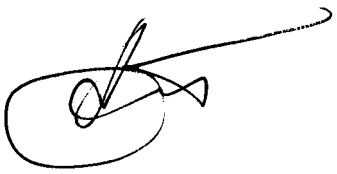
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ТЕРЕЙКОВСЬКИЙ ІГОР АНАТОЛІЙОВИЧ



УДК 004.056.5:004.8(043.3)

НЕЙРОМЕРЕЖЕВІ МОДЕЛІ, МЕТОДИ І ЗАСОБИ ОЦІНЮВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ІНТЕРНЕТ-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Спеціальність 05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ 2015

Дисертацією є рукопис
Робота виконана в Національному авіаційному університеті Міністерства освіти і науки України

Науковий консультант: лауреат Державної премії України в галузі науки і техніки, доктор технічних наук, професор, **Корченко Олександр Григорович**, Національний авіаційний університет, завідувач кафедри безпеки інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор **Широчин Валерій Павлович**, Національний технічний університет України "КПІ", завідувач лабораторії "НТУУ КПІ – Самсунг-електронікс";

доктор технічних наук, доцент **Скопа Олександр Олександрович**, Одеський національний економічний університет, завідувач кафедри інформаційних систем в економіці

доктор технічних наук, професор **Яремчук Юрій Євгенович**, Вінницький національний технічний університет, директор центру інформаційних технологій і захисту інформації

Захист відбудеться « 28 » травня 2015 р. о 14^{00} годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, Київ, пр.Космонавта Комарова, 1.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету.

Автореферат розісланий « 28 » квітня 2015 року

Учений секретар
спеціалізованої вченої ради
к.т.н., доцент С. О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасний стан розвитку вітчизняних інформаційних систем (ІС), інтегрованих до глобальної мережі Інтернет, характеризується підвищеним рівнем вимог до безпеки інформації, який вже складно забезпечити за допомогою систем захисту, в підсистемах контролю та управління яких використовуються виключно класичні методи оцінки параметрів безпеки (ПБ). Разом з тим, в різних галузях науки та техніки проявляється інтерес до використання методів та моделей 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 вирішувати при оцінюванні ПБ для виявлення кібератак. На сьогодні відомі спроби використання НМ в різноманітних комерційних та вільнодоступних системах захисту інформації (СЗІ). Так, НМ використовуються для розпізнавання кібератак в міжмережевих екранах компанії Cisco та для розпізнавання вірусів в антивірусах Norton Antivirus виробництва корпорації Symantec та F-Prot виробництва компанії CYREN GlobalView Security Lab. Також за допомогою НМ визначаються DDOS-атаки в вільнопоширюваному модулі, призначеному для інтегрування в програмний комплекс Snort. Крім того, компанією Facebook задекларовано використання нейромережевих засобів (НМЗ) розпізнавання спаму. Вказані 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. Крім того, недоліком поширених закордонних комерційних НМЗ розпізнавання кібератак являється висока вартість та відсутність детальної науково-технічної документації.

Питанням розробки нейромережевих моделей та методів параметричного оцінювання стану ІС в різний час займалися такі вчені як Є. Бодянський, Д. Деннінг, О. Додонов, О. Корченко, А. Лукацький, О. Петров, О. Резнік, О. Руденко, С. Форестер, В. Харченко, В. Хорошко та ін. Однак в галузі захисту інформації побудову таких моделей та методів засновано на різнорідних підходах, вони носять точковий характер застосування та практично не взаємопов’язані, що ускладнює їх використання при створенні ефективних систем розпізнавання кібератак.

Таким чином, посилення вимог до ефективності систем розпізнавання кібератак на ресурси Інтернет-орієнтованих інформаційних систем, перспективність використання нейромережевих засобів 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 при обмежених обчислювальних ресурсах обумовлюють актуальність обраної науково-прикладної проблеми дисертаційного дослідження – створення комплексної методології розробки широкодоступних ефективних нейромережевих засобів оцінки параметрів безпеки Інтернет-орієнтованих інформаційних систем, які за рахунок теоретично обґрунтованого вибору характеристик дозволяють оперативно розпізнавати нові види кібератак при обмежених обчислювальних ресурсах та варіативності умов застосування.

Зв'язок роботи з науковими програмами, планами, темами. Одержані результати дисертаційної роботи безпосередньо пов’язані з виконанням держбюджетних науково-дослідних робіт Національного авіаційного університету («Організація систем захисту інформації від кібератак», №0111U000171), Національного технічного університету України «Київський політехнічний інститут» («Методи організації високоефективних спеціалізованих сховищ даних науково-освітнього призначення на основі кластерних обчислювальних технологій», №0210U000261) та Кіровоградського національного технічного університету («Розробка методів підвищення оперативності передачі та захисту інформації у телекомунікаційних системах», №0113U003086).

Мета і задачі дослідження. Мета роботи полягає у підвищенні ефективності систем розпізнавання кібератак в Інтернет-орієнтованих інформаційних системах на основі створення комплексної методології розробки нейромережевих засобів оцінки параметрів безпеки інформаційних систем, які за рахунок теоретично обґрунтованого вибору характеристик дозволяють оперативно розпізнавати нові види кібератак при обмежених обчислювальних ресурсах та варіативності умов застосування.

Для досягнення поставленої мети необхідно розв'язати наступні **задачі:**

– проаналізувати сучасні нейромережеві засоби оцінки параметрів безпеки інформаційних систем;

– розвинути теоретичні положення побудови нейромережевих моделей та методів оцінки параметрів безпеки інформаційних систем, що враховують особливості сучасних видів кібератак, умови використання нейромережевих моделей та надають можливість верифікації отриманих рішень;

– побудувати моделі, що враховують запропоновані теоретичні рішення та використовуються в нейромережевих засобах оцінки параметрів безпеки;

– розробити методи створення нейромережевих засобів оцінювання параметрів безпеки, що враховують запропоновані теоретичні рішення та побудовані моделі;

– розробити нейромережеві системи оцінки параметрів безпеки інформаційних систем, які дозволяють розпізнавати шкідливе програмне забезпечення, класифікувати листи електронної пошти та розпізнавати мережеві кібератаки.

Об'єктом дослідження є процеси оцінки параметрів безпеки ресурсів Інтернет-орієнтованих інформаційних систем для розпізнавання кібератак.

Предметом дослідження є нейромережеві моделі, методи та засоби процесів оцінювання параметрів безпеки ресурсів Інтернет-орієнтованих інформаційних систем для розпізнавання кібератак.

Методи дослідження. Використано методи теорії захисту інформації, НМ, марківських процесів, прикладної статистики, оптимізації та комп'ютерного моделювання.

Наукова новизна отриманих результатів. У результаті проведених досліджень науково обгрунтовано комплексну методологію розробки широкодоступних ефективних нейромережевих засобів оцінки параметрів безпеки ресурсів Інтернет-орієнтованих інформаційних систем, які дозволяють оперативно розпізнавати нові види кібератак при обмежених обчислювальних ресурсах та варіативності умов застосування.

При цьому отримано наступні нові наукові результати:

– отримали подальший розвиток теоретичні положення побудови нейромережевих засобів оцінки параметрів безпеки, які за рахунок вперше розроблених підходів до розпізнавання поступових та неочікуваних кібератак, визначення оптимального виду нейромережевої моделі, доцільності застосування та ефективності розробки нейромережевих засобів, класифікації статистично подібних кібератак, застосування продукційних правил для подання експертних знань, верифікації нейромережевих моделей, запропонованих критеріїв оцінки ефективності нейромережевих засобів, критеріїв вибору оптимального виду нейромережевої моделі та застосуванню розробленого функціоналу приведеної помилки навчання багатошарового персептрону дозволяють вдосконалювати нейромережеві засоби шляхом їх адаптації до поступових і неочікуваних кібератак, умов застосування, навчання за допомогою експертних даних та зменшувати похибки класифікації;

– отримали подальший розвиток моделі нейромережевих засобів оцінки параметрів безпеки, які за рахунок застосування розроблених теоретичних положень побудови нейромережевих засобів**,** експертного оцінювання вагомості параметрів безпеки, введення в модель MPNN нейронного шару фільтрації з лінійною біполярною з насиченням функцією активації, розроблених аналітичних залежностей для розрахунку параметрів ланцюгів Маркова, призначених для прогнозування параметрів безпеки на стаціонарних інтервалах та для оцінки оптимальної кількості схованих нейронів, кількості обчислювальних навчальних операцій, обсягу пам’яті і помилки навчання багатошарового персептрону дозволяють: визначити перелік параметрів безпеки, які доцільно оцінювати

нейромережевими засобами; створювати шаблони поведінки, адаптовані до складного характеру параметрів безпеки; зменшити ресурсоємність процесу визначення оптимальної структури багатошарового персептрону; апріорно оцінювати обчислювальні потужності, необхідні для реалізації нейромережевої моделі; за допомогою експертних даних навчати нейромережеву модель; формалізувати процес створення ефективних нейромережевих засобів, що є основою для підвищення ефективності методів їх розробки;

– вперше розроблено метод подання експертних знань для нейромережевих засобів оцінки параметрів безпеки, в якому за рахунок розробленого математичного забезпечення детермінування параметрів статистично подібних кібератак, продукційних правил представлення навчальних прикладів та структури і вагових коефіцієнтів синаптичних зв'язків нейромережевої моделі типу MPNN, забезпечується оперативність розпізнавання та розширення множини видів кібератак, характеристики яких не представлені в статистичних даних;

– вперше розроблено метод визначення часових характеристик використання нейромережевих засобів, в якому завдяки розробленим аналітичним залежностям для визначення очікуваного терміну розробки, допустимих термінів формування навчальної вибірки та навчання нейромережевої моделі, запропонованим співвідношенням між очікуваним і допустимим терміном розробки та очікуваним і допустимим терміном навчання, розробленій множині допустимих видів нейромережевих моделей отримана можливість визначення доцільності застосування нейромережевих засобів оцінки параметрів безпеки для виявлення кібератак на заданий об'єкт захисту;

– вперше розроблено метод проектування шаблону поведінки, який використовується для навчання нейромережевих моделей, в якому за рахунок застосування багатоперіодичних рядів динаміки, розробленого математичного забезпечення для розрахунку періодичних складових та розробленої негомогенної марківської моделі забезпечується зменшення похибки шаблону, що є основою для зменшення терміну формування навчальної вибірки та зменшення похибок класифікації нейромережевих моделей при розпізнаванні поступових кібератак;

– вперше розроблено метод визначення ефективності розробки нейромережевих засобів оцінки параметрів безпеки, який за рахунок застосування запропонованих параметрів оцінки ефективності, що відображають ступінь виконання основних вимог до побудови та застосування нейромережевих засобів, запропонованих вагових коефіцієнтів важливості параметрів ефективності та розробленого інтегрального показника ефективності нейромережевих засобів дозволяє, відповідно до визначених показників, обрати найбільш ефективний засіб;

– вперше розроблено комплексну методологію нейромережевої оцінки параметрів безпеки, яка за рахунок взаємопов'язаного використання розроблених підходів до верифікації нейромережевих

засобів, визначення оптимального виду нейромережевої моделі, розроблених моделей створення ефективних нейромережевих засобів оцінки параметрів безпеки, інтеграції параметрів безпеки та методів подання експертних знань, проектування шаблонів поведінки, визначення часових характеристик використання та ефективності розробки нейромережевих засобів забезпечує можливість їх верифікації, дозволяє розширити функціональні можливості та, відповідно до розробленого інтегрального показника, обрати найбільш ефективний нейромережевий засіб;

– отримали подальший розвиток структурні рішення нейромережевих систем оцінки параметрів безпеки для розпізнавання кібератак, які за рахунок використання модулів класифікації параметрів кібератак, формування статистично подібних кібератак, формування параметрів розробленої марківської моделі шаблону поведінки, підсистеми первинного визначення параметрів кібератак, модулів інтеграції параметрів безпеки, визначення обчислювальних обмежень, розрахунку критеріїв оптимізації виду та показників ефективності нейромережевої моделі, формування продукційних правил підсистеми експертного оцінювання параметрів нейромережевих засобів, модулів розробки MPNN, визначення доцільності застосування, оптимізації виду та верифікації нейромережевих моделей підсистеми розробки нейромережевих моделей, дозволяють зменшити похибку класифікації кібератак, верифікувати отримані результати і забезпечити оперативну адаптацію до умов застосування та нових типів кібератак.

Практичне значення одержаних результатів. Отримані у дисертаційній роботі наукові результати є методологічною базою для розробки і впровадження ефективних інструментальних засобів у вигляді програмних або програмно-апаратних модулів оцінки параметрів безпеки Інтернет-орієнтованих інформаційних систем для розпізнавання кібератак, які мають підвищену оперативність, адаптованість до умов застосування, нових видів кібератак та низьку обчислювальну ресурсоємність.

Практична цінність полягає у наступному:

– розроблені алгоритми визначення параметрів багатошарового персептрону, які базуються на створеній моделі багатошарового персептрону, дозволяють в 1,5-6 разів зменшити обчислювальні витрати на навчання та до 2 разів зменшити сумарну похибку його навчання, що забезпечує зменшення ресурсоємності та похибки класифікації інструментальних засобів оцінки параметрів безпеки для розпізнавання кібератак, які створені на його основі;

– на основі розробленого методу подання експертних знань для навчання нейромережевої моделі створено прикладне програмне забезпечення, яке на основі динамічної оцінки параметрів мережевого трафіку може оперативно адаптуватись до розпізнавання нових типів мережевих кібератак;

– на основі розробленого методу проектування шаблону поведінки створено прикладне програмне забезпечення для прогнозування

параметрів навантаження веб-серверу, яке дозволяє до 2 разів підвищити точність прогнозу зазначених параметрів;

– розроблене спеціалізоване програмне забезпечення, що базується на створених нейромережевих методах та моделях, дозволило підвищити захищеність інформаційних ресурсів та підвищити оперативність створення алгоритмів функціонування апаратних засобів захисту інформації, що підтверджується актами впровадження у діяльність Київського національного університету будівництва і архітектури (акт впровадження від 24.02.2014) та Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України (акт впровадження від 12.01.2015).

– розроблені програми, що реалізують запропоновані моделі та методи, впроваджені в навчальний процес на кафедрі безпеки інформаційних технологій Національного авіаційного університету (акт впровадження від 17.02.2015) та на кафедрі системного програмування та спеціалізованих комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут» (акт впровадження від 24.02.2015).

Особистий внесок здобувача. Всі основні результати дисертаційної роботи отримані здобувачем самостійно. У роботах, опублікованих із співавторами, здобувачу належить: метод оцінки ефективності нейромережевих засобів [2, 58, 59], підхід до верифікації нейромережевих методів розпізнавання кібератак [3], метод застосування продукційних правил [6], підхід до застосування нейромережевих моделей [12], визначення типу та параметрів архітектури нейронної мережі [13, 16, 51], метод оцінки нейромережевих засобів щодо можливостей виявлення кібератак [14], критерій оптимізації та оптимізаційна моделі [25, 50], концепція застосування спектрального аналізу статистичних даних [34], методологія використання нейромережевих технологій в системах розпізнавання атак [40], марківська модель динаміки параметрів технічного стану та марківська оптимізаційна модель [41-44], негомогенна марківська модель [55], метод оптимізації нейромережевої моделі [57].

Апробація результатів дисертації. Основні результати дисертації доповідались, обговорювались та отримали позитивні оцінки на наступних конференціях: Міжрегіональний семінар наукової міжвідомчої Ради НАН України «Технічні засоби захисту інформації» (2004-2008); V Міжнародна науково-практична конференція «Проблеми впровадження інформаційних технологій в економіці» (Ірпінь, 2004); Международная научно-практическая конференция «Единое информационное пространство '2004», (Днепропетровск, 2004); 70 наукова конференція молодих вчених, аспірантів та студентів (Київ, 2004); VI Всеукраїнська науково-практична конференція «Комп'ютерне моделювання та інформаційні технології в науці, економіці та освіті» (Кривий Ріг, 2005); Четверта науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» (Київ, 2006); IX Международная научно-

практическая конференция «Безопасность информации в информационно-телекоммуникационных системах» (Киев, 2006); Міжнародна науково-теоретична конференція «Актуальні проблеми державного управління та документо-інформаційного забезпечення апарату влади» (Київ, 2006); II Міжнародна науково-технічна конференція «Сучасні інформаційно-комунікаційні технології /COMINFO' 2006/» (Київ, 2006); III Міжнародна науково-методична конференція «Болонський процес: трансформація навчального процесу у технологію навчання» (Київ, 2007); IV Міжнародна науково-методична конференція «Сучасні тенденції розвитку вищої освіти, трансформація навчального процесу у технологію навчання» (Київ, 2007); VI Міжнародна науково-практична конференція «Проблеми впровадження інформаційних технологій в економіці» (Ірпінь, 2007); Науково-практична конференція «Інформаційна безпека» (Київ, 2009); Міжнародна науково-практична конференція «Моделювання об'єктів, процесів та систем» (Київ, 2011); V Міжнародна науково-технічна конференція ACSN-2011 «Сучасні комп'ютерні системи та мережі: розробка та використання» (Львів, 2011); VIII Наукова конференція Державного університету інформаційно-комунікаційних технологій «Сучасні тенденції розвитку технологій в інфокомунікаціях та освіті» (Київ, 2011); VII Міжнародна науково-технічна конференція «Сучасні інформаційно-комунікаційні технології» COMINFO' 2011 (Київ, 2011); VIII Міжнародна науково-практична інтернет-конференця «Проблеми впровадження інформаційних технологій в економіці» (Ірпінь, 2012); Перша всеукраїнська науково-практична конференція Moodle Moot Ukraine 2013 «Теорія і практика використання системи управління навчанням Moodle» (Київ, 2013); II Всеукраїнська науково-практична конференція «Соціальні комунікації: стан, проблеми, тенденції» (Київ, 2014); Друга міжнародна науково-практична конференція MoodleMoot Ukraine 2014 «Теорія і практика використання системи управління навчанням Moodle» (Київ, 2014); Всеукраїнська науково-практична конференція «Стратегії розвитку інформаційного культурно-освітнього та економічного простору України» (Київ, 2014); IV міжнародна науково-технічна конференція ITSEC (Київ, 2014); The Sixth World Congress «Aviation in the XXI-st Century», «Safety in Aviation and Space Technologies» (Kyiv, 2014).

Публікації. За тематикою дослідження опубліковано 59 наукових праць, серед них 1 одноосібна монографія, 44 статей у фахових наукових виданнях (з них 31 одноосібна), 13 у збірниках праць конференцій, 12 статей опубліковано у виданнях, які включені до міжнародних наукометричних баз.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, п’яти розділів, висновків та списку використаних джерел (278 найменувань) на 31 сторінках, 2 додатків на 33 сторінках. Загальний обсяг дисертації становить 312 сторінок, у тому числі 245 сторінки основного тексту, ілюстрацій – 41 (з них 1 – на 1 окремій сторінці), таблиць – 26 (з них 2 – на 2 окремих сторінках).

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційної роботи, зазначено її зв'язок з науковими програмами, планами та темами, сформульовано мету та задачі досліджень, охарактеризовано наукову новизну та практичне значення отриманих результатів. Наведено відомості про впровадження результатів роботи, їх апробацію та публікації.

У першому розділі охарактеризовано предмет дослідження, а також проведено аналіз сучасного стану та тенденцій розробки і застосування нейромережевих методів, моделей і засобів оцінки параметрів безпеки (ПБ) ІС. Показано, що в більшості випадків доцільність застосування нейромережевих систем (НМС) та вид нейромережевої моделі (НММ) мало обґрунтовані, параметри НММ оптимізуються емпірично, подання експертних знань в такі системи не передбачено, достовірність отриманих результатів підтверджується на фрагментарних тестових прикладах, а методи оцінки ефективності такого застосування відсутні. Разом з тим, визначено ряд параметрів, на основі яких можливо оцінити ефективність застосування нейромережевого інструментарію для розпізнавання кібератак. Також показано, що для оцінки ПБ доцільно використовувати наступні види НММ: багатошаровий персептрон (БШП), згорткові (ЗНМ), радіальної базисної функції (РБФ), ймовірнісні (PNN), адаптивної резонансної теорії (АРТ), асоціативні мережі Хеммінга, Хопфілда та Коско (АНМ), Елмена (ЕНМ), Джоржана (ДНМ), мережу Кохонена (ТК), семантичну нейронну мережу (СНМ). Проведено дослідження основних характеристик вказаних НММ. Доведено, що підвищити ефективність розпізнавання розподілених в часі кібератак можливо за рахунок використання НМ для визначення відхилень ПБ від шаблонів поведінки (ШП) ПБ, розрахованих за допомогою марківських моделей (ММ). При цьому визначено необхідність вдосконалення існуючих ММ за рахунок більш повної адаптації до складної нестаціонарної динаміки ПБ. Обгрунтована необхідність використання вдосконалених НМС для розпізнавання кібератак, пов'язаних з шкідливим програмним забезпеченням (ШПЗ), витоками текстової інформації по мережевим каналам зв'язку; нецільовими електронними листами (спаму); віддаленими мережевими кібератаками на Інтернет-сервери. Таким чином, на підставі проведеного аналізу показано, що підвищити ефективність розпізнавання кібератак на ресурси Інтернет-орієнтованих ІС можливо за рахунок розробки та застосування комплексної методології нейромережевої оцінки параметрів безпеки. Для створення такої методології необхідно розвинути теоретичні положення, моделі та методи побудови нейромережевих засобів, що забезпечать можливість їх функціонування при обмежених обчислювальних ресурсах та дозволять оперативно адаптуватись до умов застосування та нових типів кібератак.

Другий розділ присвячено розвитку теоретичних положень побудови нейромережевих засобів оцінки ПБ ІС.

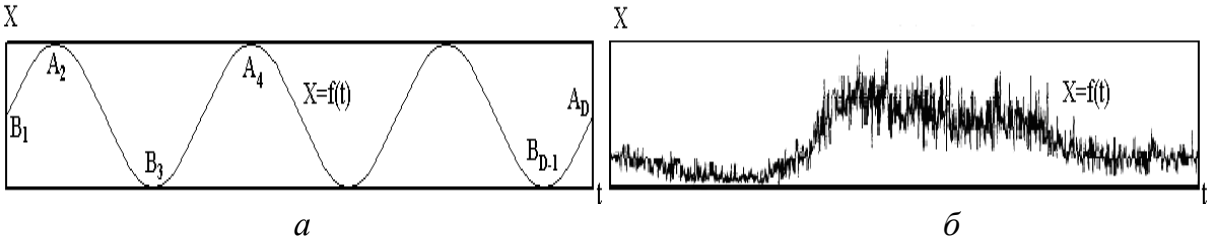
Показано, що використання НММ для оцінки ПБ багато в чому залежить від характеру кібератаки – поступового або неочікуваного.

Визначення 1. Неочікуваною є кібератака, пов'язана з стрибкоподібним та неочікуваним, з точки зору СЗІ, виходом ПБ за безпечні межі.

Визначення 2. Поступовою є кібератака, яка виникає в результаті тривалої та очікуваної, з точки зору СЗІ, зміни ПБ до значень, які перевищують безпечні межі.

Підхід для розпізнавання неочікуваних кібератак. Оскільки неочікувана кібератака (НК) характеризується деструктивним впливом, результативність якого не залежить від терміну експлуатації, то для її своєчасного виявлення потрібно реалізувати постійний контроль та оцінку ПБ. Виявити НК необхідно до того, коли ПБ вийдуть за межі попереджувального допуску. В якості бази визначення ПБ доцільно використовувати параметри зовнішніх програмних запитів до ІС. Рішення про наявність кібератаки приймається, якщо виявлено відповідність параметрів цих запитів відомому шаблону атаки (ША) або не відповідність шаблону нормальної поведінки (ШНП). Тобто Якщо $\{X(t_k)\} \subset \left(\{X\}_A \cup \{D\}_A\right) \wedge / \vee \{X(t_k)\} \not\subset \left(\{X\}_N \cup \{D\}_N\right) \rightarrow A$, де $\{X(t_k)\}$ – множина значень ПБ в *k*-ий момент часу, $\{X\}_A$ – значення ПБ, що відповідають ША, $\{X\}_N$ – комбінація значень ПБ, що відповідають ШНП, $\{D\}_A$ – множина попереджувальних допусків на ПБ ША, $\{D\}_N$ – множина попереджувальних допусків на ПБ ШНП, A – кібератака.

Підхід для розпізнавання поступових кібератак. Оскільки поступова кібератака (ПК) є тривалим процесом, то для її своєчасне виявлення доцільно скористатись ШП, розрахованими на протязі деякого інтервалу часу. В якості ПБ можливо використовувати параметри зовнішніх запитів та функціональні параметри РІС. Правило класифікації ПК має вигляд: Якщо $\{X(t_k)\} \subset \left(\{X(t)_{t=t_k}\}_A \cup \{D\}_A\right) \wedge / \vee \{X(t_k)\} \not\subset \left(\{X(t)_{t=t_k}\}_N \cup \{D\}_N\right) \rightarrow A$, де $\{X(t)_{t=t_k}\}_A$ – комбінація значень ПБ, що відповідають ША в *k*-ий момент часу, $\{X(t)_{t=t_k}\}_N$ – комбінація значень ПБ, що відповідають ШНП в k-ий момент часу. Показано, що в залежності від характеру зміни ПБ ШП розділяються на одноперіодичні (рис. 1, *а*) та багатоперіодичні (рис. 1, *б*). В одноперіодичних ШП ПБ має характер одноперіодичної часової функції, а в багатоперіодичному ШП – характер багатоперіодичної часової функції.



а *б*

Рис. 1. Графіки шаблону поведінки

З метою спрощення моделювання піддослідний часовий діапазон розділено на стаціонарні інтервали типу $B_d A_{d+1}$ та $A_{d+1} B_{d+2}$, де $d \in [1,2,...,D]$ – номер поточної перехідної точки, D – кількість перехідних точок. На інтервалах типу $B_d A_{d+1}$ функція зростає, а на інтервалах типу $A_{d+1} B_{d+2}$ – спадає. Запропоновано представити багатоперіодичний ШП як суму одноперіодичних ШП. Введена множина характеристик об'єкту захисту (***O***), аналіз яких дозволяє визначити перелік ПБ. В першому наближенні елементами ***O*** є: структура (o_1), призначення (o_2), вразливості (o_3), функціональність (o_4), загрози (o_5).

Для визначення оптимального виду НММ запропоновано підхід – ефективність застосування НММ залежить від того, наскільки характеристики виду НММ відповідають значимим умовам задач оцінки ПБ. В базовому варіанті множина значимих умов (***У***) поділяється на категорії, що характеризують навчальні дані (y_1), обмеження процесу навчання (y_2), обчислювальні потужності (y_3), вихідну інформацію (y_4), технічну реалізацію (y_5), сферу застосування (y_6) НМЗ розпізнавання. Проведена деталізація наведених категорій. При цьому *i*-ий критерій оптимізації вказує на відповідність *i*-ої характеристики виду НММ *i*-ій умові. Значимість критерію враховується шляхом використання вагових коефіцієнтів, що розраховуються на основі експертних даних. Критерії розділені відповідно категорій характеристик видів НММ. Виставлені в першому наближенні величини цих критеріїв фрагментарно наведено в табл.1. Критерій E_i=1, якщо *i*-а умова повністю забезпечується у НММ, E_i=0 – якщо забезпечується частково і E_i=-1 – якщо не забезпечується. Визначено інтегральний критерій оптимізації для *i*-го виду НММ $E_i^{\Sigma} = \sum_{j=1}^{J} \sum_{n=1}^{N} \left(\left(v_{j,n} \times E_{j,n}(m_i) \right) \right) \to \max, \quad m_i \in \boldsymbol{M}, i = 1,2,...,I$, де $E_{j,n}(m_i)$ – оцінка *j,n*-ого критерію для *i*-ої НММ, $v_{j,n}$ – ваговий коефіцієнт, m_i – *i*-ий вид НММ, ***M*** – множина допустимих НММ, I – кількість допустимих НММ, J – кількість категорій критеріїв, N – кількість критеріїв в J-ій категорії.

Таблиця 1

Оцінки одиничних критеріїв

№ з/п	Вид нейромережевої моделі				
	БШП	Згорткові	РБФ	АРТ	PNN
$E_{1,1}$	-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

Розроблено *підхід до визначення принципової доцільності застосування НМЗ оцінки ПБ*, котрий базується на визначенні можливості в прийнятний термін розробити параметри НММ. Показано, що доцільність використання НМЗ можливо визначити за допомогою виразу: $T_f = T_n + t_n \le T_a$, де T_a – допустимий термін створення системи розпізнаваня, T_n – термін формування навчальної вибірки, t_n – термін навчання НМ.

Розроблено *підхід до визначення ефективності розробки НМЗ оцінки ПБ*. Підхід передбачає співвідношення ефективності застосування з виконанням основних вимог до побудови та застосування НМЗ. Ефективність виконання вимог оцінюється за допомогою критеріїв оцінки ефективності, визначених в процесі аналізу НМЗ. Важливість вимоги враховується за допомогою вагових коефіцієнтів, визначених на основі експертних даних. Ефективність НМЗ вважається достатньою, якщо вона перевищує мінімально допустимий рівень.

Запропоновано *підхід до класифікації подібних кібератак*: *i*-та та *k*-та кібератаки вважаються подібними, якщо вони мають однаковий характер – неочікуваний (Ks) або поступовий (Kq), а приведена різниця параметрів безпеки (R_p), не перевищує максимальну ($R_{\max}$): $\exists\left(Ka_i = Ks \wedge Ka_k = Ks\right) \vee \left(Ka_i = Kq \wedge Ka_k = Kq\right) \wedge \left(R_p \le R_{\max}\right) \rightarrow \left(Ka_i \sim Ka_k\right)$, де $R_p = \left|R_i - R_k\right| / R$, R_i, R_k – кількість ПБ при розпізнаванні *i*-ої та *k*–ої кібератак, $R = \max\left(R_i, R_k\right)$. $R_{\max}$ визначається на основі експертних даних.

Розроблено *підхід до застосування продукційних правил при поданні експертних знань в НМЗ оцінки ПБ для виявлення подібних кібератак*. Передбачено представлення навчальних прикладів у вигляді продукційних правил: Якщо $p_1 \in \left\lfloor P_1^{\min}, P_1^{\max} \right\rfloor_l \wedge \ldots \wedge p_K \in \left\lfloor P_K^{\min}, P_K^{\max} \right\rfloor_l \rightarrow Y_l$, де $p_1, \ldots, p_K$ – ПБ, $\left\lfloor P_1^{\min}, P_1^{\max} \right\rfloor, \ldots, \left\lfloor P_K^{\min}, P_K^{\max} \right\rfloor$ – задані діапазони величин ПБ, K – кількість ПБ, l, Y_l – номер та результат продукційного правила. Визначена можливість застосування даного підходу для навчання НММ типу PNN.

Розроблено *функціонали оцінки ПБ* при реалізації кібератаки та в процесі нормального функціонування: $A \rightarrow \left\{l(t)\right\} \subset \left\{L_a(t)\right\}$, $N \rightarrow \left\{l(t)\right\} \subset \left\{L_n(t)\right\}$, де $\{l(t)\}$ – множина значень ПБ на момент часу t, $\left\{L_a(t)\right\}$ – множина значень ПБ при реалізації атаки, $\left\{L_n(t)\right\}$ – множина значень ПБ, характерних для нормального стану ІС на момент часу t, A – реалізація кібератаки, N – нормальний стан захищеності РІС. Показано, що функції $l(t), L_a(t), L_n(t)$ в багатьох випадках є неперервними та гладкими.

Вдосконалено *математичне забезпечення процесу навчання БШП*, що дозволяє вирівняти приведену помилку навчання для прикладів з мінімальними та максимальним величинами вхідних параметрів, що характерно при оцінюванні мережевих ПБ. Показано, що використання вдосконаленого математичного забезпечення дозволяє до 2 разів зменшити помилку навчання НММ.

Проведена *верифікація НММ оцінки ПБ для розпізнавання кібератак.* Обгрунтовано можливість представлення процесу нейромережевого оцінювання ПБ як нейромережевої апроксимації функціоналів оцінок ПБ. Показано, що функції $l(t), L_a(t), L_n(t)$ можливо з заданою точністю представити за допомогою НМ з прямим розповсюдженням сигналу.

Третій розділ присвячено розробці моделей, що використовуються для оцінювання ПБ ІС. *Розроблено модель процесів інтеграції ПБ ІС*, що використовуються для розпізнавання ПК та НК (рис. 2). Вхідною інформацією моделі являється множина характеристик об'єкту захисту (***O***), а виходом моделі є множина ПБ, оцінювання яких дозволяє визначити ПК та НК, характерні для об'єкту захисту. Модель складається із п'яти базових процесів, котрі співвідносяться з процесами інтеграції.

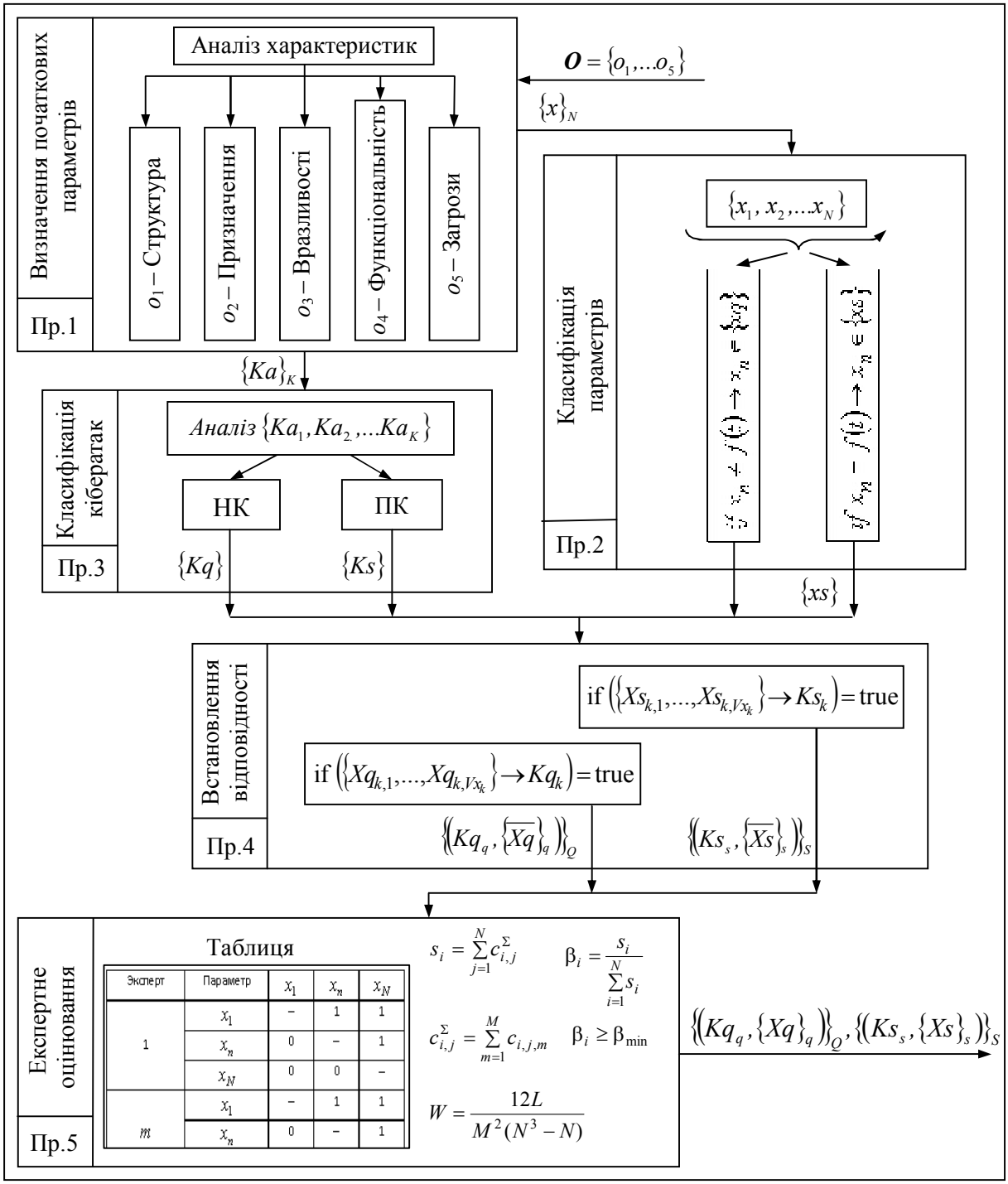


Рис. 2. Відображення моделі процесів інтеграції параметрів безпеки

Процес 1 – визначення початкових параметрів, що відбувається в результаті аналізу ***O***. Початковими параметрами являється множина

кібератак, характерних для об'єкту захисту $\{Ka\}_K$ та множина підконтрольних ПБ $\{x\}_N$, де K – кількість кібератак, N – кількість ПБ.

Процес 2 – класифікація ПБ. Результатом даного процесу є визначення із $\{x\}_N$ множини ПБ, придатних для розпізнавання НК $\{xq\}$ та множини ПБ, придатних для розпізнавання ПК $\{xs\}$. Правила класифікації визначаються виразами: if $x_n \neq f(t) \to x_n \in \{xq\}$, if $x_n = f(t) \to x_n \in \{xs\}$.

Процес 3 – класифікація кібератак. Процес орієнтований на аналіз $\{Ka\}_K$ з метою виділення множини НК $\{Kq\}$ та множини ПК $\{Ks\}$. В процесі аналізу використано підходи до розпізнавання НК та ПК.

Процес 4 – встановлення відповідності. В даному процесі в першому наближенні для кожної кібератаки встановлюється відповідність з множиною ПБ, що можуть використовуватись як вхідні параметри НММ. Виходом процесу є $\{(Kq_q, \{\overline{Xq}\}_q)\}_Q$ та $\{(Ks_s, \{\overline{Xs}\}_s)\}_S$, де $\{\overline{Xq}\}_q, \{\overline{Xs}\}_s$ – множини ПБ, що можуть використовуватись для розпізнавання q-ої НК та s-ої ПК, Q, S – кількість можливих НК та ПК.

Процес 5 – експертне оцінювання. В результаті реалізації даного процесу остаточно визначається множина ПБ, що використовується в якості вхідних параметрів НМЗ. Для k-ої кібератаки вихід процесу задається виразом $(K_k, \{X\}_k)$, де $\{X\}_k$ – множина ПБ, визначених в процесі 4. В процесі 5 використовується експертне оцінювання ступеню важливості ПБ. Застосовано метод парних порівнянь, котрий передбачає подання експертних даних у вигляді $C = \{c_{1,1,1}, ...c_{i,j,m}, ...c_{N,N,M}\}$, де $c_{i,j,k}$ – виставлена m-им експертом оцінка порівняння i-го ПБ з j-им ПБ, N – кількість ПБ, M – кількість експертів. Узгодженість експертних даних перевіряється за допомогою коефіцієнта конкордації (W).

Основна відмінність розробленої моделі полягає у використанні експертного оцінювання важливості вхідних параметрів НМЗ виявлення ПК та НК. Апробація моделі дозволила визначити набір ПБ, які були використані для розпізнавання НК, реалізованих за допомогою веб-орієнтованого ШПЗ, написаного на мові програмування JavaScript.

Побудовано марківську модель одноперіодичного ШП ПБ M_{BAB} (рис. 3). Відповідно розробленого одноперіодичного ШП, M_{BAB} складається із двох однорідних ланцюгів Маркова (ЛМ) M_{BA} та M_{AB}, призначених для моделювання ПБ на стаціонарних інтервалах типу $B_d A_{d+1}$ і $A_{d+1} B_{d+2}$, де d – номер перехідної точки.

Для визначення M_{BA} та 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 ймовірностей $\pi^{(A)} = \left\| p_{i,i+1}^{(A)} \right\|$ і $\pi^{(B)} = \left\| p_{i,i+1}^{(B)} \right\|$ та вектор початкового розподілу $\left\| P^{(A)}(0) \right\| = \left\langle P_1^{(A)}(0), P_2^{(A)}(0), ..., P_N^{(A)}(0) \right\rangle$, де $p_{i,j}$ –

ймовірність переходу із стану i в стан i+1 за один крок процесу, $i, j \in [1, N]$, N – кількість станів ЛМ, $P_i^{(A)}(0)$ – ймовірність перебування ПБ в стані i в початковий момент часу.

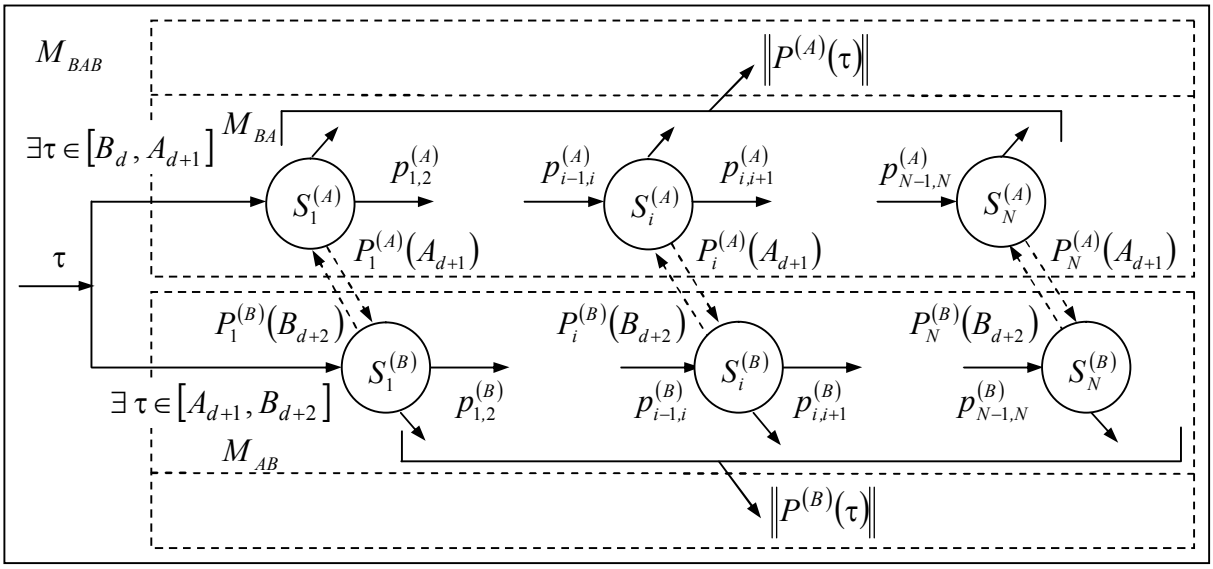


Рис. 3. Марківська модель одноперіодичного шаблону поведінки

На вхід моделі подається номер кроку моделювання τ. При цьому поточний час моделювання $t = \tau \times \Delta t$, де Δt – тривалість кроку моделювання. Для обчислення ймовірностей станів M_{BA} (M_{AB}) використовується система рівнянь Колмогорова-Чепмена – $\|P^{(A)}(\tau)\| = \|P^{(A)}(\tau - 1)\| \times \pi^{(A)}$, $\left(\|P^{(B)}(\tau)\| = \|P^{(B)}(\tau - 1)\| \times \pi^{(B)}\right)$, де $\|P^{(A)}(\tau)\|$ $\left(\|P^{(B)}(\tau)\|\right)$ – вектор ймовірностей станів M_{BA} (M_{AB}) на τ-му кроці. Також використовується умова нормування $\sum_{i=1}^{N} P_i^{(A)} = 1$ $\left(\sum_{i=1}^{N} P_i^{(B)} = 1\right)$. При переході τ із інтервалу $B_d A_{d+1}$ в $A_{d+1} B_{d+2}$ початковий вектор розподілу M_{AB} дорівнює кінцевому вектору розподілу M_{BA} – $\|P^{(B)}(A_{d+1})\| = \|P^{(A)}(A_{d+1})\|$. При переході τ із інтервалу $A_{d+1} B_{d+2}$ в $B_{d+2} A_{d+3}$ – $\|P^{(A)}(B_{d+2})\| = \|P^{(B)}(B_{d+2})\|$. M_{BAB} дозволяє для одноперіодичного ШП розрахувати розподіл ймовірності станів ЛМ.

Побудовано марківську модель багатоперіодичного ШП ПБ M_{BAB}^{Σ}, яка базується на запропонованій моделі M_{BAB} та складається із модулів $M_{BAB}^{(1)}, M_{BAB}^{(2)}, ..., M_{BAB}^{(K)}$, призначених для моделювання K значимих періодів багатоперіодичного ШП. В свою чергу, $M_{BAB}^{(k)}$ складається із ЛМ ($M_{BA}^{(k)}$, $M_{AB}^{(k)}$), призначених для моделювання k-ої періодичної складової ШП на стаціонарних інтервалах типу $B_d A_{d+1}^{(k)}$ і $A_{d+1} B_{d+2}^{(k)}$. Виходом $M_{BAB}^{(k)}$ є

$\left\|P^{(k)}(\tau)\right\|$ – вектор розподілу ймовірностей для *k*-ої періодичної складової ШП на *τ*-му кроці розрахунку. Також в M^{Σ}_{BAB} розраховується інтегральний вектор розподілу ймовірностей $\left\|P^{(\Sigma)}(\tau)\right\| = \left\langle P_1^{(\Sigma)}(\tau), P_2^{(\Sigma)}(\tau), ... P_N^{(\Sigma)}(\tau)\right\rangle$, де $P_i^{(\Sigma)}(\tau) = K^{-1}\sum_{k=1}^{K} P_i^{(k)}(\tau)$. На відміну від відомих, модель M^{Σ}_{BAB} дозволяє враховувати типовий багатоперіодичний характер ШП ПБ.

Розроблені ММ застосовано для створення ШП Веб-серверу. В якості ПБ *X* використано кількість звернень (рис. 4). На рис. 4 цифрою 1 позначено графік на основі статистичних даних, цифрою 2 – на основі M_{BAB}, а цифрою 3 – на основі M^{Σ}_{BAB}. Для M_{BAB} середня похибка моделювання 0,09, для M^{Σ}_{BAB} – 0,07, що в 1,5–2 рази менше похибок відомих моделей.

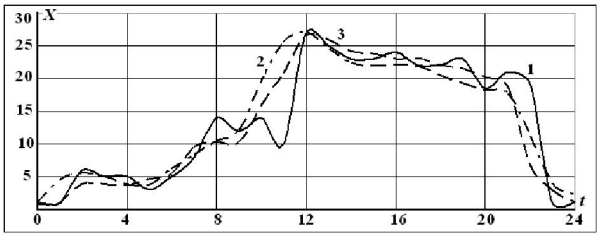


Рис. 4. Графіки динаміки математичного сподівання кількості звернень до веб-серверу

Розроблена модель БШП для оцінки ПБ. Особливістю моделі є застосування в процесі навчання створеного математичне забезпечення та розрахунок оптимальної кількості схованих нейронів (N_1^{opt}) за допомогою розробленого виразу $(0{,}4N_X + 0{,}2)\sqrt{P \times N_X}\,/(N_X + N_Y) \le N_1^{\text{opt}} \le 2\sqrt{P \times N_X}\,/N_Y$, де N_X, N_Y – кількість вхідних та вихідних нейронів, *P* – кількість навчальних прикладів. Отримані рішення верифіковані експериментально шляхом застосування БШП для апроксимації поліноміальних функцій. Для прикладу на рис. 5 показано графіки залежності відносної помилки (δ) навчання, інтерполяції та екстраполяції функції $y = 2x + 1$ від кількості схованих нейронів (N_1). На рис. 5 цифрою *1* позначено графік помилки навчання, цифрою *2* – графік помилки інтерполяції і цифрою *3* – графік помилки екстраполяції. Аналіз графіків підтверджує мінімізацію помилки БШП при $6 \le N_1 \le 20$, що відповідає теоретичним викладкам. Доведено, що використання розробленої моделі забезпечує зменшення діапазону пошуку N_1^{opt} в 1,5-6 разів, що дозволяє пропорційно зменшити

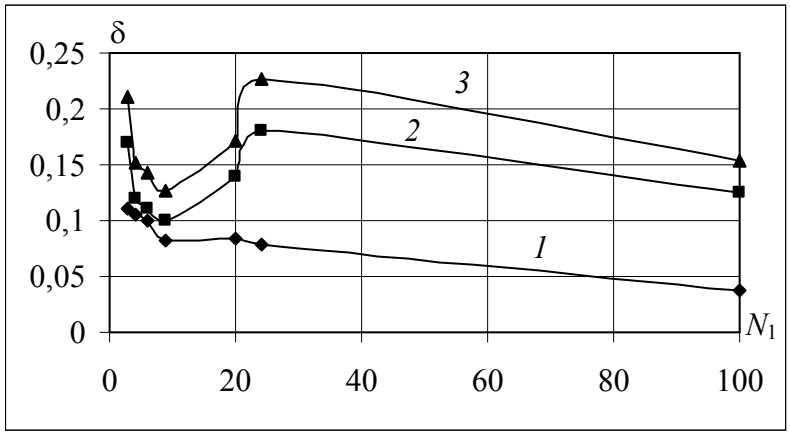


Рис. 5. Графіки залежності помилки БШП від кількості схованих нейронів

обчислювальні витрати на розробку БШП. Також отримано вирази, які дозволяють апріорно оцінити обсяг обчислювальних ресурсів, необхідних для реалізації БШП з заданими властивостями.

Побудована модифікована модель ймовірнісної мережі (MPNN), призначена для оцінки ПБ, яка, відповідно розробленого підходу, дозволяє проводити навчання НМ із застосуванням продукційних правил. Структура моделі для оцінки ПБ з метою класифікації станів *A* (безпечний стан) та *B* (реалізація кібератаки) показана на рис. 6.

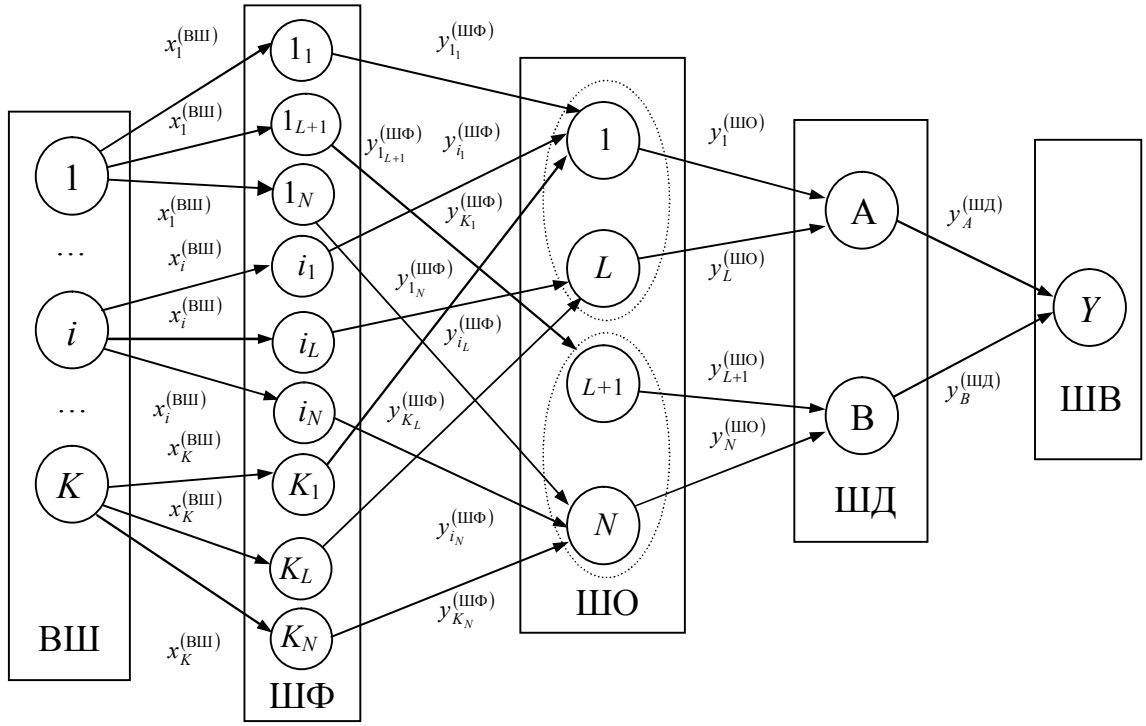


Рис. 6. Структура моделі MPNN

До складу мережі входять п’ять шарів нейронів: вхідний (ВШ), шар фільтрації (ШФ), образів (ШО), додавання (ШД) та вихідний (ШВ). Нейрони ВШ асоціюються з ПБ, а нейрони ШД асоціюються з класами, що розпізнаються. Вагові коефіцієнти вхідних зв’язків нейронів ШФ, ШД та ШВ дорівнюють 1. Вагові коефіцієнти вхідних зв’язків ШО дорівнюють компонентам навчальних прикладів. Кількість нейронів ВШ (*K*) дорівнює кількості ПБ, котрі подаються на вхід НМ. Кожен нейрон ВШ, пов’язаний з такою кількістю нейронів ШФ, яка дорівнює кількості нейронів ШО, кожен із яких асоціюється з власним продукційним правилом. Нейрони ШФ пронумеровані як i_k, де *i* – номер пов’язаного з ним вхідного нейрону, а *k*– номер пов’язаного з ним нейрону ШО (номер продукційного правила). Завданням i_l нейрону ШФ є фільтрація *i*-го ПБ відповідно *l*–го продукційного правила. Для цього застосовується функція активації виду: $\exists x_i^{(\text{ВШ})} \in \left\lfloor P^{\min}, P^{\max} \right\rfloor_l \rightarrow y_{j_l}^{(\text{ШФ})} = x_i^{(\text{ВШ})}, \exists x_i^{(\text{ВШ})} \notin \left\lfloor P^{\min}, P^{\max} \right\rfloor \rightarrow y_{j_l}^{(\text{ШФ})} = 0$, де $x_i^{(\text{ВШ})}$ – значення *i*-го ПБ, $y_{j_l}^{(\text{ШФ})}$– вихідний сигнал j_l нейрону ШФ. Вихідний сигнал *l*-го нейрону ШО розраховується так:

$y_l^{(\text{ШО})} = \sum_{k=1}^{K} \exp\left(-(w_{k_l,l} - y_{k_l}^{(\text{ШФ})})^2 \Big/ 2\sigma^2\right)$, де $w_{k_l,l}$ – ваговий коефіцієнт зв'язку між k_l-им нейроном ШФ та l-им нейроном ШО, K – кількість компонент вхідного вектора-образу, σ – радіус функції Гауса.

В нейронах ШД використовується лінійна функція активації. Вихідний сигнал j-го нейрону ШД ($y_j^{(\text{ШД})}$) розраховується так: $y_j^{(\text{ШД})} = \sum_{i=1}^{N} y_i^{(\text{ШО})}$, де N – кількість нейронів ШО, пов'язаних з j-им нейроном ШД, $y_i^{(\text{ШО})}$ – активність i-ого нейрону ШО, пов'язаного з j-им нейроном ШД.

Завданням єдиного нейрону ШВ є визначення максимального вихідного сигналу нейронів ШД. Даний нейрон вказує на розпізнаний клас.

Побудована модель процесу створення ефективних НМЗ розпізнавання кібератак (рис. 7). Вхідними даними моделі являються множина доступних НМЗ $\boldsymbol{M}$, множина умов задачі оцінювання ПБ $\boldsymbol{У}$ та множина характеристик об'єкту захисту $\boldsymbol{O}$. Першочерговий аналіз вхідних параметрів відбувається у відповідних модулях. В результаті аналізу елементів $\boldsymbol{M}$ для кожного з них визначаються величини критеріїв ефективності ($m(\phi_1, \phi_2, ..., \phi_N)$), функціональна залежність мінімальної кількості навчальних прикладів від кількості вхідних параметрів ($P_{\min}(N_x)$), функціональні залежності похибки навчання (ε) і кількості обчислювальних операцій (ξ) від кількості синаптичих зв'язків (L_w), навчальних прикладів (P), кількості вхідних (N_x) та вихідних параметрів (N_y) – $m\left(\varepsilon = f\left(L_w, P, N_x, N_y\right), \xi = f\left(L_w, P, N_x, N_y\right)\right)$. Також для кожного $m_k \in \boldsymbol{M}$ визначається залежність терміну навчання (T) від тривалості навчальної ітерації (τ), допустимої похибки навчання ($\varepsilon_{\max}$), кількості навчальних прикладів (P), кількості вхідних параметрів і вихідних параметрів – $T_k = f_k\left(\tau, \varepsilon_{\max}, P, N_x, N_y\right)$.

В результаті аналізу $\boldsymbol{У}$ та $\boldsymbol{O}$ визначаються оцінки важливості показників ефективності ($\boldsymbol{C} = \{c_1, c_2, ..., c_K\}$), набір ПБ ($\{x\}_I$), допустимий термін створення НМЗ (T_a), залежність терміну створення навчальної вибірки від P ($t_p = f_p(P)$), допустима помилка навчання ($\varepsilon_{\max}$), допустима кількість навчальних ітерацій ($\xi_{\max}$), тривалість однієї навчальної ітерації (τ), кількість вхідних та вихідних параметрів.

Подання величин τ, P, $\varepsilon_{\max}$, N_x, N_y, визначених в модулях аналізу, в вираз $T_{f_i} = f_p(P_i) + f_i\left(\tau, \varepsilon_{\max}, N_x, N_y\right)$ дозволяє розрахувати тривалість терміну розробки параметрів кожного i-го НМЗ, а порівняння T_{f_i} з T_a призводить до визначення принципової доцільності застосування НМЗ. Остаточне формування множини допустимих НМЗ $\{m\}_D$ реалізується в

модулі «Допустимі засоби». Вихідні дані даного модулю $\{m(\phi_1,...\phi_N,\varepsilon,\xi=f(L_w,P,N_x,N_y))\}_D$ поступають в модуль «Управління створенням ефективних засобів», в якому визначається множина ефективних НМЗ ($\{m\}_E$), за допомогою розробленої моделі проводиться інтеграція ПБ та оптимізуються параметри визначених ефективних НМЗ.

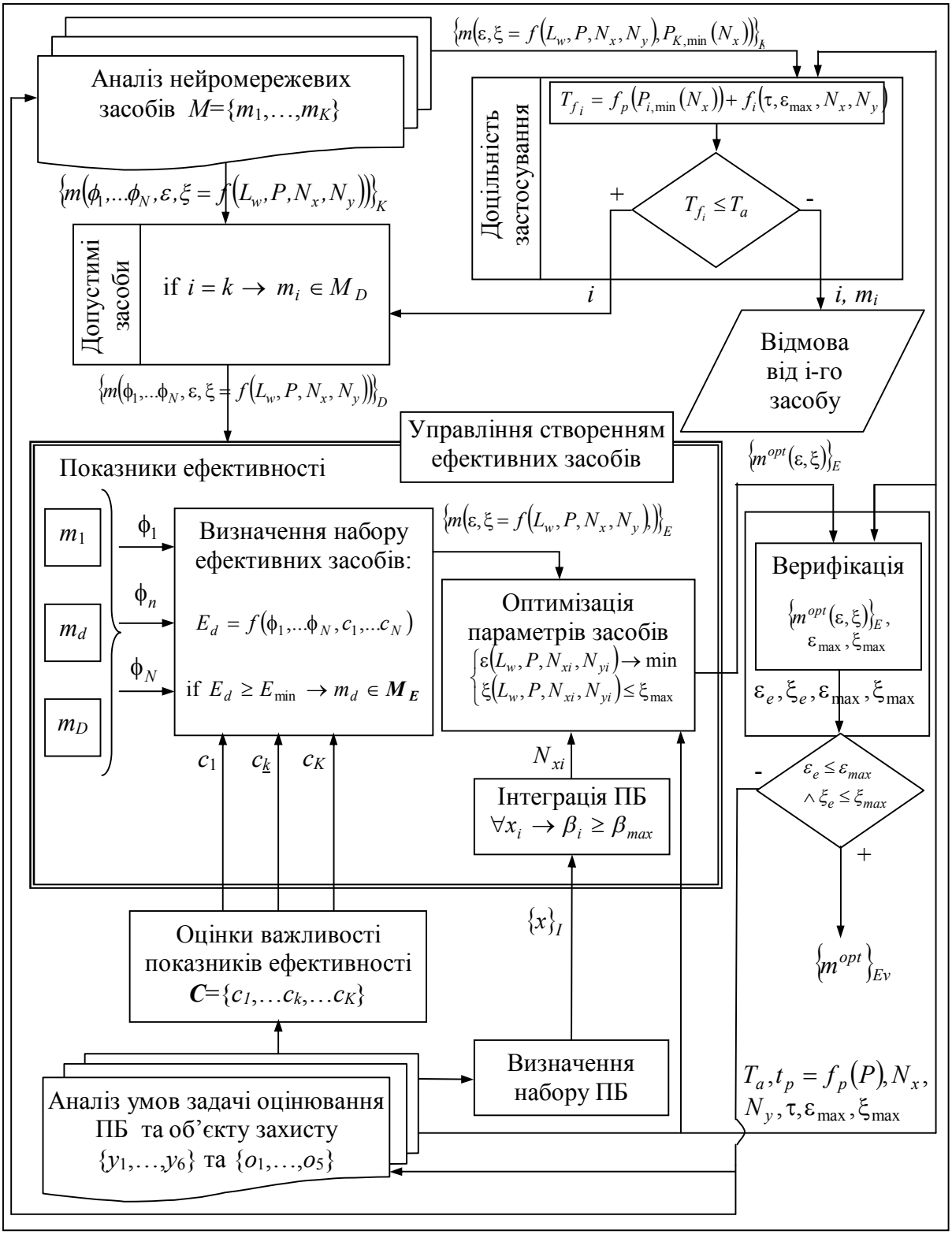


Рис. 7. Схема відображення моделі процесу створення ефективних нейромережевих засобів оцінки параметрів безпеки

Множина ефективних НМЗ визначається на основі розроблених критеріїв оцінки ефективності. Параметри $\{m\}_E$ оптимізуються з точки зору мінімізації помилки навчання – $\varepsilon(L_w, P, N_{xi}, N_{yi}) \to \min$, при обмеженні на кількість навчальних операції – $\xi(L_w, P, N_{xi}, N_{yi}) \le \xi_{\max}$. Результатом оптимізації є $\left\{m^{opt}(\varepsilon,\xi)\right\}_E$, де ε,ξ – величини похибки навчання та кількість навчальних ітерацій для визначеного набору ефективних НМЗ з оптимізованими параметрами. Вказана множина передається до модулю «Верифікації», де на основі порівняння кожного із її компонентів з $\varepsilon_{\max}$ та $\xi_{\max}$ приймається рішення про можливість використання.

На відміну від відомих, в описаній моделі передбачено: процес інтеграції ПБ на основі експертних даних, визначення принципової доцільності застосування НМЗ, оптимізацію виду та параметрів НМЗ.

Четвертий розділ присвячено розробці методів побудови НМЗ оцінювання ПБ ІС. *Розроблено метод подання експертних знань в НМЗ оцінки ПБ.* В методі використано підхід для визначення статистично подібних кібератак, модель процесу інтеграції ПБ ІС, MPNN та модель створення ефективних НМЗ оцінки ПБ. Вхідними даними методу є $\boldsymbol{O} = \{o_1, ...o_5\}$. Реалізація методу полягає у виконанні наступних етапів:

Етап 1 – формування множини можливих кібератак. Етап передбачає аналіз множини $\boldsymbol{O}$, в результаті якого визначається множина кібератак, котру повинна розпізнавати НМ – $\boldsymbol{Ka} = \{Ka_1, Ka_2, ..., Ka_J\}$, де *J*– кількість кібератак.

Етап 2 – визначення ПБ для розпізнавання довільної кібератаки. На цьому етапі, використовуючи розроблену модель інтеграції ПБ, для кожної Ka_j визначається множина ПБ, котрі будуть використані як вхідні параметри НМЗ оцінювання – $Ka_j \to \{X_j\}_{N_j}$, де N_j – кількість ПБ, що використовуються для розпізнавання *j*-ої кібератаки.

Етап 3 – визначення подібних кібератак. Етап орієнтований на виділення із $\boldsymbol{Ka}$ подібних між собою кібератак: $\left\{\boldsymbol{Ka}_1^{(p)}, ..., \boldsymbol{Ka}_J^{(p)}\right\}, \forall \boldsymbol{Ka}_1^{(p)} \subset \boldsymbol{Ka}, ..., \boldsymbol{Ka}_J^{(p)} \subset \boldsymbol{Ka}$, $\boldsymbol{Ka}_1^{(p)} \cup \boldsymbol{Ka}_2^{(p)} ... \cup \boldsymbol{Ka}_J^{(p)} = \boldsymbol{Ka}$, де $\boldsymbol{Ka}_i^{(p)}$– *i*-та множина подібних кібератак. Відповідно розробленого підходу, подібність довільної *k*-ої та *j*-ої кібератак визначається кортежем: $\left\langle T_{(k,j)}(Ka_k, Ka_j), R_{(k,j)}\left(\{X_k\}_{N_k}, \{X_j\}_{N_j}\right)\right\rangle$, де $T_{(k,j)}(Ka_k, Ka_j)$ – функція подібності типу *k*-ої та *j*-ої кібератак, а $R_{(k,j)}\left(\{X_k\}_{N_k}, \{X_j\}_{N_j}\right)$ – функція подібності множин ПБ, що використовуються для розпізнавання *k*-ої та *j*-ої кібератак. Етап виконується за п’ять кроків: визначення типу кібератак, розрахунок функції подібності типу кібератак, визначення множини

спільних ПБ, розрахунок коефіцієнту подібності множин ПБ, визначення подібності кібератак.

Етап 4 – визначення ПБ для розпізнавання подібних кібератак. Етап орієнтований на визначення множини ПБ, що використовуються в якості вхідних параметрів НМ для розпізнавання подібних кібератак: $\{\boldsymbol{X}_1^{(p)},...,\boldsymbol{X}_J^{(p)}\}$, де $\boldsymbol{X}_j^{(p)}$ – множина ПБ, відповідних *j*-ій множині подібних кібератак $\boldsymbol{Ka}_j^{(p)} = \{Ka_{1,j},...,Ka_{M_j,j}\}$, M_j – кількість елементів $\boldsymbol{Ka}_j^{(p)}$. Використовується вираз $\boldsymbol{X}_j^{(p)} = \boldsymbol{X}_{1,j} \cup ... \boldsymbol{X}_{M,j}$, 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 можливо розробити продукційні правила розпізнавання. Якщо для деякої *j*-ої множини $\boldsymbol{Ka}_j^{(p)} \in \boldsymbol{Ka}$ отримати представницькі експертні дані для розробки продукційних правил на основі аналізу $\boldsymbol{X}_j^{(p)}$ достатньо складно, то $\boldsymbol{Ka}_j^{(p)} \not\subset \overline{\boldsymbol{Ka}}^{(p)}$. В протилежному випадку $\boldsymbol{Ka}_j^{(p)} \subset \overline{\boldsymbol{Ka}}^{(p)}$.

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: $\boldsymbol{Net} = \{net_1, net_2, ...net_M\}$, де net_j – *j*-та НМ, призначена для розпізнавання *j*-ої множини подібних кібератак $\boldsymbol{Ka}_j^{(p)}$.

Етап 7 – розробка структури вхідного шару. В результаті виконання даного етапу для кожної $net_j \in \boldsymbol{Net}$ визначається кількість нейронів у ВШ MPNN. Використовується вираз $N_{x,j} = N_j^{\max}$. Також встановлюється відповідність між *i*-им входом НМ та *i*-им 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 основі експертних даних розроблюється множина продукційних правил їх розпізнавання $\boldsymbol{Pr}_j = \{pr_{1,j},...pr_{L_j,j}\}$, де $pr_{i,j}$ – *i*-те продукційне правило для розпізнавання $Ka_{i,j} \in \boldsymbol{Ka}_j^{(p)}$, L_j – кількість продукційних правил для розпізнавання множини $\boldsymbol{Ka}_j^{(p)}$. Правила задані виразами виду $x_1 \in \left[x_1^{\min}, x_1^{\max}\right] \wedge ... x_{N^{\max}} \in \left[x_{N^{\max}}^{\min}, x_{N^{\max}}^{\max}\right] \to Ka_{i,j}$, 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 – розробка ШД. На цьому етапі для кожної $net_j \in \boldsymbol{Net}$ в ШД визначається стільки нейронів, скільки подібних кібератак повинна

розпізнавати НМ: $N_{\text{ШД},j} = M_j$. Також встановлюється відповідність між кожним *n*-им нейроном ШД та *n*-ою кібератакою: $n_{\text{ШД},j} \to Ka_{n,j}$.

Етап 10 – визначення структури ШО та ШФ. Для кожної $net_j \in \boldsymbol{Net}$ виконання етапу являється пристосуванням структури ШО та ШФ MPNN до заданих продукційних правил $\langle \boldsymbol{N}_{\text{ШФ}}, \boldsymbol{N}_{\text{ШО}}, \boldsymbol{L}_{\text{ШФ}}, \boldsymbol{L}_{\text{ШО}}, \boldsymbol{L}_{\text{ШД}} \rangle = f(Pr_j)$, де $\boldsymbol{N}_{\text{ШФ}}, \boldsymbol{N}_{\text{ШО}}$ – множина нейронів ШФ та ШО, $\boldsymbol{L}_{\text{ШФ}}, \boldsymbol{L}_{\text{ШО}}, \boldsymbol{L}_{\text{ШД}}$ – множина вхідних зв'язків ШФ, ШО та ШД. Визначення кожного продукційного правила виконується за п'ять кроків: визначення нейрону ШО, модифікація вхідних зв'язків ШД, визначення нейронів ШФ, модифікація зв'язків вхідних ШО та модифікація вхідних зв'язків ШФ.

Етап 11 – верифікація розроблених MPNN. Верифікація кожної $net_j \in \boldsymbol{Net}$ полягає у порівнянні похибки розпізнавання (ε_j) та обчислювальної складності (ξ_j) з максимально допустимими значеннями цих параметрів ($\varepsilon_{\max}, \xi_{\max}$). ε_j та ξ_j розраховуються на прикладах тестової вибірки. Якщо для всіх прикладів тестової вибірки $\varepsilon_j \le \varepsilon_{\max} \wedge \xi_j \le \xi_{\max}$, то net_j придатна для практичного використання.

Метод використано для розробки MPNN, призначеної для розпізнавання кібератак класу U2R, з метою несанкціонованого підвищення привілеїв користувачів. Розроблена НММ показала абсолютну точність розпізнавання кібератак класу U2R, сигнатури яких представлені в базі даних (БД) KDD-99, що в 5 разів перевищує результати інших відомих НММ.

Розроблено метод визначення часових характеристик використання нейромережевих засобів. В результаті реалізації методу формується множина НМЗ, які доцільно використовувати для оцінки ПБ з метою розпізнавання кібератак. Метод апробовано на кібератаках, представлених в БД KDD-99. Доведено доцільність НМЗ для розпізнавання НК типу СП, Neptune, Smurf і недоцільність – для виявлення НК типу phf та multihop. Також доведена можливість розпізнавання веб-орієнтованого скриптового ШПЗ.

Сформовано метод розробки шаблонів поведінки параметрів безпеки. Розробка базується на створених ММ ШП і складається із наступних етапів:

Етап 1 – вирівняння ряду. Етап орієнтований на розрахунок вирівнянного ряду $\hat{X}(t) = X'(t) - Y(t) - \overline{X}$, $t \in [0, T]$, де $X'(t)$ – ряд даних, $Y(t)$ – тренд, а $\overline{X}$ – середнє значення ряду.

– розрахунок параметрів ЛМ. На етапі розраховуються параметри ЛМ, призначених для моделювання складових періодичного ряду: $\left\langle \{AB\}_K, \{BA\}_K, \left\{ \left| p^{(AB)} \right| \right\}_K, \left\{ \left| p^{(BA)} \right| \right\}_K \right\rangle$, де $\{AB\}_K, \{BA\}_K$ – множини розроблених стаціонарних інтервалів для значимих періодів, *K* – кількість

періодів, $\left\{ \left| p^{(AB)} \right| \right\}_K, \left\{ \left| p^{(BA)} \right| \right\}_K$ – множини перехідних ймовірностей для кожного із ЛМ. Структурна схема розрахунку параметрів ЛМ показана на рис.8. Не враховуючи процедури вводу та виводу даних, розрахунок реалізується за чотири кроки, що відповідають 3-7 вершинам структурної схеми: розрахунок періодичних складових, визначення значимих періодів, визначення нестаціонарних точок, розрахунок ймовірностей переходів.

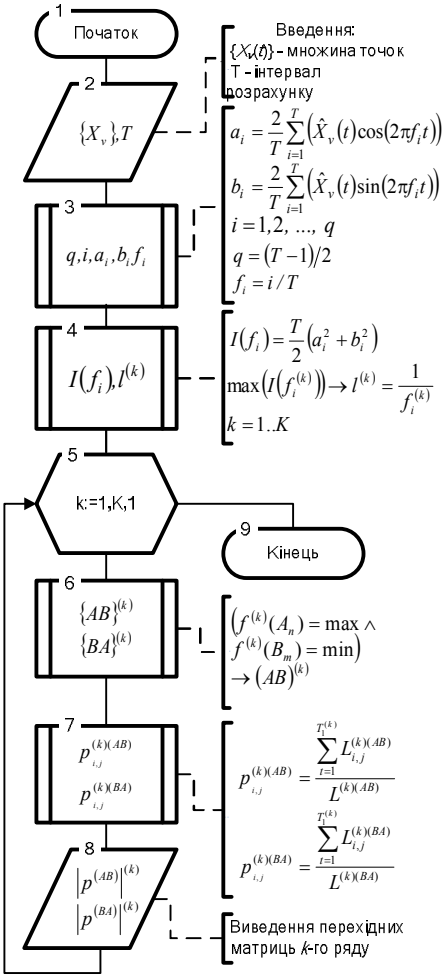


Рис. 8. Схема розрахунку параметрів ЛМ

Етап 2 – <u>розрахунок ймовірностей станів ЛМ</u>. На даному етапі для кожного *k*-го ЛМ розраховують ймовірність *i*-го стану в довільний момент часу ($P_i^{(k)}(t)$). Для цього матриці ймовірностей переходів $\left| p^{(AB)} \right|$ та $\left| p^{(BA)} \right|$ підставляються в систему рівнянь Колмогорова-Чепмена.

Етап 3 – <u>розрахунок ймовірностей станів ММ</u>. На даному етапі для ММ розраховують ймовірність кожного із станів. Використовують вираз $P_i(t) = \frac{1}{K} \sum_{k=1}^{K} P_i^{(k)}(t)$, де $P_i(t)$ – ймовірність *i*-го стану марківської моделі, $P_i^{(k)}(t)$ – ймовірність *i*-го стану для *k*-го ЛМ в момент часу *t*.

Етап 4 – <u>розрахунок поведінки.</u> На цьому етапі для заданого *t* розраховується очікуване значення ПБ: $\hat{X}(t) = M(t) + Y(t) + \overline{X}$, де $M(t)$ – математичне очікування ПБ, розраховане за допомогою ММ.

Створено метод визначення ефективності розробки НМЗ оцінювання ПБ. Вхідними даними методу є $\langle \boldsymbol{У}, \boldsymbol{О}, \boldsymbol{М}, D_{\min} \rangle$, де $\boldsymbol{У} = \{y_1, ..., y_6\}$ – умови задачі оцінювання ПБ, $\boldsymbol{О} = \{o_1, ..., o_5\}$ – характеристики об'єкту захисту, $\boldsymbol{М} = \{m_1, ..., m_{N_m}\}$ – доступні НМЗ, N_m – кількість доступних НМЗ, $D_{\min}$ – мінімально допустима величина інтегральної ефективності. Метод виконується за п'ять етапів:

Етап 1 – <u>визначення параметрів оцінки ефективності</u>. На цьому етапі для кожного $m_n \in \boldsymbol{М}$ за допомогою експертних даних визначаються величини параметрів оцінки ефективності, розроблених в результаті аналізу НМЗ.

Етап 2 – визначення напрямків вдосконалення НМЗ. На цьому етапі проводиться аналіз величин $d_i \in \boldsymbol{D}, i = 1,2..,9$. Якщо величина деякого *i*-го параметру $d_i < 1$, то це вказує на можливість вдосконалення НММ у відповідному напрямку.

Етап 3 – визначення вагових коефіцієнтів параметрів ефективності. Етап спрямований на аналіз $\boldsymbol{У}$ та $\boldsymbol{О}$ для визначення вагових коефіцієнтів критеріїв ефективності. В результаті аналізу формується множина величин коефіцієнтів $\{\alpha\}$, елементи якої відповідають елементам $\boldsymbol{D}$.

Етап 4 – розрахунок інтегральної ефективності. На цьому етапі за допомогою виразу $D^{\Sigma} = 2^{\sum_{i=1}^{9} \alpha_i d_i}$ розраховується інтегральний показник ефективності НММ.

Етап 5 – оцінка інтегральної ефективності. На даному етапі проводиться остаточне оцінювання ефективності НМЗ. Для цього розрахована величина D^{Σ} порівнюється із мінімально допустимою величиною $D_{\min}$. Якщо $D^{\Sigma} < D_{\min}$, то такий НМЗ може використовуватись тільки після виправлення недоліків, визначених на етапі 2. НМЗ, у якого показник D^{Σ} більший, вважається більш ефективним.

Таким чином, вперше створено метод, котрий дозволяє розрахувати інтегральну ефективність розробки НМЗ оцінки. За допомогою даного методу визначено, що типовими недоліками більшості НМЗ є низька пристосованість до використання всієї множини НММ, неможливість використання експертних даних, недостатнє обґрунтування доцільності використання НММ та вибору оптимального виду НММ.

П'ятий розділ присвячено розробці нейромережевих систем оцінювання параметрів безпеки.

Розроблено комплексну методологію нейромережевого оцінювання параметрів безпеки для розпізнавання кібератак. Вхідними даними методології є $\langle \boldsymbol{У}, \boldsymbol{О}, \boldsymbol{М} \rangle$. Також в методології використовуються експертні дані: $\langle \boldsymbol{C}_1, \boldsymbol{C}_2, ..., \boldsymbol{C}_K \rangle$ – вагові коефіцієнти ПБ, $\boldsymbol{C}_k = \{c_{1,1,1}, ...c_{i,j,m}, ...c_{N_p, N_p, M_e}\}$ –експертні оцінки парних порівнянь вагомості *i*-го та *j*-го ПБ для розпізнавання *k*-ої кібератаки, M_e – кількість експертів, $\boldsymbol{B} = \{\beta_1, ...\beta_K\}$ – мінімальні значення коефіцієнтів вагомості ПБ, R_{max} – максимальна приведена різниця номенклатур ПБ, $\boldsymbol{E}$ – критерії оптимізації виду НММ, $\boldsymbol{V}$ – вагові коефіцієнти критеріїв оптимізації виду НММ, k_E – коефіцієнт відхилення, $\boldsymbol{\Lambda} = \{\lambda_1, \lambda_2, ...\}$ – оптимізуємі параметри НММ, $\varepsilon_{\max}$ – максимально допустима помилка розпізнавання НМ, $\xi_{\max}$ – максимально допустима обчислювальна складність НМ, T_a – допустимий термін створення НМЗ, $\boldsymbol{D}$ – критерії оцінки ефективності НМЗ, $D_{\min}$ – мінімально допустима ефективність НМЗ, $\boldsymbol{A}$ – коефіцієнти важливості елементів $\boldsymbol{D}$. Результатом методології є визначення параметрів найбільш ефективних НМЗ. Методологя розділена на дев'ять етапів (рис. 9):

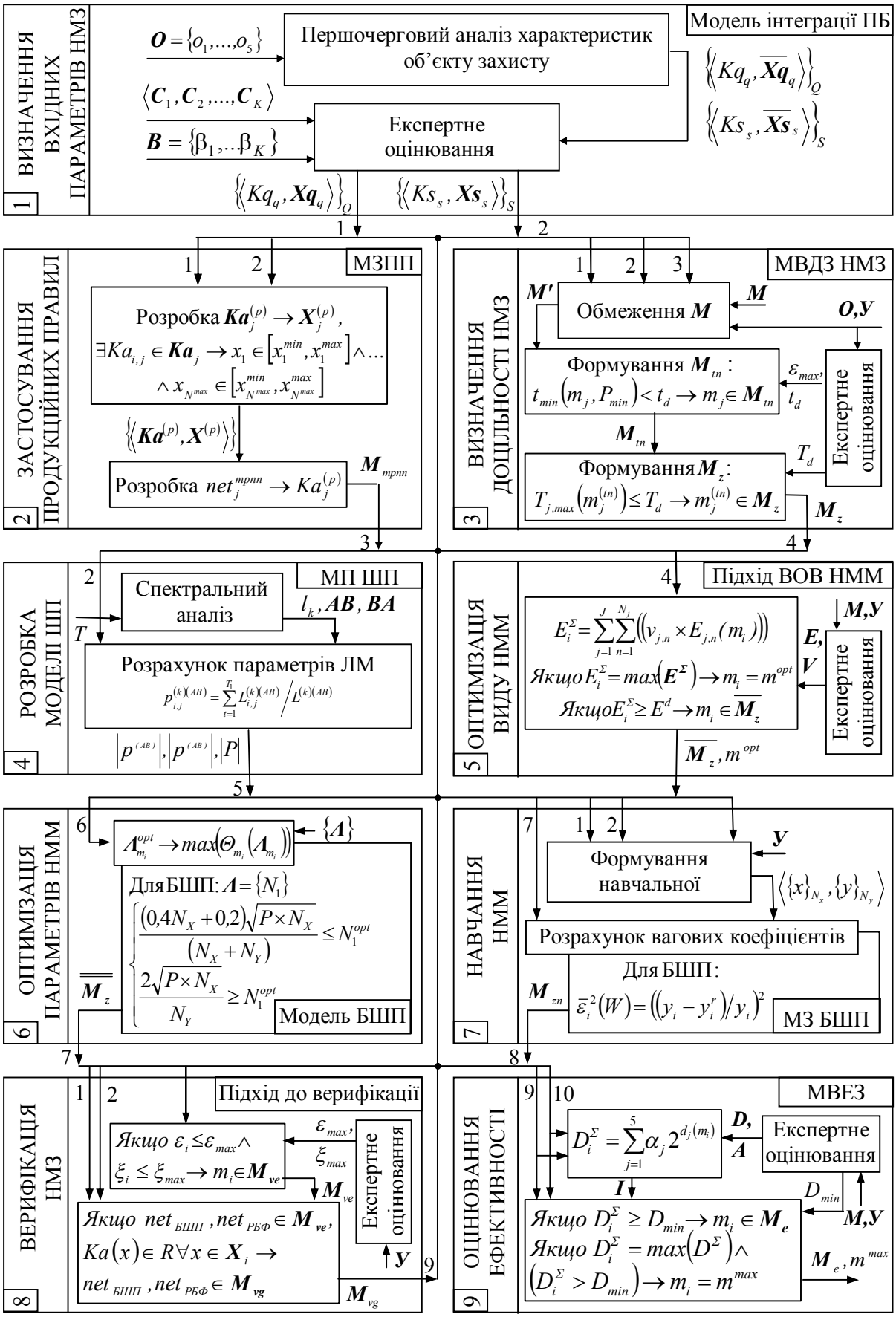


Рис. 9. Схема комплексної методології нейромережевої оцінки ПБ

Етап 1 – визначення вхідних параметрів НМЗ. Виконання етапу полягає у застосуванні моделі інтеграції ПБ для визначення множин ПК $\boldsymbol{Ks}$ і НК $\boldsymbol{Kq}$ та відповідних їм множин ПБ $\boldsymbol{Xq}$ і $\boldsymbol{Xs}$, що використовуються як вхідні параметри НМЗ. Вихідною інформацією етапу є $Ka_k \to \boldsymbol{X}_k$.

Етап 2 – застосування продукційних правил. Призначенням даного етапу є навчання НММ оцінки ПБ за рахунок подання в них експертних знань про відповідність величин ПБ з наявністю/відсутністю очікуваних кібератак. Вхідними даними етапу являються $\left\{\left\langle Kq_q, \boldsymbol{Xq}_q \right\rangle\right\}_Q$ та $\left\{\left\langle Ks_s, \boldsymbol{Xs}_s \right\rangle\right\}_S$. В базовому варіанті подання експертних знань реалізується за допомогою розробленого методу застосування продукційних правил для навчання НМ типу MPNN. Етап виконується за 2 кроки. Крок 1 відповідає 3,4 етапу, а крок 2 – 5-10 етапам методу застосування продукційних правил. Вихідною інформацією етапу є $\boldsymbol{M}_{mpnn} = \left\{net_1^{mpnn}, ..., net_{M_{mpnn}}^{mpnn}\right\}$, де net_j^{mpnn} – j-та MPNN, призначена для розпізнавання $\boldsymbol{Ka}_j^{(p)} \in \overline{\boldsymbol{Ka}}^{(p)}$.

Етап 3 – визначення доцільності застосування НМЗ. На даному етапі визначається множина НМЗ $\boldsymbol{M}_z$, які доцільно застосувати для оцінки інтегрованих ПБ. Для формування $\boldsymbol{M}_z$ використовується правило: Якщо $T_{j,\max} \le T_d \to m_j \in \boldsymbol{M}_z$, де $m_j \in \boldsymbol{M}_{tn}$ – j-та НММ з допустимим терміном навчання, $T_{j,\max}$ – тривалість формування навчальної вибірки для j-ої НММ, T_d – допустимий термін формування навчальної вибірки з мінімальною кількістю начальних прикладів. Етап реалізується за рахунок виконання 2-12 етапів методу визначення доцільності застосування НМЗ.

Етап 4 – розробка моделі шаблону поведінки. Етап орієнтовано на розробку запропонованої ММ ШП. Вхідними даними етапу є множина параметрів ПБ $\boldsymbol{Xs}$, що залежать від терміну експлуатації і використовуються для розпізнавання ПК. Розробка ММ реалізується за допомогою створеного методу і полягає в розрахунку множин перехідних матриць $\boldsymbol{p}^{(AB)}$, $\boldsymbol{p}^{(BA)}$ та матриці ймовірностей $\left|P(t)\right|$.

Етап 5 – оптимізація виду НММ. На даному етапі визначається $\overline{\boldsymbol{M}_z}$ –множина оптимальних видів НММ. Етап базується на розробленому підході до оптимізації та виконується за три кроки: розрахунку $\boldsymbol{E}^{\Sigma} = \left\{E_1^{\Sigma}, ..., E_{N_m}^{\Sigma}\right\}$ – інтегральних критеріїв оптимізації, визначення оптимального виду НММ та формування $\overline{\boldsymbol{M}_z} = \left\{m_1^{\text{opt}}, ..., m_I^{\text{opt}}\right\}$ – множини оптимальних видів НММ.

Етап 6 – оптимізація параметрів НММ. Етап орієнтовано на визначення $\overline{\overline{\boldsymbol{M}_z}}$ – множини оптимальних видів НММ з оптимізованими параметрами. Використано критерій оптимізації виду: $\Theta(\Lambda) \to \max$, де Θ – обчислювальна потужність моделі. Оптимізація проводиться методами, специфічними для виду НММ. Для БШП застосовується розроблена модель.

Етап 7 – 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: формування навчальної вибірки та реалізації процесу навчаня.

Етап 8 – верифікація НМЗ. Етап орієнтовано на верифікацію НМЗ. Для кожної $Ka_i \in \boldsymbol{Ka}$ даний етап реалізується за два кроки: визначення достатньої обчислювальної потужності та доведення гладкості функції, що апроксимується. Вихідною інформацією етапу є $\boldsymbol{M}_{ve}$ – множина НМЗ верифікованих експериментально та $\boldsymbol{M}_{vg}$ – множина гарантовано верифікованих НМЗ.

Етап 9 – оцінка ефективності НМЗ. Призначенням етапу є розробка множини ефективних НМЗ та визначення шляхів їх можливого вдосконалення. Для цього використовується розроблений метод оцінювання ефективності. Виходом етапу є $\boldsymbol{M}_e$ – множина ефективних НМЗ та $m^{\max}$ – найбільш ефективний НМЗ.

Показано, що використання даної методології дозволяє до 4 разів підвищити інтегральний показник ефективності розробки НМЗ.

За допомогою запропонованої комплексної методології розроблено *структуру нейромережевої системи оцінки параметрів безпеки* (НСОПБ) для розпізнавання кібератак на ресурси Інтернет-орієнтованих ІС. До складу НСОПБ входять (рис. 10): підсистема первинного визначення параметрів кібератак (ППВПК), призначена для формування множини очікуваних видів кібератак, попереднього визначення переліку ПБ та формування навчальної вибірки НММ; підсистема експертної оцінки параметрів НМЗ (ПЕОП), в якій на основі експертних даних для кожного виду кібератак формуються відповідні множини ПБ, розроблюються продукційні правила для розпізнавання кібератак, визначаються обмеження та критерії ефективності НММ; підсистема розробки нейромережевих моделей (ПРНММ), що призначена для визначення параметрів НММ, їх верифікації та оцінки ефективності; підсистема розпізнавання та сигналізації (ПРС), в якій реалізується застосування розроблених НММ для розпізнавання кібератак та виробляється інформація для адміністратора системи; модуль управління системою (МУС), що служить для переведення системи в режими ініціалізації налаштувань (РІН), навчання НММ (РН), розпізнавання кібератак (РРК) та зупинки (РЗ). У свою чергу, ППВПК складається з модулів визначення очікуваних кібератак (МВОК), попереднього визначення параметрів безпеки (МПВПБ), класифікації параметрів кібератак (МКПК), формування статистично подібних кібератак (МФСПК), накопичення статистичних даних (МНСД), розробки марківської моделі ШП (МРММ), формування навчальної вибірки НММ (МФНВ).

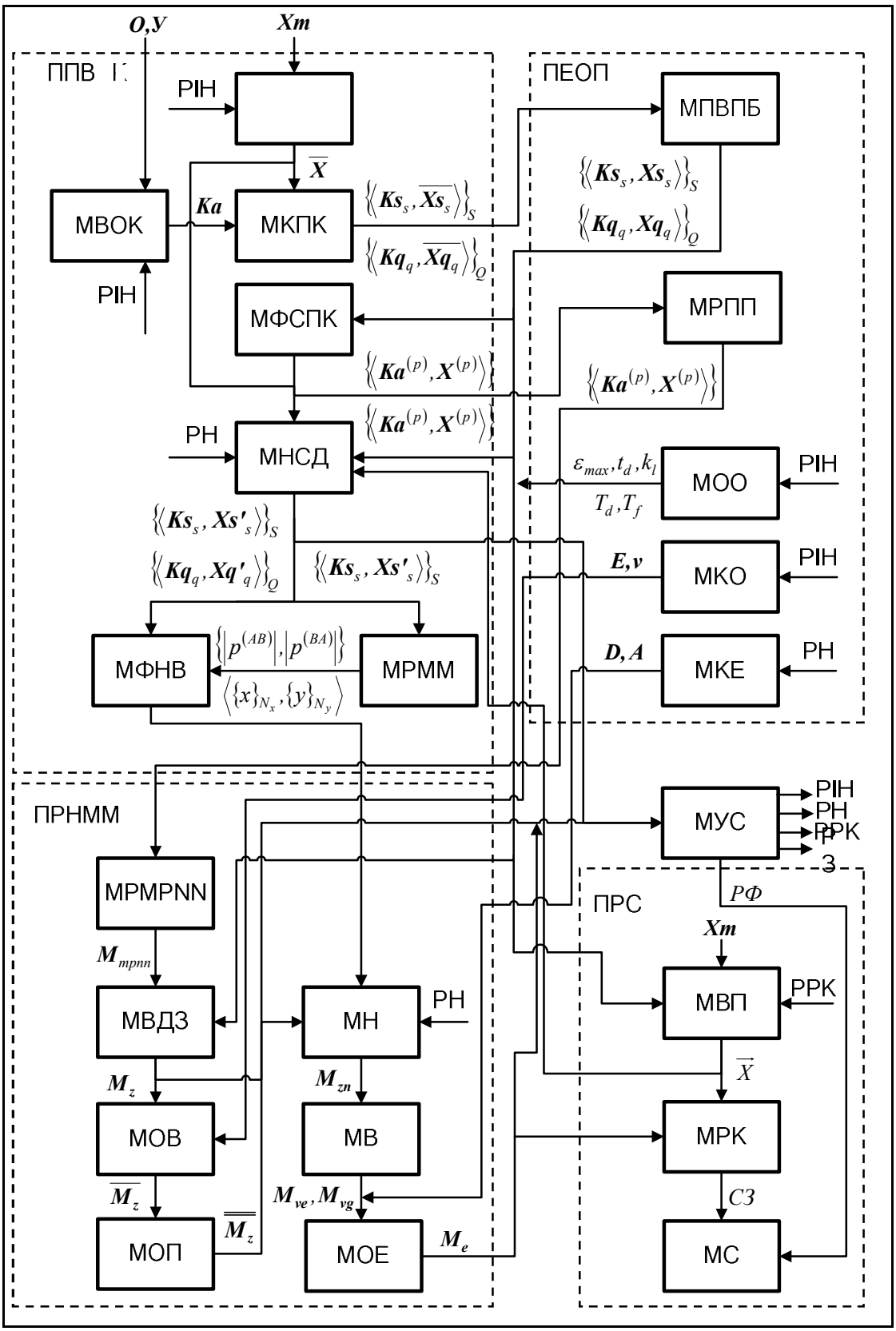


Рис. 10. Структура нейромережевої системи оцінки параметрів безпеки

До складу ПЕОП входять модулі інтеграції ПБ (МІПБ), обчислювальних обмежень НМЗ (МОО), критеріїв оптимізації НММ (МКО), критеріїв ефективності (МКЕ), розробки продукційних правил (МРПП). ПРНММ складається з модулю розробки MPNN (MPMPNN), визначення доцільності застосування НМЗ (МВДЗ), оптимізації виду НММ

(МОВ), оптимізації параметрів НММ (МОП), навчання (МН), верифікації НММ (МВ) та оцінювання ефективності (МОЕ). ПРС складається із модулів сигналізації (МС), розпізнавання кібератак (МРК) та вхідних параметрів НМЗ (МВП). НСОПБ починає функціонувати в РІН. Відповідно моделі інтеграції ПБ, на основі характеристик обраного об'єкту (***О***) захисту та умов задачі захисту (***У***) в МВОК ППВПК формується множина очікуваних кібератак ***Ka***, а в МПВПБ на основі хостових та мережевих параметрів ***Xm*** визначається множина ПБ $\overline{\boldsymbol{X}}$, що може використовуватись для розпізнавання ***Ka***. ***Ka*** та $\overline{\boldsymbol{X}}$ поступають в МКПК, в якому кібератаки класифікуються на поступові ***Ks*** і неочікувані ***Kq*** та визначаються множини ПБ $\overline{\boldsymbol{Xs}}$ та $\overline{\boldsymbol{Xq}}$. $\left\{\left\langle \boldsymbol{Ks}_s, \overline{\boldsymbol{Xs}_s}\right\rangle\right\}_S$ та $\left\{\left\langle \boldsymbol{Kq}_q, \overline{\boldsymbol{Xq}_q}\right\rangle\right\}_Q$ подаються в МІПБ ПЕОП, де за допомогою експертного оцінювання формуються портрети ПК та НК: $\left\{\left\langle \boldsymbol{Ks}_s, \boldsymbol{Xs}_s\right\rangle\right\}_S$, $\left\{\left\langle \boldsymbol{Kq}_q, \boldsymbol{Xq}_q\right\rangle\right\}_Q$. Паралельно з МІПБ в ПЕОП спрацьовують МОО, МКО та МКЕ. Результатом спрацювання являються: допустима помилка розпізнавання НММ ($\varepsilon_{\max}$), допустима кількість навчальних обчислювальних ітерацій ($\xi_{\max}$), допустимий термін навчання (t_d), коефіцієнт обсягу статистичних даних (k_l), допустимий термін розробки НММ (T_f), термін формування навчальної вибірки (T_d), множини критеріїв оптимізації виду НММ (***E***), коефіцієнтів значимості критеріїв оптимізації (***v***), показників ефективності НМЗ (***D***) та значимості показників ефективності (***A***).Отримані портрети кібератак поступають в МФСПК, в якому формуються множини подібних кібератак та відповідних їм ПБ $\left\{\left\langle \boldsymbol{Ka}^{(p)}, \boldsymbol{X}^{(p)}\right\rangle\right\}$. $\left\{\left\langle \boldsymbol{Ka}^{(p)}, \boldsymbol{X}^{(p)}\right\rangle\right\}$ подаються в МРПП, в якому на основі експертних даних для кожної множини подібних кібератак створюються множини продукційних правил – $\left\{\left\langle \boldsymbol{Ka}^{(p)}, \boldsymbol{R}\left(\boldsymbol{X}^{(p)}\right)\right\rangle\right\}$.

Множина $\left\{\left\langle \boldsymbol{Ka}^{(p)}, \boldsymbol{R}\left(\boldsymbol{X}^{(p)}\right)\right\rangle\right\}$ передається в MPMPNN, в якому на основі запропонованого методу застосування продукційних правил для кожної множини статистично подібних кібератак розроблюється MPNN. Отримана множина $\boldsymbol{M}_{mpnn}$ разом з $\left\{\left\langle \boldsymbol{Ks}_s, \boldsymbol{Xs}_s\right\rangle\right\}_S$, $\left\{\left\langle \boldsymbol{Kq}_q, \boldsymbol{Xq}_q\right\rangle\right\}_Q$, $\varepsilon_{\max}$, t_d, T_d та T_f подається в МВДЗ, в якому за допомогою розробленого методу формується $\boldsymbol{M}_z$ – множина НММ, які доцільно використовувати для розпізнавання ***Ka***. Якщо $\boldsymbol{M}_z = \varnothing$, то ця інформація передається в МУС, який за допомогою МС ПРС надає адміністратору НСОПБ сигнал про недоцільність застосування НМЗ та переводить НСОПБ в РЗ. Якщо $\boldsymbol{M}_z \neq \varnothing$, то спрацьовує МОВ, в якому за допомогою розробленого підходу до визначення оптимального виду НММ, на основі $\boldsymbol{M}_z$, ***E*** та ***v***

відбувається визначення множини оптимальних видів НММ ($\overline{\boldsymbol{M}_z}$). Подальша оптимізація параметрів НММ, що входять до складу $\overline{\boldsymbol{M}_z}$, відбувається в МОП. Оптимізація параметрів БШП відбувається за допомогою розробленої моделі. Виходом МОП являється множина оптимальних видів НММ з оптимізованими параметрами $\overline{\overline{\boldsymbol{M}_z}}$. Після спрацювання МОП НСОПБ переходить в РН. Спрацьовує МНСД ППВПК, за допомогою якого відбувається накопичення статистичних даних щодо ПБ. Вихідними даними МНСД є $\left\{\left\langle \boldsymbol{Ks}_s, \boldsymbol{Xs'}_s \right\rangle\right\}_S$ та $\left\{\left\langle \boldsymbol{Kq}_q, \boldsymbol{Xq'}_q \right\rangle\right\}_Q$. $\left\{\left\langle \boldsymbol{Ks}_s, \boldsymbol{Xs'}_s \right\rangle\right\}_S$ передається в МРММ, де за допомогою розробленого методу проектування ШП визначаються $\hat{X}(t)$ – очікувані значення ПБ на протязі заданого терміну функціонування. $\left\{\left\langle \boldsymbol{Ks}_s, \boldsymbol{Xs'}_s \right\rangle\right\}_S$, $\left\{\left\langle \boldsymbol{Kq}_q, \boldsymbol{Xq'}_q \right\rangle\right\}_Q$ та $\hat{X}(t)$ подаються в МФНВ, в якому формуються $\left\langle \{x\}_{N_x}, \{y\}_{N_y} \right\rangle$ – кортежі множин вхідних та вихідних параметрів, що використовуються в МН. Виходом МН є $\boldsymbol{M}_{zn}$, елементи якої за допомогою розробленого підходу проходять верифікацію в МВ. Виходом МВ є $\boldsymbol{M}_{ve}$ та $\boldsymbol{M}_{vg} \subset \boldsymbol{M}_{ve}$, котрі передаються в МОЕ. МОЕ функціонує на основі методу визначення ефективності застосування НМЗ. Результатом його спрацювання є $\boldsymbol{M}_e$ – множина параметрів ефективних НММ та $\boldsymbol{m}^{\max}$ – параметри найбільш ефективної НММ, які передаються в МРК ПРС і НСОПБ переходить в РРК.

У режимі РРК контрольовані ПБ подаються на вхід МПВП ПРС, в якому формується $\vec{X}$ – вектор ПБ, які оцінюються НМЗ. $\vec{X}$ надходить в МРК ПРС, де на його основі формується сигнал *СЗ* про стан захисту та в МНСД ППВПК для подальшого накопичення. *СЗ* за допомогою МС передається адміністратору НСОПБ. Якщо поточний обсяг накопичених статистичних даних МНСД в k_l разів перевищує обсяг даних останнього навчання НММ, то НСОПБ може бути переведена в РН для уточнення параметрів НММ.

НСОПБ адаптована для вирішення множини актуальних задач оцінювання ПБ. В результаті розроблені НМС розпізнавання веб-орієнтованого ШПЗ, спаму та витоків текстової інформації (РШПЗСВ) та НМС розпізнавання мережевих кібератак (РМК). Проміжні результати розробки наведені в розділах 3, 4 в якості прикладів застосування розроблених методів та моделей. Використані в цих НМС ПБ наведені в табл. 2.

Зазначимо, що небезпечними функціями JavaScript, VBScript та API Windows є ті функції, за допомогою яких ШПЗ саморозповсюджується та виконує деструктивні дії. Приклади навчальних даних НММ, призначених для розпізнавання ШПЗ, написаного на JavaScript, та витоків текстової інформації наведені в табл. 3, 4.

Таблиця 2

Параметри безпеки НМС

НМС	Тип кібератаки	Використані ПБ
РШПЗСВ	Т1 – ШПЗ написане на JavaScript	Небезпечні функції JavaScript
	Т2 – ШПЗ написане на VBScript	Небезпечні функції VBScript
	Т3 – поведінка ШПЗ	Небезпечні функції API Windows
	Т4 – спам	Частоти зустрічі в тексті інформативних слів
	Т5 – витік	
РМК	Т6 –мережева кібератака класу U2R	Параметри мережевих з'єднань
	Т7 – шторм запитів	Кількість запитів за 1 с., термін отримання запитів

Таблиця 3

Навчальні дані ДШП при розпізнаванні ШПЗ, написаного на JavaScript

Номер прикладу	Вихідний сигнал Y	Вхідні параметри													
		eval	function	script	iframe	location	File	FileReader	FileList	Blob	cookie	javaEnabled	plugins	unescape	escape
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	-1	-1	1	1	1	1	-1	-1	1	-1
3	1	1	1	1	1	-1	-1	1	1	1	1	-1	-1	1	-1
4	1	1	1	1	1	-1	-1	1	1	-1	-1	-1	-1	-1	1
5	1	1	1	1	1	-1	-1	1	1	-1	-1	1	-1	1	1
6	-1	1	-1	-1	-1	1	-1	-1	-1	-1	-1	-1	-1	-1	-1
7	-1	1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	1	-1
8	-1	-1	1	-1	-1	1	-1	-1	-1	1	-1	-1	1	-1	-1
9	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	1
10	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	-1	1	-1	-1	-1	-1

Таблиця 4

Навчальні дані ТК при розпізнаванні витоків текстової інформації

Номер прикладу	Вхідні параметри			
	Відносна кількість інформативних слів	СТАЖ	ОСВІТА	НАРОДИВСЯ
1	0,433	0	0,02	0
2	0,412	0,03	0,04	0
3	0,527	0	0	0
4	0,493	0	0	0,001
5	0,521	0,04	0,0263	0

Апробація розроблених НМС проведена з використанням програмних пакетів NeuroPro, DeductorStudio та створеного програмного забезпечення. Розрахунки здійснені з використанням персонального

комп'ютера з процесором Intel Core Quard з тактовою частотою 2,4 ГГц та обсягом оперативної пам'яті 3,5ГБ. Для всіх випадків термін навчання НММ $t_н \le 60c$. Результати розпізнавання ДШП тестових прикладів скриптів JavaScript показані в табл. 5. В табл. 6 представлені максимальна ($\delta^p_{\max}$) та середня помилки (δ^p_s) виходу ДШП для всіх тестових прикладів JavaScript-скриптів.

Таблиця 5

Результати розпізнавання ДШП тестових прикладів скриптів JavaScript

Номер прикладу	Похибка виходу	Номер прикладу	Похибка виходу
Скриптове ШПЗ		Безпечні скрипти	
1	0,003523	6	0,012763
2	0,002787	7	0,064381
3	0,025412	8	0,004235
4	0,417221	9	0,021688
5	0,004672	10	0,011725

Таблиця 6

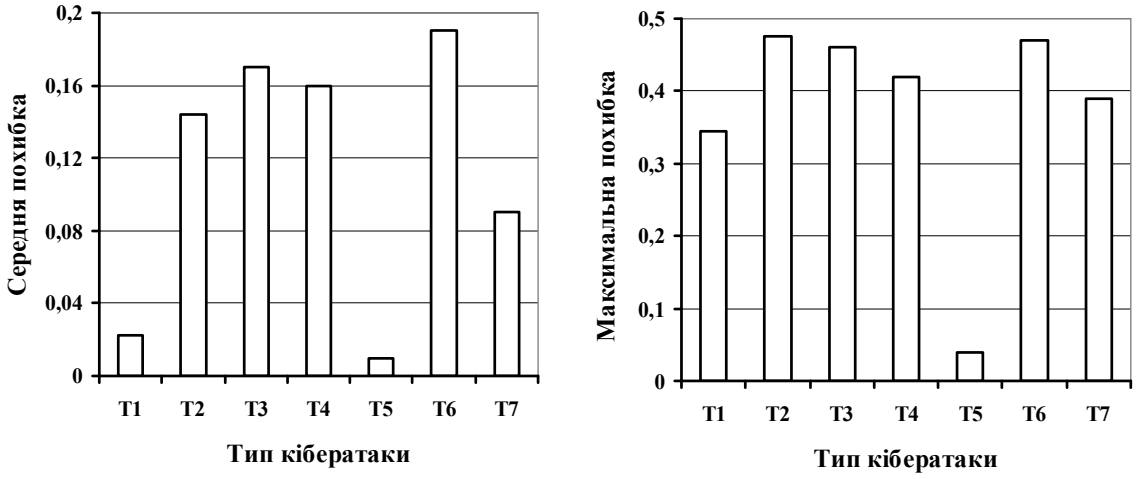
Помилки виходу ДШП при розпізнаванні скриптів JavaScript

Розпізнаний клас	$\delta^p_{\max}$	δ^p_s
Скриптове ШПЗ	0,3454137	0,0225612
Безпечні скрипти	0,1722524	0,0053734
Для всіх тестових прикладів	0,3454137	0,013967

Зазначимо, що використана методика класифікації, в якій допустимою є помилка виходу $\delta<0,5$. Виходячи з цього, дані табл. 5, 6 вказують на те, що всі тестові приклади розпізнані правильно. Таким чином, результати проведених експериментів підтверджують можливості розроблених НМС.

В підсумку побудовані гістограми середньої та максимальної похибки вихідного сигналу НММ на тестових прикладах, що відповідають реалізації типів кібератак, наведених в табл. 2. (рис. 11). Аналіз рис. 11 вказує на правильну класифікацію всіх тестових прикладів, оскільки кібератака класифікується при $Y > 0,5$. Порівняння похибок розроблених НМС з похибками розповсюджених систем розпізнавання кібератак вказує на можливість в 1,2–2 рази зменшити похибку розпізнавання нових типів кібератак.

Таким чином, низька похибка класифікації, короткий термін навчання, можливість функціонування на розповсюдженому апаратному забезпеченні, широкий спектр типів кібератак, що можуть бути розпізнані, можливість інтеграції в різнотипні системи захисту та використання широкої номенклатури ПБ, підтверджують адекватність розроблених НМС щодо можливості якісного розпізнавання нових типів кібератак при обмежених обчислювальних ресурсах та варіативності умов застосування.



а *б*

Рис. 11. Гістограми похибок вихідного сигналу нейромережевої системи

У додатках вміщено акти впроваджень результатів дисертаційної роботи та фрагменти кодів програм, що відображають практичну частину дисертаційного дослідження.

ВИСНОВКИ

У дисертації запропоноване нове вирішення актуальної науково-прикладної проблеми, що полягає у створенні комплексної методології розробки широкодоступних ефективних нейромережевих засобів оцінки параметрів безпеки Інтернет-орієнтованих інформаційних систем, які за рахунок теоретично обґрунтованого вибору характеристик дозволяють оперативно розпізнавати нові види кібератак при обмежених обчислювальних ресурсах та варіативності умов застосування. Проведені дослідження дозволяють зробити наступні висновки:

1. Визначено, що недоліки сучасних нейромережевих засобів оцінки параметрів безпеки Інтернет-орієнтованих інформаційних систем для розпізнавання кібератак спричинені недосконалістю теоретико-методологічних підходів до розробки нейромережевих систем оцінювання параметрів безпеки, які не в повній мірі адаптовані до умов застосування та нових типів кібратак. Обґрунтовано перспективність створення комплексної методології нейромережевої оцінки параметрів безпеки, для розробки якої необхідно розвинути теоретичні положення, моделі та методи побудови нейромережевих засобів.

2. Отримали подальший розвиток теоретичні положення побудови нейромережевих засобів оцінки параметрів безпеки, які за рахунок вперше розроблених підходів до розпізнавання поступових та неочікуваних кібератак, визначення оптимального виду нейромережевої моделі, доцільності застосування та ефективності розробки нейромережевих засобів, класифікації статистично подібних кібератак, застосування продукційних правил для подання експертних знань, верифікації нейромережевих моделей, запропонованих критеріїв оцінки ефективності

нейромережевих засобів, критеріїв вибору оптимального виду нейромережевої моделі та застосуванню розробленого функціоналу приведеної помилки навчання багатошарового персептрону дозволяють вдосконалювати нейромережеві засоби шляхом їх адаптації до поступових і неочікуваних кібератак, умов застосування, навчання за допомогою експертних даних та зменшувати похибки класифікації.

3. Отримали подальший розвиток моделі нейромережевих засобів оцінки параметрів безпеки, які за рахунок застосування розроблених теоретичних положень побудови нейромережевих засобів**,** експертного оцінювання вагомості параметрів безпеки, введення в модель MPNN нейронного шару фільтрації з лінійною біполярною з насиченням функцією активації, розроблених аналітичних залежностей для розрахунку параметрів ланцюгів Маркова, призначених для прогнозування параметрів безпеки на стаціонарних інтервалах, та для оцінки оптимальної кількості схованих нейронів, кількості обчислювальних навчальних операцій, обсягу пам’яті і помилки навчання багатошарового персептрону дозволяють: визначити перелік параметрів безпеки, які доцільно оцінювати нейромережевими засобами; створювати шаблони поведінки, адаптовані до складного характеру параметрів безпеки; в 1,5-6 разів зменшити ресурсоємність процесу визначення оптимальної структури багатошарового персептрону; апріорно оцінювати обчислювальні потужності, необхідні для реалізації нейромережевої моделі; за допомогою експертних даних навчати нейромережеву модель; формалізувати процес створення ефективних нейромережевих засобів, що є основою для підвищення ефективності методів їх розробки.

4. Вперше розроблено метод подання експертних знань для нейромережевих засобів оцінки параметрів безпеки, що за рахунок розробленого математичного забезпечення детермінування параметрів статистично подібних кібератак, продукційних правил представлення навчальних прикладів та структури і вагових коефіцієнтів синаптичних зв’язків нейромережевої моделі типу MPNN дозволяє забезпечити оперативність розпізнавання та розширити множину типів кібератак, характеристики яких не представлені в статистичних даних. Апробація методу на сигнатурах кібератак, представлених в базі даних KDD-99, показала абсолютну повноту класифікації кібератак типу U2R, що в 5 разів перевищує результати інших відомих нейромережевих методів.

5. Вперше розроблено метод визначення часових характеристик використання нейромережевих засобів, в якому завдяки використанню розроблених аналітичних залежностей для визначення очікуваного терміну їх розробки, допустимих термінів формування навчальної вибірки та навчання нейромережевої моделі, запропонованих співвідношень між очікуваним і допустимим терміном розробки та очікуваним і допустимим терміном навчання, розробленій множині допустимих видів нейромережевих моделей отримана можливість визначення доцільності застосування нейромережевих засобів оцінки параметрів безпеки для

виявлення очікуваних кібератак на заданий об’єкт захисту. Доведена можливість застосування нейромережевих засобів для розпізнавання типових Інтернет-орієнтованих кібератак: сканування портів, Dos-атак, IP-спуфінгу та веб-орієнтованих скриптових вірусів та троянів.

6. Вперше розроблено метод проектування шаблону поведінки, який використовується для навчання нейромережевих моделей, в якому за рахунок застосування багатоперіодичних рядів динаміки, розробленого математичного забезпечення для розрахунку періодичних складових та розробленої негомогенної марківської моделі забезпечується зменшення похибки шаблону в 1,5-2, що є основою для зменшення терміну формування навчальної вибірки, та зменшення похибок класифікації нейромережевих моделей при розпізнаванні поступових кібератак.

7. Вперше розроблено метод визначення ефективності розробки нейромережевих засобів оцінки параметрів безпеки, який за рахунок застосування запропонованих параметрів оцінки ефективності, що відображають ступінь виконання основних вимог до побудови та застосування нейромережевих засобів, запропонованих вагових коефіцієнтів важливості параметрів ефективності та розробленого інтегрального показника ефективності нейромережевих засобів дозволяє, відповідно до визначених показників, обрати найбільш ефективний засіб. Застосування методу дозволило визначити, що типовими недоліками більшості відомих нейромережевих засобів є недостатня обґрунтованість доцільності використання, низька пристосованість до застосування всієї множини перспективних нейромережевих моделей, неможливість використання експертних даних та емпіричний вибір виду нейромережевої моделі.

8. Вперше розроблено комплексну методологію нейромережевої оцінки параметрів безпеки, яка за рахунок взаємопов’язаного використання розроблених підходів до верифікації нейромережевих засобів, визначення оптимального виду нейромережевої моделі, розроблених моделей створення ефективних нейромережевих засобів оцінки параметрів безпеки, інтеграції параметрів безпеки та методів подання експертних знань, проектування шаблонів поведінки, доцільності застосування та визначення ефективності розробки нейромережевих засобів, що забезпечує можливість їх верифікації, дозволяє розширити функціональні можливості та, відповідно до розробленого інтегрального показника, обрати найбільш ефективний нейромережевий засіб. Використання запропонованої методології дозволяє до 4 разів підвищити інтегральний показник ефективності розробки нейромережевих засобів.

9. На основі комплексної методології розроблено структуру нейромережевої системи оцінки параметрів безпеки для розпізнавання кібератак, яка за рахунок використання модулів класифікації параметрів кібератак, формування статистично подібних кібератак, формування параметрів розробленої марківської моделі шаблону поведінки, підсистеми первинного визначення параметрів кібератак, модулів інтеграції параметрів безпеки, визначення обчислювальних обмежень, розрахунку

критеріїв оптимізації виду нейромережевої моделі та показників ефективності, формування продукційних правил підсистеми експертного оцінювання параметрів нейромережевих засобів, модулів розробки MPNN, визначення доцільності застосування, оптимізації виду та верифікації нейромережевих моделей підсистеми розробки нейромережевих моделей забезпечує верифікацію отриманих результатів та підвищення ефективності інструментальних засобів розпізнавання кібератак завдяки зменшенню похибок класифікації кібератак, оперативній адаптації до умов застосування та нових типів кібератак.

10. З використанням комплексної методології та структурних рішень системи оцінки параметрів безпеки, розроблено системи та відповідне програмне забезпечення для розпізнавання шкідливого програмного забезпечення, класифікації листів електронної пошти та розпізнавання мережевих кібератак. Експериментальне дослідження розроблених систем підтвердили їх адекватність щодо можливості забезпечення повноти класифікації відомих та нових типів кібератак, пристосованості до функціонування при обмежених обчислювальних ресурсах та оперативної адаптації до умов застосування.

11. Зазначені результати впроваджені у діяльність Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Національного авіаційного університету, Національного технічного університету України «КПІ», Національного університету будівництва і архітектури, що підтверджено відповідними актами впровадження, які містяться у додатках до дисертаційної роботи.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Терейковський І. Нейронні мережі в засобах захисту комп’ютерної інформації: монографія / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.

2. 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.

3. Корченко О. Г. Верифікація нейромережевих методів розпізнавання кібератак / О. Г. Корченко, І. А. Терейковський, С. В. Казмірчук // Науково-технічний збірник «Управління розвитком складних систем» Київського національного університету будівництва і архітектури. – 2014. – Вип. 17. – С. 168–172.

4. Терейковський І. А. Нейромережева методологія розпізнавання інтернет-орієнтованого шкідливого програмного забезпечення / І. А. Терейковський // Безпека інформації. – 2013. – Т. 19, № 1. – С. 24–28.

5. Терейковський І. А. Методологія класифікації листів електронної пошти з використанням нейронних мереж / І. А. Терейковський // Захист інформації. – 2013. – Т. 15, № 2. – С. 115–121.

6. 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.

7. Терейковський І. А. Нейромережевий поведінковий аналізатор антивірусної системи / І. А. Терейковський // Захист інформації. – 2012. – № 2. – С. 67–70.

8. 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» Київського національного університету будівництва і архітектури. – 2010. – Випуск 3. – С. 111–114.

9. Терейковський І. А. Розпізнавання скриптових вірусів за допомогою нейронної мережі з радіальними базисними функціями / І. А. Терейковський // Науково-технічний збірник «Управління розвитком складних систем» Київського національного університету будівництва і архітектури. – 2010. – Вип. 4. – С. 104–108.

10. 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» Київського національного університету будівництва і архітектури. – 2011. – Вип. 5. – С. 128–131.

11. Терейковський І.А. Оптимізація архітектури нейронної мережі, призначеної для діагностики стану комп'ютерної мереж / І. А. Терейковський // Науково-технічний збірник «Управління розвитком складних систем» Київського національного університету будівництва і архітектури. – 2011. – Вип. 6. – С. 155–158.

12. 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» Київського національного університету будівництва і архітектури. – 2013. – Вип. 13. –С. 157–161.

13. 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» Київського національного університету будівництва і архітектури, 2014, Вип. 19. – С 118–123.

14. Корченко О. Г. Метод оцінки нейромережевих засобів щодо можливостей виявлення інтернет-орієнтованих кібератак / О. Г. Корченко, І. А. Терейковський // Вісник інженерної академії наук. – 2014. – Вип. 2. – С. 87–93.

15. Терейковський І. А. Використання семантичної нейронної мережі в задачах моніторингу текстової інформації / І. А. Терейковський // Вісник ДУІКТ. – 2012. – Т. 10, № 1. – С. 36–41.

16. 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.

17. 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. – Вип. 2(24). – С. 65–70.

18. Терейковский И. А. Безопасность программного обеспечения, созданного с использованием семейства технологий COM, DCOM, COM+ / И. А. Терейковский // Захист інформації. – 2006. – № 1. – С. 55–67.

19. Терейковський І. А. Визначення оптимального методу контролю об’єктів захисту комп’ютерних мереж / І. А. Терейковський // Вісник КНУТД. – 2006. – № 5. – С. 39–44.

20. Терейковский И. А. Концепция защиты программного обеспечения Internet-сервера с использованием активной составляющей / И. А. Терейковский // Захист інформації. – 2005. – Спец. випуск. – С. 6-11.

21. Терейковський І. А. Концепція атаки Web-орієнтованих пошукових систем / І. А. Терейковський // Вісник ДУІКТ. – 2006. – Т. 3, № 3–4. – С. 67–71.

22. 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.

23. Терейковский И. А. Парольная защита офисного электронного документооборота / И. А. Терейковский // Вісник ДУІКТ. – 2006. – Т. 4, № 2. – С. 109–115.

24. 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.

25. Терейковський І. Оптимізація захисту відкритих корпоративних мереж / І. Терейковський, Л. Терейковська // Вісник КНТЕУ. – 2004. – № 1. – С. 103–112.

26. Терейковський І. А. Захищеність Web-серверів Apache та IIS / І. А. Терейковський // Проблеми програмування. – 2005. – № 2. – С. 42–51.

27. 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.

28. Терейковський І. А. Дослідження стійкості серверних технологій Java від атак на відмову / І. А. Терейковський // Захист інформації. – 2004. – № 4. – С. 34–42.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. Терейковський І. А. Методи коннективізму та захист в них / І.А. Терейковський // Захист інформації. – 2009. – № 1. – С. 59–70.

35. Терейковський І. А. Підвищення ефективності функціонування корпоративних web – сайтів / І .А. Терейковський // Вісник КНУТД. – 2004. – № 4. – С. 41–46.

36. Терейковський І.А. Оптимізація структури та змісту корпоративних Web–сайтів / І.А. Терейковський // Вісник КНТЕУ. – 2004. – № 3. – С. 95–104.

37. 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.

38. Терейковский И.А. Моделирование профилей нормального поведения компьютерных систем / И. А. Терейковский // Защита информации: сб. науч. трудов НАУ. – 2006. – Вып. 13. – С. 103–108.

39. Терейковський И. А. Применение семантического анализа содержимого электронных писем в системах распознавания спама / И. А. Терейковский // Захист інформації. – 2006. – № 4. – С. 49–60.

40. 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.

41. 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.

42. 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.

43. Цуриков О. М. Оптимизация режима многопараметрического контроля на примере многопараметрического контроля / О. М. Цуриков, И. А. Терейковский // Вісник КМУЦА. 2-е видання : зб. наук. праць. – К. : КМУЦА, 1999. – С. 217–221.

44. 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-е видання : зб. наук. пр. – К. : КМУЦА, 1999. – С. 7–15.

45. 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.

46. 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.

47. Терейковський І. А. Оптимізація захисту Web-орієнтованих інформаційних систем органів державної влади / І. А. Терейковський // Державне управління і право: зб. наук. праць Київського національного університету культури і мистецтв.– 2006. – Вип. 1. Ч. 2. – С. 97–105.

48. 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.

49. 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.

50. 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 допов. – К., 2006. – С. 224–225.

51. 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 допов. – К. : 2006. – С. 103–104.

52. 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-ої міжнар. наук.-техн. конф. (29 вересня – 01 жовтня 2011). – Львів : ЛПНУ, 2011. – С. 93–96.

53. 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 листопада 2011 р.). – К. : ДУІКТ, 2011. – С. 372–379.

54. Терейковський І.А. Використання семантичної нейронної мережі в задачах моніторингу текстової інформації / Терейковський І.А. // Сучасні інформаційно-комунікаційні технологі. COMINFO'2011: матер. VII міжнар. наук.-техн. конф. (10-14 жовтня 2011 р.). – К. : ДУІКТ, 2011. – С. 218–220.

55. 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 : матер. VIII міжнар. наук.-практ. інтернет-конф. (23.01.2012–30.03.2012). – Ірпінь : НУДПСУ, 2012. – С. 320–325.

56. 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.

57. 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: матер. 2 міжнар. наук.-практ. конф. "MoodleMoot Ukraine-2014", (22–23 травня 2014 р.). – К. : КНУБА, 2014. – С. 36.

58. Корченко О. Г. Метод оцінки нейромережевих засобів щодо можливостей виявлення інтернет-орієнтованих кібератак / О. Г. Корченко, І. А.Терейковський // ITSEC : матер. IV міжнар. наук.-техн. конф. (20–23 травня 2014 р.). – К. : НАУ, 2014. – С. 57.

59. 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 Technologies. 23–25 September, 2014, Kyiv, Ukraine, – 2014. – P. 1.11.72.

АНОТАЦІЯ

Терейковський І. А. Нейромережеві моделі, методи і засоби оцінювання параметрів безпеки Інтернет-орієнтованих інформаційних систем. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Національний авіаційний університет, Київ, 2015.

Дисертація присвячена вирішенню науково-прикладної проблеми, що полягає у створенні комплексної методології розробки широкодоступних ефективних нейромережевих засобів оцінки параметрів безпеки Інтернет-орієнтованих інформаційних систем, які за рахунок теоретично обґрунтованого вибору характеристик, дозволяють оперативно розпізнавати нові види кібератак при обмежених обчислювальних ресурсах та варіативності умов застосування. На основі створеної методології побудовано нейромережеву систему оцінки параметрів безпеки, яка в порівнянні з аналогами дозволяє зменшити похибку класифікації, верифікувати отримані результати і забезпечити оперативну адаптацію до умов застосування та нових типів кібератак.

З використанням запропонованих рішень розроблено засоби розпізнавання шкідливого програмного забезпечення, спаму, витоків текстової інформації та мережевих кібератак.

Ключові слова: захист інформації, нейронна мережа, кібератака, параметр безпеки, шкідливе програмне забезпечення, спам, витік інформації.

АННОТАЦИЯ

Терейковский И.А. Нейросетевые модели, методы и средства оценивания параметров безопасности Интернет-ориентированных информационных систем. – На правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.21 – Системы защиты информации. – Национальный авиационный университет, Киев, 2015.

Диссертация посвящена решению научно-прикладной проблемы, которая заключается в создании комплексной методологии разработки широкодоступных эффективных нейросетевых средств оценки параметров безопасности Интернет-ориентированных информационных систем, которые за счет теоретически обоснованного выбора характеристик позволяют оперативно распознавать новые виды кибератак при ограниченных вычислительных ресурсах и вариативности условий использования.

Получили дальнейшее развитие теоретические положения построения нейросетевых средств оценки параметров безопасности, которые заключаются в впервые разработанных подходах к распознаванию постепенных и неожиданных кибератак, определении оптимального вида нейросетевой модели, целесообразности применения и эффективности разработки нейросетевых средств, классификации статистически подобных

кибератак, применении продукционных правил для представления экспертных знаний, верификации нейросетевых моделей, предложенных параметрах оценки эффективности нейросетевых средств, критериях выбора оптимального вида нейросетевой модели и функционала приведенной ошибки обучения многослойного персептрона, что позволяет совершенствовать нейросетевые средства путем их адаптации к постепенным и неожиданным кибератакам, условиям применения, обучению с помощью экспертных данных и уменьшить погрешности классификации.

Получили дальнейшее развитие модели создания и использования нейросетевых средств оценки параметров безопасности, которые за счет применения разработанных теоретических положений позволяют: определить перечень параметров безопасности, которые целесообразно оценивать нейросетевыми средствами; создавать шаблоны поведения, адаптированные к сложному характеру параметров безопасности; в 1,5-6 раз уменьшить ресурсоемкость процесса определения оптимальной структуры многослойного персептрона; априорно оценивать вычислительные мощности, необходимые для реализации нейросетевой модели; с помощью экспертных данных обучать нейросетевую модель; формализовать процесс создания эффективных нейросетевых средств.

Впервые разработан метод представления экспертных знаний для нейросетевых средств оценки параметров безопасности, который позволяет обеспечить оперативность распознавания и расширить множество типов кибератак, для которых отсутствуют статистические данные. Апробация метода на сигнатурах кибератак, представленных в базе данных KDD-99, показала абсолютную полноту классификации кибератак типа U2R, что в 5 раз превышает результаты известных нейросетевых методов.

Впервые разработан метод определения временных характеристик использования нейросетевых средств, в котором благодаря использованию разработанных аналитических зависимостей определения ожидаемого срока разработки, допустимых сроков формирования обучающей выборки и обучения нейросетевой модели, предложенных соотношений между ожидаемыми и допустимыми сроками разработки и обучения обеспечивается возможность определения целесообразности применения нейросетевых средств оценки параметров безопасности.

Впервые разработан метод проектирования шаблона поведения, используемый для обучения нейросетевых моделей, который за счет применения многопериодических рядов динамики, разработанного математического обеспечения для расчета периодичности и разработанной марковской модели позволяет в 1,5–2 уменьшить погрешность шаблона.

Обоснован метод определения эффективности разработки нейросетевых средств оценки параметров безопасности, который за счет применения предложенных параметров оценки эффективности и сформированного интегрального показателя эффективности позволяет

выбрать наиболее эффективное средство. Применение метода позволило определить, что типичными недостатками известных нейросетевых средств является недостаточная обоснованность целесообразности использования, низкая приспособленность к применению всего множества перспективных нейросетевых моделей, невозможность использования экспертных данных и эмпирический выбор вида нейросетевой модели.

Впервые разработана комплексная методология нейросетевой оценки параметров безопасности, которая за счет взаимосвязанного использования разработанных подходов, моделей и методов позволяет расширить функциональные возможности нейросетевых средств и выбрать из них наиболее эффективное.

На основе комплексной методологии разработана структура нейросетевой системы оценки параметров безопасности для обнаружения кибератак, в которой за счет использования предложенных решений обеспечивается уменьшение ошибок классификации, верификация полученных результатов, а также оперативная адаптация к условиям применения и новым типам кибератак. На основании структурных решений предложенной системы оценки параметров безопасности разработаны инструментальные средства для распознавания вредоносного программного обеспечения, спама, утечек текстовой информации и сетевых кибератак.

Ключевые слова: защита информации, нейронная сеть, кибератака, параметр безопасности, вредоносное программное обеспечение, спам, утечка информации.

ABSTRACT

Tereykovskiy I. A. Neural models, methods and tools for evaluating Internet security settings-oriented information systems. – Manuscript.

Thesis for the degree of doctor of technical sciences, specialty 05.13.21 – information security systems. – National Aviation University, Kyiv, 2015.

The thesis deals with scientific and applied problems is to create an integrated development methodology widely-efficient neural evaluating the security settings of Internet-oriented information systems by theoretically informed choice characteristics, can efficiently identify new types of cyber attacks with limited computing resources variability and conditions of use. Based on the established methodology is based neural network evaluation system security settings, which in comparison with analogues can reduce the error classification, to verify the results and provide timely adaptation to the conditions of use and new types of cyber attacks.

Using the proposed solutions developed means of identification of malware, spam, data leaks text and network cyber attacks.

Key words: information security, neural network, cyber attacks, security setting, malware, spam, data leakage.

Підп. до друку 27.04.2015. Формат 60х84/16. Папір офс.
Офс. друк. Ум. друк. арк. 2,56. Обл.-вид. арк. 2,75.
Тираж 100 пр. Замовлення № 80-1.

Видавець і виготівник
Національний авіаційний університет
03680. Київ – 58, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002