КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.764
УДК 004.056

Палко Дмитро Володимирович
аспірант кафедри кібербезпеки та захисту інформації
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-2886-1975
palko.dmytro@gmail.com

ІНТЕЛЕКТУАЛЬНІ МОДЕЛІ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ СИСТЕМАХ НА ОСНОВІ НЕЙРОМЕРЕЖЕВОГО ПІДХОДУ

Анотація. У сучасних умовах функціонування інформаційних систем, стрімке зростання масштабів, складності та розподіленості обчислювальних ресурсів стає однією з визначальних тенденцій розвитку цифрової інфраструктури. В рамках широкого впровадження складних багатокомпонентних інформаційних систем, які мають розподілений характер і містять велику кількість вузлів, а також суттєвого зростання кількості та складності кіберзагроз, орієнтованих на масштабовані системи — ризики кібербезпеки слід розглядати як ключовий фактор стратегічного планування бізнес-процесів. Регулярний аналіз та оцінка ризиків кібербезпеки дозволяє визначити необхідну і достатню сукупність засобів захисту інформації, нормативно-правових та організаційних механізмів щодо зниження загроз ІБ, та забезпечує процес побудови максимально ефективної архітектури комплексної системи менеджменту інформаційної безпеки. Існуючий інструментарій та сучасні методології оцінки, що в переважній більшості носять концептуальний характер та засновані на статистичних підходах, є малоефективними в умовах аналізу великих обсягів високорозмірних гетерогенних даних та метрик розподілених систем. Стаття зосереджується на аналізі сучасних трендів та існуючих підходів до оцінювання ризиків кібербезпеки у розподілених інформаційних системах. Розглянуто важливість процесу управління ризиками в контексті забезпечення інформаційної безпеки та описано основні принципи інтелектуальної оцінки ризиків у розподіленому середовищі на основі нейромережевого підходу. У дослідженні представлено динамічну та комплексну модель оцінки кіберризиків у розподілених інформаційних системах на основі архітектури глибокої нейронної мережі та кількох методів її оптимізації, що забезпечує достатньо високу точність та надійність оцінки ризиків в умовах аналізу великих масивів гетерогенних вхідних даних.

Ключові слова: інформаційна безпека; кібербезпека; ризик кібербезпеки; оцінка ризиків; моделювання ризиків; інтелектуальні моделі оцінки; управління ризиками; розподілена інформаційна система; нейронна мережа; метрики безпеки; метадані; інформаційний актив.

ВСТУП

З розвитком комп’ютерних мереж і, зокрема, глобальної мережі Інтернет, питання безпеки розподілених систем набули особливого значення. Розподілені інформаційно-обчислювальні мережі об’єднують всі структурні підрозділи та філії організацій в єдину систему, дозволяють одночасно працювати з розподіленими і централізованими додатками, базами даних та іншими службами, а також з’єднувати комп’ютерні системи між собою для розподілу функцій і спільного використання ресурсів. З одного боку, такий підхід дозволяє більш оптимально використовувати величезний набір обчислювальних потужностей, що доступний на даний момент розвитку інформаційно-комунікаційних технологій, але з іншого — це породжує низку проблем, пов’язаних насамперед із складністю забезпечення безпеки та управління потенційними ризиками в розподіленому середовищі [1]. Перехід до комплексних, масштабованих і структурно

складних інформаційних систем підвищує ймовірність непередбачуваних і незапланованих подій, які впливають на продуктивність і ефективність функціонування системи. Організація процесу управління ризиками кібербезпеки в розподілених системах передбачає вирішення комплексу задач пов'язаних з функціональною розподіленістю та ієрархічністю, високим ступенем розпаралелювання ресурсів і практично повною відсутністю централізованого управління [2]. Особливої уваги заслуговують питання оцінки ризиків інформаційної безпеки в таких системах.

Організація оцінки ризиків кібербезпеки в розподілених системах є вкрай складним та комплексним завданням. При його вирішенні необхідно враховувати велику кількість факторів і чинників, що можуть мати негативний вплив на діяльність компанії, становити загрозу конфіденційності, цілісності та доступності інформації, а також якості та швидкості її обробки і передачі. Обмежені ресурси та постійно змінний мінливий ландшафт зовнішніх загроз та наявних вразливостей унеможливлюють повне зниження всіх наявних ризиків [3].

Виконання періодичної оцінки допомагає своєчасно ідентифікувати ризики кібербезпеки та вжити необхідні заходи безпеки щодо їх обробки та управління. Щоб підготуватися до потенційної атаки, організації повинні постійно оцінювати свій профіль ризику, впроваджувати рекомендовані міри безпеки та проактивно покращувати систему захисту [4].

Ризик за своєю суттю, це потенційна можливість використання певною загрозою наявних вразливстей активу чи групи активів з метою спричинення збитку компанії чи порушення властивостей інформації, що обробляється. Ризик носить потенційний, імовірнісний характер, та завжди пов'язаний з деякою невизначеністю, яка передбачає можливість втрат та збитків. Причому останні можуть бути як матеріальні (втрата доходу, несправність обладнання, крадіжка активів), так і нематеріальні (зниження репутації та втрата довіри). У якості активів виступають ключові елементи інфраструктури та інформація, що обробляється в розподіленій інформаційній системі та може нести певну цінність [5].

Відповідно до класичного підходу ризик кібербезпеки можна визначити як поєднання ймовірності несприятливої події та наслідків її впливу.

$$R = P(T \to V) * I(T), \quad (1)$$

де $P(T \to V)$ — ймовірність реалізації загрози T при наявності вразливості V;

$I(T)$ — очікуваний вплив реалізації загрози T.

В свою чергу, ці показники можна визначити наступним чином:

$$P(T \to V) = f(vulnerabilities, exposure, threats, mitigation\ controls), \quad (2)$$

$$I(T) = f(business\ criticality), \quad (3)$$

Проведення оцінки ризиків кібербезпеки має вирішальне значення для ефективного моніторингу факторів потенційних загроз та покращення можливостей подальшого реагування. Саме тому процес ризик-менеджменту слід розглядати як ключовий фактор стратегічного планування бізнес-процесів [6].

Глобальна пандемія COVID-19, також відома як епідемія коронавірусу, мала значний вплив і змінила підходи до оцінки корпоративних ризиків за останні роки. Масовий перехід на дистанційний режим роботи, викликаний пандемією, спричинив додаткові проблеми з інформаційною безпекою підприємств. Багато компаній раніше взагалі не практикували можливість надання віддаленого доступу до корпоративних ресурсів своїм співробітникам, а організація тимчасових каналів доступу в поодиноких випадках не становила складності й адмініструвалась вручну. Загрози, що раніше були

неактуальними оскільки перекривались периметром безпеки офісів і не становили небезпеки для внутрішньої корпоративної мережі наразі почали відігравати чималу роль при розробці стратегії захисту даних інформаційних систем. Головним викликом в умовах пандемії стала швидкість з якою можна було б досягти неперервності бізнес-процесів. У гонитві за мінімізацією втрат від простою бізнесу та пришвидшенням робіт з адаптації та пристосування інфраструктури до нового режиму роботи витікає ряд проблем пов'язаних з наданням користувачам надлишкових прав, ігноруванням вимог безпеки при конфігуруванні доступу, відвертим нехтуванням очевидними загрозами, що пов'язані з передачею конфіденційних даних через незахищені канали тощо. Зміна характеру і структури інформаційних потоків, розширення використання хмарних сервісів, збільшення кількості кіберзагроз та суттєва зміна ландшафту корпоративних ризиків в умовах пандемії сприяла подальшій еволюції підходів до оцінювання та управління ризиками у розподілених інформаційних системах, підкреслюючи необхідність у створенні більш досконалих, гнучких та адаптивних методологій оцінки.

Аналіз останніх досліджень і публікацій. Питаннями розробки класичної концепції розподілених інформаційних систем, а також дослідженням основних аспектів та проблем забезпечення кібербезпеки в розподілених середовищах, в тому числі оцінки ризиків ІБ, займались Ендрю С. Таненбаум (Andrew S. Tanenbaum), Леслі Лампорт (Leslie Lamport), Ненсі Лінч (Nancy Lynch), Джордж Кулуріс (George Coulouris), Джин Доллімор (Jean Dollimore), Тім Кіндберг (Tim Kindberg), Росс Андерсон (Ross Anderson), Кліффорд Нюрнберг (Clifford Neuman) та багато інших. Серед вітчизняних дослідників можна виокремити внесок В.А. Заславського, О.А. Машкова, О.В. Барабаша, Ю.В. Кравченка, Н.В. Лукової-Чуйко, О.Ю. Ільїна, Ю.М. Коростіля, О.А. Кононова, В.А. Савченка, Д.М. Обідіна, тощо.

Окрім цього, на сьогоднішній день розробляється та розвивається чимала кількість стандартів та нормативно-правових документів у сфері аналізу та оцінки ризиків інформаційної безпеки. Ключовими регулюючими документами в даній сфері, на які необхідно опиратись при побудові зрілої системи менеджменту інформаційної безпеки (СМІБ, англ. information security management system, ISMS), є NIST SP 800-30 та серія міжнародних стандартів ISO/IEC 27000 (зокрема ISO/IEC 27005:2022). У порівнянні з ISO/IEC 27005:2022, NIST SP 800-30 надає більш детальний та методичний опис самого процесу оцінювання ризиків, включаючи етапи збору даних, аналізу загроз та вразливостей, оцінювання ймовірностей та впливу, а також формування рекомендацій щодо реагування, тоді як ISO/IEC 27005:2022 концентрується на концептуальних аспектах управління ризиками та його інтеграції з системним менеджментом, надаючи узагальнену методологічну основу для процесу оцінки ризиків ІБ. Окрім розглянутих документів, існує велика різноманітність інструментів та методологій оцінки, що широко застосовуються на практиці. Серед них можна виділити методологію аналізу та контролю інформаційних ризиків CRAMM (CCTA Risk Analysis and Managment Method), що пропонує класичний підхід із фокусом на автоматизацію та деталізацію процесів, методологію оцінки операційно критичних загроз, активів та вразливостей OCTAVE (Operationally Critical Threats, Assets and Vulnerability Evaluation), що фокусується на операційно-орієнтованому підході та зосереджується на бізнес-контексті, методологію пропорційного аналізу ризиків MEHARI (Method for Harmonized Analysis of Risk), що орієнтована на практичні аспекти застосування з акцентом на вразливості системи, методологію Міжнародного Форуму з інформаційної безпеки для аналізу інформаційних ризиків IRAM (Information Risk Assessment Methodology), що зосереджується на оптимізації бізнес-пріоритетів, тощо. Останнім часом все більша увага приділяється

методиці факторного аналізу інформаційних ризиків FAIR (Factor Analysis of Information Risk), яка націлена на кількісну оцінку ризику та пошук фінансових еквівалентів потенційних втрат. Стандарти, розроблені асоціацією ISACA та платформою COBIT [6], також пропонують корпоративні підходи до управління ризиками, інтегруючи аспекти IT-управління та інформаційної безпеки.

Попри широке розповсюдження та популярність, стан розробки даної теми у вітчизняній та зарубіжній науці залишається на доволі низькому рівні. Класичні підходи до оцінки, що висвітлюються в профільній літературі, стандартах ІБ та сучасних методологіях оцінки ризиків не забезпечують належного ефекту в умовах аналізу великих масивів даних та здебільшого носять концептуальний характер при використанні в розподілених інформаційних системах.

Згідно з результатами щорічного глобального дослідження стану кібербезпеки «STATE OF CYBERSECURITY 2022: GLOBAL UPDATE ON WORKFORCE EFFORTS, RESOURCES AND CYBEROPERATIONS» від компанії ISACA, проведеного в четвертому кварталі 2021 року, переважна більшість компаній-респондентів принаймні один раз на рік проводять регулярну оцінку ризиків інформаційної безпеки (41% проти минулорічних 39%). Збільшення відсотка респондентів, чиї підприємства проводять оцінку кібер-ризиків частіше, ніж щорічно, невелике (33% у 2022 році та 32% у 2021 році), але це може сигналізувати про позитивну тенденцію, на яку варто звернути увагу.

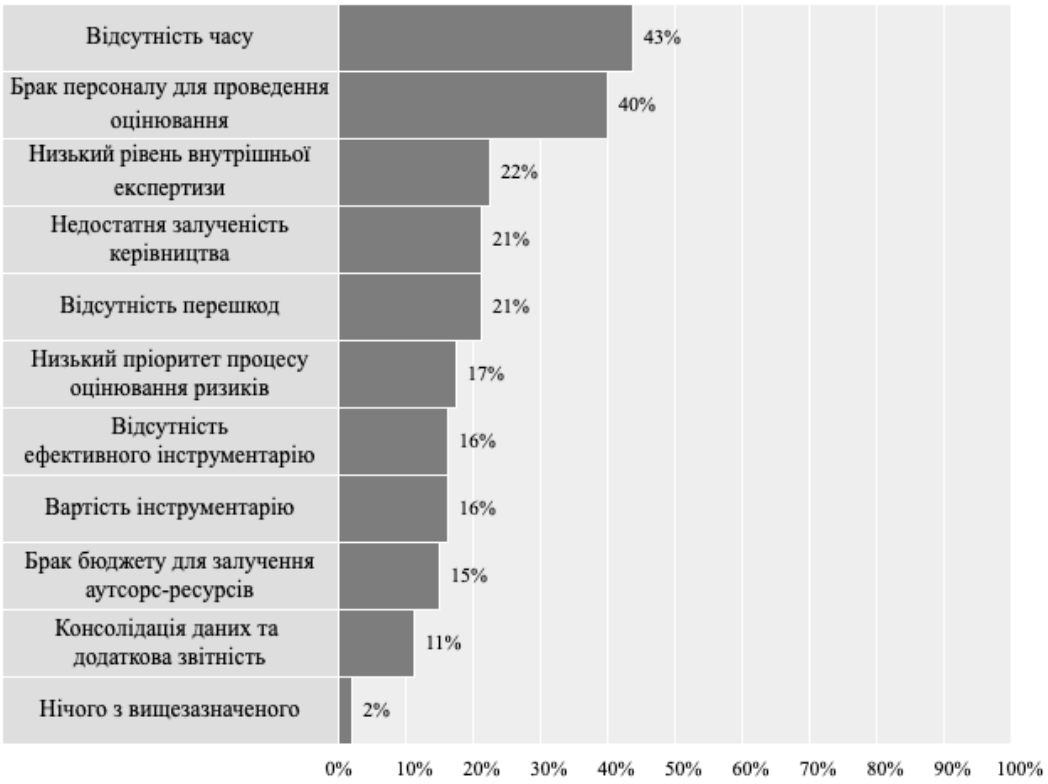

Рис. 1. Перешкоди для частішого проведення оцінки ризиків кібербезпеки

В сучасних реаліях компанії стикаються з багатьма перешкодами для проведення частих оцінок кіберризиків. За результатами опитування, відсутність часу (зазначений 43% респондентів) був основною перешкодою, брак персоналу для проведення оцінювання (40%) займає друге місце за критичністю. Іншими перешкодами стали

низький рівень внутрішньої експертизи, відсутність правильних кіберінструментів для ефективного проведення оцінювання або їх вартість (рис. 1). А це, у свою чергу, вказує на важливу проблему, пов'язану з відсутністю ефективних та універсальних методів оцінки ризиків кібербезпеки та їх недостатньою адаптованістю до мінливих умов динамічного середовища зі швидкозмінним горизонтом потенційних загроз в умовах розподілених інфраструктур [7].

Постановка проблеми. Класичні статистичні методи аналізу ризиків (якісні, кількісні чи навіть комбіновані) не надають бажаного результату через їх недосконаліть та суттєві обмеження щодо використання в розподіленому середовищі [8].

Експертний аналіз вимагає від фахівців ІБ значного рівня компетентності та великого практичного досвіду. З іншого боку, такий підхід займає багато часу, пов'язаний з певного роду суб'єктивністю та не може бути застосований для аналізу великих масивів первинних даних без попередньої обробки [9].

Дуже перспективним напрямком досліджень у галузі оцінки ризиків для складних, масштабованих та розподілених систем є застосування інтелектуальних методів моделювання на основі нейромережевого підходу. Необхідною умовою для використання інтелектуальних моделей є наявність невизначеності через брак інформації, складність системи або наявність якісної інформації. Безумовною перевагою нейромережевих структур є їх здатність до навчання, самоорганізації та узагальнення, а також можливість вирішувати складні комплексні завдання. Такий підхід дозволяє отримати моделі, здатні швидко адаптуватися до мінливих умов швидкозмінного середовища розподілених систем [10]. Навіть найпростіша архітектура нейронної мережі на основі алгоритму зворотного поширення помилки (англ. backpropagation) може виконувати розпізнавання образів у реальному часі з прийнятною швидкістю та високим рівнем точності. Архітектура типової нейронної мережі складається з вхідного рівня, прихованих шарів і вихідного рівня (рис. 2) [11].

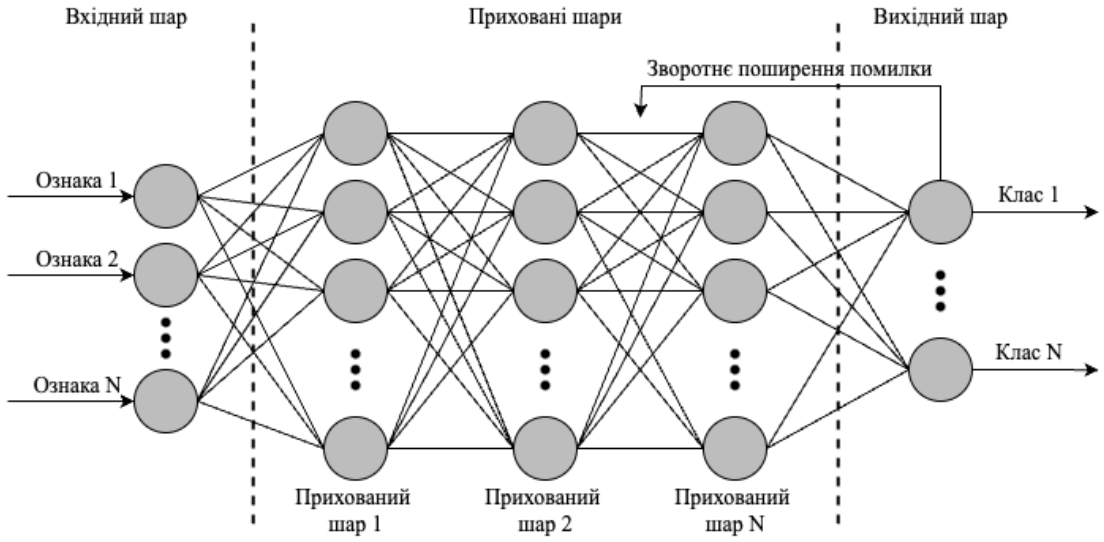

Рис. 2. Архітектура багатошарового перцептрону на основі навчання методом зворотного поширення помилки

Ваги та параметри моделі встановлюються шляхом обчислення похибки між фактичними та очікуваними вихідними даними нейронної мережі, коли їй надаються навчальні дані в процесі тренування. В подальшому механізм оптимізації на основі значення помилки використовується для зміни вагових коефіцієнтів і параметрів моделі, з метою покращення продуктивності та точності нейронної мережі у видачі правильного результату, коли наступного разу на її вхід буде представлено такий же вхідний вектор даних [12].

Функція помилки в класичному алгоритмі зворотного поширення є середньоквадратичною помилкою (mean squared error, MSE).

$$E(X,\theta) = \frac{1}{2N}\sum_{i=1}^{N}(\widehat{y_i} - y_i)^2, \quad (4)$$

де y_i — є цільовим значенням для пари входу-виходу $(\overrightarrow{x_i}, y_i)$, а $\widehat{y_i}$ — є обчисленим виходом мережі при вході $\overrightarrow{x_i}$, та наборі вхідної вибірки розмірністю N.

Можуть застосовуватись інші функції обрахунку помилки, але історичний зв'язок середньоквадратичної похибки зі зворотним поширенням і його зручні математичні властивості роблять його гарним вибором для вивчення методу [13].

Нейронні мережі не є новою концепцією, але лише в останні роки різні компанії почали досліджувати та розуміти їх повний потенціал. Інтелектуальні системи відіграють все більш важливу роль в управлінні мережею та забезпеченню безпеки сучасних компаній. Більшість досліджень у галузі систем виявлення вторгнень та оцінки ризиків широко покладаються на методи AI для розробки, впровадження та вдосконалення систем моніторингу безпеки.

Останні оновлення зловмисного програмного забезпечення та вдосконалення методів здійснення кібератак важко виявляти за допомогою традиційних методів кібербезпеки. Важливою перевагою нейронних мереж є їх здатність «вивчати» характеристики вхідних даних і ідентифікувати елементи, які не схожі на ті, що спостерігалися в мережі раніше. Нові алгоритми штучного інтелекту використовують машинне навчання для швидкої адаптації і аналізу нових даних, покращення результатів та визначення нових векторів реалізації загроз [14].

На відміну від експертних систем, які можуть надати однозначну відповідь про відповідність розглянутих характеристик закладеним у базі знань правилам, нейронна мережа проводить аналіз інформації та надає можливість оцінити, чи узгоджуються дані з характеристиками, які вона навчена розпізнавати.

Таким чином, розробка інтелектуальних моделей на основі нейромережевого підходу для оцінки ризиків у розподілених інформаційних системах на сьогодні є пріоритетним і дуже перспективним напрямком досліджень.

Очевидно, що здійснення аналізу і моделювання ризиків інформаційної безпеки завдання вкрай складне, а тому вимагає розробки комплексної масштабованої моделі оцінки ризиків, що буде ефективною незалежно від середовища досліджуваного об'єкта, розмірів інфраструктури та кількості інформаційних активів.

Окрім цього, повинні вирішуватись наступні завдання:

- Аналіз метаданих та метрик розподіленої системи про складові ризиків, що мають різну природу походження та формат представлення (вирішення проблеми некоректного представлення даних);
- Забезпечення уніфікації та стандартизації процесу аналізу для оцінки будь-яких інформаційних активів без прив'язки до конкретної платформи, мережевого обладнання чи програмного забезпечення (уніфікація рішення);

- Підвищення адекватності оцінок без необхідності залучення експертних рішень фахівців з аналізу ризиків (здатність до навчання);
- Підтримка актуальності результатів аналізу шляхом скорочення тривалості процесу оцінювання (оцінка в режимі часу, близькому до реального);
- Забезпечення гнучкого, адаптивного та масштабованого рішення, що дозволяє виконати комплексну оцінку ризиків ІБ для інфраструктури будь-якого розміру незалежно від кількості інформаційних активів (здатність до масштабування);

Враховуючи вищеописані обмеження, **дане дослідження має на меті** запропонувати рішення вказаних проблем із застосуванням методів моделювання процесу оцінки ризиків інформаційної безпеки на основі нейромережевого підходу з метою оптимізації точності ідентифікації рівня ризику шляхом корегування гіперпараметрів нейронної мережі, а також комплексного дослідження гетерогенних метрик і метаданих про роботу типової розподіленої інформаційної системи та методів їх інтелектуального аналізу. Дослідження представляє динамічну та комплексну модель оцінки кіберризиків у розподіленому середовищі на основі архітектури глибокої нейронної мережі зі зворотним поширенням помилки та ряду методів її оптимізації, що забезпечують достатню точність та надійність оцінки ризиків в умовах аналізу гетерогенних метрик безпеки у великих масивах різнорідних розподілених даних.

МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

Практична реалізація аналітичного модуля виконана на основі мови програмування JavaScript та інструментарію фреймворку TensorFlow.js — провідної та універсальної бібліотеки з відкритим вихідним кодом, призначеної для завдань інтелектуального аналізу даних і машинного навчання. Результатом моделювання є побудова «навченої» моделі, яка може ідентифікувати рівень ризику безпеки для певного інформаційного активу на основі ряду мережевих показників. Цільова метрика представлена якісним показником «Рівень ризику», що носить категоріальний характер та може набувати значення одного з п’яти класів відповідно до визначеної градації рівня ризику, наведеної далі. Таким чином, має бути вирішена задача класифікації та навчання з учителем.

Вхідними даними моделі є набір розподілених метаданих і метрик інформаційних систем, агрегованих з типових корпоративних підсистем і платформ, таких як Active Directory, CMDB, системи управління інвентаризацією та активами, системи моніторингу мережі та веб-фільтрації, сканери вразливостей і антивірусні програми. Вхідний масив також включає метрики даних безпеки з джерела IBM QRadar SIEM (система управління ІБ та подіями безпеки) і додаткових ресурсів моніторингу, що дозволило отримати інформацію про такі важливі показники, як кількість задетектованих подій і вразливостей для кожного активу, перелік інстальованого програмного забезпечення, інформація про встановленні виправлення та патчі безпеки, графік та режим резервного копіювання, застосовані політики безпеки та засоби контролю і пом’якшення наслідків реалізації загроз, а також ступінь важливості та пріоритетності активів (критичність для бізнес-процесів), що, безперечно, є перевагою для навчання під наглядом із промаркованими даними.

Таблиця 1

Приклад розподілених метаданих і метрик мережевих активів

Назва метрики	Ідентифікатор у наборі даних	Тип	Опис	Приклад значення
Asset category	asset_category	category	Загальна категорія активу на основі типу пристрою	Server / Workstation / Network / Device…
Device type	device_type	category	Тип пристрою	SRV / PC / TAB / NB / IOT / NET…
Environment	environment	category	Тип середовища функціонування активу	Prod / Test / Dev …
OS type	os_type	category	Тип, версія та номер збірки операційної системи	Windows Server 2019 10.0 17763 / CentOS 7.3…
Network name	network_name	category	Назва мережі	Net.DC0.App_All / Net.DC1. App_EX…
VLAN	vlan	category	Віртуальна локальна мережа	701 / 504 / 35…
Last activity	last_activity	datetime	Дата-час останньої активності об’єкту	13.09.2024 10:43
Is critical	is_critical	binary	Чи належить актив до критичних	Yes / No
Is wireless	is_wireless	binary	Чи використовує об’єкт бездротове підключення	Yes / No
Backup status	backup_status	binary	Наявність механізмів резервного копіювання	Yes / No
Drive encryption	drive_encryption	binary	Наявність механізмів шифрування дисків	Yes / No
Last logon	last_logon	datetime	Дата-час останнього входу	11.09.2024 15:40
When created	when_created	datetime	Дата-час появи об’єкту в Active Directory	18.08.2019 12:25
Is blocked	blocked_in_ad	binary	Статус блокування об’єкту в Active Directory	Yes / No
Antivirus type	av_type	category	Тип антивірусного ПЗ	Microsoft Defender / McAfee...
Antivirus last update	last_av_update	datetime	Дата-час останнього оновлення агента	04.04.2024 13:29
Last vulnerability scan	last_vuln_scan	datetime	Дата-час останнього сканування вразливостей	12.11.2023 11:51
Total vulnerabilities	total_vulnerabilities	number	Загальна кількість виявлених вразливостей	17
Last event	last_siem_event	datetime	Дата-час останньої події в SIEM	30.08.2024 15:13
Average EPS	average_eps	number	Середня кількість подій в секунду за останню хвилину	12

Таким чином, сформований набір даних включає та відображає всі важливі метрики, що описані в класичному підході до оцінки ризиків інформаційної безпеки (1–3). А отже, можна зробити висновок, що він відповідає необхідним та достатнім умовам моделювання, повністю задовільняє поставлені вимоги та може бути використаний в процесі вирішення визначених завдань.

В ході проведеного аналізу вхідних наборів даних ідентифіковано та визначено найбільш важливі параметри, що характеризують стан забезпечення інформаційної безпеки активу, сформовано датасет для проведення дослідження та тренування нейронної мережі. Кількість вхідних метрик, на основі яких навчається нейронна мережа та розраховується цільовий атрибут (предиктори), становить 15. Слід враховувати, що кількість стовпців вибірки динамічно змінюється на етапі попередньої обробки вхідних даних в залежності від кількості категоріальних метрик, число яких пропорційно зростає зі збільшенням об'єму навчальної множини. Ці параметри включають тип та категорію активу, середовище, тип операційної системи, тип підключення, статус резервного копіювання та статус підключених джерел журналювання, показники стану блокування активу в домені, тип антивірусного ПЗ, кількість вразливостей, дати останнього сканування та останнього оновлення сигнатур Windows Defender і McAfee, оцінку важливості активу та його критичності для бізнес процесів.

Набір даних із 4,094 записів використовувався для навчання нейромережевої моделі. Початковий набір даних був розділений на набір даних для тренування (80% початкового) і набір даних для тестування та перевірки результатів (20%). Навчальні дані — це числова матриця розмірності $m \times (n + 1)$, в якій кількість рядків m відповідає розміру навчальної вибірки, перші n стовпців — значенню вхідних змінних моделі, а останній — значенню вихідної змінної (цільового параметру). Тренувальна вибірка буде використовуватися для навчання спроектованої моделі, а матриця тренувальних даних — для перевірки отриманих результатів на адекватність. Після навчання дані тестової вибірки подаються на вхід створеної моделі для отримання значення прогнозованого показника ризику для кожного екземпляру перевірочного набору даних.

Оскільки дані неоднорідні за природою, типом і форматом представлення, вони потребують додаткової попередньої обробки. В ході роботи була реалізована бібліотека користувацьких функцій для попередньої обробки вхідних метрик. Вона реалізує таку функціональність, як попереднє очищення даних, нормалізація та векторизація параметрів, які мають непідтримуваний формат, а також розбиття та формування наборів даних для навчання моделі та її валідації.

Для окремих інформативних параметрів необхідно здійснити препроцессінг та їх представлення для навчання моделі оскільки інструментарій TensorFlow.js при побудові нейронних мереж не може приймати на вхід дані категоріального (текстового) формату та в подальшому обробляти їх. Більшість метрик мають саме категоріальний характер тому на даному етапі необхідна їх векторизація. Для використання алгоритмів машинного навчання доцільно інтерпретувати дані нечислового формату із застосуванням кодування LabelEncoder в цілочисловий формат. Даний метод підійде для номінальних категоріальних параметрів, що можуть набувати лише 2 різних значення і кодуватись відповідно нулем або ж одиницею. Якщо ж кількість категорій більша, то для уникнення пошуку нейронною мережею додаткових взаємозв'язків та встановлення кореляції між числовими показниками (що негативно вплине на точність прогнозування), доцільно застосувати кодування OneHotEncoder (або ж метод get_dummies бібліотеки pandas для мови програмування python). Їх використання передбачає побудову додаткових стовпців вхідної матриці даних для кожної категоріальної величини, що нівелює вищеописані проблеми, але в свою чергу призводить до значного розростання простору вхідних змінних. Оскільки вищеописаний інструментарій доступний лише для мови програмування Python, цю функціональність попередньої обробки даних було реалізовано самостійно.

Всі дата-часові параметри (вигляду «Дата-час останнього оновлення/сканування/ завантаження тощо») модифікуються шляхом динамічного визначення зрізу часу, що минув з моменту події до поточного часу. Таким чином, навчальна вибірка буде оперувати значеннями тривалості часу, що минув замість використання статично прописаних абсолютних значень часових метрик, що значно спрощує їх інтерпретацію та подальше використання (наприклад, чим менше часу пройшло з моменту останнього оновлення сигнатур антивірусного ПЗ, тим відповідно нижчим буде рівень ризику реалізації потенційних загроз).

Результатом моделювання є побудова моделі, здатної прогнозувати показник рівня загроз для конкретного інформаційного активу базуючись на різноманітних мережевих метриках. Для підтвердження адекватності запропонованого рішення виконано обрахунок рівня точності (Accuracy score) нейромережевого компоненту та показника середньо-квадратичної помилки (mean squared error, MSE) для візуалізації продуктивності та ефективності алгоритму контрольованого навчання.

Покращення результатів навчання відбувається шляхом зміни гіперпараметрів моделі. Задача оптимізації полягає в тому, щоб вирішити, наскільки змінити кожен параметр моделі з урахуванням поточного прогнозу, з метою підвищення показника точності прогнозування та отримання більш оптимального результату вцілому.

Деякі параметри можуть бути змінені до початку тренування, інші ж отримуються в процесі навчання. Прикладами другої групи є ваги нейронів та значення зміщення (biases). Ці дані є внутрішніми для моделі та змінюються залежно від вхідних даних. Перша група включає такі фактори як безпосередньо архітектура нейронної мережі, кількість прихованих шарів та нейронів на кожному з них, функції активації (activation functions) та коефіцієнт швидкості навчання (learning rate), кількість епох (epochs) та розмір пакета (batch size), функція втрат (loss/cost function) тощо. Окрім цього значною мірою на результат впливає якість вхідних даних. Знайшовши оптимальну комбінацію значень гіперпараметрів, ми можемо зменшити помилку та побудувати найбільш точну модель [16].

Для розробленої моделі була обрана наступна конфігурація:

- Layers: 2 приховані шари (10 нейронів з функцією активації «sigmoid» та 5 нейронів з функцією активації «relu»);
- Batch size: 64;
- Learning rate 0.01;
- Epochs: 50 ітерацій обрано для навчання;
- Error function: середньоквадратична помилка (mean squared error, MSE);

Зазначені параметри були підібрані експериментальним шляхом, та показали найкращі результати щодо якості навчання.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для підтвердження адекватності запропонованого рішення, розраховано показник точності (acc/val_acc) і значення функції втрат (loss/val_loss) для навчального та перевірочного наборів даних (рис. 3–4).

ISSN 2663 - 4023

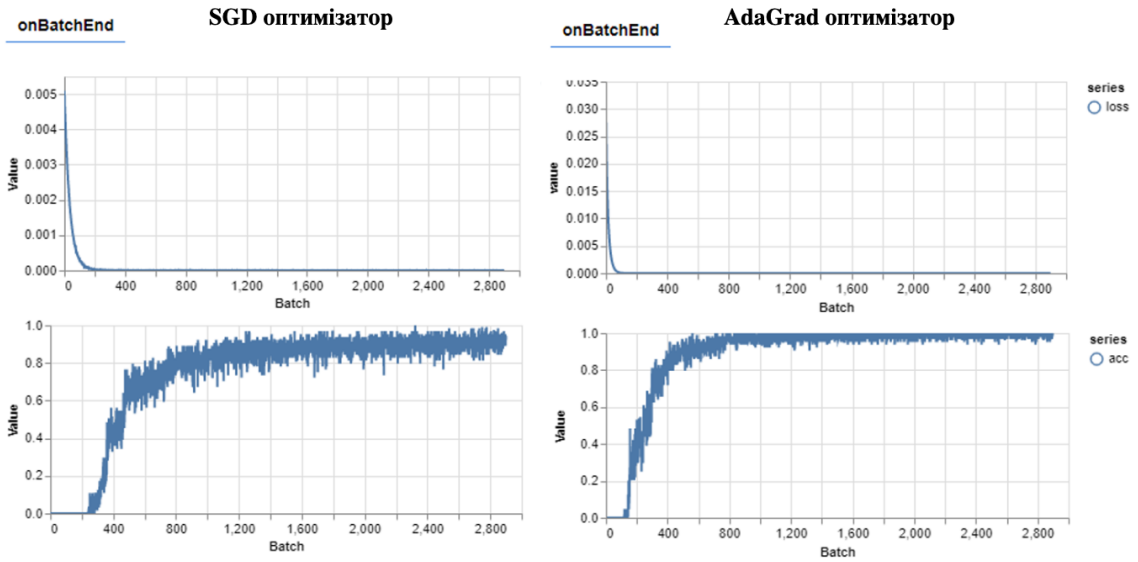

Рис. 3. Візуалізація динаміки процесу навчання за результатами кожного пакету (on batch end) для оптимізаторів SGD та AdaGrad

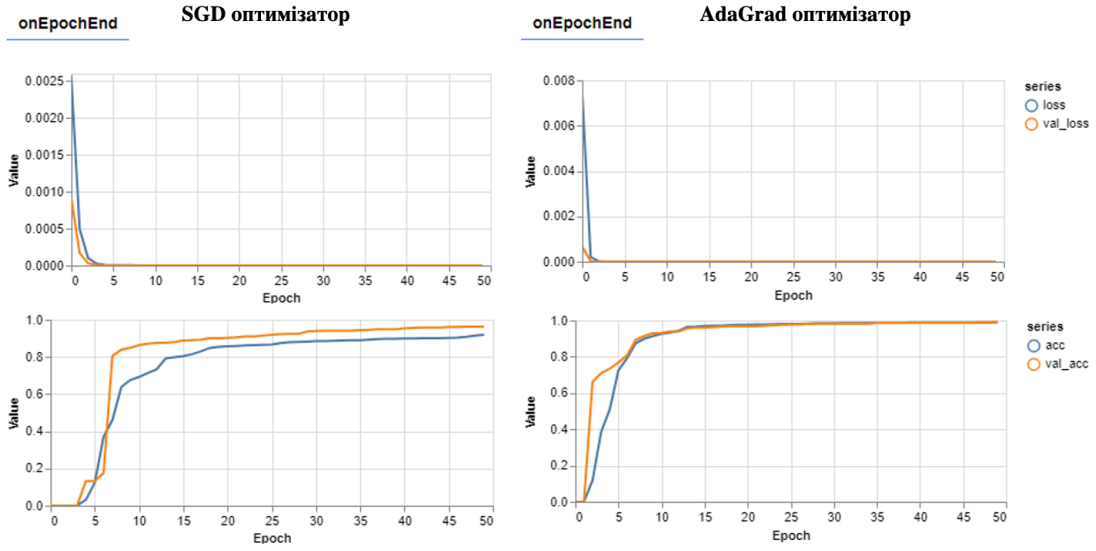

Рис. 4. Візуалізація динаміки процесу навчання наприкінці кожної епохи (on epoch end) для оптимізаторів SGD та AdaGrad

Принципова мета поточного дослідженя полягає в тому, щоб створити модель, яка працює ефективно і дає точні прогнози рівня ризику у визначеному наборі випадків. Щоб досягти цього, різні методи оптимізації машинного навчання застосовувалися в процесі навчання моделі [17].

Порівняння результатів представлено в табл. 2.

Таблиця 2

Порівняння ефективності основних методів оптимізації

Оптимізатор	Epoch 5 Accuracy | Val accuracy	Epoch 25 Accuracy | Val accuracy	Epoch 50 Accuracy | Val accuracy	Загальний час
sgd	0.159456 | 0.160234	0.884319 | 0.911012	0.918838 | 0.963414	5:12 min
adagrad	0.721422 | 0.787231	0.982514 | 0.981453	0.990244 | 0.990243	5:57 min
rmsprop	0.981332 | 0.979383	0.990247 | 0.991711	0.997561 | 0.997560	6:42 min

Наведена вище таблиця демонструє динаміку показника точності для тестового та валідаційного наборів даних на різних етапах навчання. Вона також ілюструє загальний витрачений час для кожного оптимізатора, який знадобився моделі для навчання на 50 епохах. Оптимізатор RMSprop демонструє найкращу точність на рівні 99% для тестового набору даних, проте часові метрики ефективності не є оптимальними. Оптимізатор Adagrad демонструє показник точності на такому ж рівні, але з кращими часовими затратами [18]. Алгоритм SGD потребував найменшого часу для навчання, проте демонструє дещо гірші результати точності (на 3% нижчий показник точності для тестового набору даних, та на 8% — для тренувального). Але щоб досягти точності інших оптимізаторів, SGD потребуватиме більше ітерацій і, отже, час обчислень збільшиться [19]. Окрім цього, проаналізувавши криві навчання можна дійти висновку, що модель на основі SGD оптимізатора демонструє найгіршу динаміку ефективності навчання. Таким чином, з точки зору точності, швидкості та ефективності в подальших дослідженнях варто зосередитися на алгоритмі оптимізації AdaGrad, оскільки він демонструє найвищі показники продуктивності з оптимальними часовими затратами.

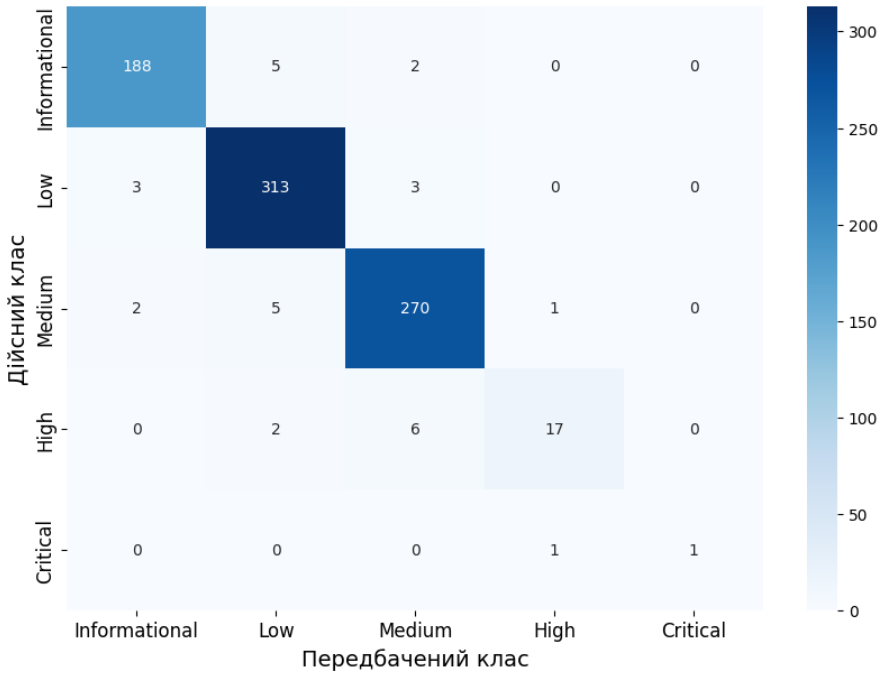

Рис 5. Приклад матриці невідповідностей (confusion matrix) для валідаційного набору даних (оптимізатор SGD)

Окрім цього за результатами моделювання побудовано матрицю невідповідностей (confusion matrix) (рис. 5) і обраховано точність моделі для кожного класу (class accuracy) (табл. 3), щоб візуалізувати продуктивність і ефективність алгоритму класифікації для кожної цільової ознаки тестового набору даних.

Таблиця 3

Показники точності моделі за цільовими класами (class accuracy) для валідаційного набору даних

Цільовий клас	Точність (Val accuracy)	Кількість екземплярів
Informational	0.964102	195
Low	0.981191	319
Medium	0.971223	278
High	0.680000	25
Critical	0.500000	2

Аналіз матриці невідповідностей демонструє, що спроектована модель добре справляється з ідентифікацією широко представлених класів з великою кількістю навчальних екземплярів, проте має проблеми з прогнозуванням значення класів High та Critical, що мають низький рівень репрезентованості в досліджуваному наборі даних. Отже, можна дійти висновку про нерівномірний розподіл даних в представленому датасеті, та висунути гіпотезу про необхідність аналізу та застосування методів додаткового збалансування класів в подальших дослідженнях.

Таким чином, спроектована модель добре підходить для опису реальних процесів аналізу та оцінки ризиків кібербезпеки в розподіленому середовищі, оскільки її точність для всіх методів оптимізації становить понад 95%, проте залишається проблема точності та ефективності ідентифікації найменш представлених класів, що безпосередньо пов’язано із природою та сутністю поняття ризику, та пропонується вирішувати в подальших дослідженнях комплексом технік оверсемплінгу (oversampling) на основі методів SMOTE та ADASYN, та застосуванням вагових коефіцієнтів (class weights).

Для візуалізації процесу навчання та виводу статистичних даних по датасету використано інструментарій бібліотек tfvis та Plotly.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, в рамках даного дослідження запропоновано комплексне та масштабоване рішення для оцінки ризиків інформаційної безпеки в сучасних розподілених системах на основі нейромережевого підходу. Реалізована модель базується на алгоритмі зворотного поширення та дозволяє динамічно аналізувати метадані та метрики про активи розподіленої інформаційної системи, здійснювати попередню обробку цих даних та прогнозувати показник ризику для кожного мережевого активу з достатньою точністю. Незважаючи на гетерогенну природу вхідних даних, результати роботи демонструють відмінні показники продуктивності, і можуть бути рекомендовані для використання в умовах експлуатації сучасних розподілених систем для комплексного аналізу ризиків ІБ, а також оцінки ефективності системи захисту інформації.

Динамічна та комплексна модель, що була розроблена в рамках дослідження має перспективи використання на базі нормалізованих даних агрегованих з різноманітних

систем безпеки корпоративного рівня (до яких можна віднести системи інвентаризації активів та управління інформаційною безпекою, системи журналювання та лог-моніторингу, засоби антивірусного захисту, сканери вразливостей, SIEM та DLP систем тощо), та подальшої інтеграції в програмні комплекси даного роду. Це дозволить забезпечити аналітиків інформаційної безпеки критично важливими даними для вчасного реагування на потенційні інциденти інформаційної безпеки, а також надасть можливість постійного моніторингу профілю можливих загроз.

Результати дослідження доводять, що методи інтелектуальної оцінки ризиків інформаційної безпеки добре підходять для вирішення задач управління ризиками в розподілених середовищах і мають низку переваг порівняно з класичними підходами.

Необхідно зазначити, що розробка системи оцінки ризиків на сьогоднішній день становить важливу задачу для організації будь-якого рівня. Запропонована методика дозволяє ефективно визначити рівень ризиків інформаційної безпеки, що забезпечує можливість їх вивчення, аналізу, прогнозування та подальшого моніторингу, а також вчасного запровадження економічно-доцільних технічних і організаційних заходів безпеки та оцінки ефективності вже існуючих мір.

Важливим аспектом поточного дослідження є теоретичне доведення ефективності застосування нейромережевого підходу на основі алгоритму зворотнього поширення в даній предметній області та практична реалізація моделі оцінки ризиків інформаційної безпеки для систем, що носять розподілений характер, а отже володіють рядом специфічних вимог та характеристик, для аналізу яких використання класичних підходів не є ефективним. Окрім розробленої моделі на базі ряду алгоритмів оптимізації, практичну цінність представляють запропоновані програмні методи попередньої обробки розподілених метаданих та метрик з метою забезпечення їх нормалізації, векторизації та приведення до формату, що підтримується нейронною мережею. Подальші напрямки досліджень передбачають поглиблене вивчення та імплементацію методів оптимізації отриманої моделі, вирішення проблеми дисбалансу класів, а також розширення інструментарію для охоплення та аналізу ширшого діапазону розподілених метрик та даних мережевих активів. Окрім цього, подальші дослідження мають на меті вдосконалення, підвищення ефективності та розширення застосування запропонованого підходу для проектування комплексу нейромережевих моделей оцінки ризику на основі інтелектуального аналізу гетерогенних даних про стан інфраструктури РІС, впровадження механізмів підвищення інтерпретованості результатів, а також подальшої інтеграції розроблених моделей для комплексного оцінювання ризиків кібербезпеки із застосуванням запропонованого адаптивного методу кількісної оцінки [20] та практичної імплементації в рамках існуючих програмних рішень забезпечення ІБ.

Таким чином, можна зробити висновок, що подальший розвиток науково-прикладних досліджень пов’язаних з розробкою методів та моделей оцінки ризиків кібербезпеки в розподілених інформаційних системах на базі інструментарію штучних нейронних мереж є актуальним та перспективним напрямком досліджень на сьогодні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. James, J. (n.d.). *Cebula A Taxonomy of Operational Cyber Security Risks.* Hanscom AFB, MA: Carnegie Mellon University.
2. Palko, D., Hnatienko, H., Babenko, T., & Bigdan, A. (2021). Determining Key Risks for Modern Distributed Information Systems. *IntSol-2021 Intelligent Solutions.*

3. Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences, 13(4),* 2393. https://doi.org/10.3390/app13042393
4. Palko, D., Vialkova, V., & Babenko, T. (2019). Intellectual models for cyber security risk assessment. *Processing, transmission and security of information: Monografia.* Tom 2. Bielsku-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 284–288.
5. Henry, K. (2017). Risk management and analysis. *Information Security Management Handbook*– 6th edition, 321–329.
6. Alberts, C. J. (2018). *Operationally Critical Threat, Asset and Vulnerability Evaluation*.
7. *2022 Global State of Cybersecurity Survey «STATE OF CYBERSECURITY 2022: GLOBAL UPDATE ON WORKFORCE EFFORTS, RESOURCES AND CYBEROPERATIONS»* (2022). ISACA® (www.isaca.org). https://www.isaca.org/state-of-cybersecurity-2022
8. Rot, A. (2008). IT Risk Assessment: Quantitative and Qualitative Approach. *Proceedings of the World Congress on Engineering and Computer Science,* 1073–1078.
9. Palko, D., Babenko, T., Myrutenko, L., & Bigdan, A. (2020). Model of information security critical incident risk assessment. *2020 IEEE International Conference «Problems of infocommunications. Science and technology» PIC S&T'2020*. https://doi.org/10.1109/PICST51311.2020.9468107
10. Haykin, S. (2006). *Neural networks.* W.: Williams.
11. Rassel, S. (2005). *Artificial Intelligence: Modern approach.* W.: Williams.
12. Adebiyi A., Arreymbi, J., & Imafidon, C. (2012). Security Assessment of Software Design using Neural Network. *International Journal of Advanced Research in Artificial Intelligence, 1(4).*
13. *Backpropagation.* (2022). Brilliant.org. https://brilliant.org/wiki/backpropagation/
14. Lee, Z. J., Yang, Z. Y., Lee, C. Y., Chen, Z. H., & BingWu, W. (2021). Using improved neural network for the risk assessment of information security. *IOP Conference Series Materials Science and Engineering, 1113(1),* 012025. https://doi.org/10.1088/1757-899X/1113/1/012025
15. Landoll, D. (2016). *The security risk assessment handbook: a complete guide for performing security risk assessments.* Boca Raton: Auerbach Publications.
16. Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science, 2(3),* 1–16.
17. Ruder, S. (2016). *An overview of gradient descent optimization algorithms*. arXiv preprint arXiv:1609.04747.
18. Zhang, Z. (2018). Improved adam optimizer for deep neural networks. *2018 IEEE/ACM 26th international symposium on quality of service (IWQoS).*
19. Wilson, A. C, Roelofs, R., Stern, M., Srebro, N., & Recht, B. (2017). The Marginal Value of Adaptive Gradient Methods in Machine Learning. *31st International Conference on Neural Information Processing Systems,* 4151–4161.
20. Palko, D., & Myrutenko, L. (2024). Method of comprehensive cybersecurity risks assessment in distributed information systems. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(26),* 487–502. https://doi.org/10.28925/2663-4023.2024.26.731

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Dmytro Palko
Postgraduate Student of the Department of Cybersecurity and Information Protection
Faculty of Information Technologies
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0002-2886-1975
palko.dmytro@gmail.com

INTELLIGENT RISK ASSESSMENT MODELS IN DISTRIBUTED SYSTEMS BASED ON THE NEURAL NETWORK APPROACH

Abstract. In modern conditions of information systems functioning, the rapid growth of scale, complexity and distribution of computing resources is becoming one of the defining trends in the development of digital infrastructure. Within the framework of the widespread implementation of complex multi-component information systems that are distributed in nature and contain a large number of nodes, as well as a significant increase in the number and complexity of cyber threats focused on scalable systems, cybersecurity risks should be considered as a key factor in strategic planning of business processes. Regular analysis and assessment of cybersecurity risks allows determining the necessary and sufficient set of information protection tools, regulatory and organizational mechanisms to reduce information security threats, and ensures the process of building the most effective architecture of a comprehensive information security management system. Existing tools and assessment methodologies, which are mostly conceptual in nature and based on statistical approaches, are ineffective in analysis of large arrays of high-dimensional heterogeneous data and metrics of distributed systems. The article focuses on the current trends and existing approaches to information security risk assessment in distributed information systems. It analyzes the importance of risk management in the process of ensuring information security, and also describes a core principles of intelligent security risk assessment in distributed information systems based on the neural network approach. Research also presents a dynamic and comprehensive model of cyber risk assessment in distributed information systems based on back propagation neural network architecture and several methods of its optimization, which provides sufficient accuracy and reliability of risk assessment in the conditions of analysis of large arrays of heterogeneous input data.

Keywords: information security; cybersecurity; cybersecurity risk; risk assessment; risk modeling; intelligent assessment models; risk management; distributed information system; neural network; security metrics; metadata; information asset.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. James, J. (n.d.). *Cebula A Taxonomy of Operational Cyber Security Risks*. Hanscom AFB, MA: Carnegie Mellon University.
2. Palko, D., Hnatienko, H., Babenko, T., & Bigdan, A. (2021). Determining Key Risks for Modern Distributed Information Systems. *IntSol-2021 Intelligent Solutions.*
3. Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences, 13(4),* 2393. https://doi.org/10.3390/app13042393
4. Palko, D., Vialkova, V., & Babenko, T. (2019). Intellectual models for cyber security risk assessment. *Processing, transmission and security of information: Monografia.* Tom 2. Bielsku-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 284–288.
5. Henry, K. (2017). Risk management and analysis. *Information Security Management Handbook*– 6th edition, 321–329.
6. Alberts, C. J. (2018). *Operationally Critical Threat, Asset and Vulnerability Evaluation*.
7. *2022 Global State of Cybersecurity Survey «STATE OF CYBERSECURITY 2022: GLOBAL UPDATE ON WORKFORCE EFFORTS, RESOURCES AND CYBEROPERATIONS»* (2022). ISACA® (www.isaca.org). https://www.isaca.org/state-of-cybersecurity-2022

8. Rot, A. (2008). IT Risk Assessment: Quantitative and Qualitative Approach. *Proceedings of the World Congress on Engineering and Computer Science*, 1073–1078.
9. Palko, D., Babenko, T., Myrutenko, L., & Bigdan, A. (2020). Model of information security critical incident risk assessment. *2020 IEEE International Conference «Problems of infocommunications. Science and technology» PIC S&T'2020*. https://doi.org/10.1109/PICST51311.2020.9468107
10. Haykin, S. (2006). *Neural networks*. W.: Williams.
11. Rassel, S. (2005). *Artificial Intelligence: Modern approach*. W.: Williams.
12. Adebiyi A., Arreymbi, J., & Imafidon, C. (2012). Security Assessment of Software Design using Neural Network. *International Journal of Advanced Research in Artificial Intelligence, 1(4).*
13. *Backpropagation.* (2022). Brilliant.org. https://brilliant.org/wiki/backpropagation/
14. Lee, Z. J., Yang, Z. Y., Lee, C. Y., Chen, Z. H., & BingWu, W. (2021). Using improved neural network for the risk assessment of information security. *IOP Conference Series Materials Science and Engineering, 1113(1),* 012025. https://doi.org/10.1088/1757-899X/1113/1/012025
15. Landoll, D. (2016). *The security risk assessment handbook: a complete guide for performing security risk assessments.* Boca Raton: Auerbach Publications.
16. Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science, 2(3),* 1–16.
17. Ruder, S. (2016). *An overview of gradient descent optimization algorithms*. arXiv preprint arXiv:1609.04747.
18. Zhang, Z. (2018). Improved adam optimizer for deep neural networks. *2018 IEEE/ACM 26th international symposium on quality of service (IWQoS).*
19. Wilson, A. C, Roelofs, R., Stern, M., Srebro, N., & Recht, B. (2017). The Marginal Value of Adaptive Gradient Methods in Machine Learning. *31st International Conference on Neural Information Processing Systems,* 4151–4161.
20. Palko, D., & Myrutenko, L. (2024). Method of comprehensive cybersecurity risks assessment in distributed information systems. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(26),* 487–502. https://doi.org/10.28925/2663-4023.2024.26.731