірантам та студентам технічних спеціальностей.

Реєстр. № НП 22/23-075. Обсяг 8,0 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Перемоги, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АНМ – асоціативна нейронна мережа

АРТ – адаптивна резонансна теорія

БШП – багатошаровий персептрон

ВШ – вхідний шар нейронів

ДШП – двохшаровий персептрон

ІС – інформаційна система

ЗЗІ – засоби захисту інформації

ЛМ – ланцюг Маркова

НК – неочікувана кібератака

НМ – нейронна мережа

НМЗ – нейромережевих засіб

НММ – нейромережева модель

ПБ – параметр безпеки

ПЗ – програмне забезпечення

ПК – поступова кібератака

РІС – ресурс інформаційної системи

РБФ – нейронна мережа з радіальними базисними функціями

СВА – система виявлення атак

СВВ – система виявлення вразливостей

СЗІ – система захисту інформації

СНМ – семантична нейронна мережа

СШН – схований шар нейронів

ТК – топографічна карта Кохонена

ША – шаблон атаки

ШВ – вихідний шар нейронів

ШД – шар додавання

ШНП – шаблон нормальної поведінки

ШО – шар образів

ШП – шаблон поведінки

ШПЗ – шкідливе програмне забезпечення

ШФ – шар фільтрації

ВСТУП

Сучасний стан розвитку вітчизняних інформаційних систем (ІС), інтегрованих у глобальну мережу Інтернет, характеризується підвищеним рівнем вимог до безпеки інформації, який вже складно забезпечити за допомогою систем захисту, у підсистемах контролю та управління яких використовуються винятково класичні методи оцінювання параметрів безпеки (ПБ). Водночас, у різних галузях науки і техніки становлять методи та моделі теорії нейронних мереж (НМ). Популярність НМ можна пояснити доведеною ефективністю їх застосування в задачах класифікації та кластеризації образів, апроксимації функцій, прогнозування, оптимізації, управління, створення інформаційно-обчислювальних систем з асоціативною пам'яттю, які частково або в комплексі доводиться розв’язувати при оцінюванні ПБ для виявлення кібератак. На тепер відомі спроби використання НМ у різноманітних комерційних та вільнодоступних системах захисту інформації (СЗІ). Так, НМ використовуються для розпізнавання кібератак у міжмережевих екранах компанії Cisco та д розпізнавання вірусів в антивірусах Norton Antivirus виробництва корпорації Symantec і F-Prot виробництва компанії CYREN GlobalView Security Lab. За допомогою НМ визначаються також DDOS-атаки в вільнопоширюваному модулі, призначеному для інтегрування в програмний комплекс Snort. Крім того, компанією Facebook задекларовано використання нейромережевих засобів (НМЗ) розпізнавання спама. Ці засоби набули певного поширення в СЗІ вітчизняних ІС, однак високий рівень помилкових спрацювань, необхідність використання потужного апаратного забезпечення, тривалість та складність пристосування до нових видів кібератак та умов застосування значно обмежують їх практичну цінність. Недоліком поширених закордонних комерційних НМЗ розпізнавання кібератак є висока вартість та відсутність детальної науково-технічної документації.

Питанням розроблення нейромережевих моделей та методів параметричного оцінювання стану ІС у різний час займалися такі вчені, як Є. Бодянський, Д. Деннінг, О. Додонов, О. Корченко, О. Петров, О. Резнік, О.

Руденко, С. Форестер, В. Харченко, В. Хорошко та ін. Однак у галузі захисту інформації побудова таких моделей та методів грунтується на різнорідних підходах, вони мають точковий характер застосування та практично не взаємопов'язані, що ускладнює їх використання для створення ефективних систем розпізнавання кібератак.

Таким чином, посилення вимог до ефективності систем розпізнавання кібератак на ресурси інтернет-орієнтованих інформаційних систем, перспективність використання НМЗ оцінювання параметрів безпеки для розпізнавання кібератак, малодоступність практичного аспекту захисту інформації для науково-критичного аналізу внаслідок широкого використання розробок рівня ноу-хау, недостатня взаємопов'язаність відомих нейромережевих методів та засобів оцінювання параметрів безпеки, невідповідність їх характеристик до змін умов застосування, нових видів кібератак та можливості функціонування за обмежених обчислювальних ресурсів обумовлюють актуальність обраної науково-прикладної проблеми – створення методології розроблення широкодоступних ефективних НМЗ оцінювання параметрів безпекиі-орієнтованих інформаційних систем, які на основі теоретично обґрунтованого вибору характеристик дозволяють оперативно розпізнавати нові види кібератак за обмежених обчислювальних ресурсах та варіативності умов застосування.

Автори вислювлюють вдячність рецензентам за слушні зауваження та поради, які сприяли підвищенню якості зміст увидання. Сподіваємось, що ця книга допоможе в процесі проектування, розроблення, тестування і впровадження в експлуатацію новітніх нейромережевих методів та засобів розпізнавання кібератак.

Розділ 1. СУЧАСНИЙ СТАН ОЦІНЮВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ІНТЕРНЕТ-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

1.1. Характеристика задач оцінювання параметрів безпеки інтернет-орієнтованих інформаційних систем

Однією з основних ознак розвитку сучасного суспільства є подальше зростання залежності від якості й надійності комп'ютеризованих ІС, що застосовуються в різноманітних галузях людської діяльності. Відповідне посилення стратегічної спрямованості інформаційних ресурсів зумовлює необхідність підвищення вимог до рівня їх інформаційної безпеки. Проблема ускладнюється тим, що особливості найбільшої глобальної мережі Інтернет, з якою інтегровано більшість ІС, і використання загальнодоступного програмного забезпечення призводять до нагромадження випадкових і непередбачених негативних впливів на вказані системи. Зазначимо, що Інтернет-орієнтація ІС розглядається в ракурсі необхідності захисту ресурсів таких систем від кібератак у процесі реалізації базових технологічних процесів отримання, зберігання, транспортування, оброблення та подання інформації. При цьому під поняттям кібератак будемо розуміти реалізацію у кібернетичному просторі загроз безпеці його компонентів (конфіденційності, цілісності та доступності) з урахуванням їх вразливостей [34]. Водночас кіберпростір – це віртуальний простір, створений у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій для підтримання та керування процесами перетворення інформації з метою забезпечення інформаційних потреб суспільства [34].

У загальному випадку під поняттям «інформаційна безпека» розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через неповноту, невчасність та

недостовірність інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [16, 224]. Водночас під поняттям безпеки інформації розуміють стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації. Під поняттям захисту інформації в інформаційних системах розуміють діяльність, яка спрямована на забезпечення безпеки оброблюваної в ІС інформації та ІС загалом, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також зменшити потенційні збитки внаслідок реалізації загроз.

У праці [214] з позиції спричинення недоліків та деструктивних впливів від інформаційної безпеки викоремулюють функціональну. При цьому у визначенні функціональної безпеки акцент ставиться на правильності функціонування і вважається, що вона в основному пов’язана з ненавмисне реалізованими деструктивними факторами; помилки мають випадковий характер, а еталонний стан об'єкта, відхилення від якого вказує на помилку – відомий. Однак складність та багатофакторність процесів функціонування ресурсів сучасних Інтернет-орієнтованих ІС в більшості випадків вказують на неможливість окремого оцінювання параметрів функціональної та інформаційної безпеки.

Підтверджується висновок про недоцільність відокремлення параметрів оцінювання також у праці [44], у якій стверджується, що рівень функціональної безпеки системного засобу визначається рівнем адекватного співвіднесення набору механізмів захисту з умовами конкретного використання і тим самим коректності реалізації цих механізмів. При цьому зазначається, що як недостатність механізмів захисту, так і некоректність їх реалізації визначають вразливість системних засобів. Поділ дестабілізуючих факторів на навмисні та випадкові не передбачається. Крім того, у [124] використано визначення інформаційної безпеки, яке включає захист інформації від випадкових або

навмисних впливів штучного або природного характеру.

У закордонних публікаціях, присвячених оцінюванню безпечності інформаційних технологій [254, 257], містяться вимоги до функціональних вимог безпеки. Тому, незважаючи на деяку неоднозначність сучасної термінології, можна вважати, що процедура оцінювання ПБ ІС зводиться до визначення величин параметрів безпеки, що свідчать про наявність/відсутність кібератак. Під поняттям множини параметрів безпеки будемо розуміти множина параметрів, які відображають стан безпеки об'єктів захисту ІС. У загальному випадку множина ПБ інтерент-орієнтоваих ІС формується на основі аналізу:

– параметрів вхідних та вихідних мережевих з'єднань за різноманітними протоколамии;

– потенційно небезпечного програмного коду, який передається в ІС;

– параметрів, що відображають функціонування системного та прикладного програмного забезпечення ІС;

– функціональних параметрів апаратного забезпечення ІС;

– параметрів, що характеризують зміст інформації, яка передається в ІС.

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

Проведемо декомпозицію проблеми оцінювання ПБ інтернет-орієнтованих ІС для розпізнавання кібератак. Зазначимо, що акцент ставиться на ІС загального призначення, які здебільшого використовуються у сферах організаційного управління, промисловості та економіки. Відповідно до праць [1, 2, 44], характерними властивостями інтернет-орієнтованих ІС є:

– підтримання типових інтернет-сервісів (веб-сайту, електронної пошти),

– складність опису (досить велика кількість функцій, процесів, елементів

даних і складні взаємозв'язки між ними);

– різнорідність методів та моделей, використаних для побудови її компонентів;

– наявність сукупності тісно взаємодійних компонентів (підсистем), що мають свої локальні завдання і цілі функціонування (наприклад, традиційних додатків), пов'язаних з обробленням транзакцій і розв’язанням регламентних задач, і додатків аналітичного оброблення (підтримання 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 новоствореного програмного забезпечення;

– використання програмного забезпечення, створеного роз'єднаними і різнорідними групами розробників з різним рівнем кваліфікації і традиціями використання тих або інших інструментальних засобів;

– використання програмного забезпечення, яке в багатьох випадках не має офіційного підтримання і містить потенційну загрозу безпеці через помилки, та люки, які можуть проявлятись тільки в певних умовах експлуатації;

– широке використання в програмному забезпеченні архітектури розподілених об’єктів;

– складності адміністрування як у штатних умовах експлуатації, так і при модифікації програмного забезпечення;

– формування управлінських рекомендацій щодо оброблення великих обсягів різнорідної інформації;

– необхідність постійної актуалізації інформаційних ресурсів;

– тісна інтегрованість з іншими інтернет-орієнтованими ІС, деякі з яких містять в собі потенційні загрози як навмисного, так і ненавмиснго характеру;

– тісна взаємодія із зовнішнім інтернет-середовищем, яке включає велику

кількість інформаційно-програмних деструктивних засобів;

– стандартизація та уніфікація процедур взаємодії між різними функціональними блоками ІС;

– інтелектуалізація процедур оброблення даних, що значно ускладнює оцінювання керувальних сигналів ІС;

– адаптованість до користувачів з різної кваліфікації, що значно знижує ефективність захисту від деструктивних впливів;

– взаємодія з віддаленими користувачами;

– децентралізованість керування як системою захисту, так і всією ІС, що в багатьох випадках зумовлює запізнення та зниження ефективності управлінських впливів.

Простір означених властивостей показано на рис. 1.1, а їх аналіз дозволяє стверджувати, що основними факторами, які визначають особливості оцінювання ПБ вітчизняних інтернет-орієнтованих ІС, є такі:

– складність розпізнавання кібератак унаслідок труднощів, зумовлених встановленням безпосереднього 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 чітко вираженої кібератаки, високої різноваріантності кібератак;

– виникнення нових видів кібератак унаслідок постійного вдосконалення методів та засобів здійснення кібератак, використання нових Інтернет-сервісів [1, 19, 61];

– необхідність функціонування за обмежених обчислювальних ресурсів, зумовлених використанням бюджетного апаратного забезпечення та розташування на одній апаратній платформі інтернет-серверів разом із СЗІ [2, 63, 66, 108];

– варіативність умов застосування, що обумовлюється реконфігурацією ІС, зміною програмно-апаратного забезпечення об’єктів ІС, модифікацією

Інтернет-сервісів, кваліфікацією адміністративного персоналу та ін.

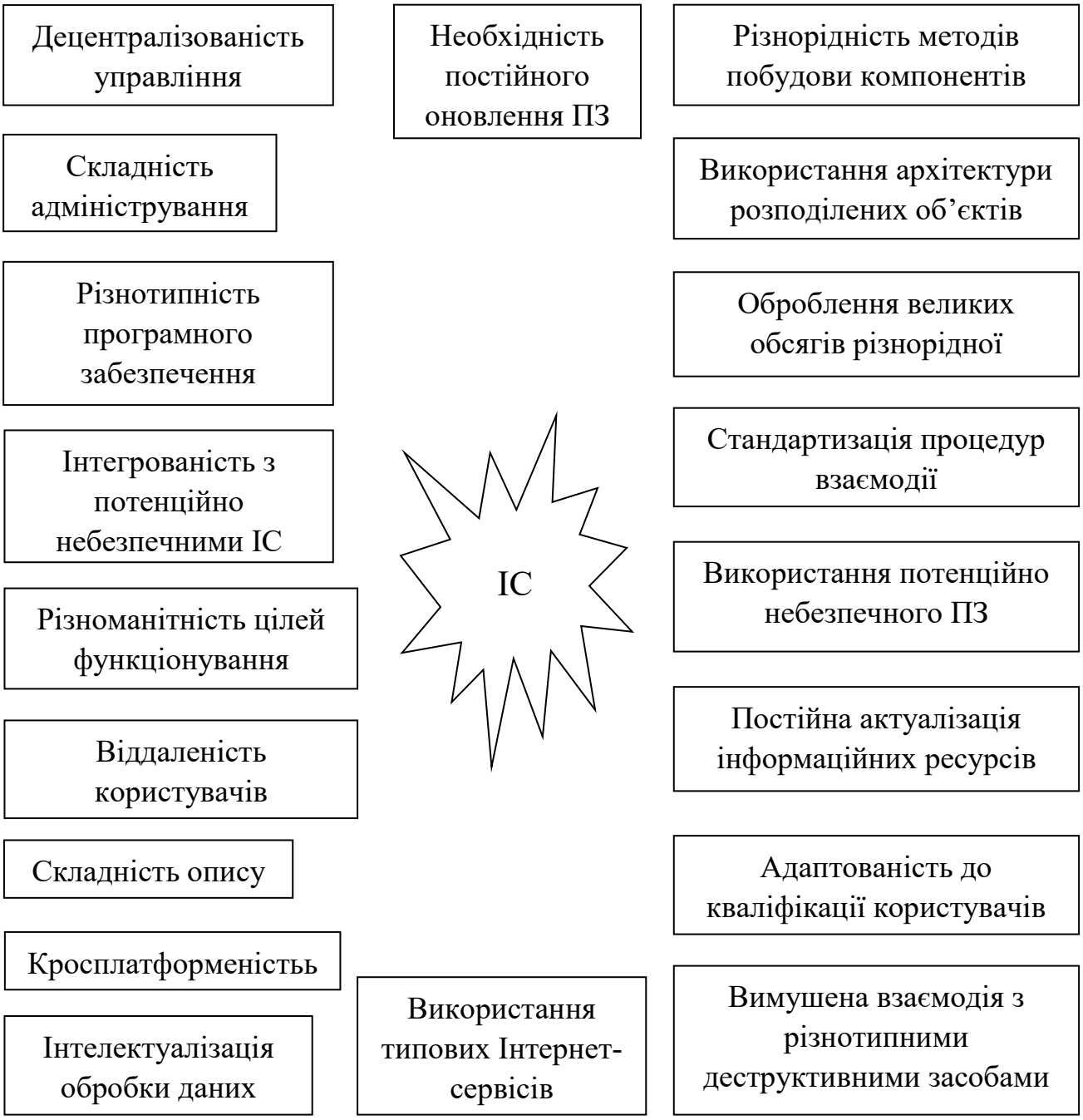

Рис. 1.1. Властивості інтернет-орієнтованих ІС

Результати праць [77, 78, 82] указують на те, що типові порушення захищеності інтернет-орієнтованих ІС спричинені деструктивним впливом:

– шкідливого програмого забезпечення (ШПЗ), розміщеного на веб-сторінках;

– ШПЗ, яке розповсюджується за допомогою електронної пошти;

– витоків текстової інформації з використанням засобів електронної

пошти;

– нецільових електронних листів (спаму);

– віддалених мережевих кібератак на інтернет-сервери.

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

У працях [12-14, 64, 88. 92] наголошується на необхідності захисту від деструктивних впливів за допомогою спеціалізованих програмних засобів захисту, функціонування яких потребує оцінювання ПБ. Найбільш важливі для інтернет-орієнтованих ІС засобів захисту показано на рис. 1.2.

Перелік основних причин порушення захисту ІС добре співвідноситься з переліком найбільш актуальних, не вирішених завдань оцінювання ПБ – розпізнавання віддалених мережевих кібератак на ІС [37, 55, 76, 88, 115], розпізнавання ШПЗ [11, 12, 13, 19, 25, 106, 109, 111] та класифікації електронних листів для розпізнавання спаму та витоків інформації [25, 193, 214, 270].

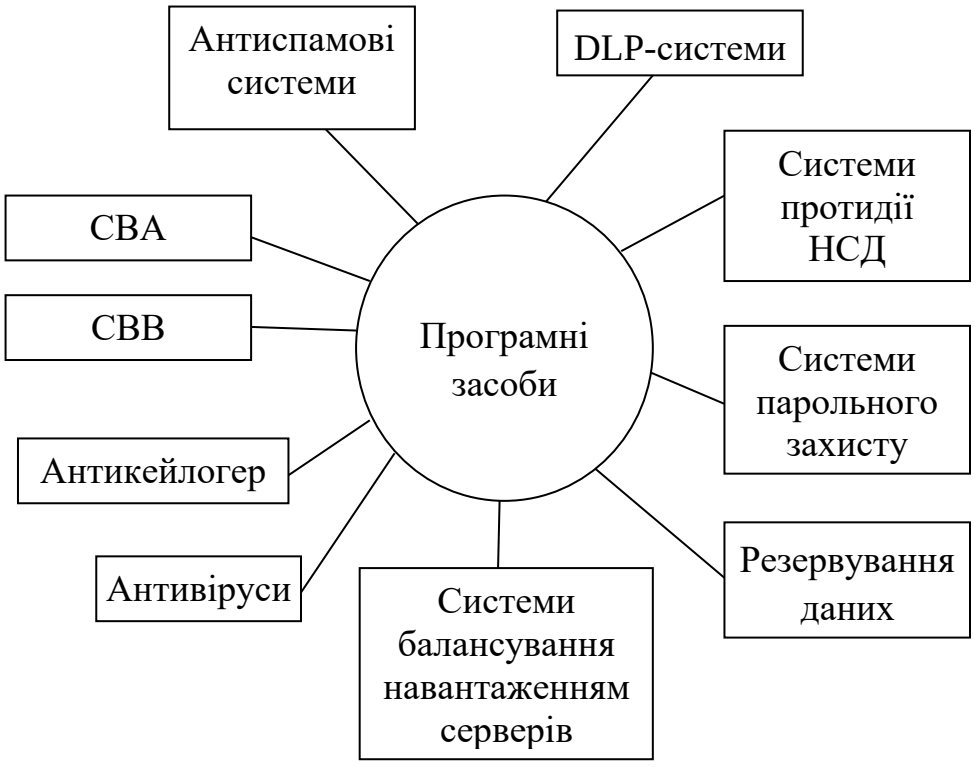

Рис. 1.2. Програмні засоби захисту за допомогою яких оцінюються ПБ

У наведених вище працях вирішувати вказані завдання пропонується через розроблення відповідних моделей моніторингу ПБ. При цьому вказується на обмеженість перспектив застосування моделей, у яких використовуються чіткі алгоритмічні правила прийняття рішень. Тому, на погляд авторів, що збігається з результатами [72, 101, 124, 125, 140, 228, 229, 231, 232], створювати методи та моделі оцінювання ПБ для розпізнавання кібератак слід на основі застосування методів теорії штучних НМ, які довели свою ефективність при розв'язанні подібних економічних, фінансових і технічних завдань. Для окреслення напрямів досліджень деталізовано актуальні завдання оцінювання ПБ для розпізнавання кібератак. Проаналізовано задачі розпізнавання мережевих кібератак, ШПЗ та спаму і витоків текстової інформації серед листів електронної пошти.

Розпізнавання мережевих кібератак. Відповідно до праці [93], під поняттям «мережева кібератака» будемо розуміти кібератаку, реалізація якої пов’язана з деструктивним впливом, здійснбваним мережевими каналами в зв’язку. Для розпізнавання мережевих кібератак використовуються СВА – комплекс засобів, призначених для моніторингу подій, що відбуваються в ІС, для подальшого аналізу з метою визначення ознак порушення безпеки об'єкта моніторингу [7, 16, 21, 22, 37, 76, 85, 115, 125, 228]. Для прийняття рішень у СВА використовуються два основних методи – визначення аномалій та визначення зловживань. Робота аналізатора для визначення аномалії грунтується на припущенні, що ознакою атаки є відхилення поточних значень ПБ від ШНП. Для визначення ШНП застосовуються статистичні моделі [89]. В деяких СВА формується комплексний показник аномалій; для визначення взаємозв'язків між його складовими використовуються коваріаційні матриці. Також застосовується 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 [104]. Як недолік слід

визначити високий рівень помилкових спрацювань, здебільшого через недосконалость моделей ШНП, які не дозволяють з достатньою точністю визначити прогнозовані величини ПБ [109]. Системи виявлення атак, що використовують метод визначення зловживань аналізують послідовність подій, пов'язаних з діяльністю об'єкта захисту і порівнюють їх зі зразками відомих атак. Такі зразки називають шаблогом атаки (ША), а сам метод полягає у визначенні атак на основі сигнатур. Через не повноту інформації та наявность шумів при реєстрації ПБ труднощі становить задача розрахунку відповідності ША реальним подіям, що стосуються об'єкта захисту. Для розв’язання цієї задачі застосовуються різноманітні методи – експертний, аналізу переходів, моделювання атак. У разі застосування експертного методу відомі кібератаки описуються у вигляді деякого набору правил, виконання яких сигналізує про реалізацію кібератак. Метод аналізу переходів передбачає подання мережевої кібератаки у вигляді послідовності переходів об'єктів захисту із одного стану в інший [119]. У разі застосування методу моделювання кібератак попередньо сформовані послідовності подій, характерні для реалізації кібератаки, порівнюються з поточними показниками, і формується висновок про ймовірність здійснення кібератаки. Часто використовуються статистичні моделі зміни ПБ ІС під час кібератаки. У цілому метод визначення зловживань дає змогу досить ефективно виявляти кібератаки відомих типів при низькому показнику хибних спрацювань, але не дозволяє виявити кібератаку, зразок якої не відомий. Важливим і досі не вирішенм завданням є формування ША. Загалом шаблон нормальної поведінки та ША називають шаблоном поведінки (ШП). Хоча розробленню ШП присвячено багато праць [7, 16, 37, 55, 85, 115, 124, 125, 133], але практичний досвід та результати [118, 121] вказують на те, що ці шаблони не достатньо адаптовані до типової динаміки ПБ інтернет-орієнтованих ІС, яка здебільшого не може бути адекватно описана за допомогою однорідних моделей. На підтвердження такої гіпотези на основі [96, 133] та статистичних даних, зібраних авторами, проаналізовано ряд типових

випадків процесу зміни ПБ об’єктів захисту інтернет-орієнтованих ІС. Так, на рис. 1.3, 1.4 показано наведені в [133] графіки зміни кількості TCP/IP пакетів [133], отриманих веб-сервером. Аналіз цих графіків показує, що за нормальних умов експлуатації екстремальні кількості запитів, які надходять до веб-сервера, значно відрізняються від середніх значень. У загальному випадку максимальні значення у 5-10 разів перевищують середні. Прослідковується також певна циклічність процесу зміни кількості запитів, що однією особливістю процесу є те, що відбувається в декількох масштабах часу. Аналіз рис. 1.4 показує наявність флуктації трафіку за невеликих вікон спостережень (1–60 с.), у межах яких кількість переглядів сторінок та відвідувачів веб-сайта не змінюється.

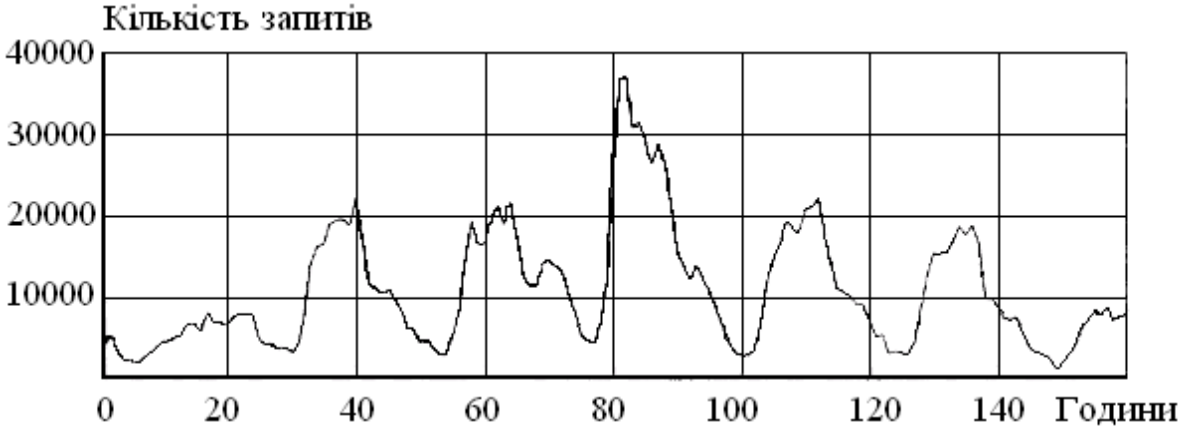

Рис. 1.3. Зміна кількості запитів за вікон спостережень 1 год

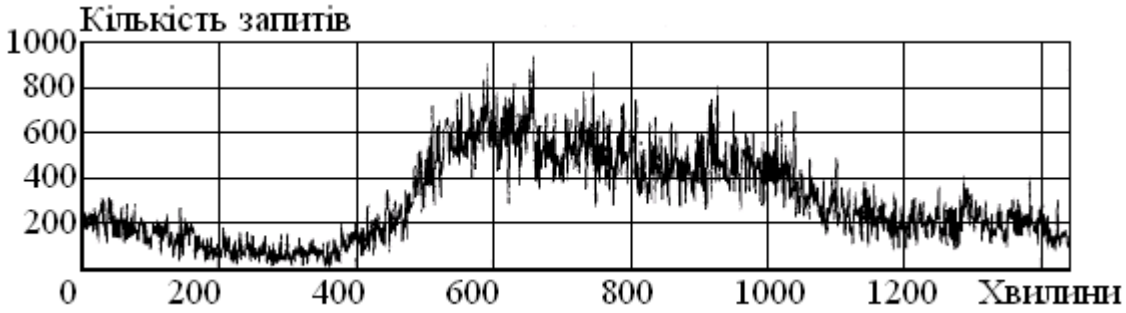

Рис. 1.4. Зміна кількості запитів за вікон спостережень 1 хвилина

Цей факт зумовлений тим, що типова веб-сторінка значно більша від максимального розміру мережевого пакета. Тому одиночний запит веб-сторінки спричиняж стрімке, короткочасне зростання кількості мережевих пакетів [129]. Досить схожі результати, отримано і в статті [92]. На відміну від [129] у цій

роботі наведено зміну обсягів вхідного та вихідного мережевих трафіків комп'ютера-сервера корпоративної ІС, який забезпечував не тільки функціонування веб-сервера, але й сервера баз даних, файлового сервера та сервера друку. У праці [96] доведено автомодельність процесу зміни трафіку з коефіцієнтом самоподібності 0,7 – 0,85. Показано наявність циклічного ефекту для різних часових діапазонів, що збігається з результатами [129]. Зазначимо, що статистичні дані зібрано за допомогою спеціалізованих програм [96]. Такий підхід доцільний при застосуванні в експериментальних дослідженнях, але не завжди прийнятний на практиці через організаційні обмеження та збільшення використання обчислювальних ресурсів комп'ютера-сервера. Крім того, статистика не містить інформації про багато параметрів, широко використовуваних у ШП, наприклад, про кількість звернень до веб-сервера з однієї IP-адреси (хости). Для усунення цих недоліків зібрано та проаналізовано статистичні дані функціонування веб-серверу, що забезпечував доступ до інформаційного сайту кредитної установи. Веб-сервер розміщувався на окремому комп'ютері та був з'єднаний з мережею Інтернет виділеним каналом. Статистичні дані отримано за допомогою аналізу log-файлів веб-сервера та лічильника відвідувань, розміщеного на всіх сторінках сайта. Мінімальний інтервал спостережень – 1 с. Термін спостережень становить 1 рік 2 місяці. Графік динаміки переглядів веб-сторінок протягом доби показано на рис. 1.5.

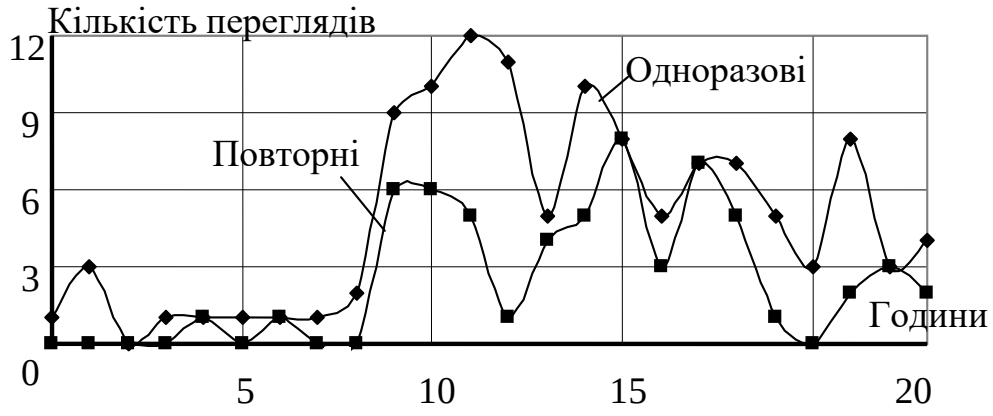

Рис. 1.5. Динаміка одноразових та повторних переглядів веб-сторінок

Аналіз рис. 1.5 підтверджує наявність циклічності у випадкових

процесах, пов'язаних з переглядом користувачами сторінок веб-сайту. Таким чином, доведено, що зміна більшості параметрів ШП для інтерент-орієнтованих ІС має циклічний характер на різних часових інтервалах. Для врахування циклічності мережевого трафіку в заданому інтервалі спостережень пропонуються відносно прості лінійні моделі, у яких флуктація описується за допомогою двох допоміжних коефіцієнтів [96, 133]. Перший коефіцієнт розраховується як відношення максимально зафіксованої вхідної інтенсивності запитів до середньої інтенсивності запитів протягом заданого інтервалу спостережень. Другий коефіцієнт розраховується як відношення часу, протягом якого миттєва вхідна інтенсивність запитів перевищувала середню інтенсивність, до загального терміну спостережень. Відзначено низьку точність таких моделей; їх рекомендується використовувати лише для приблизних розрахунків. Зроблено спробу створення моделі динаміки трафіку з різними степенями самоподібності. Однак запропонована модель дозволяє лише розраховувати коефіцієнти самоподібності процесу лише з одним циклом. Крім того, не показано можливості безпосереднього моделювання динаміки процесу. Тому доцільність її застосування у ШП викликає сумніви. Водночас, спільний висновок [96, 133,252] полягає в неадекватності пуасонівської моделі динаміки більшості функціональних параметрів. Указані причини підтверджують актуальність та важливість удосконалення ШП, яке можливе завдяки використанню апарату марковської апроксимації, що широко застосовується для прогнозування діагностичних параметрів задач технічних систем [8, 9, 18, 99, 138, 144, 172, 206]. У літературі не наведено методів побудови марковських моделей ШП ПБ, які б адекватно враховували типові статистичні залежності ПБ Інтернет-орієнтованих ІС і могли б бути використані для навчання нейромережевих моделей (НММ), призначених для розпізнавання мережевих кібератак. При цьому марковські моделі мають бути неоднорідними, а для визначення перехідних точок необхідно враховувати можливу циклічність процесу на різних часових інтервалах. На наш погляд, що збігається з

висновками [235], врахувати циклічність процесу доцільно за допомогою добре апробованого методу Фур'є спектрального аналізу даних.

Розпізнавання шкідливого програмного забезпечення. Відповідно до статті [96], шкідливим будемо називати будь-яке програмне забезпечення (ПЗ), яке може заподіяти шкоду ІС. За останні декілька років саме ШПЗ стало однією з основних причин порушень захищеності ІС [11, 12, 13, 19, 25, 109, 111, 129, 225]. При цьому для більшості інтернет-орієнтованих ІС характерним є організація електронного документообігу за адміністративного обмеження повноважень користувачів на інсталяцію ПЗ та доступу до файлів. У; цьому випадку ймовірними шляхами зараження є використання листів електронної пошти, офісних документів та перегляд веб-сайтів. Для вказаних ресурсів ШПЗ, як правило, розроблюється за допомогою скриптових мов програмування. Таким чином, ШПЗ, створене за допомогою скриптових мов програмування, є однією з основних загроз інформаційній безпеці ІС [96, 113]. Зазначимо, що до скриптового ШПЗ також належать шкідливі макроси, які використовують можливості макромов, убудованих в системи оброблення даних. Найбільш поширені макровіруси та макротрояни, написані мовою VBA і пристосовані для функціонування в середовищах MS Office, AutoCAD, 1С «Предприятие» та 1С «Бухгалтерия». Крім того, у сучасних версіях операційних систем (ОС) Windows вбудовано скриптовий інтерпретатор Windows Scripting Host, який дозволяє виконувати скрипти (макроси), написані мовами VBScript та JScript. Запускати макрос може користувач при відкритті файлу. Ця особливість використовується для активізації скриптових вірусів та троянів, що розповсюджуються у вигляді файлів, прикріплених до листів електронної пошти. Результати [54, 101, 177, 189, 191, 192, 194, 200, 229] показують, що більшість поштових вірусів та троянів функціонують в середовищі інтерпретатора WScript і написані мовою програмування VBScript. Тому більшість поштових вірусів і троянів не відрізняється від макровірусів та макротроянів MS Office. Шкідкливе програмне забезпечення, призначене для

заподіяння шкоди під час перегляду веб-сайтів, має певні відмінності. Воно вбудоване у веб-сторінку і виконується в середовищі браузеру. Для створення такого ШПЗ використовуються мови програмування: Java, C++, VBA, JavaScript, JScript, VBScript та ActiveScript. Для захисту від скриптового ШПЗ використовуються переважно антивірусні сканери та поведінкові аналізатори. Найчастіше для виявлення ШПЗ застосовується метод пошуку сигнатур. Особливістю пошуку сигнатур скриптового ШПЗ є те, що сканер може аналізувати програмний код скрипту в текстовому вигляді. Порівняно зі стандартними файловими вірусами означена особливість значно спрощує роботу сканера і дозволяє аналізувати функціональність макроса. Однак найбільш поширений метод пошуку сигнатур дає змогу розпізнавати тільки відоме ШПЗ і відкриває шлях для обходу антивірусного захисту поліморфному та зашифрованому (обфусифікованому) ШПЗ. Іншими важливими недоліками методу сигнатур є відносно низька швидкість пошуку всіх видів ШПЗ та необхідність постійного оновлення бази сигнатур. Крім того, у більшості антивірусних сканерів задекларовано використання евристичних методів пошуку ШПЗ, реалізація яких не документується. Проте аналіз праць [1, 19, 62, 82] показує те, що в більшості випадків базою цих методів є статистичний аналіз послідовності виконання програмного коду об'єкта, який перевіряється. Відзначимо, що навіть за явно завищеними рекламними заявами розробників сучасні евристичні методи дозволяють виявити лише близько 50% ШПЗ з невідомою сигнатурою. Що стосується поведінкових аналізаторів, то вони досить вузько застосовуються на практиці, оскільки більшість дій, характерних для ШПЗ, можуть виконуватися і звичайними програмами. Ще одним засобом захисту від скрипового ШПЗ є модулі блокування скриптів (макросів), що входять до складу СЗІ офісних пакетів та браузерів. Однак їх широкому застосуванню перешкоджає значна складність їх оперативного налаштування та значне обмеження функціональних можливостей використання офісних документів і веб-сторінок. Наприклад, блокування браузером спливаючих вікон

значно спотворює інформацію веб-сторінки, а дозвіл їх перегляду є прогалиною в захисті. Отже, задача розпізнавання скриптового ШПЗ залишається не розв’язана, що підтверджується незалежним тестуванням антивірусних засобів [121, 122].

Розпізнавання спаму та витоків текстової інформації серед листів електронної пошти. Електронна пошта є одним із найпоширеніших та важливих сервісів сучасних ІС. Натепер вважається, що ефективність та безпечність функціонування електронної пошти в основному визначається рівнем захисту від спаму та від витоків інформації [194]. Під терміном «спам» розуміють масово розповсюджувані листи, зміст яких має рекламний або шахрайський характер. В сучасних умовах розсилання спама – це надто прибутковий бізнес, підкріплений відповідним ринком і стабільним попитом. У російськомовній зоні Інтернету обсяг спама становить близько 70–90% від загального обсягу всієї електронної пошти [193, 270]. Програмно-технічні методи боротьби зі спамом функціонують за принципом розпізнавання – блокування (знищення) спама [250]. Основною проблемою є класифікація отриманих листів на цільові та спам. Проаналізуємо особливості сучасних методів класифікації електронних листів.

Метод чорного, білого і сірого списків. Базою методу є аналіз зворотної адреси відправника листа. Основний недолік методу полягає в тому, що адреса не обов'язково вказує на джерело спама. Наприклад, спам-лист може надійти з динамічної IP-адреси, або розсилання здійснена без відома власника адреси. Використання сірого списку доцільне лише за невеликого обсягу листування з обмеженим колом осіб. У противному випадку ведення сірого списку потребує великих затрат на переконфігурацію. Крім того, сучасні спам-засоби дозволяють генерувати підтвердження відправлення спам-листа.

Метод фіксації масових розсилань електронних листів. Листи класифікуються як спам, якщо обсяг відправки пошти з однієї адреси (з однієї підмережі) за короткий термін часу перевищує граничну величину. Недоліками

методу є необхідність контролю за всім простором поштових відправлень Інтернет та неефективність за невеликих спам-розсилань.

Технологія верифікації відправника Sender Permitted From. Адміністратор домену публікує дані, які описують можливі джерела електронної пошти з адресами відправника з цього домену. Опубліковані дані називаються SPF-записом або SPF-політикою. Приймальний поштовий сервер класифікує спам на основі порівняння адреси відправника з SPF-записом. Однак спамер може самостійно зареєструвати велику кількість доменів з коректними SPF-записами і розсилати спам з цих доменів. Спамери можуть використовувати безкоштовні домени третього і більших рівнів. Крім того, підтримання SPF зумовлює великі обчислювальні витрати системи пересання електронної пошти. Метод розпізнавання спама за ключовими словами (словосполученнями), які визначаються користувачем у вигляді набору правил. Метод метод не знайшов широкого застосування через складності при формуванні вказаних правил.

Метод байєсовської фільтрації. Кожному слову або тегу, що використовується в електронній переписці, присвоюються два значення: імовірність його наявності в спамі та ймовірність його наявності у звичайних листах. Для кожного нового листа за допомогою формули Байєса розраховується загальна спам-оцінка листа. Якщо величина спам-оцінки більша від граничного значення, то лист класифікується як спам. Ефективність методу безпосередньо залежить від правильності спам-оцінок слів листа. Для цього виконується статистичний аналіз як спама, так і звичайних листів кожного користувача. Таким чином, метод байєсовської фільтрації передбачає деяке запізнення, спричинене нагромадженням кожним користувачем достатнього обсягу статистичного матеріалу. Ще одним недоліком цього методу є висока ймовірность пропуску спама, якщо в листі мало слів з високою спам-оцінкою.

У більшості сучасних антиспамових системах реалізовано комплексні методи захисту, які декларують фільтрацію 98% спама. Однак навіть у найсучасніших поштових службах реакція на новий вид спам-листів становить

20–30 хвилин. При цьому багатьо мільйонів спам-листів розсиляються за 1–2 години. Тому з великою імовірністю поштові служби проведуть неправильну класифікацію спама. Отже, майже всі існуючі системи розпізнавання спама не можуть адекватно реагувати на сучасні методи формування і розповсюдження спам-листів.

Подібною виглядає ситуація захисту електронної пошти від витоків інформації, яка в більшості ІС реалізується за допомогою DLP-систем. Принцип роботи цих систем полягає у сигналізації та/або блокуванні електронних листів, які містять конфіденційні дані. Труднощі виявлення конфіденційної текстової інформації подібні до труднощів розпізнавання спама і полягають в недостатньому врахуванні змісту листів. Усунути цей недолік можна застосуванням НММ, що вже довели свою ефективність у системах оброблення текстової інформації.

1.2. Дослідження нейромережевих моделей та методів оцінювання параметрів безпеки інформаційних систем

Базою дослідження нейромережевих моделей та методів, що застосовуються для оцінювання ПБ ІС, стали праці [1, 4, 7, 15, 19, 37, 48, 58, 59, 86, 87, 100, 111, 134, 146, 199, 212, 247-250, 252]. У більшості проаналізованих праць є певна невідповідність термінологічного аспекту описаної розробки: нейромережевий метод, модель, система, технологія, засіб. Як правило, наводиться комплексний опис розробки, хоча назва праці вказує, наприклад, на створення НММ. У більшості випадків у назвах декларується використання НМ для вирішення певних завдань захисту інформації, наприклад, для розпізнавання мережевих атак. При цьому суть використання НМ зводиться до оцінювання ПБ. Тому ці праці аналізуються з єдиних позицій визначення основних характеристик НММ та методів для оцінювання ПБ. Наведемо отримані дані.

Методи простої та семантичної класифікації мережевих атак. Методи

розроблено в межах нейромережевої технології виявлення мережевих комп'ютерних атак за допомогою програмного комплексу «Snort», описаної у праці [37]. Технологія передбачає застосування двох нейромережевих методів виявлення атак – **простої класифікації (ПСК)** та **семантичної класифікації (ССК)**. Як вхідні параметри використовуються параметри мережевих пакетів транспортного рівня стеку протоколів TCP/IP. У методі ПСК використано БШП з 10 вхідними нейронами та 2 нейронами у вихідному шарі. Для оптимізації кількості схованих нейронів пропонується застосування конструктивних алгоритмів. Наведено вираз для розрахунку корегувальних вагових коефіцієнтів нейронів вихідного шару:

$$\Delta w_{jk}(i) = -\eta(y_n(i) - f(x_i))\varphi'(v_n(i))y_n,$$

де η – коефіцієнт швидкості навчання; n – номер нейрона у вихідному шарі; i – номер навчальної ітерації; v_n – інформаційне поле, отримане на вході функції активації; y_n – вихідний сигнал n-го вихідного нейрона; φ' – похідна функції активації; $f(x_i)$ – бажаний відгук i-го нейрона.

Зазначимо відсутність детального опису процесу оптимізації структури БШП. У методі семантичної класифікації пропонується використання ТК, вибір якої обґрунтовується її невисокою ресурсомісткістю. В обох методах передбачено оброблення вхідних параметрів для зменшення кількості вхідних параметрів НМ.

Метод нейромержевої фільтрації спаму (НФС) [249]. Доводиться оптимальність використання адитивних НМ. Вид НММ обрано з позицій максимізації точності розпізнавання, можливості автоматизації навчання та можливості подання результатів у графічному вигляді. Тобто використано процедуру багатокритеріальної оптимізації процесу визначення архітектури НМ. Як вхідні параметри НММ використано частість вживання в спамі та в цільових електронних листах інформативних слів. Також запропоновано процедуру багатокритеріальної оптимізації параметрів НМ, у якій використано критерії максимізації обчислювальної потужності та мінімізації терміну

навчання.

Метод визначення фрагментів програмного коду (ВФПК) [24]. Метод застосовується для визначення переліку та оцінювання значень вхідних параметрів НМ, що використовуються в системах детектування шкідливого програмного забезпечення. У праці [248] наведено опис та результати експериментів за розпізнавання ШПЗ, проведених за допомогою БШП. Аналіз наведених результатів підтверджує перспективність запропонованого методу. Можна зробити висновок про використання в методі процедури попереднього оброблення вхідних параметрів НМ, яка підвищує їх інформативність.

Нейромережева системи виявлення вторгнень (НСВВ) [250]. Система орієнтована на використання БШП для розпізнавання мережевих атак. Наведено результати експериментів, що підтверджують ефективність системи при розпізнаванні атак, сигнатури яких подані в базі KDD-99. Вибір типу НМ обґрунтовано з позицій максимальної обчислювальної потужності. Проведено однокритеріальну оптимізацію архітектури БШП.

Нейромережевий підхід виявлення SQL-ін'єкцій (НПВІ) [252]. Запропоновано розглядати проблему визначення зловмисних SQL-запитів у вигляді проблеми прогнозування часових рядів. Відповідно до цієї пропозиції пропонується використовувати рекурентні НМ типу Джордана та Елмана. Тобто тип НМ обрано за критерієм апробованості в задачах прогнозування часових рядів. Наведено процедуру попереднього оброблення вхідних параметрів та процедуру однокритеріальної оптимізації структури НМ. Використано критерій максимізації обчислювальної потужності. Наведені результати експериментальних досліджень, проведених на основі даних порталу Php-Nuke, підтверджують перспективність запропонованого підходу.

Бінарний нейромережевий метод (БНМ) [111]. Метод застосовується для виявлення мережевих атак. В основу методу покладено спеціальну бінарну нейронну мережу, яка має дві важливі властивості: 1) модель пристосована для вирішення завдань, у яких вхідна інформація має складну, багатозв'язкову і

навіть фрактальну структуру; 2) метод навчання моделі є безпосередньою обчислювальною процедурою і не зводиться до пошуку глобального екстремуму складної нелінійної функції, що не накладає жодних обмежень на розмірність завдання. Таким чином, у методі передбачено вибір виду НММ за критерієм апробованості в задачах певного типу та за критерієм мінімізації тривалості навчання. На жаль, у праці немає експериментальних даних, що ускладнює порівняльний аналіз. В методі не передбачено проводити оптимізації структури НМ, застосування та процедури оброблення вхідних даних.

Метод виділення мережевих атак із типового мережевого трафіку (ВМА) [100]. Метод застосовується для розпізнавання мережевих атак. Запропоновано застосування БШП з 2 СШН. Вхідний шар нейронів такого БШП складається із 9 нейронів, а ШВ – з 1 нейрона. Зазначено, що вибір БШП з такою структурою зумовлюється вимогами гнучкості та функціональності. Тобто використано багатокритеріальну оптимізацію структури НМ. Указано на попереднє оброблення статистики, що використовувалась для навчальної та тестової вибірок.

Спосіб виявлення DDoS-атак (СВДА) [146]. Запропоновано використання нечітких НМ. Пропозиція ґрунтується на перспективності НМ такого типу. Акцентується розпізнавання DDoS-атаки типу SYN Flood. Для формалізації знань експертів про DDoS-атаки створено 5 лінгвістичних змінних, кожна з яких характеризує одну з компонент вектора параметрів мережевого трафіку, що використовується для формування вхідних параметрів НМ. До вказаних лінгвістичних змінних належать: X_1 – час отримання пакетів; X_2 – відсоток пакетів з різних зовнішніх ір-адрес; X_3 – відсоток пакетів з різних портів; X_4 – відсоток пакетів з пошкодженими заголовками; S – ступінь впевненості. Розроблено предикатні правила вигляду: якщо X_1 = «великий»$\rightarrow$ $Y\rightarrow$ «висока». Запропоновано представити нечіткий класифікатор у вигляді НМ з прямим поширенням сигналу, що навчається за допомогою

модифікованого алгоритму зворотного поширення помилки. Модифікація полягає у пристосуванні класичного алгоритму до нечітких нейронів «І» та «АБО». Таким чином, основною відмінністю способу виявлення DDoS-атак є можливість застосування для навчання НМ експертних знань.

Метод використання нейронної мережі гібридної структури типу CounterPropagation (НМГС) [19, 199]. Метод призначено для виявлення мережевих атак на веб-сервер. Особливістю мережі CounterPropagation є комбінація ТК з БШП. Вхідними даними методу є параметри мережевого трафіку, що передається по протоколах IP, TCP, HTTP, HTTPS, CGI, SQLNet. У методі передбачено процедуру попереднього оброблення вхідних параметрів НМ через подання їх у вигляді графічних образів (піфограм), котрі використовуються в когнітивній графіці. Метою попереднього оброблення є мінімізація розмірності вхідних даних. Графічне зображення визначило необхідність застосування в методі шару Кохонена. Використання персептронного шару обґрунтоване з позицій обчислювальної ефективності. Таким чином, у методі передбачено багатокритеріальну оптимізацію виду та однокритеріальну оптимізацію параметрів НММ. У методі застосовано процедуру оптимізації параметрів навчання НМ, яка дозволяє до 10 разів зменшити величину помилки розпізнавання атак.

Метод побудови сукупного класифікатора трафіку (ПСКТ) [86]. Метод призначений для ієрархічної класифікації комп’ютерних атак на інформаційно-телекомунікаційні мережі. Особливістю ПСКТ є використання математичного методу головних компонент для стиснення статистичних даних, що використовуються як навчальна вибірка НМ. У методі використано об’єднання з 22 нейромережевих детекторів, кожен із яких навчений розпізнавати певний тип атаки, наведений в базі даних KDD-99. Детектор являє собою тришарову НМ з 12 вхідними нейронами та 2 вихідними нейронами, один із яких відповідає за наявність, а другий за відсутність атаки. Як СШН використано шар Кохонена. Зазначимо, що обґрунтування архітектури та

параметрів нейромережевого детектора не наведено. У разі виявлення детектором атаки вихід першого вихідного нейрона дорівнює 1. Для унеможливлення ситуації, коли декілька детекторів одночасно сигналізують про власний тип атаки, на другий вихід кожного з них передається мінімальна евклідова відстань між вхідним образом (вхідними параметрами x_i) і ваговими коефіцієнтами схованих нейронів $w_{i,j}$:

$$E_j = \min_{\text{i}} \sqrt{\left(x_1 - w_{1,j}\right)^2 + \ldots \left(x_{12} - w_{12,j}\right)^2}$$

Надалі класифікується та атака, детектор якої має мінімальну евклідову відстань. У ПСКТ у неявному вигляді передбачено оптимізацію навчання та функціонування нейромережевого детектора.

Нейромережевий підхід до виявлення мережевих атак (ПВМА) на ІС [87]. Акцентується розпізнавання атак, сигнатури яких подані у БД KDD-99. Відповідно до даних цієї БД кількість вхідних параметрів 41. Запропоновано використовувати критерій вибору оптимального НММ у вигляді мінімуму обсягу навчальної вибірки. Аналізуванням літературних джерел визначено, що до допустимих типів належать: ТК, БШП з одним схованим шаром нейронів та РБФ. Зазначено, що для ТК мінімальний обсяг навчальної вибірки L має в 2 рази перевищувати кількість вхідних нейронів n. Тобто $L \geq 2n$. Для БШП та РБФ обсяг навчальної вибірки розраховується так: $L \approx W / \varepsilon$, де W – кількість синаптичних зв'язків; ε – допустима помилка навчання. У праці [12] зроблено спробу визначити оптимальну структуру БШП. Заявлено, що визначена експериментальним шляхом кількість схованих нейронів дорівнює $m = 10$, кількість вихідних нейронів – 2. Відповідно, необхідний обсяг навчальної вибірки ТК становить $L = 82$, а для БШП і РБФ при $\varepsilon = 0{,}1$, $L = (m(n+3)+2)/\varepsilon = 4420$. Тому оптимальним типом нейромережевої моделі обрано ТК. Зазначимо, що правильність розрахованих величин викликає сумніви, оскільки згідно з теорією НМ [17] за заданої точності навчання кількість схованих нейронів БШП безпосередньо залежить від величини

навальної вибірки. Надалі у праці [12] проводиться оптимізація структури ТК. Неявно використано критерій максимізації точності навчання. Також використано аналогічна [12] процедура попереднього оброблення вхідних параметрів.

Адаптивна система виявлення атак (АСВА) [148]. Система призначена для розпізнавання мережевих атак, грунтується на спільній роботі ТК і БШП, що виконують завдання кластеризацію і класифікацію даних. Виявлення атак, що проводиться в декілька етапів, стало можливим завдяки внесенню в базу даних експертної системи інформації про зміни в поведінці конкретного об'єкта протягом деякого відрізка часу. Доводиться, що оптимізація архітектури дозволить підвищити точність та оперативність розпізнавання. Як вхідні дані використано параметри мережевого трафіку по протоколу TCP. Для оброблення вхідних даних застосовано метод ковзного часового вікна. Топографічну карту Кохонена використана для попередньої оброблення даних, що надходять на вхід БШП для їх стиснення та підвищення інформативності. Наведено математичний вираз для розрахунку частоти визначення нейрона в позиції *i,j* в якості нейрона-переможця:

$$\beta_{i,j} = f_{i,j} + \sum_{x=1}^{r}\left(\frac{f_{i-x,j} + f_{i,j-x} + f_{i+x,j} + f_{i,j+x}}{1+x}\right),$$

де $f_{i,j}$ – кількість разів, коли нейрон в позиції *i,j* був нейроном-переможцем; *r* – відстань між центрами кластерів; *x* – довжина вхідного вектора.

Надалі ця частота використовується для визначення центрів та меж кластерів. Структуру БШП оптимізовано щодо відповідності обсягу контрольованих ресурсів.

Нейромережева технологія виявлення та класифікації мережевих атак (ВКМА) [249]. У технології запропоновано використання тришарової НМ, що навчається методом зворотного поширення помилки. Для розпізнавання кожного виду мережевої атаки застосовується окрема НМ.

Як вхідні параметри використовуються параметри мережевого трафіку по

стеку протоколів TCP/IP. Для формування навчальної вибірки пропонується використати базу даних KDD-99.

Наведено словесний опис та фрагменти програмного коду для підготовки вхідних даних із цієї бази даних до виду вхідних параметрів НМ. Однією із цілей підготовки є зменшення обсягу навчальної вибірки НМ. Підходи до оптимізації виду та параметри НММ не описуються.

Система виявлення аномальної поведінки обчислювальних процесів (ВАОП) [7]. Система призначена для виявлення атак на компоненти інформаційної системи, які функціонують на базі мікроядерних операційних систем. Детально розроблено методику збирання та підготовки вхідних параметрів для НМ. Пропонується використовувати ТК і БШП. Опису процедури оптимізації виду та параметрів НММ не наведено.

Модель кібернейрона (МКН) [48]. Модель пропонується використовуватися для розпізнавання комп'ютерних вірусів. Основною відмінністю моделі кібернейрона є відсутність функції активації, замість якої використовується таблиця підстановки, а основною перевагою – потенційно висока обчислювальна потужність. Розроблені алгоритми навчання кібернейрона. Як вхідні параметри використовуються або фрагменти піддослідного файлу, або хеш-коди цих фрагментів. Їх визначення пропонується реалізувати методом ковзногоо вікна. Нейтронна мережа розпізнає чисті та заражені фрагменти.

Модель кібернейрона з'явилась відносно недавно і не апробовувалася, а використання табличної активаційної функції теоретично недостатньо обґрунтоване. Відповідно, застосування кібернейрона для оцінки ПБ потребує грунтовного доопрацювання.

Метод розпізнавання аномалій мережевого трафіку (РАМТ) [1]. Методом передбачено використання НМ типу БШП. Як вхідні дані НМ використано параметри заголовків IP-дейтаграм. Вибір архітектури НМ грунтується на твердженні про високі апроксимаційні можливості БШП.

Багатошаровий персептон складається із трьох шарів нейронів. Кількість нейронів ВШ – 18, що дорівнює кількості параметрів заголовка IP-дейтаграми. Кількість нейронів у ШВ – 2.

Вихід нейрона 1 відповідає за наявність аномалії, а вихід нейрону 2 – за безпечний стан мережевого трафіку. Наведено вирази для розрахунку кількості нейронів у СШН. Таким чином, методом передбачено оптимізацію параметрів архітектури НМ.

Для спрощення створення репрезентативної вибірки розроблено метод уточнювальних сигнатур, суть якого полягає у введенні додаткових штучно створених сигнатур, що описують апріорно аномальний трафік. Отже, в методі у неявному вигляді можна використовувати експертні дані про мережеві атаки.

Нейромережева штучна імунна система (НШІС) [7, 247]. Ця систма призначена для розпізнавання в сканованих файлах ШПЗ. Використано НМ типу ТК. Вибір типу НМ обґрунтовано за критерієм мінімізації допустимого обсягу навчальної вибірки L, який для ТК залежить тільки від кількості нейронів СШН m: $L \geq 2m$.

У свою чергу, $m = p + r$, де p – кількість прикладів безпечних програм у навчальній вибірці, а r – кількість прикладів ШПЗ. Процедури попереднього оброблення вхідних параметрів та оптимізації процесу навчання не передбачені.

Модель ТК для розпізнавання комп'ютерних вірусів (МТК) [4]. Модель призначена для використання в антивірусних сканерах. Передбачено блок попереднього оброблення вхідних параметрів. Вибір типу моделі реалізовано шляхом порівняльних числових експериментів. Як критерій порівняння використано термін навчання. Оптимізація параметрів та процедури навчання нейромережевої моделі не проводилась.

Метод виявлення несанкціонованого доступу до бази даних (ВНДБД) [62]. Крім виявлення атак, метод передбачає виявлення вразливостей у базі даних. Запропоновано використання ДШП. Вхідний шар нейтронів складається

із 4 нейронів, а ШВ – з одного.

Як вхідні дані використано: обсяг інформації, що завантажується в базу даних, кількість транзакцій за одну хвилину, кількість операцій модифікації за одну хвилину, ознаки звернень до словника. Попереднє оброблення вхідних параметрів полягає у їх ранжуванні та нормалізації.

Алгоритм перетворення параметрів трафіку (АППТ) [15]. Алгоритм призначений для отримання з мережевого трафіку вхідних даних для нейромережевої системи виявлення мережевих атак. Як вхідна інформація зазначеного алгоритму використовуються параметри TCP-сесії.

Перетворення параметрів трафіку застосовується для зменшення кількості вхідних параметрів НМ та збільшення їх інформативності та реалізується за допомогою математичного апарату, що грунтується на методі головних компонент. В алгоритмі оптимізації виду та параметрів НММ не передбачено.

Нейромережева технологія виявлення мережевих атак (ТВМА) на інформаційні ресурси [58, 59, 148]. У технології передбачено модуль стиснення вхідних даних, що грунтується на застосуванні нейромережевого аналогу методу головних компонент – рециркуляційної нейронної мережі з двома шарами нейронів.

Числовими експериментами доведено можливість використання запропонованої технології для виявлення мережевих атак, сигнатури яких подано в базі даних KDD-99.

Базові характеристики проаналізованих методів наведено в табл. 1.2. Аналіз даних цієї таблиці показує, що більшість наведених методів призначені для розпізнавання мережевих атак за допомогою використання класичних видів НММ, адаптованих до умов поставленої задачі. Як базі види НММ використовуються БШП і ТК. Також визначено, що ефективність сучасних нейромережевих методів та моделей забезпечується в них певних можливостей, які можна характеризувати за допомогою таких критеріїв:

- $ф_{п.об}$ – попередня обробка вхідних параметрів,
- $ф_{одн.оп.ар}$ – однокритеріальна оптимізація виду архітектури,
- $ф_{б.оп.ар}$ – багатокритеріальна оптимізація виду архітектури,
- $ф_{одн.оп.п.ар}$ – однокритеріальна оптимізація параметрів архітектури,
- $ф_{б.оп.п.ар}$ – багатокритеріальна оптимізація параметрів архітектури,
- $ф_{оп.м.н}$ – оптимізація методу навчання,
- $ф_{в.ек.п}$ – можливість використання експертних правил.

Наведений перелік доповнено критеріями $ф_{мна}$ і $ф_{одв}$, які вказують на можливість застосування в методі класичних і перспективних видів НММ та на можливість принципової оцінки доцільності застосування НМ для вирішення поставленого завдання.

Підґрунтям використання $ф_{мна}$ є наведене у працях [17, 20] твердження про те, що в СЗІ необхідно пристосовувати базові та перспективні види НММ до умов поставлених практичних завдань.

Підґрунтям використання критерію $ф_{одв}$ є об'єктивна необхідність чіткого окреслення області застосувань НМ в СЗІ. Величини запропонованих критеріїв у першому наближенні можна оцінити так:

- критерій дорівнює -1, коли відповідна можливість у нейромережевому методі або моделі не забезпечується;
- 0 – коли забезпечується частково,
- 1 – коли забезпечується повністю.

Для проаналізованих випадків величини означених критеріїв наведено в табл. 1.3. Для всіх проаналізованих методів $ф_{мна}= ф_{одв} =-1$. Лише для АППТ $ф_{мна}=1$, а $ф_{одв}=0$. Тобто в більшості із проаналізованих методів не можна використовувати весь перелік перспективних видів НММ, і в жодному із методів не передбачено оцінювання принципової доцільності його застосування, оптимізації НММ, відповідно до всіх умов поставленого завдання та повноцінного використання в такій моделі експертних правил. Базовий перелік критеріїв може бути в надалі розширений.

Таблиця 1.2

Базові характеристики нейромережевих методів

№	Метод	Розпізнавання				Тип НМ								
		ШПЗ	атак на базу даних	спаму	мере-жевих атак	БШП	КН	ТК	НМДЕ	АНМ	ННМ	БНМ	РНМ	Всі типи
1	ВФПК	+	-	-	-	+	-	-	-	-	-	-	-	-
2	МКН					-	+	-	-	-	-	-	-	-
3	МТК					-	-	+	-	-	-	-	-	-
4	НШІС													
5	НПВІ	-	+	-	-	-	-	-	+	-	-	-	-	-
6	ВНДБД					+	-	-	-	-	-	-	-	-
7	НФС	-	-	+	-	-	-	-	-	+	-	-	-	-
8	АППТ	-	-	-	+	-	-		-	-	-	-	-	+
9	ПСК					+	-		-	-	-	-	-	-
10	НСВВ													
11	ТВМА													
12	РАМТ													
13	ВМА													
14	ССК					-	-	+	-	-	-	-	-	-
15	НМГС	-	-	-	+	+	-	+	-	-	-	-	-	-
16	ПСКТ													
17	ПВМА													
18	АСВА													
19	ВАОП													
20	СВДА					-	-		-	-	+	-	-	-
21	БНМ					-	-		-	-	-	+	-	-
22	ВКМА					-	-		-	-	-	-	+	-

Практична цінність даних табл. 1.3 полягає у окресленні недоліків та перспектив удосконалення сучасних нейромережевих методів та моделей.

Таблиця 1.3

Величини критеріїв, що характеризують нейромережеві методи та моделі

№ з/п	Модель, метод	Критерій								
		$ф_{п.об}$	$ф_{одн.оп.ар}$	$ф_{б.оп.ар}$	$ф_{одн.оп.ар}$	$ф_{б.оп.п.ар}$	$ф_{оп.м.н.}$	$ф_{в.ек.п}$	$ф_{мна}$	$ф_{одв}$
1	ВФПК	1	0	-1	0	-1	0	1	-1	-1
2	МКН	1	1	-1	-1	-1	-1	-1	-1	-1
3	МТК	1	1	-1	0	-1	-1	-1	-1	-1
4	НШІС	-1	1	-1	1	-1	-1	-1	-1	-1
5	НПВІ	1	1	0	0	-1	0	-1	-1	-1
6	ВНДБД	1	0	-1	0	-1	-1	-1	-1	-1
7	НФС	1	1	0	1	0	1	-1	-1	-1
8	АППТ	1	-1	-1	-1	-1	-1	-1	0	-1
9	ПСК	1	0	-1	0	-1	0	-1	-1	-1
10	НСВВ	0	0	-1	0	-1	0	-1	-1	-1
11	ТВМА	1	0	-1	0	-1	-1	-1	-1	-1
12	РАМТ	-1	1	-1	0	-1	-1	0	-1	-1
13	ВМА	0	0	-1	0	-1	-1	1	-1	-1
14	ВМА	1	0	-1	0	-1	0	-1	-1	-1
15	ВМА	1	1	0	0	-1	-1	-1	-1	-1
16	ПСКТ	1	0	-1	0	-1	0	-1	-1	-1
17	ПВМА	1	1	-1	0	-1	0	-1	-1	-1
18	АСВА	1	1	0	1	1	0	-1	-1	-1
19	ВАОП	1	-1	-1	-1	-1	-1	-1	-1	-1
20	СВДА	0	0	-1	0	-1	0	-1	-1	-1
21	БНМ	-1	0	-1	-1	-1	1	-1	-1	-1
22	ВКМА	1	-1	-1	-1	-1	-1	-1	-1	-1

Наприклад, величини $ф_{п.об}=0$, $ф_{б.оп.ар}= -1$ свідчать про те, що як недолік методу НСВВ можна зазначити недостатню оптимізацію виду НММ.

У результаті проведеного аналізу можна зробити висновок про те, що важливим та актуальним напрямом підвищення ефективності систем розпізнавання кібератак на ресурси інтернет-орієнтованих ІС є застосування НМЗ оцінювання ПБ.

Незважаючи на певні досягнення в цій галузі, ефективному застосуванню таких НМЗ перешкоджають деякі недоліки. Основні з них такі:

– недостатня оперативність реагування на нові види кібератак;

– недостатня адаптація до варіативності умов застосування та функціонування за обмежених обчислювальних ресурсів;

– недостатня точність розпізнавання кібератак;

– недостатня взаємопов’язаність відомих нейромережевих підходів, моделей та методів оцінювання ПБ для виявлення кібератак.

Для усунення цих недоліків проведено дослідження у таких напрямах:

– розвиток теоретичного базису нейромережевого оцінювання ПБ;

– застосування розроблених теоретичних рішень для створення нейромережевих моделей, методів та методології оцінювання ПБ. Визначення напрямів розвитку теоретичного базису ґрунтується на таких передумовах:

1. Ефективне використання НМЗ потребує розроблення типових підходів до застосування НММ для розпізнавання різних видів кібератак.

2. Неоперативносте розпізнавання нових типів кібератак в основному зумовлюється тривалим нагромадженням статистичних даних, потрібних для побудови (навчання) НММ. Для забезпечення оперативності можливо для навчання НММ можна використовувати експертні дані.

3. Пристосувати НМЗ до варіативності умов застосування можна шляхом оптимізації виду та параметрів НММ, на яких базуються такі засоби.

4. Для адаптації НМЗ до функціонування за обмежених обчислювальних ресурсів необхідно як оптимізувати вид та параметри НММ,

так і апріорно оцінювати обсяг обчислювальних ресурсів для її реалізації.

5. Використання НМЗ пов’язане з певним набором умов та обмежень, що визначаються умовами задачі оцінювання та характеристиками НММ. Тому необхідно провести як визначення принципової доцільності застосування НМЗ, так і оцінювання ефективності їх розробки.

6. Підвищити точність розпізнавання кібератак можна за рахунок адаптації математичного забезпечення НММ до функціональних залежностей, що відповідають процесам розпізнавання. Для підвищення точності розпізнавання довготривалих кібератак доцільно використати марківський ШП ПБ, який дозволяє нівелювати часову складову процесу розпізнавання.

7. Використання НМ у високовідповідальних засобах розпізнавання кібератак потребує теоретичної верифікації НММ оцінювання ПБ.

Реалізація другого напрямку досліджень пов’язана з комплексним розробленням моделей та методів, що грунтується на запропонованих теоретичних рішеннях і враховують особливості сучасних видів кібератак.

Таким чином, для вирішення проблеми підвищення ефективності розпізнавання кібератак на ресурси інтернет-орієнтованих ІС через застосування НМЗ оцінювання ПБ необхідно:

– розвинути теоретичні положення побудови НМЗ оцінювання ПБ ІС, що дозволяють навчатись за допомогою експертних даних, зменшувати похибки класифікації, враховувати особливості сучасних видів кібератак, умови використання та верифікувати отримані рішення.

– побудувати моделі, що враховують запропоновані теоретичні рішення та адаптовані до застосування у НМЗ оцінювання ПБ.

– розробити методи створення НМЗ оцінювання ПБ, що враховують запропоновані теоретичні рішення та побудовані моделі.

– розробити нейромережеву методологію, яка за рахунок комплексного застосування створених моделей та методів дозволить підвищити ефективність вирішення актуальних завдань оцінювання ПБ ІС.

Розділ 2. РОЗВИТОК ТЕОРЕТИЧНИХ ПОЛОЖЕНЬ ПОБУДОВИ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ ОЦІНЮВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ІНТЕРНЕТ-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1. Базові підходи до оцінювання параметрів безпеки за допомогою нейромережевих засобів

Розпізнавання неочікуваних та поступових кібератак. Аналіз праць [247–250] вказує, що використання НМ для розпізнавання кібератак пов'язане з визначенням на базі аналізу вектора контрольованих подій ($\overline{\boldsymbol{Z}}$) оператора переходу ІС у різні стани захищеності Sz:

$$Sz = \mathrm{Net}(\overline{\mathrm{Z}}),$$

де Net – нейромережевий оператор.

Очевидно, що формування Net багато в чому залежить від вектора $\overline{\boldsymbol{Z}}$, який за своєю суттю відображає характер кібератаки. Застосування методології технічної діагностики [71] до аналізу $\overline{\boldsymbol{Z}}$ дозволило за аналогією з класифікацією відмов технічних систем, виділити два класи кібератак: поступові (ПК) та неочікувані (НК).

Визначення 1. Неочікуваною кібератакою будемо називати кібератаку, реалізація якої пов'язана із стрибкоподібним та неочікуваним щодо СЗІ виходом ПБ за безпечні межі.

У більшості випадків НК зумовлюється використанням у процесі реалізації кібератаки схованих вразливостей системи захисту РІС або є результатом виходу з ладу СЗІ. Як типовий приклад НК можна назвати «атаку нульового дня» [77].

Визначення 2. Поступовою є кібератака, яка супроводжується тривалою та очікуваною щодо СЗІ змінюванням ПБ до значень, які перевищують безпечні межі.

Типовим прикладом ПК є DDos-атака на веб-сервер, спрямована на вичерпання його обчислювальних ресурсів і реалізована за рахунок масових звернень. У багатьох випадках РІС одночасно є ціллю як ПК, так і НК. Із цього

погляду доцільно розглянути комбіновані кібератаки.

Маючи на увазі, що відповідно до праць [31, 251] кібератака є випадковою подією для оцінювання кількісних характеристик рівня захищеності, можна використати статистичні моделі ПК і НК. У таких моделях основною статистичною характеристикою зовнішніх негативних впливів на безпеку ресурсів ІС є інтенсивність кібератак $\lambda(t)$, де t – термін експлуатації ресурсів ІС. За допомогою ствтистичних моделей визначають імовірність забезпечення безпечного стану $P(t)$, імовірність успішної кібератаки протягом заданого терміну експлуатації $F(t)=1-P(t)$ та щільність розподілу часу безвідмовної роботи $f(t)$. Основною ознакою моделі НК є стала величина інтенсивності кібератак $\lambda(t)=\text{const}$, тоді $P(t)=e^{-\lambda t}$, $F(t)=1-P(t)=1-e^{-\lambda t}$, $f(t)=\lambda e^{-\lambda t}$. Графічною інтерпретацією статистичної моделі НК є рис. 2.1.

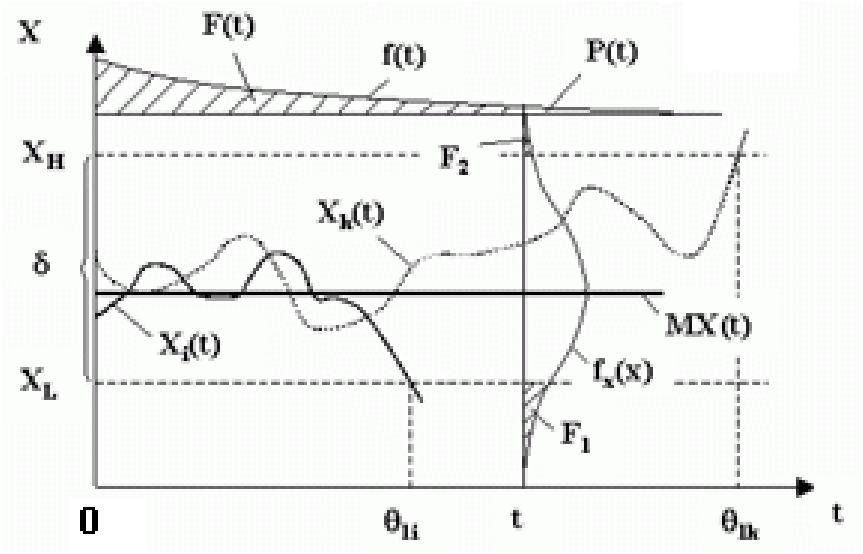

Рис. 2.1. Графічне зображення моделі НК

Складовими частинами такої моделі є: X – ПБ; кібератака реалізується, якщо X виходить за межі встановленого допуску δ, обмеженого верхньою X_H та нижньою X_L межами; $X(t)$ – стаціонарний випадковий процес, математичне сподівання $MX(t)$, дисперсія $DX(t)$ та функція щільності розподілу $f_x(x,t)$ якого не залежать від терміну експлуатації. Тобто $MX(t)=\text{const}$, $DX(t)=\text{const}$, $f_x(x,t)=f_x(t)$. Зміна $X_i(t)$ і $X_k(t)$ реалізацій

ПБ для *i*-го та *k*-го РІС зумовлена різними умовами експлуатації та різними негативними впливами. Моменти часу θ_{1i} та θ_{1k} виходу окремих реалізацій X за межі допуску свідчать про кібератаку на РІС.

Графічну інтерпретацію статистичної моделі ПК показано на рис. 2.2. Основними її відмінностями від моделі НК є: кібератака реалізується, якщо величина X перевищує встановлену межу $X_{\max}$; величина ПБ є довільною часовою функцією (на рис. 2.2 використана функцію $X(t) = \bar{a} + \bar{\gamma}_x t$, де $\bar{a}$ – математичне сподівання величини X у нульовий момент часу; $\bar{\gamma}_x$ – математичне сподівання швидкості зміни X); математичне сподівання, дисперсія та функція щільності розподілу ПБ залежать від терміну експлуатації.

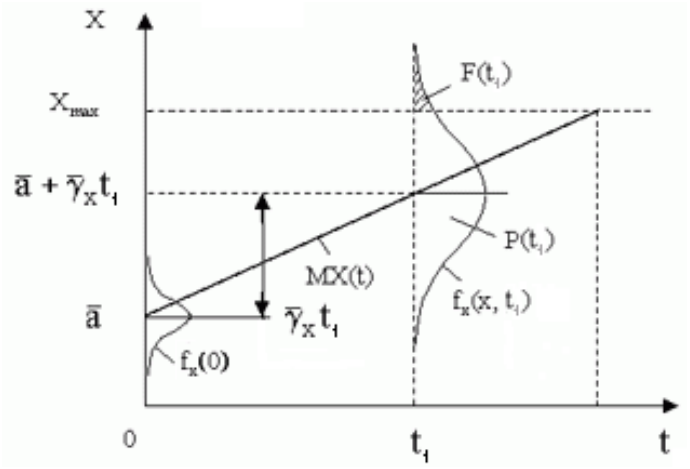

Рис. 2.2. Графічне зображення моделі ПК

До спрощень показаної на рис. 2.2 моделі належать: лінійність функції $X(t)$ та нормальний закон розподілу $f_x(t)$. Як приклад на рис. 2.2 схематично показано розрахунок моменту часу t_1, коли $F(t_1) > 0$. Випадок зміни величини ймовірності забезпечення безпеки РІС під впливом комбінованої кібератаки показано на рис. 2.3, де індекси 1, 2, 3 відповідають НК, ПК та комбінованій кібератаціВипадок, коли НК незалежить від ПК, показано на рис. 2.3. Тому ймовірність забезпечення безпеки у разі комбінованої кібератаки розраховувалась так: $P_3(t) = P_1(t)P_2(t)$.

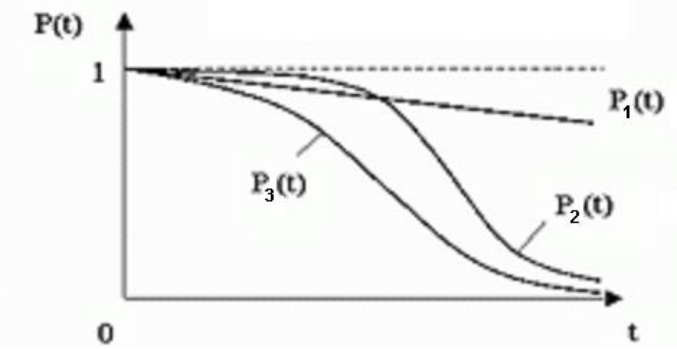

Рис. 2.3. Графік зміни ймовірності забезпечення безпеку разі комбінованої кібератаки

Використання вказаних моделей дозволяє на основі знань динаміки ПБ розрахувати основні статистичні показники, пов'язані з кібератаками – $P(t), F(t), f(t)$. Крім того, аналіз цих моделей дозволяє запропонувати підходи до розпізнавання НК і ПК.

Підхід для розпізнавання неочікуваних кібератак. Оскільки НК характеризується деструктивним впливом, результативність якого не залежить від терміну експлуатації, то для її своєчасного виявлення потрібно реалізувати постійний контроль та оцінювання ПБ. Виявити НК необхідно до того, коли ПБ вийдуть за межі попереджувального допуску. Як базу визначення ПБ доцільно використовувати параметри зовнішніх програмних запитів до ІС. Рішення про наявність кібератаки приймається, якщо виявлено відповідність параметрів цих запитів шалону атаки (ША) або не відповідність шаблону нормальної поведінки (ШНП):

$$якщо\ \{X(t_k)\} \subset \left(\{X\}_A \cup \{D\}_A\right) \wedge / \vee \{X(t_k)\} \not\subset \left(\{X\}_N \cup \{D\}_N\right) \rightarrow A, \qquad (2.1)$$

де $\{X(t_k)\}$ – множина значень ПБ у k-й момент часу; $\{X\}_A$ – значення ПБ, що відповідають ША; $\{X\}_N$ – комбінація значень ПБ, що відповідають ШНП; $\{D\}_A$ – множина попереджувальних допусків на ПБ для ША; $\{D\}_N$ – множина попереджувальних допусків на ПБ для ШНП; A – кібератака.

Наприклад, для виявлення скриптового ШПЗ слід проаналізувати використані в ньому потенційно небезпечні програмні конструкції до виконання скрипта. Аналіз відомих прикладів НК [60, 69] показує те, що

труднощі їх виявлення в першу чергу зумовленні з багатоваріантним характером комбінацій ПБ, що вказують на наявність кібератаки. Цей факт значно ускладнює визначення граничних меж значень ПБ, які входять до множини $\{ X \}_A$.

Підхід для розпізнавання поступових кібератак. Оскільки ПК є тривалим процесом, то для її своєчаснго виявлення доцільно скористатись ШП, розрахованими протягом деякого інтервалу часу. Як ПБ можнавикористовувати параметри зовнішніх запитів та функціональні параметри РІС. Правило класифікації ПК має вигляд:

$$якщо \{X(t_k)\} \subset \left(\{X(t)_{t=t_k}\}_A \cup \{D\}_A\right) \wedge\vee \{X(t_k)\} \not\subset \left(\{X(t)_{t=t_k}\}_N \cup \{D\}_N\right) \rightarrow A, \quad (2.2)$$

де $\{ X(t)_{t=t_k} \}_A$ – значення ПБ для ША в *k*-й момент часу, $\{ X(t)_{t=t_k} \}_N$ – значення ПБ для ШНП у *k*-й момент часу.

Результати [124, 125] дозволяють подати ШП ПБ у вигляді одноперіодичного або багатоперіодичного динамічного ряду даних. В одноперіодичних ШП ПБ протягом заданого терміну має характер одноперіодичної часової функції, а в багатоперіодичному ШП – характер багатоперіодичної часової функції. Відповідно до положень теорії динамічних рядів даних багатоперіодичний ШП можна виразити у вигляді суми одноперіодчних ШП [79, 125]. Графік одноперіодичного ШП показано на рис. 2.4, а графік багатоперіодичного ШП – на рис. 2.5. Шаблон поведінки відповідає функції $X = f(t)$. На рис. 2.5 літерами *A* і *B* позначено перехідні (екстремальні) точки функції $X = f(t)$. При цьому A_2, A_4,…A_D відповідають максимумам, а B_1, B_2,…B_{D-1} – мінімумам цієї функції. Індекси 1,2,…D означають номер перехідної точки. На інтервалах типу $B_d A_{d+1}$ і $A_{d+1} B_{d+2}$ одноперіодичний ШП має стаціонарний характер. На інтервалах $B_d A_{d+1}$ функція $X = f(t)$ зростає, а на інтервалах $A_{d+1} B_{d+2}$ – спадає. Для випадку односторонньої області оцінки рівня захищеності та умови збільшення *i*-го ПБ у разі виникнення кібератаки (див. рис. 2.2) $X_{i,min} = 0$, а $X_i = 0$ відповідає

найкращому стану захищеності. За рахунок цього (2.2) змінюється так:

$$якщо\ X_i(t) \in \lfloor 0, X_{i,\max} - D \rfloor,\ t = t_k \rightarrow A, \tag{2.3}$$

де D – величина допуску на X_i.

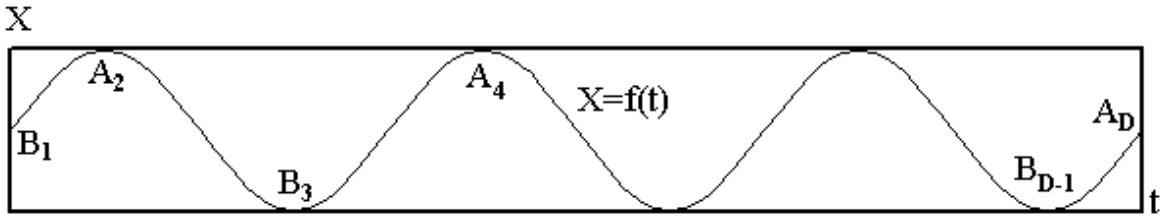

Рис. 2.4. Графік одноперіодичного шаблону поведінки

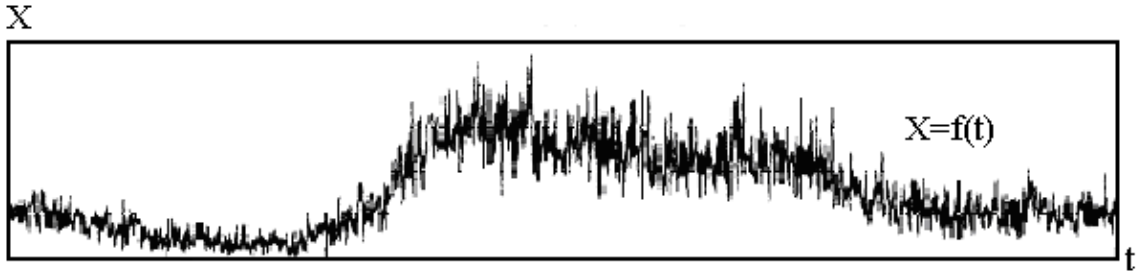

Рис. 2.5. Графік багатоперіодичного шаблону поведінки

Графічну інтерпретацію виразу (2.4) показано на рис. 2.6. Прикладом використання цієї моделі може бути виявлення мережевої кібератаки для підбору парольних даних. Для її виявлення можна встановити допуск на кількість неправильних уведень парольних даних з певної підмережі за встановлений проміжок часу.

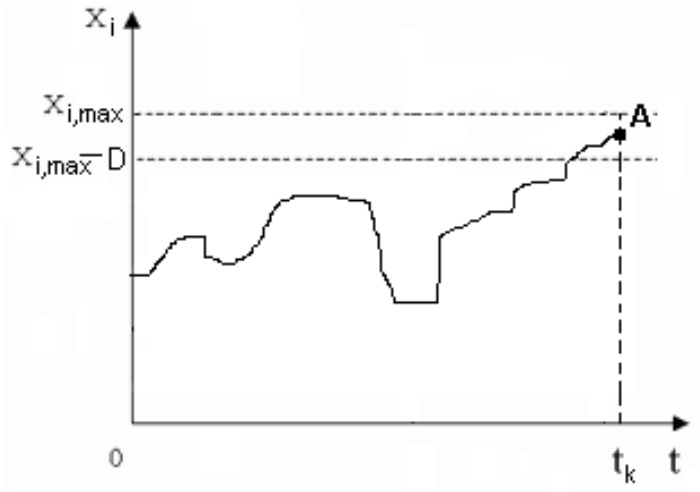

Рис. 2.6. Графічне зображення моделі оцінювання ПБ у разі виявлення ПК

Відповідно до праці [71] величина D має випадковий характер іповинна враховувати динаміку ПБ:

$$D = F(X_i(t)).$$

Надто велике значення D призведе до зменшення функціонала ІС, а надто мале – до збільшення ймовірності успіху кібератаки. Труднощі прийняття рішення про наявність/відсутність ПК спричинені складним характером $X_i(t)$. Тому для розроблення ефективних НМЗ виявлення різнотипних кібератак необхідно створити відповідну модель оцінювання ПБ.

У цій моделі, як зазанечено у працях [71, 89], має бути врахована множина характеристик об'єкта захисту $\boldsymbol{O}$, аналіз яких дозволяє визначити перелік ПБ. Базовими характеристиками об'єкта захисту є: структура o_1, призначення o_2, вразливості o_3, функціональність o_4, загрози o_5. Тобто

$$\boldsymbol{O} = \{o_1, ..o_5\}. \quad (2.6)$$

Підхід до визначення оптимального виду нейромережевої моделі. Проведений в підрозділі 1.3 аналіз дозволяє стверджувати, що ефективні НМЗ розробляються пристосуванням визначених характеристик НММ до значущих умов задачі оцінювання ПБ. Звідси можна запропонувати такий підхід – оптимальним є той вид НММ, характеристики якого більш повно відповідають значущим умовам задачі оцінювання ПБ. У базовому варіанті множина значущих умов поділяється на категорії (див. підрозозд.. 1.3), що характеризують навчальні дані, обмеження процесу навчання, обчислювальні потужності, вихідну інформацію, технічну реалізацію та сферу застосування НМЗ. Можливою інтерпретацією підходу є вираз

$$e(a_i) \to \max,\ a_i \in A,\ i = 1,2,...,I,$$

де e – критерій оптимізації; a_i – i-й вид НММ; A – множина допустимих видів НММ; I – кількість допустимих видів НММ.

Очевидно, що використаний у виразі (2.) критерій оптимізації потребує деталізації з позицій врахування визначених характеристик виду НММ. Крім того, слід враховувати можливу близькість величини критерію оптимізації для різних видів НММ. Тому доцільно визначати множину оптимальних видів НММ, до якої входитимуть НММ, у яких величина критерію оптимізації

близька до максимальної (близькість оцінюється коефіцієнтом відхилення – k_E).

Підхід до визначення принципової доцільності застосування нейромережевих засобів оцінювання параметрів безпеки. Відповідно до аналізу теоретичних праць [140] принципова доцільність застосування НМЗ визначається можливістю в прийнятний термін знайти параметри НММ, які забезпечують достатню точність розпізнавання. За заданої архітектури визначення параметрів НММ реалізується в процесі навчання. Для цього необхідно виконати такі умови:

1. у піддослідному процесі визначити ПБ, які будуть використані як вхідні та вихідні параметри НМ;

2. сформувати навчальну вибірку НМ;

3. не допустити в разі використання визначеного обсягу обчислювальних ресурсів та помилки навчання перевищення терміну навчання НМ від заданого інтервалу часу.

Потенційно як вхідні параметри НМ можуть бути використані всі зареєстровані ПБ ІС. Перед поданням у НМ ці параметри потрібно відповідним чином закодувати та нормалізувати [49]. У найпростішому випадку вихід НМ має вказувати на наявність або відсутність кібератаки, а у складніших випадках – на вид кібератаки. Відповідно для формування навчальних прикладів потребності статистичні дані про величини ПБ у випадку реалізації кібератаки та під час нормального функціонування ІС. Необхідно також враховувати такі вимоги:

1. Нейронна мережа навчена на прикладах функціонування однієї ІС може видавати неправильний результат для інших ІС.

2. Додавання та вилучення зі складу ІС навіть окремих об’єктів приводить до зміну величин ПБ, а відповідно і до необхідності внесення змін до навчальної вибірки НМ.

3. Мінімальна кількість навчальних прикладів має щонайменше в 10–20

разів перевищувати кількість вхідних параметрів [8, 13]:

$$P_{\min} \geq (10...20)N_x, \qquad (2.5)$$

де $P_{\min}$ – мінімальна кількість навчальних прикладів; N_x – кількість вхідних параметрів НМ.

4. Кількість навчальних прикладів має бути обмеженою.

5. У прикладах навчальної вибірки потрібно пропорційно подавати всі класи, які повинна розпізнати НМ.

Тому формування достатнього обсягу навчальних прикладів може викликати труднощі, спричинені масштабуванням навчальних даних (вимоги 1, 2), так і збиранням достатньої кількості статистичної інформації (вимоги 3, 4, 5). Таким чином, термін визначення параметрів НММ можна оцінити за допомогою формули:

$$T_f = T_n + t_n,$$

де T_n – термін формування навчальної вибірки; t_n – термін навчання НМ.

Відповідно НМЗ доцільно використовувати тільки в тому випадку, якщо розрахований за допомогою (2.5) термін визначення параметрів НММ менший від допустимого терміну розроблення НМЗ. Тобто

$$T_f \leq T_a, \qquad (2.6)$$

де T_a – допустимий термін створення системи розпізнавання.

Підхід до визначення ефективності розроблення НМЗ оцінювання ПБ ІС. Аналіз сучасних НМЗ, що використовуються у СЗІ, дозволив визначити ряд базових критеріїв, кожен з яких дозволяє оцінити ефективність певного аспекту застосування вказаних засобів. При цьому з погляду теорії НМ [49, 101], критерії $\varphi_{\text{п.об}}, \varphi_{\text{одн.оп.п.ар}}, \varphi_{\text{б.}}, .\varphi_{\text{одн.оп.ар}}, \varphi_{\text{б.оп.п.ар}}, \varphi_{\text{оп.м.н}}, \varphi_{\text{мна}}$ вказують на потрібний обсяг обчислювальних ресурсів, які співвідносяться із кількістю обчислювальних операцій, необхідних для досягнення заданої точності класифікації. Критерії $\varphi_{\text{одн.оп.п.ар}}, \varphi_{\text{б.}}, \varphi_{\text{мна}}$ вказують на можливість адаптації НМЗ до варіативності умов застосування. Критерії $\varphi_{вер}$ та $\varphi_{мна}$ співвідносяться із

забезпеченням адаптації до кібератак, для яких немає статистичних даних, а $\phi_{одв}$ вказує на можливість принципової оцінки доцільності застосування НМЗ.

Таким чином, ефективність НМЗ оцінки ПБ можна оцінити шляхом використання інтегральних критеріїв, що характеризують точність класифікації кібератак $d_{ткк}$, можливість принципової оцінки доцільності застосування НМЗ $d_{одв}$, адаптацію до нових видів кібератак $d_{анв}$, пристосованість до варіативності умов застосування $d_{вуз}$ та до функціонування за обмежених обчислювальних ресурсів $d_{оор}$. При цьому

$$d_{ткк} = f\left(\phi_{ота}, \phi_{бва}, \phi_{омн}, \phi_{опа}, \phi_{бпа}, \phi_{мна}\right), \tag{2.7}$$

$$d_{одв} = f\left(\phi_{одв}\right), \tag{2.8}$$

$$d_{анв} = f\left(\phi_{веп}, \phi_{мна}\right), \tag{2.9}$$

$$d_{вуз} = f\left(\phi_{ота}, \phi_{бва}, \phi_{мна}\right), \tag{2.10}$$

$$d_{оор} = f\left(\phi_{по}, \phi_{ота}, \phi_{бва}, \phi_{омн}, \phi_{опа}, \phi_{бпа}, \phi_{мна}\right). \tag{2.11}$$

Інтеграція вказаних критеріїв дозволяє визначити інтегральну ефективність НМЗ. При цьому важливість критерію для конкретної задачі можлна врахувати за допомогою вагових коефіцієнтів, визначених на основі експертних даних. Ефективність НМЗ буде вважатись достатньою, якщо вона перевищує заданий апріорно мінімально допустимий рівень.

Підхід до класифікації подібних кібератак. Підхід полягає в тому, що *i*-а Ka_i та *k*-а Ka_k кібератаки вважаються подібними, якщо вони мають однаковий характер – неочікуваний Ks або поступовий Kq, а приведена різниця ПБ R_p, що використовується для їх розпізнавання, не перевищує максимальну $R_{\max}$:

$$\left(Ka_i = Ks \wedge Ka_k = Ks\right) \vee \left(Ka_i = Kq \wedge Ka_k = Kq\right) \wedge \left(R_p \le R_{\max}\right) \rightarrow Ka_i \sim Ka_k,$$

$$R_p = \left|R_i - R_k\right| / R,$$

$$R = \max\left(R_i, R_k\right),$$

де R_i, R_k – кількість ПБ при розпізнаванні *i*-ї та *k*-ї кібератак.

Параметр $R_{\max}$ визначається апріорно на основі експертних даних.

Підхід до застосування продукційних правил при поданні експертних знань у нейромережеві засоби оцінювання параметрів безпеки. Підхід грунтується на аналогії між експертними знаннями у вигляді продукційних правил та навчальними прикладами НМ.

У спрощеному випадку елементарне продукційне правило вигляду *Якщо умова істина/хибна* $\rightarrow$ *(Висновок),* можна вважати аналогом навчального прикладу НМ:

$$X = a \rightarrow Y, \tag{2.11}$$

де X – вхідний параметр НМ; a – значення вхідного параметру; Y – очікуваний вихідний сигнал НМ.

У більш складному випадку типовий навчальний приклад НМ (2.11) – це комбінація продукційних правил вигляду

$$X_1 = a_1, \ldots X_N = a_N \rightarrow Y, \tag{2.12}$$

якщо умова1 істина/хибна,… умоваN істина/хибна $\rightarrow$ *(Висновок),* (2.13)

де X_N – n-й вхідний параметр; a_N – значення n-го вхідного параметра; Y – очікуваний вихід НМ.

Оцінюючи ПБ для виявлення кібератак, вираз (2.13) можнатрансформувати так:

$$\text{якщо } p_1 \in \left[P_1^{\min}, P_1^{\max}\right]_l \wedge \ldots \wedge p_K \in \left[P_K^{\min}, P_K^{\max}\right]_l \rightarrow Y_l, \tag{2.14}$$

де $p_1, \ldots p_K$ – ПБ, $\left[P_1^{\min}, P_1^{\max}\right], \ldots \left[P_K^{\min}, P_K^{\max}\right]$ – задані діапазони величин ПБ; K – кількість ПБ; l – номер продукційного правила; Y_l – результат продукційного правила.

Достатньо відомі й апробовані види НММ, що можуть навчатись шляхом безпосереднього запам’ятовування поданих навчальних прикладів, тобто поданням експертних знань у вигляді продукційних правил. Тому такі види НММ мають містити експертні знання у вигляді продукційних правил вигляду (2.14) про значення ПБ, що стосуються розпізнавання кібератак.

2.2. Критерії оптимізації виду нейромережевої моделі

Для формування критеріїв оптимізації виду НММ використано розроблений підхід до визначення оптимального виду НММ та результати дослідження можливостей застосування методів теорії НМ для оцінювання ПБ. Базовий перелік отриманих критеріїв наведено в табл. 2.1. Перелік може бути розширений, наприклад, за рахунок деталізації певних критеріїв або врахування нових сфер застосування НМ.

Таблиця 2.1

Критерії оптимізації

№ з/п	Категорія	Пояснення критерію
$E_{1,1}$	Навчальні дані	Обмеженість кількості вхідних параметрів
$E_{1,2}$		Обмеженість навчальної вибірки
$E_{1,3}$		Допустимість шуму
$E_{1,4}$		Допустимість кореляції
$E_{1,5}$		Необхідність відображення всіх аспектів процесу
$E_{1,6}$		Необхідність пропорційного представлення прикладів
$E_{1,7}$		Можливість використання дискретних вхідних параметрів
$E_{1,8}$		Можливість використання неперервних вхідних параметрів
$E_{1,9}$		Можливість використання навчальної вибірки, обсяг якої менший за кількість вхідних параметрів
$E_{2,1}$	Процес навчання	Короткий термін навчання
$E_{2,2}$		Необхідність подання в навчальних прикладах очікуваного виходу

Продовження. табл. 2.1

№ з/п	Категорія	Пояснення критерію

$E_{2,3}$		Автоматизація навчання
$E_{2,4}$		Можливість донавчання
$E_{2,5}$	Процес навчання	Якість навчання
$E_{2,6}$		Можливість навчання за експертними даними
$E_{2,7}$		Незмінність результатів
$E_{3,1}$	Обчислювальна потужність	Ємність пам'яті
$E_{3,2}$		Екстраполяції результатів навчання
$E_{4,1}$	Вихідна інформація	Інтерпретованість виходу у вигляді ймовірності
$E_{4,2}$		Інтерпретованість виходу у графічному вигляді
$E_{4,3}$		Можливість вербалізації
$E_{5,1}$	Технічна реалізація	Швидкість прийняття рішення
$E_{5,2}$		Обсяг програмної реалізації
$E_{6,1}$	Сфера застосування	Розпізнавання образів
$E_{6,2}$		Аналіз тексту
$E_{6,3}$		Управління параметрами захисту
$E_{6,4}$		Пристосованість до автономного функціонування
$E_{6,5}$		Моделювання часових рядів
$E_{6,6}$		Аналіз зображень
$E_{6,7}$		Аналіз звуку
$E_{6,8}$		Розвідувальний аналіз даних

Результати підрозділу 1.3 дозволили в першому наближенні виставити оцінки відповідності основних видів НММ запропонованим критеріям, за трибальною шкалою (табл. 2.2 та 2.3).

Критерій E_i=1, якщо *i*-а характеристика задачі оцінювання ПБ повністю забезпечується у вигляді НММ, E_i=0 – якщо забезпечується частково, і E_i=-1 – якщо не забезпечується.

Таблиця 2.2

Величини критеріїв оптимізації для НМ з прямим поширенням сигналу та АРТ

№ з/п	Вид нейромережевої моделі				
	БШП	Згорткові	РБФ	АРТ	Імовірнісні
$E_{1,1}$	-1	-1	-1	-1	-1
$E_{1,2}$	-1	-1	-1	0	-1
$E_{1,3}$	1	1	0	-1	0
$E_{1,4}$	1	1	1	1	1
$E_{1,5}$	-1	-1	1	-1	1
$E_{1,6}$	-1	1	-1	-1	-1
$E_{1,7}$	1	1	1	1	1
$E_{1,8}$	1	1	1	1	1
$E_{1,9}$	-1	-1	1	1	1
$E_{2,1}$	-1	-1	0	1	1
$E_{2,2}$	1	1	1	-1	1
$E_{2,3}$	1	1	-1	1	1
$E_{2,4}$	0	0	1	1	1
$E_{2,5}$	1	1	0	1	1
$E_{2,6}$	-1	-1	-1	-1	1
$E_{2,7}$	1	1	1	1	1
$E_{3,1}$	1	1	-1	-1	-1
$E_{3,2}$	1	0	-1	-1	-1
$E_{4,1}$	0	-1	0	-1	1
$E_{4,2}$	-1	0	-1	-1	-1
$E_{4,3}$	1	-1	0	-1	0
$E_{5,1}$	1	1	1	1	1

Продовж. табл. 2.2

№ з/п	БШП	Згорткові	РБФ	АРТ	Імовірнісні

$E_{5,2}$	-1	-1	1	0	-1
1	2	3	4	5	6
$E_{6,1}$	1	0	1	1	1
$E_{6,2}$	-1	-1	-1	0	0
$E_{6,3}$	-1	-1	-1	-1	-1
$E_{6,4}$	0	-1	1	1	-1
$E_{6,5}$	1	-1	0	0	0
$E_{6,6}$	1	1	-1	-1	-1
$E_{6,7}$	1	0	-1	-1	-1
$E_{6,8}$	-1	-1	-1	-1	-1

Таблиця 2.3

Величини критеріїв оптимізації для рекурентних НМ, СНМ та ТК

№ з/п	Вид нейромережевої моделі				
	Елмена	Джордана	СНМ	АНМ	ТК
$E_{1,1}$	-1	-1	1	-1	-1
$E_{1,2}$	-1	-1	1	-1	-1
$E_{1,3}$	1	1	1	-1	1
$E_{1,4}$	1	1	1	-1	1
$E_{1,5}$	-1	-1	-1	0	1
$E_{1,6}$	1	1	-1	0	1
$E_{1,7}$	1	1	1	1	1
$E_{1,8}$	1	1	-1	0	1
$E_{1,9}$	-1	-1	1	1	1
$E_{2,1}$	-1	-1	0	1	1
$E_{2,2}$	1	1	-1	1	-1

Продовж. табл. 2.3

№ з/п	Елмена	Джордана	СНМ	АНМ	ТК
$E_{2,3}$	-1	-1	1	0	0
$E_{2,4}$	0	0	1	0	1
1	2	3	4	5	6
$E_{2,5}$	0	0	1	1	0
$E_{2,6}$	-1	-1	-1	-1	-1
$E_{2,7}$	1	1	1	0	0
$E_{3,1}$	1	1	0	0	-1
$E_{3,2}$	1	1	0	1	0
$E_{4,1}$	0	0	-1	0	0
$E_{4,2}$	-1	-1	-1	-1	1
$E_{4,3}$	1	1	-1	-1	-1
$E_{5,1}$	1	1	0	-1	1
$E_{5,2}$	-1	-1	-1	0	-1
$E_{6,1}$	0	0	0	1	1
$E_{6,2}$	-1	-1	1	-1	1
$E_{6,3}$	-1	-1	-1	1	1
$E_{6,4}$	-1	-1	1	-1	-1
$E_{6,5}$	1	1	-1	-1	-1
$E_{6,6}$	0	-1	-1	-1	-1
$E_{6,7}$	0	0	-1	-1	0
$E_{6,8}$	-1	-1	-1	1	1

З урахуванням трибальної числової оцінки (2.4) модифікується так:

$$E_{\Sigma} = \sum_{k=1}^{K} E_k(a_i) \to \max,\ a_i \in \mathrm{A},\ i = 1,2,...,7,$$

де E_{Σ} – інтегральний критерій оптимізації виду НММ; $\boldsymbol{A}$ – множина допустимих видів НММ.

Відповідно до результатів підрозділу1.3., компоненти $\boldsymbol{A}$ визначаються так:

$$\boldsymbol{A}=\{БШП,РБФ,PNN,ТК,АРТ,АНМ,СНМ\}.$$

Для конкретної задачі оцінювання ПБ вагомість критеріїв оптимізації можна врахувати, увівши в рівняння (2.13) відповідні вагові коефіцієнти:

$$E_{\Sigma}=\sum_{k=1}^{K}\left(r_k\times E_k(a_i)\right)\to\max,\ a_i\in\mathrm{A},\ i=1,2,\ldots,7,$$

де r_k – ваговий коефіцієнт k-го критерію оптимізації.

2.3. Удосконалення математичного забезпечення процесу навчання багатошарового персептрона

Проведені дослідження вказують на те, що можливою причиною великої відносної помилки навчання в області мінімальних значень вихідних параметрів БШП є запис критерію оцінки якості навчання у вигляді квадратичного функціонала вигляду:

$$\varepsilon(W)\to\min,\ \varepsilon^2(W)=\left(y_i-y_i^r\right)^2,$$

де y_i, y_i^r – очікуваний та реальний вихідний сигнали i-го нейрона БШП; W – матриця вагових коефіцієнтів синаптичних зв'язків.

Можливим шляхом зменшення відносної помилки є використання функціонала відносної квадратичної помилки:

$$\bar{\varepsilon}_i^2(W)=\left(\varepsilon_i(W)/y_i\right)^2=\left(y_i-y_i^r/y_i\right)^2, y_i\neq 0,. \qquad (2.15)$$

де $\bar{\varepsilon}_i$ – зведена помилка навчання i-го вихідного нейрона; y_i – очікуваний сигнал i-го вихідного нейрона; y_i^r – реальний сигнал i-го вихідного нейрона.

Зазначимо, що умова $y_i\neq 0$ визначається, виходячи з використання логістичної сигмоїдальної функції активації штучного нейрона:

$$y^r(z)=1/1+e^{-\alpha\cdot z}. \qquad (2.16)$$

де α – деякий коефіцієнт; z – зважена сума вхідних сигналів для нейрона.

Модифікація (2.15) зумовлює певні зміни в математичній моделі

класичного алгоритму зворотного поширення помилки. Визначимо ці зміни для БШП з довільною кількістю схованих шарів. Будемо базуватись на описі алгоритму навчання, наведеному у праці [4]. При цьому

$$\frac{d}{dz} y^r(z) = \alpha y^r(z)\left(1 - y^r(z)\right). \tag{2.17}$$

Розглянемо обчислення вагових коефіцієнтів зв'язків *i*-го нейрона ШВ. Зведений квадратичний критерій якості навчання (2.15) та постулат [210] про розгляд складових (2.15–2.17) у вигляді неперервних величин дозволяють записати математичне забезпечення градієнтного алгоритму корегування вагових коефіцієнтів у режимі навчання on-line у вигляді

$$\Delta w_{s,i}^{(j+1)} = -\gamma_{s,i}^{(j+1)} \frac{\partial \bar{\varepsilon}_i^2}{\partial w_{s,i}^{(j+1)}}, . \tag{2.18}$$

де $\gamma_{s,i}^{(j+1)}$ – коефіцієнт швидкості навчання зв'язку між *i*-м нейроном ШВ та *s*-м нейроном попереднього шару; $\Delta w_{s,i}^{(j+1)}$ – величина корегування зв'язку між *i*-м нейроном ШВ та *s*-м нейроном попереднього шару; $\bar{\varepsilon}_i$ – зведена помилка навчання *i*-го нейрона ШВ.

Розрахуємо частинну похідну

$$\frac{\partial \bar{\varepsilon}_i^2}{\partial w_{s,i}^{(j+1)}} = \frac{\partial \bar{\varepsilon}_i^2}{\partial y_i^r} \frac{\partial y_i^r}{\partial z_i} \frac{\partial z_i}{\partial w_{s,i}^{(j+1)}}, \tag{2.19}$$

де z_i – зважена сума вхідних сигналів для *i*-го вихідного нейрона.

Зазначимо, що z_i розраховується так:

$$z_i = \sum_{s=1}^{S} \left(w_{s,i}^{(j+1)} y_s^{(j)} \right), \tag{2.20}$$

де *S* – кількість нейронів у передостанньому СШН; $y_s^{(j)}$ – вихідний сигнал *s*-го нейрона останнього схованого шару.

Ураховуючи вирази (2.16)–(2.18, 2.20), визначимо множники добутку (2.19):

$$\frac{\partial\bar{\varepsilon}_i^2}{\partial y_i^r}=\frac{\partial\left(\frac{y_i-y_i^r}{y_i}\right)^2}{\partial y_i^r}=\frac{1}{y_i^2}\frac{\partial\left(y_i-y_i^r\right)^2}{\partial y_i^r}=-\frac{2\left(y_i-y_i^r\right)}{y_i^2}=-\frac{2\varepsilon_i}{y_i^2}. \quad (2.21)$$

$$\frac{\partial y_i^r}{\partial z_i}=\alpha y_i^r\left(1-y_i^r\right); \quad (2.22)$$

$$\frac{\partial z_i}{\partial w_{s,i}^{(j+1)}}=y_s^{(j)}, \quad (2.23)$$

де $y_s^{(j)}$ – вихід *s*-го нейрона СШН, зв'язаного з *i*-м нейроном ШВ.

Підставивши вирази (2.21)–(2.23) у рівняння (2.19) отримаємо

$$\frac{\partial\bar{\varepsilon}_i^2}{\partial w_{s,i}^{(j+1)}}=-\frac{2\left(y_i-y_i^r\right)}{y_i^2}\alpha y_i^r\left(1-y_i^r\right)y_s^{(j)}.$$

Кінцевий вираз для корегування зв'язку між *i*-м нейроном вихідного (*j*+1)-го шару та *s*-м нейроном попереднього шару виглядає так:

$$\Delta w_{s,i}^{(j+1)}=\frac{2\alpha\gamma_{s,i}^{(j+1)}y_i^r\left(1-y_i^r\right)\left(y_i-y_i^r\right)y_s^{(j)}}{y_i^2}. \quad (2.24)$$

За аналогією з [140] використаємо позначення локальної помилки синаптичного зв'язку між *i*-м нейроном вихідного (*j*+1)-го шару та *s*-м нейроном попереднього шару у вигляді $\delta_{s,i}^{(j+1)}$. З урахуванням логістичної функції активації та функціоналу приведеної квадратичної помилки для зв'язку *i*-го нейрону вихідного шару з *s*-им нейроном попереднього шару вказана локальна помилка розраховується за допомогою виразу

$$\delta_{s,i}^{(j+1)}=\frac{y_i^r\left(1-y_i^r\right)\left(y_i-y_i^r\right)}{y_i^2}. \quad (2.25)$$

Із використанням $\delta_{s,i}^{(j+1)}$ виразу (2.18) можна надати вигляду

$$\Delta w_{s,i}^{(j+1)}=2\alpha\gamma_{s,i}^{(j+1)}\delta_{s,i}^{(j+1)}y_s^{(j)}. \quad (2.26)$$

Розглянемо математичний апарат визначення величини корекції зв'язку між *s*-им нейроном останнього *j*-го схованого шару та *k*-м нейроном попереднього шару ($\Delta w_{k,s}^{(j)}$). Використовуючи зведений функціонал помилки,

величину корегування вказаного зв’язку запишемо так:

$$\Delta w_{k,s}^{(j)} = -\gamma_{k,s}^{(j)} \frac{\partial \bar{\varepsilon}_s}{\partial w_{k,s}^{(j)}}. \qquad (2.27)$$

де $\bar{\varepsilon}_s$ – відносна помилка *s*-го нейрона *j*-го СШН; $\gamma_{k,s}^{(j)}$ – швидкість навчання зв’язку між *s*-м нейроном *j*-го СШН та *k*-м нейроном (*j*-1)-го СШН.

Обчислимо частинну похідну:

$$\frac{\partial \bar{\varepsilon}_s}{\partial w_{k,s}^{(j)}} = \sum_{i=1}^{M} \frac{\partial \bar{\varepsilon}_i^2}{\partial w_{k,s}^{(j)}} = \sum_{i=1}^{M} \frac{\partial \left(\frac{y_i - y_i^r}{y_i} \right)^2}{\partial w_{k,s}^{(j)}} = \sum_{i=1}^{M} \frac{1}{y_i^2} \frac{\partial \varepsilon_i^2}{\partial y_i^r} \frac{\partial y_i^r}{\partial z_i} \frac{\partial z_i}{\partial y_s^{(j)}} \frac{\partial y_s^{(j)}}{\partial z_s^{(j)}} \frac{\partial z_s^{(j)}}{\partial w_{k,s}^{(j)}}, . \qquad (2.28)$$

де M – кількість нейронів у ШВ; $\bar{\varepsilon}_i$ – зведена помилка на *i*-му виході БШП; $z_s^{(j)}$ – зважена сума вхідних сигналів для *s*-го нейрона в *j*-му шарі,

Запишемо вирази для визначення множників добутку (2.26)

$$\frac{\partial \varepsilon_i^2}{\partial y_i^r} = \frac{-2(y_i - y_i^r)}{y_i^2}; . \qquad (2.29)$$

$$\frac{\partial y_i^r}{\partial z_i} = \alpha y_i^r (1 - y_i^r); . \qquad (2.30)$$

$$\frac{\partial z_i}{\partial y_s^{(j)}} = w_{s,i}^{(j+1)}; . \qquad (2.31)$$

$$\frac{\partial y_s^{(j)}}{\partial z_s^{(j)}} = \alpha y_s^{(j)} (1 - y_s^{(j)}); . \qquad (2.32)$$

$$\frac{\partial z_s^{(j)}}{\partial w_{k,s}^{(j)}} = y_k^{(j-1)}, \qquad (2.33)$$

де $y_k^{(j-1)}$ – вихідний сигнал *k*-го нейрона (*j*-1)-го шару.

Підставивши вирази (2.29)–(2.33) у (2.28) отримаємо:

$$\Delta w_{k,s}^{(j)} = 2\gamma_{k,s}^{(j)} \alpha^2 \sum_{i=1}^{M} \left(\frac{y_i - y_i^r}{y_i^2} y_i^r (1 - y_i^r) w_{s,i}^{(j+1)} y_s^{(j)} (1 - y_s^{(j)}) y_k^{(j-1)} \right). \qquad (2.34)$$

Для розрахунку локальної помилки зв’язків вираз (2.34) підставимо в (2.25):

$$\Delta w_{k,s}^{(j)} = 2\gamma_{k,s}^{(j)}\alpha^2 y_s^{(j)}\left(1-y_s^{(j)}\right)y_k^{(j-1)}\sum_{i=1}^{M}\left(\delta_s^{(j+1)}w_{s,i}^{(j+1)}\right). \quad (2.35)$$

Узагальнивши рівняння (2.25, 2.35) за аналогіює з працею [140], отримаємо вирази

$$\delta_{k,s}^{g} = \left(1-y_s^{(g)}\right)y_s^{(g)}\sum_{i=1}^{M}\delta_s^{(g+1)}w_{s,i}^{(g+1)};$$

$$\Delta w_{k,s}^{(g)} = 2\gamma_{k,s}^{(g)}\alpha^{N-g+1} y_s^{(g)}\left(1-y_s^{(g)}\right)y_k^{(g-1)}\sum_{i=1}^{M}\left(\delta_s^{(g+1)}w_{s,i}^{(g+1)}\right).$$

для визначення локальної помилки та величини корекції вагових коефіцієнтів для вхідних зв'язків довільного *g*-го шару нейронів:

Розглянемо модифікацію алгоритму зворотного поширення помилок у разі використання як функції активації гіперболічного тангенса. У цьому випадку вихідний сигнал нейрона розраховується відповідно до виразу

$$y^r(z) = \tanh(\alpha z) = \frac{e^{\alpha z} - e^{-\alpha z}}{e^{\alpha z} + e^{-\alpha z}}. \quad (2.36)$$

де α – деякий коефіцієнт; z – зважена сума вхідних сигналів для нейрона.

При цьому

$$\frac{d}{dz}y^r(z) = 1-\tanh(\alpha z)^2 = 1-\left(y^r(z)\right)^2. \quad (2.37)$$

Розглянемо особливості обчислення вагових коефіцієнтів зв'язків *i*-го нейрона ШВ. На відміну від виразу (2.17) частинна похідна ∂y_i^r розраховується так:

$$\frac{\partial y_i^r}{\partial z_i} = 1-\left(y_i^r\right)^2.$$

Для формування (2.15) знову використано постулат про можливість розгляду складових (2.21)–(2.23) як неперервних величин. Підставивши рівності (2.21), (2.23), (2.36) у вираз (2.19), дістаємо:

$$\frac{\partial\bar{\varepsilon}_i^2}{\partial w_{s,i}^{(j+1)}} = -\frac{2\left(y_i - y_i^r\right)}{y_i^2}\left(1-\left(y_i^r\right)^2\right)y_s^{(j)}.$$

Вираз для розрахунку величини корегування зв'язку між *i*-м нейроном

вихідного (j+1)-го шару та s-м нейроном попереднього шару отримаємо, підставивши випаз (2.37) в (2.24)

$$\Delta w_{s,i}^{(j+1)} = -\gamma_{s,i}^{(j+1)} \frac{-2\left(y_i - y_i^r\right)}{y_i^2}\left(1-\left(y_i^r\right)^2\right)y_s^{(j)}.$$

Після тривіальних спрощень маємо:

$$\Delta w_{s,i}^{(j+1)} = \frac{2\gamma_{s,i}^{(j+1)}\left(y_i - y_i^r\right)\left(1-\left(y_i^r\right)^2\right)y_s^{(j)}}{y_i^2}. \qquad (2.38)$$

За аналогією із працею[140] використаємо поняття локальної помилки синаптичного зв'язку. З урахуванням функції активації типу гіперболічного тангенса та функціонала зведеної квадратичної помилки для зв'язку i-го нейрону вихідного шару із s-м нейроном попереднього шару локальна помилка розраховується так:

$$\delta_{s,i}^{(j+1)} = \frac{\left(y_i - y_i^r\right)\left(1-\left(y_i^r\right)^2\right)}{y_i^2}. \qquad (2.39)$$

Із використанням виразу (2.39) записуємо рівність (2.38) у вигляді

$$\Delta w_{s,i}^{(j+1)} = 2\gamma_{s,i}^{(j+1)}\delta_{s,i}^{(j+1)}y_s^{(j)}.$$

За аналогією з випадком використання логістичної функції активації, розглянемо математичний апарат визначення величини корегування зв'язку між s-м нейроном останнього j-го СШН і k-м нейроном попереднього шару ($\Delta w_{k,s}^{(j)}$). Вирази (2.18)–(2.21) залишаються без змін, оскільки до їх складу в явному вигляді ні функція активації, ні її похідна не входять. Однак при визначенні множників добутку (2.21) вирази (2.22), (2.23) змінюються на такі:

$$\frac{\partial y_i^r}{\partial z_i} = 1-\left(y_i^r\right)^2; \qquad (2.40)$$

$$\frac{\partial y_s^{(j)}}{\partial z_s^{(j)}} = 1-\left(y_s^{(j)}\right)^2, \qquad (2.41)$$

де $y_s^{(j)}$ – вихідний сигнал s-го нейрона j-го шару.

Підставивши вирази (2.18)–(2.21), (2.40), (2.41) у (2.27), отримаємо:

$$\Delta w_{k,s}^{(j)} = -\gamma_{k,s}^{(j)} \sum_{i=1}^{M} \left(-\frac{2\left(y_i - y_i^r\right)}{y_i^2} \left(1 - \left(y_i^r\right)^2\right) w_{s,i}^{j+1} y_s^{(j)} \left(1 - \left(y_s^{(j)}\right)^2\right) y_k^{(j-1)} \right).$$

Після тривіальних спрощень отримаємо кінцевий вираз для розрахунку величини корегування зв'язку між *s*-м нейроном останнього *j*-го схованого шару та *k*-м нейроном попереднього шару:

$$\Delta w_{k,s}^{(j)} = 2\gamma_{k,s}^{(j)} \sum_{i=1}^{M} \left(\frac{2\left(y_i - y_i^r\right)}{y_i^2} \left(1 - \left(y_i^r\right)^2\right) w_{s,i}^{(j+1)} y_s^{(j)} \left(1 - \left(y_s^{(j)}\right)^2\right) y_k^{(j-1)} \right). \qquad (2.42)$$

Використавши рівність (2.25), вираз (2.42) для розрахунку локальної помилки зв'язку схованих нейронів перепишемо так:

$$\Delta w_{k,s}^{(j)} = 2\gamma_{k,s}^{(j)} \left(1 - \left(y_s^{(j)}\right)^2\right) y_k^{(j-1)} \sum_{i=1}^{M} \left(\delta_s^{(j+1)} w_{s,i}^{(j+1)}\right). \qquad (2.43)$$

Узагальнивши вирази (2.25, 2.35), отримаємо розрахункові вирази для визначення локальної помилки та величини корегування вагових коефіцієнтів для вхідних зв'язків довільного *g*-го шару нейронів з використанням гіперболічного тангенса:

$$\delta_{k,s}^{g} = \left(1 - \left(y_s^{(g)}\right)^2\right) \sum_{i=1}^{M} \delta_s^{(g+1)} w_{s,i}^{(g+1)}; .$$

$$\Delta w_{k,s}^{(g)} = 2\gamma_{k,s}^{(g)} \left(1 - \left(y_s^{(g)}\right)^2\right) y_k^{(g-1)} \sum_{i=1}^{M} \left(\delta_s^{(g+1)} w_{s,i}^{(g+1)}\right).$$

З метою верифікації отриманих результатів проведено експерименти, у яких БШП застосовано для моделювання поліноміальних функцій, у яких мінімальні та максимальні значення аргументів відрізнялись між собою в 100 разів. Різниця між мінімальними та максимальними значеннями області визначення функції є характерною для ПБ багатьох об'єктів захисту інтернет-орієнтованих ІС.

Наприклад, таким ПБ може бути завантаження каналу зв'язку веб-сервера. Як ілюстрацію на рис. 2.7–2.12 зображено графіки абсолютної та відносної помилок навчання та екстраполяції функції $y = x^3 + x^2 + x$, апроксимованої ДШП із класичним та модифікованим алгоритмом навчання. Визначено, що оптимальна кількість схованих нейронів у ДШП дорівнює 12.

На рис. 2.7–2.12 позначено: *1* – графіки, отримані з використанням класичного алгоритму навчання, а цифрою *2* позначено графіки, які відповідають модифікованому алгоритму.

Вісь ординат на графіках рис. 2.7, 2.9, 2.11 відповідає абсолютній помилці навчання Δ, а на графіках рис. 2.8, 2.10, 20.12 – зведеній помилці навчання δ. На всіх графіках вісь абцис відповідає значенню піддослідної функції *x*.

Як показує аналіз рис. 2.7, 2.8, використання запропонованої модифікації алгоритму зменшує відносну помилку навчання в середньому у 2 рази. При цьому в області малих значень модельованої функції відносна помилка навчання зменшилась приблизно в 10 разів.

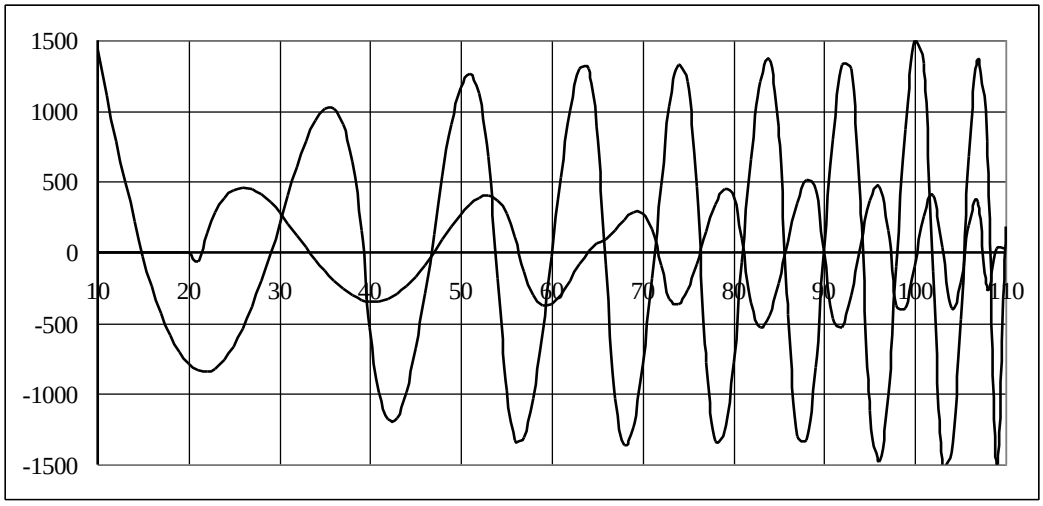

Рис. 2.7. Графіки абсолютної похибки навчання

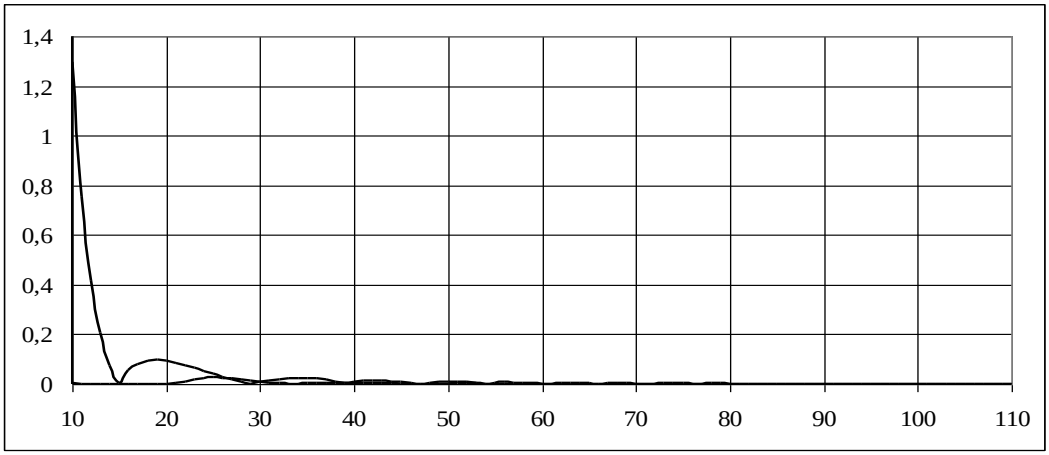

Рис. 2.8. Графіки відносної похибки навчання

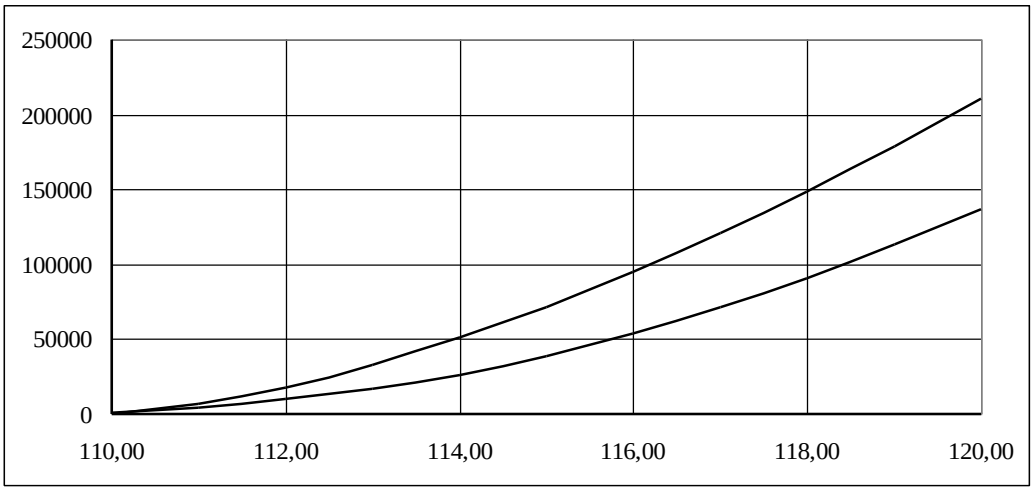

Рис. 2.9. Графіки абсолютної похибки екстраполяції за верхню межу навчальних даних

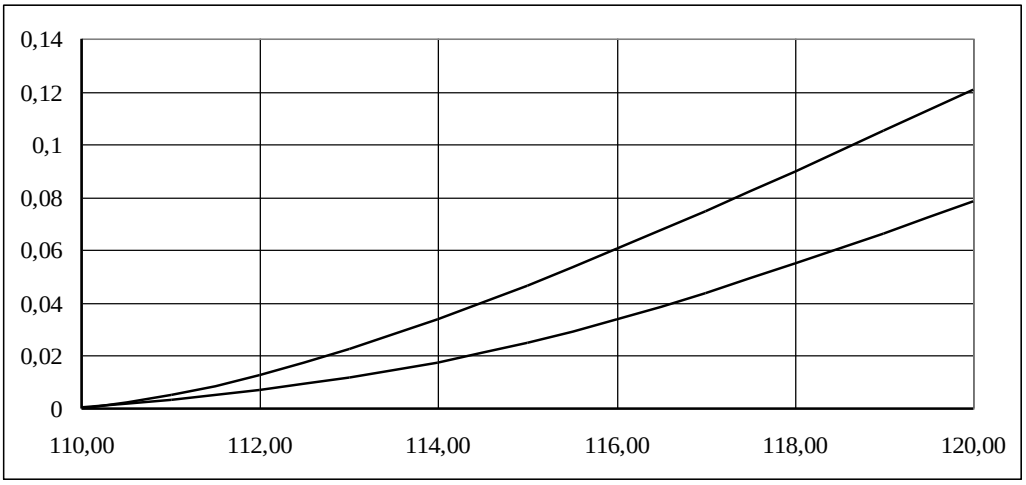

Рис. 2.10. Графіки відносної похибки екстраполяції за верхню межу навчальних даних

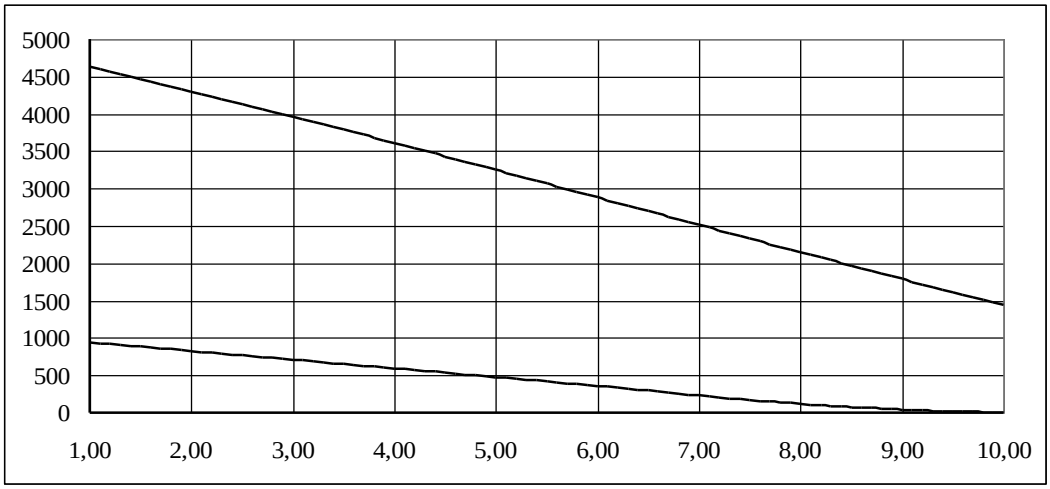

Рис. 2.11. Графіки абсолютної похибки екстраполяції за нижню межу навчальних даних

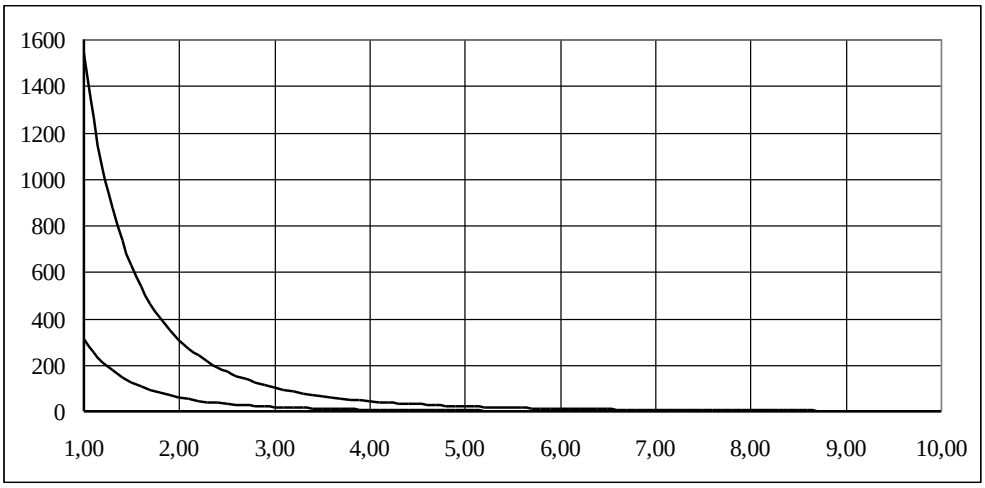

Рис. 2.12. Графіки відносної похибки екстраполяції за нижню межу навчальних даних

Аналіз показаних на рис. 2.9, 2.10 графіків показує, що використання модифікованого алгоритму навчання приблизно в 1,5 разу зменшує похибку екстраполяції за верхню межу навчальних даних. При цьому аналіз графіків, зображених на рис. 2.11, 2.12, свідчить про приблизно семикратне зменшення відносної похибки екстраполяції за нижню межу навчальних даних. Таким чином, результати числових експериментів підтверджують доцільність запропонованої модифікації алгоритму навчання БШП.

2.4. Верифікація нейромережевих моделей оцінювання параметрів безпеки

Як відправний пункт дослідження використано результати праць [33, 49, 140], у яких показано можливість використання НМ для апроксимації із заданою точністю довільної функцій. Так, у праці [33] показано доведення теореми Хехт–Нільсена, у якій подано принципову можливість вираження неперервної довільної функції багатьох змінних за допомогою НМ з прямим поширенням сигналу, що містить щонайменше один СШН. Структурно така НМ складається з N вхідних нейронів щонайменше з $2N+1$ схованих нейронів з сигмоїдальними функціями активації вигляду (2.12), (2.30) і M вихідних нейронів з невідомими функціями активації. У праці [210] результати цієї

теореми дещо розширені. Доведено, що параметри сигмоїдальної функції активації можуть бути задані апріорно, а у вихідному шарі нейронів – використано лінійну функцію активації вигляду:

$$g(x) = ax + b,$$

де g – лінійна функція активації; x – сумарний вхідний сигнал нейрона, a, b – коефіцієнти.

Зазначимо, що описаний тип НММ з одним шаром схованих нейронів отримав назву двошароовго персептрона, а з декількома шарами схованих нейронів – багатошарового персептрона [49]. Схожий результат, але вже для НММ типу РБФ, отримано в роботах Д. Парка та І. Сандберга [33]. Доведено, в разі виконання певних структурних правил (достатня кількість схованих нейронів), за допомогою РБФ можна апроксимувати довільну гладку функцію. Отже, теоретичній верифікації підлягають НММ типу БШП або РБФ.

Оскільки стан захищеності ІС залежить від подій, які в ньому відбуваються, та характеризуються набором певних підконтрольних ПБ, то модель виявлення кібератак можна записати так:

$$\exists\, s(t) \in S_a(t) \wedge p(t) \in P_a(t) \Rightarrow A, \tag{2.44}$$

$$\exists\, s(t) \notin S_n(t) \vee p(t) \notin P_n(t) \Rightarrow A, \tag{2.45}$$

де $s(t)$ – множина подій, що відбулись в ІС; $p(t)$ – множина значень ПБ на момент t; $S_a(t), P_a(t)$ – множина подій та множина значень ПБ, характерних при реалізації атаки; $S_n(t), P_n(t)$ – множина подій та множина значень ПБ, за нормального стану ІС на момент t; A – реалізація кібератаки.

Доповненням до виразів (2.44), (2.45) можуть бути вирази

$$\exists\, s(t) \notin S_a(t) \wedge p(t) \notin P_a(t) \Rightarrow N; \tag{2.46}$$

$$\exists\, s(t) \in S_n(t) \wedge p(t) \in P_n(t) \Rightarrow N, \tag{2.47}$$

де N – нормальний стан захищеності РІС,

за допомогою яких можна виявити нормальний стан захищеності ІС.

Метод виявлення кібератак на основі (2.44), (2.45) отримав назву «виявлення зловживань», а метод виявлення кібератак на основі (2.46), (2.47) –

«виявлення аномалій» [37]. Використавши вирази (2.44)–(2.47), узагальнювальну модель виявлення кібератаки виразимо неперервною функцію багатьох змінних:

$$\begin{cases} U = F(s(t), p(t), S_a(t), S_n(t), P_a(t), P_n(t)); \\ U \in (A, N). \end{cases} \quad (2.48)$$

Подібну модель виявлення кібератак на ІС використано у праці [48]. При цьому модель (2.48), як і моделі (2.44)–(2.47), має узагальнений характер. У багатьох випадках для виявлення атак використовуються лише окремі компоненти.

У підсумку застосування до функціонала (2.46) теореми Хехт–Нільсена та результатів Д. Парка та І. Сандберга дозволяє стверджувати, що за допомогою БШП та РБФ можна із заданою точністю розпізнати кібератаки на ІС. При цьому необхідною умовою для верифікації НММ є можливість подання ПБ у вигляді неперервних функцій.

Розглянемо використання отриманого результату на конкретному прикладі.

Дано: базу даних KDD-99, яка містить приклади нормального функціонування ІС та сигнатури мережевих кібератак.

Довести: гарантованість розпізнавання представлених мережевих кібератак за допомогою нейромережевих моделей типу БШП і РБФ.

Розв'язання. База даних KDD-99 містить близько 5000000 записів – образів мережевих з'єднань, зареєстрованих через певні проміжки часу [18]. 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 і т.ін. У 42-му полі записано інформацію, що характеризує стан захищеності ІС – або відсутність атаки (normal), або її тип. У базі міститься 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 та сканування портів (Probe). Тому для виявлення кібератак можна використати тільки величини 41 ПБ (параметри мережевого трафіку), множина виявлених атак складається із 22 елементів (видів атак), множина нормальних станів – з одного елемента. Це дозволяє переписати (2.44) у вигляді функції

$$\begin{cases} U = F(p_1, p_2, \ldots p_{41}), \\ U \in (A_1, A_2, \ldots A_{22}, N_1\}, \end{cases} \tag{2.49}$$

де $p_1, p_2, \ldots p_{41}$ – ПБ; $A_1, A_2, \ldots A_{22}$ – види мережевих кібератак; N_1 – нормальний стан ІС.

Застосування до функції (2.49) теореми Хехт-Нільсена і результатів Д. Парка та І. Сандберга показує можливість використання БШП і РБФ для виявлення кібератак.

Розділ 3. МОДЕЛІ ОЦІНЮВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ІНТЕРНЕТ-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

3.1. Модель процесів інтеграції параметрів безпеки, що використовуються нейромережевими засобами розпізнавання кібератак

Для створення моделі оцінюванняя параметрів, які використовуються у НМЗ розпізнавання кібератак, застосовано три множини – множину можливих кібератак $\boldsymbol{Ka}$, множину можливих ПБ $\boldsymbol{X}$ та множину вихідних параметрів НМ $\boldsymbol{Y}$. У загальному випадку

$$\mathrm{Ka} = \bigcup_{j=1}^{J} Ka_j , \tag{3.1}$$

$$\mathrm{X} = \bigcup_{i=1}^{I} X_i , \tag{3.2}$$

$$\mathrm{Y} = \bigcup_{g=1}^{G} Y_g , \tag{3.3}$$

де Ka_j – j-а кібератака; J, G, I – кількість можливих кібератак, вихідних параметрів НММ і ПБ; Y_g – g-й вихідний параметр, X_i – i-й ПБ.

Кожному елементу (типу кібератаки) множини $\boldsymbol{Ka}$ поставлено у відповідність підмножину вихідних параметрів $\boldsymbol{Y}_N$ (значення яких свідчать про наявність кібератаки), що складається з елементів множини $\boldsymbol{Y}$. У свою чергу, кожній $\boldsymbol{Y}_N$ поставлено у відповідність підмножину вхідних параметрів $\boldsymbol{X}_V$ (необхідних для виявлення кібератаки), яка складається з елементів множини $\boldsymbol{X}$. Таким чином, для виявлення кібератаки слід сформувати множини трійок «вхідні параметри→вихідні параметри→ кібератака»:

$$\begin{aligned}
&\mathrm{X}_V \to \mathrm{Y}_N \to \mathrm{Ka} = \bigcup_{i=1}^{V_j} X_i \to \bigcup_{g=1}^{N_j} Y_g \to \bigcup_{j=1}^{J} Ka_j = \\
&= (\{X_{1,1}, X_{1,2}, \ldots X_{1,V_1}\} \to \{Y_{1,1}, Y_{1,2}, \ldots Y_{1,N_1}\} \to Ka_1), \\
&(\{X_{1,1}, X_{1,2}, \ldots X_{1,V_1}\} \to \{Y_{1,1}, Y_{1,2}, \ldots Y_{1,N_1}\} \to Ka_1), \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&(\{X_{J,1}, X_{J,2}, \ldots X_{J,V_J}\} \to \{Y_{J,1}, Y_{J,2}, \ldots Y_{J,N_J}\} \to Ka_J).
\end{aligned} \tag{3.4}$$

Використання НМ передбачає, що множини $\boldsymbol{X}$ і $\boldsymbol{Y}$ визначені на $[0..1]$. За відомих трійок (3.4) виявлення кібератаки *k*-го типу зводиться до встановлення відповідності між поточними величинами вхідних параметрів $\{x_{k,1}, x_{k,2}, ... x_{k,V_k}\}$ та величинами множинами вхідних параметрів $\{X_{k,1}, X_{k,2}, ... X_{k,V_k}\}$, які відповідають величинзначенням вихідних параметрів $\{Y_{k,1}, Y_{k,2}, ... Y_{k,N_k}\}$, що свідчать про Ka_k:

$$\{x_{k,1}, x_{k,2} ... x_{k,V_k}\} \cong \{X_{k,1}, X_{k,2} ... X_{k,V_k}\} \Rightarrow \{Y_{k,1}, Y_{k,2} ... Y_{k,N_k}\} \Rightarrow Ka_k. \quad (3.5)$$

Модель (3.4) деталізовано з урахуванням розроблених підходів до розпізнавання НК і ПК. Для цього множину можливих кібератак подано у вигляді:

$$\boldsymbol{Ka} = (\boldsymbol{Ks}, \boldsymbol{Kq}), \quad (3.6)$$

де $\boldsymbol{Ks}, \boldsymbol{Kq}$ – відповідно множина поступових та несподіваних кібератак.

Множину вхідних параметрів $\boldsymbol{X}$ також поділено на дві частини:

$$\boldsymbol{X} = (\boldsymbol{Xs}, \boldsymbol{Xq}), \quad (3.7)$$

де $\boldsymbol{Xs}$ – множина ПБ, що використовується для розпізнавання ПК; $\boldsymbol{Xq}$ – множина ПБ, що використовуються для розпізнавання НК.

Підставивши вирази (3.6), (3.7) у (3.5), отримаємо:

$$\{xs_{k,1}, xs_{k,2} ... xs_{k,V_k}\} \cong \{Xs_{k,1}, Xs_{k,2} ... Xs_{k,V_k}\} \rightarrow \{Ys_{k,1}, Ys_{k,2} ... Ys_{k,N_k}\} \rightarrow Ks_k; \quad (3.8)$$

$$\{xq_{k,1}, xq_{k,2} ... xq_{k,V_k}\} \cong \{Xq_{k,1}, Xq_{k,2} ... Xq_{k,V_k}\} \rightarrow \{Yq_{k,1}, Yq_{k,2} ... Yq_{k,N_k}\} \rightarrow Kq_k. \quad (3.9)$$

За виразами (3.8), (3.9) можна визначити модель нейромережевої оцінки вхідних параметрів для виявлення *k*-ї ПК чи НК у такому вигляді:

$$\{xs_{k,1}, xs_{k,2} ... xs_{k,V_k}\}[nnet]\{Xs_{k,1}, Xs_{k,2} ... Xs_{k,V_k}\} \rightarrow \{Ys_{k,1}, Ys_{k,2} ... Ys_{k,N_k}\}, \quad (3.10)$$

$$\{xq_{k,1}, xq_{k,2} ... xq_{k,V_k}\}[nnet]\{Xq_{k,1}, Xq_{k,2} ... Xq_{k,V_k}\} \rightarrow \{Yq_{k,1}, Yq_{k,2} ... Yq_{k,N_k}\}, \quad (3.11)$$

де $[nnet]$ – оператор нейромережевого порівняння.

Ураховуючи (3.10), (3.11), узагальнені вирази для нейромережевої оцінки поточних вхідних параметрів можна подати так:

$$xs_i[nnet]Xs_i \rightarrow Ys_i; \quad (3.12)$$

$$xq_i[nnet]Xq_i \to Yq_i. \quad (3.13)$$

Згідно з розробленим підходом до розпізнавання ПК та результатами [40] у виразі (3.12) необхідно врахувати залежності xs_i і Xs_i від терміну експлуатації. Тому

$$xs_i(t)[nnet]Xs_i(t) \to Ys_i. \quad (3.14)$$

Отжеу разі виявлення ПК НМ потрібно застосовувати для класифікації часових рядів даних, що відповідно до праці [124] може зумовити значні труднощі.

Для подолання цих труднощів запропоновано проводити попередньо обробляти поступово ПБ для позбавлення їх часової залежності. Відповідно до результатів [21–23] визначити часову залежність пропонується за допомогою додаткової марковської моделі поступових ПБ. Це дозволяє видозмінити виразм (3.14) так:

$$(xs_i(t) - \overline{Xs}_i(t))[nnet](Xs_i(t) - \overline{Xs}_i(t)) \to Ys_i, \quad (3.15)$$

де $\overline{Xs}_i(t)$ – розрахована за допомогою марківської моделі величина ПБ у момент часу t.

Для розроблення ефективних НМЗ оцінювання ПБ ІС з метою виявлення кібератак необхідно визначити номенклатуру вхідних параметрів НММ з урахуванням таких чинників:

– використання як вхідні параметри НММ великої кількості ПБ ІС значно збільшує обсяг обчислювальних ресурсів та ускладнює процес нагромадження навчальних прикладів;

– використання малоінформативних ПБ призводить до навчання НММ на зашумлених даних, що негативно впливає на правильність класифікації невідомих прикладів та збільшує обсяг обчислювальних ресурсів;

– вилучення із вхідних параметрів НММ інформативних ПБ може спричинити повну втрату її класифікаційних властивостей.

Результати праць [59, 86] показують, що остаточне рішення про номенклатуру вхідних параметрів НМ приймається в результаті досить

тривалих порівняльних експериментів. Для зменшення кількості цих експериментів доцільно визначити важливість кожного з можливих ПБ.

Оскільки сучасні формалізовані методи оцінювання важливості ПБ не відповідають вимогам точності [88], прийнято рішення про застосування експертного оцінювання. Пропонується використати метод парних порівняньз огляду на його доведену ефективність у випадках великої кількості піддослідних об'єктів, з якими асоціюються ПБ [90].

Вхідними даними моделі є вектор, елементами якого є матриці експертних оцінок вагомості ПБ:

$$\overline{T} = \{E_1, E_2, ...E_M\}, \tag{3.16}$$

де E_m – матриця оцінок *m*-го експерта; M – кількість експертів.

У свою чергу матриця оцінок має такий вигляд:

$$E_m = \begin{vmatrix} e_{1,1} & \dots & e_{1,j} & \dots & e_{1,N} \\ \dots & \dots & \dots & \dots & \dots \\ e_{i,1} & \dots & e_{i,j} & \dots & e_{j,N} \\ \dots & \dots & \dots & \dots & \dots \\ e_{N,N} & \dots & e_{N,j} & \dots & e_{N,N} \end{vmatrix}, \tag{3.17}$$

де $e_{i,j}$ – оцінка *i*-го ПБ відносно *j*-го параметра; *N* – кількість ПБ.

Для заповнення матриці (3.17) експерт повинен попарно порівняти вагомості ПБ. Якщо експерт вважає, що *i*-й ПБ вагоміший від *j*-го параметраа, то $e_{i,j} = 1$. У противному випадку $e_{i,j} = 0$. Оскільки порівняння значущості параметра з самим собою беззмістовне, то діагональ матриці (3.17) не заповнюється. Приклад заповнення M експертами відповідних матриць оцінок ПБ наведено в табл. 3.1.

У підсумку в узагальненому вигляді вхідні дані моделі являють собою тривимірний масив вигляду:

$$\boldsymbol{C} = \{c_{1,1,1}, ...c_{i,j,k}, ...c_{N,N,M}\}, \tag{3.18}$$

де $c_{i,j,k}$ – виставлена *k*-м експертом оцінка порівняння *i*-го та *j*-го ПБ.

Таблиця 3.1

Оцінка ПБ

Експерт	ПБ	x_1	x_n	x_N
1	x_1	–	1	1
	x_n	0	–	1
	x_N	0	0	–
m	x_1	–	0	1
	x_n	1	–	1
	x_N	0	0	–
M	x_1	–	1	1
	x_n	0	–	1
	x_N	0	0	–

Результатом оцінювання вагомості ПБ є вектор коефіцієнтів вагомості:

$$\overline{\mathrm{B}} = \{\beta_1, \beta_2, .. \beta_N\}, \tag{3.19}$$

де β_i – коефіцієнт вагомості *i*-го ПБ.

Узагальнено процес оцінювання вагомості ПБ можна записати у вигляді функції:

$$f : \boldsymbol{C} \to \overline{\boldsymbol{B}}\,. \tag{3.20}$$

Основу математичного забезпечення перетворення (3.20) становлять наступні вирази:

$$\beta_i = \frac{s_i}{\sum_{i=1}^{N} s_i}, \tag{3.21}$$

$$s_j = \sum_{j=1}^{M} c_{i,j}^{\Sigma}\,, \tag{3.22}$$

де $c_{i,j}^{\Sigma}$ – елемент матриці переваг C^{Σ}; s_i – значущість *i*-го ПБ.

Елементи матриці переваг розраховуються так:

$$c_{i,j}^{\Sigma} = \sum_{m=1}^{M} c_{i,j,m} \,. \tag{3.23}$$

Приклад матриці переваг, заповненої за даними табл. 3.1 за умови, що $M = 3$ і $N = 3$, подано у вигляді табл. 3.2.

Для перевірки правильності визначення коефіцієнтів вагомості значущості можна скористатися умовою нормування:

$$\sum_{i=1}^{N} \beta_i = 1. \tag{3.24}$$

Крім розрахунку коефіцієнтів вагомості, математичне забезпечення оцінювання важливості ПБ включає в себе вираз для визначення ступеня узгодженості експертних даних:

$$\begin{cases} \textit{якщо } W > 0{,}5 \Rightarrow \textit{експертні дані узгоджені,} \\ \textit{якщо } W \le 0{,}5 \Rightarrow \textit{експертні дані не узгоджені,} \end{cases} \tag{3.25}$$

де W – коефіцієнт конкордації, $W \in [0,1]$

Таблиця 3.2

Приклад матриці переваг

Експерт	ПБ		
	x_1	x_2	x_3
1	1	2	3
2	2	1	3
3	1	2	3

У випадку неузгодженості експертних даних процедуру експертного оцінювання слід повторити. При цьому розрахунок коефіцієнта конкордації реалізується за допомогою натакихступних виразів:

$$W = \frac{12L}{M^2(N^3 - N)}; \tag{3.26}$$

$$L = \sum_{n=1}^{N} (r_n - r_{\text{сер}})^2; \tag{3.27}$$

$$r_{\text{сер}} = 0{,}5M(N+1); \tag{3.28}$$

$$r_n = \sum_{m=1}^{M}\sum_{i=1}^{N} c_{n,i,m}, n = 1,2...N, \tag{3.29}$$

де W – коефіцієнт конкордації; r_n – сумарний ранг оцінок n-го ПБ усіма експертами; $r_{\text{сер}}$ – середній ранг експертних оцінок вагомості ПБ; L – коефіцієнт відхилення сумарних рангів від середнього.

Як вхідні параметри НМЗ потрібно використовувати лише ті ПБ, для яких коефіцієнт вагомості більший від заданого мінімального значення ($\beta_{\min}$). Тобто

$$\textit{якщо } \beta_i > \beta_{\min} \Rightarrow i-\textit{й параметр використовувати доцільно}. \tag{3.30}$$

У результаті розроблено модель процесів інтеграції ПБ ІС, що використовується для розпізнавання ПК та НК (рис.3.1). Вхідною інформацією моделі є введена множина характеристик об'єкту захисту ***O***, що визначається виразом (2.4), а виходом моделі є – ПБ, оцінювання яких дозволяє визначити ПК і НК, характерні для об'єкта захисту ІС. Модель складається із п'яти базових процесів, що співвідносяться з процесами інтеграції.

Процес 1 – визначення початкових параметрів у результаті аналізу множини ***O***. Початковими параметрами є множина кібератак, характерних для об'єкта захисту ІС $\{Ka\}_K$ та множина підконтрольних ПБ $\{x\}_N$, де K – кількість кібератак; N – кількість ПБ.

Процес 2 – класифікація ПБ. Результатом цього процесу є визначення із $\{x\}_N$ множини ПБ, придатних для розпізнавання НК $\{xq\}$, та множини ПБ, придатних для розпізнавання ПК $\{xs\}$.

На підставі розроблених підходів придатність n-го ПБ розпізнавати ПК і НК визначається за вирами:

$$if\ x_n \neq f(t) \rightarrow x_n \in \{xq\}; \tag{3.31}$$

$$if\ x_n = f(t) \rightarrow x_n \in \{xs\}. \tag{3.32}$$

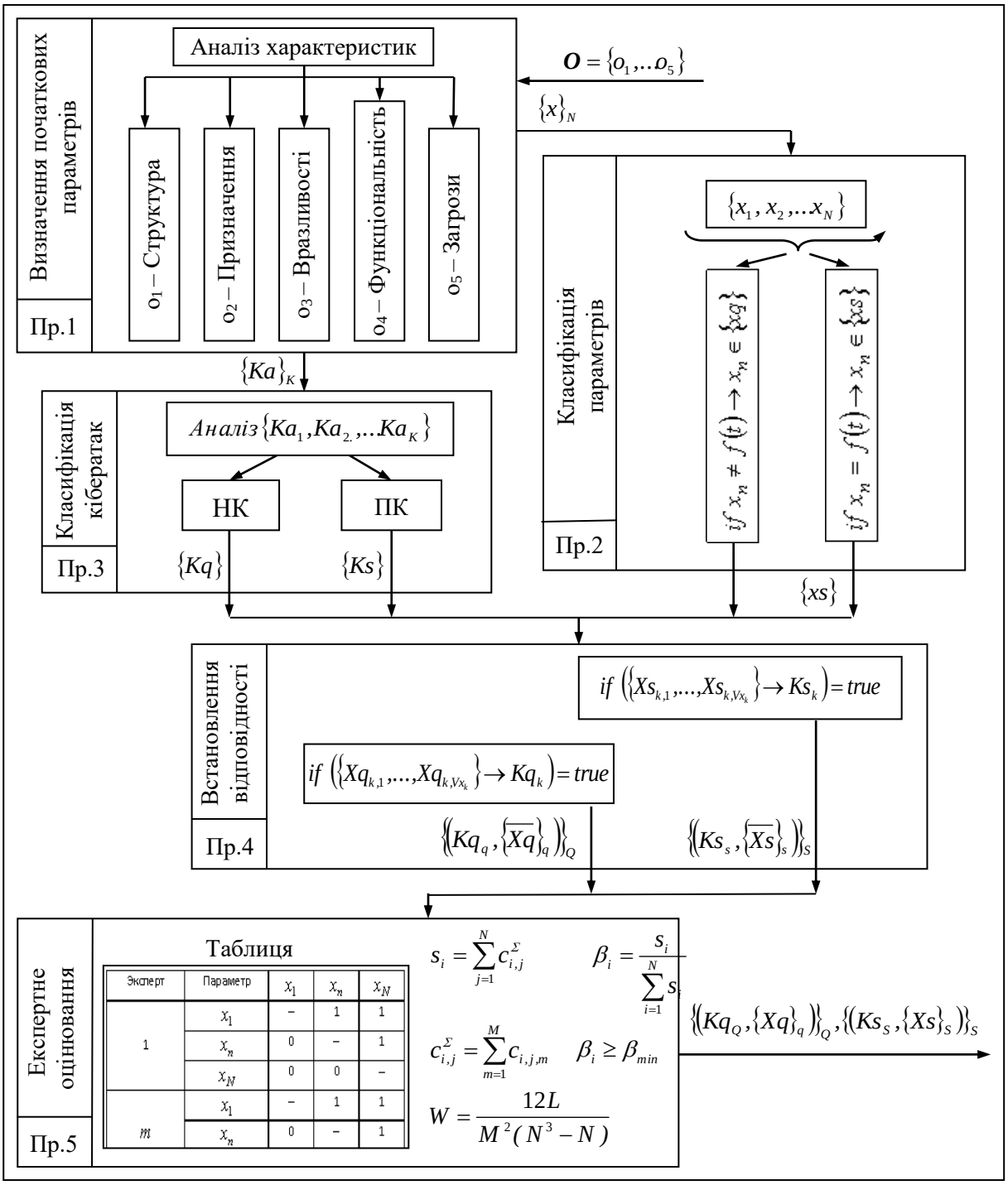

Рис. 3.1. Відображення моделі процесів інтеграції параметрів безпеки

Процес 3 – класифікація кібератак. Процес орієнтований на аналіз $\{Ka\}_K$ для виділення множини НК $\{Kq\}$ та множини ПК $\{Ks\}$. У процесі аналізу використовуються підходи до розпізнавання НК і ПК.

Процес 4 – установлення відповідності. Уцьому процесі в першому наближенні для кожної можливої кібератаки встановлюється відповідність з

множиною ПБ, які можуть використовуватись як вхідні параметри НММ. Відповідність установлюється, якщо для *k*-го виду ПК та/або НК справедливими є вирази:

$$if\left(\left\{Xs_{k,1},...,Xs_{k,Vx_k}\right\}\rightarrow Ks_k\right)=true; \tag{3.33}$$

$$if\left(\left\{Xq_{k,1},...,Xq_{k,Vx_k}\right\}\rightarrow Kq_k\right)=true, \tag{3.34}$$

де $\left\{Xs_{k,1},...,Xs_{k,Vx_k}\right\}$, $\left\{Xq_{k,1},...,Xq_{k,Vx_k}\right\}$ – множини ПБ, що використовуються для розпізнавання ПК і НК; Vx_k – кількість ПБ, що використовуються для розпізнавання *k*-го виду ПК та/або НК.

Виходом процесу є визначені в першому наближенні $\left\{\left\langle Kq_q,\left\{\overline{Xq}\right\}_q\right\rangle\right\}_Q$ і $\left\{\left\langle Ks_s,\left\{\overline{Xs}\right\}_s\right\rangle\right\}_S$, де *Q*, *S* – кількість можливих НК іПК.

Процес 5 – експертне оцінювання. У результаті реалізації цього процесу остаточно визначається множина ПБ, використовувана як вхідні параметри НМЗ. Для цього методом парних порівнянь оцінок експертних даних за допомогою виразів (3.16)–(3.30) розраховуються ПБ, які доцільно використовувати для розпізнавання. Для *k*-ї кібератаки вихід процесу задається виразом $\left\langle K_k,\left\{X\right\}_k\right\rangle$, де $\left\{X\right\}_k$ – множина вагомих ПБ. Слід зазначити, що процеси 1–4 можуть реалізовуватись за допомогою наведеного методу парних порівнянь відповідно до виразів (3.16)–(3.30). Можна застосовувати й інші методи оцінювання експертних даних, наведені в працях [88, 90].

Розроблену модель використано для визначення ПБ, які можуть застосовуватись в НМЗ антивірусних сканерів для виявлення веб-орієнтованих скриптових вірусів, написаних мовою програмування JavaScript. Зазначимо, що, відповідно специфіки антивірусних сканерів як ПБ використовуються назви операторів мови програмування JavaScript, отримані в результаті аналізу програмного коду веб-сторінки [169]. Результати [46] вказують на можливість використання в НМ одного вихідного параметра, величина якого свідчать про наявність певного скриптового вірусу. Тому вирази (3.1)–(3.3)

трансформуються так:

$$Ka = \{\, скриптовий\ вірус\ 1, \ldots, скриптовий\ вірус\ J \,\}, \tag{3.35}$$

$$X = \{\, оператор 1, \ldots, оператор\ I \,\}, \tag{3.36}$$

$$Y = \{\, вихідний\ параметр\ 1 \,\}, \tag{3.37}$$

де J – кількість скриптових вірусів, які можуть бути розпізнані; I – кількість операторів мови програмування JavaScript.

Значення ПБ не залежать від часу, а про реалізацію кібератаки (наявність вірусу) свідчить певна комбінація їх значень, яка щодо апроксимації статистичних даних має неочікуваний характер. Тому виявлення веб-орієнтованих вірусів класифіковано як виявлення НК, а в оцінюванні ПБ враховано, що $\boldsymbol{Ka} = \boldsymbol{Kq}$, $\boldsymbol{X} = \boldsymbol{Xq}$ і використано вирази (3.11), (3.13), (3.15). Для зменшення обсягу аналізованих НМ вхідних параметрів використано задану виразами (3.16)–(3.30) процедуру експертного оцінювання вагомості параметрів. У виразі (3.30) прийнято, $\beta_{\min} = 0{,}5$. У кінцевому підсумку визначено множина вхідних параметрів, які відповідають назвам потенційно небезпечних операторів JavaScript.

3.2. Марковська модель одноперіодичного шаблону поведінки

Відповідно до розробленого одноперіодичного ШП марковська модель повинна описувати нестаціонарний процес $X = f(t)$, який послідовно зростає на стаціонарних інтервалах типу $B_d A_{d+1}$ і спадає на стаціонарних інтервалах типу $A_{d+1} B_{d+2}$, де d – номер перехідної точки (див. рис. 2.4). Тому розроблена марковська модель одноперіодичного ШП M_{BAB} складається із двох однорідних ланцюгів маркова (ЛМ) M_{BA} і M_{AB}, призначених для моделювання ПБ на стаціонарних інтервалах типу $B_d A_{d+1}$ і $A_{d+1} B_{d+2}$ відповідно. Структуру розробленої моделі M_{BAB} показано на рис. 3.2.

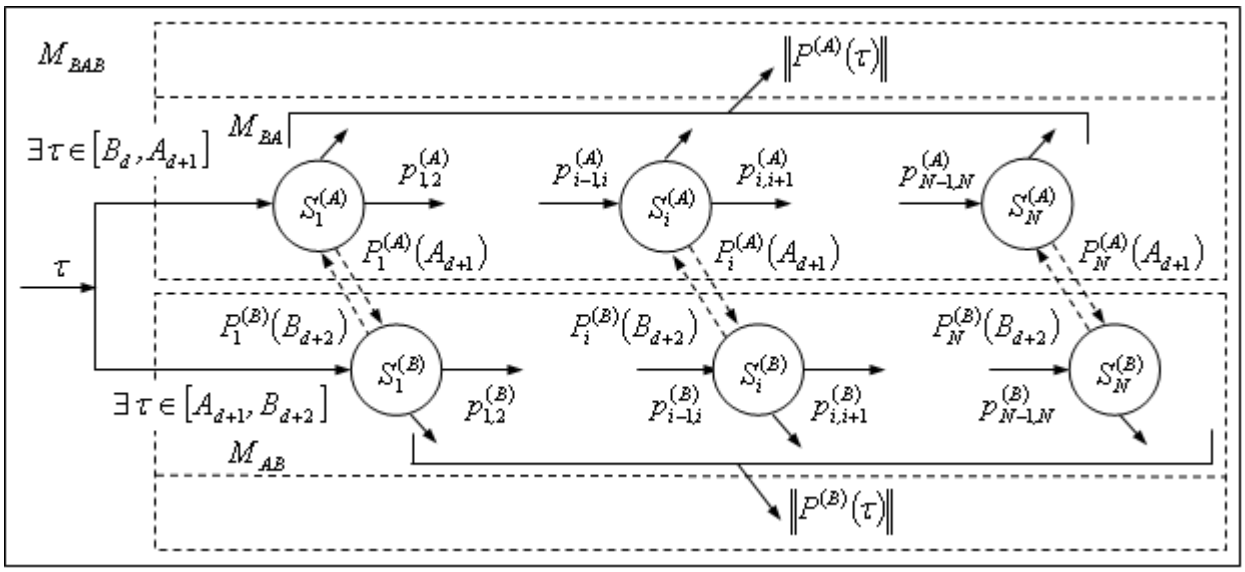

Рис. 3.2. Марковська модель одноперіодичного шаблону поведінки:

τ – крок розрахунку; $S_i^{(A)}$ та $S_i^{(A)}$ – *i*-й стан M_{BA} і M_{AB}; $p_{i,i+1}^{(A)}$ і $p_{i,i+1}^{(B)}$ – імовірність переходу з *i*-го в *(i+1)*-й стан для M_{BA} і M_{AB}; $P_i^{(A)}(A_{d+1})$ – імовірність перебування процесу в *i*-му стані для M_{BA} у перехідній точці (d+1); $P_i^{(B)}(B_{d+2})$ – імовірність перебування процесу в *i*-му стані для M_{AB} у перехідній точці (d+2); $\|P^{(A)}(\tau)\|$ – вектор розподілу ймовірностей на τ-му кроці розрахунку для M_{BA}; $\|P^{(B)}(\tau)\|$ – вектор розподілу ймовірностей на τ-му кроці розрахунку для M_{AB}; N – кількість станів M_{BA} та M_{AB}.

Для визначення параметрів M_{BA} і M_{AB} використовуються апріорно розраховані інтервали $B_d A_{d+1}$ та $A_{d+1}B_{d+2}$, кількість та межі станів ЛМ, матриці перехідних імовірностей $\pi^{(A)} = \|p_{i,i+1}^{(A)}\|$ і $\pi^{(B)} = \|p_{i,i+1}^{(B)}\|$ та вектор початкового розподілу імовірностей $\|P^{(A)}(0)\| = \langle P_1^{(A)}(0), P_2^{(A)}(0), \ldots, P_N^{(A)}(0)\rangle$. Поточний час моделювання:

$$t = \tau\Delta t, \tag{3.38}$$

де Δt – тривалість кроку моделювання.

Для обчислення ймовірностей станів ЛМ M_{BA} (M_{AB}) використовується система рівнянь Колмогорова–Чепмена:

$$\left\|P^{(A)}(\tau)\right\| = \left\|P^{(A)}(\tau-1)\right\|\pi^{(A)}; \quad (3.39)$$

$$\left\|P^{(B)}(\tau)\right\| = P\left\|^{(B)}(\tau-1)\right\|\pi^{(B)}, \quad (3.40)$$

де $\left\|P^{(A)}(\tau)\right\|$ ($\left\|P^{(B)}(\tau)\right\|$) – вектор імовірностей станів M_{BA}(M_{AB}) на τ-му кроці розрахунку.

Використовуються також умови нормування:

$$\sum_{i=1}^{N} P_i^{(A)} = 1;$$

$$\sum_{i=1}^{N} P_i^{(B)} = 1.$$

Якщо τ переходить з інтервалу $B_d A_{d+1}$ в $A_{d+1}B_{d+2}$, початковий вектор розподілу M_{AB} дорівнює кінцевому вектору розподілу M_{BA}:

$$\left\|P^{(B)}(A_{d+1})\right\| = \left\|P^{(A)}(A_{d+1})\right\|.$$

Якщо τ переходить з інтервалу $A_{d+1}B_{d+2}$ в $B_{d+2}A_{d+3}$ навпаки, початковий вектор розподілу M_{BA} дорівнює кінцевому вектору розподілу M_{AB}:

$$\left\|P^{(A)}(B_{d+2})\right\| = \left\|P^{(B)}(B_{d+2})\right\|.$$

Таким чином, марківська модель M_{BAB} дозволяє моделювати одноперіодичний ШП ПБ ІС.

3.3. Марковська модель багатоперіодичного шаблону поведінки

Розроблення марковської моделі багатоперіодичного ШП грунтується на визначеній у праці [125] можливості подання багатоперіодичного ряду динаміки у вигляді суперпозиції декількох одноперіодичних рядів. Тому розроблена марковська модель багатоперіодичного ШП M_{BAB}^{Σ}, структуру якої показано на рис. 3.3, складається з модулів $M_{BAB}^{(1)}, M_{BAB}^{(2)}, \ldots, M_{BAB}^{(K)}$, призначених для моделювання *K* значущих періодів ШП. Довільний *k*-й модуль $M_{BAB}^{(k)}$ являє собою розроблену в підрозділі 3.2 марковську модель одноперіодичного ШП,

призначену для моделювання *k*-ї періодичної складової.

У першому наближенні для всіх модулів кількість та межі станів ЛМ однакові. У свою чергу, $M_{BAB}^{(k)}$ складається із двох ЛМ – $M_{BA}^{(k)}$ і $M_{AB}^{(k)}$, призначених для моделювання *k*-ї періодичної складової ШП на стаціонарних інтервалах цього періоду $B_d A_{d+1}{}^{(k)}$ і $A_{d+1} B_{d+2}{}^{(k)}$.

Виходом *k*-го модуля $M_{BAB}^{(k)}$ на τ-му кроці розрахунку є $\left\|P^{(k)}(\tau)\right\|$ – вектор розподілу ймовірностей для *k*-ї періодичної складової ШП.

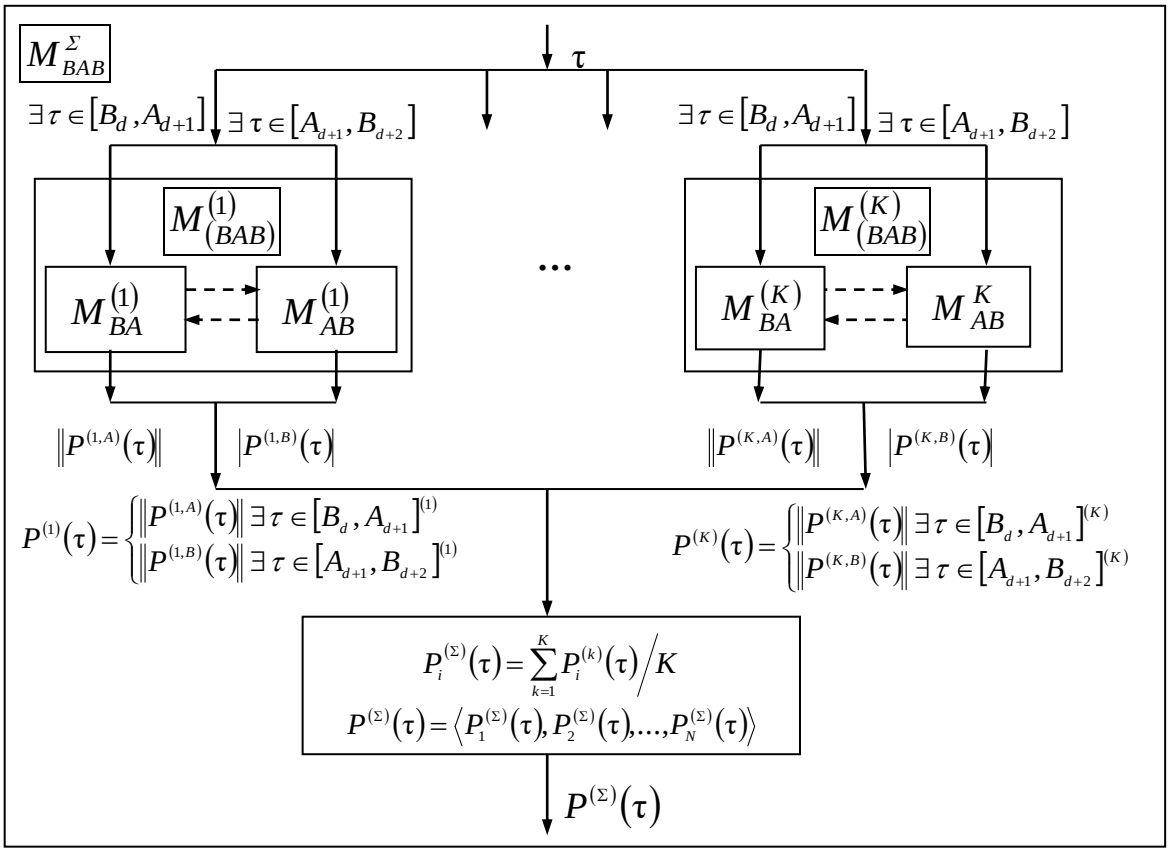

Рис. 3.3. Марковська модель багатоперіодичного ШП ПБ

Виходом моделі M_{BAB}^{Σ} на τ-му кроці розрахунку є інтегральний вектор розподілу ймовірностей вигляду:

$$\left\|P^{(\Sigma)}(\tau)\right\|=\left\langle P_1^{(\Sigma)}(\tau),P_2^{(\Sigma)}(\tau),\ldots,P_N^{(\Sigma)}(\tau)\right\rangle,$$

де $P_i^{(\Sigma)}(\tau)$ – інтегральна ймовірність перебування ПБ в *i*-му стані Л на *τ*-му кроці розрахунку.

У свою чергу, $P_i^{(\Sigma)}(\tau)$ розраховується так:

$$P_i^{(\Sigma)}(\tau) = K^{-1} \sum_{k=1}^{K} P_i^{(k)}(\tau),$$

де $P_i^{(k)}(\tau)$ – імовірність перебування ПБ в *i*-му стані *k*-го ЛМ на τ-му кроці розрахунку.

Розроблені марковські моделі застосовано для створення ШП веб-сервера. Як ПБ *X* використано кількість звернень до веб-сервера. Графіки динаміки математичного сподівання даного ПБ, побудовані на підставі статистичних даних та за допомогою запропонованих марківських моделей M_{BAB} і M_{BAB}^{Σ}, показано на рис. 3.4.

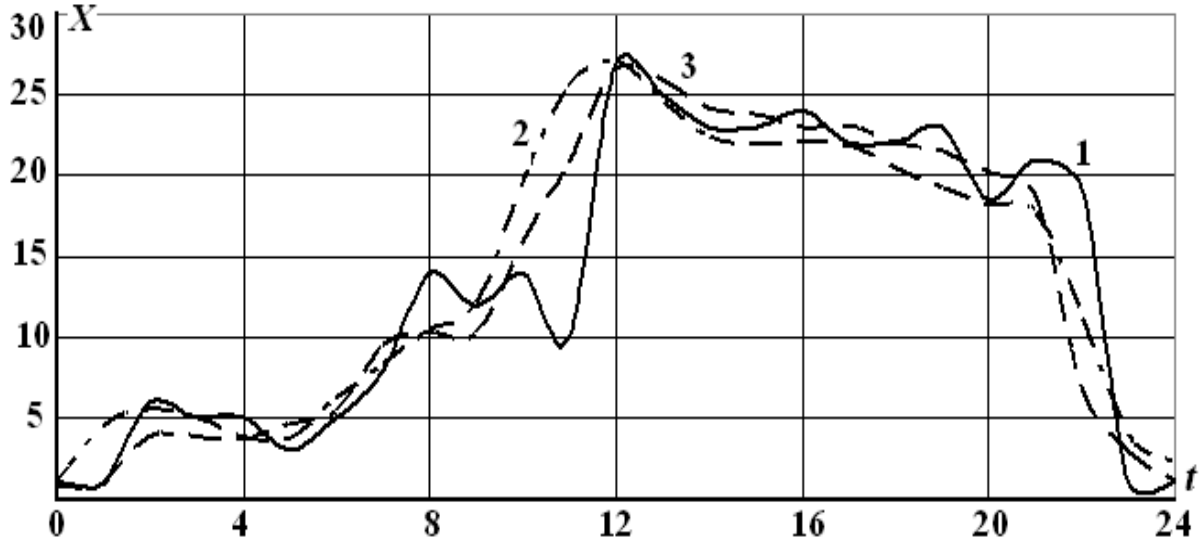

Рис. 3.4. Графіки динаміки математичного сподівання кількості звернень: *1* – графік на основі статистичних даних; *2* – на основі одноперіодичної моделі M_{BAB}; а *3* – на основі двоперіодичної моделі M_{BAB}^{Σ}.

Для одноперіодичної моделі M_{BAB} середня похибка моделювання становить 0,09, а для двоперіодичної моделі M_{BAB}^{Σ} – 0,07. При цьому середня похибка моделювання, розрахована на основі поліноміальних моделей [115], становить 0,14…0,18. Таким чином, застосування моделей M_{BAB} і M_{BAB}^{Σ} дозволяє зменшити похибку моделювання в 1,5–2 рази, що підтверджує доцільність їх застосування.

3.4. Модель на основі багатошарового персептрона

Відповідно до праці [49] розроблення структурної моделі БШП грунтується на визначенні загальної кількості синаптичних зв'язків. За аналогією з підручником [140] в основу такого визначення покладемо критерій мінімізації відносної помилки БШП за дотримання обмежень для актуальних задач оцінювання ПБ:

$$\begin{cases} G_{MLP} \to min, \\ O \le O_d. \end{cases} \tag{3.41}$$

де G_{MLP} – відносна помилка БШП; O_d –обмеження.

Відносна помилка БШП дорівнює відношенню помилки узагальнення ε до кількості синаптичних зв'язків L_w;

$$G_{MLP} = \frac{\varepsilon}{L_w}. \tag{3.42}$$

Перепишемо вираз(3.41) з урахуванням співвідношення (3.42):

$$\begin{cases} \dfrac{\varepsilon}{L_w} \to \min, \\ O \le O_d. \end{cases}.$$

Для визначення точки мінімуму, яка відповідає оптимальній кількості синаптичних зв'язків (L_w^{opt}),розв'яз уємо рівняння

$$\frac{\partial L_w}{\partial \varepsilon} = 0.$$

У дослідженні [49] помилку узагальнення БШП розраховано як сума помилок апроксимації ε_a та опису моделі ε_o

$$\varepsilon = \varepsilon_a + \varepsilon_o. \tag{3.43}$$

Помилка апроксимації (навчання) співвідноситься із запам'ятовуванням БШП навчальних даних, а помилка опису моделі – з узагальненням (стисненням) цих даних. Зазначимо, що як запам'ятовування, і стиснення навчальних даних відбуваються унаслідок зміни вагових коефіцієнтів синаптичних зв'язків.

Вважають [40, 210] , що помилка апроксимації БШП ε_a пропорційна

відношенню кількості синаптичних зв'язків до кількості компонент вхідного вектора N_X:

$$\varepsilon_a \sim \frac{N_X}{L_w}. \tag{3.44}$$

Помилка опису моделі БШП пропорційна відношенню кількості синаптичних зв’язків до кількості навчальних прикладів P:

$$\varepsilon_o \sim \frac{L_w}{P}. \tag{3.45}$$

Узагальнений вираз для оцінки загальної помилки отримаємо, підставивши (3.43) і (3.44) в (3.45):

$$\varepsilon \sim \left(\frac{N_X}{L_w} + \frac{L_w}{P} \right).$$

Після тривіальних перетворень маємо точку максимуму:

$$L_w^{\text{opt}} \sim \sqrt{PN_X}. \tag{3.46}$$

Вираз (3.46) для розрахунку оптимальної кількості синаптичних зв’язків дозволяє перейти до визначення оптимальної кількості схованих нейронів. Зазначимо, що співвідношення між кількістю синаптичних зв’язків та кількістю схованих нейронів БШП задається виразом

$$L_w = N_X N_1 + \sum_{s=1}^{S-1} \left(N_s N_{s+1} \right) + N_S N_Y. \tag{3.47}$$

де N_X – кількість вхідних нейронів; N_1 – кількість нейронів у першому СШН; N_s – кількість нейронів у s-му СШН; N_Y – кількість нейронів у ШВ; S – кількість СШН.

Урахуємо теорему Хехта–Нільсена [33, 34], у якій доведено, що для подання довільної функції достатньо двошарової НМ прямого поширення сигналу з повнозв'язною структурою, що складається з n вхідних нейронів, $(2n+1)$ схованих нейронів і m вихідних нейронів. Це дозволяє спростити модель БШП до ДШП.

Таке спрощення, хоча і суперечить [32, 34] у контексті зменшення

обчислювальних можливостей, однак відповідає таким вимогам до НМ у задачах оцінювання ПБ, як максимальна простота та надійність. Адаптований до ДШП вираз (3.47) виглядає так:

$$L_w = (N_X + N_Y)N_1. \tag{3.48}$$

Для багатьох задач оцінювання ПБ для розпізнавання кібератак вихід НМ може вказувати тільки на ймовірність (впевненість) виникнення очікуваної події, наприклад, реалізації мережевої кібератаки на ІС. Тоді НМ може мати один вихідний елемент ($N_Y = 1$), що зумовлює зміну виразу (3.48):

$$L_w = (N_X + 1) \times N_1.$$

Дорівняємо вираз (3.48) до (3.46). Отримаємо

$$\sqrt{PN_X} \sim (N_X + N_Y)N_1^{\text{opt}},$$

$$N_1^{\text{opt}} \sim \frac{\sqrt{PN_X}}{N_X + N_Y}, \tag{3.49}$$

де N_1^{opt} – оптимальна кількість схованих нейронів у ДШП з довільною кількістю вихідних нейронів.

Для ДШП з одним вихідним зв’язком вираз (3.49) можна спростити так:

$$Ns_1^{\text{opt}} \sim \frac{\sqrt{PN_X}}{N_X + 1}, \tag{3.50}$$

де Ns_1^{opt} – оптимальна кількість схованих нейронів у ДШП з одним вихідним нейроном.

Вирази (3.49), (3.50) являють собою пропорції, а отже, не дозволяють безпосередньо розрахувати оптимальну кількість нейронів у СШН. Для переходу до рівняння введемо у вираз (3.49) коефіцієнт пропорційності:

$$N_1^{opt} = k \frac{\sqrt{PN_X}}{N_X + N_Y}, \tag{3.51}$$

де k – коефіцієнт пропорційності.

Оцінимо коефіцієнт пропорційності. У загальному випадку[34] мінімально допустима кількість схованих нейронів визначається теоремою

Хехта–Нільсена, а максимально допустима кількість обмежується кількістю навчальних прикладів. Тобто

$$N_1^{\min} \geq 2N_X + 1; \tag{3.52}$$

$$N_2^{\max} \leq P, \tag{3.53}$$

де $N_1^{\min}$, $N_2^{\max}$ – мінімальна та максимальна кількість нейронів у СШН.

Порівнявши вирази (3.51) з (3.52) та (3.52) з (3.53), отримаємо

$$\begin{cases} k\dfrac{\sqrt{PN_X}}{N_X + N_Y} \geq 2N_X + 1; \\ k\dfrac{\sqrt{PN_X}}{N_X + N_Y} \leq P. \end{cases}.$$

Як наслідок,

$$\begin{cases} k \geq \dfrac{(2N_X + 1)\times(N_X + N_Y)}{\sqrt{P \times N_X}}, \\ k \leq \dfrac{P \times (N_X + N_Y)}{\sqrt{P \times N_X}}. \end{cases}. \tag{3.53}$$

У теорії НМ [140] вважається доведеним, що кількість навчальних прикладів повинна перевищувати кількість вхідних параметрів ща найменше в 10 разів. Тобто

$$N_X P \geq 10N_X^2. \tag{3.54}$$

Підставивши вираз (3.54) в (3.53), отримаємо

$$\begin{cases} k \geq \dfrac{(2N_X + 1)(N_X + N_Y)}{10N_X}, \\ k \leq \dfrac{P(N_X + N_Y)}{10N_X}; \end{cases}$$

$$\begin{cases} k \geq \dfrac{(2N_X + 1)(N_X + N_Y)}{10N_X}, \\ k \leq \dfrac{PN_X + PN_Y}{10N_X}; \end{cases}$$

$$\begin{cases} k \geq \dfrac{(2N_X + 1)(N_X + N_Y)}{10N_X}, \\ k \leq \dfrac{10N_X^2 + PN_Y}{10N_X}. \end{cases} \tag{3.55}$$

Уточнемо межі діапазону значень коефіцієнта пропорційності з урахуванням специфіки актуальних задач оцінювання ПБ. Як правило, у таких задачах кількість вихідних параметрів не перевищує кількості вхідних параметрів, а кількість навчальних прикладів повинна перевищувати кількість розрізнюваних класів (вихідних параметрів) шайнаменше в 10 разів. Тому, не порушуючи нерівності (3.55), можна вважати, що

$$N_Y \approx N_X; \tag{3.56}$$

$$N_Y P \approx 10N_X^2. \tag{3.57}$$

Після підставлення виразів (3.56), (3.57) в (3.55) отримаємо

$$\begin{cases} k \geq \dfrac{(2N_X + 1)(N_X + N_X)}{10N_X}, \\ k \leq \dfrac{10N_X^2 + 10N_X^2}{10N_X}; \end{cases}$$

$$\begin{cases} k \geq 0{,}4N_X + 0{,}2, \\ k \leq 2N_X. \end{cases} \tag{3.58}$$

Якщо (3.58) підставити у (3.51), тоді вирази для оцінювання діапазону оптимальної кількості схованих нейронів ДШП набудуть вигляду:

$$N_1^{\text{opt}} \geq (0{,}4N_X + 0{,}2)\frac{\sqrt{PN_X}}{N_X + N_Y}; \tag{3.59}$$

$$N_1^{\text{opt}} \leq \frac{2\sqrt{PN_X}}{N_Y}. \tag{3.60}$$

Оскільки у виразах (3.59), (3.60) кількість схованих нейронів має бути цілим числом, отримаємо остаточні розрахункові вирази:

$$N_1^{\text{opt}}(\min) = Round\left((0{,}4N_X + 0{,}2)\frac{\sqrt{PN_X}}{N_X + N_Y}\right); \tag{3.61}$$

$$N_1^{\text{opt}}(\max) = Round\left(2N_Y^{-1}\sqrt{PN_X}\right), \tag{3.62}$$

де $N_1^{\text{opt}}(\max)$, $N_1^{\text{opt}}(\min)$ – максимальна та мінімальна межі діапазону оптимальної кількості схованих нейронів; *Round(X)* – операція визначення найближчого цілого числа від аргумента *X*.

Схема відображення оптимізації структури БШП показано на рис. 3.5.

З урахуванням виразів (3.61), (3.62), для ДШП з одним вихідним нейроном оптимальну кількість схованих нейронів можна оцінити так:

$$Ns_1^{\text{opt}}(\min) = Round\left((0{,}4N_X + 0{,}2)\sqrt{PN_X}\,(N_X + 1)^{-1}\right); \tag{3.63}$$

$$Ns_1^{\text{opt}}(\max) = Round\left(2\sqrt{PN_X}\right), \tag{3.64}$$

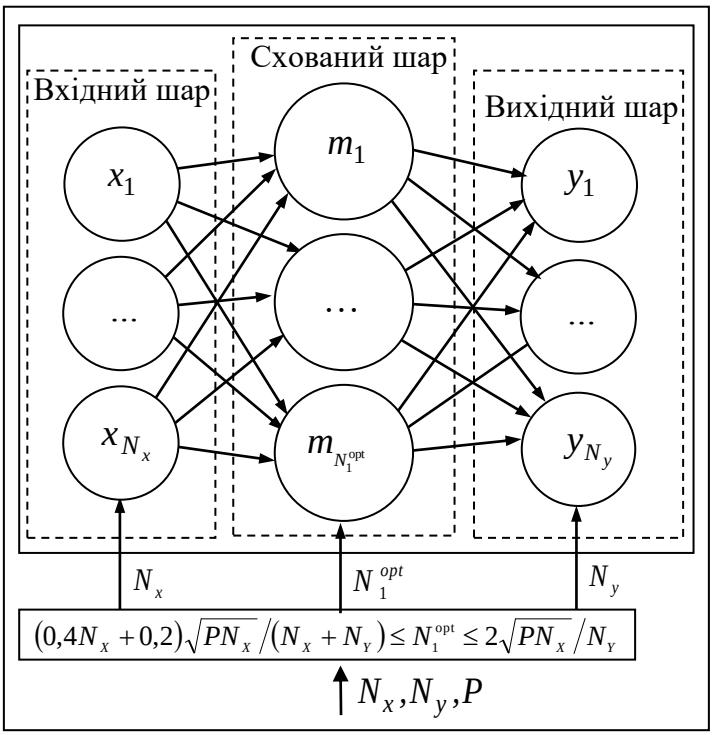

Рис.3.5. Схема оптимізації структури БШП

Для ряду задач оцінювання ПБ кількість вхідних параметрів значно перевищує кількість вихідних параметрів:

$$N_X >> N_Y, N_X >> 1. \tag{3.65}$$

Використання (3.65) дозволяє спроститивирази (3.61)–(3.64) так:

$$N_1^{\text{opt}}(\min) = Round\left((0{,}4N_X + 0{,}2) \times \sqrt{P/N_x}\right), \tag{3.66}$$

$$N_1^{\text{opt}}(\max) = Round\left(2\sqrt{PN_X}\right), \tag{3.67}$$

Для оцінювання інформативності отриманих результатів розглянемо зміну діапазону пошуку оптимальної кількості схованих нейронів при використанні розробленої моделі. Зміну діапазону будемо оцінювати за виразом

$$\delta = \frac{N_1^{\text{opt}}(\max) - N_1^{\text{opt}}(\min)}{N_1^{\max} - N_1^{\min}}. \qquad (3.68)$$

Врахуємо, що для більшості практичних задач оцінювання ПБ для розпізнавання кібератак на ІС кількість вхідних параметрів менша від 100 ($N_x \approx 100$), а кількість навчальних прикладів, необхідних для ефективного навчання НМ, повинна перевищувати 10000 ($P \approx 10000$). Вважатимемо, що застосовується ДШП з одним виходом ($N_Y=1$). Використавши вказані параметри в розробленій моделі (3.66), (3.67), отримаємо $Ns_1^{\text{opt}}(\min) \approx 400$, $Ns_1^{\text{opt}}(\max) \approx 2000$. Для загальної моделі (3.61), (3.62) відповідні результати інші – $N_1^{\min} \approx 200$, $N_1^{\max} \approx 10000$. Використавши ці результати в (3.68), отримаємо $\delta \approx 0{,}16$. Таким чином, діапазон пошуку оптимальної кількості схованих нейронів звузився приблизно у 6 раз.

Розглянемо загальний варіант – $N_x \approx 100$, а $P/N_x \approx 10$. У цьому випадку $Ns_1^{\text{opt}}(\min) \approx 120$, $Ns_1^{\text{opt}}(\max) \approx 620$, $N_1^{\min} \approx 200$, $N_1^{\max} \approx 1000$. Відповідно, $\delta \approx 0{,}63$. Отже, діапазон пошуку оптимальної кількості схованих нейронів звузився приблизно в 1,6 разу. Для елементарного випадку $N_x \approx 1$, а $P \approx 100$, тоді $Ns_1^{\text{opt}}(\min) = 6$, $Ns_1^{\text{opt}}(\max) = 20$, $N_1^{\min} = 3$, $N_1^{\max} = 100$. Підставивши ці величини в (3.68), отримаємо $\delta \approx 0{,}18$. Таким чином, діапазон пошуку оптимальної кількості схованих нейронів звузився приблизно в 5,7 разу. Ураховуючи працю [32], можна очікувати, що застосування розробленої моделі дозволить зменшити обчислювальні витрати на загальну розробку ДШП в 1,1–2 рази.

Для верифікації отриманих результатів проведені численні експерименти з апроксимації одно-, дво- та багатопараметричної поліноміальної функції за допомогою ДШП, кількість схованих нейронів якого розраховувалась за

допомогою виразів (3.61), (3.62), (3.66), (3.67) та за допомогою виразів, отриманих в результаті аналізу праць [101, 140, 210]:

$$\frac{0{,}5P}{1+\ln P} \le N_2^{\min} \tag{3.69}$$

$$N_2^{\max} \le \frac{1{,}5P+1{,}5}{N_1} + 0{,}5N_1 \tag{3.70}$$

$$\frac{P}{20} - 0{,}5N_1 - 0{,}5N_0 \le N_3^{\min}, \tag{3.71}$$

$$N_3^{\max} \le \frac{P}{4} - 0{,}5N_1 - 0{,}5N_0, \tag{3.72}$$

де $N_2^{\min}$, $N_2^{\max}$ – мінімальна та максимальна межі діапазону оптимальної кількості схованих нейронів [101]; $N_2^{\min}$, $N_2^{\max}$ – мінімальна та максимальна межі [210] .

Результати експериментів підтвердили звуження діапазону пошуку оптимальної кількості схованих нейронів у середньому в 1,5–2 рази.

Як ілюстрацію проведених експериментів на рис. 3.6–3.10 показано зміну відносних помилок навчання та узагальнення ДШП, який застосовано для інтерполяції та екстраполяції функції $y = 2x + 1$.

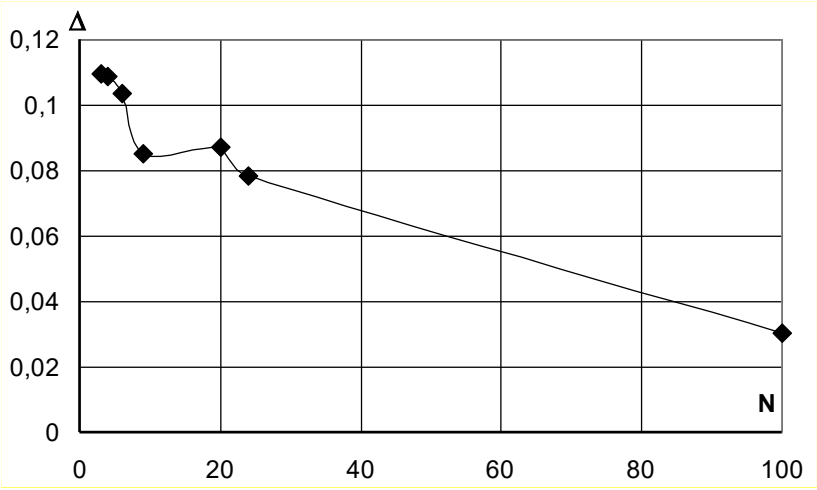

Рис. 3.6. Середня відносна помилка навчання ДШП:

Δ – відносна абсолютна помилка результатів, отриманих за допомогою ДШП;

X – аргумент функції; N – кількість схованих нейронів

Кількість схованих нейронів ДШП розраховувались за допомогою виразів

(3.61), (3.62), (3.66), (3.67), (3.69)–(3.72). Для проведення експериментів потрібно, щоб кількість навчальних прикладів P=100, а кількість вхідних та вихідних нейронів N_X=N_Y=1. Відповідно у виразах (3.61), (3.62), (3.66), (3.67), (3.69)–(3.72) $N_1^{\min}=3$, $N_2^{\max}=100$, $N_1^{\text{opt}}(\min)=6$, $N_1^{\text{opt}}(\max)=20$, $N_2^{\min}=9$, $N_2^{\max}=152$, $N_3^{\min}=4$, $N_3^{\max}=24$. Як показує аналіз рис. 3.6, помилка ДШП на навчальних прикладах пропорційно зменшується зі збільшенням кількості схованих нейронів, що в цілому відповідає висновкам [46]. Помилка узагальнення ДШП оцінювалась за величиною відносної помилки інтерполяції даних за допомогою ДШП (рис. 3.7).

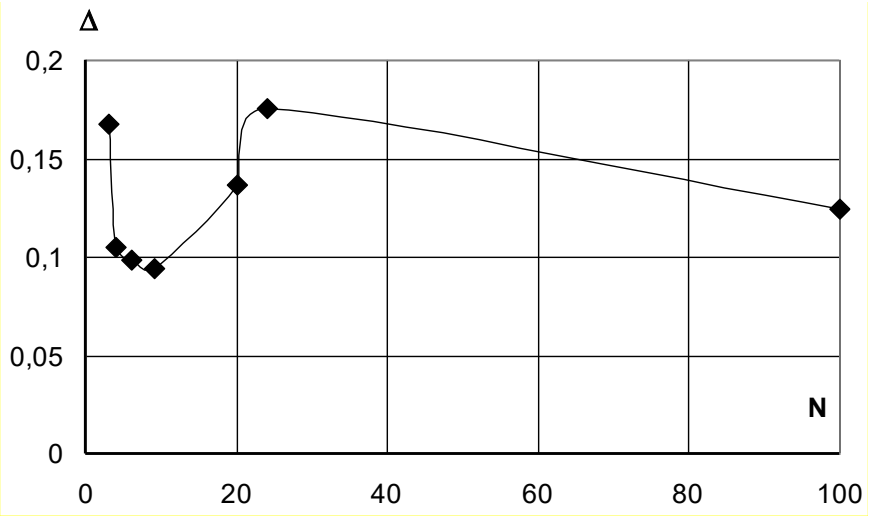

Рис. 3.7. Середня відносна абсолютна помилка інтерполяції ДШП

Аналіз рис. 3.7 вказує на мінімізацію помилки інтерполяції ДШП за кількості схованих нейронів у межах від 6 до 20, що відповідає виразам (3.46), (3.47) і підтверджує достовірність теоретичних викладок. Для повноти аналізу придатності використання ДШП у задачах оцінювання ПБ проаналізовано обчислювальну складність його навчання. Оскільки в більшості випадків оптимальний розподіл вагових коефіцієнтів шукається здубільшого за допомогою градієнтних методів [140], то кількість операцій ξ_1, потрібних для розрахунку градієнта функції помилки $\partial\varepsilon/\partial L_w$, визначається пропорцією вигляду:

$$\xi_1 \sim PL_w,$$

де L_w – кількість синаптичних зв'язків; P – кількість навчальних прикладів.

Ураховуючи, що швидкість сходження найкращих методів навчання пропорційна кількості синоптичних зв'язків [140], загальну кількість обчислювальних операцій ξ, потрібних для досягнення нульової помилки, розрахуємо так:

$$\xi = \mu P L_w^2, \tag{3.73}$$

де μ – коефіцієнт пропорційності, що в першому наближенні дорівнює 1.

Вираз (3.73) дозволяє оцінити мінімальну кількість навчальних операцій для БШП з довільною структурою.

Зазначимо, що для ДШП кількість синаптичних зв’язків

$$L_w = (N_X + N_Y) N_1. \tag{3.74}$$

Підставивши вираз (3.73) у (3.74), отримаємо

$$\xi = \mu P (N_X + N_Y)^2 N_1^2. \tag{3.75}$$

Для розрахунку мінімальної кількості навчальних операцій ξ_{opt} у ДШП з оптимальною структурою підставимо вирази (3.66), (3.67) в (3.75):

$$\xi_{\min}^{opt} = \mu P (N_X + 1)^2 \left(Round \left((0{,}4 N_X + 0{,}2) \frac{\sqrt{P N_X}}{N_X + N_Y} \right) \right)^2;$$

$$\xi_{\max}^{opt} = \mu P (N_X + 1_Y)^2 \left(Round \frac{\left(2\sqrt{P N_X} \right)}{N_Y} \right)^2,$$

де $\xi_{\min}^{opt}, \xi_{\max}^{opt}$ – кількість обчислювальних операцій для ДШП з кількістю схованих нейронів, яка дорівнює нижній і верхній межами оптимального діапазону.

Після перетворень та спрощень отримаємо:

$$\xi_{\min}^{opt} \approx 0{,}16 \mu P^2 N_X^3; \tag{3.76}$$

$$\xi_{\max}^{opt} \approx 4 \mu P^2 N_X^3. \tag{3.967}$$

Вирази (3.76), (3.77) визначають залежність між кількістю обчислювальних операцій оптимізованого ДШП та максимальною кількістю статистично подібних прикладів, яку він може безпомилково запам’ятати. З виразів (3.76) і (3.77) показує, що

$$\xi_{\max}^{opt} \approx 25\xi_{\min}^{opt}.$$

Убільшості задач оцінювання ПБ кількість обчислювальних навчальних операцій обмежена максимально допустимим терміном навчання. Позначимо максимально допустиму кількість навчальних операцій як ξ_d. Підставивши ξ_d в (3.76), (3.77) та виконавши відповідні перетворення, отримаємо вираз для оцінювання максимальної кількості навчальних прикладів ДШП з оптимальною структурою за умовибезпомилкового навчання:

$$P_{1,\max} \approx 2{,}5\frac{\sqrt{\xi_d}}{\sqrt{\mu}N_X^{1,5}};$$

$$P_{2,\max} \approx 0{,}5\frac{\sqrt{\xi_{\mathrm{d}}}}{\sqrt{\mu}N_X^{1,5}}, \qquad (3.78)$$

де $P_{1,\max}$, $P_{2,\max}$ – максимальна кількість навчальних образів для ДШП з кількістю схованих нейронів, яка дорівнює нижній та верхній межами оптимального діапазону.

При цьому

$$P_{1,\max} = 5P_{2,\max}. \qquad (3.79)$$

Виразивирази (3.76), (3.77), (3.78), (3.79) отримано за умови нульової помилки апроксимації (навчання) $\varepsilon_a = 0$. Водночас результати [140] вказують на можливість навчання з деякою допустимою помилкою:

$$\varepsilon_a \le \varepsilon_{ad} \qquad (3.80)$$

де ε_{ad} – допустима помилка навчання (апроксимації).

Аналіз праць [140, 210] вказує на експоненційний характер залежності між кількістю обчислювальних навчальних операцій та помилкою навчання. Це дозволяє модифікувати вирази (3.76), (377), (3.78), (3.79) для врахування очікуваної помилки навчання:

$$\xi_{\min}^{opt} \approx 0{,}16e^{-\chi\varepsilon_a}\mu P^2 N_X^3; \qquad (3.81)$$

$$\xi_{\max}^{opt} \approx 4e^{-\chi\varepsilon_a}\mu P^2 N_X^3; \qquad (3.82)$$

$$P_{1,\max} \approx \frac{\sqrt{\xi_d}}{0{,}4\sqrt{e^{-\chi\varepsilon_a}\mu}N_X^{1,5}}; \tag{3.83}$$

$$P_{2,\max} \approx \frac{\sqrt{\xi_d}}{2\sqrt{e^{-\chi\varepsilon_a}\mu}N_X^{1,5}}, \tag{3.84}$$

де χ – деяка константа.

Упершому наближенні можна вважати, що $\chi \approx 1$. При цьому в багатьох задачах оцінювання ПБ для виявлення кібератак [88, 94] очікувана розмірність вхідного сигналу, а відповідно, і кількість вхідних нейронів не буде перевищувати 1000 ($N_X \leq 10^3$). Разом з тим очікувана розмірність вихідного сигналу, яка відповідає кількості вихідних нейронів, дорівнює 1, тобто $N_Y=1$. Також можна вважати, що загальновживаний термін навчання НМ має перебувати в межах однієї доби ($\approx 10^5$ с).

Для прикладу розглянемо задачу побудови БШП для розпізнавання поштових скриптових вірусів. Відповідно до праць [158, 164] кількість параметрів ПБ, за допомогою яких можна розпізнати найбільш поширені поштові скриптові віруси, написані мовою VBS, менша ніж 100 ($N_X \leq 100$). Можна застосувати БШП з одним вихідним нейроном, вихідний сигнал якого вказує: вірусу немає ($0 \leq N_Y < 0{,}33$), підозра на вірус ($0{,}33 \leq N_Y < 0{,}66$) і вірус є ($0{,}66 < N_Y \leq 1$). У разі використання персонального комп'ютера з потужністю близько 10^{10} операцій за секунду терміну навчання 10^5 с відповідатиме $\xi \approx 8{,}64 \cdot 10^{14}$ обчислювальних операцій. На підставі виразів (3.83), (3.84) визначено, що при умові безпомилкового навчання обсяг навчальної бази даних ДШП становитиме $P \approx 1{,}5 \cdot 10^4 \ldots 7{,}5 \cdot 10^4$ прикладів, що відповідає обсягу баз даних сучасних антивірусних засобів. Діапазон очікуваної помилки узагальнення становить [0,03...0,14], що вважається прийнятним для евристичних аналізаторів сучасних антивірусних систем.

Розрахований обсяг навчальної вибірки та очікувана помилкаузагальнення підтверджують високий потенціал використання БШП з

оптимізованою структурою для розв’язання задач оцінювання ПБ ІС з метою виявлення кібератак.

3.5. Модель мережі MPNN

Для створення мережі MPNN використано розроблений підхід до застосування продукційних правил для подання експертних знань у НММ, придатних для навчання шляхом безпосереднього запам’ятовування начальних прикладів. У результаті досліджень, проведених в підрозділі 1.2, визначено, що з точки зору оцінки ПБ для виявлення кібератак серед таких НММ високий потенціал має PNN. Структуру мережі PNN, призначеної для розпізнавання мережевих кібератак за рахунок класифікації одного із двох можливих станів ІС (*A* – безпечного стану, *B* – реалізації мережевої кібератаки), показано на рис. 3.8.

У цій мережі нейрони ШО з номерами від *1* до *L* відповідають навчальним прикладам, які співвідносяться з безпечним станом, а нейрони з номерами від *L+1* до *N* співвідносяться з реалізацією кібератак.

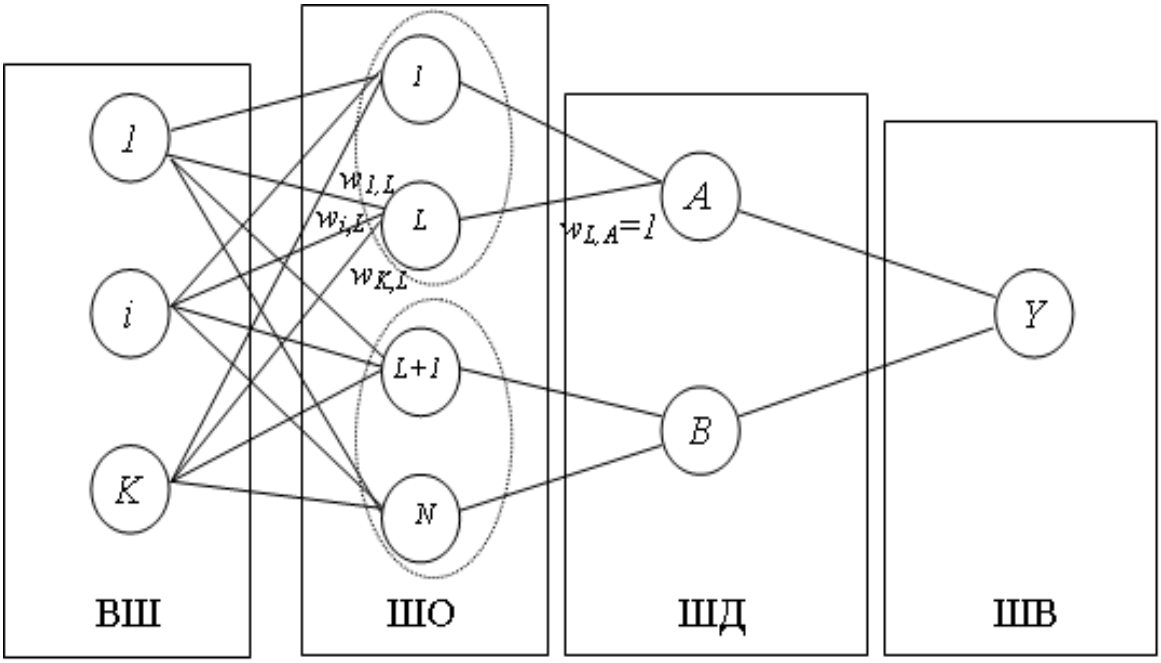

Рис. 3.8. Структура мережі PNN

Безпечний стан співвідноситься з нейроном ШД *A*, а стан реалізації мережевої атаки – з нейроном ШД *B*. На нейрони ВШ подають інформацію, яка

відповідає нормалізованим значенням контрольованих ПБ ІС, значення яких можуть сигналізувати про наявність/відсутність кібератак. Наприклад, для мережевої кібератаки ПБ можуть бути частота мережевих запитів, завантаженість лінії зв´язку, кількість неправильних пакетів, протокол, по якому передаються дані, завантаженість процесора, IP-адреса, з якої передаються дані і т.ін. Кількість вхідних нейронів дорівнює кількості контрольованих ПБ.

Для внесення у НМ знань про правило класифікації безпечного стану або реалізації кібератаки вигляду достатньо:

- визначити у ШД два нейрони А і В, що співвідносяться з безпечним та небезпечним станами ІС;
- внести в ШО новий нейрон;
- співвіднести для нього вагові коефіцієнти вхідних зв´язків з величинами параметрів, які відповідають заданому прикладу безпечного стану або реалізації атаки;
- установити для нового нейрона вихідний зв´язок з відповідним нейроном ШД *A* або *B*.

Для прикладу на рис. 3.8 показано вагові коефіцієнти $w_{L,1}$, $w_{i,L}$, $w_{K,L}$ і $w_{L,A}$, за рахунок яких у мережу PNN внесено приклад *i*, який відповідає безпечному стану ІС. Відповідно до посібника [140] для підвищення ефективності процесу розрахунку вихідного сигналу мережу PNN доцільно подати в матричній формі.

Елементами матриць будуть вагові коефіцієнти зв’язків між сусідніми шарами нейронів. Якщо ж зв’язок між нейронами не передбачено, то вважається що його ваговий коефіцієнт дорівнює 0. Аналіз відомих прикладів правил визначення безпечного/небезпечного стану ІС, що застосовуються у СВА, виявив дві властивості, які недостатньо враховуються у структурі та математичному забезпеченні класичної мережі PNN [184]:

1. Кожному окремому типу кібератаки може відповідати одна комбінація ПБ. Тобто кількість класів, що розпізнаються, може дорівнювати кількості

навчальних прикладів. Таким чином, кількість нейронів у ШД буде дорівнювати кількості нейронів у ШО. Очевидно, що в таких випадках використання ШД буде недоцільним. Вихідний сигнал від нейронів ШО може безпосередньо подаватись до нейрона ШВ. Відповідно змінену структуру мережі PNN показано на рис. 3.9.

2. У багатьох випадках продукційні правила матимуть вигляд (2.11).

Безпосереднє визначення такого правила у PNN неможливе, оскільки лінійна активаційна функція ШО не в змозі відобразити складову

$$p_i \in \left[P_i^{\min}, P_i^{\max}\right]. \tag{3.85}$$

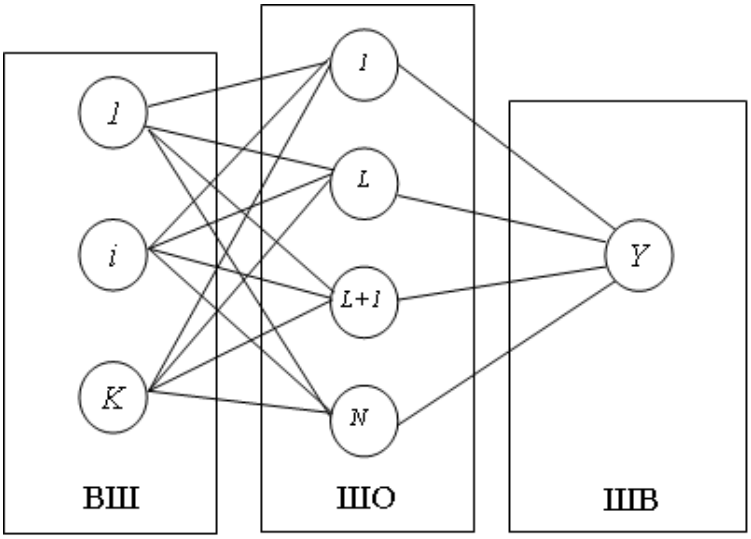

Рис. 3.9. Структура мережі PNN без ШД

Умову (2.11) можна подат за допомогою системи рівнянь вигляду

$$\begin{cases} p_1 = P_1^{\min} \wedge p_2 = P_2^{\min} \wedge \ldots, \\ p_1 = P_1^{\min} + \Delta_1 \wedge p_2 = P_2^{\min} + \Delta_2 \wedge \ldots, \\ p_1 = P_1^{\max} \wedge p_2 = P_2^{\max} \wedge \ldots, \end{cases} \tag{3.86}$$

де $\Delta_1, \Delta_2, \ldots$– задані коефіцієнти.

Однак використання виразу (3.86) призводить до вагомого ускладнення PNN унаслідок значного збільшення кількості нейронів ШО. Можливим шляхом адаптації моделі PNN до умови (3.86) є введення до її складу

проміжного (фільтрувальног) шару нейронів для фільтрації вхідного сигналу відповідно до виразу (3.86). Фільтрувальний шар (ШФ) має міститись між ВШ і ШО.

Структуру модифікованої мережі PNN, що отримала назву MPNN, показано на рис. 3.10.

Функцією i_l нейрона ШФ є фільтрація i-го ПБ відповідно до l–го продукційного правила. Для цього застосовується функція активації вигляду

$$\exists x_i^{(\text{ВШ})} \in \left[P^{\min}, P^{\max}\right]_l \rightarrow y_{j_l}^{(\text{ШФ})} = x_i^{(\text{ВШ})}, \exists x_i^{(\text{ВШ})} \notin \left[P^{\min}, P^{\max}\right] \rightarrow y_{j_l}^{(\text{ШФ})} = 0, \quad (3.87)$$

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

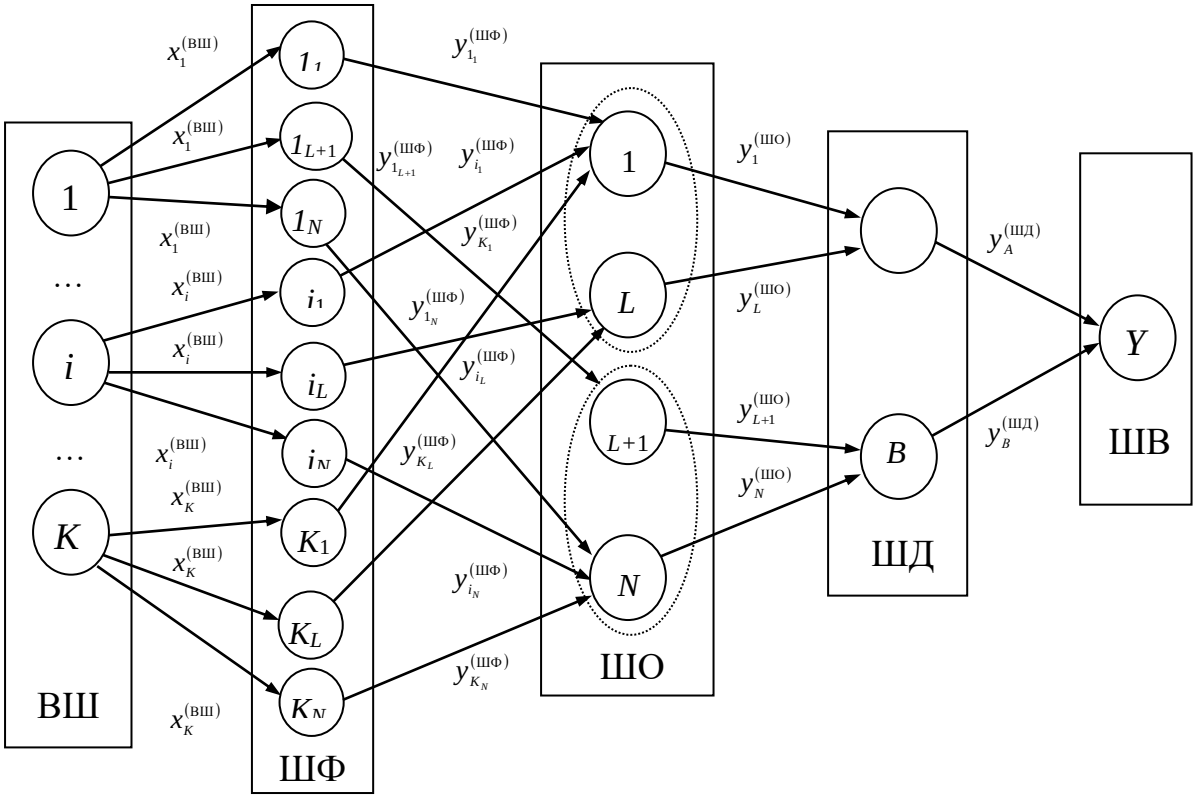

Рис. 3.10. Структура моделі MPNN

Вихідний сигнал l-го нейрона ШО розраховується так:

$$y_l^{(\text{ШО})} = \sum_{k=1}^{K} \exp\left(-\left(w_{k_l,l} - y_{k_l}^{(\text{ШФ})}\right)^2 / 2\sigma^2\right), \quad (3.88)$$

де $w_{k_l,l}$ – ваговий коефіцієнт зв’язку між k_l-м нейроном ШФ та l-м

нейроном ШО; K – кількість компонент вхідного вектора-образу, σ – радіус функції Гауса.

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

$$y_j^{(\text{ШД})} = \sum_{i=1}^{N} y_i^{(\text{ШО})}, \tag{3.89}$$

де N – кількість нейронів ШО, пов'язаних з j-м нейроном ШД; $y_i^{(\text{ШО})}$ – активність i-го нейрона ШО, пов'язаного з j-м нейроном ШД.

Функцією єдиного нейрона ШВ є визначення максимального вихідного сигналу нейронів ШД. Цей нейрон вказує на розпізнаний клас.

3.6. Модель створення ефективних нейромережевих засобів оцінювання параметрів безпеки

Згідно з результатами першого розділу ефективність НМЗ оцінювання ПБ ІС для виявлення кібератак багато в чому залежить від відповідності типу та параметрів НММ умовам поставленої задачі. Загальну ефективність застосування НМЗ можна оцінити за допомогою розроблених критеріїв, визначених виразами (2.16)–(2.9).

Крім того, процес створення НМЗ повинен починатись із визначення принципової можливості їх ефективного використання для розв’язання конкретної задачі розпізнавання кібератак. Варто звернути увагу на те, що верифікацію розроблених НМЗ слід реалізувати не лише за допомогою окремих числових експериментів, які в багатьох випадках не дозволяють гарантувати ефективність виявлення, але і шляхом формалізованих викладок.

На підставі означених викладок та розроблених підходів до визначення оптимального виду НММ, принципової доцільності та ефективності застосування НМЗ розроблені показано на рис. 3.11 модель створення ефективних НМЗ.

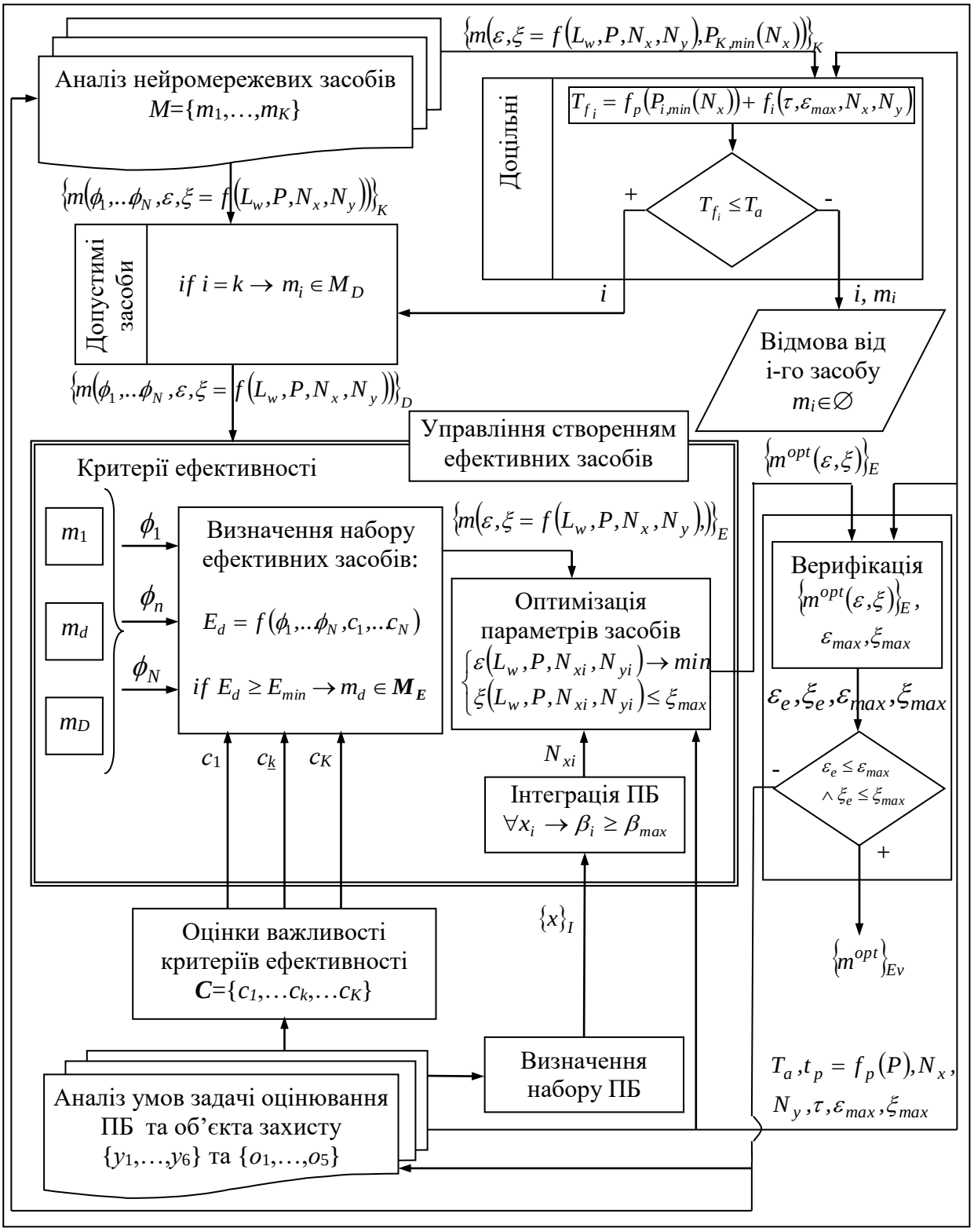

Рис. 3.11. Модель процесу створення ефективних НМЗ виявлення кібератак

Вхідними даними моделі є:

$$\boldsymbol{M} = \{m_1,..,m_K\}, \tag{3.90}$$

$$\boldsymbol{O} = \{o_1, \ldots, o_5\}, \tag{3.91}$$

$$\boldsymbol{У} = \{y_1, \ldots, y_6\}, \tag{3.92}$$

де $\boldsymbol{M}$ – множина доступних видів НМЗ; $\boldsymbol{O}$ – множина характеристик об'єкту захисту; $\boldsymbol{У}$ – множина умов задачі оцінювання ПБ.

У першому наближенні множина $\boldsymbol{M}$ формується на основі досліджених НММ виду: БШП, РБФ, ТК, АНМ, СНМ, PNN, MPNN, АРТ.

Множина $\boldsymbol{O}$ введена в підходах до розпізнавання НК і ПК, а множина $\boldsymbol{У}$ визначена в процесі аналізу можливостей НММ і складається з елементів, що характеризують навчальні дані y_1, обмеження процесу навчання y_2, обчислювальні потужності y_3, вихідну інформацію y_4, технічну реалізацію y_5 та сферу застосування НМЗ y_6.

Першочерговий аналіз вхідних параметрів, який виконується у модулях «Аналіз нейромережевих засобів», «Допустимі засоби» та «Аналіз умов задачі оцінки ПБ та об'єкта захисту» реалізується на основі оброблення експертних даних. У базовому випадку можназастосовувати метод парних порівнянь, використаний в підрозділі 3.1. Надалі можливе використання інших експертних методів, характеристики яких наведено у статті [90].

У результаті аналізу елементів $\boldsymbol{M}$ для кожного з них визначаються:

– множина величин критеріїв ефективності ($\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_N\}$);

– залежність мінімальної кількості навчальних прикладів P_{min} від кількості вхідних параметрів N_x;

– залежності похибки навчання ε і кількості обчислювальних операцій ξ від кількості синаптичних зв'язків L_w, навчальних прикладів P, кількості вхідних N_x та вихідних параметрів N_y.

Таким чином, результатом аналізу кожного $m_k \in \boldsymbol{M}$ є визначення функціоналів вигляду:

$$P_{\min} = f(N_x), \tag{3.93}$$

$$\varepsilon = f(L_w, P, N_x, N_y), \tag{3.94}$$

$$\xi = f\left(L_w, P, N_x, N_y\right), \tag{3.95}$$

Для кожного $m_k \in \boldsymbol{M}$ визначається залежність терміну навчання (T) від тривалості навчальної ітерації τ, допустимої похибки навчання ε_{max}, кількості навчальних прикладів, кількості вхідних параметрів і вихідних параметрів:

$$T_k = f_k\left(\tau, \varepsilon_{max}, P, N_x, N_y\right), \tag{3.96}$$

У результаті аналізу множин ***У*** та ***О***, що виконується в модулі «Аналіз умов задачі оцінки ПБ та об'єкта захисту» визначається набір ПБ ($\{x_i\}$), допустимий термін створення НМЗ T_a, допустима помилка навчання, допустима кількість навчальних ітерацій ξ_{max}, тривалість однієї навчальної ітерації τ, кількість вхідних та вихідних параметрів.

Розраховується залежність терміну створення навчальної вибірки t_p від кількості навчальних прикладів і визначається множина оцінок важливості критеріїв ефективності ***С***:

$$t_p = f_p(P), \tag{3.96}$$

$$\boldsymbol{C} = \{c_1, c_2, \ldots c_K\}, \tag{3.97}$$

де c_k – коефіцієнт важливості *k*-го критерію оцінювання ефективності.

Подання величин τ, P, ε_{max}, N_x, N_y, визначених у модулях аналізу, у вираз

$$T_{f_i} = f_p(P_i) + f_i(\tau, \varepsilon_{max}, N_x, N_y),$$

де T_{f_i} – тривалість розробки *i*-го НМЗ,

дозволяє розрахувати тривалість терміну розроблення параметрів кожного *i*-го НМЗ:

Рішення про принципову доцільність застосування *i*-го НМЗ приймається у випадку істинності виразу

$$T_{f_i} \le T_a,$$

де T_a – максимально допустима тривалість розробленняНМЗ.

Остаточне формування множини допустимих НМЗ $\{m\}_D$ реалізується в

модулі «Допустимі засоби». Вихідні дані цього модуля, що визначаються виразами (3.90)–(3.94), надходить у модуль «Управління створенням ефективних засобів», у якому на підставі підходу до визначення ефективності НЗМ за допомогою розробленої моделі інтеграції ПБ формується множина ефективних НМЗ з оптимізованими параметрами ($\{m\}_E^{\text{opt}}$). Для цього використовується розроблена модель інтеграції ПБ і проводиться оптимізація параметрів визначених ефективних НМЗ.

Для того щоб визначити пналежність деякого *d*-го НМЗ, що є елементом $\{m\}_D$, до множини ефективних НМЗ, використовуються таке правило:

$$\textit{якщо } E_d \geq E_{\min} \rightarrow m_d \in \{m\}_E,$$

де E_d – ефективність *d*-го НМЗ; $E_{\min}$ – мінімально допустима ефективність НМЗ; $\{m\}_E$ – множина ефективних НМЗ.

У свою чергу, ефективність *d*-го НМЗ є функціоналом від критеріїв ефективності та їх вагових коефіцієнтів:

$$E_d = f(\varphi_1,..\varphi_N, c_1,..c_N).$$

Параметри НМЗ, що входять до складу множини ефективних НМЗ, оптимізуються за критерієм мінімізації помилки розпізнавання з урахуванням максимально допустимої кількості обчислювальних операцій:

$$\begin{cases} \varepsilon(L_w, P, N_{xi}, N_{yi}) \rightarrow \min; \\ \xi(L_w, P, N_{xi}, N_{yi}) \leq \xi_{\max}, \end{cases}$$

де ε – помилка розпізнавання НМЗ; ξ – кількість обчислювальних операцій для досягнення мінімальної помилки розпізнавання; $\xi_{\max}$ – максимально допустима кількість обчислювальних операцій; N_{xi} – кількість вхідних параметрів НММ; N_{yi} – кількість вихідних параметрів НММ.

Множина ефективних нейромережевих засобів з оптимізованими параметрами передається до модуля «Верифікації», у якому на основі порівняння ефективності кожного з компонентів зазначеної множини з величинами $\varepsilon_{\max}, \xi_{\max}$ приймається рішення про можливість використання:

$$якщо\ (\varepsilon_e \le \varepsilon_{\max} \wedge \xi_e \le \xi_{\max}) \to m_e \in \{m^{\text{opt}}\}_{Ev},$$

де ε_e – помилка розпізнавання для $m_e \in \{m\}_E$; ξ_e – кількість обчислювальних операцій для $m_e \in \{m\}_E$, $\{m^{\text{opt}}\}_{Ev}$ – множина верифікованих нейромережевих засобів.

Множина $\{m^{\text{opt}}\}_{Ev}$ є результуючим виходом моделі. Якщо ця множина порожня, то слід додатково проаналізувати доступні нейромережеві засоби, умови задачі оцінювання ПБ та об'єкт захисту з метою визначення шляхів підвищення ефективності вказаних засобів.

На відміну від відомих, в описаній моделі передбачено процес інтеграції ПБ на підставі експертних даних, визначення принципової доцільності застосування НМЗ, оптимізації виду та параметрів НМЗ. Застосування цієї моделі є підґрунтям для формалізації процесу створення методів розробленняефективних НМЗ.

Розділ 4. МЕТОДИ ПОБУДОВИ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ ОЦІНЮВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ІНТЕРНЕТ-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

4.1. Метод застосування продукційних правил для подання експертних знань

Відправною точкою розроблення цього методу став описаний в підрозділі 3.5. узагальнений метод подання навчальних прикладів–продукційних правил для навчання PNN (див. рис. 3.8). У процесі навчання PNN визначаються вагові коефіцієнти синаптичних зв’язків і формується структура мережі (ШО та ШД). Оскільки метод застосування продукційних правил для подання експертних знань орієнтовано на розроблену MPNN, що відрізняється від PNN наявністю ШФ (див. рис. 3.10), то узагальнений метод дещо модифікується. Для подання в MPNN нового прикладу–продукційного правила необхідно:

- додати в ШО новий нейрон, який відповідатиме новому навчальному прикладу–продукційному правилу;
- залежно від класифікації навчального прикладу встановити для нового нейрона вихідний зв’язок з відповідним нейроном ШД;
- додати у ШФ нейрони, що будуть відповідно до виразу (3.80), перетворювати сигнали, які передаються від вхідних нейронів, у новий нейрон ШО;
- установити зв’язки між новими нейронами ШО і ШФ;
- установити зв’язки між новими нейронами ШФ та відповідними вхідними нейронами;
- установити для нових нейронів ШФ вагові коефіцієнти вхідних зв´язків, які дорівнювали б величинам параметрів нового навчального прикладу.

Для підвищення універсальності запропонованих рішень передбачено використання методу подання продукційних правил не тільки в складі комплексної методології розроблення НМЗ, але й самостійно. Тому процес

побудови методу базувався на розробленій моделі створення ефективних НМЗ оцінювання ПБ. Крім того, для визначення множин ПБ та кібератак, на основі яких формуються вхідні параметри НММ та продукційні правила, застосовано розроблену модель процесу інтеграції ПБ ІС. Це дозволило як вхідні даніметоду множину характеристик об'єкта захисту ІС $\boldsymbol{O}$, складові якої задані виразом (2.4). Процес формування продукційних правил щодо розпізнавання кібератак реалізується за допомогою розробленого підходу до визначення статистично подібних кібератак. У підсумку метод застосування продукційних правил для подання експертних знань у MPNN, призначену для розпізнавання кібератак на ІС, складається з таких етапів.

Етап 1 – *формування множини можливих кібератак*. Етап передбачає аналіз множини характеристик об'єкта захисту ІС, у результаті якого визначається множина кібератак, яку повинна розпізнавати НМ:

$$\boldsymbol{Ka} = \{Ka_1, Ka_2, ..., Ka_J\}$$

де *J*– кількість кібератак; Ka_j – j-а кібератака.

Етап 2 – *визначення ПБ для розпізнавання довільної кібератаки.* На цьому етапі із застосвуванням розробленої моделі інтеграції ПБ для кожної Ka_j визначається множина ПБ, які будуть використані як вхідні параметри НМЗ оцінювання:

$$Ka_j \to \{Xj\}_{Nj}$$

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

Етап 3 – *визначення подібних кібератак*. Етап орієнтований на виділення із $\boldsymbol{Ka}$ статистично подібних між собою кібератак:

$$\left\{\boldsymbol{Ka}_1^{(p)}, ..., \boldsymbol{Ka}_J^{(p)}\right\}, \forall \boldsymbol{Ka}_1^{(p)} \subset \boldsymbol{Ka}, ..., \boldsymbol{Ka}_J^{(p)} \subset \boldsymbol{Ka}, \ \boldsymbol{Ka}_1^{(p)} \cup \boldsymbol{Ka}_2^{(p)} ... \cup \boldsymbol{Ka}_J^{(p)} = \boldsymbol{Ka}, \quad (4.1)$$

де $\boldsymbol{Ka}_i^{(p)}$ – *i*-а множина подібних кібератак.

Відповідно до розробленого підходу подібність довільної *k*-ї та *j*-ї кібератак визначається кортежем:

$$\left\langle T_{(k,j)}\left(Ka_k, Ka_j\right), R_{(k,j)}\left(\left\{X_k\right\}_{N_k}, \left\{X_j\right\}_{N_j}\right)\right\rangle, \quad (4.2)$$

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

Розрахунок подібності *k*-ї та *j*-ї кібератак виконується за п’ять кроків.

Крок 1 – *визначення типу кібератак*. На цьому кроці визначається тип *k*-ї та *j*-ї кібератак:

$$Ka_k \to Ks_k \vee Kq_k, Ka_j \to Ks_j \vee Kq_j. \quad (4.3)$$

Крок 2 – *розрахунок функції подібності типу кібератак*. Для розрахунку порівнюються типи *k*-ої та *j*-ої кібератак. Використовується функціонал:

$$якщо \left(Ks_k \wedge Ks_j\right) \vee \left(Kq_k \wedge Kq_j\right) \to T_{(k,j)} = 0 \neg T_{(k,j)} \neq 0. \quad (4.4)$$

Крок 3 – *визначення множини спільних ПБ.* Цей крок спрямований на визначення множини ПБ, які використовуються для розпізнавання і *k*-ї, і *j*-ї кібератак:

$$\left\{X_{(k,j)}\right\}_{N_{(k,j)}} = \left\{X_k\right\}_{N_k} \cap \left\{X_j\right\}_{N_j}, \quad (4.5)$$

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

Крок 4 – *розрахунок коефіцієнта подібності множин ПБ.* Для розрахунку коефіцієнта подібності використовується вираз:

$$R_{(k,j)} = N_{(k,j)} / N^{\max}_{(k,j)}, \text{ де } N^{\max}_{(k,j)} = N_k \exists N_k > N_j \neg N^{\max}_{(k,j)} = N_j. \quad (4.6)$$

Крок 5 – визначення подібності кібератак. На даному кроці приймається остаточне рішення про подібність *k*-ї та *j*-ї кібератак. Кібератаки вражаються подібними, якщо є справедливий вираз

$$T_{(k,j)} = 0 \wedge R_{(k,j)} \le R_{\max}, \quad (4.7)$$

де $R_{\max}$ – апріорно заданий коефіцієнт.

Етап 4 – *визначення ПБ для розпізнавання подібних кібератак.* Етап орієнтований на визначення множини ПБ, що використовуються як вхідні

параметри НМ для розпізнавання подібних кібератак:

$$\left\{\boldsymbol{X}_1^{(p)},...,\boldsymbol{X}_J^{(p)}\right\}\rightarrow \boldsymbol{Ka}_j^{(p)}, \tag{4.8}$$

де $\boldsymbol{X}_j^{(p)}$ – множина ПБ, що відповідають j-й множині подібних кібератак; $\boldsymbol{Ka}_j^{(p)}=\left\{Ka_{1,j},...,Ka_{M_j,j}\right\}$; M_j – кількість елементів $\boldsymbol{Ka}_j^{(p)}$.

Для визначення $\boldsymbol{X}_j^{(p)}$ використовується вираз

$$\boldsymbol{X}_j^{(p)}=\boldsymbol{X}_{1,j}\cup...\boldsymbol{X}_{M,j}, \tag{4.9}$$

де $\boldsymbol{X}_{m,j}$ – множина ПБ для розпізнавання $Ka_{m,j}$.

Етап 5 – *отримання експертних даних.* Даний етап спрямований на формування множин подібних кібератак $\overline{\boldsymbol{Ka}}^{(p)}$, для яких можна розробити продукційні правила розпізнавання. Якщо для деякої j-ї множини $\boldsymbol{Ka}_j^{(p)}\in\boldsymbol{Ka}$ отримати представницькі експертні дані для розроблення продукційних правил на основі аналізу $\boldsymbol{X}_j^{(p)}$ досить складно, то

$$\boldsymbol{Ka}_j^{(p)}\not\subset\overline{\boldsymbol{Ka}}^{(p)}. \tag{4.10}$$

У противному випадку

$$\boldsymbol{Ka}_j^{(p)}\subset\overline{\boldsymbol{Ka}}^{(p)}. \tag{4.11}$$

Етап 6 – *розробка множини нейромережевих моделей*. Даний етап орієнтований на формування множини НМ типу MPNN, кожна з яких призначена для розпізнавання окремої множини подібних кібератак:

$$\boldsymbol{Net}=\left\{net_1,net_2,..net_M\right\}, \tag{4.12}$$

де net_j – j-а НМ, призначена для розпізнавання j-ї множини $\boldsymbol{Ka}_j^{(p)}$.

Етап 7 – *розробка структури вхідного шару*. У результаті виконання цього етапу для кожної $net_j\in\boldsymbol{Net}$ визначається кількість нейронів у ВШ MPNN. Використовується вираз

$$N_{x,j}=N_j^{\max}. \tag{4.13}$$

Установлюється відповідність між i-м входом НМ та i-м ПБ із множини

$\boldsymbol{X}_j^{(p)}$.

Етап 8 – *розробка продукційних правил.* На цьому етапі для кожної множини $\boldsymbol{Ka}_j^{(p)} \in \boldsymbol{Ka}$ на підставі експертних даних розроблюється множина продукційних правил їх розпізнавання:

$$\boldsymbol{Pr}_j = \left\{pr_{1,j},...pr_{L_j,j}\right\}, \tag{4.14}$$

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

Продукційні правила задаються виразами вигляду:

$$x_1 \in \left[x_1^{\min}, x_1^{\max}\right] \wedge x_2 \in \left[x_2^{\min}, x_2^{\max}\right] ... \wedge x_{N^{\max}} \in \left[x_{N^{\max}}^{\min}, x_{N^{\max}}^{\max}\right] \rightarrow Ka_{i,j}, \tag{4.15}$$

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.

Етап 9 – *розроблення ШД*. На цьому етапі для кожної $net_j \in \boldsymbol{Net}$ у ШД визначається стільки нейронів, скільки подібних кібератак повинна розпізнавати НМ:

$$N_{\text{ШД},j} = M_j. \tag{4.16}$$

Також встановлюється відповідність між кожним *n*-им нейроном ШД та *n*-ою кібератакою:

$$n_{ШД,j} \rightarrow Ka_{n,j}. \tag{4.17}$$

Етап 10 – *визначення структури ШО та ШФ*. Для кожної $net_j \in \boldsymbol{Net}$ виконання етапу є пристосуванням структури ШО і ШФ MPNN до заданих продукційних правил:

$$\left\langle \mathrm{N}_{\text{ШФ}}, \mathrm{N}_{\text{ШО}}, \mathrm{L}_{\text{ШФ}}, \mathrm{L}_{\text{ШО}}, \mathrm{L}_{\text{ШД}} \right\rangle = f\left(\mathrm{Pr}_j\right), \tag{4.18}$$

де $\mathrm{N}_{\text{ШФ}}$ – множина нейронів ШФ; $\mathrm{N}_{\text{ШО}}$ – множина нейронів ШО; $\mathrm{L}_{\text{ШФ}}, \mathrm{L}_{\text{ШО}}, \mathrm{L}_{\text{ШД}}$ – множина вхідних зв'язків ШФ, ШО і ШД.

Довільне *n*-е продукційне правило визначається за п'ять кроків:

Крок 1 – *визначення нейрона ШО*. На цьому кроці в ШО додається *n*-й

нейрон, який буде відповідати *n*-му продукційному правилу:

$$n_{\text{ШО},j} \to \text{Pr}_{n,j}. \tag{4.19}$$

Крок 2 – *модифікація* $L_{\text{ШД}}$. Модифікація полягає у встановленні для *n*-го нейрона ШО зв'язку з нейроном ШД, що відповідає *n*-й кібератаці.

Крок 3 – *визначення нейронів ШФ*. На цьому кроці у ШФ додається множина нейронів $N_{n,\text{ШФ}} \in N_{\text{ШФ}}$, що відповідно до *n*-го продукційного правила перетворюють сигнали від вхідних нейронів до *n*-го нейрона ШО. Перетворення задається виразом

$$\exists x_i^{(\text{ВШ})} \in \left[P^{\min}, P^{\max}\right]_l \to y_{j_l}^{(\text{ШФ})} = x_i^{(\text{ВШ})}, \exists x_i^{(\text{ВШ})} \notin \left[P^{\min}, P^{\max}\right]_l \to y_{j_l}^{(\text{ШФ})} = 0, \tag{4.20}$$

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

Крок 4 – *модифікація зв'язків* $L_{\text{ШО}}$. Реалізація кроку полягає у встановленні зв'язків між $n_{ШО,j}$ та $N_{n,ШФ}$.

Крок 5 – *модифікація зв'язків* $L_{\text{ШФ}}$. На цьому кроці встановлюються зв'язки між N_x і $N_{n,\text{ШФ}}$.

Кроки 1–5 виконуються для всіх заданих продукційних правил.

Етап 11 – *верифікація розроблених MPNN*. Верифікація кожної $net_j \in \boldsymbol{Net}$ полягає у порівнянні її похибки розпізнавання та обчислювальної складності з максимально допустимими значеннями цих параметрів. Для кожної net_j похибка розпізнавання та обчислювальна складність розраховуються на прикладах тестової вибірки. Мережа net_j вважається придатною для практичного використання, якщо для всіх прикладів тестової вибірки справедливий вираз

$$\varepsilon_j \le \varepsilon_{\max} \wedge \xi_j \le \xi_{\max},$$

де ε_j – похибка розпізнавання net_j; ξ_j – обчислювальна складність; $\varepsilon_{\max}$ – максимально допустима похибка розпізнавання; $\xi_{\max}$ – максимально допустима обчислювальна складність.

Для перевірки ефективності запропонованого методу проведено

експериментальні дослідження, у яких MPNN застосовувалась для виявлення мережевих атак. Як джерело статистичних даних для формування навчальної і тестової множини НМ використано базу даних KDD-99, котра містить близько 5000000 записів – образів мережевих з'єднань [1]. 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 і т.ін. У 42-му полі записано інформацію, що характеризує стан захищеності ІС – або відсутність атаки (normal), або її тип. У базі міститься 22 види атак, які поділяються на 4 основні класи – відмова в обслуговуванні (DoS), несанкціоноване отримання прав доступу незареєстрованим користувачем (R2L), несанкціоноване підвищення привілеїв (U2R) зареєстрованим користувачем та сканування портів (Probe). Кількість записів, що відповідають відсутності кібератак, дорівнює 972781.

Оскільки основною передумовою застосування експертних знань у НМ є недостатня повнота навчальних даних, то основну увагу зосереджено на розпізнаванні кібератак U2R, для яких кількість записів у KDD-99 найменша. Із залученням експертів в галузі захисту інформації розроблено 4 продукційні правила для розпізнавання кібератак buffer_overflow, що належать до U2R. Приклад продукційного правила для розпізнавання buffer_overflow має такий вигляд:

Якщо тривалість з'єднання (duration) = 0 ∧ протокол (protocol_type) – tcp ∧ сервіс (service)– ftp_data ∧ flag – SF ∧ кількість отриманих байтів (src_bytes) – 0 ∧ кількість переданих байтів (dst_bytes) – від 2000 до 6000 ∧ land – 0 ∧ wrong_fragment – 0 ∧ urgent – 0 ∧ 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 ∧ 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 ∧

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 ∧ dst_host_same_srv_rate = 0,00 ∧ dst_host_diff_srv_rate = 0 ∧ dst_host_same_src_port_rate = 1 ∧ dst_host_srv_diff_host_rate = від 0 до 0,02 ∧ dst_host_serror_rate = 0 ∧ dst_host_srv_serror_rate = 0 ∧ dst_host_rerror_rate = 0 ∧ dst_host_srv_rerror_rate = 0.

Розроблено 14 продуційних правил для визначення нормального стану ІС за відсутності кібератаки. Згідно із вказаними продукційними правилами та наведеними вище методом, побудовано MPNN, призначену для виявлення кібератак типу U2R. Основні параметри мережі такі: кількість вхідних параметрів мережі K=41, кількість нейронів ШД дорівнює 2 (нейрон А відповідає атаці, нейрон В – нормальному стану), кількість нейронів ШО дорівнює 18, а кількість нейронів ШФ – 738, основу математичного забезпечення складають вирази (3.80)–(3.83). Структура розробленої MPNN відповідає рис. 3.10 з урахуванням наведених величин.

Апробація розробленої моделі на даних KDD-99 показала абсолютну точність розпізнавання всіх видів кібератак buffer_overflow. Для порівняння отриманих результатів використано працю [3], у якій наведено результати розпізнавання цього ж типу кібератак з використанням сигнатур, наявних у базі KDD-99. Для розпізнавання використано БШП і ТК. Точність розпізнавання атак типу buffer_overflow ТК становить 0.0458. При цьому БШП через малий обсяг навчальних даних взагалі не вдалось навчити розпізнавати кібератак типу buffer_overflow. Для розпізнавання buffer_overflow застосовано спеціальну адаптивну модель, точність розпізнавання якої не перевищує 0,5 [4]. Тому можна вважати, що запропонований метод дозволить підвищити точність розпізнавання кібератак, сигнатур яких недостатньо в базах даних. Порівняння також указує на те, що застосування запропонованого методу дає змогу підвищити точність розпізнавання кібератак класу U2R, сигнатури яких подані в базі даних KDD-99 щонайменше в 2 рази.

Незважаючи на можливості подання експертних знань, широкому застосуванню модифікованої мережі PNN у галузі захисту інформації перешкоджає недолік – низька здатність узагальнювати навчальну інформацію. Зазначимо, що здатність НМ до узагальнення загальноприйнято оцінювати відношенням 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 ШО з кількістю синаптичних зв'язків, яка на одиницю перевищує кількість вхідних параметрів. Водночас у БШП з одним вихідним нейроном і такою ж кількістю синаптичних зв'язків співвідноситься 10–100 навчальних прикладів [5, 7, 8]. Тому при розпізнаванні кібератак узагальнювальні можливості БШП у 10-100 вищі, ніж у MPNN. Разом з тим MPNN та БШП мають подібні структурні схеми і належать до одного класу НМ з прямими поширенням сигналу. Крім того, аналіз [5, 7] вказує на те, що за допомогою конструктивних алгоритмів можна створити БШП, базою якого є мережа PNN. Тому перспективною є розроблення методу закладення експертних знань у БШП, призначений для розпізнавання мережевих кібератак. Ще одним важливим напрямом удосконалення запропонованого методу повинна бути його адаптація до використання експертних знань про мережеві кібератаки, поданих за допомогою апарату нечіткої логіки [4].

4.2. Метод визначення часових характеристик використання нейромережевих засобів

Основою розроблення методу є підхід до визначення принципової доцільності застосування НМЗ оцінювання ПБ, метод застосування продукційних правил для подання експертних знань у НМЗ оцінювання ПБ і модель створення ефективних НМЗ оцінювання ПБ. Крім того, передбачається можливість застосування методу визначення доцільності як у складі комплексної методології, так і самостійно. Тому в методі застосовано модель

процесів інтеграції ПБ, що використовуються НМЗ розпізнавання кібератак. Реалізація методу полягає у виконанні таких етапів:

Етап 1 – *формування множини вхідних та вихідних параметрів НМ*. Етап передбачає використання розробленої моделі інтеграції ПБ, що дозволяє на основі аналізу характеристик об'єкта захисту $\boldsymbol{O} = \{o_1,..o_5\}$ та характеристик кібератаки $\Phi = \{\varphi_1,..\varphi_\Phi\}$ визначити множину ПБ, що будуть використані як вхідні параметри НМ:

$$\boldsymbol{X} = \{x_1,...x_{N_x}\},$$

де N_x – кількість вхідних параметрів НММ.

Визначається множина вихідних параметрів НММ, що свідчитимуть про наявність/відсутність кібератак певного типу:

$$\boldsymbol{Y} = \{y_1,...y_{N_y}\},$$

де N_y – кількість вихідних параметрів.

Етап 2 – *отримання статистичних даних*. У результаті аналізу характеристик об'єкта захисту, умов задачі оцінювання ПБ та множини доступних НМЗ $\boldsymbol{M}=\{m_1,\ldots,m_K\}$ оцінюється можливість реєстрації ПБ, що використовуються для визначення $\boldsymbol{X}$ і $\boldsymbol{Y}$. Якщо оцінка негативна, то НМЗ, крім MPNN, використовувати недоцільно. Тобто

$$\boldsymbol{M} = \{m_{MPNN}\}. \tag{4.21}$$

Етап 3 – *подання експертних знань.* Використовуючи розроблений метод застосування продукційних правил для подання експертних знань у НМЗ, оцінюється можливість розроблення моделі MPNN. Якщо оцінка негативна, то модель MPNN виключається із подальшого розгляду:

$$m_{MPNN} \notin \boldsymbol{M}. \tag{4.22}$$

У противному випадку

$$m_{MPNN} \in \boldsymbol{M}. \tag{4.23}$$

Етап 4 – *перевірка множини допустимих видів НМ.* Етап орієнтовано на перевірку непорожності множини допустимих НМЗ. Якщо справедливий вираз

(4.22), то НМЗ використовувати недоцільно:

$$\boldsymbol{M} = \varnothing. \tag{4.24}$$

Етап 5 – *визначення допустимої помилки навчання НМ*. На даному етапі в результаті аналізу характеристик об'єкту захисту визначаються мінімально допустимі величини пропуску кібератаки та хибного розпізнавання кібератаки. Менша із величин використовується як мінімально допустима помилка навчання НМ. Таким чином, для визначення ε використовується правило

$$якщо\ \delta_1 \le \delta_2 \to \varepsilon = \delta_1\ інакше\ \varepsilon = \delta_2. \tag{4.25}$$

де δ_1 – мінімально допустима величина пропуску кібератак; δ_2 – мінімально допустима величина хибного розпізнавання кібератак; ε – мінімально допустима помилка навчання НММ.

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

Етап 6 – *визначення часових обмежень процесу розробки НМ.* На цьому етапі визначається допустима тривалість розроблення (T_f) і допустимий термін навчання НМ (t_d). Тривалість розроблення T_f визначається на основі експертного оцінювання. Для визначення t_d використовується залежність

$$P(t_d) \ge P_n, \tag{4.26}$$

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

У першому наближенні $P_n = 10^{-5}$, згідно з виразами (4.24) та працею [32] $t_d \approx 10^5$ с. Тобто допустимий термін навчання НМЗ приблизно дорівнює одній добі.

Етап 7 – *визначення мінімального обсягу навчальної вибірки.* Етап орієнтований на визначення мінімально допустимої кількості навчальних прикладів для НМ.

Розрахунок виконується так:

$$P_{\min} = 20N_x. \tag{4.27}$$

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

Етап 8 – *розрахунок терміну навчання.* На цьому етапі розраховується $t_{\min}$ – термін навчання НММ на мінімально допустимій кількості навчальних прикладів. Для ТК, РБФ, PNN і MPNN

$$t_{\min} \approx 0{,}1\tau e^{-\varepsilon} P_{\min}\left(N_X + N_Y\right), \tag{4.28}$$

де τ – тривалість однієї обчислювальної операції процесу навчання.

Для БШП:

$$t_{\min} \approx 0{,}001\tau e^{-\varepsilon} P_{\min}^2\left(N_X + N_Y\right)^2. \tag{4.29}$$

Етап 9 – *перевірка терміну навчання.* Етап передбачає для всіх НМЗ, що входять до $\boldsymbol{M}$, порівняння допустимого терміну навчання з терміном навчання на мінімально допустимій кількості навчальних прикладів. Входження j-го НМЗ до множини ефективних НМЗ з допустимим терміном навчання визначається за допомогою такого правила:

$$t_{\min}\left(m_j\right) \geq t_d \rightarrow m_j \notin \mathrm{M}^{(tn)}, \tag{4.30}$$

де $\boldsymbol{M}^{(tn)}$ – множина ефективних НМЗ з допустимим терміном навчання; m_j – j-й НМЗ.

У противному випадку $m_j \in \boldsymbol{M}^{(tn)}$. Якщо $\boldsymbol{M}^{(tn)} = \varnothing$, то НМЗ взагалі використовувати недоцільно.

Етап 10 – *розрахунок максимально допустимої тривалості формування навчальної вибірки.* На цьому етапі для кожної $m_j^{(tn)} \in \boldsymbol{M}^{(tn)}$ розраховується максимально допустима тривалість формування навчальної вибірки $T_{j,max}$. Оскільки в MPNN як навчальні приклади використовуються експертні дані, то для НМЗ на базі цієї НММ тривалість формування навчальної вибірки дорівнює тривалості розроблення продукційних правил.

Для розрахунку $T_{j,\max}$ використовується вираз

$$T_{j,\max} = T_f - t_j, \tag{4.31}$$

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

Результатом виконання етапу є сформована множина

$$\{T_{1,\max},..,T_{L,\max}\}, \tag{4.32}$$

де L – кількість елементів $\boldsymbol{M}^{(tn)}$.

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

$$T_d = f(\boldsymbol{O},\boldsymbol{Y}), \tag{4.32}$$

де T_d – термін формування навчальної вибірки.

Етап 12 – *перевірка терміну формування навчальної вибірки.* На цьому етапі для кожної $m_j^{(tn)} \in \boldsymbol{M}^{(tn)}$ порівнюються $T_{j,\max}$ і T_d. Множина НМЗ, які доцільно використовувати для оцінки ПБ, формується за допомогою виразів:

$$якщо\ T_{j,\max} > T_d \rightarrow m_j^{(tn)} \notin \mathrm{Mz}, \tag{4.33}$$

$$якщо\ T_{j,\max} < T_d \rightarrow m_j^{(tn)} \in \mathrm{Mz}, \tag{4.34}$$

де $\boldsymbol{Mz}$ – множина НМЗ, які доцільно використовувати для оцінки ПБ.

У результаті реалізації методу формується множина НМЗ, які доцільно використовувати для оцінювання ПБ з метою розпізнавання кібератак.

Зазначимо, що використання запропонованого методу багато в чому ускладнюється необхідністю залучення висококваліфікованих експертів, знання яких потрібно для оцінювання можливості формування в прийнятний термін мінімально допустимої навчальної вибірки (дев'ятий та одинадцятий етапи). Разом з тим достатньо відомі бази даних, у яких подані образи кібератак, які можуть бути використані як навчальні приклади нейромережевих засобів розпізнавання. Очевидно, якщо кількість таких образів більша від мінімально допустимої кількості навчальних прикладів, то дев'ятий та десятий етапи виконувати не потрібно, а оцінка одинадцятого пункту позитивна. Тому в спрощеному варіанті методу замість етапів 10–12 слід оцінити можливість

формування мінімальної навчальної вибірки на підставі доступних баз даних образів кібератак.

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

Етап 1. Для виявлення атак цього типу необхідна статистика, яка стосується таких функціональних параметрів: кількість одночасних підключень, швидкість оброблення запитів, затримка між запитами, кількість пакетів з однаковими адресами відправника та отримувача, вік віртуального каналу та кількість віртуальних каналів. Номенклатура вхідних параметрів НМ буде відповідати вказаним функціональним параметрам. Кількість вхідних параметрів $N_X = 5$. Для виявлення кібератаки цього типу можна обмежитись одним вихідним параметром, величина якого вказуватиме на впевненість СВА у наявності/відсутності атаки типу IP-спуфінг. Тобто $N_Y = 1$.

Етап 2. Реєстрацію наведених ПБ можна здійснити мережевими екранами та СВА. При цьому як доступну базу даних можна використати KDD-99.

Етап 3. У першому наближенні мережа MPNN вилучена із розгляду. Тому $m_{MPNN} \notin \boldsymbol{M}$.

Етап 4. Оскільки результат другого етапу позитивний, то $\boldsymbol{M} \neq \varnothing$.

Етап 5. Відповідно до результатів [35] визначено, що допустима помилка навчання НМ $\varepsilon = 0{,}05$.

Етап 6. На основі експертного оцінювання визначено, що термін, на протягом якого ризик від реалізації кібератаки не перевищує встановлену межу, становить $T_a = 30$ діб. Використавши отриману величину отримано $T_f \leq 30$. Таким чином, максимально допустима тривалість розробленням НМ становить 30 діб. Відповідно до праць [13, 15] допустимий термін навчання НМ становить $t_d \approx 10^5$ с (24 год.).

Етап 7. Підставивши $N_X = 5$ у вираз (4.27), отримаємо:

$$P_{\min} \geq (10..20) N_x = 20 \cdot 5 = 100.$$

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

Етап 8. Для розрахунку терміну навчання НММ виду ТК, РБФ, PNN на мінімально допустимій навчальній вибірці у вираз (4.28) підставлено $P_{\min} = 100$, $N_X = 5$, $N_Y = 1$, $\chi = 1, \tau = 10^{-2}$. Отримано:

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

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

Для розрахунку терміну навчання БШП ці ж дані підставлено у вираз (4.28). Отримано:

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

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

Етап 9. Підставлення термінів навчання БШП, ТК, РБФ, PNN у вираз (4.30) вказує на входження НММ у множину $\boldsymbol{M}^{(tn)}$. Відповідно до праці [256] допустимий термін навчання НММ становить $t_d \approx 10^5$ с (24 год.).

Етап 10. Як доступну базу даних зареєстрованих ПБ можна використати KDD-99. Відповідно, $\boldsymbol{Mz} = \boldsymbol{M}^{(tn)}$. Отже, у першому наближенні для розпізнавання кібератак типу IP-спуфінг можна використовувати НМЗ на базі НММ виду БШП, ТК, РБФ та PNN.

Із використанням спрощеного варіанта запропонованого методу проведено визначено доцільність застосування НМЗ для виявлення типових кібератак на ІС. Аналіз праць [253, 255, 256] дозволяє стверджувати, що в сучасних умовах як доступні джерела статистичних даних ПБ, призначених для формування начальної вибірки НМ, доцільно використовувати параметри, що реєструються операційними системами, мережевими серверами і такими СЗІ, як міжмережеві екрани, антивіруси, системи захисту від спаму та DLP-системи.

Для кожної ІС ведуться відповідні бази даних, куди записуються

зареєстровані величини вказаних ПБ.

Крім того, бази даних СЗІ містять величини ПБ, які сигналізують про відсутність/наявність атаки на ІС. Тому, за наведеною у праці [93] класифікацією в першому наближенні визначено, що номенклатура та обсяг зареєстрованих статистичних параметрів дають змогу сформувати навчальну вибірку НМ, призначених для виявлення таких видів кібератак:

– мережевих кібератак, що реалізуються на транспортному і прикладному рівнях стеку протоколів TCP/IP;

– ШПЗ – комп'ютерних вірусів і троянів;

– спаму;

– витоків текстової інформації за допомогою листів електронної пошти.

Очевидно, що визначений перелік кібератак потребує подальшої деталізації, реалізувати яку в повному обсязі заважає велика кількість відомих підтипів атак, постійна поява нових підтипів атак та необхідність використання експертних даних для визначення максимально допустимої тривалості розроблення НМЗ. Тому реалізовано тільки часткову деталізацію.

На основі спрощеного варіанта методу розглянуто доцільність використання НММ для виявлення кібератак таких типів: СП, Dos-атак, веб-орієнтованих скриптових вірусів і троянів (ВСВ) та несанкціонованого отримання прав доступу незареєстрованим користувачем (R2L). Розглядались підтипи R2L, як phf та multihop [121].

Як вхідні параметри НМ використано:

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

– ВСВ – назви 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 і т.ін.).

Результати розрахунків показано на рис. 4.1 та наведено в табл. 4.1.

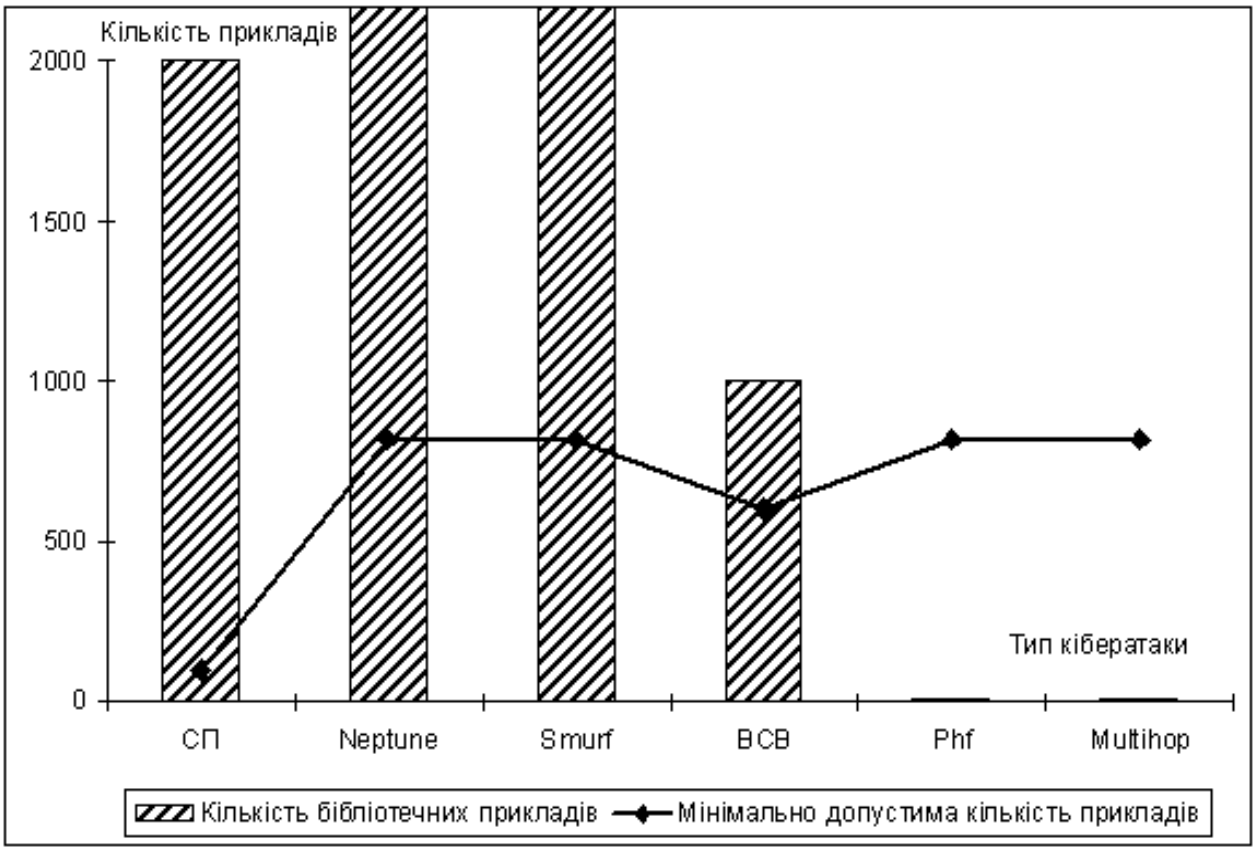

Рис. 4.1. Оцінювання можливості застосування нейромережевих засобів для виявлення кібератак:

Аналіз даних табл. 4.1 і рис. 4.1 дозволяє позитивно оцінити можливість навчання НММ на мінімально допустимій кількості навчальних прикладів за допустимий термін навчання та можливість формування мінімальної навчальної вибірки на основі існуючих баз даних для кібератак типу СП, Neptune, Smurf та ВСВ.

Для кібератак типу phf та multihop оцінка можливості формування мінімальної навчальної вибірки на основі існуючих баз даних негативна. Тому відповідно до спрощеного варіанта запропонованого методу НМЗ на основі БШП, ТК, РБФ і PNN доцільно використовувати для розпізнавання кібератак типу СП, Neptune, Smurf та ВСВ і недоцільно – для розпізнавання атак типу phf і multihop.

Таблиця 4.1

Проміжні результати оцінювання

Етап оцінювання	Вид кібератаки					
	СП	Dos-атак		ВСВ	R2L	
		Neptune	Smurf		Phf	Multihop
Кількість вхідних параметрів	5	41		30	41	
Допустима помилка навчання	0,05					
Тип НМ	БШП					
Мінімальна кількість навчальних прикладів	100	820		600	820	
Допустимий термін навчання, с	$\approx 10^5$					
Тривалість однієї навчальної 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 у базі даних	2000	10^6	$3 \cdot 10^6$	10^3	4	7
Оцінка можливості формування навчальної вибірки на основі бази даних	Позитивна				Негативна	

4.3. Метод проектування шаблону поведінки параметрів безпеки

Метод проектування шаблону поведінки ПБ грунтується на запропонованому підході до розпізнавання ПК та розроблених марковських моделях ШП. Відповідно до цього методу розроблення ШП ПБ складається п’яти етапів:

Етап 1 – *вирівняння ряду.* Етап орієнтований на розрахунок вирівняного

ряду зареєстрованих статистичних даних:

$$\hat{X}(t) = X'(t) - Y(t) - \overline{X},\ t \in [0,T], \tag{4.35}$$

де $X'(t)$ – ряд даних; $Y(t)$ – тренд; $\overline{X}$ – середнє значення ряду.

Етап 2 – *розрахунок параметрів ЛМ.* На етапі розраховуються параметри ЛМ, призначені для моделювання складових періодичного ряду:

$$\left\langle \{AB\}_K, \{BA\}_K, \left\{ p^{(AB)} \right\}_K, \left\{ p^{(BA)} \right\}_K \right\rangle, \tag{4.36}$$

де $\{AB\}_K, \{BA\}_K$ – множини розроблених стаціонарних інтервалів для кожного із значущих періодів; K – кількість періодів; $\left\{ p^{(AB)} \right\}_K, \left\{ p^{(BA)} \right\}_K$ – перехідні ймовірностей для кожного із ЛМ.

Структурну схему розрахунку параметрів ЛМ показано на рис.4.2.

Без урахування процедури введення та виведення даних розрахунок параметрів ЛМ реалізується за чотири кроки, що відповідають 3–7 вершинам структурної схеми:

Крок 1 – *розрахунок періодичних складових.* На цьому кроці, що відповідає вершині *3* (рис.4.2), за допомогою спектрального аналізу методом Фур'є розраховують періодичні складові вирівняного ряду:

$$\hat{X}(t) = a_0 + \sum_{i=1}^{q} \left(a_i c_i(t) + b_i s_i(t) \right) + e(t), \tag{4.37}$$

де a_0 – коефіцієнт; $c_i(t) = \cos(2\pi f_i t)$, $s_i(t) = \sin(2\pi f_i t)$, $f_i = i/T$ – *i*-а гармоніка основної частоти *1/T*; a_i, b_i – коефіцієнти регресії, що вказують на ступінь кореляції функцій $c_i(t)$ і $s_i(t)$ зі статистичними даними; $q = (T-1)/2$; T – кількість точок ряду; $e(t)$ – випадкова складова; $2\pi f_i$ – колова частота.

Розрахунок періодичних складових полягає у визначенні коефіцієнтів регресії:

$$a_i = \frac{2}{T} \sum_{t=1}^{T} \left(\hat{X}(t) c_i(t) \right), i = 1,2,..q; \tag{4.38}$$

$$b_i = \frac{2}{T}\sum_{t=1}^{T}(\hat{X}(t)s_i(t)), i = 1,2,..q\,. \qquad (4.39)$$

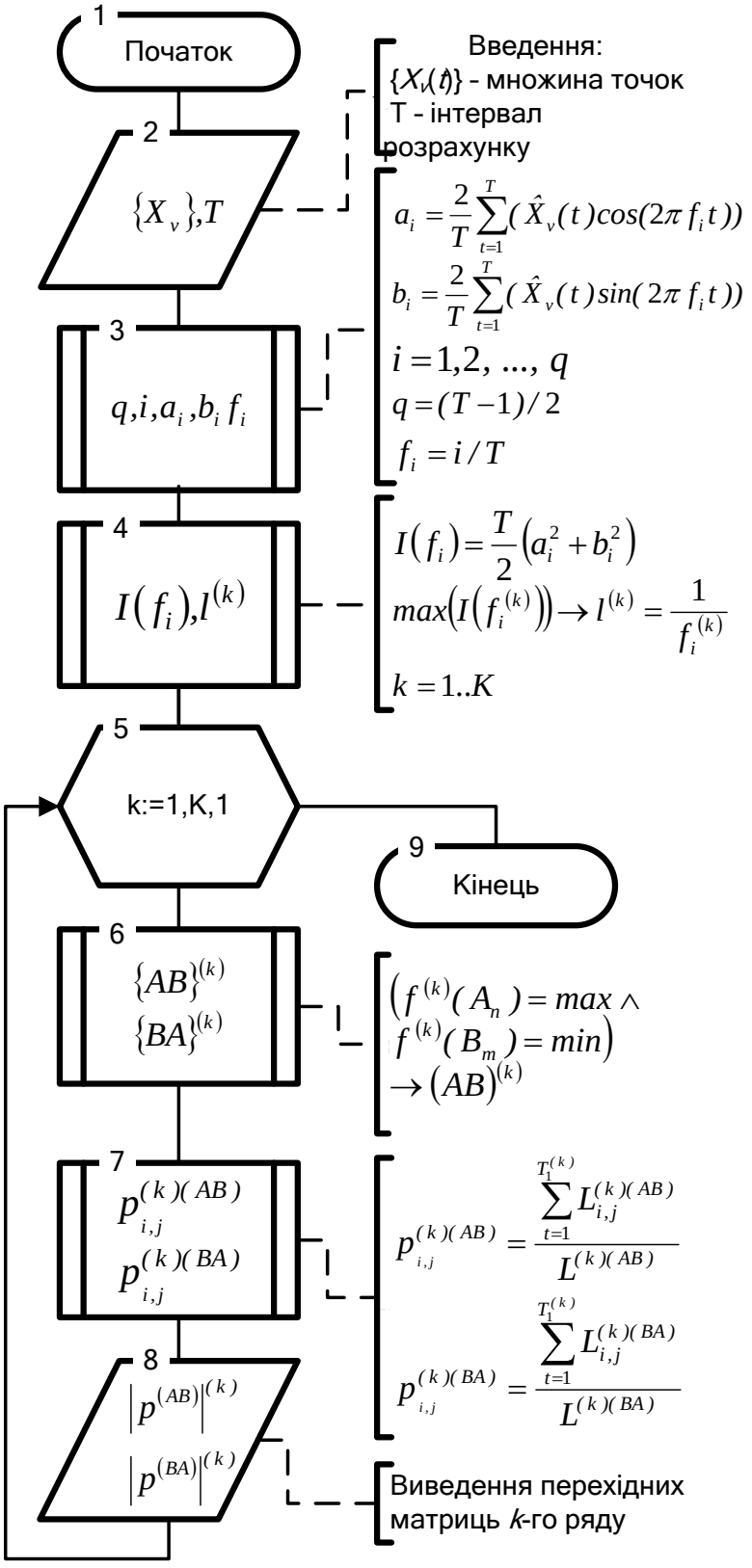

Рис. 4.2. Схема розрахунку параметрів ЛМ

Крок 2 – *визначення значущих періодів.* Виконання кроку, що відповідає вершині *4* (рис.4.2), орієнтоване на визначення значущих періодів вирівняного ряду $\hat{X}(t)$. Для цього на відрізку $[0,T]$ за допомогою.

$$I(f_i) = T\left(a_i^2 + b_i^2\right)/2 \tag{4.40}$$

формули будують періодограму вирівняного ряду даних

Найбільші величини періодограми відповідають значущим періодам процесу:

$$\max\left(I\left(f_i^{(k)}\right)\right) \to l^{(k)} = 1/f_i^{(k)},\ k = 1,2,\ldots K, \tag{4.41}$$

де K – кількість значущих періодів; $f_i^{(k)}$ – i-а частота ряду даних, що відповідає k-му значущому періоду; $l^{(k)}$ – k-й значущий період.

Якщо кількість значущих періодів $K = 1$, то використовується марковська модель одноперіодичного ШП. Якщо кількість значущих періодів $K > 1$, то використовується марківська модель багатоперіодичного ШП.

Крок 3 – *визначення нестаціонарних точок.* Робота цього кроку, якому відповідає вершина *6* рис. 4.2, полягає у визначенні нестаціонарних точок у межах кожного k-го періоду ($k \in 1,\ldots,K$). Для цього розраховують значення t, які відповідають точкам максимумів і мінімумів функції $f_k(t)$:

$$\left(f^{(k)}(A_n) = \max \wedge f^{(k)}(B_m) = \min\right) \to (AB)^{(k)} \forall\, n = 1\ldots N,\ m = 1\ldots M,\ k = 1\ldots K. \tag{4.42}$$

де $\{A\}_N$ – множина точок максимумів $f_k(t)$; $\{B\}_M$ – множина точок мінімумів $f_k(t)$.

Крок 4 – *розрахунок ймовірностей переходів*. На цьому кроці, якому відповідає вершина *7* (рис.4.2), розраховують матриці ймовірностей переходів. Статистичні дані на інтервалах *AB* використовують для розрахунку $\left|p^{(AB)}\right|$, а статистичні дані на інтервалах *BA* – для розрахунку $\left|p^{(BA)}\right|$.

Для розрахунку ймовірностей переходів із стану i у стан j на *AB* і *BA* кожного з k-го негомогенного ЛМ, що відповідає k-му виділеному одноперіодичному ряду, використовують вирази:

$$p_{i,j}^{(k)(AB)} = \sum_{t=1}^{T_1} L_{i,j}^{(k)(AB)} \Big/ L^{(k)(AB)}; \quad (4.43)$$

$$p_{i,j}^{(k)(BA)} = \sum_{t=1}^{T_2} L_{i,j}^{(k)(BA)} \Big/ L^{(k)(BA)}, \quad (4.44)$$

де $p_{i,j}^{(k)(AB)}$ – імовірність переходу між станами *i* та *j* на інтервалах типу *BA* на *k*-му періоді; $p_{i,j}^{(k)(BA)}$ – імовірність переходу між станами *i* та *j* на інтервалах типу *AB* на *k*-му періоді; $L^{(k)(AB)}$ – загальна кількість реалізацій, що перейшли зі стану *i* у стан *j* між *t*-ю та (*t*-1)-ю реєстрацією на *AB* на *k*-му періоді; $L^{(k)(BA)}$ – загальна кількість реалізацій, що перейшли зі стану *i* у стан *j* між *t*-ю та (*t*-1)-ю реєстрацією на *BA* на *k*–му періоді; T_1 – кількість реєстрацій на інтервалах типу *AB*; T_2 – кількість реєстрацій на інтервалах типу *BA*.

Етап 3 – *розрахунок імовірностей станів ЛМ.* На цьому етапі для кожного *k*-го ЛМ розраховують імовірність *i*-го стану в довільний момент часу ($P_i^{(k)}(t)$). Для цього матриці ймовірностей переходів $\left|p^{(AB)}\right|$ і $\left|p^{(BA)}\right|$ підставляються в систему рівнянь Колмогорова-Чепмена виду (3.39) та (3.40).

Етап 4 – *розрахунок імовірностей станів ММ.* На даному етапі для марковської моделі розраховують імовірність кожного зі станів. Використовують вираз:

$$P_i(t) = \frac{1}{K} \sum_{k=1}^{K} P_i^{(k)}(t), \quad (4.45)$$

де $P_i(t)$ – імовірність *i*-го стану марковської моделі в момент часу *t*; $P_i^{(k)}(t)$ – імовірність *i*-го стану для *k*-го ЛМ у момент часу *t*.

Етап 5 – *розрахунок поведінки.* На цьому етапі для заданого *t* розраховується очікуване значення ПБ:

$$\hat{X}(t) = M(t) + Y(t) + \overline{X}, \quad (4.46)$$

де $M(t)$ – математичне сподівання ПБ, розраховане за допомогою побудованої марковської моделі.

Розроблений метод став основою для створення прикладної програми

MarkPr, призначеної для побудови комп’ютерних моделей ШП нормалізованих ПБ.

Програма грунтується на виразах (3.36)–(3.38), (4.35)–(4.46) і дозволяє визначити основні параметри ЛМ.

Результати розрахунків записуються у файл та виводяться на екран комп'ютера у вигляді графіка математичного сподівання ПБ і графіків імовірностей розподілу ПБ за станами в точках:

$$0{,}2T;\ 0{,}4T;\ 0{,}6T;\ 0{,}8T;\ T,$$

де T – інтервал розрахунку.

У тих же точках виводяться величини ймовірностей розподілу за станами. Графік математичного сподівання – напівжирною лінією, а графіки розподілу ймовірностей показано звичайними лініями.

Для побудови показаних графіків розподілу ймовірностей вважається, що в межах стану ПБ є розподіленим за нормальним законом. Сірим кольором виділено площу розподілу, обмежену кожним із графіків розподілу ймовірностей. Для зручності вертикальна вісь рисунків має два ряди позначок – величину зведеного ПБ (x) і номер стану ЛМ (N). Припускається, що величини станів, на які поділяється діапазон можливих значень параметра, рівні між собою.

Інші параметри ЛМ – кількість квантів, імовірності (інтенсивності) переходів, термін функціонування та початковий розподіл імовірностей перебування можуть бути довільно задані.

Для прикладу на рис. 4.3 та 4.4 показано графіки математичного сподівання та розподілу імовірностей перебування марковської моделі ШП протягом 600 етапів розрахунку.

Рис. 4.3 відповідає стаціонарному ШП, що моделювався ЛМ з матрицею імовірностей переходів

$$\pi = \begin{vmatrix} 0{,}97 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0{,}01 & 0{,}96 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 & 0 & 0 \\ 0{,}01 & 0{,}01 & 0{,}95 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 & 0 \\ 0{,}01 & 0{,}01 & 0{,}01 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 \\ 0 & 0{,}01 & 0{,}01 & 0{,}01 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 \\ 0 & 0 & 0{,}01 & 0{,}01 & 0{,}01 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 & 0 \\ 0 & 0 & 0 & 0{,}01 & 0{,}01 & 0{,}01 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 \\ 0 & 0 & 0 & 0 & 0{,}01 & 0{,}01 & 0{,}01 & 0{,}95 & 0{,}01 & 0{,}01 \\ 0 & 0 & 0 & 0 & 0 & 0{,}01 & 0{,}01 & 0{,}01 & 0{,}96 & 0{,}01 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0{,}01 & 0{,}01 & 0{,}01 & 0{,}98 \end{vmatrix} \quad (4.47)$$

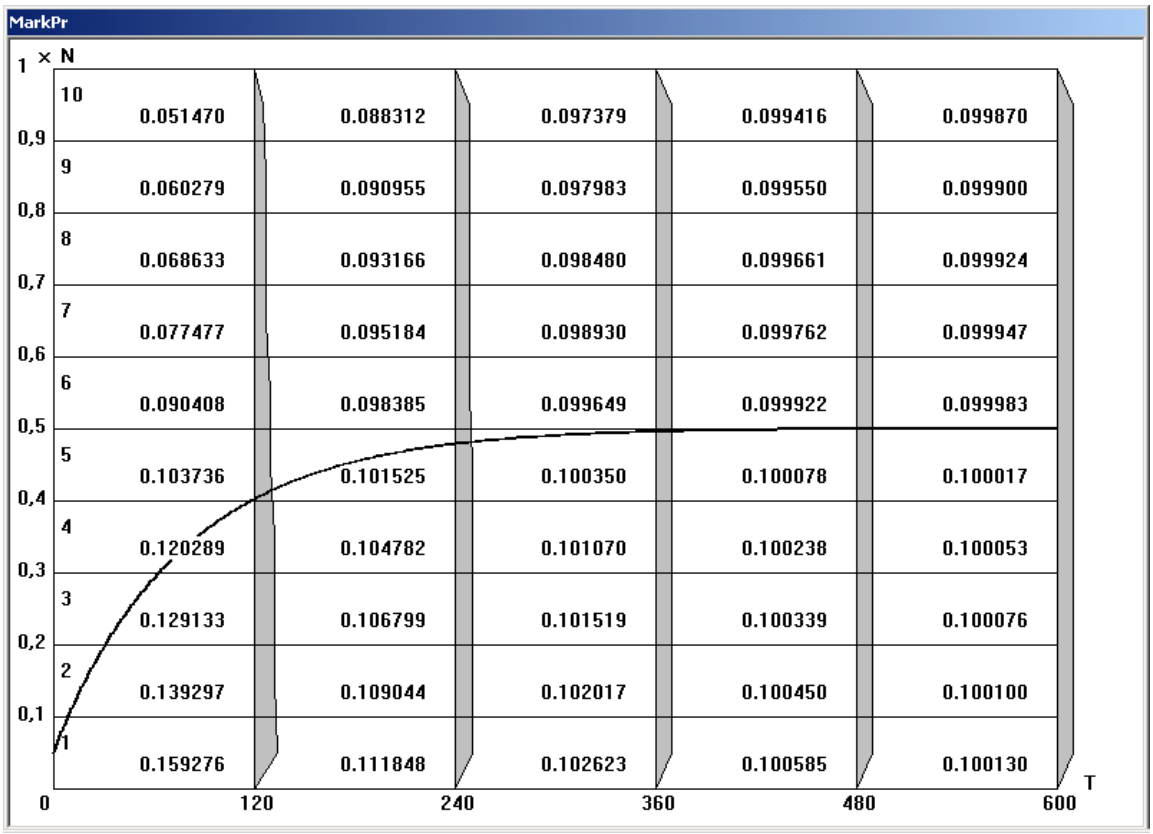

Рис. 4.3. Параметри стаціонарного ЛМ характерного ШНП

Графік рис. 4.4 відповідає марковській моделі двоперіодичного ШП. У марківській моделі використано два ЛМ з матрицями переходів заданих виразами (4.47), (4.48). Зазначимо, що матриця (4.48), отримана з матриці (4.47) подвоєнням величин імовірностей переходів з *i*-го стану в (*i*-1)-й, (*i*-2)-й і (*i*-3)-й стани.

$$\pi = \begin{vmatrix} 0{,}97 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0{,}02 & 0{,}96 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 & 0 & 0 \\ 0{,}02 & 0{,}02 & 0{,}95 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 & 0 \\ 0{,}02 & 0{,}02 & 0{,}02 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 & 0 \\ 0 & 0{,}02 & 0{,}02 & 0{,}02 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 & 0 & 0 \\ 0 & 0 & 0{,}02 & 0{,}02 & 0{,}02 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 & 0 \\ 0 & 0 & 0 & 0{,}02 & 0{,}02 & 0{,}02 & 0{,}94 & 0{,}01 & 0{,}01 & 0{,}01 \\ 0 & 0 & 0 & 0 & 0{,}02 & 0{,}02 & 0{,}02 & 0{,}95 & 0{,}01 & 0{,}01 \\ 0 & 0 & 0 & 0 & 0 & 0{,}02 & 0{,}02 & 0{,}02 & 0{,}96 & 0{,}01 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0{,}02 & 0{,}02 & 0{,}02 & 0{,}98 \end{vmatrix} \quad (4.48)$$

Нестаціонарні точки марківської моделі двоперіодичного ШП відповідають t_1=121, t_2=241, t_3=361, t_4=481 етапам розрахунку.

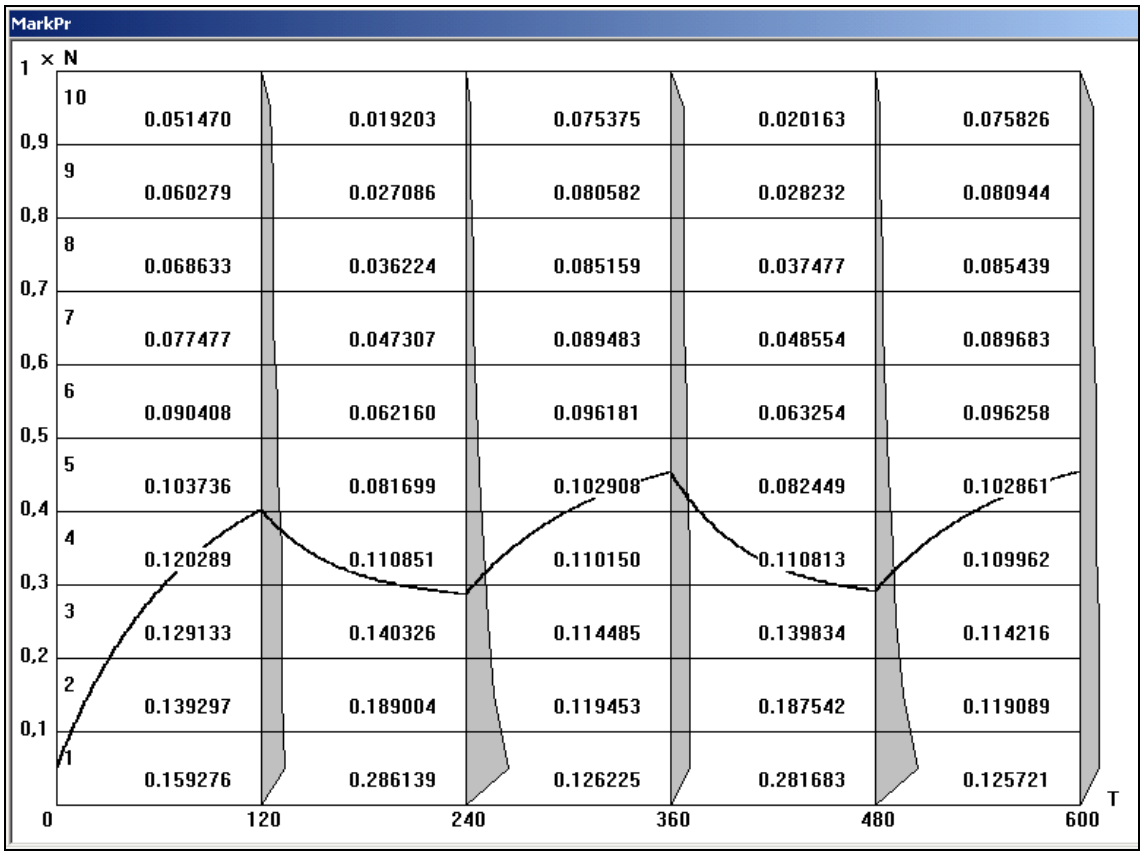

Рис. 4.4. Графіки параметрів одноперіодичної марковської моделі

Приклад використання методу для розроблення одноперіодичної та двоперіодичної марковської моделі ПБ веб-сервера наведено в підрозділі 3.3.

Зазначимо, що застосування марковської моделі ШП має враховувати специфіку захисту ресурсів інтернет-орієнтованих ІС і традиційних сфер застосування ШП. Найбільш перспективним і важливим є застосування ШП для розпізнавання мережевих кібератак на веб-сервери з метою викликати відмову в обслуговуванні та/або отримати несанкціонований доступ до ресурсів ІС. Хоча не слід виключати і можливість розпізнавання активності ШПЗ. Однак останній напрям потребує грунтовного доопрацювання. Тому при формуванні множини ПБ для побудови ШП слід розглядати тільки ті контрольовані параметри ІС, що можуть вказувати на зміну рівня захищеності їх ресурсів унаслідок реалізації мережевих кібератак. Ці параметри повинні відповідати характеристикам працездатного стану компонентів ресурсів та/або характеристикам мережевої кібератаки. До першого класу параметрів можна віднести завантаження центрального процесора, довжину черги мережевих запитів, кількість відкритих файлів, завантаження оперативної пам'яті, вільна ємність жорсткого диска, кількість процесів, що відбуваються в операційній системі. Зазначимо, що цей клас параметрів в основному дозволяє діагностувати зміну рівня захищеності мережевих ресурсів ІС унаслідок реалізації атаки з метою викликати відмову в обслуговуванні. До другого класу параметрів належать: інтенсивність загального, вхідного та вихідного мережевого трафіку та трафіку по кожному із мережевих протоколів (SNMP, ARP, TCP, IP, ICMP, HTTP), інтенсивність мережевих запитів різного типу, відношення правильних та неправильних мережевих пакетів за одиницю часу, кількість правильних та неправильних спроб уведення парольних даних. Цей клас параметрів можна застосовувати для розпізнавання атак на відмову в обслуговуванні та з метою отримання несанкціонованого доступу. Доцільно використовувати зареєстровані, фільтровані та зведені значення параметрів. Наприклад, кількість TCP/IP запитів (пакетів) за одиницю часу з однієї IP-адреси або з однієї підмережі. Остаточний перелік ПБ повинен базуватись на специфіці об'єкта захисту. Наприклад, у формуванні номенклатури

діагностичних параметрів для веб-сервера можна враховувати географію запитів, яку легко визначити на основі зворотної IP-адреси. Відповідний параметр – інтенсивність запитів до веб-серверу з обмеженої географічної зони, міг бути досить інформативним при розпізнаванні атаки на відмову в обслуговуванні державних веб-сайтів України, що сталися 2007–2012 рр. Адже за свідченнями засобів масової інформації вказана кібератака була реалізована з трьох досить обмежених географічних зон. Шаблон нормальної поведніки та ША можнаасформувати на основі одних і тих самих ПБ. При цьому діапазон зміни ПБ можна визначити на основі діапазону змін характеристик програмно-апаратного забезпечення ресурсів ІС. Наприклад, мінімальне завантаження центрального процесора X=0%, а максимальне X=100%. Визначення реальних $X_{\min}$ і $X_{\max}$ дозволяє перейти до моделювання з використанням нормалізованих величин:

$$x = (X - X_{\min})/(X_{\max} - X_{\min}), \tag{4.49}$$

де X – реальна величина ПБ; x – нормалізована величина ПБ.

Таким чином, $x_{\min} = 0$, а $x_{\max} = 1$, а $x \in [0,1]$.

Під час формування ШП на підставі деякого параметра X слід показати можливість застосування апарату марковської апроксимації для моделювання процесу зміни випадкової величини X на піддослідному інтервалі [t_1, t_2]. Для цього необхідно показати, що такий процес є випадковим, відповідає умові відсутності післядії, а функція $X = f(t)$ неперервна на інтервалі [t_1, t_2] [35]. Наприклад, для формування ШНП веб-сервера як ПБ можна використовуватизначення кількості звернень за одну секунду. Відповідно до праць [115, 267, 268] в умовах нормальної експлуатації вказаний параметр неперервний, а його величина є випадковою і залежить тільки від величини в поточний момент часу, що доводить відсутність післядії. Розвиток даного методу може бути спрямований на застосування в ШП декількох ПБ ІС. Також модель ШП може стати основою керувального ЛМ, призначеного для оптимізації параметрів засобів захисту ІС.

4.4. Метод визначення ефективності розроблення нейромережевих засобів оцінювання параметрів безпеки

Запропонований метод грунтується на розробленому підході до визначення ефективності розробки НМЗ оцінювання ПБ та на розробленій моделі створення ефективних НМЗ. У методі використано базові критерії оцінювання ефективності НМЗ, визначені в процесі аналізу відомих НМЗ, що використовуються в СЗІ для виявлення кібератак.

Вхідними даними методу є кортеж вигляду:

$$\langle \boldsymbol{У,О,М},D_{\min} \rangle, \tag{4.50}$$

де $\boldsymbol{У}$ – множина умов задачі оцінювання ПБ; $\boldsymbol{О}$ – множина характеристик об'єкта захисту; $\boldsymbol{М}$ – множина доступних НМЗ; N_m – кількість доступних НМЗ; $D_{\min}$ – мінімально допустима величина інтегральної ефективності.

Елементи $\boldsymbol{У,О,М}$ визначаються виразами (3.92), (3.91) та (3.90).

Реалізація методу полягає у виконанні п'яти етапів.

Етап 1 – *визначення базових критеріїв оцінки ефективності.* На цьому етапі для кожного $m_n \in \boldsymbol{М}$ за допомогою експертних даних визначаються величини елементів базової множини критеріїв оцінювання ефективності, розроблених у результаті аналізу сучасних НМЗ, що використовуються для виявлення кібератак:

$$\boldsymbol{\Phi} = \{\phi_{ов}, \phi_{ота}, \phi_{бва}, \phi_{ооа}, \phi_{боа}, \phi_{омн}, \phi_{веп}, \phi_{мна}, \phi_{дв}\}. \tag{4.51}$$

Компоненти $\boldsymbol{\Phi}$ призначені для оцінки НМЗ з точки зору $\varphi_{ов}$ – можливості попередньої обробки вхідних параметрів; $\varphi_{ота}$ –однокритеріальної оптимізації виду архітектури НММ; $\varphi_{бва}$ –багатокритеріальної оптимізації виду НММ, $\varphi_{ооа}$ – однокритеріальної оптимізації параметрів НММ; $\varphi_{боа}$ – багатокритеріальної оптимізації параметрів НММ; $\varphi_{омн}$ – оптимізації методу навчання НММ; $\varphi_{веп}$ – можливості використання експертних правил для навчання НММ; $\varphi_{мна}$ – можливості застосування у НМЗ різноманітних класичних і перспективних видів НММ; $\varphi_{дв}$ – визначення принципової оцінки доцільності застосування

НММ. У першому наближенні для визначення величин базових критеріїв оцінювання ефективності використовується дискретна трибальна шкала – -1,0,1. Критерій дорівнює -1, коли в НМЗ можливість не забезпечується, 0 – коли забезпечується частково і 1 – коли забезпечується повністю. У подальшому підхід до визначення величин критеріїв може бути вдосконалений.

Для кожного *n*-го НМЗ результатом виконання етапу є множина величин критеріїв $\mathbf{\Phi}_n$.

Етап 2 – *визначення напрямків вдосконалення НМЗ.* На цьому етапі за допомогою формули

$$\phi_i < 1, \tag{4.52}$$

виконується аналіз величин $\phi_i \in \mathbf{\Phi}, i = 1,2..,9$.

Якщо для *i*-го критерію вираз (4.62) справджується, то це вказує на можливість вдосконалення НМЗ у відповідному напрямі.

Етап 3 – *визначення вагових коефіцієнтів важливості базових критеріїв ефективності.* Етап спрямований на аналіз ***У*** та ***О*** для визначення вагових коефіцієнтів важливості елементів множини базових критеріїв ефективності відносно інтегральних критеріїв:

$$\boldsymbol{D} = \{d_{ткк}, d_{одв}, d_{анв}, d_{вуз}, d_{ооп}\}, \tag{4.53}$$

де $d_{ткк}$ – точність класифікації кібератак; $d_{одв}$ – можливість оцінки доцільності застосування НМЗ; $d_{анв}$ – рівень забезпечення адаптації до нових видів кібератак; $d_{вуз}$ – пристосованість до варіативності умов застосування; $d_{ооп}$ – пристосованість до функціонування за обмежених обчислювальних ресурсів.

Етап виконується за п’ять кроків, кожен з яких співвідноситься з визначенням коефіцієнтів важливості стосовно одного з інтегральних критеріїв.

Крок 1 – *розрахунок вагових коефіцієнтів для* $d_{ткк}$. Розраховуються вагові коефіцієнти базових критеріїв $\alpha_{1,ота}, \alpha_{1,бва}, \alpha_{1,омн}, \alpha_{1,опа}, \alpha_{1,бпа}, \alpha_{1,мна}$, необхідних для розрахунку залежності (2.7).

Крок 2 – *розрахунок вагових коефіцієнтів для* $d_{одв}$. Розраховуються вагові

коефіцієнти базових критеріїв $\alpha_{2,одв}$, необхідні для розрахунку залежності (2.8).

Крок 3 – *розрахунок вагових коефіцієнтів для* $d_{анв}$. Розраховуються вагові коефіцієнти базових критеріїв $\alpha_{3,веп}, \alpha_{3,мна}$, необхідні для розрахунку залежності (2.9).

Крок 4 – *розрахунок вагових коефіцієнтів для* $d_{вуз}$. Розраховуються вагові коефіцієнти базових критеріїв $\alpha_{4,ота}, \alpha_{4,бва}, \alpha_{4,мна}$, необхідні для розрахунку залежності (2.10).

Крок 5 – *розрахунок вагових коефіцієнтів для* $d_{ооп}$. Розраховуються вагові коефіцієнти базових критеріїв $\alpha_{5,по}, \alpha_{5,ота}, \alpha_{5,бва}, \alpha_{5,омн}, \alpha_{5,опа}, \alpha_{5,бпа}, \alpha_{5,мна}$, необхідні для розрахунку залежності (2.11).

Етап 4 – *розрахунок інтегральних критеріїв ефективності.* На цьому етапі виконується розрахунок величини кожного з інтегральних критеріїв $d_{ткк}$, $d_{одв}$, $d_{анв}$, $d_{вуз}$ $d_{ооп}$. Для розрахунку використовуються такі вирази:

$$d_{ткк} = 2^{\alpha_{1,ота}\varphi_{ота}+\alpha_{1,бва}\varphi_{бва}+\alpha_{1,омн}\varphi_{омн}+\alpha_{1,опа}\varphi_{опа}+\alpha_{1,бпа}\varphi_{бпа}+\alpha_{1,мна}\varphi_{мна}};$$

$$d_{одв} = 2^{\alpha_{2,одв}\varphi_{одв}};$$

$$d_{анв} = 2^{\alpha_{3,веп}\varphi_{веп}+\varphi_{мна}\alpha_{3,мна}};$$

$$d_{вуз} = 2^{\alpha_{4,ота}\varphi_{ота}+\alpha_{4,бва}\varphi_{бва}+\alpha_{4,мна}\varphi_{мна}};$$

$$d_{ооп} = 2^{\alpha_{5,по}\varphi_{по}+\alpha_{5,ота}\varphi_{ота}+\alpha_{5,бпа}\varphi_{бпа}+\alpha_{5,омн}\varphi_{омн}+\alpha_{5,опа}\varphi_{опа}+\alpha_{5,бва}\varphi_{бва}+\alpha_{5,мна}\varphi_{мна}}.$$

Етап 5 – *розрахунок вагових коефіцієнтів інтегральних критеріїв.* Етап спрямований на аналіз ***У*** та ***О*** для визначення вагових коефіцієнтів інтегральних критеріїв ефективності. У результаті аналізу формується множина вагових коефіцієнтів інтегральних критеріїв ефективності вигляду:

$$\boldsymbol{H} = \{\gamma_1, ..\gamma_5\},$$

де γ_1 – ваговий коефіцієнт *і*-го інтегрального критерію ефективності.

Етап 6 – *розрахунок генерального критерію ефективності*. На цьому етапі розраховується генеральний критерій ефективності НМЗ. Для цього

використовується вираз

$$D^{\Sigma} = \sum_{i=1}^{5} \gamma_i d_i \ ,$$

де $d_1=d_{ткк}$, $d_2=d_{одв}$, $d_3=d_{анв}$, $d_4=d_{вуз}$, $d_5=d_{ооп}$.

Етап 7 – *оцінка ефективності.* На цьому етапі остаточно оцінюється ефективность НМЗ. Для цього розрахована величина D^{Σ} порівнюється з мінімально допустимою величиною D_{min}:

$$D^{\Sigma} < D_{min}, \tag{4.54}$$

Якщо нерівність (4.54) справджується, то НМЗ може використовуватись тільки після виправлення недоліків, визначених на другому етапі. Серед декількох доступних НМЗ більш ефективним вважається той, показник D^{Σ} якого більший. Таким чином, вперше створено метод, який дає змогу розрахувати і порівняти інтегральну ефективність розробки НМЗ оцінювання ПБ та визначити напрямки вдосконалення таких засобів. Застосування методу до НМЗ, наведених у працях [1, 4, 7, 15, 19, 37, 48, 58, 59, 86, 87, 100, 111, 134, 146, 199, 212, 247-250, 252], дозволило визначити, що типовими недоліками більшості з них є низька пристосованість до використання всієї множини перспективних НММ, неможливість подання експертних даних у НММ, недостатнє обґрунтування доцільності використання НММ та вибору оптимального виду НММ.

4.5. Методологія нейромережевого оцінювання параметрів безпеки інформаційних систем

У результаті інтеграції запропонованих підходів, моделей та методів з відомими моделями та методами створення НМЗ для розпізнавання кібератак побудовано комплексну методологію оцінювання ПБ (рис. 4.6). Вхідними даними методології є кортеж, що складається із множини умов задачі оцінювання, характеристик об’єкта захисту та доступних видів НМЗ:

$$\langle \boldsymbol{У}, \boldsymbol{О}, \boldsymbol{М} \rangle .$$

Множина умов задачі оцінювання ПБ $\boldsymbol{У}$ визначається виразом (3.92), множина характеристик об'єкта захисту $\boldsymbol{О}$ визначається виразом (2.4), а множина доступних видів НМЗ $\boldsymbol{М}$ – виразом (3.90). У методології використовуються також експертні дані:

$\langle \boldsymbol{C}_1, \boldsymbol{C}_2, ..., \boldsymbol{C}_K \rangle$ – кортеж вагових коефіцієнтів вагомості ПБ та $\boldsymbol{B} = \{\beta_1, .. \beta_K\}$ – множина мінімальних значень коефіцієнтів вагомості ПБ, визначені в моделі інтеграції ПБ;

R_{max} – максимальна зведена різниця номенклатур ПБ, наведена в пілході до класифікації подібних кібератак;

$\boldsymbol{E}$ – множина критеріїв оптимізації; $\boldsymbol{V}$ – множина вагових коефіцієнтів критеріїв оптимізації виду НММ та k_E – коефіцієнт відхилення, наведені в підході до визначення оптимального виду НММ;

$\boldsymbol{Ф}$ – множина значень базових критеріїв оцінювання ефективності НМЗ; $D_{\min}$ – мінімально допустима ефективність НМЗ; $\boldsymbol{A}$, $\boldsymbol{H}$ – множини значень вагових коефіцієнтів базових та інтегральних критеріїв оцінки ефективності, наведені в методі визначення ефективності розробки НМЗ оцінювання ПБ;

$\boldsymbol{\Lambda} = \{\lambda_1, \lambda_2, ...\}$ – множина оптимізуємих параметрів НММ, що визначається на основі аналізу конкретного виду НММ;

$\varepsilon_{\max}$ – максимально допустима помилка розпізнавання НММ; $\xi_{\max}$ – максимально допустима обчислювальна складність НММ; T_a – допустимий термін створення НМЗ, що визначаються на основі аналізу поставленої задачі розпізнавання кібератак.

У базовому випадку обробляти експертні дані пропонується проводити методом парних порівнянь за допомогою виразів (3.16)–(3.30). Надалі можнавикористати інші методи оброблення експертних даних, наведені у працях [90, 110]. Результатом методології є визначення параметрів ефективніших НММ оцінювання ПБ для виявлення кібератак на обраний об'єкт захисту. Її реалізація полягає у виконанні дев'яти етапів:

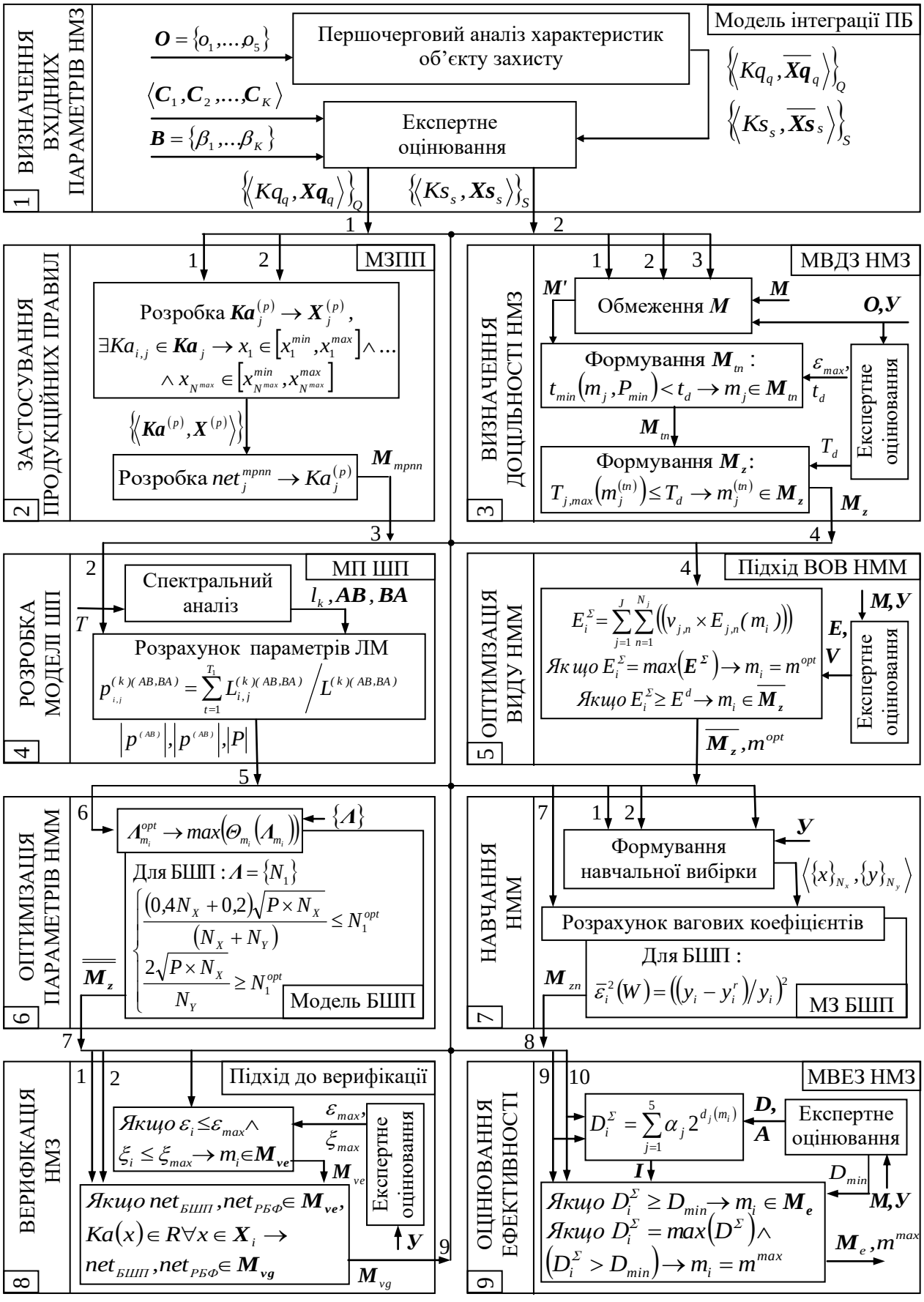

Рис. 4.6. Схема методології нейромережевого оцінювання ПБ

Етап 1 – *визначення вхідних параметрів НМЗ.* Виконання етапу полягає у застосуванні розробленої моделі інтеграції ПБ для визначення очікуваних множин ПК $\boldsymbol{Ks}$ і НК $\boldsymbol{Kq}$ та відповідних їм множин ПБ $\boldsymbol{Xq}$ і $\boldsymbol{Xs}$, що будуть використані як вхідні параметри НМЗ. Отже, вихідною інформацією етапу є вирази

$$\left\{\left\langle Kq_q, \boldsymbol{Xq}_q \right\rangle\right\}_Q;$$

$$\left\{\left\langle Ks_s, \boldsymbol{Xs}_s \right\rangle\right\}_S,$$

де $\boldsymbol{Xq}_q$, $\boldsymbol{Xs}_s$ – множини ПБ для розпізнавання q-ї НК та s-ї ПК.

Вхідною інформацією етапу є множини $\boldsymbol{O}$, $\boldsymbol{B}$ і кортеж $\langle \boldsymbol{C}_1, \boldsymbol{C}_2, ..., \boldsymbol{C}_K \rangle$. Етап виконується за два кроки.

Крок 1 – *першочерговий аналіз характеристик об'єкта захисту*. Першочерговий аналіз множини $\boldsymbol{O}$ полягає у побудові 1–4 процесів моделі інтеграції ПБ. Використовуються вирази (3.31)–(3.34). Результатом аналізу є

$$\left\{\left\langle Kq_q, \overline{\boldsymbol{Xq}}_q \right\rangle\right\}_Q, \tag{4.55}$$

$$\left\{\left\langle Ks_s, \overline{\boldsymbol{Xs}}_s \right\rangle\right\}_S, \tag{4.56}$$

де $\overline{\boldsymbol{Xq}}_q$, $\overline{\boldsymbol{Xs}}_s$ – у першому наближенні множини ПБ, що застосовуються для розпізнавання q-ї НК та s-ї ПК.

Крок 2 – *експертне оцінювання.* Крок орієнтовано на встановлення відповідності між k-м видом кібератаки та множиною ПБ, що використовується для її розпізнавання:

$$Ka_k \to \boldsymbol{X}_k.$$

Для цього за допомогою експертного оцінювання (4. 55, 4.56.) визначається кортеж $\langle \boldsymbol{C}_1, \boldsymbol{C}_2, ..., \boldsymbol{C}_K \rangle$ та множина $\boldsymbol{B}$. Для встановлення відповідності (4.56) використовується математичний апарат п'ятого процесу моделі інтеграції ПБ.

Етап 2 – *застосування продукційних правил*. Призначенням цього етапу є

навчання НММ оцінювання ПБ за рахунок подання в них експертних знань про відповідність величин ПБ з наявністю/відсутністю очікуваних кібератак.

У базовому варіанті подання експертних знань реалізується за допомогою розробленого методу застосування продукційних правил для навчання НМ типу MPNN. В подальшому можуть використовуватись і інші методи подання експертних знань.

Етап виконується за 2 кроки. Крок 1 відповідає трутьому і четвертому етапам, а крок 2 відповідає п'ятому-дусятому етапам методу застосування продукційних правил.

Крок 1 – *визначення ПБ для розпізнавання подібних кібератак.* Призначанням даного кроку є визначається множини ПБ, котрі використовуються для розпізнавання множини подібних кібератак:

$$\left\{\left\langle \boldsymbol{Ka}^{(p)}, \boldsymbol{X}^{p} \right\rangle\right\}. \tag{4.57}$$

Для визначення (4.57) використовується математичний апарат (4.1)–(4.9).

Крок 2 – *розробка моделей MPNN*. Крок орієнтовано на розроблення множини MPNN, кожна з яких призначена для розпізнавання окремого виду подібних кібератак.

Крок 3 У процесі розроблення використовується математичний апарат (4.10)–(4.20).

Вихідною інформацією етапу є:

$$\boldsymbol{M}_{mpnn} = \left\{net_1^{mpnn}, \ldots, net_{M_{mpnn}}^{mpnn}\right\}$$

де net_j^{mpnn} – j-а MPNN, призначена для розпізнавання $\boldsymbol{Ka}_j^{(p)} \in \overline{\boldsymbol{Ka}}^{(p)}$.

Етап 3 – *визначення доцільності застосування НМЗ*. На цьому етапі визначається множина НМЗ $\boldsymbol{M}_z$, які доцільно застосувати для оцінювання інтегрованих ПБ.

Етап 4 Вхідними даними етапу є множини $\boldsymbol{O}$, $\boldsymbol{У}$, $\boldsymbol{M}$, $\boldsymbol{M}_{mpnn}$, $\langle \boldsymbol{Kq}, \boldsymbol{Xq} \rangle$ і $\langle \boldsymbol{Ks}, \boldsymbol{Xs} \rangle$.

Етап 5 Етап реалізується за рахунок виконання 2–12 етапів методу визначення доцільності застосування НМЗ. Відповідний математичний апарат задається виразами (4.21)–(4.32). Для формування $\boldsymbol{M}_z$ використовуються правила (4.33)–(4.34).

Етап 6 – *розробка моделі шаблону поведінки*. Етап орієнтовано на розроблення марковської моделі ШП, що використовується для розпізнавання очікуваних ПК. Вхідними даними етапу є множина параметрів ПБ $\boldsymbol{Xs}$, що залежать від терміну експлуатації об'єкта захисту і використовуються для розпізнавання ПК.

Етап 7 Марковська модель розробляється за допомогою створеного методу проектування ШП ПБ. Застосовується математичний апарат (4.35)–(4.44). Виходом етапу є множини перехідних матриць $\boldsymbol{p}^{(AB)}$, $\boldsymbol{p}^{(BA)}$ та матриця ймовірностей станів $|P(t)|$ марковської моделі ШП ПБ.

Етап 8 – *оптимізація виду НММ.* На цьому етапі визначається множина оптимальних видів НММ вигляду

$$\overline{\mathrm{M}_z} = \left\{m_1^{\mathrm{opt}},\ldots,m_I^{\mathrm{opt}}\right\}.$$

Вхідними даними є множини $\boldsymbol{M_z}$, $\boldsymbol{E}$, $\boldsymbol{V}$. Етап грунтується на розробленому підході до оптимізації і виконується за три кроки:

Крок 1 – *розрахунок інтегрального критерію оптимізації НММ*. Для елементів $\boldsymbol{M_z}$ розраховується множина інтегральних критеріїв оптимізації:

$$\boldsymbol{E}^{\Sigma} = \left\{E_1^{\Sigma},\ldots,E_{N_m}^{\Sigma}\right\};$$

$$E_i^{\Sigma} = \sum_{j=1}^{J}\sum_{n=1}^{N}\left(\left(v_{j,n}E_{j,n}(m_i)\right)\right),\ i=1,2,\ldots,I\ ,$$

де $E_{j,n}$ – оцінка n-го критерію в j-й категорії для i-ї НММ; $v_{j,n}\in\boldsymbol{V}$ – ваговий коефіцієнт n j-го критерію оптимізації; I – кількість допустимих НММ; J – кількість категорій критеріїв; N_J – кількість критеріїв в J-й категорії.

Крок 2 – *визначення оптимального виду моделі.* Визначається оптимальний вид НММ. Для цього використовується правило:

$$\textit{як}\ \text{що}\ E_i^{\Sigma} = \max\left(\mathrm{E}^{\Sigma}\right) \to m_i = m^{\mathrm{opt}}.$$

Крок 3 – *формування множини оптимальних видів НММ.* Для формування множини $\overline{\boldsymbol{M}_z}$ використовуються вирази:

$$\textit{я}\ \text{кщо}\ E_i^{\Sigma} \geq E^d \to m_i \in \boldsymbol{M}^{\mathrm{opt}};$$

$$E^d = k_E E^{\Sigma}\left(m^{opt}\right),$$

де $k_E = 0{,}8$ (у першому наближенні).

Етап 9 – *оптимізація параметрів НММ.* Етап орієнтовано на визначення $\overline{\overline{\boldsymbol{M}_z}}$ – множини оптимальних видів НММ з оптимізованими параметрами. Вхідною інформацієї етапу є множина $\overline{\boldsymbol{M}_z}$. Використано критерій оптимізації

$$\boldsymbol{\Theta}(\boldsymbol{\Lambda}) \to \max,$$

де $\boldsymbol{\Theta}$ – обчислювальна потужність моделі.

Розрахунок оптимальних величин $\{\lambda_1, \lambda_2, ...\}$ виконується за методами, специфічними для виду НММ. У випадку використання БШП, який в більшості випадків входить до складу $\overline{\boldsymbol{M}_z}$, етап виконується з використанням розробленої структурної моделі. Діапазон оптимальних параметрів визначається за виразами (3.61), (3.62).

Етап 10 – *навчання НММ.* Етап орієнтовано на розрахунок $\boldsymbol{M}_{zn}$ множини вагових коефіцієнтів синаптичних зв'язків НММ, що входять до множини $\overline{\overline{\boldsymbol{M}_z}}$. Етап виконується за два кроки.

Крок 1 – *формування навчальної вибірки*. На цьому кроці формується навчальна вибірка НМ. Для НМ, що навчаються «з учителем», навчальна вибірка являє собою кортежі виляду $\left\langle \{x\}_{N_x}, \{y\}_{N_y} \right\rangle$, а для НМ, що самонавчаються – множини $\{x\}_{N_x}$.

Крок 2 У випадку розпізнавання $\boldsymbol{Kq}$ множина вхідних параметрів $\{x\}_{N_x}$ формується на основі $\boldsymbol{Xq}$, а у випадку розпізнавання $\boldsymbol{Ks}$ – на основі множини $\boldsymbol{Xs}$ та множини відхилень $\boldsymbol{Xs}$ від ШП $\boldsymbol{DXs}(t)$. Відхилення *i*-го ПБ у момент

часу t від ШП розраховується так:

$$DXs_i(t) = MXs_i(t) - Xs_i(t),$$

де $Xs_i(t)$ – величина i-го ПБ у момент часу t; $MXs_i(t)$ – математичне сподівання i-го ПБ, розраховане за допомогою марковської моделі ШП.

Обсяг навчальної вибірки P_n розраховується за допомогою виразу (4.27). Із навчальної вибірки виділяється тестова вибірка обсягом $P_t = 0{,}05P_n$.

Крок 3 – *реалізація процесу навчання.* У процесі подання навчальних прикладів розраховуються вагові коефіцієнти синаптичних зв'язків за допомогою методів, характерних для виду НММ. Для БШП вагові коефіцієнти коригуються за використовується розробленими виразами (2.34), (2.35), (2.42), (2.43).

Етап 11 – *верифікація НМЗ.* Етап орієнтовано на верифікацію НМЗ з позицій достатньої обчислювальної потужності та можливості нейромережевої апроксимації піддослідної функції зміни ПБ. Для кожної кібератаки $Ka_i \in \boldsymbol{Ka}$ етап реалізується за два кроки:

Крок 1 – *визначення достатньої обчислювальної потужності*. Виконання цього кроку полягає у реалізації правила:

$$якщо\ \exists m_i \in \boldsymbol{M}_z\ \varepsilon_i \le \varepsilon_{\max} \wedge \xi_i \le \xi_{\max} \to m_i \in \boldsymbol{M}_{ve},$$

де ε_i – помилка узагальнення для m_i; ξ_i – обчислювальна складність навчання m_i; $\boldsymbol{M}_{ve}$ – множина НМЗ верифікованих експериментально.

В першому наближенні ε_i дорівнює помилці навчання m_i на тестовій вибірці, а ξ_i – кількості навчальних ітерацій m_i.

Крок 2 – *доведення гладкості функції.* Крок виконується за умови

$$net_{\text{БШП}} \wedge / \vee net_{\text{РБФ}} \in \boldsymbol{M}_{ve},$$

де $net_{\text{БШП}}, net_{\text{РБФ}}$ – НМЗ на основі БШП та РБФ.

Виконання кроку базується на розробленому підході і полягає у доведенні того, що

$$Ka_i = f_i(\boldsymbol{X}_i) \to гладка\ функція,$$

де $\boldsymbol{X}_i$ – множина ПБ, що використовуються для розпізнавання Ka_i.

Доведення реалізується за допомогою експертного оцінювання множин $\boldsymbol{У, О, X}_i$. Якщо гладкість функції доведена, то $\boldsymbol{M}_{vg}$ – множина гарантовано верифікованих НМЗ складається із БШП і РБФ. У противному випаку $\boldsymbol{M}_{vg} = \varnothing$. Вихідною інформацією етапу є $\boldsymbol{M}_{ve}$ – множина НМЗ верифікованих експериментально і $\boldsymbol{M}_{vg}$ – множина гарантовано верифікованих НМЗ.

Етап 12 – *оцінювання ефективності НМЗ.* Призначенням етапу є розроблення множини ефективних НМЗ та визначення шляхів їх можливого вдосконалення. Для цього використовується розроблений метод оцінювання ефективності. Вхідними даними етапу є $\langle \boldsymbol{У, О, M}_{ve}, \boldsymbol{M}_{vg}, D_{min} \rangle$. Етап виконується за два кроки. Крок 1 відповідає першому, третьому-шостому етапам, а крок 2 – сьомому етапу методу оцінювання ефективності.

Крок 1 – *розрахунок показників ефективності.* На цьому кроці визначаються величини елементів $\boldsymbol{Ф, D, A}$, за допомогою яких для кожного $m_i \in \boldsymbol{M}_{ve}$ розраховується інтегральний показник ефективності D_i^{Σ}. Для визначення елементів $\boldsymbol{Ф, D, A}$ використовуються вирази (4.46), (4.47)–(4.52). Для розрахунку D_i^{Σ} – вираз (4.53).

Крок 2 – *порівняння ефективності.* Крок призначено для формування $\boldsymbol{M}_e$ – множини ефективних НМЗ $\boldsymbol{M}_e$ та визначення найбільш ефективного НМЗ. Для формування $\boldsymbol{M}_e$ використовується правило

$$якщо\ D_i^{\Sigma} > D_{\min} \rightarrow m_i \in \boldsymbol{M}_e .$$

Правило для визначення найбільш ефективного НМЗ виглядає так:

$$якщо\ D_i^{\Sigma} = \max(D) \wedge \left(D_i^{\Sigma} > D_{\min}\right) \rightarrow m_i = m^{\max} .$$

Виходом цього етапу є $\boldsymbol{M}_e$ – множина ефективних НМЗ і $m^{\max}$ – найбільш ефективний НМЗ.

Проведено порівняння ефективності відомих нейромережевих методів розпізнавання кібератак та запропонованої методології нейромережевого

оцінювання ПБ ІС – КМНО. Для цього застосовано розроблений метод оцінювання ефективності.

Величини базових критеріїв оцінювання ефективності наступні: $\varphi_{по}=0$, $\varphi_{ота}=1$, $\varphi_{бва}=1$, $\varphi_{опа}=1$, $\varphi_{бпа}=0$, $\varphi_{омн}=0$, $\varphi_{веп}=1$, $\varphi_{мна}=1$, $\varphi_{дв}=1$.

Визначені вагові коефіцієнти базових критеріїв оптимізації: $\alpha_{1,ота}=0{,}5$, $\alpha_{1,бва}=1$, $\alpha_{1,опа}=0{,}5$, $\alpha_{1,бпа}=1$, $\alpha_{1,омн}=1$, $\alpha_{1,мна}=0{,}5$, $\alpha_{2,одв}=1$, $\alpha_{3,веп}=1$, $\alpha_{3,мна}=0{,}5$, $\alpha_{4,ота}=0{,}5$, $\alpha_{4,бва}=1$, $\alpha_{4,мна}=1$, $\alpha_{5,по}=0{,}5$, $\alpha_{5,ота}=0{,}5$, $\alpha_{5,бва}=1$, $\alpha_{5,опа}=0{,}5$, $\alpha_{5,бпа}=1$, $\alpha_{5,омн}=0{,}5$, $\alpha_{5,мна}=0{,}5$. В першому наближенні припускається, що всі вагові коефіцієнти інтегральних критеріїв дорівнюють $\gamma=1$, а для розрахунку генерального критерію ефективності застосовано вираз (4.53).

Визначені критерії ефективності відомих нейромережевих методів та розробленої методології. Аналіз отриманих результатів свідчить, що використання запропонованої методології дозволяє підвищити генеральний показник ефективності розроблення в 3,85 разів відносно найкращих нейромережевих методів подібного призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.

2. Айвенс К. Компьютерные сети / К. Айвенс ; пер. с. англ. – СПб. : Питер, 2006. – 304 с.

3. Андерсон Т. Статистический анализ временных рядов / Т. Андерсон Т; пер. с. англ. И. Г. Журбенко. – М. : Мир, 1976. – 757 с.

4. Артеменко А.В., Анализ нейросетевых методов распознавания компьютерных вирусов / А.В. Артеменко, В.А. Головко //Материалы секционных заседаний. Молодежный инновационный форум «ИНТРИ» – 2010. — Минск: ГУ «БелИСА», 2010. – С. 47–48.

5. Архипов А. Применение моделей обнаружения аномалий для выявления атак / А. Архипов, А. Ишутин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. конф., 1–3 берез. 2006 р. : тези доп. – К., 2006. – С. 71–72.

6. Барский А. Б. Нейронные сети: распознавание, управление, принятие решений / А. Б. Барский. – М. : Финансы и статистика, 2004. – 176 с.

7. Безобразов С.В. Алгоритмы исскуственных имунных систем и нейронних сетей для обнаружения вредоносных программ / С.В.Безобразов, В.А.Головко//Нейроинформатика. – 2010. – №7. – С. 273–288.

8. Безруков Н. Н. Компьютерная вирусология / Н. Н. Безруков. – К. : Инкомбук, 1990. – 450 с.

9. Беллман Р. Процессы регулирования с адаптацией / Беллман Р. ; пер. с. англ. – М. : Наука, 1964. – 364 с.

10. Беляев А. Системы обнаружения аномалий: новые идеи в защите информации / А. Беляев, С. Петренко // Экспресс-Электроника. – 2004. – № 2.

– С. 12–14.

11. Берзон В. Е. Об одном подходе к проблеме автоматического реферирования и автоматического свертывания индексируемых текстов / В. Е. Берзон // НТИ. Сер.2.– 1971, № 10.– С.16-21.

12. Білощицький А. О. Інформаційна система для прогнозування і прийняття рішень у фінансовій сфері / А. О.Білощицький, О.Ю. Берзлев // Зб.наук. праць: Управління розвитком складних систем. – К.:КНУБА, 2014. – Вип. 18. – С. 106-111.

13. Білощицький А. О. Оптимізація системи пошуку збігів за допомогою використання алгоритмів локально-чутливого хешування наборів текстових даних / А. О. Білощицький, О.В. Діхтяренко //Зб.наук. праць: Управління розвитком складних систем.– К.:КНУБА, 2014. – Вип. 19. – С. 113-115.

14. Білощицький А. О. Способи пошуку неточних дублікатів зображень в наукових роботах. / А. О. Білощицький, О.В. Діхтяренко // Зб.наук. праць: Управління розвитком складних систем. – К.:КНУБА, 2015. – Вип. 21. – С. 149-153.

15. Блюменау Д. И. Экстрагирование как один из подходов к автоматизации реферирования / Д. И. Блюменау, И. С. Добронравов, Д. Г. Лахути // НТИ. Сер.2. – 1982. – № 2. – С. 108–128.

16. Богуш В.М. Інформаційна безпека: термінологіч. навч. довід. / В. М. Богуш, В. Г. Кривуца , А. М. Кудін. – К. : ДВК, 2004. – 508 с.

17. Бокс Дж. Анализ временных рядов, прогноз и управление / Бокс Дж., Дженкинс Г. М.; пер. с англ. – М. : Радио и свіязь, 1969. – 408 с.

18. Большев А. К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. дисс. на соискание научн. степени канд. техн. наук : спец. 05.13.19 – Методы и системы защиты информации, информационная безопасность / А. К. Большев – Спб, 2011. – 36 с.

19. Браіловський М. М. Захист інформації у банківській діяльності / М.

М. Браіловський, Г. П. Лазарєв, В. О. Хорошко. – К. : ПоліграфКонсалтинг, 2004. – 216 с.

20. Бриллинджер Д. Р. Временные ряды. Обработка данных и теорія / Д. Р. Бриллинджер ; пер. с англ. А. В. Булинского. – М. : Мир, 1980. – 536 с.

21. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С. 104–114.

22. 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.

23. Вапник В. Н. Восстановление зависимостей по эмпирическим данням / В. Н. Вапник. – М. : Наука, 1979. – 448 с.

24. Вентцель Е. С. Элементы теории игр / Е. С. Вентцель. – М. : Гос. изд. физ.-мат. лит., 1961. – 68 с.

25. Вентцель Е. С. Исследование операций / Е. С. Вентцель. – М. : Сов. радио, 1972. – 552 с.

26. Вентцель Е.С. Теория вероятностей / Е. С. Вентцель, Л. А. Овчаров. – М. : Наука,1976. – 378 с.

27. Вилков А.С. Информационная безопасность персональных ЭВМ и мониторинг компьютерных сетей / А.С. Вилков. – М. : МИНИТ ФСБ России, 2005. – 210 с.

28. Волосов К. А. Методика анализа эволюционных систем с распределенными параметрами специальность: дис. … доктора. техн. наук: 05.13.01 / К. А. Волосов – М., 2007. – 264 с.

29. Вороновский Г. К. Генетические алгоритмы, искусственные нейронные сети и проблемы виртуальной реальности / Г. К. Вороновский, К. В. Махотило, С. А. Сергеев. – Харьков: Основа, 1997. – 112 с.

30. Галушкин А. И. Теория нейронных сетей / А. И. Галушкин. – М. :

ИПРЖР, 2000. – 416 с.

31.Гареев А. Ф. Применение вероятностной нейронной сети для автоматического рубрицирования текстов / А. Ф. Гареев // Нейроинформатика-99 : науч. конф., 20-22 января 1999 г. : тезисы докл. – М., 1999. – С. 71–79.

32.Гарнаев А. Ю. Microsoft Office 2000 / А. Ю. Гарнаев. – СПб. : БХВ, 2000. – 656 с.

33.Глибовець М. М. Штучний інтелект / М. М. Глибовець, О. В. Олецький. – К. : Києво-Могилян. акад., 2002. – 366 с.

34.Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк // Безпека інформації. – 2013. – Т. 9, №2. – С. 118 – 129.

35.Головко В. А. Нейронные сети: обучение, организация и применение / В. А. Головко. – М. : ИПРЖР, 2001. – 256 с.

36.Горбань А. Н. Нейронные сети на персональном компьютере / А. Н. Горбань, Д. А. Россиев. – Новосибирск : Наука, 1996. – 276 с.

37.Горбань А. Н. Обучение нейронных сетей / А. Н. Горбань. – М. : ParaGraph, 1990. – 160 с.

38.Горбань А. Н. Визуализация данных методом упругих карт / А. Н. Горбань, А. Ю. Зиновьев, А. А. Питенко // Информационные технологии, – 2000. – № 6. – С. 26–35.

39.Грамматический словарь русского языка: Словоизменение / [сост. Зализняк А. А.] – М. : Рус. яз., 1980. – 880 с.

40.Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак / А.В. Гришин // Информационные технологии и вычислительные системы – 2011. – №1. – С. 53 -64.

41.Данілов В. О. Розроблення процесу оптимальної модернізації телефонного електрозв’язку : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец 05.13.06 «Автоматизовані системи управління та прогресивні

інформаційні технології» / В. О. Данілов. – К., 2003. – 19 с.

42. Джерри Х. Реестр Microsoft Windows XP / Джерри Х. ; пер. с англ. – М. : Эком, 2006. – 656 с.

43. Довлад О. А. Дослідження та розробка моделі процесу атаки та трафіку локальної мережі / О. А. Довлад // Захист інформації. – 2009. – № 1 – С. 83–86.

44. Додонов А. Г. Живучесть информационных систем / Додонов А. Г., Д. В. Ландэ. – К. Наук. думка, 2011. – 256 с.

45. Дорогов А. Ю. Структурный синтез быстрых нейронных сетей / А. Ю. Дорогов // Нейрокомпьютер. – 1999. – № 1 – С. 11–24.

46. Дорогов А. Ю. Структурный синтез двухслойных быстрых нейронных сетей / А. Ю. Дорогов // Кибернетика и системный анализ. – 2000. – № 4. – С. 47–56.

47. Дорогов А. Ю. Быстрые нейронные сети / А. Ю. Дорогов, А. А. Алексеев // Пятьдесят лет развития кибернетики : междунар. науч.-техн. конф., 5–7 окт. 1999 г. : тезисы докл. – СПб., 1999. – С. 120–121.

48. Дорогов А. Ю. Категории ядерных нейронных сетей / А. Ю. Дорогов, А. А. Алексеев // Нейроинформатика-99 : науч. конф., 20-22 января 1999 г. : тезисы докл. – М., 1999. – С. 55–64.

49. Дударь З. В. Реализация нейронов в семантических нейронных сетях / З. В. Дударь, Д. Е. Шуклин // Радиоэлектроника и информатика. – Х., 2000. – № 4. – С. 89–96.

50. Дударь З. В. Семантическая нейронная сеть как формальный язык описания и обработки смысла текстов на естественном языке / З. В. Дударь, Д. Е. Шуклин // Радиоэлектроника и информатика. – Х., 2000. – № 3. – С. 72–76.

51. Дьяконов М.Ю. Нейросетевая система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем: автореф. дисс. на соискание науч. степени канд. техн. наук : спец. 05.13.19

«Методы и системы защиты информации, информационная безопасность» / М. Ю. Дьяконов – Уфа, 2010. – 28 с.

52. Ежов А. А. Нейрокомпьютинг и его применения в экономике и бизнесе / А. А. Ежов, С. А. Шумский. – М. : МИФИ, 1998. – 224 с.

53. Ермаков А. Е. Поиск фактов в тексте / А. Е. Ермаков // Мир ПК. – 2005. – №2. – С. 64–66.

54. Ермаков А. Е. Проблемы полнотекстового поиска и их решение / А.Е. Ермаков // Мир ПК. – 2001. – №5. – С. 64–66.

55. Ермаков А. Е. Тематический анализ текста с выявлением сверхфразовой структуры /А. Е. Ермаков // Информационные технологии. – 2000. – №11. – С. 45–47.

56. Ермаков А. Е. Эксплицирование элементов смысла текста средствами синтаксического анализа-синтеза / А. Е. Ермаков // Компьютерная лингвистика и интеллектуальные технологи : междунар. науч. конф., 12–14 окт. 2003 г. : тезисы докл. – М., 2003. – С. 136–140.

57. Ермаков А. Е. Компьютерная морфология в контексте анализа связного текста / А. Е. Ермаков, В. В. Плешко // Компьютерная лингвистика и интеллектуальные технологи : междунар. науч. конф., 16–18 окт. 2004 г. : тезисы докл. – М., 2004. – С. 185–190.

58. Ермаков А. Е. Компьютерный анализ текста при сборе информации к досье из открытых источников / А. Е. Ермаков, В. В. Плешко // Конкурентная разведка в металлургии : междунар. науч. конф., 19–20 янв. 2005 г. : тезисы докл. – М., 2005. – С. 124–126.

59. Ермаков А. Е. Синтаксический разбор в системах статистического анализа текста / А. Е. Ермаков, В. В. Плешко // Информационные технологии. – 2002. – № 7. – С. 30–34.

60. Ермаков А. Е. Тематическая навигация в полнотекстовых базах данных / А. Е. Ермаков, В. В. Плешко // Мир ПК. – 2001. – № 8. – С. 52–55.

61. Емельянова Ю. Г. Анализ проблем и перспективы создания

интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления / Ю. Г. Емельянова, В. П. Фраленко // Программные системы: теория и приложения: электрон. науч. журн. – 2011. – № 4(8). – С. 17–31. [Электронный ресурс]. URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf.

62. 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.

63. Жульков Е. Поиск уязвимостей в современных системах IDS / Е. Жульков // Открытые системы. – 2003. – № 7–8. – С. 16–18.

64. Заенцев И.В. Нейронные сети: основные модели / И. В. Заенцев. – Воронеж : Воронежский гос. ун-т, 1999. – 76 с.

65. Зайцев О. Нейросети в системах безопасности/О.Зайцев // IT-Спец. – 2007. – № 6. – С. 54–59.

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

67. Захарова М.В. Програмна модель процесу вибору ефективних механізмів захисту інформаційних ресурсів / М.В. Захарова, А.О. Корченко, І.В. Хропата // Захист інформації. – 2011. – №2 (51). – С. 129-134.

68. Замаруева И.В. Математические модели семантики свободных словосочетаний с родовидовыми компонентами и их применение в АИС : дис. ... канд. техн. наук : 05.13.23 / Замаруева Ирина Валерьевна. – Х., 1990. – 134 с.

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

70. Зиновьев А. Ю. Визуализация многомерных даннях / А. Ю. Зиновьев. – М. : СК Пресс, 2005. – 180 с.

71. Зиновьев А. Ю. Визуализаци данных методом упругих карт / А. Ю.

Зиновьев, А. А. Питенко // Радіоелектроніка. Інформатика. Управління.– 2000. – № 1. – С. 76–85.

72. Зуев А. В. Определение оптимальной совокупности контролируемых параметров при косвенном контроле средств защиты информации / А. В. Зуев , Ю. М. Хмелько // Защита информации : сб. науч. тр. – К. : НАУ, 2000. – С.70–75.

73. Иванов А.И. Быстрое обучение искусственных нейронных сетей в системах биометрической аутентификации личности : автореф. дисс. на соискание научн. степени доктора. техн. наук : спец. 05. 13. 01 «Управление в технических системах» / А. И. Иванов – Пенза, 2000. – 36 с.

74. Игнатов В. А. Элементы теории оптимального обслуживания технических изделий / В. А. Игнатов, Г. Г. Маньшин, В. В. Костановский. – Минск : Наука и техника, 1974. – 192 с.

75. Игнатов В. А. Статистическая оптимизация качества функционирования электронных систем / В. А. Игнатов, Г. Г. Маньшин, В. А. Трайнев. – М. : Энергия, 1974. – 264 с.

76. Ильницкий С. В. Работа сетевого сервера при самоподобной (self-similar) нагрузке / С. В. Ильницкий // сб. науч. Тр. Риж. техн. ун-та. – Рига : РТУ, 2004 – С. 80–94.

77. Информационная технология. Методы защиты .Менеджмент рисков информационной безопасности : BS ISO/IEC 27005:2008. – К. : 2011. – 70 с.

78. Каллан Р. Основные концепции нейронных сетей / Каллан Р. ; пер. с англ. А. Г. Сивака. – М. : Вильямс, 2003. – 288 с.

79. Карташов А. П. Построение сети нейроподобных элементов с ациклической активностью и экспоненциальным временем затухания / А. П. Карташов, Е. А. Карташова // Автоматика и телемеханика. – 1989. – № 2. – С. 147–157.

80. Касперски К. Техника и философия хакерских атак / К. Касперски. –

М. : Солон, 2001. – 256 с.

81. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться / Е. В. Касперский. – М. : СК Пресс, 1998. – 288 с.

82. Кендалл М. Многомерный статистический анализ и временные ряды / Кендалл М., Стюарт А. ; пер. с англ. – М.: Наука, 1976. – 722 с.

83. Кирьянов Д.В. Mathcad 14 / Д. В. Кирьянов. – СПб. : БХВ-Петербург, 2007. – 704 с.

84. Китинг Д. Flash MX. Искусство создания web-сайтов / Китинг Д. ; пер. с англ. – К. : ТИД ДС, 2002. – 848 с.

85. Коваленко М.М. Комп'ютерні віруси і захист інформації / М. М. Коваленко. – К. : Наук. думка, 1999. – 268 с.

86. Кокс Д. Теория очередей / Кокс Д., Смит У. ; пер. с англ. – М. : Мир, 1966. – 452 с.

87. Колганов С. К. Построение в условиях дефицита информации сводных оценок сложных систем / С. К. Колганов, В. В. Корников, П. Г. Попов, Н. В. Хованов. – М. : Радио и связь, 1994. – 80 с.

88. Колисниченко Д.Н. Rootkits под Windows / Д. Н. Колисниченко. – СПб. : Наука и техника, 2006. – 320 с.

89. Комар М.П. Метод построения совокупного классификатора трафика информационно-телекоммуникационных сетей для иерархической классификации компьютерных атак / М.П.Комар // Системи обробки інформації.– 2012. – Вип. 3 (101), т. 1 – С.134–138.

90. Комар М.П. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы / М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив // Інформатика та математичні методи в моделюванні. – 2011. – Т. 1, №2. – С. 156–160.

91. Корченко А.А. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // Захист інформації. – 2012. – № 2 (55). – С. 47–51.

92. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80–84.

93. Корченко А.О. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації. – 2012. – №1 (54). – С. 108–121.

94. Корченко О. Г. Верифікація нейромережевих методів розпізнавання кібератак / О. Г. Корченко, І. А. Терейковський, С. В. Казмірчук // Науково-техн. Зб. «Управління розвитком складних систем» Київ. нац. ун-ту будівництва і архітектури. – 2014. – Вип. 17. – С. 168–172.

95. Корченко О. Г. Метод оцінки нейромережевих засобів щодо можливостей виявлення інтернет-орієнтованих кібератак / О.Г. Корченко, І.А. Терейковський, С.В. Казимірчук // Вісник інженерної академії наук. – 2014. – Вип. 2. – С. 87–93.

96. Корченко О.Г. Системи захисту інформації : моногр. / О.Г. Корченко. – К. : НАУ, 2004. – 264 с.

97. Корченко О. Г. Сучасні нейромережеві методи та моделі оцінки параметрів безпеки ресурсів інформаційних систем / О. Г. Корченко, І. А. Терейковський, А. О. Дзюбаненко // Захист інформації. – 2014. – Т. 16, № 3. – С. 223–232.

98. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко – К. : МК-Пресс, 2006. – 320 с.

99. Корченко О. Г. Шкідливі програми та їх класифікація / О. Г. Корченко, К. П. Ануфрієнко // Защита информации : сб. науч. тр. – К. : НАУ, 2007. – С.26–32.

100. Котеров Д. PHP 5 / Д. Котеров, А. Костарев. – СПб. : БХВ-Петербург, 2005. – 1120 с.

101. Крамер Г. Математические методы статистики / Крамер Г. ; пер. с

англ. А. С. Монина. – М. : Мир, 1976. – 648 с.

102. Красоткин А. Обнаружение сетевых атак / А. Красоткин // Мир ПК. – 2003. – № 6. – С. 24–26.

103. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак / А.В. Кржыжановский // Доклады ТУСУРа. – 2008. – № 2 (18), ч. 1. – С. 37–41.

104. Круглов В.В. Искусственные нейронные сети / В. В. Круглов, В. В. Борисов. – М. : Горячая линия-Телеком, 2002. – 382 с.

105. Круглов В. В. Нечеткая логика и искусственные нейронные сети / В. В. Круглов, М. И. Дли, Р. Ю. Голунов. – М. : Горячая линия-Телеком, 2004. – 242 с.

106. Кузнецов Г. В. Классификация и анализ систем и методов обнаружения атак / Г. В. Кузнецов, А. М. Иванов // Захист інформації. – 2004. – № 4 – С. 4–11.

107. Кузнецов Г. В. Методы анализа данных для обнаружения атак в компьтерных сетях банковских структур / Г. В. Кузнецов, А. М. Иванов // Защита информации : сб. науч. тр. – К. : НАУ, 2004. – С. 45–50.

108. Кузьменко В.Г. VBA 2002 / В. Г. Кузьменко. – М. : БИНОМ, 2002. – 624 с.

109. Куссуль Э. М. Ассоциативные нейроподобные структуры / Э. М. Куссуль. – К. : Наук. думка, 1990, – 160 с.

110. Ли Ц. Оценивание параметров марковских моделей по агрегированным временным рядам / Ли Ц. ; пер.с англ. – М. : Статистика, 1977. – 221 с.

111. Лукацкий А. В. Корреляция на службе безопасности / А. В. Лукацкий // Byte. – 2003. – №10. – С. 10–12.

112. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. – СПб. : БХВ-Петербург, 2003. – 624 с.

113. Люгер Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. – 4-е изд. / Люгер Ф.; пер. с англ. Н. И. Галагана – М. : Вильямс, 2003. – 864 с.

114. Магницкий Ю.Н. Использование бинарной нейронной сети для обнаружения атак на ресурсы распределенных информационных систем / Ю.Н. Магницкий // Динамика неоднородных систем. — 2008. — С. 200–205.

115. Макаренко Н. Г. Лекции по нейроинформатике. Часть 2 / Н. Г. Макаренко. – М. : МИФИ, 2004. – 200 с.

116. Макнамара Д. Секреты компьютерного шпионажа / Макнамара Д. ; пер. с англ. – М. : БИНОМ, 2004. – 536 с.

117. Мелкумян К. В. COM как средство для реализации достоверной вычислительной базы / К. В. Мелкумян // Защита информации : сб. науч. тр. – К. : КМУГА, 1999. – С. 104–106.

118. Менаске Д. Производительность Web-служб. Анализ, оценка и планирование / Менаске Д., Виргилио А. ; пер. с англ. – СПб. : ДиаСофтЮп", 2003. – 480 с.

119. Нейман Дж. Теория самовоспроизводящихся автоматов / Нейман Дж. ; пер. с англ. – М. : Мир, 1971. – 384 с.

120. Нейман Дж. Теория игр и экономическое поведение / Нейман Дж., Моргенштерн О. ; пер. с англ. – М. : Наука, 1970. – 326 с.

121. Нижник Е. И. Математическое моделирование производительности файловых систем: автореф. дисс. на соискание научн. степени канд. техн. наук: спец. 05.13.18 «Математическое моделирование, численные методы и комплексы программ» / Е. И. Нижник. – М., 2007. – 4 с.

122. Новак Дж. Как обнаружить вторжение в сеть. Настольная книга специалиста по системному анализу = Network Intrusion Detection. An Analyst's Handbook / Джуди Новак, Стивен Норткатт, Дональд Маклахен; пер. И. Дранишникова. – М. : Лори, 2012. – 384 с.

123. Оберг Р. Технология COM+. Основы и программирование /

Оберг Р. ; пер. с англ. – М. : Вильямс, 2001. – 480 с.

124. Обнаружение атак [Электронный ресурс] / Maxim Chirkov // Проект OpenNet : Портал по открытому ПО, Linux, BSD и Unix системам. – Электрон. дан. – [РФ], [2010]. – Режим доступа: World Wide Web. – URL: http://www.opennet.ru/prog/sml/85.shtml. – Загл. с экрана.

125. Огарок А. Виртуальные войны. Искусственный интеллект на защите от вирусов и программных закладок / А. Огарок, Д. Комашинский, Д. Школьников // Конфидент. – 2003. – №2 (50). – С. 64–69, 97.

126. Олешко Д. М. Інформаційна технологія прискорення синтезу нейронних мереж для вирішення задач прогнозування при прийнятті рішень : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец 05.13.06 «Автоматизовані системи управління та прогресивні інформаційні технології»/ Д. М. Олешко. – Одеса, 2005. – 19 с.

127. Орлов А. И. Высокие статистические технологи / А. И. Орлов // Заводская лаборатория. – 2003. – Т. 69, №11. – С. 55-60.

128. Орлов А. И. Прикладная статистика / А.И. Орлов. – М. : Экзамен, 2004. – 656 с.

129. Осовский С. Нейронные сети для обработки информации / С. Осовский. – М. : Финансы и статистика, 2002. – 344 с.

130. Осинский Л. М. Постановка и методы решения задач оптимального планирования мониторинга информационной безопасности вычислительных систем / Л. М. Осинский, А. Н. Мудрак // Защита информации : сб. науч. тр. – К. : НАУ, 2001. – С. 136–144.

131. Отнес Р. Прикладной анализ временных рядов / Отнес Р., Эноксон Л. ; пер. с англ. – М. : Мир, 1982. – 547 с.

132. Паркер Т. TCP/IP для профессионалов / Паркер Т., Сиян К. ; пер. с англ. Е. Матвеева. – СПб. : Питер, 2004. – 859 с.

133. Петров А. А. Определение оперативно-технических характеристик систем активной защиты информации / А. А. Петров // Захист інформації. –

2009. – № 1 – С. 73–75.

134. Петров А. С. Обеспечение защиты информации обрабатываемой динамической Web-системой за счет моделирования устойчивой к уязвимостям архитектуры / А. С. Петров, О. А.Талыкин // Вісник СНУ ім. Володимира Даля. – 2007. – №5. – С. 17–21.

135. Петров О. С. Аналіз уязвимости Web-систем / О. С. Петров, О. А. Таликін // Захист інформації. – 2006. – №2. – С. 32–42.

136. Плешко В. В.TopSOM: визуализация информационных массивов с применением самоорганизующихся тематических карт / В. В. Плешко, А. Е. Ермаков , Г. В. Липинский // Информационные технологии. – 2001. – № 8. – С. 8–11.

137. Поликарпов С.В. Новая модель искусственного нейрона: кибернейрон и области его применения [Електронний ресурс] / С.В. Поликарпов, В.С. Дергачёв, К.Е. Румянцев, Д.М. Голубчиков. Режим доступу: http://arxiv.org/ftp/arxiv/ papers/0907/0907.0229.pdf.

138. Пучков Н. В. Использование искусственных нейронных сетей для контроля корректности информационно - технологического процесса / Н. В. Пучков // Новые промышленные технологи. – 1999. – № 3. – С. 79–84.

139. Рабинович З. Л. Подход к моделированию мыслительных процессов на основе нейроподобных растущих сетей / З. Л. Рабинович, В. А. Ященко // Кибернетика и системный анализ. – 1996. – № 5. – С.3–20.

140. Рассел С., Норвиг П. Искусственный интеллект: современный подход, 2-е изд / Рассел С., Норвиг П. ; пер.с англ. К.А. Птицына. – М. : Вильямс, 2007. – 1408 с.

141. Резник А. М. О природе интеллекта /А. М. Резник// Математические машины и системы. – 2008. – №1. – С.23–45.

142. Розенблат Ф. Аналитические методы изучения нейронных сетей / Розенблат Ф. ; пер.с англ. – М. : Зарубеж. радиоэлектроника, 1965. – 150 с.

143. Руденко О.Г. Штучні нейронні мережі: навч. посіб. / О.Г. Руденко,

Є.В. Бодянський. – Х.: ТОВ «Компанія СМІТ», 2006. – 404 с.

144. Свинцов В. И. Смысловой анализ и обработка текста / В. И. Свинцов. – М. : Книга, 1979. – 272 с.

145. Сенешова М. Ю. Погрешности нейронных сетей. Вычисление погрешностей весов синапсов / М. Ю. Сенешова // Методы нейроинформатики : сб. науч. тр. – Красноярск : КГТУ. – 1998. – С. 204 – 212.

146. Сигеру О. Нейроуправление и его приложения / Сигеру О., Марзуки Х., Рубия Ю. ; пер. с англ. – М. : ИПРЖР, 2000. – 272 с.

147. Скопа О. О. Конвергенція глобальної інформаційної мережі: питання управління гетерогенними середовищами з урахуванням вимог тріади CIA / О. О. Скопа, Н. Ф. Казакова, Ж. Ю. Зеленцова // Сучасна спеціальна техніка. — 2014. — № 3(38). — С. 28–37.

148. Скопа, О. О. Показники якості та життєві цикли захищених інформаційно-вимірювальних систем / О. О. Скопа, С. Л. Волков, О. В. Грабовський // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15(204). – Ч. 1. – С. 192–198.

149. Слеповичев И.И. Обнаружение DDoS-атак нечеткой нейронной сетью / И. И. Слеповичев, П. В. Ирматов, М. С. Комарова, А. А. Бежин // Известия Саратовского университета. – 2009. – Т. 9, [Сер. Математика. Механика. Информатика] вып. 3. – С. 84-89.

150. Стаханов А. А. Linux / А. А. Стаханов. – СПб. : БХВ-Петербург, 2004. – 912 с.

151. Талалаев А.А.Разработка нейросетевого модуля мониторинга аномальной сетевой активности / А.А. Талалаев, И.П. Тищенко, В.П.Фраленко, В.М. Хачумов // Нейрокомпьютеры: разработка и применение. — 2011. — № 7. — С. 32-38.

152. Таненбаум Э. Архитектура компьютера / Таненбаум Э. ; пер. с англ. – СПб. : Питер, 2006. – 697 с.

153. Таненбаум Э. Компьютерные сети / Таненбаум Э. ; пер. с англ.

А. Леонтьева. – СПб.: Питер, 2002. – 848 с.

154. Таненбаум Э. Современные операционные системы. – 2-е изд. / Таненбаум Э. ; пер. с англ. – СПб. : Питер, 2002. – 1036 с.

155. Тарасенко В. П. Метод застосування продукційних правил для подання експертних знань в нейромережевих засобах розпізнавання мережевих атак на комп'ютерні системи / В. П. Тарасенко, О. Г. Корченко, І. А. Терейковський // Безпека інформації. – 2013. – Т. 19, № 3. – С. 168–174.

156. Тейлор Дж. Введение в теорию ошибок / Тейлор Дж. ; пер. с англ. Л. Г. Деденко. – М. : Мир, 1985. – 272 с.

157. Терейковська Л.О. Визначення найбільш ефективної архітектури нейронної мережі, призначеної для розпізнавання голосових сигналів в Moodle / Л.О. Терейковська, І.А. Терейковський // Теорія і практика використання системи управління навчанням Moodle: матеріали 2 міжнар. наук.-практ. конф. «MoodleMoot Ukraine-2014» (22–23 травня 2014 р.). – К.: КНУБА, 2014. – С.36.

158. Терейковська Л. О. Проблема голосової взаємодії в дистанційному навчанні вищого навчального закладу / Л. О. Терейковська, І. А. Терейковський // Науково-технічний збірник «Управління розвитком складних систем» Київ. наці. ун-ту будівництва і архітектури. – 2013. – Вип. 13. – С. 157–161.

159. Терейковский И. А. Безопасность программного обеспечения, созданного с использованием семейства технологий COM, DCOM, COM+ / И. А. Терейковский // Захист інформації. – 2006. – № 1. – С. 55–67.

160. Терейковський І. А. Вдосконалення алгоритму навчання багатошарового персептрону, призначеного для розпізнавання мережевих атак / І. А. Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – Випуск 2(24). – С. 65–70.

161. Терейковський І.А. Вдосконалення антивірусного захисту комп'ютерної мережі вищого навчального закладу / І. А. Терейковський // Сучасні тенденції розвитку вищої освіти, трансформація навчального процесу у

технологію навчання: міжнар. наук.-метод. конф., 25-26 жовт. 2007 р.: тези допов. – К., 2007. – С. 366–367.

162. Терейковський І. А. Вдосконалення методики захисту інформації в корпоративних мережах, що використовують ресурси Internet / І.А. Терейковський // Вісник національного транспортного університету. – 2003. – № 8 – С. 13–16.

163. Терейковський І. А. Визначення оптимального методу контролю об’єктів захисту комп’ютерних мереж / І. А. Терейковський // Вісник КНУТД. – 2006. – № 5. – С. 39–44.

164. Терейковський І.А. Визначення оптимального типу нейронної мережі, призначеної для використання в програмних засобах захисту інформації / Терейковський І.А. // Сучасні тенденції розвитку технологій в інфокомунікаціях та освіті : матер. VIII наук. конф. (24–25 лист. 2011 р.). – К.: ДУІКТ, 2011. – С. 372–379.

165. Терейковський І. А. Використання нейронної мережі з радіальними базисними функціями в задачах діагностики стану захищеності програмного забезпечення / І. А. Терейковський // Науково-технічний збірник "Управління розвитком складних систем" Київ. нац. ун-ту будівництва і архітектури. – 2010. – Вип. 3. – С. 111–114.

166. Терейковський І. А. Використання нейронної мережі Кохонена для розпізнавання спаму / І. А. Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2007. – Вип. 1(14). – С. 106–114.

167. Терейковський І. А. Використання нейронних мереж при розпізнаванні макровірусів / І. А. Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – Вип. 2(13). – С. 176–183.

168. Терейковський І. А. Використання семантичної нейронної мережі в задачах моніторингу текстової інформації / І. А. Терейковський // Вісник

ДУІКТ. – 2012.– Т.10, № 1.– С. 36–41.

169. Терейковський І.А. Використання експертних знань в процесі навчання нейронних мереж / І.А. Терейковський // Стратегії розвитку інформаційного культурно-освітнього та економічного простору України: Всеукр. наук.-практ. конф., 20–21 травня 2014 р.: тези допов. – К., 2014. – С.134–136.

170. Терейковський І.А. Використання семантичної нейронної мережі в задачах моніторингу текстової інформації / І.А. Терейковський // Сучасні інформаційно-комунікаційні технологі. COMINFO'2011: матер. VII міжнар. наук.-техн. конф. (10–14 жовт. 2011 р.). – К.: ДУІКТ, 2011. – С. 218–220.

171. Терейковський І. А. Дослідження ефективності функціонування веб-серверу / І. А. Терейковський // Комп'ютерне моделювання та інформаційні технології в науці, економіці та освіті: зб. наук. праць КЕІ КНЕУ. – Кривий Ріг, 2005. – С. 216–217.

172. Терейковський І. А. Дослідження стійкості серверних технологій Java від атак на відмову / І. А. Терейковський // Захист інформації. – 2004. – № 4. – С. 34–42.

173. Терейковський І. А. Использование возможностей Microsoft Word при создании Web-ориентированных вирусов / І. А. Терейковський // Защита информации: сб. науч. трудов НАУ. – 2004. – Вып. 11. – С. 87–96.

174. Терейковський І. Захист Web-сайтів корпоративних інформаційних систем від атак на відмову / І. Терейковський // Зб. наук. праць ВІТІ НТУ України «КПІ». – 2004. – № 4 – С. 201–208.

175. Терейковський І. А. Захищеність Web-серверів Apache та IIS / І. А. Терейковський // Проблеми програмування. – 2005. – № 2. – С. 42–51.

176. Терейковський І. А. Концепція атаки Web-орієнтованих пошукових систем / І. А. Терейковський // Вісник ДУІКТ. – 2006. – Т. 3, № 3-4. – С. 67–71.

177. Терейковський І. А. Концепція визначення оптимального режиму контролю захищеності програмного забезпечення комп’ютерних систем / І. А.

Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – Вип. 1(12). – С. 88–96.

178. Терейковський І.А. Концепція використання марківських процесів для контролю атак на програмне забезпечення комп'ютерних систем та мереж / І.А. Терейковський // Захист інформації. – 2005. – № 3. – С. 4–12.

179. Терейковский И. А. Концепция защиты программного обеспечения Internet-сервера с использованием активной составляющей / И. А. Терейковский // Захист інформації. – 2005. – Спец. випуск. – С. 6–11.

180. Терейковський І. А. Методологія класифікації листів електронної пошти з використанням нейронних мереж / І. А. Терейковський // Захист інформації. – 2013. – Т. 15, № 2. – С. 115–121.

181. Терейковський І. А. Методи коннективізму та захист в них / І.А. Терейковський // Захист інформації. – 2009. – № 1 – С. 59–70.

182. Терейковський І. А. Методи обробки статистики при формуванні шаблонів нормальної поведінки Інтернет-серверів / І. А. Терейковський, Л. О. Терейковська // Інформаційна безпека: наук.-практ. конф., 26–27 березня 2009 р. : зб. текстів виступів. – К., 2009. – С. 56–60.

183. Терейковский И.А. Моделирование профилей нормального поведения компьютерных систем / И. А. Терейковский // Защита информации: сб. науч. трудов НАУ. – 2006. – Вып. 13. – С. 103–108.

184. Терейковський І.А. Моделювання експлуатаційних параметрів веб-серверу системи дистанційного навчання / Терейковський І.А. // Сучасні комп'ютерні системи та мережі: розробка та використання ACSN'2011 : матер. 5-ї міжнар. наук.-техн. конф. (29 вересня – 01 жовтня 2011). – Львів: ЛПНУ, 2011. – С. 93–96.

185. Терейковський І. А. Негомогенна марківська модель прогнозування параметрів захисту веб-орієнтованих комп'ютерних систем / І. А. Терейковський, Л. О. Терейковська // Проблеми впровадження інформаційних технологій в економіці : матеріали VIII міжнар. наук.-практ.

інтернет-конф. (23.01.2012–30.03.2012). – Ірпінь: НУДПСУ, 2012. – С. 320–325.

186. Терейковський І. А. Нейромережева методологія розпізнавання інтернет-орієнтованого шкідливого програмного забезпечення / І. А. Терейковський // Безпека інформації. – 2013. – Т. 19, № 1. – С. 24–28.

187. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації: моногр. / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.

188. Терейковський І. А. Нейромережевий поведінковий аналізатор антивірусної системи / І. А. Терейковський // Захист інформації. – 2012. – № 2. – С. 67–70.

189. Терейковський І. А. Оцінка документованих можливостей Flash Macromedia для здійснення несанкціонованого доступу до інформації клієнтів Інтернет / І. А. Терейковський // Проблеми програмування. – 2004. – № 4 – С.112–118.

190. Терейковський І.А. Оптимізація архітектури нейронної мережі, призначеної для діагностики стану комп'ютерної мереж / І. А. Терейковський // Науково-технічний збірник «Управління розвитком складних систем» Київ. нац. ун-ту будівництва і архітектури. – 2011. – Випуск 6. – С. 155–158.

191. Терейковський І. Оптимізація захисту відкритих корпоративних мереж / І. Терейковський, Л. Терейковська // Вісник КНТЕУ. – 2004. – № 1. – С. 103–112.

192. Терейковський І. А. Оптимізація захисту Web-орієнтованих інформаційних систем органів державної влади / І. А. Терейковський // Державне управління і право: зб. наук. праць Київ. нац. ун-ту культури і мистецтв.– 2006. – Вип. 1, Ч. 2. – С. 97–105.

193. Терейковський І. А. Оптимізація структури двохшарового персептрону, призначеного для розпізнавання аномальних величин експлуатаційних параметрів комп'ютерної мережі / І. А. Терейковський // Науково-технічний збірник «Управління розвитком складних систем» Київ.

нац. ун-ту будівництва і архітектури. – 2011. – Вип. 5. – С. 128–131.

194. Терейковський І.А. Оптимізація структури та змісту корпоративних Web–сайтів / І.А. Терейковський // Вісник КНТЕУ. – 2004. – № 3. – С. 95–104.

195. Терейковский И.А. Парольная защита офисного электронного документооборота / И. А. Терейковский // Вісник ДУІКТ. – 2006. – Т. 4, № 2 – С. 109–115.

196. Терейковський І. А. Підвищення ефективності функціонування корпоративних web – сайтів / І .А. Терейковський // Вісник КНУТД. – 2004. – № 4. – С. 41–46.

197. Терейковський И. А. Применение семантического анализа содержимого электронных писем в системах распознавания спама / И. А. Терейковский // Захист інформації. – 2006. – № 4. – С. 49–60.

198. Терейковський І.А. Про використання вейвлет-перетворень та нейронних мереж для розпізнавання аномального стану комп'ютерної мережі / І. А. Терейковський // Вісник Університету "Україна". – 2011. – № 2. – С.60–65.

199. Терейковський І. А. Розпізнавання скриптових вірусів за допомогою нейронної мережі з радіальними базисними функціями / І. А. Терейковський // Науково-технічний збірник «Управління розвитком складних систем» Київ. нац. ун-ту будівництва і архітектури. – 2010. – Вип. 4. – С. 104–108.

200. Терейковський І. А. Розпізнавання скриптових вірусів за допомогою багатошарового персептрону / І. А. Терейковський // Защита информации: сб. науч. трудов НАУ. – 2007. – Вып. 14. – С. 206–212.

201. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст] : НД ТЗІ 1.1-003 – 1999. – К. : ДСТСЗІ СБ України, 1999. – 12 с.

202. Тимофеев А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевіїх атак / А.Тимофеев, А.Браницкий // International Journal Information Technologies & Knowledge. – 2012. – Vol.6,

Number 3. – P. 257–265.

203. Тимченко А. А. Модель самоорганизации нейронной сети на примере задачи оценки уровня пожарной безопасности объекта / Тимченко А. А., Джулай А.Н. // Нейросетевые технологии и их применение : междунар. науч. конф., 4–5 дек. 2002 г. : тезисы докл. – Краматорск, 2002. – С.144–146.

204. Тихонов Э. Е. Методы и алгоритмы прогнозирования экономических показателей на базе нейронных сетей и модулярной арифметики / Э. Е. Тихонов, В. А. Кузьмищев. – Невинномысск: НИЭУП, 2004. – 166 с.

205. Ткаченко Р. О. Нейронні мережі прямого поширення з неітераційним навчанням : автореф. дис. на здобуття наук. ступеня доктора. техн. наук : спец 05.13.06 «Автоматизовані системи управління та прогресивні інформаційні технології» / Р. О. Ткаченко. – Л., 2000. – 32 с.

206. Тэрано Т. Прикладные нечеткие системы / Тэрано Т., Асаи К., Сугэно М. ; пер. с япон. Ю. Н. Чернышева – М. : Мир, 1993. – 364 с.

207. Тынкевич М.А. Экономико-математические методы / М. А. Тынкевич. – Кемерово, Кузбас. гос. техн. ун-т, 2000. – 177 с.

208. Уэйнпрат П. Apache для профессионалов / Уэйнпрат П. ; пер. с англ. И. Дранишников. – М. : Лори, 2001. – 473 с.

209. Уэнстром М. Организация защиты сетей Cisco / Уэнстром М. ; пер. с англ. – М. : Вильяме, 2005. – 768 с.

210. Уссермен Ф. Нейрокомпьютерная техника / Уссермен Ф. ; пер. с англ. – М. : Мир, 1992. – 284 с.

211. Федотов Е. В. Механизмы возможных атак в сети Internet / Е. В. Федотов // Защита информации : сб. науч. тр. – К. : НАУ, 2001. – С. 30–42.

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

213. Хайкин С. Нейронные сети: полный курс. – 2-е изд., испр. / Хайкин С. ; пер. с англ. Н. Н. Куссуль – М. : Вильямс, 2006. – 1104 с.

214. Харченко В.С. Новые информационные технологии и безопас-ность информационно–управляющих систем АЭС / В.С.Харченко, М.А. Ястребенецкий, В.В. Скляр // Ядерная и радиационная безопасность. – 2003. – Т. 6, № 2. – С. 19–28.

215. Хафизов А.Ф. Нейросетевая система обнаружения атак на WWW-сервер: дис. ... канд. техн. наук : 05.13.11 / А.Ф. Хафизов– Уфа, 2004–172 с.

216. Хеннан Э. Многомерные временные ряды / Хеннан Э. ; пер. с англ. А. С. Холева. – М. : Мир, 1974. – 576 с.

217. Хильер С. Создание приложений COM+ в среде Visual Basic. Руководство разработчика / Хильер С. ; пер. с англ.– М. : Вильямс, 2001. – 416 с.

218. Хмелёв Д. В. Распознавание автора текста с использованием цепей Маркова / Д. В. Хмелёв // Вестник МГУ, сер.9: Филология. – 2000. – № 2. – С. 115–126.

219. Хоглунд Г. Руткиты: внедрение в ядро Windows / Хоглунд Г., Батлер Дж. ; пер. с англ. – СПб. : Питер, 2007. – 285 с.

220. Хорошко В. О. Використання багатошарового персептрону для розпізнавання поштових скриптових вірусів / В.О. Хорошко, І.А. Терейковський // Сучасні інформаціно-комунікаційні технології: міжнар. наук.-техн. конф., 8–14 жовт. 2006 р. : тези доп. – К. : 2006. – С. 103–104.

221. Хорошко В. А. Использование искусственных нейронных сетей в задачах распознавания атак на компьютерные системы / В. А. Хорошко, И. А. Терейковский // Захист інформації. – 2006. – № 3. – С. 57–65.

222. Хорошко В. О. Концепція визначення оптимального режиму контролю Web-серверу системи дистанційного навчання / В. О. Хорошко, Д. В. Чирков, І. А. Терейковський // Болонський процес: трансформація навчального процесу у технологію навчання: міжнар. наук.-метод. конф., 26–27

жовт. 2006 р. : тези доп. – К., 2006. – С. 224-225.

223. Хорошко В. О. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України / В. О. Хорошко, В. А. Кудінов // Захист інформації. – 2004. – №4. – С. 11–18.

224. Хорошко В. О. Основи інформаційної безпеки / В. О. Хорошко, В. С. Чередниченко. – К. : ДУІКТ, 2008. – 186 с.

225. Хорошко В.О. Термінологічний довідник з питань технічного захисту інформації / В. О. Хорошко , С. Р. Коженевський , Д. В. Чирков. – К. : ДУІКТ, 2007. – 365 с.

226. Царегородцев В.Г. Извлечение явных знаний из таблиц данных при помощи обучаемых и упрощаемых искусственных нейронных сетей / В. Г. Царегородцев // Материалы XII междунар. конф. по нейрокибернетике "Проблемы нейрокибернетики". – Ростов н/Д: СКНЦ ВШ, 1999. – С. 245–249.

227. Царегородцев В. Г. Редукция размеров нейросети не приводит к повышению обобщающих способностей / В. Г. Царегородцев // Материалы XII Всеросс. семинара "Нейроинофрматика и ее приложения". – Красноярск : КГТУ, 2004. – С. 163–165.

228. Царегородцев В. Г. Упрощение нейронных сетей – цели , идеи и методы / В. Г. Царегородцев // Нейрокомпьютеры: разработка , применение . – 2002. – № 4. – С. 5–13.

229. Цуриков О. М. Исследование конструктивно – эксплуатационных факторов в задаче оптимизации режима контроля / О. М. Цуриков, И. А. Терейковский // Техническая диагностика и неразрушающий контроль. – 1999. – №3. – С. 51 – 56.

230. Цуриков О. М. Исследование режима контроля и промывки фильтров жидкостных функциональных систем воздушных судов / О. М. Цуриков, И. А. Терейковский // Техническая диагностика и неразрушающий контроль. – 1999. – № 1. – С. 75–85.

231. Цуриков О. М. Оптимизация режима многопараметрического

контроля на примере многопараметрического контроля / О. М. Цуриков, И. А. Терейковский // Вісник КМУЦА. – 2-ге вид. : зб. наук. праць. – К. : КМУЦА, 1999. – С. 217–221.

232. Цуриков О. М. Оптимизация режима однопараметрического контроля и связанных с ним профилактических работ агрегатов функциональных систем воздушных судов / О.М. Цуриков, И.А. Терейковский // Вісник КМУЦА. – 1-ше вид. : зб. наук. пр. – К. : КМУЦА, 1999. – С. 7–15.

233. Цюцюра С. В. Застосування нейронних мереж для розпізнавання «ідеального співрозмовника» серед користувачів соціальних мереж / С. В. Цюцюра, І. А.Терейковський, С. В. Палій // Системи навігації та управління. – 2013. – Вип. 4(28). – С.123–127.

234. Цюцюра С. В. Модифікація класичної нейронної мережі ймовірнісного типу для розпізнавання «ідеального співрозмовника» серед користувачів соціальних мереж / С. В. Цюцюра, І. А.Терейковський, С. В. Палій // Науково-технічний збірник «Управління розвитком складних систем» Київ. нац. ун-ту будівництва і архітектури, 2014, Вип. 19. – С 118–123.

235. Цыбаков Б. С. Модель телетрафика на основе самоподобного случайного процесса / Б. С. Цыбаков // Радиотехника. – 1999. – № 5. – С. 34–38.

236. Червяков Н.И. Методы и принципы построения модулярных нейрокомпьютеров / Н. И. Червяков. – Ставрополь : Ставроп. военный ин-т сязи ракетных войск, 2000. – 212 с.

237. Шампандар А. Искусственный интеллект в компьютерных играх: как обучить виртуальные персонажи реагировать на внешние воздействия / Шампандар А. ; пер. с. англ. К. А. Птицына. – М. : Вильямс, 2007. – 786 с.

238. Широчин В.П. Біт-орієнтовані оцінки стійкості криптографічних алгоритмів. / В.П. Широчин, В.Є. Мухін, С.С. Широчин // Сучасна спеціальна техніка. – № 1, 2010. – С. 54–59.

239. Широчин В.П. Мінімізація об’єму управляючого списку для планування подій в Petri-Nets моделях / Ю.Н. Шилов // Вісник Нац. техн. ун-ту

України «КПІ» «Інформатика, управління та обчислювальна техніка». – № 56, 2012. – С. 8–12.

240. Широчин В.П. Основи безпеки комп'ютерних систем. / С.В Широчин., В.Є. Мухін. – К: «Корнійчук», 2009. – 286 с.

241. Шохін Б. П. Вдосконалення контролю за станом захищеності ком'ютерної мережі на основі адаптивного моніторингу / Б. П. Шохін, О. М. Юдін, О. Є. Мазулевський // Зб. наук. праць Військового ін-ту телекомунікацій та інформатизації нац. техн. ун-ету України "КПІ". – К. : КНТУ, 2004. – № 4. – С. 208–217.

242. Шуклин Д. Е. Модели семантических нейронных сетей и их применение в системах искусственного интеллекта : дис. … кан. техн. наук : 05.13.23 / Шуклин Дмитрий Евгеньевич. – Х., 2003. – 196 с.

243. Шумский С. А. Самоорганизующиеся карты финансовых индикаторов 200 крупнейших российских предприятий / С. А. Шумский, А. Н. Кочкин // Нейроинформатика-99 : науч. конф., 20–22 янв. 1999 г. : тезисы докл. – М., 1999. – С. 122–127.

244. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2004. – 384 с.

245. Щеглов И.Н. Алгоритм формирования репрезентативной обучающей выборки искусственной нейронной сети / И.Н. Щеглов, С. А. Демченко , А. А. Подлесских // Нейроинформатика-99 : науч. конф., 20-22 янв. 1999 г. : тезисы докл. – М., 1999. – С. 405–407.

246. Яремчук Ю. Є. Вирішення проблеми доступності до мережі Інтернет шляхом динамічного балансування пропускної здатності каналу web-трафіку / Ю. Є. Яремчук, Д. О. Кец, Т. М. Жевега, К. В. Безпалий // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 1(23), 2012. – С. 58–64.

247. Яремчук Ю.Є. Моделювання вибору оптимального методу протидії

загрозам інформаційній безпеці / Ю. Є. Яремчук, А. А. Шиян, Л. О. Нікіфорова // Реєстрація, зберігання і обробка даних. – Т. 16, №4, 2014. – С. 28–33.

248. Яремчук Ю.Є. Підхід до формування ієрархічних класифікацій методів захисту телекомунікаційних мереж від негативного впливу / Ю. Є. Яремчук, А. А. Шиян // Вимірювальна та обчислювальна техніка в технологічних процесах. – №4, 2014. – С. 226–230.

249. Яремчук Ю.Є. Вирішення проблеми доступності однотипних об'єктів мережі за доменним ім'ям в протоколі трансляції мережевих адрес / Ю. Є. Яремчук, Д. О. Кец, Є. С. Ніколаєв, Д. О. Іванішина // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2(21), 2010. – С. 65–69.

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

251. Bivens A. Network–Based Intrusion Detection Using Neural Networks / A. Bivens, C. Palagiri, R. Smith, B. Szymansky, M. Embrechts // Proc. Intelligent Engineering Systems through Artificial Neural Networks ANNIE–2002, St. Louis, MO, Volume 12. – New York: ASME Press, 2002. – P. 579–584.

252. Chen Y. Multiple sequence alignment and artificial neuralnetworks for malicious software detection / Y. Chen, A. Narayanan , Shaoning Pang , Ban Tao. // Natural Computation, 2012. – P. 261 – 265.

253. Du Toit T. Filtering spam e-mail with Generalized AdditiveNeural Networks / T. Du Toit, H. Kruger // Information Security for South Africa. 2012. – P.1-8.

254. Hnatiuk S. Cyberterrorism: History of current trends and countermeasures. / S. Hnatiuk // Privacy Notice . – 2013 . – Vol. 9 , № 2. – S. 118 – 129.

255. Skaruz J. Recurrent neural networks towards detection of SQL attacks /

J. Skaruz , F. Seredynski // Parallel and Distributed Processing Symposium. – 2007.

256. Koch R. Attack Trends in Present Computer Networks / R. Koch, B. Stelte, M. Golling // 4th International Conference on Cyber Conflict [CYCON 2012], (Tallinn, Estonia, 5–8 June 2012). – 2012. – P. 225–236.

257. Mantel H. A Uniform Framework for the Formal Specification and Verification of Information Flow Security: Diss. … Doctor der Ingenieurwissenschaften / Heiko Mantel. – Saarbrücken, 2003. – 275 p.

258. AirSnare [Electronic resource] : [Intrusion Detection Software for Windows] / [AirSnare Project]. – Electronic data. – [USA], [2011]. – Mode of access: World Wide Web. – URL: http://home.comcast.net/~jay.deboer/airsnare/. – Language: English. – Description based on home page (viewed on Oct. 07, 2012).

259. Anderson J. Computer security threat monitoring and surveillance [Electronic resource] / J. Anderson // Computer Security Resource Center of National Institute of Standards and Technology / Computer Security Laboratory Department of Computer Science University of California at Davis. – Electronic data. – Gaithersburg, MD, USA : NIST, 1980. – Mode of access: World Wide Web. – URL: http://csrc.nist.gov/publications/history/ande80.pdf. – Language: English. – Description based on home page (viewed on Oct. 20, 2011).

260. Callegari C. A new statistical approach to network anomaly detection / C. Callegari, S. Vaton, M. Pagano // Proc. of Performance Evaluation of Computer and Tele-communication Systems (SPECTS). – 2008. – P. 441-447.

261. Denning D. An Intrusion Detection Model / D. Denning // IEEE Transactions on Software Engineering, v. SE-13. – № I. – 1987. – P. 222-232.

262. Forrester S. A sense of self for Unix process / S. Forrester, S. Hofmeyr, T. Longstaff // Proceedings of the 1996 IEEE Symposium on Security and Privacy. P/120-128? Los Alamos. CA. 1996. IEEE Computer Society Press.

263. Gavrilis D. Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features / D. Gavrilis, E. Dermatas // Computer Networks. – 2005. – № 48. – P. 235–245.

264. IBM Proventia Network Anomaly Detection System [Electronic resource] / IBM // IBM. – Electronic data. – [Armonk, New York, USA]: IBM, [2011]. – Mode of access: World Wide Web. – URL: http://www.ibm.com/ru/services/iss/proventia_network_ anomaly_detection_system.html. – Language: English. – Description based on home page (viewed on Oct. 20, 2012).

265. IBM RealSecure Network [Electronic resource] / IBM // IBM. – Electronic data. – [Armonk, New York, USA]: IBM, [2010]. – Mode of access: World Wide Web. – URL: http://www.ibm.com/ru/services/iss/realsecure_network.html. – Language: English. – Description based on home page (viewed on Mar. 08, 2012).

266. Kazakova, Nadia. Model that Solve the Information Recovery Problems [Текст] / Nadia Kazakova, Oleksandr Skopa, Mikołaj Karpiński // Jornal of Telecommunications and Information Technology. — 2014. — №4. — P. 116–121. – ISSN 1509-4553 (SCOPUS).

267. Kharchenko V. Dependability of Safety–Critical Computer Systems through Component–Based Evolution / V. Kharchenko, V. Sklyar, A. Siora // Proceeding of International Conference on Dependability of Computer systems “DepCoS – RELCOMEX 2009”, 02.07.2009. – Poland, Brunow, 2009. – P. 42–49.

268. Koch R. Attack Trends in Present Computer Networks / R. Koch, B. Stelte, M. Golling // 4th International Conference on Cyber Conflict [CYCON 2012], (Tallinn, Estonia, 5–8 June 2012). – 2012. – P. 225–236.

269. Korchenko O.G. Modern methods and neural network model parameter estimation of information systems security / O.G. Korchenko, I.A. Terejkowski// Aviation in the XXI-st century. Safety in Aviation And Space.

270. Kotov V. Detection of web server attacks using principles of immunocomputing / V. Kotov, V. Vasilyev // Proc. of 2nd World Congress on Nature and Biologically Inspired Computing. – 2010. – P. 25-30.

271. Kotov V. Detection of web server attacks using principles of immunocomputing / V. Kotov, V. Vasilyev // Proc. of 2nd World Congress on Nature

and Biologically Inspired Computing. – 2010. – P. 25-30.

272. Planquart J.-P. Application of neural networks to intrusion detection [Electronic resource] / Jean-Philippe Planquart // SANS Information Security Reading Room. – Electronic data. – [USA] : SANS Institute, 2001. – Mode of access: World Wide Web. – URL: http://www.sans.org/reading_room/whitepapers/detection/application-neural-networks-intrusion-detection_336. – Language: English. – Description based on home page (viewed on May. 10, 2010).

273. Peng T. Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems / T. Peng, C. Leckie, K. Ramamohanarao // ACM Computing Surveys. – 2007. – Vol. 39, N 1. – 42 p.

274. Prelude-IDS [Electronic resource] : [Universal Open-Source Security Information & Event Management system] / The Prelude Team. – Electronic data. – [USA] : CS Systèmes d'Information, 2012. – Mode of access: World Wide Web. – URL: https://www.prelude-ids.org/. – Language: English. – Description based on home page (viewed on Oct. 20, 2012).

275. Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800–53. Revision 3. National Institute of Standards and Technology, 2009. – 237 p.

276. Reznik A.M. "Non-Iterative Learning for Neural Networks" Proceedings International Joint Conference on Neural Networks, Washington DC, July 10-16. – 1999.– №548.

277. Self-nonself fiscrimination in a computer / S. Forrest [et al.] // Proc. of 1994 IEEE Symp. on Research in Security and Privacy. – 1994. – P. 202–212.

278. Shyrochin V. Adaptive security mechanisms for the computer networks based on risk analysis. (Mukhin V.) // Journal of Qafqaz University: AZN. Mathematics and Computer Science. – Num. 1, Vol. 1. – 2013. – P. 11–16.

279. The Bro Network Security Monitor [Electronic resource] / The Bro Project. – Electronic data. – [USA] : The Bro Project, 2011. – Mode of access: World

Wide Web. – URL: http://www.bro-ids.org/. – Language: English. – Description based on home page (viewed on Oct. 20, 2012).

280. The White House, Cyber space policy review. Assuring a Trusted and Resilient Information and Communications Infrastructure, 2010. – 76p. – [Эл. ресурс] Режим доступу: http://msisac.cisecurity.org/awareness/documents/Cyberspace_Policy_Review_final.pdf.

281. Tripwire [Electronic resource] / [Tripwire, Inc.]. – Electronic data. – [Portland, OR, USA] : [Tripwire, Inc.], 2011. – Mode of access: World Wide Web. – URL: http://www.tripwire.org/. – Language: English. – Description based on home page (viewed on Oct. 20, 2012).

Наукове видання

Олександр Григорович Корченко,
Ігор Анатолійович Терейковський,
Андрій Олександрович Білощицький

МЕТОДОЛОГІЯ РОЗРОБЛЕННЯ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Редактор.
Технічний редактор
Коректор