МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені Тараса Шевченка

Кваліфікаційна наукова праця

на правах рукопису

**ПАЛКО ДМИТРО ВОЛОДИМИРОВИЧ**

УДК 004.056+004.057.2+004.75:004.85/.89:681.5(043.3)

**ДИСЕРТАЦІЯ**

# АДАПТИВНИЙ МЕТОД ТА МОДЕЛІ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

125 – Кібербезпека

Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Палко Д.В.

Науковий керівник

Мирутенко Лариса Вікторівна,

кандидат технічних наук, доцент

Київ – 2025

# АНОТАЦІЯ

**Палко Д.В. Адаптивний метод та моделі оцінювання ризиків кібербезпеки у розподілених інформаційних системах.** Кваліфікаційна наукова праця на правах рукопису.

*Дисертація на здобуття наукового ступеня доктора філософії в галузі інформаційних технологій за спеціальністю 125 «Кібербезпека». Київський національний університет імені Тараса Шевченка, Факультет інформаційних технологій, Кафедра кібербезпеки та захисту інформації, Київ, 2025.*

Дисертаційна робота присвячена вирішенню актуального **науково-прикладного завдання**, що полягає в підвищенні ефективності процесу оцінювання ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем (РІС).

На сьогоднішній день стрімке зростання розподіленості обчислювальних ресурсів стає однією з визначальних тенденцій розвитку цифрової інфраструктури, а забезпечення кіберстійкості РІС набуває пріоритетного значення. Підвищена складність управління ризиками інформаційної безпеки (ІБ) у розподілених середовищах через децентралізовану структуру та динамічний характер РІС, різнорідність обладнання та інфраструктури, широкий спектр наявних загроз, а також обмеженість класичних методів, що не враховують раніше невідомі типи атак, передбачають високу суб’єктивність, ресурсоємність і складність практичної імплементації в умовах масштабованих розподілених систем, вимагають розробки більш гнучких та адаптивних підходів до оцінювання ризиків кібербезпеки розподіленого середовища.

Суттєва обмеженість та ряд принципових недоліків існуючих стандартів та методологій, акцент на загальних та концептуальних аспектах оцінювання, брак узгодженості та низька інтегрованість між різними підходами**,** що фрагментарно оцінюють окремі аспекти безпеки, не забезпечуючи комплексного аналізу, а також складність оперативної обробки великих масивів різнорідних за природою походження та форматом представлення даних РІС підкреслюють необхідність розробки практичного інструментарію на основі уніфікованих моделей для

комплексного оцінювання ризиків, що забезпечить оперативність, гнучкість та адаптивність аналізу в умовах невизначеності та динамічності сучасних розподілених інформаційних систем.

В рамках дослідження **запропоновано** комплексний підхід до оцінювання ризиків кібербезпеки розподілених систем на основі синтезу метрико-орієнтованого та стандарт-орієнтованого принципів оцінки, та розроблено ряд нейромережевих моделей багатофакторного аналізу великих масивів складних гетерогенних даних та безпекових метрик про стан інформаційних активів інфраструктури РІС, агрегованих в процесі їх моніторингу, з однієї сторони, та показників контролю відповідності нормативно-правовій базі і вимогам провідних стандартів ІБ з іншої.

Відповідно до поставленої мети та сформульованих задач дослідження в рамках **першого розділу** дисертаційної роботи здійснено аналіз основних тенденцій розвитку сучасних РІС, проведено дослідження теоретичних та науково-методологічних аспектів оцінювання ризиків кібербезпеки в розподілених системах, виконано аналіз публікацій, методологій та провідних стандартів з ризик-менеджменту, що сприяло виявленню наявних прогалин в теорії та практиці управління ризиками розподіленого середовища РІС. Суттєва обмеженість класичних методів, а також відсутність універсальних та ефективних підходів до оцінювання ризиків в динамічних та масштабованих розподілених системах доводять актуальність обраного наукового завдання.

У **другому розділі** вдосконалено метод побудови профілю ключових факторів ризику сучасних РІС за допомогою інструментарію математичної статистики, ідентифіковано основні чинники ризику, проведено кореляційний аналіз та дослідження їх взаємозв’язків, а також визначено та структуровано основні заходи та контролі інформаційної безпеки, що демонструють найкращі показники ефективності в умовах розподіленості середовища. Запропонований підхід до виокремлення найбільш вагомих факторів ризику та оптимізації вибору вхідного набору ознак забезпечив покращення на 4% загальних показників точності класифікації для проєктованих моделей багатокритеріального аналізу гетерогенних даних РІС на основі штучних нейронних мереж, що були розроблені на наступному етапі.

Емпірично доведено ефективність використання парадигми глибоких нейронних мереж в задачах машинного аналізу ключових індикаторів безпеки розподіленого середовища – побудовано комплекс нейромережевих моделей оцінювання ризиків ІБ в розподілених інформаційних системах з кращими показниками зважених середніх значень точності (на рівні 94%), F1-міри та AUC-ROC; проведено порівняння їх якісних характеристик при вирішенні задач класифікації, в тому числі в залежності від ступеня інформаційної наповненості та міри повноти вхідних даних, що підтверджує ефективність запропонованих моделей багатокритеріального аналізу гетерогенних даних розподіленого середовища щодо масштабування, адаптації під різноманітні топології РІС та динамічні умови розподіленого середовища.

В рамках **третього розділу** продовжено розробку ряду моделей оцінювання ризиків РІС на основі контролю відповідності вимогам провідних стандартів ІБ. Для цього здійснено аналіз та формалізацію технологічних актив-орієнтованих вимог та контролів безпеки провідних міжнародних та національних стандартів ІБ (ISO 27001, ISO 27002, PCI DSS v4, SWIFT, NBU-95), як багатовимірних вхідних метрик, сумісних з інструментами машинного навчання (ML), що дозволяє врахувати кращі світові практики, забезпечити інтероперабельність, відповідність вимогам регуляторів, а також сприяє підвищенню зрілості процесів кібербезпеки. Окрім цього, проведено аналіз теоретико-методологічних принципів застосування алгоритмів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж для вирішення задач підвищення ефективності процесу оцінювання ризиків кібербезпеки в розподілених системах та покращення точності прийнятих управлінських рішень. Здійснено SWOT-аналіз основних підходів до моделювання на основі алгоритмів машинного навчання та порівняльний аналіз програмних фреймворків, в результаті чого обрано необхідний інструментарій для проведення емпіричної частини дослідження. Емпірична перевірка стандарт-орієнтованого підходу в рамках експериментальних досліджень продемонструвала чудові якісні характеристики проєктованих моделей із середнім показником точності 90,75% та підтвердила їх здатність гнучко аналізувати рівень ризику на основі даних контролю відповідності вимогам регулюючих нормативно-правових актів, що є критично

важливим для ефективного управління безпекою сучасних РІС. На останньому етапі дослідження запропоновано універсальний адаптивний метод комплексного кількісного оцінювання ризиків кібербезпеки в РІС з використанням спроєктованих моделей та загальної системи оцінки вразливостей, що на відміну від класичного підходу враховує динамічний характер розподіленого середовища, забезпечує гнучкий підхід до процесу оцінювання та просту практичну імплементацію, а також дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних. Комплексне застосування та синтез результатів декількох моделей, що фрагментарно оцінюють окремі домени безпеки, забезпечує ґрунтовний системний підхід до аналізу стану ІБ, враховуючи всі фактори та аспекти функціонування РІС, аналізуючи всі доступні дані та об’єднуючи їх результати в єдиному аналітичному середовищі.

У **Висновках** викладено основний зміст отриманих наукових результатів. Запропонований підхід на основі багатофакторного нейромережевого аналізу універсальних стандартизованих метрик та індикаторів безпеки розподілених систем, що враховує не лише технічні аспекти функціонування сучасних розподілених інфраструктур, а й показники відповідності вимогам регуляторів, дозволяє забезпечити комплексний, гнучкий та адаптивний аналіз безпекової ситуації, та надає можливість підвищення ефективності процесу оцінювання ризиків в умовах динамічних змін інформаційної інфраструктури сучасних масштабованих розподілених систем.

**Ключові слова**: кібербезпека; ризик кібербезпеки; розподілена інформаційна система; розподілене середовище; мережева безпека; оцінювання ризиків; управління ризиками; загрози; вразливості; CVSS; інформаційна система; модель; машинне навчання; нейронна мережа; глибинне навчання.

# ABSTRACT

*Dmytro Palko.* Adaptive method and models for cybersecurity risk assessment in distributed information systems. – Scientific qualification work as a manuscript.

Dissertation on the achievement of the Doctor of Philosophy scientific level, Specialty 125 – Cybersecurity – Taras Shevchenko National University of Kyiv, 2025.

This dissertation addresses a pressing scientific and applied challenge – enhancing the effectiveness of cybersecurity risk assessment in the dynamic environment of modern scalable distributed information systems (DIS).

In today's digital landscape, the rapid expansion of distributed computing resources has become a defining trend in infrastructure development, making the cybersecurity resilience of DIS a critical priority. The increasing complexity of risk management in distributed environments – driven by their decentralized nature, heterogeneous infrastructure, dynamic topology, a broad spectrum of threats, and the limitations of classical approaches incapable of addressing previously unknown attack vectors, highly subjective, resource-intensive, and impractical for large-scale implementation – necessitates the development of more flexible and adaptive approaches to risk assessment tailored for distributed environments.

The significant limitations and fundamental flaws of current standards and methodologies – such as their focus on general conceptual aspects, lack of interoperability, and low integration between fragmented assessment methods – fail to provide comprehensive risk analysis. Moreover, the challenge of promptly processing vast volumes of heterogeneous data inherent to DIS further emphasizes the need for practical tools based on unified models capable of delivering comprehensive, real-time, flexible, and adaptive cybersecurity risk assessment under uncertainty and dynamic conditions.

This research proposes a comprehensive approach to cybersecurity risk assessment in distributed systems based on the synthesis of metric-oriented and standard-oriented evaluation principles. A set of neural network models was developed to enable multifactor analysis of large-scale, heterogeneous datasets and security metrics reflecting the state of DIS information assets aggregated during monitoring, on the one hand, and provide

compliance indicators analysis, aligned with legal regulations and leading cybersecurity standards, on the other hand.

In accordance with the research objectives, Chapter 1 analyzes key trends in the development of modern DIS and examines the theoretical and methodological foundations of cybersecurity risk assessment in distributed environments. A thorough review of the literature, methodologies, and leading risk management standards revealed gaps in the theory and practice of distributed environment risk management. The limitations of classical methods and the lack of universal, effective approaches for assessing risk in dynamic, scalable distributed systems underline the relevance of the chosen research problem.

Chapter 2 enhances the method for constructing risk factor profile for modern DIS using mathematical statistics. Key risk factors were identified, correlations analyzed, and their interrelations studied. Security controls with the highest efficiency in distributed environments were also determined and structured. The proposed approach to identifying the most influential risk factors and optimizing the feature selection process improved classification accuracy by 4% in the developed multi-criteria neural models for analyzing heterogeneous DIS data. The empirical results confirm the effectiveness of deep neural network paradigms in machine analysis of key security indicators in distributed environments. A suite of neural network models for cybersecurity risk assessment in DIS was created, achieving superior performance with average weighted accuracy of 94%, high F1-scores, and AUC-ROC values. A detailed comparison of these models' performance across varying data completeness and informational richness further confirmed their scalability and adaptability to diverse DIS topologies and dynamic conditions.

Chapter 3 extends the research by developing models that assess DIS risks through compliance with leading cybersecurity standards. Security requirements and controls from internationally recognized standards (ISO 27001, ISO 27002, PCI DSS v4, SWIFT, NBU-95) were formalized as multi-dimensional input metrics compatible with machine learning algorithms. This enabled the incorporation of global best practices, ensured interoperability, regulatory compliance, and improved cybersecurity process maturity. Theoretical and methodological foundations of data mining, machine learning, and deep neural networks were analyzed for enhancing risk assessment and decision-making accuracy in distributed

environments. A SWOT analysis of major ML-based modeling approaches and a comparative evaluation of software frameworks led to the selection of appropriate tools for empirical experiments. The standard-oriented approach demonstrated excellent results in experimental settings, with an average classification accuracy of 90,75%, confirming its flexibility in evaluating risk levels based on regulatory compliance data – an essential aspect of effective DIS security management. The final stage of the research presents a universal adaptive method for comprehensive quantitative cybersecurity risk assessment in DIS, which integrates the developed models results with vulnerabilities assessment based on unified common vulnerability scoring system. Unlike traditional approaches, it accounts for the dynamic nature of distributed environments, enabling flexible evaluation, simple implementation, and automated risk score calculation under uncertainty and large-scale heterogeneous data. The combined use and synthesis of results from multiple models – each assessing specific security domains – ensure a robust, systemic approach to analyzing the cybersecurity posture of DIS. It processes all available data and aggregates findings within a unified analytical environment.

Conclusions summarize the main scientific contributions. The proposed approach, based on multifactor neural analysis of standardized security metrics and indicators for distributed systems, addresses both technical and compliance-related aspects. It enables comprehensive, flexible, and adaptive risk assessment and improves the overall effectiveness of cybersecurity risk evaluation in modern scalable distributed environments.

Keywords: cybersecurity; cybersecurity risk; distributed information system; distributed environment; network security; risk assessment; risk management; threats; vulnerabilities; CVSS; information system; model; machine learning; neural network; deep learning.

## Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

### Статті у вітчизняних фахових виданнях і міжнародних журналах

1. Palko, D.; Babenko, T.; Bigdan, A.; Kiktev, N.; Hutsol, T.; Kuboń, M.; Hnatiienko, H.; Tabor, S.; Gorbovy, O.; Borusiewicz, A. Cyber Security Risk Modeling in Distributed Information Systems. Appl. Sci. 2023, 13, 2393. DOI: https://doi.org/10.3390/app13042393 **[індексація в наукометричній базі SCOPUS, наукове періодичне видання віднесене до першого-третього квартилів (Q1 – Q3) відповідно до класифікації SCImago Journal and Country Rank / Journal Citation Reports]**
2. Д.В. Палко, Л.В. Мирутенко «Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах», Кібербезпека: освіта, наука, техніка, Том 2 № 26 (2024), с. 487 – 502. DOI: https://doi.org/10.28925/2663-4023.2024.26.731
3. Д.В. Палко «Інтелектуальні моделі оцінки ризиків кібербезпеки в розподілених системах на основі нейромережевого підходу», Кібербезпека: освіта, наука, техніка, Том 3 № 27 (2025), с. 429 – 448. DOI: https://doi.org/10.28925/2663-4023.2025.27.764
4. Д.В. Палко, Л.В. Мирутенко «Метод побудови профілю ключових факторів ризику кібербезпеки сучасних розподілених інформаційних систем», Захист інформації, Том 26, № 2, липень-грудень 2024, с. 236 – 252. DOI: https://doi.org/10.18372/2410-7840.26.20014
5. Д. Палко, Л. Мирутенко, О. Шайна «Протоколи безпеки в кіберфізичних системах», Безпека інформаційних систем і технологій («Information systems and technologies security»), № 2(8)/2024, с. 66 – 73. DOI: https://doi.org/10.17721/ISTS.2024.8.66-73

### Наукові праці, які засвідчують апробацію матеріалів дисертації

1. Dmitry Palko, Tetiana Babenko, Larysa Myrutenko, Andrii Bigdan «Model of information security critical incident risk assessment» // Proceedings of the 2020 IEEE International Conference «Problems of infocommunications. Science and technology» PIC S&T′2020, pp. 157–161, 6-9 October 2020, Kharkiv, Ukraine DOI:

https://doi.org/10.1109/PICST51311.2020.9468107 **[індексація в наукометричній базі SCOPUS]**

2. Dmytro Palko, Hrygorii Hnatienko, Tetiana Babenko, Andrii Bigdan «Determining Key Risks for Modern Distributed Information Systems» // IntSol-2021 Intelligent Solutions - CEUR Workshop Proceedings, Volume 3018, pp. 81–100, 28–30 September 2021, Kyiv, Ukraine **[індексація в наукометричній базі SCOPUS]**

3. Dmytro Palko, Tetiana Babenko, Larysa Myrutenko, Andrii Bigdan «Intelligent risk assessment models in DIS based on the neural network approach» // IX International conference «Information Technology and Implementation (Satellite)» (IT&I-2022), ISBN 978-966-969-154-5 (e-book), pp. 118–120, 1 December, 2022, Kyiv, Ukraine

4. Dmytro Palko, Tetiana Babenko «Evaluation of key risk factors for modern distributed information systems» // V Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) 27-28 жовтня 2022 року

5. Dmytro Palko, Tetiana Babenko «Risk Assessment Driven Use Of Advanced Intelligent Solutions Approach In Modern Distributed Systems» // VI Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) 27 квітня 2023 року

6. Dmytro Palko, Tetiana Babenko, Hnatiienko Hryhorii, Larysa Myrutenko and Andrii Bigdan «Intelligent risk assessment models in distributed systems based on the neural network approach» // Next Generation Cybersecurity Systems and Applications NGSEC (NGSEC-2023) Conference Proceedings, 26-27 April, 2023, Kyiv, Ukraine

7. Dmytro Palko, Kateryna Mokliakova, Tetiana Babenko «Cybersecurity level assessment models» // Next Generation Cybersecurity Systems and Applications NGSEC (NGSEC-2023) Conference Proceedings, 26-27 April, 2023, Kyiv, Ukraine

8. Dmytro Palko, Vira Vialkova, Tetiana Babenko «Intellectual models for cyber security risk assessment» // Processing, transmission and security of information : Monografia. Tom 2. / Akademia Techniczno-Humanistyczna w Bielsku-Białej. –Bielsku-Biała : Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2019. – S. 284–288.

9. Д.В. Палко, Л.В. Мирутенко, В.І. Вялкова «Захист інформаційних ресурсів та транзакцій в корпоративних мережах» // І Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS), 5-6 квітня 2018 року, с. 268-272

10. Д. Палко, Т. Бабенко, Л. Мирутенко «Інтелектуальні моделі оцінки ризиків кібербезпеки» // ІІІ Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS). – 2020. – 4 с.

11. Д.В. Палко «Моделі інтелектуального аналізу кіберризиків у масштабованих розподілених середовищах» // VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем» (CPICS), 11 квітня 2025 року, – 4 с.

**ЗМІСТ**

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

| | | |
|---|---|---|
| AI | – | Artificial Intelligence |
| ANN | – | Artificial Neural Network |
| CPU | – | Central Processing Unit |
| CRAMM | – | CCTA Risk Analysis and Managment Method |
| CVSS | – | Common Vulnerability Scoring System |
| DDOS | – | Distributed Denial of Service Attack |
| DOS | – | Denial of Service Attack |
| FAIR | – | Factor Analysis of Information Risk |
| GANs | – | Generative Adversarial Network |
| GPU | – | Graphics Processing Unit |
| IEC | – | International Electrotechnical Commission |
| IoT | | Internet of Things |
| IRAM | – | Information Risk Analysis Methodology |
| ISACA | – | Information Systems Audit and Control Association |
| ISO | – | International Organization for Standardization |
| KNN | – | K-Nearest Neighbors Algorithm |
| LDA | – | Linear Discriminant Analysis |
| MEHARI | – | Method for Harmonized Analysis of Risk |
| MITRE ATT&CK | – | Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations |
| MLP | – | MultiLayer Perceptron |
| NIST | – | National Institute of Standards and Technology |
| OCTAVE | – | Operationally Critical Threats, Assets and Vulnerability Evaluation |
| PCA | – | Principal Component Analysis |
| PDCA | – | Plan-Do-Check-Act |
| SIEM | – | Security Information and Event Management |
| SMOTE | – | Synthetic Minority Oversampling Technique |

| | | |
|---|---|---|
| SVM | – | Support Vector Machine |
| SWOT | – | Strengths, Weaknesses, Opportunities, and Threats Analysis |
| БД | – | База даних |
| ІА | – | Інформаційний актив |
| ГНМ | – | Глибока нейронна мережа |
| ІБ | – | Інформаційна безпека |
| ІС | – | Інформаційна система |
| МН | – | Машинне навчання |
| НСД | – | Несанкціонований доступ |
| ПЗ | – | Програмне забезпечення |
| РІС | – | Розподілена інформаційна система |
| СМІБ | – | Система менеджменту інформаційної безпеки |
| ШНМ | – | Штучна нейронна мережа |

# ВСТУП

**Актуальність теми.** У сучасному цифровому середовищі розподілені інформаційні системи (РІС) стають фундаментом діяльності більшості організацій, забезпечуючи доступність критичних сервісів, обробку великих обсягів даних та інтеграцію широкого спектру інформаційних активів, роззосереджених у просторі. Стрімкий розвиток цифрових технологій та постійне розширення архітектури розподілених інформаційних систем зумовлює високу складність керування їх безпекою. Різнорідність обладнання, динамічні мережеві топології, використання хмарних платформ, мікросервісних архітектур та широка диференціація різновидів інформаційних активів значно ускладнюють завдання оцінювання ризиків інформаційної безпеки (ІБ). Окрім цього, організація аналізу ризиків кібербезпеки в розподілених системах передбачає вирішення комплексу задач пов’язаних з функціональною розподіленістю та ієрархічністю, високим ступенем розпаралелювання ресурсів і практично повною відсутність централізованого управління.

Варто зауважити, що національний сегмент розподілених інформаційних систем функціонує в умовах додаткового тиску, спричиненого російсько-українською війною. Збройний конфлікт, що розпочався у 2014 році, у лютому 2022 року перейшов у повномасштабне вторгнення, суттєво посиливши загрози для інформаційної інфраструктури. Масовані кібератаки з боку держави-агресора спрямовані на дестабілізацію роботи критичної інфраструктури, порушення функціонування комунікаційних каналів, зрив постачання послуг та компрометацію даних.

Водночас, у глобальному контексті пандемія COVID-19 (пандемія коронавірусу) суттєво вплинула на характер і структуру інформаційних потоків, спричинила масовий перехід до віддаленої роботи, розширення використання хмарних сервісів та збільшення кількості кіберзагроз. 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 оцінювання.

Традиційні підходи до аналізу та управління ризиками інформаційної безпеки, засновані переважно на статичних моделях та методах експертних оцінок, виявляють низку обмежень у масштабованому та динамічному середовищі РІС і підкреслюють ряд важливих науково-прикладних проблем:

- Неповнота та невизначеність даних: Розподілені системи генерують величезні обсяги високорозмірних гетерогенних даних та метрик про стан різних компонентів та активів, значна частина яких є неповною, неточною або неоднорідною за структурою та форматом. Класичні підходи не завжди здатні ефективно аналізувати такі дані, що призводить до неточностей у прогнозуванні рівня ризику.
- Складність і нелінійність взаємозв'язків між факторами ризику: Через відсутність гнучких механізмів виявлення прихованих патернів і закономірностей традиційні аналітичні методи часто не здатні адекватно врахувати нелінійні залежності, складні кореляції та причинно-наслідкові зв'язки між факторами ризику й зазвичай втрачають частину релевантної інформації, недооцінюючи значущість окремих чинників.
- Недостатня адаптивність та реактивність: Класичні підходи до оцінювання ризику не враховують динамічний характер змін у РІС, потребують ручного оновлення, постійних експертних втручань та не забезпечують оперативного корегування оцінок у режимі часу, близькому до реального.

Окрім цього, проблемними питаннями оцінювання ризиків в контексті РІС є необхідність оперативного аналізу великих масивів складних за структурою та гетерогенних за природою вхідних даних, що надходять із різних систем безпеки та моніторингу, журналів подій, аудиторських звітів та інших джерел, а також важливість урахування аспектів нормативно-правового регулювання та відповідності вимогам провідних стандартів інформаційної безпеки.

Таким чином, діючі підходи до оцінювання ризиків інформаційної безпеки не в змозі повною мірою створити умови для забезпечення ефективного процесу ризик-менеджменту з урахуванням сучасних вимог та реалій функціонування розподілених середовищ. Зростання складності РІС і підвищення ролі інформаційної безпеки у стратегічному розвитку організацій вимагають нових методів аналізу ризиків, здатних

оперативно реагувати на динамічні зміни оточення і забезпечувати високий рівень точності та надійності прогнозів, долаючи обмеження класичних підходів.

Науково-прикладна актуальність дослідження визначається нагальною потребою у створенні методологічних та технологічних рішень, які здатні підвищити ефективність, достовірність та динамічність процесу оцінювання інформаційних ризиків у розподілених системах. Запропонований підхід на основі застосування нейромережевої парадигми створює умови для переходу від статичних, експертно-орієнтованих моделей до гнучких та самоадаптивних систем, що використовують інструменти машинного навчання та інтелектуального аналізу даних, покращуючи здатність організацій протидіяти сучасним кіберзагрозам, забезпечуючи сталий розвиток у цифровому середовищі та безперервне підвищення зрілості у сфері ІБ.

Організація системи інтелектуального аналізу великих масивів гетерогенних та розподілених метаданих, які відображають стан мережевої інфраструктури, ефективність засобів забезпечення безпеки та рівень відповідності нормативно-правовим вимогам, повинна передбачати одночасне вирішення завдань зменшення часу реагування та аналітичної обробки інформації із забезпеченням високої точності прогнозування рівня ризику враховуючи специфіку масштабованих РІС, що пропонується вирішити на основі використання парадигми штучних нейронних мереж. Застосування методів інтелектуального аналізу даних, машинного навчання (МН) та глибоких нейронних мереж (ГНМ) забезпечує ефективну інтеграцію гетерогенних та високорозмірних даних із різних джерел, виявлення прихованих закономірностей, динамічну адаптацію до змін у середовищі, а також підвищення точності в розв’язанні задач класифікації рівня ризику. Основною перевагою запропонованого підходу є здатність нейронних мереж до нелінійного моделювання складних взаємозв’язків, потенціал до обробки великих обсягів даних, а також здатність до масштабування у відповідь на надходження нових вхідних даних, зміни топології, конфігурації інфраструктури чи появу нових загроз, що створює передумови для побудови більш адаптивних прогностичних систем ризик-менеджменту. Нейромережеві моделі можуть бути перенавчені або оновлені в режимі реального часу, що сприяє підвищенню стійкості та адаптивності рішення.

З огляду на вищезазначене, у дисертаційній роботі досліджувались ключові аспекти забезпечення безпеки та ризик-менеджменту в розподілених інформаційних системах, а також вирішувалась прикладна задача з розробки та імплементації моделей оцінювання ризику на основі алгоритмів машинного навчання та глибоких нейронних мереж з метою побудови комплексного підходу, що поєднує аспекти оцінювання ризику на основі багатокритеріального аналізу розподілених метрик про роботу інформаційних активів та контролю відповідності вимогам стандартів ІБ, забезпечує високий рівень точності аналізу з мінімальними часовими затратами та навантаженням на обчислювальні ресурси.

На основі проведених досліджень можна зробити висновок, що розробка методів та моделей оцінювання ризику в розподілених системах з використанням інструментарію інтелектуального аналізу даних та штучних нейронних мереж **складає актуальне науково-прикладне завдання**.

Розробка наукових і методологічних принципів комплексного підходу до оцінювання ризиків кібербезпеки в РІС була заснована на дослідженнях вітчизняних та зарубіжних вчених. Зокрема питаннями дослідження проблем забезпечення кібербезпеки в розподілених інформаційних системах, а також основних аспектів оцінювання ризиків ІБ для розподілених середовищ 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), Юджин Спаффорд (Eugene Spafford), Фред Шнайдер (Fred B. Schneider), Кліффорд Ньюман (Clifford Neuman). Серед вітчизняних дослідників можна виокремити внесок В.А. Заславського, А.Б. Качинського, О.А. Машкова, О.В. Барабаша, О.В. Потія, С.Ф. Гончара, О.Г. Корченка, Ю.В. Кравченка, Н.В. Лукової-Чуйко, О.А. Кононова, В.А. Савченка, Д.М. Обідіна, О.А. Замули, В.О. Хорошко, В.П. Широчина, Л.В. Загоруйко тощо.

**Зв’язок роботи з науковими програмами, планами, темами.** Дисертаційне дослідження виконано відповідно до поточних та перспективних планів науково-дослідної діяльності кафедри кібербезпеки та захисту інформації, факультету інформаційних технологій Київського національного університету імені Тараса

Шевченка. Автор приймав участь у науково-дослідних роботах: «Дослідження та розробка моделей, методів і засобів захисту від кібератак в інформаційних системах та мережах» №16 КП 064-03 (номер державної реєстрації НДР: 0116U007996), «Методи та моделі захисту персональних даних з урахуванням специфіки соціальних мереж» (номер державної реєстрації НДР: 0121U113248).

**Мета і завдання дослідження.** Метою роботи є підвищення ефективності процесу оцінювання ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем.

Розробка і наукове обґрунтування нових методологічних та практичних принципів оцінювання ризиків кібербезпеки в розподілених інформаційних системах із застосуванням методів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж на основі врахування багатокритеріального аналізу розподілених метрик про роботу інформаційних активів та контролю відповідності вимогам провідних стандартів ІБ, дозволить підвищити точність, адаптивність і надійність процесу управління ризиками в масштабованих динамічних середовищах.

Для досягнення мети дослідження в дисертаційній роботі вирішені наступні завдання:

- проведено комплексний аналіз сучасних підходів та методологій оцінювання ризиків кібербезпеки у РІС, визначено їх сильні та слабкі сторони, а також окреслено наявні прогалини в теорії та практиці управління ризиками;
- вдосконалено метод побудови профілю ключових факторів ризику, що можуть спричинити потенційні інциденти ІБ в умовах фізичної та функціональної розподіленості ресурсів, а також основних контролів безпеки сучасних РІС, досліджено показники їх статистичної важливості та кореляції, з метою оптимізації вибору ознак і підвищення точності та надійності проєктованих моделей;
- узагальнено теоретико-методологічні аспекти застосування алгоритмів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж для вирішення задач підвищення ефективності процесу ризик-менеджменту в РІС та покращення точності прийнятих управлінських рішень;

- обґрунтовано концептуальну методику оцінювання ризиків ІБ із врахуванням комплексного підходу на основі синтезу методів обробки та аналізу великих обсягів гетерогенних даних про стан інфраструктури РІС з однієї сторони, та контролю відповідності нормативно-правовій базі та вимогам провідних стандартів ІБ з іншої;
- здійснено аналіз та формалізацію технологічних актив-орієнтованих вимог та контролів безпеки провідних міжнародних та національних стандартів ІБ (ISO 27001, ISO 27002, PCI DSS v4, SWIFT, NBU-95 тощо);
- побудовано комплекс нейромережевих моделей прогнозування рівня ризику ІБ в розподіленому середовищі для вищеописаних підходів;
- здійснено порівняльну оцінку розроблених нейромережевих моделей та класичних алгоритмів машинного навчання за характеристиками точності та ефективності при вирішенні задач класифікації;
- розроблено адаптивний метод комплексного кількісного оцінювання ризиків кібербезпеки в РІС з використанням спроєктованих моделей.

**Об’єктом дослідження** є процес оцінювання ризиків кібербезпеки в розподілених інформаційних системах.

**Предметом дослідження** є моделі та методи оцінювання ризиків кібербезпеки розподілених інформаційних систем, а також теоретико-методологічні та практичні принципи моделювання процесу оцінювання ризиків ІБ у масштабованому розподіленому середовищі методами машинного навчання та штучного інтелекту.

**Методи дослідження.** При розв’язанні задач дослідження використано методи моделювання та інтелектуального аналізу даних, зокрема підходи на основі машинного навчання та штучних нейронних мереж, методологія системного аналізу та синтезу, методи формалізації та статистичного аналізу, а також методи узагальнення, порівняння та систематизації.

Інструментальними засобами моделювання та статистичного аналізу були програмна платформа IBM SPSS Statistics та мова програмування Python 3.9. Для програмної реалізації методів та відповідних моделей використано програмні фреймворки та бібліотеки TensorFlow та scikit-learn.

Емпіричною базою для дослідження стали:

- наукові дослідження та розробки вітчизняних і зарубіжних дослідників з обраної проблематики;
- національні та іноземні нормативно-правові акти, стандарти та методології в області оцінювання ризиків ІБ;
- набори даних розподілених мережевих метрик, що описують стан захищеності інформаційних активів та вузлів типової розподіленої системи, а також дані відповідності вимогам та контролям провідних стандартів ІБ;
- статистичні дані, отримані в ході опитування;
- дані дослідницьких компаній (ISACA, ENISA, ITU, Microsoft, тощо) щодо окремих статистичних показників в дотичних до тематики дослідження областях.

**Наукова новизна отриманих результатів** полягає в поглибленні теоретико-методичних положень і розробці практичних рекомендацій щодо вдосконалення процесу оцінювання ризиків кібербезпеки в умовах системної розподіленості та динамічності середовища, аналізі ключових факторів ризику для РІС та їх взаємозв'язків, а також розробці комплексу моделей оцінювання кіберризику на основі методів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж, що дозволяє підвищити точність та адаптивність процесу управління ризиками і сприяє підвищенню ефективності операційної та стратегічної діяльності компаній під впливом випадкових чинників в масштабованих динамічних середовищах. Основні положення дисертаційного дослідження, що визначають елементи його наукової новизни, полягають у наступному:

1. **Вдосконалено метод побудови профілю ключових факторів ризику** сучасних розподілених інформаційних систем на основі врахування кореляційного аналізу та моделювання їх взаємозв'язків, що дозволив оптимізувати процес вибору вхідного вектору ознак проєктованих моделей та підвищити їх ефективність.

2. Вперше **розроблено комплекс нейромережевих моделей оцінювання ризиків** кібербезпеки в розподілених інформаційних системах на основі синтезу метрико-орієнтованого та стандарт-орієнтованого підходів, що дозволило

автоматизувати обчислення показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

3. Вперше **розроблено адаптивний метод комплексного кількісного оцінювання** ризиків кібербезпеки в розподілених інформаційних системах з використанням спроєктованих моделей та загальної системи оцінки вразливостей, що дозволило підвищити ефективність процесу оцінювання ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем.

Отримані результати розширюють наукові уявлення щодо комплексної інтеграції формальних методів ризик-менеджменту, алгоритмів інтелектуального аналізу даних та практик оцінки на основі показників відповідності вимогам стандартів ІБ у масштабованих розподілених системах, формуючи цілісну концепцію оцінювання ризиків, що відрізняється від існуючих аналогів багатовимірним урахуванням факторів, адаптивністю і підвищеною точністю прогнозування.

**Практичне значення отриманих результатів** полягає в реалізації цілісного та системного підходу до оцінювання ризиків кібербезпеки у РІС шляхом побудови комплексу моделей оцінювання ризику на основі алгоритмів машинного навчання та інструментарію глибоких нейронних мереж, що враховують особливості предметної області та надають ряд переваг у порівнянні з класичними підходами до аналізу ризиків ІБ в умовах розподілених інформаційних систем, а також розробки адаптивного методу комплексного кількісного оцінювання ризиків кібербезпеки в РІС з використанням спроєктованих моделей, що забезпечує гнучкий підхід до аналізу розподілених ризиків, просту практичну імплементацію в програмні продукти ІБ та системи корпоративної безпеки, а також відкриває можливості для комплексного впровадження інтелектуальних систем управління інформаційною безпекою.

Розроблений підхід до багатофакторного аналізу універсальних та стандартизованих метрик розподілених систем дозволяє компаніям підвищити точність оцінювання рівня ризику для кожного інформаційного активу, забезпечуючи оперативний розподіл ресурсів на першочергові напрями посилення безпеки та прийняття обґрунтованих управлінських рішень в режимі реального часу. Це в свою

чергу сприяє підвищенню ефективності процесу ризик-менеджменту та надає можливість вивчення, аналізу, моніторингу і прогнозування потенційних загроз, а також своєчасного впровадженню економічно доцільних заходів безпеки.

Продемонстрована здатність запропонованих моделей до масштабування та адаптації під різноманітні топології розподілених інформаційних систем і різні обсяги вхідних даних надає змогу ефективно використовувати результати дисертаційного дослідження в організаціях з неоднорідними інфраструктурами та динамічними умовами середовища. Інтеграція контролів безпеки, визначених міжнародними та галузевими стандартами, у моделі оцінювання ризику спрощує процеси аудиту, полегшує виявлення критичних прогалин у безпеці та підвищує загальний рівень зрілості організації у сфері ІБ. Розроблені моделі оцінювання ризику можуть бути рекомендовані для використання в розподілених інформаційних системах для комплексного аналізу ризиків ІБ, а також для оцінки ефективності систем захисту та впроваджених механізмів безпеки. Результати дослідження можуть бути використані для побудови прикладних програмних модулів або сервісів підтримки прийняття рішень, що автоматично формують інтегральні показники ризику, виявляють закономірності та аномалії в даних і пропонують рекомендації з оптимального впровадження захисних заходів. Це сприяє покращенню якості, швидкості та прозорості процесів управління інформаційною безпекою.

Результати дисертаційної роботи мають наукову та практичну цінність, апробовані та прийняті до впровадження у діяльність ТОВ «ІТ СПЕЦІАЛІСТ» (акт впровадження результатів дослідження від 13.02.2025 р.) та ТОВ «АПІ Коннект» (акт впровадження результатів дослідження від 13.02.2025 р.). Результати дослідження знайшли своє відображення та практичне застосування при розробці програмних продуктів **ITS Inventory**, **ITS Cybersecurity Awareness Tracker (ITS CSAT), ITS Incident Management** та **ITS Compliance and Risk Management**.

**Особистий внесок здобувача.** Дисертаційна робота є одноосібною та самостійно виконаною науковою працею, у якій відображається авторське розуміння особливостей процесу ризик-менеджменту в умовах розподілених середовищ, висвітлені власні ідеї і розробки здобувача, що дозволили вирішити поставлені

завдання. Усі теоретичні положення, наукові розробки, практичні рекомендації, а також висновки та пропозиції, що отримані в ході проведення дослідження та виносяться на захист, є результатом власних досліджень та авторських здобутків. Із наукових праць, опублікованих у співавторстві, використано лише ті положення та ідеї, які є результатом власних досліджень. Зокрема, у статтях [61-62, 64, 66] здобувачем особисто проведено основний обсяг наукового дослідження, включаючи постановку задач, розробку методології дослідження та нових наукових положень, а також експериментальну частину та моделювання. В рамках статті [65] особистий внесок здобувача включав аспекти концептуалізації та аналізу теоретичних засад дослідження. Висвітлені в дисертаційній роботі гіпотези та ідеї інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

**Апробація результатів дисертації.** Основні теоретичні положення та практичні результати дисертаційної роботи доповідались на 8 міжнародних та всеукраїнських науково-практичних конференціях і семінарах.

**Публікації.** Результати дисертаційної роботи викладено та опубліковано у 16 наукових працях (у т.ч. 3 публікації – у виданнях, що входять до міжнародних наукометричних баз Scopus та Web of Science), серед яких: 4 статті у вітчизняних фахових виданнях; 1 стаття у науковому періодичному виданні іноземної держави віднесеного до першого-третього квартилів (Q1 – Q3) відповідно до класифікації SCImago Journal & Country Rank / Journal Citation Reports та індексацією в наукометричній базі Scopus; 11 тез доповідей та публікацій за матеріалами міжнародних науково-практичних конференцій (зокрема 1 апробація на конференції, яка входить до складу міжнародної організації IEEE).

**Структура та обсяг дисертації.** Дисертаційна робота складається з анотації, вступу, трьох розділів, висновків до кожного розділу та загальних висновків, а також списку використаних джерел та додатків. Загальний обсяг дисертації – 228 сторінок, а основний зміст роботи викладено на 188 сторінках. Робота містить 21 таблицю (з яких 3 таблиці займають усю площу сторінки), та 46 рисунків. Список використаних джерел налічує 135 найменувань, що представлені на 14 сторінках. Дисертація містить 4 додатки на 10 сторінках.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА НАУКОВО-МЕТОДОЛОГІЧНІ АСПЕКТИ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Перший розділ присвячений дослідженню теоретичних та науково-методологічних аспектів оцінювання ризиків кібербезпеки в розподілених інформаційних системах (РІС). В умовах зростаючої цифрової трансформації та масштабного впровадження розподілених систем у критично важливі галузі економіки, промисловості та державного управління, питання забезпечення їх кіберстійкості набуває стратегічного значення. Оцінювання ризиків кібербезпеки є фундаментальним етапом процесу управління інформаційною безпекою (ІБ), оскільки дозволяє ідентифікувати, аналізувати та прогнозувати загрози, знижуючи ймовірність кібератак і мінімізуючи потенційні наслідки їх реалізації.

У розділі здійснено аналіз сучасного стану та тенденцій розвитку РІС, виявлено ключові проблеми забезпечення їх кібербезпеки та обґрунтовано значущість завдань оцінювання ризиків у цьому контексті. Досліджено теоретичні основи ризик-менеджменту в розподіленому середовищі, розглянуто математичні підходи до формалізації ризику та проведено аналіз існуючих методів оцінювання ризиків кібербезпеки. Окрему увагу приділено аналізу та порівнянню міжнародних стандартів і ключових методологій ризик-менеджменту, що дозволило визначити їх переваги, обмеження та можливості застосування в контексті розподілених інформаційних систем.

За результатами досліджень встановлено, що існуючі методи не забезпечують у повній мірі ефективного процесу оцінювання ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем. Систематизація теоретичних підходів і критичний аналіз існуючих методів оцінювання формують основу для подальшої розробки науково обґрунтованих моделей та методів прогнозування й мінімізації ризиків, що є ключовим науково-прикладним завданням дослідження.

## 1.1. Сучасний стан та тенденції розвитку розподілених інформаційних систем

Упродовж останніх десятиліть світ зазнав якісну трансформацію інформаційного середовища, спричинену глобалізацією економічних, соціальних та технологічних процесів. Глобальна інтеграція ринків, підвищення мобільності населення, поширення міжнародної співпраці у сферах торгівлі та виробництва, а також стрімкий розвиток телекомунікаційної інфраструктури призвели до того, що кількість комп'ютерів, комп'ютерних мереж та рівень цифрової взаємодії між організаціями і користувачами зростають у геометричній прогресії.

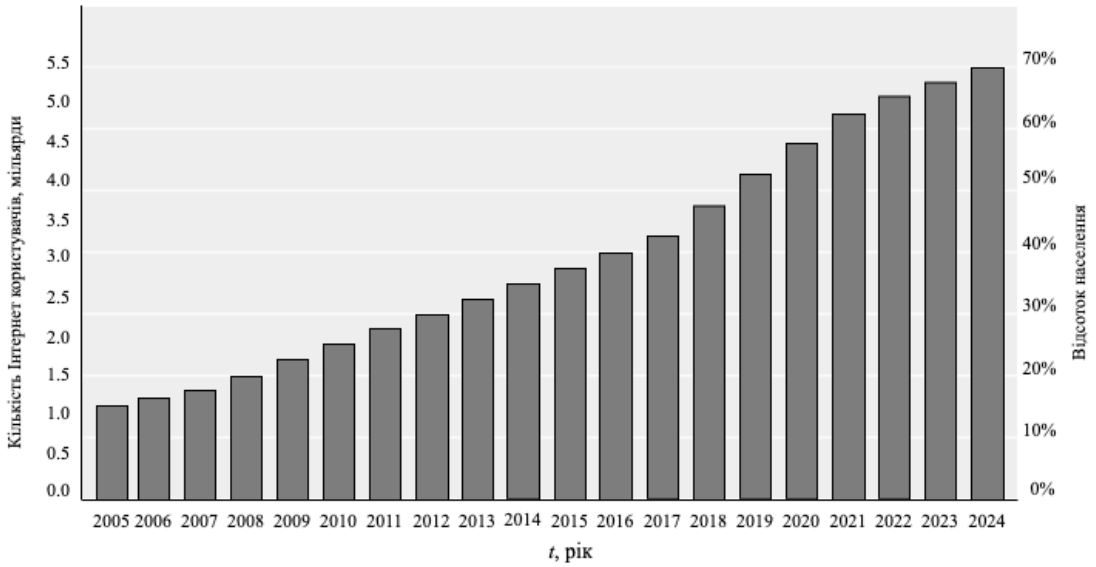


*Рис. 1.1. Графік експоненційного росту кількості користувачів глобальної мережі Інтернет 2005-2024 рр.*

За даними Міжнародного союзу електрозв'язку (International Telecommunication Union, ITU), кількість інтернет-користувачів у світі перевищила позначку у 4,5 млрд осіб на початку 2020-х років, продемонструвавши більш ніж 10-кратне зростання порівняно з кінцем 1990-х років. За оцінками ITU, у 2024 році приблизно 5,5 мільярда людей, або 68 відсотків населення нашої планети, користуються Інтернетом [1].

Поширення та здешевлення доступу до обчислювальних ресурсів, стрімкий розвиток хмарних технологій, віртуалізації та контейнеризації підсилюють можливості для ефективного розподілу обчислень. Це, в свою чергу, стимулює збільшення кількості та масштабів розподілених інформаційних систем, які нині

обслуговують мільярди транзакцій і запитів на хвилину, забезпечують роботу глобальних пошукових систем, соціальних мереж, банківських платформ, систем електронної-комерції й логістики. Протягом останніх двох десятиліть масове впровадження мобільних пристроїв, розвиток Інтернету речей (Internet of Things, IoT) та перехід до архітектур мікросервісів стали додатковими передумовами розширення топології РІС, підвищення їх складності та функціонального навантаження [2].

У сучасних умовах функціонування інформаційних систем, стрімке зростання масштабів, складності та розподіленості обчислювальних ресурсів стає однією з визначальних тенденцій розвитку цифрової інфраструктури. Протягом останніх десятиліть поширення РІС спостерігається практично в усіх сферах – від телекомунікацій та фінансового сектору до енергетики та промисловості. Зростання кількості обчислювальних вузлів, географічна розосередженість елементів інфраструктури, взаємопов’язаність різноманітних архітектурних рішень та використання хмарних технологій призводять до принципово нових вимог до надійності, масштабованості та інформаційної безпеки РІС.

Паралельно з цим спостерігається суттєве зростання кількості та складності кіберзагроз. Кіберзлочинці активно використовують розподілену природу систем для поширення зловмисного програмного забезпечення, проведення DoS (Denial of Service Attack) та DDoS-атак (Distributed Denial of Service Attack), викрадення або модифікації чутливих даних. У результаті, безпекові виклики набувають нових форм, а традиційні механізми захисту стають недостатніми. Це зумовлює необхідність пошуку і впровадження більш гнучких, динамічних та інтелектуальних підходів до забезпечення кібербезпеки, які б могли виявляти та реагувати на загрози в режимі реального часу, а також ефективно оцінювати ризики, пов’язані з вразливостями та атаками на масштабовані розподілені інфраструктури [3].

Оцінювання ризиків кібербезпеки в РІС стає не просто одним із ключових завдань, а критичним елементом управління інформаційною безпекою. Без розуміння природи існуючих і потенційних загроз, без кількісної оцінки ймовірності та впливу атак, неможливо приймати обґрунтовані рішення щодо пріоритезації захисних заходів, оптимального розподілу ресурсів на безпеку, впровадження відповідних

політик та стандартів ІБ. Процес оцінювання ризиків дозволяє сформувати більш стійку та адаптивну систему кібербезпеки, що здатна оперативно реагувати на зміну умов середовища і динаміку загроз, одночасно забезпечуючи конфіденційність, цілісність та доступність критичних даних та сервісів [69].

### 1.1.1. Аналіз архітектурних концепцій, технологій та тенденцій впровадження РІС у різних галузях промисловості та бізнесу

Перед тим, як зосередитися на особливостях розподілених інформаційних систем, доцільно проаналізувати загальне поняття «інформаційна система». Під **інформаційною системою (ІС)** розуміють інтегрований комплекс апаратного та програмного забезпечення, даних, процедур і людських ресурсів, призначений для збору, обробки, зберігання, передачі та використання інформації з метою ефективного забезпечення управлінських, виробничих, наукових та інших процесів в рамках певної предметної області. Таке визначення охоплює широкий діапазон рішень, починаючи від локальних програмних продуктів і закінчуючи складними корпоративними системами, що взаємодіють з різними джерелами даних та користувачами. На цьому фундаменті можна глибше зрозуміти сутність розподілених інформаційних систем та їх специфічні властивості.

Згідно з позицією Ендрю С. Таненбаума (Andrew S. Tanenbaum), одного з основоположників концепції РІС, – не існує загальноприйнятого та однозначного визначення розподіленої системи [4]. Ключовим параметром, що відрізняє розподілену систему, є розподіл її функцій між кількома обчислювальними вузлами. У цьому контексті розподілені інформаційні системи розглядаються як географічно розосереджені комплекси, що складаються з взаємодіючих обчислювальних пристроїв та терміналів, з’єднаних між собою каналами передачі даних. Завдяки об’єднанню можливостей розподілених компонентів, така система часто перевершує типові централізовані рішення за масштабом та продуктивністю. Прикладами розподілених систем є комп’ютерні мережі, розподілені бази даних, системи керування технологічними процесами в реальному часі, а також розподілені системи обробки інформації.

Таким чином, **розподілені інформаційні системи** – це клас інформаційно-технологічних систем, у яких обчислювальні ресурси, дані та сервіси фізично розподілені між множиною окремих вузлів, що з'єднані каналами зв'язку і взаємодіють через мережеві середовища. Кожен вузол може мати власні обчислювальні потужності, локальні дані та програмні компоненти, проте з точки зору користувачів РІС прагне виступати як цілісна платформа, що забезпечує прозорий доступ до необхідних ресурсів і сервісів. На відміну від централізованих архітектур, де вся логіка та дані зосереджені в одному місці, РІС дозволяють розподіляти навантаження, підвищувати відмовостійкість та гнучко масштабувати систему залежно від вимог до продуктивності та надійності.

До основних характерних ознак розподілених систем можна віднести:

1. **Спільне використання ресурсів**. Розподілені системи надають можливість колективно використовувати доступні ресурси – обчислювальні потужності, сховища даних, програмне забезпечення або апаратні пристрої. Завдяки цьому забезпечується ефективніше завантаження обладнання, зниження витрат та підвищення гнучкості при вирішенні широкого кола завдань.

2. **Відкритість**. Відкрита архітектура розподілених систем полягає у застосуванні загальноприйнятих стандартів, відкритих протоколів та узгоджених інтерфейсів. Такий підхід спрощує інтеграцію нових компонентів, сприяє взаємодії різнорідних систем та технологій, а також стимулює інновації та розвиток екосистеми програмних продуктів.

3. **Прозорість**. Прозорість означає приховування від користувачів складності та неоднорідності внутрішньої архітектури системи. На верхньому рівні розподілена система виглядає для користувача як єдиний цілісний комплекс, незалежно від фізичного розташування вузлів, особливостей мережевої інфраструктури чи обчислювальних платформ.

4. **Паралелізм**. Розподілені системи здатні виконувати декілька завдань одночасно, розподіляючи робочі навантаження між різними вузлами. Це дозволяє ефективніше використовувати обчислювальні ресурси, знижувати час обробки та прискорювати реакцію на запити користувачів.

5. **Масштабованість та гнучкість**. Можливість безперешкодно додавати нові вузли чи ресурси в розподілену систему дозволяє їй зростати разом із підвищенням потреб користувачів та збільшенням обсягів оброблюваних даних. Масштабування може бути як вертикальним (збільшення потужності окремих вузлів), так і горизонтальним (додавання нових обчислювальних одиниць).

6. **Висока продуктивність та ефективність**. Завдяки паралельній обробці, ефективному розподілу ресурсів та можливостям масштабування розподілені системи здатні забезпечувати високий рівень продуктивності. Це особливо актуально для систем, що обслуговують значні обсяги запитів, обробляють великі об’єми даних чи виконують складні аналітичні обчислення.

7. **Надійність та відмовостійкість**. Відмовостійкість передбачає здатність системи продовжувати коректну роботу навіть за умови виходу з ладу окремих компонентів. Розподілені системи зазвичай проєктуються з урахуванням можливості відмов окремих вузлів або каналів зв’язку. Реплікація даних, запасні маршрути, механізми резервного копіювання та розподілу навантаження підвищують загальну надійність інфраструктури, мінімізуючи вразливість до збоїв та зменшуючи ймовірність катастрофічних наслідків для стабільної та безперервної роботи системи.

Таким чином, ключовим завданням сучасних РІС є створення умов для зручного доступу користувачів до віддалених ресурсів, а також забезпечення можливостей їх спільного використання. Оскільки розподілені системи характеризуються просторовою віддаленістю їх компонентів, ефективна комунікація та взаємодія між ними здійснюється за допомогою ряду стандартних протоколів, які визначають узгоджені процедури обміну даними. Дотримання єдиних мережевих протоколів різними компонентами дає змогу їм коректно взаємодіяти між собою. Для опису таких взаємодій широко застосовується еталонна модель взаємодії відкритих систем OSI (Open Systems Interconnection), яка структурує роботу розподілених компонентів за рівнями протоколів і охоплює всі ключові аспекти обчислювальних комунікацій [5].

Наукові засади розподілених систем формувалися завдяки працям провідних дослідників, серед яких:

- Ендрю С. Таненбаум (Andrew S. Tanenbaum): один з основоположників концепцій розподілених систем, автор класичних підручників та наукових праць, що заклали фундаментальні принципи побудови розподілених обчислень [3-5].
- Леслі Лампорт (Leslie Lamport): запропонував поняття логічного часу та сформулював базові концепти узгодженості станів у розподілених системах. Його алгоритми консенсусу, зокрема Paxos, стали еталонними рішеннями для забезпечення узгодженості розподілених даних [6-7].
- Ненсі Лінч (Nancy Lynch): відома своїми роботами у сфері формальної теорії розподілених систем та обчислень, заклала міцний математичний фундамент аналізу коректності протоколів розподілених систем [8].
- Джордж Кулуріс (George Coulouris), Джин Доллімор (Jean Dollimore), Тім Кіндберг (Tim Kindberg): автори відомих наукових праць та підручників, присвячених розподіленим системам, що узагальнили сучасні теоретичні засади та практичні підходи до побудови РІС [9].
- Кен Бірман (Kenneth Birman): досліджував надійність та толерантність до відмов у розподілених обчислювальних середовищах, ставши піонером у розробці систем із гарантованою доставкою повідомлень і забезпеченням високої доступності [10-12].
- Росс Андерсон (Ross Anderson): активно досліджував питання кібербезпеки в розподіленому середовищі, зробивши значний науковий внесок в області криптографії включаючи розробку ряду шифрів та криптографічних алгоритмів, а також виявлення вразливостей в протоколах та системах безпеки [13].
- Кліффорд Ньюман (Clifford Neuman): сфера наукових інтересів включає питання управління розподіленими ресурсами, масштабування та забезпечення безпеки сучасних РІС, окрім цього науковець став одним з ключових розробників системи автентифікації Kerberos, що використовується для надійної автентифікації користувачів та захисту від несанкціонованого доступу (НСД) в комп’ютерних мережах [14-16].

Наукові здобутки вищезазначених вчених та багатьох інших дослідників сформували фундамент для розвитку галузі та появи низки архітектурних концепцій, які сьогодні широко застосовуються на практиці.

Архітектурні рішення для РІС можна систематизувати за кількома ключовими ознаками, зокрема за структурою взаємодії компонентів, способом розподілу функціональних ролей, технологічними стеками та моделями обчислень.

**За логікою взаємодії вузлів**:

- **Клієнт-серверна архітектура (Client-Server)**: класична модель, де сервер надає сервіси, а клієнти ініціюють запити до нього. Централізація частково зберігається, проте сервери можуть бути розподілені та балансувати навантаження. У цій моделі роль сервера полягає в централізованому керуванні ресурсами та наданні послуг, тоді як клієнтська сторона зосереджується переважно на представленні даних і взаємодії з користувачами.
- **Рівноправна архітектура (Peer-to-Peer, P2P)**: усі вузли мають рівний статус і можуть виступати як клієнт або сервер. Така модель дозволяє ефективно масштабувати систему та забезпечувати підвищену відмовостійкість без центрального вузла. Однорангові вузли взаємодіють між собою для спільного використання ресурсів, наприклад файлів або обчислювальних потужностей, без необхідності комунікації з центральним сервером. При цьому всі вузли виступають рівноправними учасниками мережі та здатні як ініціювати, так і приймати запити.

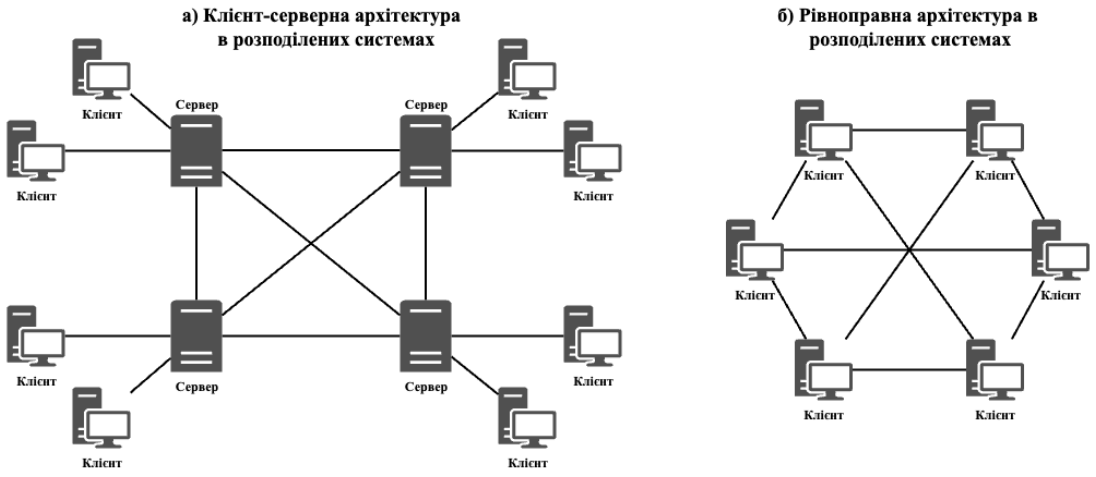


*Рис. 1.2. Клієнт-серверна (Client-Server) та рівноправна (Peer-to-Peer, P2P) архітектури в розподілених системах.*

- **Багаторівнева архітектура (Layered)**: включає декілька обов’язкових логічних шарів, що можуть бути розподілені між різними вузлами:
  - рівень подання (інтерфейсу користувача);
  - рівень бізнес-логіки (оброблення даних);
  - рівень даних.

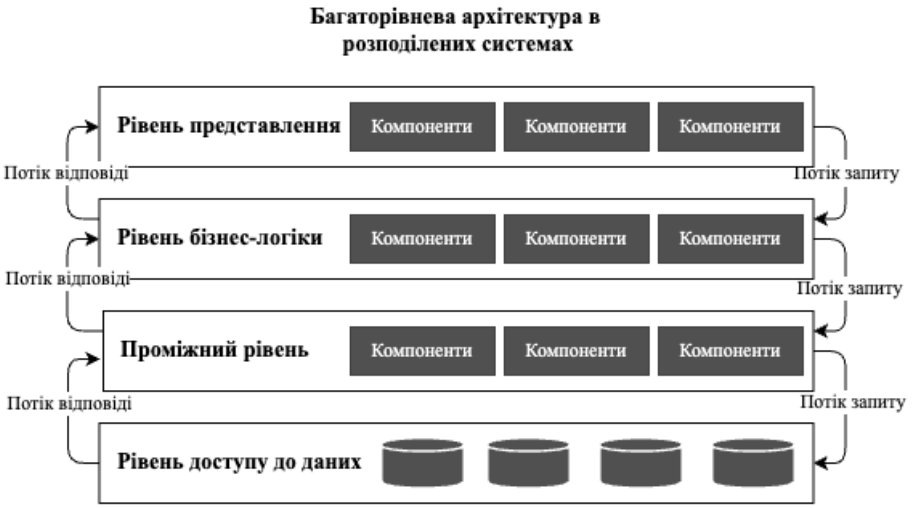


*Рис. 1.3. Багаторівнева (Layered) архітектура в розподілених системах.*

Багаторівнева архітектура у розподілених системах формує ієрархічну структуру, у якій кожен рівень відповідає за певний набір функцій та взаємодіє здебільшого з безпосередньо сусідніми шарами. Такий підхід спрощує управління системою та полегшує розподіл обов’язків між її компонентами.

**За підходом до організації сервісів**:

- **Сервіс-орієнтована архітектура (Service-Oriented Architecture, SOA)**: заснована на ідеї надання доступу до функціональності у вигляді окремих розподілених сервісів із чітко визначеними інтерфейсами для взаємодії за стандартизованими протоколами. Такі сервіси слабко пов’язані між собою, їх можна розробляти, розгортати та керувати самостійно. Взаємодія між ними відбувається через мережу за допомогою набору стандартних технологій обміну даними (HTTP, SOAP, REST тощо), що дає змогу налагодити ефективну комунікацію між різними системами та сервісами.


*Рис. 1.4. Сервіс-орієнтована (Service-Oriented Architecture, SOA) архітектура в розподілених системах.*

Деталі реалізації інкапсулюються від інших компонентів, таким чином забезпечуючи легку інтеграцію і багаторазове використання елементів для побудови складних розподілених систем, забезпечуючи незалежність від використовуваних платформ та інструментів розробки.

- **Мікросервісна архітектура (Microservices)**: являє собою розвиток SOA, коли застосунок поділений на набір дрібних, незалежних сервісів, що можуть автономно масштабуватись, розгортатись і оновлюватись. При цьому такий архітектурний стиль передбачає, що кожен мікросервіс будується навколо окремих бізнес-потреб, розгортається незалежно від інших, проте використовує прості протоколи передачі даних для комунікацій з ними.

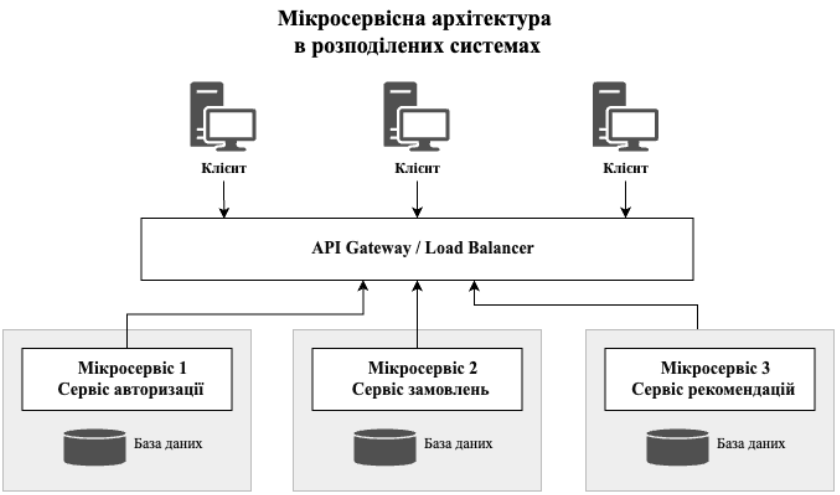


*Рис. 1.5. Мікросервісна архітектура (Microservices) в розподілених системах.*

Такий підхід надає ряд переваг, основним з яких є незалежність елементів, зручність розгортання та підтримки, а також можливість реалізації окремих компонент з використанням різних наборів технологій, мов програмування і підходів до зберігання даних.

- **Архітектура, орієнтована на події (Event-Driven Architecture, EDA)**: взаємодія між компонентами системи відбувається через обмін подіями й повідомленнями, що дозволяє ефективно реагувати на динамічні зміни у середовищі. Подія передбачає зміну стану системи або її окремих компонентів, що потребує відповідної реакції.


*Рис. 1.6. Архітектура, орієнтована на події (Event-Driven Architecture, EDA) в розподілених системах.*

Така архітектурна парадигма проєктування дозволяє створювати системи, здатні динамічно пристосовуватися до непередбачуваних, асинхронних умов функціонування. Крім того, EDA може доповнювати сервіс-орієнтовану архітектуру, оскільки сервіси можуть активовуватися тригерами, що спрацьовують у разі настання певних подій.

**За моделлю узгодженості та керування даними**:

- Централізовані системи керування даними (із розподіленим кешуванням): базу даних розташовано у відносно централізованому місці, проте для підвищення продуктивності застосовують розподілене кешування.
- Розподілені бази даних та NoSQL-сховища: дані розміщено у кількох вузлах, а протоколи реплікації та шардінгу забезпечують масштабованість і відмовостійкість.

- Розподілені журнали та блокчейн-архітектури: використання розподілених реєстрів, узгоджених протоколів консенсусу та криптографічних методів забезпечує цілісність даних без довіри до окремого центрального вузла.

**За технологічними підходами**:

- Хмарні обчислення (Cloud Computing): використання інфраструктури як сервісу (Infrastructure-as-a-Service, IaaS), платформ як сервісу (Platform-as-a-Service, PaaS) та програмного забезпечення як сервісу (Software-as-a-Service, SaaS). Ці моделі дозволяють динамічно масштабувати ресурси, забезпечуючи економічну ефективність та гнучкість.
- Контейнеризація та оркестрація (Docker, Kubernetes): контейнеризація надає можливість ізоляції застосунків у окремих середовищах, а системи оркестрації автоматизують управління їх життєвим циклом, балансування навантаження та забезпечення стійкості.
- Розподілені черги повідомлень та системи обміну даними (Apache Kafka, RabbitMQ): застосування асинхронних механізмів комунікації між компонентами дозволяє обробляти великі потоки даних у реальному часі, масштабувати системи та підвищувати їх адаптивність.

**За моделлю обчислень**:

- Паралельні обчислення (MPI, OpenMP): використання спеціалізованих бібліотек для розподілених обчислень, характерне для наукових і високопродуктивних середовищ.
- Розподілені обчислювальні платформи (Apache Spark, Hadoop): застосування фреймворків, орієнтованих на обробку великих даних, інтелектуальний аналіз та виконання складних обчислювальних завдань у розподіленому середовищі.

Слід відзначити, що розвиток та еволюція парадигми розподілених інформаційних систем істотно вплинули на формування сучасного інформаційно-технологічного ландшафту. Розширення масштабів їх застосування, зумовлене збільшенням обсягів даних, кількості користувачів та географічною розосередженістю ресурсів, стимулювало перехід від централізованих до розподілених архітектурних підходів. Це, у свою чергу, стало каталізатором стрімкого

розвитку різноманітних архітектурних концепцій та сприяло впровадженню широкого спектра відповідних технологій – від розробки універсальних протоколів і відкритих стандартів до хмарних обчислень, механізмів контейнеризації та оркестрації. Зрештою, послідовне розширення функціональних можливостей РІС, активне застосування методів автоматизації, машинного навчання та інтелектуального аналізу даних стали рушіями формування складних, динамічних та високопродуктивних інформаційних систем нового покоління [4, 9-10].

Широке впровадження розподілених інформаційних систем на сьогоднішній день є характерним майже для всіх галузей людської діяльності, де на них покладається вирішення все важливіших задач. Від якості функціонування РІС залежить оперативність прийняття рішень й ефективність функціонування багатьох економічних, соціальних, політичних та військових структур.

**Промисловість та виробництво.** Однією з ключових сфер активного впровадження РІС є промисловість, зокрема сектори, що зазнають все більш обширної цифровізації процесів. Розподілені системи, інтегровані з технологіями IoT, дають змогу контролювати виробничі процеси в реальному часі, оптимізувати логістику та керувати ланцюгами поставок, забезпечувати гнучке конфігурування виробничих ліній та прогнозувати вихід з ладу обладнання на основі даних про його фактичний стан. Завдяки цьому підприємства можуть підвищувати продуктивність, знижувати витрати на простої та ефективніше реагувати на зміни ринкового попиту.

**Енергетика та транспортна інфраструктура.** У галузі енергетики РІС використовуються для моніторингу розподілених джерел енергії, оптимізації роботи мереж електропостачання, управління інтелектуальними лічильниками та прогнозування споживання електроенергії. Розподілена архітектура дозволяє адаптивно керувати навантаженням, регулювати пропозицію та попит, а також вчасно реагувати на аварійні ситуації. Аналогічні підходи застосовуються в транспортній інфраструктурі, де РІС підтримують інтелектуальні системи керування дорожнім рухом та логістикою.

**Фінансовий сектор та електронна комерція.** У фінансовому секторі та електронній комерції розподілені системи стали критично важливими для обробки

великих обсягів транзакцій, забезпечення низької затримки доступу до фінансових даних та підвищення надійності платіжних платформ. Наприклад, у високочастотній торгівлі розподілена інфраструктура сприяє зменшенню часу відгуку торговельних систем, а у банківській сфері – забезпечує надійні та безпечні платіжні сервіси на глобальному рівні. Сервісно-орієнтований підхід дозволяє швидко оновлювати функціональність фінансових застосунків, інтегрувати зовнішні сервіси та адаптуватися до постійно змінних вимог клієнтів.

**Охорона здоров'я та фармацевтика.** У медичній галузі РІС відіграють важливу роль у забезпеченні безпечного обміну та обробки даних пацієнтів, підтримці телемедичних послуг, дистанційному моніторингу стану здоров'я пацієнтів, а також в інтеграції медичних пристроїв у єдині платформи електронної охорони здоров'я (eHealth). Такі системи дозволяють знизити навантаження на центральні медичні заклади, покращити доступ до медичних послуг у віддалених регіонах та підвищити якість діагностики та лікування.

**Державний сектор та електронне врядування.** Розподілені системи стають основою для електронних урядових сервісів, оптимізації документообігу та надання адміністративних послуг онлайн. Прозорість, масштабованість та відмовостійкість РІС сприяють підвищенню ефективності державного управління та доступності державних послуг, зменшенню бюрократичних процедур, а також оптимізації витрат, що забезпечує більш ефективне використання ресурсів.

**Науково-дослідна діяльність.** РІС активно застосовуються у науково-дослідних проєктах, що передбачають моделювання складних явищ, обробку великих обсягів експериментальних даних та співпрацю наукових колективів з різних країн і установ. Хмарні та грід-системи, розподілені аналітичні платформи та спеціалізовані розподілені бази даних допомагають дослідникам ефективно обмінюватися результатами, використовувати віддалені обчислювальні ресурси та знижувати витрати на обслуговування ІТ-інфраструктур.

У сучасних умовах динамічного вдосконалення цифрових технологій РІС перетворилися на ключовий елемент стратегічного розвитку багатьох галузей промисловості та бізнесу. Тенденції впровадження розподілених систем

демонструють їх універсальність та гнучкість для вирішення широкого спектра завдань у різних областях діяльності. РІС забезпечують глобалізацію та масштабування процесів, ефективне використання та розподіл ресурсів, оперативну адаптацію до змінних умов середовища та високий рівень надійності.

Таким чином, здійснений аналіз основних архітектурних концепцій, технологій та тенденцій впровадження РІС підкреслює ряд важливих аспектів, пов'язаних із динамічністю середовища функціонування сучасних розподілених систем, значною різнорідністю та гетерогенністю програмно-апаратних технологій їх імплементації. Розуміння цих принципів є важливим для подальшого дослідження питань забезпечення кібербезпеки в розподілених інформаційних системах, а також викликів в задачах оцінювання ризиків розподіленого середовища.

### 1.1.2. Основні принципи забезпечення кібербезпеки в РІС, проблеми та виклики в задачах оцінювання ризику

Інтенсивний розвиток та впровадження розподілених систем у різноманітні галузі промисловості та бізнесу стимулює появу нових архітектурних підходів, технологій оркестрації ресурсів, методів оптимізації даних та систем керування розподіленими обчисленнями. Це створює фундамент для інновацій, але водночас породжує низку викликів, пов'язаних із забезпеченням кібербезпеки: зростає складність інфраструктури, множаться потенційні вектори атак, а кібер-ризики стають більш диференційованими та важкопрогнозованими. Система, що має розгалужену, динамічну природу та складається з численних географічно розподілених вузлів, гетерогенних інфраструктур та різнорідних програмно-апаратних компонентів, потребує комплексного підходу до захисту від загроз, а також розвинених механізмів оцінювання та управління ризиками.

Варто підкреслити, що зростання кількості вузлів та розширення географії розташування обчислювальних ресурсів призводять до збільшення обсягів інформації, яка циркулює між різними вузлами. За оцінками аналітичних компаній (зокрема, International Data Corporation, IDC), загальний обсяг даних, які обробляються у світовому масштабі, збільшується експоненційно: якщо у 2010 році

світовий обсяг даних оцінювався в декілька зетабайт (ЗБ), то до середини 2020-х років цей показник наближається до сотень ЗБ, і за прогнозами вже найближчим часом може перевищити 175 ЗБ [17].

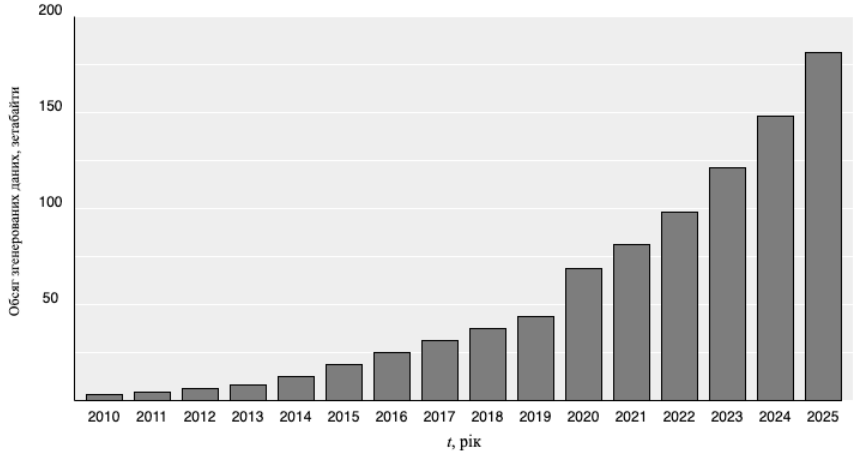


*Рис. 1.7. Графік росту обсягу даних, створених, скопійованих і використаних (у зетабайтах) 2010-2025 рр.*

Із зростанням обсягу інформації, що обробляється та передається між різними інформаційними системами, організації та окремі користувачі все більше залежать від безперервності та коректності цих процесів, що супроводжується підвищенням вимог до безпеки передачі, обробки та зберігання даних.

Водночас, постійне нарощування обсягів інформації, що генерується, обробляється та передається між обчислювальними вузлами РІС, значно ускладнює завдання оперативного аналізу та моніторингу загроз кібербезпеки. Різноманітність та значна диференційованість джерел даних, динамічність конфігурацій мережевого обладнання, нерівномірний розподіл інформаційних потоків, а також високий обсяг та швидка зміна характеристик мережевого трафіку ускладнюють кореляцію безпекових подій, виявлення аномалій та інцидентів ІБ. Традиційні підходи до моніторингу, засновані на статичному аналізі сигнатур, поступово втрачають ефективність у контексті мінливих механізмів реалізації атак та складних поведінкових патернів активності зловмисників [116]. Це обумовлює необхідність застосування передових технологій інтелектуального аналізу даних, машинного навчання, а також поведінкової аналітики для виявлення аномалій та підозрілих дій у режимі реального часу [126].

Таким чином, можна підсумувати наступні ключові проблеми кібербезпеки в розподілених системах:

- **Децентралізована структура та гетерогенність компонентів** – складність управління безпекою через велику кількість взаємодіючих вузлів, що використовують різні платформи та технології.
- **Динамічність середовища** – постійна зміна топології мережі, поява нових сервісів і користувачів ускладнюють традиційні методи контролю доступу та моніторингу загроз.
- **Розширена поверхня атаки** – велика кількість точок входу для зловмисників через використання хмарних сервісів, IoT-рішень і мобільних пристроїв.
- **Недостатня адаптивність традиційних механізмів захисту** – класичні методи виявлення загроз та управління ризиками не завжди ефективні для динамічних і масштабованих РІС.

Розподілена природа РІС створює широкий ландшафт для зловмисних дій: від спрямованих атак, фішингових кампаній, DoS та DDoS-атак до внутрішніх загроз, пов’язаних із неконтрольованим доступом до критичних даних. Іншим важливим аспектом є складність управління доступом та автентифікацією. Наявність численних користувачів, пристроїв і сервісів, які взаємодіють у РІС, вимагає застосування гнучких та надійних механізмів контролю доступу, багатофакторної автентифікації, авторизації, шифрування та аудиту, а також гнучких моделей керування політиками безпеки [65-66].

Кібербезпекові загрози у РІС можуть призвести не лише до компрометації даних чи зловмисного доступу, але й до тимчасової чи повної втрати доступності критичних сервісів. Забезпечення стійкості та толерантності до відмов у цьому контексті означає впровадження механізмів резервного копіювання, реплікації та відновлення даних, а також використання протоколів консенсусу та розподіленого журналювання подій, які гарантують коректне відновлення системи після інцидентів. Дослідженню методологічних аспектів підвищення надійності і функціональної стійкості розподілених інформаційних систем до кібернетичних загроз та впливів присвячено

ряд наукових робіт вітчизняних вчених – О.А. Машкова [18-21], І.Ю. Субача [22-23], О.В. Барабаша [18, 21, 24 -27], Д.М. Обідіна [21], Ю.В. Кравченка [27], Н.В. Лукової-Чуйко [24, 28-32], І.В. Рубана [28, 33], С.В. Толюпи [31-32] та багатьох інших.

Окрім цього, дотримання вимог стандартів ІБ та регіональних нормативно-правових актів (наприклад, General Data Protection Regulation, GDPR) у розподіленому середовищі є складнішим, оскільки контролі безпеки мають узгоджуватися між різними доменами та системами, а аудит безпеки вимагає застосування комплексних підходів до збору та аналізу даних з різних вузлів.

Таким чином, забезпечення кібербезпеки в розподілених інформаційних системах постає багатогранним завданням, яке вимагає поєднання технологічних, організаційних та управлінських підходів, а також передбачає врахування наступних принципів:

1. **Захист за принципом глибокої оборони (Defense-in-Depth)** – багаторівнева стратегія безпеки, що включає аутентифікацію, контроль доступу, шифрування, моніторинг активності та виявлення аномалій.
2. **Принцип нульової довіри (Zero Trust)** – відсутність автоматичної довіри між вузлами системи, перевірка кожного запиту незалежно від його походження.
3. **Адаптивність та автоматизація** – використання інтелектуальних методів аналізу загроз для прогнозування та нейтралізації потенційних атак.
4. **Сегментація мережі та мінімізація привілеїв** – поділ системи на ізольовані зони та обмеження доступу для зниження ймовірності компрометації.
5. **Моніторинг у режимі реального часу та реакція на інциденти** – впровадження SIEM-систем і автоматизованих механізмів виявлення аномалій для оперативного реагування на актуальні загрози.

Комплексне застосування цих принципів дозволяє підвищити стійкість РІС до кібератак та мінімізувати ризики ІБ. Саме **процес оцінювання ризиків кібербезпеки** є ключовим та невід'ємним компонентом управління безпекою в розподілених інформаційних системах. Оцінювання ризиків надає основу для розробки ефективних стратегій та заходів захисту, що дозволяє зменшити ймовірність реалізації загроз та мінімізувати потенційні збитки.

За даними щорічного глобального дослідження стану кібербезпеки «STATE OF CYBERSECURITY 2024: GLOBAL UPDATE ON WORKFORCE EFFORTS, RESOURCES AND CYBEROPERATIONS» від компанії ISACA переважна більшість компаній-респондентів принаймні один раз на рік проводять регулярне оцінювання ризиків ІБ, і цей показник збільшується з кожним роком, що сигналізує про позитивну тенденцію та демонструє посилення уваги до питань ризик-менеджменту [34].

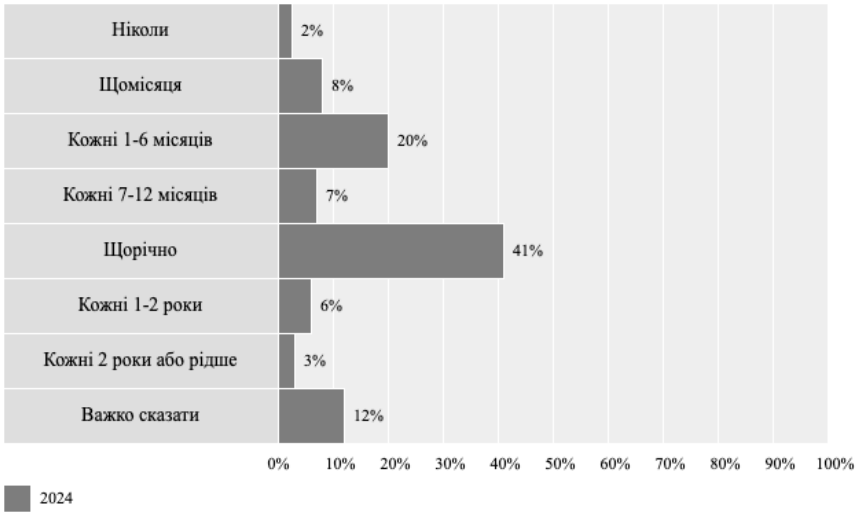


*Рис. 1.8. Тенденції оцінювання корпоративних кіберризиків 2024 р.*

Відповідно до Bitdefender Cybersecurity Assessment Report 2024 більше половини організацій (57%) зазнали порушення або витоку даних за останні 12 місяців (на 6% більше, ніж у попередньому році), при цьому 93% опитаних планують збільшити інвестиції в оцінювання ризиків ІБ та проактивні стратегії захисту [35].

Зважаючи на масштабованість, гетерогенність та динамічність розподілених систем, традиційні методи управління ризиками часто виявляються неефективними або недостатньо точними. Основні методологічні складнощі оцінювання ризиків у РІС пов’язані з наступними аспектами:

1. **Висока складність, динамічність та масштабованість середовища** – різнорідність обладнання та інфраструктури, постійна зміна мережевих конфігурацій, поява нових сервісів та користувачів, необхідність врахування численних взаємозалежностей між компонентами системи створюють труднощі у визначенні актуальних загроз.

2. **Значна фрагментованість та неповнота даних, відсутність єдиного формату представлення у різних системах** – ефективне оцінювання ризику в розподіленому середовищі потребує значного обсягу актуальних даних, які часто розподілені між різними доменами, можуть бути неповними та мати складну структуру.

3. **Проблеми агрегування та аналізу даних** – необхідність збору та оперативної обробки великих масивів складних за структурою та гетерогенних за природою даних, що надходять із різноманітних систем безпеки та моніторингу, журналів подій, аудиторських звітів та інших джерел.

4. **Відсутність єдиних стандартів та методологій** – необхідність універсального підходу, що враховував би специфіку розподілених систем та надавав уніфіковану процедуру оцінювання з врахуванням адаптації до динамічних змін середовища та мінливості ландшафту потенційних загроз.

5. **Низька ефективність традиційних методів оцінювання** – класичні підходи виявляють низку обмежень у масштабованому та динамічному середовищі розподілених систем, пов’язаних із складністю і нелінійністю взаємозв’язків між факторами ризику, відсутністю гнучких механізмів аналізу гетерогенних даних PIC та виявлення нелінійних залежностей і прихованих закономірностей, недостатньою адаптивністю та реактивністю, а також необхідністю оперативного аналізу в режимі часу, близькому до реального.

Дослідженню питань оцінювання ризиків в умовах невизначеності складних та масштабованих інформаційних систем приділено увагу в працях В.А. Заславського [36-39], В.О. Акімова, О.Є. Архіпова [40, 46, 109], О.М. Астахова, В.Є. Бенінга, В.В. Бєгуна, О.М. Богданова [41], В.П. Буянова, Я.Д. Вишнякова, В.В. Вітлінського, О.Г. Додонова, Ю.Л. Забулонова, О.А. Замули [42, 99], А.Б. Качинського [43], В.Ю. Корольова, О.Г. Корченка [44-48, 108], В.В. Костерєва, Г.В. Лисиченка, І.Д. Медведовського, В.В. Мохора [41, 49, 103-105], О.О. Недосєкіна, О.М. Новікова, А.А. Новосєлова, Н.Д. Панкратової, С.А. Петренка, О.В. Потія [50], М.М. Радька, І.О. Рябініна, Є.Д. Соложенцева, Д.В. Стефанишина, В.С. Ступакова, В.С. Харченка, М.В. Хованова, В.О. Хорошка [51], М.В. Хохлова, В.П. Широчина [52], С.Я. Шоргіна, С.Ф.

Гончара [103-107, 110], Л.В. Загоруйко [116] та інших вітчизняних й іноземних науковців.

Враховуючи широке застосування РІС у різних сферах діяльності, розробка ефективних підходів до оцінювання ризиків кібербезпеки в розподілених системах має критично важливий вплив на суспільство, економіку, науку, та технології [102-107]. Вирішення проблеми оцінювання ризиків кібербезпеки в сучасних РІС забезпечить низку важливих наукових, технологічних та практичних результатів, які позитивно вплинуть на безпеку цифрового середовища та стабільність інформаційних процесів:

- Розробка та впровадження ефективних моделей оцінювання ризику дозволить своєчасно ідентифікувати загрози, оцінювати їх вплив і вживати превентивних заходів.
- Автоматизовані системи аналізу ризиків підвищать точність прогнозування атак та скоротять час реакції на потенційні загрози.
- Вчасне виявлення і усунення кіберзагроз мінімізує фінансові збитки від атак, простоїв систем та витрат на відновлення інфраструктури.
- Оптимізація ресурсів за рахунок використання інтелектуальних підходів до аналізу ризиків дозволить зменшити операційні витрати на управління безпекою.
- Впровадження сучасних підходів, зокрема методів штучного інтелекту та машинного навчання, для моделювання ризиків забезпечить новий рівень автоматизації та точності оцінки загроз.
- Використання розширених аналітичних підходів сприятиме розвитку міждисциплінарних досліджень у галузі кібербезпеки, штучного інтелекту та розподілених обчислень.

З огляду на зростаючу складність та масштаби сучасних РІС, необхідність розробки ефективних моделей оцінювання ризиків, здатних працювати в умовах високої динамічності загроз, стає дедалі актуальнішою та формує важливе науково-прикладне завдання, вирішення якого забезпечить підвищення рівня кіберстійкості сучасних розподілених інформаційних систем [108-109].

## 1.2. Теоретичні аспекти ризик-менеджменту в розподіленому середовищі

Забезпечення кібербезпеки у розподілених інформаційних системах неможливе без системного підходу до аналізу та управління ризиками ІБ. Ризик-менеджмент надає концептуальну основу для ідентифікації, оцінювання та контролю загроз, враховуючи як поточні умови функціонування системи, так і потенційні вектори атак. Розуміння сутності ризику та його складових дозволяють обґрунтовано визначати пріоритети захисних заходів та оптимально розподіляти ресурси [73, 78].

### 1.2.1. Сутність та математична інтерпретація поняття ризику кібербезпеки в розрізі PIC

На сьогоднішній день управління інформаційною безпекою відіграє ключову роль в процесах життєдіяльності практично будь-якої організації, яка застосовує сучасні технології збору, обробки та зберігання інформації. Даний процес заснований на регулярному проведенні оцінювання ризиків кібербезпеки, що дозволяє своєчасно виявляти нові загрози та вразливості, впроваджувати відповідні заходи щодо їх нейтралізації та здійснювати постійний моніторинг стану інформаційної безпеки системи, з огляду на попередній досвід та нові фактори впливу [46].

Поняття ризику є однією з фундаментальних категорій у сфері управління ІБ, оскільки воно відображає ступінь невизначеності та можливих негативних наслідків, пов’язаних з реалізацією певних загроз щодо критичних ресурсів. У контексті інформаційної безпеки розподілених систем ризик можна розглядати як функцію від ймовірності виникнення загрози за умови експлуатації наявної вразливості та ступеня впливу потенційного інциденту на конфіденційність, цілісність або доступність інформаційного активу розподіленого середовища. Таким чином, загальну модель обрахунку ризику часто формалізують у вигляді функції від ймовірності певної загрози та оцінки впливу наслідків її реалізації [53]:

$$R = f\big((P(T \to V), I(T)\big), \tag{1.1}$$

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

$I(T)$ – очікуваний негативний вплив реалізації загрози $T$.

При цьому, доцільно розглянути основні компоненти ризику:

1. **Загроза (threat)**: чинник, умова або дія, яка потенційно може порушити безпеку інформаційної системи. Загрозами можуть виступати як цілеспрямовані атаки зловмисників, так і випадкові збої апаратури, стихійні лиха чи помилки користувачів.

2. **Вразливість (vulnerability)**: слабке місце в системі, процедурі або організаційній структурі, що може бути використане загрозою для досягнення негативних наслідків. Вразливості можуть виникати через недосконаліть програмного забезпечення, помилки в конфігурації, неправильні налаштування системи керування доступом, недостатній рівень інформованості персоналу про безпекові політики тощо.

3. **Ймовірність (probability or likelihood)**: оцінка шансів реалізації загрози за рахунок експлуатації наявної вразливості. Ймовірність визначається на основі статистики минулих інцидентів, аналітичних оцінок, зовнішніх факторів (наприклад, активності кіберзлочинців), а також внутрішніх умов (рівень підготовки персоналу, ефективність контролів безпеки тощо).

4. **Вплив (impact)**: масштаби та ступінь негативних наслідків, спричинених успішною реалізацією загрози. Це може бути фінансова шкода, порушення репутації, витік конфіденційних даних, недоступність критичних сервісів, правові санкції чи зниження конкурентоспроможності.

Саме така інтерпретація ризику наводиться в NIST Special Publication 800-30 Rev. 1 «Guide for conducting risk assessments» [57]. Однак документ не надає чіткого числового підходу до обчислення цього показника.

Найпростішим та найбільш розповсюдженим математичним представленням є обрахунок ризику як добутку ймовірності настання загрози на очікуваний вплив (збиток):

$$R = P(T) \cdot I(T), \tag{1.2}$$

де $P(T)$ – ймовірність реалізації загрози $T$.

В окремих випадках ймовірність настання загрози може бути деталізована з урахуванням наявних вразливостей системи:

$$R = P(\mathrm{V}) \cdot P(V|T) \cdot I(T), \tag{1.3}$$

де $P(\mathrm{V})$ – ймовірність наявності вразливості $V$;

$P(V|T)$ – ймовірність успішної експлуатації вразливості $V$ за умови виникнення загрози $T$.

Таким чином, ризик за своєю суттю – це потенційна можливість використання певною загрозою 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, несправності обладнання, крадіжка активів), так і нематеріальні (зниження репутації та втрата довіри). Активами є ключові елементи інфраструктури та інформація, що обробляється в PIC та може нести певну цінність [43].

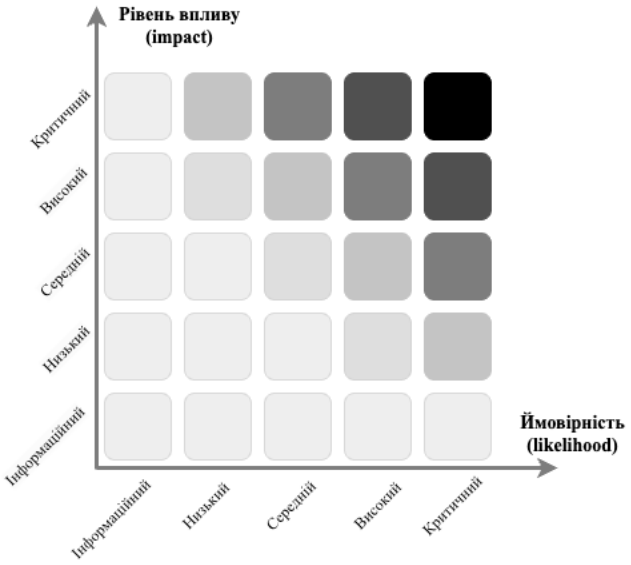


*Рис. 1.9. Приклад еталонної матриці оцінювання ризиків кібербезпеки відповідно до ймовірнісного підходу.*

Розглядаючи ризик в інформаційній безпеці з позицій наукового аналізу, важливо мати формальну математичну інтерпретацію, що дозволить кількісно та об’єктивно оцінювати ймовірність та вплив потенційних загроз. При цьому необхідно забезпечити виконання ряду вимог:

1. Чітка формалізація складових ризику: математичне представлення ризику має враховувати його основні компоненти, такі як ймовірність реалізації загроз, ступінь вразливості системи, масштаби потенційних збитків та впливу.

2. Здатність до адаптації та оновлення: в умовах динамічного середовища кіберзагроз підхід до обрахунку ризику повинен враховувати актуальні сценарії атак, а також забезпечувати гнучкість та оперативне оновлення оцінок у відповідь на зміну вхідних параметрів.

3. Підтримка сценарного аналізу та прогнозування: математичні моделі повинні сприяти моделюванню різноманітних сценаріїв реалізації ризиків, оцінці їх наслідків та визначенню оптимальних стратегій захисту.

Одним із найпоширеніших напрямів є **імовірнісне моделювання**, яке передбачає використання інструментів теорії ймовірностей і статистики в задачах оцінювання ризиків. Розрахунок ймовірностей реалізації загроз базується на історичних даних про атаки, частоту вразливостей та результатах застосування контролів безпеки [133].

Класичне математичне представлення в рамках ймовірнісного підходу (1.2-1.3) може бути розширене для врахування таких метрик безпеки як конфіденційність, доступність та цілісність інформації. Для цього можна ввести додаткові коефіцієнти та представити загальний показник ризику як суму ризиків, які впливають на окремі властивості інформації. В загальному, цей підхід може бути представлений за допомогою формул 1.4, 1.5, 1.6 та 1.7.

$$R = R_{\text{c}} + R_i + R_a = P(T) \cdot P(V) \cdot (K_{\text{c}} + K_i + K_a), \quad (1.4)$$

$$R_{\text{c}} = K_{\text{c}} \cdot P(T) \cdot P(V), \quad (1.5)$$

$$R_i = K_i \cdot P(T) \cdot P(V), \quad (1.6)$$

$$R_a = K_a \cdot P(T) \cdot P(V), \quad (1.7)$$

де $R$ – загальний рівень ризику;

$R_{\text{c}}$ – ризик порушення конфіденційності;

$K_{\text{c}}$ – коефіцієнт конфіденційності інформаційного активу;

$R_i$ – ризик порушення цілісності;

$K_i$ – коефіцієнт цілісності інформаційного активу;

$R_a$ – ризик порушення доступності;

$K_a$– коефіцієнт доступності інформаційного активу.

Такий підхід, попри свою простоту, забезпечує прозорість у тлумаченні результатів та полегшує порівняння різних сценаріїв. Проте в складних умовах масштабованих PIC залежності між факторами ризику часто є нелінійними, а ймовірності не завжди піддаються точному оцінюванню. Відтак, математичне представлення ризику в кібербезпеці не обмежується базовими ймовірнісними сценаріями, а включає використання більш складних підходів до моделювання [56].

**Баєсові мережі** дозволяють врахувати причинно-наслідкові зв'язки між факторами ризику, загрозами, вразливостями та потенційними наслідками, динамічно оновлюючи оцінки ймовірностей у реальному часі при надходженні нової інформації [131]. За теоремою Байеса, ймовірність події $H$ при настанні події $E$ вираховується за формулою 1.8:

$$P(H|E) = \frac{P(E|H)\cdot P(H)}{P(E)}, \tag{1.8}$$

де $H$ – гіпотеза (наприклад, певний вид атаки або сценарій загрози);

$E$ – нова інформація (дані моніторингу, результати аудиту безпеки тощо);

$P(H)$ – апріорна ймовірність гіпотези;

$P(E|H)$ – ймовірність спостереження $E$ за умови істинності $H$;

$P(E)$ – загальна ймовірність спостереження $E$.

Таким чином, баєсові мережі сприяють адаптивному управлінню ризиками, даючи змогу динамічно враховувати зміни у середовищі або появу нових загроз.

**Марковські моделі** використовуються для опису систем, стан яких змінюється з плином часу за певними ймовірнісними законами. У контексті кібербезпеки вони застосовуються для прогнозування ймовірності переходу системи з безпечного стану в скомпрометований та повернення до безпечного стану після реагування. Аналіз стаціонарних розподілів таких процесів дозволяє оцінити середній рівень ризику, очікуваний час до інциденту безпеки та ефективність контрзаходів.

У випадку моделювання перехідних станів системи (наприклад, від «безпечного» стану до «скомпрометованого») застосовують марковські ланцюги. Нехай система має множину станів $S = \{S_0, S_1, \dots, S_n\}$, серед яких є стани «скомпрометованості». Марковська модель описує ймовірності переходу між цими

станами. Ймовірності переходу визначаються матрицею переходів $P$, де елемент $p_{ij}$ – ймовірність переходу системи зі стану $S_\text{i}$ до стану $S_\text{j}$.

Якщо розглядати систему, яка досягла стаціонарного розподілу, де ймовірності перебування в кожному стані залишаються постійними, то цей розподіл $\pi$ буде задовільняти рівняння 1.9 та виконувати умову 1.10:

$$\pi P = \pi, \tag{1.9}$$

де $\pi$ – вектор стаціонарних ймовірностей;

$P$ – матриця переходів.

$$\sum_i \pi_i = 1, \tag{1.10}$$

де $\pi_i$ – стаціонарна ймовірність стану $S_i$.

Тоді можна розглянути ймовірності станів у момент часу *t* або оцінити ризик компроментації системи. Обмеженнями даного підходу є припущення, що ймовірності перебування в кожному стані залишаються незмінними, а також умова, що перехід системи залежить лише від теперішнього стану та не залежить від попередніх.

**Теорія ігор** дає змогу уявити ризики кібербезпеки як протистояння атакуючого та захисника, аналізуючи стратегії обох сторін для пошуку рівноваги в умовах невизначеності. Теоретико-ігрові моделі застосовуються для аналізу взаємодії між атакуючим і захисником як раціональних гравців, які прагнуть максимізувати свою вигоду. Такі моделі допомагають визначити рівноважні стратегії, оптимальні інвестиції в безпеку та оптимальну поведінку обох сторін у ситуаціях із конфліктом інтересів.

Нехай $A = \{A_0, A_1, \dots, A_n\}$ – множина можливих стратегій атакуючого, а $D = \{D_0, D_1, \dots, D_n\}$ – множина можливих стратегій захисника, та існує функція виграшу (або збитку) $U(D, A)$:

$$R = \min_D \max_A U(D, A), \tag{1.11}$$

де $R$ – оптимальний рівень ризику для захисника, обраний згідно зі стратегією мінмаксу (стратегією найгіршого випадку).

В цьому випадку захисник прагне мінімізувати негативні наслідки від дій атакуючого, проте дану задачу можна розглядати і з точки зору атакуючого: максимізація можливих збитків. Таким чином, цей підхід допомагає знаходити рівноважні стратегічні рішення, які мінімізують ризик незалежно від дій атакуючої сторони.

**Нечіткі моделі** в задачах оцінювання ризиків кібербезпеки корисні тоді, коли якісні категорії ризику необхідно перетворити на кількісні оцінки за умов неповноти або неточності наявних даних, що особливо актуально для розподілених середовищ. Оскільки у кібербезпеці часто доводиться враховувати неточні, суб'єктивні або неповні дані (наприклад експертні оцінки), нечіткі логічні моделі дозволяють кодувати ймовірнісні оцінки у термінах лінгвістичних змінних. Це дає змогу визначати ризики у якісному форматі з точнішою інтерпретацією, інтегрувати різноякісну інформацію та приймати більш зважені рішення [47].

Для ситуацій із неточною чи неповною інформацією застосовують нечіткі множини. Ймовірність та вплив можуть бути представлені нечіткими лінгвістичними змінними (наприклад, «Низький», «Середній», «Високий» рівень) з відповідними функціями належності. Тоді оцінку ризику можна отримати через нечітку логіку:

$$R = F(P, I) \tag{1.12}$$

де $F$ – нечітка функція перетворення вхідних лінгвістичних оцінок ймовірності та впливу у результуючий рівень ризику.

Методи **машинного навчання та штучного інтелекту** дають змогу автоматизувати процес виявлення складних закономірностей у великих обсягах даних про атаки та інциденти, прогнозувати можливі ризики та їх наслідки, опираючись на історичні відомості та характеристики поточного стану системи. Такі підходи особливо корисні у динамічному середовищі, де постійно з'являються нові типи загроз та вразливостей.

При наявності великих обсягів поточних та ретроспективних даних, ризик можна моделювати статистично або із застосуванням машинного навчання. Наприклад, якщо позначити характеристичний вектор системи як $x$, а функцію оцінки ризику як $f(x)$, то ризик може бути представлений як:

$$R = f(x) \quad (1.13)$$

де $x$ – характеристичний вектор системи;

$f(x)$ – функція оцінки ризику.

Таким чином, важливим аспектом математичного моделювання процесу оцінювання ризиків кібербезпеки є можливість його інтеграції в безперервний цикл управління ризиками, коли оцінки корегуються за результатами моніторингу, тестувань на проникнення, аудиту безпеки, а також у відповідь на появу нових технологічних рішень чи змін у структурі розподілених систем. Такий підхід дозволяє автоматизувати частину процесу прийняття рішень, створюючи фундамент для адаптивних систем ризик-менеджменту, здатних враховувати мінливі умови кіберпростору сучасних РІС [76, 83].

Окрім цього, важливо розуміти основні типи ризиків, що є характерними для типової розподіленої інформаційної системи. Класифікація ризиків ІБ в розподіленому середовищі може здійснюватися за різними ознаками, залежно від мети аналізу, типу системи та характеру загроз:

**За джерелами загроз:**

- Внутрішні ризики: зумовлені діями або помилками персоналу, системними збоями у внутрішній інфраструктурі, несанкціонованим доступом з боку користувачів або ненавмисною компрометацією даних.
- Зовнішні ризики: спричинені діями зловмисників поза межами організації, хакерськими атаками, шкідливим програмним забезпеченням, кібершпигунством, а також природними катастрофами, що впливають на інфраструктуру РІС.

**За природою впливу:**

- Технічні ризики: пов’язані з уразливостями у програмному та апаратному забезпеченні, мережевих протоколах і застосунках.
- Організаційні ризики: виникають через недоліки у політиках безпеки, недостатню підготовку персоналу, відсутність чітких регламентів взаємодії та реагування на інциденти тощо.

**За об’єктом впливу:**

- Ризики для конфіденційності: пов’язані з витоком або несанкціонованим використанням конфіденційної інформації.
- Ризики для цілісності: пов’язані з модифікацією даних або несанкціонованими змінами в системі.
- Ризики для доступності: пов’язані з недоступністю критичних сервісів та ресурсів.

**За інтенсивністю та масштабом впливу:**

- Стратегічні ризики: впливають на довгострокові цілі та конкурентні переваги організації.
- Операційні ризики: пов’язані з повсякденною діяльністю, процесами обробки даних та функціонуванням застосунків.

Оцінювання ризиків кібербезпеки є фундаментальним аспектом стратегії захисту даних компанії. Воно проводиться з метою підтримки прийняття рішень та негайного реагування на виявлені загрози. Окрім цього, аналіз ризиків ІБ надає можливість визначити необхідну і достатню сукупність засобів захисту інформації, нормативно-правових та організаційних механізмів щодо зниження ризиків кібербезпеки, що дозволяє забезпечити процес побудови максимально ефективної для даної організації архітектури комплексної системи менеджменту інформаційної безпеки СМІБ [71].

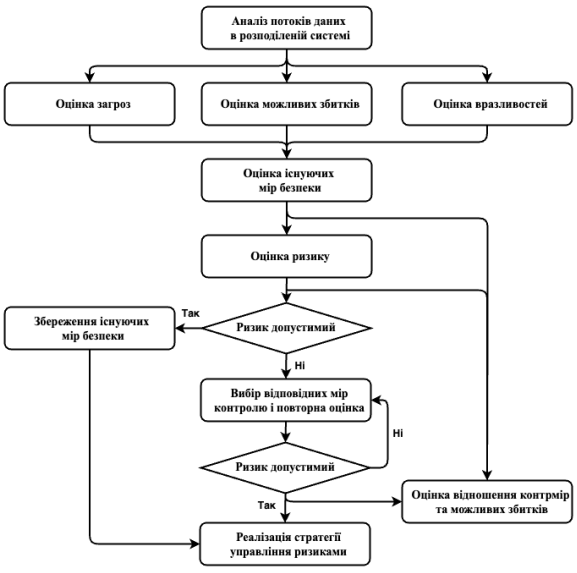


*Рис. 1.10. Процедура організації процесу аналізу ризиків інформаційної безпеки.*

Управління ризиками ІБ передбачає ітеративний процес виявлення, кількісної оцінки, аналізу та управління ризиками, з якими стикається організація. Ризик-менеджмент призначений для забезпечення стабільного режиму роботи інформаційної системи та мінімізації можливих втрат в разі реалізації загроз ІБ [36]. Як невід'ємна частина практики управління ІБ, ризик-менеджмент повинен здійснюватись на регулярній основі з метою підтримки організаційних поліпшень, вдосконалення існуючих засобів та механізмів безпеки, збільшення ефективності управлінських рішень. В умовах системної розподіленості ризик менеджмент повинен передбачати комплексний характер і враховувати оцінювання ризиків по кожному активу та підсистемі ІС [70].


*Рис. 1.11. Життєвий цикл процесу управління ризиками інформаційної безпеки.*

Типовий підхід до управління ризиками кібербезпеки в контексті розподілених інформаційних систем включає наступні етапи:

1. **Визначення прийнятного для організації рівня ризику** – критерію, що використовується для рішень про прийняття ризику або його обробку.

2. **Ідентифікація ризиків** – виявлення всіх потенційних ризиків, що можуть вплинути на безпечне функціонування системи.

На цьому етапі проводиться:

- Інвентаризація ресурсів: визначення активів (сервісів, даних, апаратних та програмних компонентів), які потребують захисту.
- Виявлення загроз та вразливостей: аналіз середовища з метою виявлення можливих загроз (зловмисні атаки, технічні збої, людські помилки, природні

катастрофи) та оцінка наявних вразливостей (некоректні налаштування, недоліки в архітектурі, слабкі місця в політиках безпеки тощо).

- Документування ризиків: формування переліку потенційних ризиків із зазначенням джерел і природи кожного з них.

3. **Аналіз ризиків** – детальний аналіз кожного ідентифікованого ризику для кращого розуміння його структури та факторів впливу.

Включає такі елементи як:

- Аналіз ймовірності та впливу: оцінка ймовірності реалізації кожної загрози та її потенційних наслідків (фінансових, репутаційних, правових чи технічних).
- Моделювання сценаріїв: розробка гіпотетичних сценаріїв реалізації загроз, визначення шляху їх поширення, аналіз можливих точок відмови та потенційних чинників, що можуть посилити чи послабити вплив ризику.
- Використання математичних і статистичних моделей: застосування методів теорії ймовірностей, математичної статистики та машинного навчання для уточнення оцінок.

4. **Оцінка ризиків** – кількісне або якісне оцінювання ризиків з метою визначення їх критичності та пріоритетності.

- Кількісна оцінка: застосування метрик на основі обрахунку, грошових еквівалентів збитків, статистичних індикаторів для прогнозування потенційних втрат тощо.
- Якісна оцінка: ранжування ризиків за рівнем / категоріями на основі експертних суджень, досвіду, порівняння з відомими еталонами або використання шкал та матриць ризику.
- Пріоритезація: процес ранжування за критеріями необхідний для розробки плану реагування на ризики та визначення їх пріоритету.

5. **Вибір стратегії поводження з ризиками** – прийняття рішення за ризиками (ризик-менеджмент) і розробка плану реагування.

- Зниження (mitigation): впровадження додаткових контролів безпеки, покращення конфігурацій, застосування криптографічного захисту, оновлення програмного забезпечення, підвищення кваліфікації персоналу тощо.
- Прийняття (acceptance): свідоме допущення існування певних ризиків, якщо потенційні витрати на їх усунення перевищують очікувані збитки.
- Передача (transfer): використання страхування, аутсорсингу безпекових послуг або угод із постачальниками для розподілу відповідальності за наслідки реалізації ризиків.
- Уникнення (avoidance): зміна архітектури, відмова від певних функцій чи процесів, які породжують надмірний ризик.

6. **Реалізація заходів з реагування та моніторингу** – розробка та впровадження обраних стратегій управління ризиками.

- Впровадження контролів безпеки: налаштування систем виявлення вторгнень, встановлення міжмережевих екранів, застосування двофакторної автентифікації, регулярні аудити ІБ та стану інфраструктури тощо.
- Моніторинг та оцінювання ефективності: постійний контроль функціонування безпекових заходів, регулярне оновлення інформації про загрози, використання систем обробки подій безпеки (SIEM) та інструментів аналітики.
- Зворотний зв’язок та адаптація: результати моніторингу дозволяють корегувати стратегії управління ризиками, удосконалювати архітектуру системи безпеки та процедури реагування на інциденти.

7. **Безперервне вдосконалення процесу** – по мірі зміни середовища та законодавчих вимог, появи нових технологій та векторів атак, необхідно переглядати ідентифіковані ризики, оновлювати моделі аналізу, корегувати стратегії та оновлювати контролі. Такий підхід дозволяє підтримувати актуальність, ефективність та надійність заходів із захисту РІС (Рис. 1.11).

Загалом, детальне опрацювання кожного з цих етапів створює методологічну й практичну основу для сталого управління ризиками кібербезпеки в динамічних та складних умовах розподілених інформаційних систем [55].

### 1.2.2. Аналіз існуючих підходів до оцінювання та моделювання ризиків інформаційної безпеки

У сучасному динамічному кіберпросторі, де розподілені інформаційні системи постають складним, неоднорідним та постійно змінним середовищем, вимоги до достовірності та оперативності оцінювання ризиків істотно зростають. Традиційні підходи, що опираються виключно на історичні дані чи експертні судження, дедалі частіше виявляються недостатньо гнучкими й адаптивними, особливо коли доводиться враховувати появу нових, раніше невідомих загроз, стрімку зміну технологічних ландшафтів або складні взаємозв'язки між компонентами системи [134]. В таких умовах на перший план виходять інтелектуальні моделі, які здатні надати формалізовану основу для дослідження ризиків у кіберпросторі розподіленого середовища [50].

Умовно серед підходів до оцінювання ризиків кібербезпеки на сьогоднішній день можна виділити наступні 3 групи:

1. Класичні математично-статистичні методи;
2. Евристичні та експертні методи;
3. Методи моделювання (симуляційні, аналітичні та методи на основі машинного навчання і штучного інтелекту).

Частина із вищезазначених методів частково була описана в попередньому параграфі. При цьому, як уже було зазначено, в рамках кожного з них може використовуватися якісний, кількісний або комбінований підхід.

До переваг кількісного підходу можна віднести точність оцінки, наочність результатів, а також можливість порівняння значення ризику, вираженого у фінансовому еквіваленті, з обсягом інвестицій, необхідних для реагування на даний ризик. Однак часта відсутність достатньої кількості статистичних даних призводить до зниження адекватності результатів оцінювання. Іншими обмеженнями є складність, висока трудомісткість і значна тривалість виконання [54].

Якісні методики більш поширені, однак в них використовуються надто спрощені шкали, що зазвичай містять три рівня оцінки ризику (високий, середній, низький). Оцінювання проводиться на основі експертних опитувань, а перспективні

інтелектуальні методи поки застосовуються недостатньо. Іншими недоліками є недостатня наочність і складність використання результатів аналізу ризиків для економічного обґрунтування та оцінки доцільності інвестицій в заходи безпеки та реагування. З іншого боку, до переваг якісного підходу можна віднести його відносну простоту, а також зменшення часових і ресурсних витрат, необхідних для проведення процедури оцінювання ризиків.

Комбінований підхід передбачає інтеграцію якісного та кількісного методів оцінювання з метою застосування переваг кожного з них та забезпечення більш збалансованого й обґрунтованого результату [51].

**Класичні математично-статистичні методи** використовують ймовірнісні моделі та статистичні підходи для оцінювання на основі історичних даних та поточного стану системи. Вони засновані на аналізі емпіричних даних про попередні інциденти, частоту реалізації загроз, час між атаками та масштаби завданих збитків для оцінки ймовірностей та очікуваних наслідків загроз [45, 99]. Прикладами застосовуваних методів первинного аналізу для кількісного обрахунку рівня ризику можуть бути підходи на основі аналізу ймовірностей, а також математичного обрахунку фінансових збитків та потенційних втрат (наприклад відповідно до FAIR методології) [79-81]. Саме класичні математично-статистичні методи надають системний підхід до аналізу загроз і вразливостей, та найкраще регламентовані міжнародними стандартами та методологіями оцінювання ризиків ІБ.

Недоліком статистичного підходу є суттєва обмеженість в динамічному середовищі сучасних РІС, недостатня адаптивність, та значна залежність від якості і репрезентативності історичних даних. Якщо дані неповні або не відображають реальних умов поточного стану середовища, оцінки ризику можуть бути неточними. Таким чином, математично-статистичні методи ефективні в стабільних статичних середовищах з доступом до великої кількості релевантних даних і менш придатні для аналізу в складних динамічних умовах масштабованих РІС, оскільки погано враховують появу нових, ще не досліджених загроз чи зміну поведінки зловмисників [42, 101].

**Евристичні та експертні методи** оцінювання передбачають використання чітко формалізованих правил та залучення кваліфікованих фахівців із інформаційної безпеки, аналітиків, інженерів та менеджерів ІБ. Сутність методу експертних оцінок полягає у проведенні експертного аналізу проблеми з застосуванням кількісної або якісної оцінки гіпотез та подальшої обробки результатів. Оцінка рівня ризику проводиться на основі суб'єктивного аналізу ймовірності настання несприятливої події шляхом вивчення та оцінювання факторів, що впливають на це. Перевагою даного методу є простота та доступність для практичного застосування.

Для об'єктивності та неупередженості результатів роботу по визначенню та оцінці ризиків інформаційної безпеки повинні проводити спеціальні експерти, які мають необхідний досвід та підготовку з цього питання. Обмеженнями для цього підходу є висока залежність від компетентності експертів, суб'єктивність оцінок та обмежена відтворюваність. Помилкова оцінка одного ключового фахівця може істотно вплинути на загальний результат, особливо в умовах обмеженої вибірки. При цьому різні експерти можуть мати нерівномірний досвід в предметній області, різний рівень обізнаності щодо контексту загроз, упередження або неоднаковий доступ до релевантних даних. Неможливість ефективного застосування в масштабованих динамічних системах через труднощі оновлення оцінок в режимі реального часу, складність у впровадженні, необхідність постійного оновлення баз знань та налаштування правил роблять обмеженим використання такого інструментарію в задачах оперативного аналізу та оцінювання ризиків в розподілених системах [40].

**Методи моделювання** передбачають використання формальних, заздалегідь визначених математичних чи логічних моделей для оцінювання ризику [100]. Такі підходи можуть включати **ймовірнісні моделі**, **баєсові мережі**, **марковські процеси**, **теоретико-ігрові моделі**, **нечітку логіку**, **методи імітаційного моделювання** та **симуляційні техніки**, а також методи засновані на **алгоритмах машинного навчання** та **штучного інтелекту**. Методи моделювання є найширше представленими на практиці, оскільки дозволяють найкращим чином відобразити складні взаємозв'язки між загрозами, вразливостями, контролями безпеки та потенційними наслідками [41].

Порівняно з попередніми підходами методам моделювання притаманний ряд переваг:

- Об’єктивність та формалізованість: такі моделі опираються на чіткі математичні або логічні правила, що зменшує суб’єктивність та покращує повторюваність результатів.
- Гнучкість та адаптивність: моделі можна оновлювати при появі нових даних або зміні умов середовища, що дозволяє динамічно корегувати оцінку ризику.
- Підтримка аналізу складних взаємозв’язків: моделі здатні враховувати нелінійні залежності між факторами ризику, взаємний вплив загроз, взаємодію різних компонентів інформаційної системи та динаміку середовища.
- Масштабованість: моделювання можна застосовувати для різних масштабів систем – від окремих компонентів до великих розподілених інфраструктур.

Класичні підходи мають цінність в окремих сценаріях застосування, проте вони часто обмежені суб’єктивністю та залежністю від історичних даних, не враховують нові раніше невідомі загрози, а також не надають належного ефекту в умовах динамічного та масштабованого середовища сучасних РІС. Методи моделювання, опираючись на формальні математичні принципи та аналітичні інструменти, пропонують більш гнучкий, адаптивний та науково обґрунтований підхід до оцінювання ризиків розподіленого середовища. Вони дозволяють врахувати складну динаміку кіберзагроз і допомагають ухвалювати аргументовані рішення в умовах невизначеності.

Безперечно, методи моделювання не є універсальним засобом розв’язання всіх проблем: вони вимагають ретельного збору даних, їх калібрування, валідації та експертної інтерпретації результатів. Проте їх переваги у вигляді формальної строгості, об’єктивності, можливості оцінки складних сценаріїв та нелінійних взаємодій, а також підтримки динамічного оновлення оцінок – роблять їх потужним інструментом у руках дослідників. Саме методи моделювання закладають основу для побудови сучасних, науково обґрунтованих систем оцінювання та управління ризиками кібербезпеки, здатних гнучко реагувати на нові виклики цифрової епохи [48-49].

До найбільш поширених та часто застосовних методів моделювання процесу оцінювання ризиків в досліджуваній предметній області відносяться:

1. **Ймовірнісне моделювання**

- Баєсові мережі (Bayesian Networks, BN) – ефективні для моделювання невизначеності, використовуються для обчислення ймовірностей складних багаторівневих загроз на основі історичних даних та аналізу причинно-наслідкових зв’язків; проте вимагають значних обчислювальних ресурсів для побудови складних моделей, та не завжди ефективні в динамічних умовах, де зв’язки між подіями можуть змінюватись [131].
- Марковські процеси (Markov Chains, Hidden Markov Models, HMM) – моделюють динаміку ризиків шляхом представлення системи як послідовності станів із ймовірнісними переходами, добре підходять для відтворення динамічних процесів; проте вимагають великих обсягів даних та мають обмежену гнучкість для моделювання складних взаємодій.

2. **Імітаційне моделювання**

- Метод Монте-Карло (Monte Carlo, MC) – використовується для аналізу ймовірностей шляхом великої кількості випадкових повторюваних симуляцій сценаріїв, широко застосовується у фінансовій та технічній оцінці ризиків; проте потребує точного визначення вхідних параметрів і розподілів ймовірностей, і є менш ефективним для динамічних загроз, що швидко змінюються.
- Agent-Based Modeling (ABM) – дозволяє симулювати складну групову поведінку шляхом моделювання дій та взаємодії великої кількості автономних агентів у заданих сценаріях, може адаптуватися до змін у поведінці загроз; проте вимагає значних обчислювальних ресурсів та передбачає високу складність розробки і налаштування моделей.
- System Dynamics (SD) – пропонує оцінювання через аналіз взаємозв’язків між компонентами системи, їх взаємний вплив та взаємодію; підходить для макроаналізу кіберзагроз, однак цей метод краще використовувати для довгострокових прогнозів та стратегічного планування, а не оперативної оцінки

ризиків; має обмежену ефективність у реальному часі та не завжди підходить для оперативного виявлення пріоритетних ризиків.

- Графові моделі атак (Attack Graphs) – використовуються для побудови сценаріїв атак на систему з метою аналізу залежностей між вразливостями та можливими шляхами проникнення; потребують актуалізації в міру появи нових вразливостей та можуть бути складними у великих масштабованих системах.

3. **Симуляція атак**

- Теорія ігор (Game Theory) – моделює взаємодію атакувальників і захисників як гру з оптимізацією стратегій, може застосовуватися для аналізу економічних аспектів оцінювання ризиків кібербезпеки; проте має обмежену застосовність для складних, нерегламентованих загроз.

- Attack Trees – ієрархічно представляють можливі атаки та шляхи їх реалізації, що спрощує аналіз вразливостей системи та дозволяє оцінювати ефективність контрзаходів; проте не враховує динамічні зміни загроз, вимагає актуалізації для нових векторів атак та може бути складним у використанні для великих систем.

- Kill Chain Analysis (MITRE ATT&CK) – аналізує атаки на основі фаз їх виконання, використовується для проактивного реагування; підхід корисний для аналізу атак, проте він більше орієнтований на виявлення загроз, ніж на прогнозування ризиків, та не завжди ефективний для нових типів атак.

4. **Машинне навчання**

- Штучні нейронні мережі (Neural Networks: ANN, CNN, RNN, LSTM) – дозволяють знаходити складні патерни в кіберзагрозах (особливо при використанні парадигми глибинного навчання), підходять для аналізу великих обсягів даних у реальному часі, мають здатність до самонавчання та адаптації; проте вимагають великих обчислювальних потужностей, та передбачають складність інтерпретації результатів.

Відповідно до результатів комплексного дослідження [82], де було здійснено систематичний аналіз останніх наукових публікацій у сфері розробки моделей динамічної оцінки ризиків (dynamic risk assessment, DRA), на сьогодні

використовується безліч різноманітних методів аналізу та оцінювання ризиків кібербезпеки, основна відмінність яких полягає в використовуваних підходах та застосовуваних шкалах оцінки рівня ризику: кількісних або якісних. В процесі дослідження 50-ти пропонованих моделей DRA, класифікованих на основі відповідних методів первинного аналізу, які вони використовували, було розглянено ключові характеристики цих моделей, включаючи рівень зрілості, область застосування, а також дані, що використовуються для отримання результатів. Результати дослідження демонструють, що переважна більшість підходів використовують кількісну шкалу оцінювання (42 моделі із 50 досліджуваних), при цьому 48% описаних моделей засновані на нейромережевих методах аналізу, що підкреслює важливу тенденцію.

Саме нейромережевий підхід в останні роки демонструє перспективні результати в задачах інтелектуального аналізу та оцінювання ризиків кібербезпеки розподіленого середовища складних та масштабованих РІС, що підтверджується рядом наукових досліджень в цьому напрямку [82-83, 95-97, 112-114, 121-125]. Окрім цього, методи засновані на алгоритмах машинного навчання та штучного інтелекту дозволяють зменшити суб’єктивність експертних суджень, надати науково-обґрунтовану основу для прийняття рішень та автоматизувати процеси оцінювання ризиків у складних, динамічних розподілених інформаційних системах.

З огляду на ряд вищеописаних переваг для предметної області, специфіку та особливості досліджуваної проблеми, що пов’язана із оцінюванням ризиків кібербезпеки в складних динамічних умовах масштабованих РІС та необхідністю оперативного аналізу великих масивів гетергенних даних розподіленого середовища, а також характеристики первинних наборів даних для аналізу – в рамках дисертаційного дослідження **пропонується обрати нейромережевий підхід в якості основного інструментарію моделювання**.

Отже, на основі проведеного аналізу можна зробити висновок, що розробка моделей та методів підвищення ефективності оцінювання ризиків кібербезпеки в складних масштабованих розподілених інформаційних системах на основі

нейромережевого аналізу гетерогенних даних розподіленого середовища складає актуальне наукове завдання [22, 61, 63, 67, 69, 71-72].

### 1.3. Порівняльний аналіз міжнародних стандартів і методологій оцінювання та управління ризиками кібербезпеки в контексті PIC

Формування науково-обґрунтованих моделей оцінювання ризиків кібербезпеки неможливе без урахування усталених міжнародних стандартів та визнаних методологій. Ці нормативні документи відображають колективний досвід фахівців з усього світу, узагальнений у вигляді рекомендацій, процедур, критеріїв та вимог, спрямованих на підвищення рівня безпеки інформаційних систем. Орієнтація на стандарти та апробовані методології не лише забезпечує узгодженість та порівнюваність підходів, а й дозволяє інтегрувати найкращі практики у процес розробки нових моделей оцінювання ризику. Відповідність прийнятим нормам полегшує взаємодію між різними організаціями та установами, підвищуючи прозорість, довіру та передбачуваність у прийнятті рішень щодо управління ризиками. Таким чином, аналіз міжнародних стандартів та методологій стає ключовим кроком на шляху до створення більш стійких, адаптивних та універсальних підходів до оцінювання ризиків розподілених систем.

На сьогоднішній день багато провідних держав та міжнародних організацій розробляють чималу кількість стандартів у сфері аналізу та оцінювання ризиків інформаційної безпеки. Це перш за все міжнародні та національні стандарти з ризик-менеджменту – ISO/IEC 31000, COSO II, FERMA, ISO/IEC 27005, NIST Risk Management Framework (RMF), оцінювання ризиків та менеджменту інформаційної безпеки – ISO/IEC 27001, ISO/IEC 17799, BS7799, NIST SP 800-30, BSI-Standard 200-3, ISO/IEC 15408; стандарти аудиту, що відображають питання інформаційної безпеки, – COBIT, SAS 55/78, SAC тощо.

Міжнародні стандарти відіграють важливу роль у формуванні єдиного підходу до розуміння процесу оцінювання та управління ризиками. Їх авторитетність зумовлена колективним досвідом експертів із різних країн та галузей, що сприяє уніфікації термінології, процедур і вимог, а також основних етапів практичного

застосування. Особливої уваги заслуговують стандарти ISO/IEC 27005 [60] та рекомендації NIST SP 800-30 [57], які часто розглядаються як базові орієнтири в процесі оцінювання ризиків.

**ISO/IEC 27005:2022** є частиною широкого сімейства стандартів ISO/IEC 27000, зосередженого на системному підході до управління інформаційною безпекою. Основна мета цього стандарту – надати узагальнену методологічну основу для процесу ризик-менеджменту, включно з ідентифікацією, аналізом, оцінкою, обробкою та моніторингом ризиків. ISO/IEC 27005 не встановлює конкретних метрик або формул для кількісного оцінювання ризику, натомість пропонує гнучку рамкову концепцію, яку можна адаптувати до специфіки конкретної організації. Такий підхід сприяє інтеграції процесів управління ризиками з іншими елементами системи менеджменту інформаційної безпеки, визначеними, зокрема, у стандарті ISO/IEC 27001 [58]. Це робить ISO/IEC 27005 важливим орієнтиром для організацій, що прагнуть впровадити найкращі світові практики, забезпечити відповідність вимогам сертифікаційних аудитів, та гармонізувати внутрішні процеси з глобальними тенденціями [60].

**NIST SP 800-30**, виданий Національним інститутом стандартів та технологій США, є детальним керівництвом з проведення оцінювання ризиків у галузі інформаційної безпеки і являє собою частину ширшого фреймворку NIST RMF. На відміну від ISO/IEC 27005, який є більш концептуальним, NIST SP 800-30 пропонує більш чітку методичну схему, включно з етапами визначення загроз, вразливостей, оцінювання ймовірності та впливу, а також формування рекомендацій щодо реагування. Цей документ містить низку прикладів, таблиць та практичних порад, що полегшують його використання у конкретних проєктах. Більш операційна спрямованість NIST SP 800-30 дозволяє організаціям проводити оцінювання ризиків із конкретними результатами, застосовуючи систематичні підходи до агрегації, обробки та інтерпретації даних. Завдяки цьому, стандарт є особливо цінним для структур, які потребують швидкого впровадження практичних рішень [57].

У порівнянні з ISO/IEC 27005, NIST SP 800-30 надає більш детальний опис самого процесу оцінювання ризиків, включаючи методики ідентифікації, аналізу

загроз і оцінки впливу, тоді як ISO/IEC 27005 концентрується на концептуальних аспектах управління ризиками та його інтеграції з системним менеджментом. Обидва стандарти можна вважати взаємодоповнювальними: ISO/IEC 27005 створює теоретичний управлінський фундамент, а NIST SP 800-30 – надає більш прикладний інструментарій для проведення оцінювання.

Аналіз стандартів та нормативних документів у сфері інформаційної безпеки свідчить про те, що створення ефективної СМІБ неможливе без ідентифікації та оцінювання ризиків. Проте жоден зі стандартів не надає чіткого пояснення, яким чином необхідно виконувати вказані процедури. Ця задача зазвичай покладається на керівників компанії, або осіб, відповідальних за впровадження та підтримку систем менеджменту інформаційної безпеки.

На сьогодні існує широка різноманітність методик для оцінювання ризиків інформаційної безпеки: методологія оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standardsand Technology, NIST), методологія аналізу та контролю інформаційних ризиків CRAMM (CCTA Risk Analysis and Managment Method, CRAMM), метод оцінки операційно критичних загроз, активів та вразливостей (Operationally Critical Threats, Assets and Vulnerability Evaluation, OCTAVE), методологія пропорційного аналізу ризиків (MEthod for Harmonized Analysis of RIsk, MEHARI), методологія аналізу інформаційних ризиків Міжнародного Форуму з інформаційної безпеки (Information Risk Analysis Methodology, IRAM) тощо. Останнім часом все більша увага приділяється методиці факторного аналізу інформаційних ризиків (Factor analysis of information risk, FAIR), яка передбачає найбільш повне врахування факторів виникнення інформаційних ризиків.

Методологія оцінки ризиків Національного інституту стандартів та технологій США NIST – є однією найвідоміших класичних систем управління ризиками в інформаційній безпеці. Вона ґрунтується на розгляненому вище стандарті NIST SP 800-30 та надає поради щодо проведення оцінювання ризику інформаційних систем різного рівня критичності. Використання такої методики передбачає етапи, наведені на Рис. 1.12.


*Рис. 1.12. Процедура управління ризиками відповідно до NIST 800-30.*

Методологія аналізу факторів ризиків інформаційних технологій FAIR – представляє собою відтворювану та структуровану модель для кількісної оцінки та управління ризиками кібербезпеки, що пропонує найкращі практики бізнес-орієнтованого підходу до вимірювання, контролю та попередження інформаційних ризиків. Методологія розроблена глобальним консорціумом по стандартам The Open Group та забезпечує факторний підхід до аналізу, заснований на аналізі чинників, які впливають на різні складові ризику. Згідно з нею, ключовими факторами є частота появи інциденту та імовірні втрати від його настання. FAIR являється єдиною міжнародною стандартизованою кількісною моделлю оцінювання ризиків. Згідно з підходом FAIR, управління ризиками передбачає інтеграцію людських ресурсів, процесів, політик і технологічних засобів для досягнення фінансово обґрунтованого контролю над прийнятним рівнем потенційних втрат (Рис. 1.13).


*Рис. 1.13. Етапи оцінювання ризику відповідно до FAIR.*

В цілому, методика розбита на чотири етапи: ідентифікація об’єктів оцінювання, оцінка частоти виникнення загроз, оцінка величини ймовірності потенційного збитку, отримання та формалізація ризику.

Як результат, обрахунок величини ризику зводиться до побудови матриці, де шукана величина буде знаходитися на перетині значення частоти подій, що призводять до втрат, і максимального значення втрат від реалізації даної загрози. Таким чином, методика забезпечує структурований та послідовний процес кількісного оцінювання ризиків. Водночас отримані результати можуть бути недостатньо зручними для практичного використання, з огляду на широкий діапазон можливих значень ризику, що ускладнює прийняття рішень в умовах невизначеності.

Методологія оцінки інформаційних ризиків CRAMM є одним з класичних і широко впроваджених методів для аналізу та управління інформаційними ризиками, що розроблений Агентством з комп’ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency, CCTA) на замовлення уряду Великобританії для підтримки стандарту BS7799 та прийнятий як державний стандарт для оцінювання ризиків інформаційної безпеки в різних галузях діяльності. Він використовується з 1985 року та в наш час представлений у вигляді окремого однойменного програмного продукту, що реалізує метод CRAMM (розробка компанії Insight Consulting Limited).

Застосування CRAMM дозволяє здійснювати економічно обґрунтоване планування витрат на заходи ІБ та ризик-менеджмент, сприяючи оптимізації бюджетів і запобіганню нераціональним витратам.

Методика CRAMM передбачає поділ процедури аналізу на 3 послідовні етапи:

1. Визначення чи достатньо для забезпечення захисту існуючих засобів та традиційних механізмів ІБ.
2. Ідентифікація та оцінювання ризиків.
3. Вибір необхідних контрзаходів.

На кожному етапі створюється звітна документація та анкети для проведення інтерв’ю, а також визначаються контрольні списки заходів контролю та перевірки. Алгоритм методики CRAMM подано на Рис. 1.14.

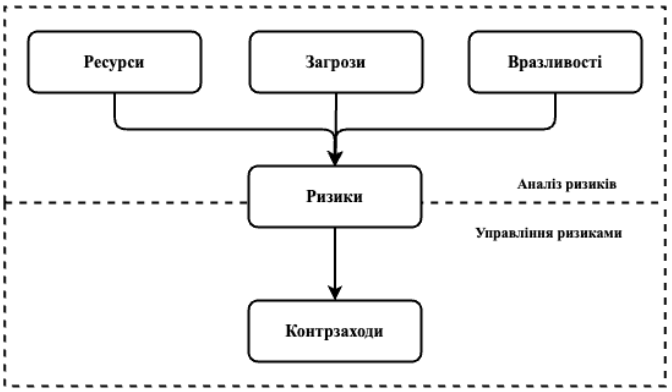


*Рис. 1.14. Структура управління ризиками відповідно до методики CRAMM.*

Незважаючи на значну універсальність та зручність, методика має суттєві недоліки, до яких відносяться значна вартість ліцензії та необхідність спеціальної підготовки користувачів.

Методологія пропорційного аналізу ризиків MEHARI – це метод оцінки та управління ризиками з відкритим вихідним кодом, призначений для професіоналів в області ІБ. Він розроблений на основі міжнародних стандартів ISO/IEC 27001 та ISO/IEC 27005 і характеризується структурованим модульним компонентно-процесним підходом до управління ризиками, який інтегрує технічні, організаційні та правові аспекти, а також дозволяє здійснювати комплексне оцінювання з урахуванням не лише параметрів інформаційної системи, а й внутрішньої організаційної структури компанії, чинної нормативно-правової бази, специфіки операційного середовища та умов праці персоналу [85].

Сутність методології можна відобразити наступними етапами:

1. Опис активів та аналіз поточного рівня захищеності;
2. Аналіз ризиків та можливих сценарії їх реалізації;
3. Ідентифікація контрзаходів та усунення причин виникнення ризиків;
4. Впровадження необхідних заходів безпеки;
5. Обробка ризиків.

Метод оцінки операційно критичних загроз, активів та вразливостей OCTAVE – методологія оцінювання критичності активів, вразливостей та загроз, що була розроблена в Університеті Карнегі-Мелон (США) та широко використовується у

всьому світі при впровадженні систем корпоративного ризик-менеджменту. Для компаній різного розміру та галузей діяльності, методологія має ряд модифікацій, що дозволяють гнучко підлаштуватись під потреби та умови замовника:

– OCTAVE – базовий варіант, призначений для великих підприємств із чисельністю персоналу понад 300 осіб;

– OCTAVE-S – спрощена версія, розроблена для середніх компаній (до 100 співробітників), із меншою потребою в ресурсах;

– OCTAVE Allegro – модифікація, орієнтована на індивідуальний експертний аналіз, яку виконує спеціальний консультант без широкого залучення персоналу організації [86].

Особливістю даної методології є те, що процес аналізу ризиків кібербезпеки здійснюється внутрішніми працівниками організації. Методологія реалізується шляхом серії спеціалізованих семінарів і воркшопів, у межах яких визначаються ключові ролі, формуються проєктні групи та координується подальша діяльність.

Наступні етапи включають розробку профілю загроз організації, аналіз наявних вразливостей, оцінювання ризиків ІБ, прийняття рішення з їх обробки та розроблення стратегії забезпечення безпеки (Рис. 1.15). Ризик обраховується як середнє значення річних втрат організації внаслідок реалізації загроз ІБ.


*Рис. 1.15. Етапи аналізу ризиків за методикою OCTAVE.*

До переваг методології OCTAVE відносять її простоту та загальнодоступність, можливість впровадження для компаній різного розміру та сфери діяльності. Методика розповсюджується на безоплатній основі, а на її базі вже створено чимало комерційних програмних продуктів, що реалізують положення OCTAVE. Слід окремо виділити високий рівень гнучкості методики та швидкість її впровадження. Разом із

тим, недоліком методології є її орієнтація на якісне оцінювання**,** що унеможливлює отримання точних числових значень рівня ризику (Рис. 1.16).

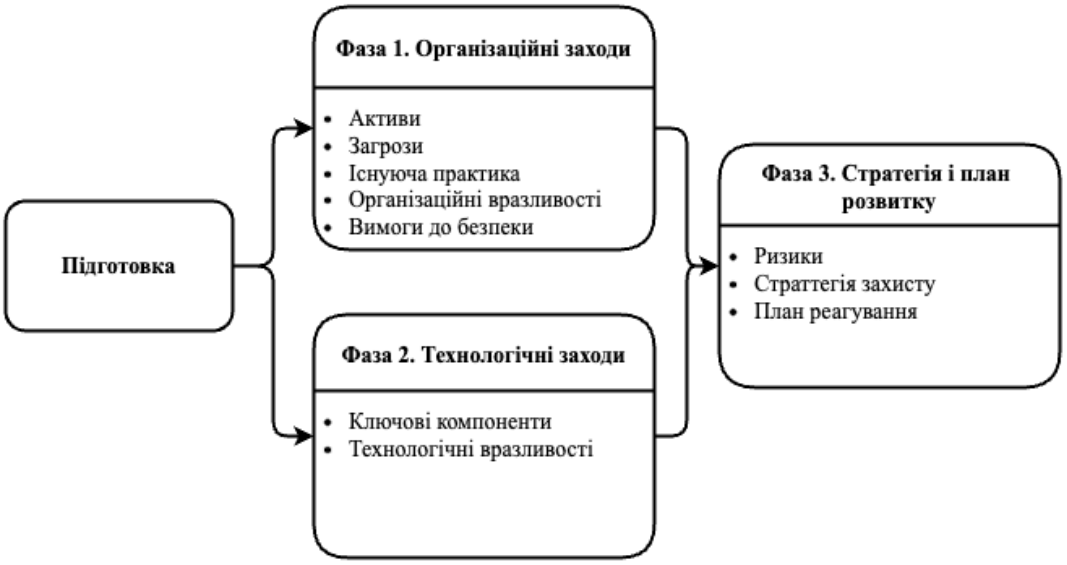


*Рис. 1.16. Послідовність трьох складових фаз методу OCTAVE.*

Методологія аналізу інформаційних ризиків Міжнародного Форуму з інформаційної безпеки IRAM – методика, що розроблена з метою допомогти компаніям краще розуміти природу ризиків інформаційної безпеки та управляти ними використовуючи комплексний підхід орієнтований в першу чергу на вимоги бізнесу. Саме через призму фактору впливу на бізнес розглядаються вимоги до конфіденційності, цілісності та доступності інформації, які можуть бути доповнені даними про імовірність втрат та збитків [87].

Методологія передбачає наступні етапи:

- Ідентифікація інформаційних активів;
- Класифікація активів з точки зору безпеки;
- Моделювання загроз;
- Заходи по зниженню та усуненню загроз;

Таким чином, проведений аналіз найпоширеніших методик з управління ризиками в сфері інформаційної безпеки дозволяє визначити їх основні переваги та недоліки, представлені в Таблиці 1.1 [40].

*Таблиця 1.1*

*Переваги та недоліки сучасних методик з управління ризиками*

| Методика | Переваги | Недоліки |
|---|---|---|
| NIST | - простота впровадження та використання;<br>- універсальність і масштабованість, гнучкість конфігурації та можливість застосування для організацій будь-якого розміру та галузі діяльності;<br>- підтримка якісного та кількісного аналізу;<br>- наявність чималої кількості програмних продуктів, що реалізовують принципи методики та дозволяють автоматизувати процеси оцінювання; | - необхідність належної підготовки та значна трудомісткість, що може бути перепоною для малого або середнього бізнесу;<br>- орієнтація на державний сектор та федеральні організації США;<br>- надмірна деталізованість та низька придатність для оперативної оцінки ризику; |
| FAIR | - структурованість підходу та підвищення прозорості;<br>- забезпечення аналізу широкого спектру факторів ризику;<br>- надання об'єктивної кількісної оцінки у вигляді грошового еквіваленту можливих втрат; | - складність впровадження та необхідність підготовки персоналу;<br>- високі вимоги до даних, які не завжди доступні;<br>- надмірна деталізованість та орієнтація на використання лише для великих організацій; |
| MEHARI | - глибокий структурований аналіз та фокус на підтримку управлінських рішень;<br>- підтримка якісного та кількісного аналізу;<br>- сумісність зі стандартами ISO/IEC 27001/27005;<br>- доступність інструментів та шаблонів, відсутність ліцензування; | - трудомісткість та складність у впровадженні без попереднього навчання;<br>- недостатня адаптація до нових ризиків, відсутність автоматизації процесів;<br>- обмежене глобальне розповсюдження, відсутність офіційної сертифікації чи підтримки; |
| CRAMM | - системність та формалізованість, чіткий, покроковий підхід до аналізу ризиків;<br>- універсальність і можливість застосування для організацій як державного, так і комерційного сектору;<br>- наявність програмних продуктів, що реалізовують принципи методики; | - небхідність спеціальної підготовки і високої кваліфікації;<br>- складність і трудомісткість, повільний процес аналізу;<br>- генерування великої кількість паперової документації;<br>- моральна застарілість та низька адаптивність до нових технологій;<br>- комерційне спрямування; |
| OCTAVE | - простота і структурованість;<br>- швидкість впровадження та гнучкість, можливість застосування для організацій різного розміру та галузей діяльності;<br>- наявність програмних продуктів, що реалізовують принципи методики;<br>- акцент на захист критичних бізнес-активів; | - надання тільки якісної оцінки ризику;<br>- висока суб'єктивність та залежність від людського фактору;<br>- обмежена автоматизація, слабкий фокус на сучасні кіберзагрози; |
| IRAM | - бізнес-орієнтований підхід;<br>- структурованість та послідовність процесу;<br>- масштабованість, інтеграція з корпоративним ризик-менеджментом; | - складність впровадження та реалізації, висока вартість;<br>- обмежена гнучкість в організаціях малого розміру; |

Задача щодо вибору та впровадження методики оцінювання ризиків інформаційної безпеки є вкрай важливим етапом створення комплексної системи захисту. Основними недоліками розглянутих методологій є врахування недостатньої кількості факторів, що впливають на оцінку ризику, обмеженість для практичного застосування в динамічних масштабованих розподілених системах та надання якісної оцінки, що не забезпечує точного показника ризику, яким би могли оперувати керівники компанії та експерти з ІБ.

Таким чином, орієнтація на міжнародні стандарти та методології надає можливість обрати найбільш відповідний спосіб оцінювання ризику, врахувати кращі світові практики, зрозуміти сильні та слабкі сторони кожного підходу, а також забезпечити інтероперабельність, масштабованість та відповідність вимогам регуляторів. Врахування стандартів ISO/IEC 27005, NIST SP 800-30 та інших комплексних підходів до оцінювання ризиків інформаційної безпеки допоможе сформувати стійкий фундамент для подальшої розробки науково-обґрунтованих моделей, які будуть здатні ефективно реагувати на сучасні виклики кіберпростору.

### 1.4. Постановка науково-прикладної проблеми та завдань дисертаційного дослідження

У сучасних умовах розвитку глобального інформаційного середовища розподілені інформаційні системи набувають дедалі ширшого застосування, демонструючи високу динамічність, масштабованість та гетерогенність. Для таких систем характерне функціонування в умовах дії випадкових чинників, наявність негативних впливів різної природи, активна взаємодія із зовнішнім середовищем та висока вартість наслідків можливих порушень чи помилок у роботі. Організація оцінювання ризиків 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. Динамічне ускладнення кіберзагроз та стрімке зростання масштабів, складності та розподіленості обчислювальних ресурсів обумовлюють необхідність удосконалення підходів до оцінювання ризиків у таких

системах. Попри значний обсяг досліджень, проведений аналіз демонструє ряд суттєвих недоліків та низьку ефективність існуючих методів оцінювання ризиків у контексті РІС [69].

Основні проблеми існуючих підходів до оцінювання ризику в РІС пов'язані з такими аспектами предметної області:

- **Висока складність аналізу ризиків у розподілених середовищах**. Децентралізована структура та динамічний характер РІС, їх масштабованість та широкий спектр наявних загроз обумовлюють аналітичну та технологічну складність організації комплексного аналізу безпекової ситуації.
- **Наявність невизначеності та неповноти даних**. Розподілені системи характеризуються генерацією великих масивів гетерогенних даних безпекового характеру, значна частина яких є неповною, неоднорідною за структурою або застарілою. Це ускладнює точність та об'єктивність оцінювання ризиків, зокрема для сценаріїв з високим ступенем динаміки та необхідністю адаптації.
- **Складність агрегації та аналізу великих обсягів даних**. РІС формують значні об'єми багатовимірних даних, які потребують комплексних механізмів збору, кореляції та оперативної обробки з урахуванням різних рівнів абстракції. Класичні методи часто неспроможні забезпечити швидкий і точний аналіз у реальному часі, що є критично важливим у контексті запобігання загрозам розподіленого середовища.
- **Концептуальний характер існуючих стандартів та методологій**. Відсутність універсального практично-орієнтованого підходу, що враховує специфіку розподілених систем, а також обмеженість наявних стандартів та методологій створює значні виклики для їх практичного застосування.
- **Необхідність забепечення адаптивності та масштабованості**. Більшість традиційних підходів не враховують специфіку динамічних умов функціонування розподілених систем та масштабування їх компонентів, що є ключовими характеристиками РІС.

Таким чином, на перешкоді постають труднощі оперативного аналізу різнорідних даних, необхідність узгодження інформації, отриманої від різних джерел, мінливість розподілених метрик, що вимагає широкого арсеналу засобів аналітичного

опрацювання та інтелектуальної обробки даних різної природи, проблема неповноти інформації про складові компоненти розподіленої системи та складність комплексного багатофакторного аналізу в цілому. Виникає потреба з однієї сторони – в наборі методів та інструментів, здатних усунути зазначені перешкоди, а з іншої – в новому підході до організації досліджень ризиків інформаційної безпеки розподіленого середовища і виконання комплексного аналітичного оброблення великих масивів розподілених даних різної природи, що враховує як технологічні аспекти оцінки, так і необхідність відповідності регуляторним документам та стандартам ІБ [61, 63].

Поточні підходи до аналізу кіберризиків переважно ґрунтуються на статистичних методах або експертних оцінках та значною мірою опираються на традиційні стандарти та методології ризик-менеджменту (ISO/IEC 27005, NIST SP 800-30, OCTAVE, FAIR тощо). При цьому регуляторне та нормативно-правове забезпечення, а також міжнародні стандарти з інформаційної безпеки, визначають загальні вимоги до процесів оцінювання ризиків, проте не надають універсальних інструментів для гнучкого та автоматизованого аналізу у режимі реального часу. Хоча вони й закладають фундаментальні принципи та структурно оформлюють процес управління ризиками ІБ, проте носять по більшій мірі концептуальний характер, не забезпечують практичних рекомендацій, часто залишаються недостатньо гнучкими та мають обмежені можливості щодо динамічного оновлення оцінок в умовах РІС.

Зокрема, класичні підходи:

- Не повною мірою враховують специфіку масштабованих РІС, де різноманіття топологій та протоколів, постійні зміни в конфігурації, великий обсяг трафіку, а також різнорідність обладнання та інфраструктури ускладнює моніторинг усіх компонентів і застосування статичних методів.
- Забезпечують низьку ефективність в задачах оперативної обробки великих масивів гетерогенних та розподілених метаданих, які відображають стан мережевої інфраструктури, ефективність контролів безпеки та рівень відповідності нормативно-правовим вимогам.

- Не враховують нові раніше невідомі загрози, та передбачають високу суб’єктивність, ресурсоємність і складність впровадження в умовах масштабованих систем.
- Передбачають низьку інтегрованість розрізнених підходів, що фрагментарно оцінюють окремі аспекти безпеки, не враховуючи комплексного підходу до аналізу загроз ІБ.

Розв’язання вищезазначених проблем вимагає розробки та впровадження нових моделей та методів, які відповідатимуть сучасним викликам і ґрунтуватимуться на алгоритмах інтелектуального аналізу даних та машинного навчання. Передумовою для застосування інтелектуальних моделей є наявність невизначеності, обумовленої відсутністю інформації або складністю системи, а також необхідність аналізувати значні за обсягом, часто неповні та різнорідні набори параметрів, що містять складні нелінійні приховані залежності [22, 132, 135].

**Метою дисертаційного дослідження** є підвищенні ефективності процесу оцінювання ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем, а також розробка і наукове обґрунтування нових методологічних та практичних принципів оцінювання ризиків сучасних РІС із застосуванням методів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж на основі врахування багатокритеріального аналізу розподілених метрик про стан інформаційних активів та даних контролю відповідності вимогам провідних стандартів ІБ, що дозволить підвищити точність, адаптивність і надійність процесу управління ризиками в масштабованих динамічних середовищах.

**Основні завдання дослідження**, що необхідно вирішити для досягнення поставленої мети включають наступні аспекти:

- Комплексний аналіз існуючих підходів та методологій оцінювання ризиків інформаційної безпеки, виявлення їх обмежень у застосуванні до масштабованих, динамічних РІС. Аналіз нормативно-правової бази та міжнародних стандартів ІБ, ідентифікація наявних прогалин в теорії та практиці управління ризиками.

- Формалізація проблеми оцінювання ризику за умов невизначеності та нерівномірної доступності даних, побудова профілю ключових факторів ризику, що можуть спричинити потенційні інциденти ІБ в умовах фізичної та функціональної розподіленості ресурсів, а також основних контролів безпеки для сучасних РІС, дослідження показників їх статистичної важливості та кореляції.
- Узагальнення теоретико-методологічних принципів застосування алгоритмів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж для вирішення задач підвищення ефективності процесу ризик-менеджменту в РІС та покращення точності прийнятих управлінських рішень.
- Обґрунтування концептуальної методики оцінювання ризиків ІБ із врахуванням комплексного підходу на основі дослідження широкого спектру факторів ризику, синтезу методів обробки та інтелектуального аналізу великих обсягів гетерогенних даних і мережевих метрик про стан інфраструктури РІС (метрико-орієнтований підхід) з однієї сторони, та контролю відповідності нормативно-правовій базі та вимогам провідних стандартів ІБ (стандарт-орієнтований підхід) з іншої.
- Аналіз та формалізація технологічних актив-орієнтованих вимог та контролів безпеки провідних міжнародних та національних стандартів ІБ.
- Побудова комплексу науково обґрунтованих нейромережевих моделей аналізу рівня ризику ІБ в розподіленому середовищі, оптимізованих для обробки великих обсягів гетерогенних даних та здатних динамічно оновлювати результат на основі актуальної інформації, забезпечувати комплексний адаптивний аналіз ризиків і інтеграцію з існуючими системами безпеки, підвищуючи рівень автоматизації та ефективності ризик-менеджменту в РІС у контексті динамічного мінливого кіберсередовища.
- Експериментальна перевірка працездатності запропонованого підходу, порівняльна оцінка розроблених нейромережевих моделей та класичних алгоритмів машинного навчання за характеристиками точності та ефективності при вирішенні задач класифікації, обґрунтування переваг розроблених моделей у контексті їх практичного застосування.

- Розробка адаптивного методу комплексного кількісного оцінювання ризиків кібербезпеки в розподілених інформаційних системах з використанням спроєктованих моделей та загальної системи оцінки вразливостей, що дозволить підвищити ефективність процесу оцінювання ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем.

В рамках дослідження пропонується вдосконалити метод побудови **профілю ключових факторів ризику кібербезпеки** на основі урахування кореляційного аналізу та моделювання їх взаємозв'язків, а також здійснити аналіз основних чинників ризику та контролів безпеки сучасних розподілених інформаційних систем, що дозволить оптимізувати процес вибору вхідного вектору ознак проєктованих моделей та підвищити їх ефективність (Рис. 1.17).


*Рис. 1.17. Структурно-логічна схема дослідження.*

На основі спроєктованого профілю пропонується розробити **комплекс нейромережевих моделей якісного аналізу ризиків** ІБ в розподілених інформаційних системах, що поєднують аспекти оцінки контролю відповідності нормативно-правовій базі і вимогам провідних стандартів ІБ в рамках стандарт-орієнтованого підходу, та інтелектуальний аналіз великих обсягів гетерогенних параметрів про стан інфраструктури РІС в рамках метрико-орієнтованого підходу. Відповідно до отриманих показників рівня ризику для кожного ІТ-активу розподіленої системи за результатами розроблених моделей, а також даних про

вразливості мережевого асету відповідно до загальної системи оцінки вразливостей CVSS, пропонується створити **універсальний адаптивний метод комплексного кількісного оцінювання ризиків**, що на відміну від класичного підходу враховує динамічний характер розподіленого середовища, забезпечує комплексний гнучкий підхід до оцінки розподілених ризиків на основі спроєктованих моделей та просту практичну імплементацію, а також дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

Запропоновані в межах дисертаційного дослідження моделі та методи сприяють розвитку науково-обґрунтованого підходу до оцінювання ризиків кібербезпеки розподіленого середовища, створюють умови для підвищення ефективності прийняття управлінських рішень, а також забезпечують кращу адаптацію до сучасних вимог нормативно-правової бази та реалій функціонування динамічних розподілених інформаційних систем.

### 1.5. Висновки до розділу 1

В результаті проведеного дослідження сучасного стану та тенденцій розвитку розподілених інформаційних систем встановлено, що динамічний, масштабований та гетерогенний характер таких систем створює суттєві виклики для традиційних підходів до оцінювання ризиків, заснованих переважно на ймовірнісно-статистичному аналізі ретроспективних даних та суб’єктивних експертних оцінках. Обґрунтовано, що класичні підходи та методології не завжди забезпечують достатню гнучкість, адаптивність та точність в умовах розподіленого середовища.

Створення сучасних теоретико-прикладних підходів, які дозволять усунути обмеження існуючих методів оцінювання ризику та сприятимуть підвищенню рівня кіберзахищеності РІС є важливим та пріоритетним науковим завданням. Глибинний огляд існуючих підходів довів необхідність розробки та залучення більш гнучких моделей та методів оцінювання ризику із застосуванням методів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж на основі врахування багатокритеріального аналізу розподілених метрик про роботу інформаційних активів та контролю відповідності вимогам провідних міжнародних

та галузевих стандартів ІБ. Саме комплексна інтеграція цих підходів дозволить підвищити ефективність оцінювання кіберризиків, та забезпечить фундамент для розробки нових моделей оцінювання, здатних оперативно реагувати на сучасні загрози РІС та адаптуватися до реалій розподілених інфраструктур в масштабованих динамічних середовищах.

Таким чином, можна зробити висновок, що подальший розвиток науково-прикладних досліджень пов'язаних з розробкою методів та моделей оцінювання ризиків кібербезпеки в розподілених інформаційних системах складає актуальне наукове завдання і потребує глибокого дослідження.

В першому розділі дисертаційної роботи було отримано наступні результати:

1. **Проаналізовано сучасний стан та тенденції розвитку розподілених інформаційних систем**, а також ключові аспекти забезпечення кібербезпеки в розподіленому середовищі. Обґрунтовано ряд проблем та викликів в задачах оцінювання ризиків кібербезпеки сучасних РІС, що головним чином пов'язані з високою складністю, динамічністю та масштабованістю розподіленого середовища, значною фрагментованістю та неповнотою даних, складністю їх ефективного агрегування в умовах масштабованих систем та оперативного аналізу, а також низькою ефективністю традиційних підходів до оцінювання.

2. **Розкрито поняття ризику, його компоненти, класифікацію та теоретичні засади ризик-менеджменту в інформаційній безпеці, проведено аналіз існуючих підходів до оцінювання ризику**. Виявлено суттєві обмеження традиційних методів в умовах динамічного середовища РІС, що полягають в першу чергу в загальних та концептуальних аспектах оцінювання, браку узгодженості між різними підходами та суб'єктивності результатів, а також недостатній гнучкості, адаптивності та оперативності аналізу, що вимагається в умовах функціонування сучасних РІС.

3. **Виконано аналіз нормативно правової бази та міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки**, проведено порівняльний аналіз сучасних методологій оцінювання та управління ризиками ІБ. Виявлено їх обмеження для практичного застосування в динамічних масштабованих розподілених системах.

4. **Сформульовано науково-прикладну проблему та завдання дослідження**, спрямовані на розробку комплексу моделей оцінювання ризику, що враховують вимоги та особливості функціонування PIC, дозволяють автоматизувати обчислення показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних. Відсутність універсальних та ефективних підходів до оцінювання ризиків в динамічних та масштабованих розподілених системах доводять актуальність обраного наукового завдання.

5. **Обґрунтовано доцільність застосування нейромережевих моделей, методів інтелектуального аналізу даних і машинного навчання** для підвищення гнучкості, адаптивності та ефективності оцінювання ризиків кібербезпеки.

# РОЗДІЛ 2. МОДЕЛІ БАГАТОКРИТЕРІАЛЬНОГО АНАЛІЗУ ГЕТЕРОГЕННИХ ДАНИХ РІС НА ОСНОВІ ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ

Результати аналізу, проведеного у попередньому розділі, засвідчують істотні обмеження класичних підходів до оцінювання ризиків в умовах розподілених інформаційних систем. Існуючі стандарти та методичні рекомендації хоча й визначають загальні принципи ризик-менеджменту, однак не надають комплексного та гнучкого інструментарію для оперативного врахування змінних векторів загроз, специфіки масштабованої інфраструктури та вимог нормативно-правової бази. Попри широкий спектр наявних методологій, стандартів та рекомендацій, їх застосування в динамічних, гетерогенних і масштабованих середовищах часто зводиться до здебільшого концептуальних, узагальнених та статичних підходів. Внаслідок цього вони не здатні забезпечити високу точність та актуальність оцінок в умовах масштабованих розподілених систем, де присутня необхідність аналізу в режимі реального часу великих обсягів даних різної природи, а чинники ризику можуть швидко змінюватися під впливом динамічного середовища.

У цих умовах особливої актуальності набувають підходи, засновані на інтелектуальному аналізі даних та машинному навчанні. Нейромережеві моделі, здатні до самонавчання, виявлення прихованих закономірностей і нелінійних залежностей, а також швидкої адаптації до нових умов динамічного середовища РІС, відкривають перспективи формування ефективних інструментів оцінювання ризиків. В умовах фізичної та функціональної розподіленості інформаційних систем управління ризиками має засновуватись на комплексному підході, який забезпечує інтеграцію всіх аспектів ризик-менеджменту [118, 128, 132, 135]. Це передбачає детальний аналіз факторів та подальшу оцінку ризиків для кожного окремого активу або підсистеми РІС, враховуючи їх взаємозв’язки, критичність для загальної безпеки та вплив на цілісність та стан захищеності інфраструктури в цілому. Такий підхід дозволяє ефективно ідентифікувати, аналізувати та пріоритизувати загрози в контексті їх системного впливу, що є ключовим для забезпечення надійності та стійкості розподілених інформаційних середовищ [110, 117].

В рамках даного розділу пропонується вдосконалити методологічні аспекти побудови профілю ключових факторів ризику, що можуть спричинити потенційні інциденти ІБ в умовах системної розподіленості ресурсів [127]. Проведено дослідження основних чинників ризику кібербезпеки, що можуть бути ідентифіковані в процесі побудови та експлуатації типової розподіленої інформаційної системи, створеної для забезпечення одного або декількох типів інформаційних процесів та надання інформаційних послуг. Результатом було ранжування основних факторів ризику відповідно до їх важливості та частоти виникнення на практиці, моделювання взаємозв'язків між факторами ризику, а також виокремлення найбільш значущих контролів безпеки.

Продовжуючи логіку проведених досліджень, наступним кроком стає перехід від узагальнених статистично-аналітичних оцінок факторів ризику та їх взаємозв'язків до побудови та експериментального дослідження комплексу нейромережевих моделей для вирішення класичної задачі класифікації та навчання з учителем, здатних інтегрувати ці знання в адаптивний механізм прогнозування та інтерпретації ризиків у розподіленому середовищі. Зокрема, ключовим завданням постає застосування глибоких нейронних мереж, які відзначаються можливостями до нелінійного моделювання складних багатовимірних взаємозв'язків, високою узагальнювальною здатністю та потенціалом для обробки великих обсягів гетерогенних даних, що є визначальною особливістю масштабованих РІС.

При цьому пропонується провести перевірку ряду гіпотез:

1. Застосування вагових коефіцієнтів (class weights) та технік оверсемплінгу (oversampling) найменш представлених класів на основі методів SMOTE та ADASYN на вході алгоритму класифікації дає можливість подолати проблему дисбалансу класів та оптимізувати ефективність вирішення задачі оцінювання ризику в розподіленому середовищі $H_{(1)}$;

2. Ступінь інформаційної наповненості та міра повноти вхідних даних має суттєвий вплив на показник достовірності результатів класифікації рівнів ризику $H_{(2)}$;

3. Застосування побудованого профілю ключових факторів ризику дозволяє оптимізувати процес вибору вхідного вектору ознак проєктованих моделей та

покращити якісні характеристики оцінки у порівнянні з класичним PCA підходом $H_{(3)}$;

У подальших параграфах буде розглянуто розробку архітектури глибокої нейронної мережі, адаптованої до задачі класифікації рівня ризику на основі багатокритеріального аналізу гетерогенних метрик про стан інфраструктури РІС. Це передбачатиме практичне застосування розглянутих теоретичних засад для побудови ряду нейромережевих моделей, оптимізацію конфігурації гіперпараметрів, а також оцінювання ефективності підходу на тестових і валідаційних наборах даних, репрезентативних для розподілених інформаційних систем різної складності та масштабу.

## 2.1. Метрико-орієнтований підхід до оцінювання стану захищеності інформаційного активу

Відсутність на сьогоднішній день стандартизованих методик аналізу захищеності розподілених інформаційних систем вносить момент невизначеності при прийнятті управлінських рішень та суб’єктивності при визначенні необхідних і достатніх заходів безпеки та механізмів захисту. Формальні підходи до оцінювання, що включають **експертний аудит**, **інвентаризацію**, **аналіз конфігурацій та налаштувань**, **перевірку відповідності корпоративним політикам**, **міжнародним стандартам чи нормативним документам**, а також технічні аспекти пов’язані з пошуком та ідентифікацією **наявних вразливостей**, **мережевим скануванням**, **перевіркою веб-додатків**, або ж **тестуванням на проникнення** є ефективними механізмами аналізу поточного стану, проте з іншого боку передбачають розрізнений та фрагментований підхід з оцінкою вузького спектру безпекових аспектів, що притаманні предметній області кожного з методів. Окрім цього, перелічений інструментарій найчастіше застосовується окремо, а отже не забезпечує комплексного погляду на стан забезпечення безпеки в розподіленому середовищі. Варто зазначити, що аналіз результатів по деяким з описаних підходів дозволяє безпосередньо судити про стан забезпечення безпеки системи (наприклад наявність вразливостей), тоді як інші лише опосередковано впливають на оцінку цього показника (відсутність політик

ІБ, невідповідність вимогам стандартів тощо). Важливим аспектом даного питання є також необхідність забезпечення інтегральної оцінки ризиків в розрізі часу, що дозволить проводити порівняння рівня захищеності та приймати рішення щодо впроваджених механізмів захисту.

Одним із засобів формальної оцінки безпеки можуть бути метрики ІБ. За своєю суттю, **метрики безпеки** – є універсальним формалізованим критерієм для оцінювання стану безпеки інформаційної системи та важливим механізмом управління та контролю. Поняття «метрики безпеки» передбачає застосування кількісного, статистичного та / або математичного аналізу для вимірювання ключових показників безпеки, в тому числі виражених у фінансовому еквіваленті потенційних втрат чи вартості відновлення компонентів системи. Таким чином, можна виділити набір універсальних атрибутів, що будуть актуальними для будь-якої розподіленої системи та в сукупності зможуть охарактеризувати рівень захищеності об’єкту чи ІТ-активу. Метрика безпеки (або їх комбінація) являє собою кількісну міру відповідного атрибуту, яким даний об’єкт володіє.

Можна виділити наступні критерії вибору метрик безпеки:

– актуальність для прийняття рішення;
– простота виміру та агрегації – доступність для обрахунку та аналізу, можливість автоматизації перевірки та контролю;
– об’єктивність оцінки та відтворюваність – незалежність та відсутність впливу суб’єктивних чинників (наприклад експертних рішень);
– вимірюваність – можливість однозначної інтерпретації (переважно кількісної) та порівняння.

Для типової розподіленої інформаційної системи можна виділити широкий спектр стандартизованих метрик безпеки та інтегрованих показників, що забезпечать можливість моніторингу, контролю та подальшого аналізу стану системи [88, 115].

Прикладами таких показників для окремого мережевого активу можуть бути:

– тип та категорія пристрою;
– тип, версія та номер збірки операційної системи;
– тип розгортання пристрою (фізичний / віртуалізація);

– кількість виявлених вразливостей;
– тип середовища функціонування активу (продуктивне, тестове тощо);
– наявність зареєстрованих інцидентів ІБ в минулому;
– дата-час останньої активності об’єкту;
– наявність та тип антивірусного ПЗ;
– дата-час останнього оновлення сигнатур / агента антивірусного ПЗ;
– статус застосування політик ІБ;
– статус підключення об’єкту до SIEM / DLP та інших систем корпоративного захисту тощо;
– дата-час останнього сканування вразливостей тощо.

Слід зазначити, що такі параметри можуть мати різні джерела походження (що пов’язано в першу чергу з гетерогенною природою РІС), а також тип даних та формат представлення, а тому вимагають додаткового інструментарію аналітичного опрацювання та стандартизації [89].

Відбір метрик безпеки має враховувати аспекти комплексного оцінювання, уніфікації процедури аналізу та врахування актуальних факторів ризику, що притаманні розподіленому середовищу. Для цього пропонується застосувати побудований в рамках наступного параграфу профіль ключових факторів ризику сучасних РІС, що можуть спричинити потенційні інциденти ІБ в умовах фізичної та функціональної розподіленості ресурсів [90].

## 2.2. Побудова профілю ключових факторів ризику ІБ для розподілених інформаційних систем

Необхідність ідентифікації та попереднього аналізу основних факторів ризику, встановлення їх взаємозв’язків та кореляційних залежностей, безпосередньо пов’язана з якістю підготовки вхідних даних для побудови архітектури ефективних моделей глибинного навчання. Попередній етап статистичного дослідження та оцінки факторів ризику дозволяє:

1. **Оптимізувати вибір вхідного вектору ознак**: Виділення найсуттєвіших факторів ризику та контролів безпеки сприяє зменшенню розмірності вхідних даних і

мінімізує «шум», що у кінцевому підсумку покращує збіжність і стабільність процесу навчання нейронних мереж. Це особливо актуально для глибинних архітектур, де надмірна кількість ознак може призвести до складнощів оптимізації та ризику перенавчання (overfitting).

2. **Покращити інтерпретованість результатів**: Попередній аналіз взаємозв'язків між факторами ризику дає змогу краще зрозуміти структуру вхідних даних. Таким чином, навіть при застосуванні глибоких нейронних мереж, які зазвичай працюють за принципом «чорної скриньки» (black box), стає можливим інтерпретувати вплив окремих груп ознак на рівень ризику. Знання про те, які фактори ризику є ключовими, дозволяє фокусувати увагу на їх динаміці та значущості при подальшій оптимізації моделі.

3. **Підвищити точність і надійність моделі**: Попереднє дослідження причинно-наслідкових зв'язків і взаємозалежностей між факторами ризику допомагає моделі глибинного навчання більш ефективно «навчитися» складним патернам при аналізі даних. Глибинні нейронні мережі здатні виявляти нелінійні закономірності, але наявність початкового, сформованого уявлення про основні детермінанти ризику підсилює впевненість у тому, що модель не буде витрачати обчислювальні ресурси на незначущі або слабо впорядковані ознаки.

4. **Узгодити аналітичний підхід із практичними вимогами**: У реальних умовах експлуатації PIC, особливо коли йдеться про оцінювання ризиків кібербезпеки, важливо, щоб результати нейромережевих моделей були не лише точними, але й корисними для ухвалення рішень. Попередня статистично-аналітична розвідка дає змогу краще «пояснити» результат моделі та коректно інтегрувати її у процеси управління безпекою.

В рамках даного параграфу **пропонується вдосконалити метод побудови профілю ключових факторів ризику** сучасних розподілених інформаційних систем на основі урахування кореляційного аналізу та моделювання їх взаємозв'язків, що дозволить підвищити ефективність проєктованих моделей оцінювання ризику. У дослідженні [91] запропоновано орієнтований на дані прогнозний аналіз загроз кібербезпеки шляхом дослідження ключових факторів ризику та вимірювання

значущості ознак на основі отриманих в ході опитування даних. Пропонується вдосконалити використаний в рамках вищеописаного дослідження метод з використанням апарату математичної статистики, проведенням кореляційного аналізу і моделювання взаємозв'язків між чинниками ризику із застосуванням коефіцієнта рангової кореляції r-Спірмена, а також побудовою актуального для предметної області динамічних розподілених інформаційних систем переліку ключових факторів ризику та контролів безпеки сучасних РІС.

Запропонована методологія побудови профілю ключових факторів ризику кібербезпеки розподілених систем заснована на комплексному підході, що поєднує анкетне опитування експертів, статистичний аналіз отриманих результатів та моделювання взаємозв'язків між факторами ризику. Основні етапи цього процесу можна представити наступним чином:

1. **Збір даних через анкетування** – підготовка опитувальників, формування репрезентативної вибірки експертів у сфері забезпечення кібербезпеки РІС, проведення опитування у два етапи (пілотне тестування та основне дослідження).
2. **Попередня обробка даних** – виявлення аномальних значень, оцінка якості вибірки, нормалізація та усунення викидів.
3. **Статистичний аналіз** – визначення середніх значень та дисперсії, ранжування факторів ризику та контрольних механізмів.
4. **Моделювання взаємозв'язків** – перевірка нормальності розподілу даних, аналіз кореляційних зв'язків між факторами ризику.
5. **Формування профілю ризиків** – побудова структурованого профілю, що дозволяє ідентифікувати найбільш значущі загрози та оптимізувати заходи кібербезпеки.

Метою побудови профілю ключових факторів ризику є ідентифікація та виокремлення основних чинників ризику ІБ, що притаманні сучасним розподіленим інформаційним системам, а також аналіз найбільш значущих контролів безпеки для розробки на основі них рекомендацій щодо усунення потенційних загроз [68].

### 2.2.1. Ідентифікація показників, що впливають на ризик

За даними щорічного дослідження «STATE OF ENTERPRISE RISK MANAGEMENT 2020» компанії ISACA, найбільшими викликами в сфері корпоративних ризиків є фактори, пов’язані з появою нових загроз, змінами / досягненнями в розвитку технологій, а також слабким кадровим потенціалом та відсутністю необхідних навичок та досвіду в існуючих командах з кіберзахисту (Рис. 2.1).

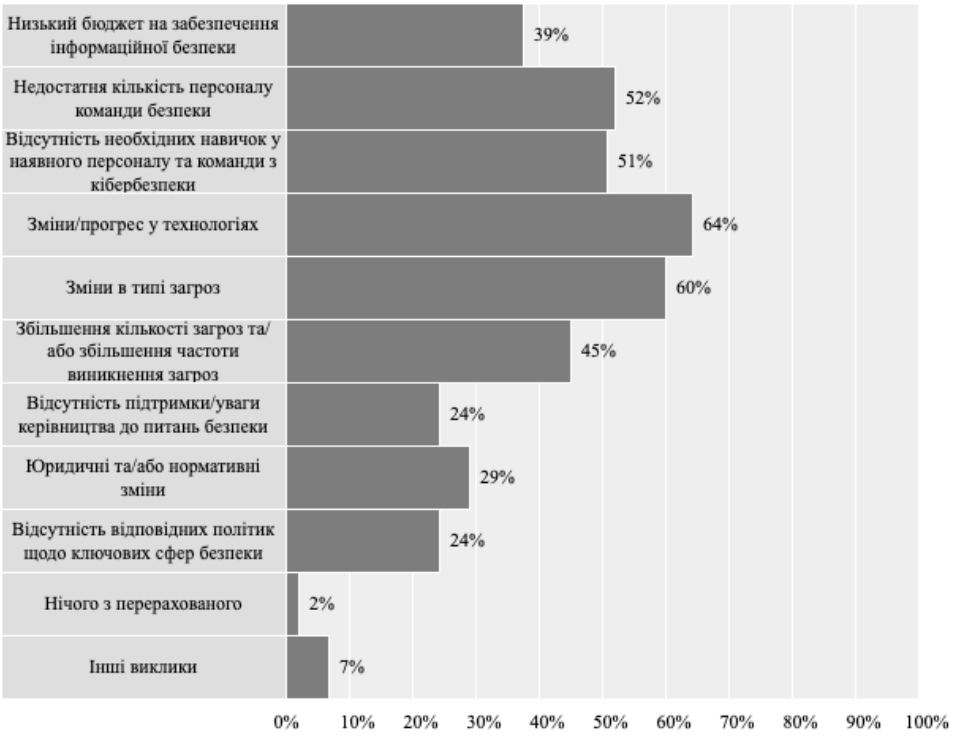


*Рис. 2.1. Основні виклики кібербезпеки корпоративного середовища.*

З іншого боку, за даними цього дослідження для попередження / пом’якшення наслідків потенційних проблем безпеки найбільш часто застосовуваним контролем є підвищення рівня обізнаності та проведення тренінгів з кібербезпеки серед персоналу (Рис. 2.2).

Вісімдесят відсотків підприємств-респондентів проводять навчання з підвищення обізнаності, 68% – використовують стратегії ліквідації наслідків та відновлення після катастроф / інцидентів ІБ, і 67% застосовують загальні контролі з управління та менеджменту ІБ.

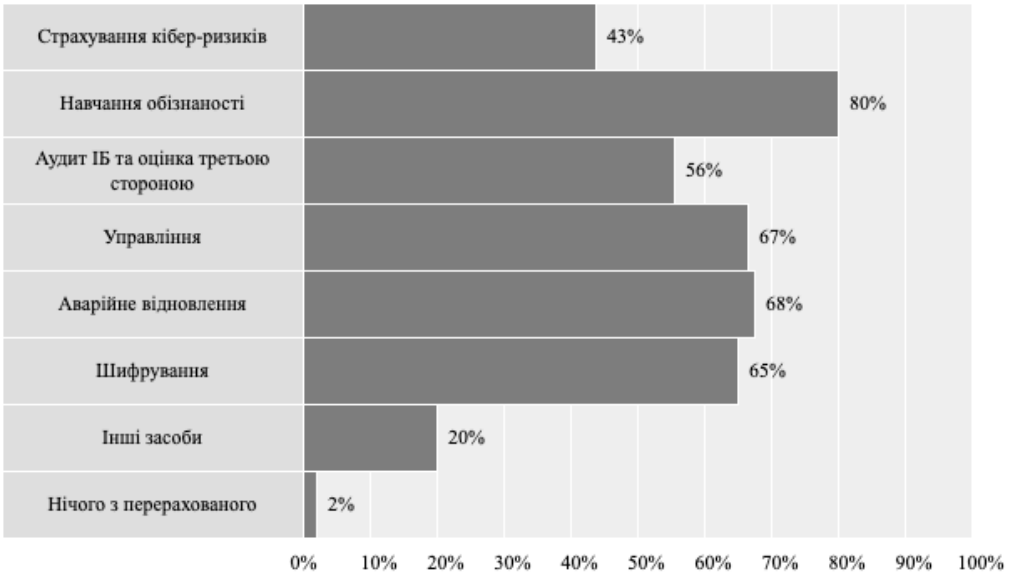


*Рис. 2.2. Основні контролі кібербезпеки та заходи щодо пом'якшення наслідків.*

Менше половини підприємств-респондентів застосовують страхування як контроль для пом'якшення наслідків; при цьому найбільшими прихильниками такого підходу є підприємства Північної Америки та Африки [92].

**Процес збору даних для аналізу.** В рамках запропонованого підходу, для збору вибірки даних для аналізу використовується метод анкетування. В якості респондентів виступили декілька десятків інженерів з інформаційної безпеки різного рівня підготовки, спеціалістів з тестування на проникнення і аудиту, та провідних фахівців в області менеджменту проєктів ІБ. Всі опитані були обрані вибірково та мають досвід забезпечення безпеки для інфраструктур інформаційних систем різного рівня складності та масштабу.

Анкетування проводиться у два етапи:

- Пілотне опитування – тестування анкети на обмеженій групі експертів для перевірки інструментарію дослідження, корегування питань і формулювань.
- Основне опитування – масштабне анкетування цільової групи за допомогою остаточного варіанту анкет за двома категоріями питань: оцінка важливості ключових загроз та факторів ризику, а також оцінка частоти застосування на практиці контрольних заходів та механізмів.

Пілотне дослідження виконується перед проведенням основного та має на меті перевірку наскільки запропонована модель анкетування підходить для аналізу кінцевих метрик.

*Таблиця 2.1*

*Класифікація учасників опитування*

| № | Категорії | Кількість респондентів | Відсоток (%) |
|---|---|---|---|
| **1** | **Стать** | | |
| 1.1 | Жінка | 6 | 26.08 |
| 1.2 | Чоловік | 17 | 73.91 |
| | Всього | **23** | **100.00** |
| **2** | **Позиція** | | |
| 2.1 | Інженер з інформаційної безпеки | 6 | 26.08 |
| 2.2 | Аудитор з інформаційної безпеки | 2 | 8.69 |
| 2.3 | Спеціаліст з тестування на проникнення | 5 | 21.73 |
| 2.4 | Аналітик зловмисного ПЗ | 2 | 8.69 |
| 2.5 | Інженер мережевої інфраструктури | 5 | 21.73 |
| 2.6 | Керівник проєктів | 3 | 13.04 |
| | Всього | **23** | **100.00** |

До основного опитування було залучено 23 спеціалісти (Таблиця 2.1). Вік учасників опитування від 24 до 47 років, з середнім показником в 34.2.

При розробці анкет враховані найбільш поширені фактори ризику, що є загальними для більшості сучасних розподілених інфраструктур. В анкету було включено 40 питань по основним факторам ризику та 14 питань щодо практики застосування контролів безпеки в умовах реальних проєктів. Респондентам пропонувалось анонімно та суб'єктивно відповісти на ці питання покладаючись на власний досвід та реальну практику роботи з масштабованими розподіленими інформаційними системами.

**Критерії дослідження та аналіз тестової вибірки.** З метою підвищення ефективності та звуження градації можливих результатів для оцінки факторів ризику в роботі було обрано 5-бальну шкалу Лайкерта (Likert scale), в якій показник «неважливо» дорівнює одиниці, а «надзвичайно важливо» дорівнює п'яти. Подібним чином виділено п'ять категорій для оцінки контролів безпеки, так, що показник «ніколи» дорівнює одиниці, а показник «завжди» дорівнює п'яти. Таким чином, усі питання щодо факторів ризику в розподілених системах вимірювались за

п’ятибальною шкалою від «незначущого» до «надзвичайно важливого», а всі контролі безпеки – від «ніколи» до «завжди». Шкалу Лайкерта досить легко побудувати, вона забезпечує відносну надійність навіть при невеликій кількості суджень, при цьому отримані дані легко обробляти. Відбір суджень для шкали проводився на основі аналізу літературних джерел в предметній області та в процесі пілотного дослідження методом відбору з первинного списку суджень з найбільшою дискримінуючою здатністю щодо вимірюваної установки. Для цього було створено початковий перелік тверджень, які пропонувались респондентам з групи, репрезентативної по відношенню до досліджуваної аудиторії (учасникам пілотного дослідження).

*Таблиця 2.2*

*Шкала вимірювання факторів ризику та заходів контролю безпеки*

| **Оцінка** | **Фактор ризику** | **Контроль безпеки** |
|---|---|---|
| 1 | Неважливо | Ніколи |
| 2 | Трохи важливо | Рідко |
| 3 | Важливо | Іноді |
| 4 | Дуже важливо | Часто |
| 5 | Критично | Завжди |

При роботі зі шкалою респонденти оцінювали ступінь своєї згоди або незгоди з кожним із запропонованих суджень, від «повністю згоден» до «повністю не згоден» (Таблиця 2.2).

**Ключові фактори ризику.** Дослідження демонструє 40 основних факторів ризику в сучасних розподілених інформаційних системах, промарковані від Factor_1 до Factor_40, що поширені в профільній літературі, часто зустрічаються на практиці та широко використовуються дослідниками та експертами в області кібербезпеки при проведенні заходів ризик-менеджменту. Ці фактори повинні бути ідентифіковані в процесі оцінювання та управління ризиками ІБ та контрольовані в подальшому (Таблиця 2.3).

Окремо слід виділити ризики, зумовлені людським фактором. Вони включають в себе не тільки помилки співробітників, але і умисні дії, які призводять до поширення конфіденційної інформації.

*Таблиця 2.3*

*Основні фактори ризиків безпеки сучасних розподілених інформаційних систем*

| Категорія | | № | Формалізація фактору ризику |
|---|---|---|---|
| **Фактори технологічного характеру** | **Логічні (програмні)** | Factor_1 | Використання незахищених додатків |
| | | Factor_2 | Недостатнє управління оновленнями та патчами безпеки |
| | | Factor_3 | Уразливості та порушення безпеки API |
| | | Factor_4 | Технічні прогалини та недоліки під час проєктування систем |
| | | Factor_5 | Недостатній рівень логування та моніторингу |
| | | Factor_6 | Порушення механізмів автентифікації та управління сесіями |
| | | Factor_7 | Використання несанкціонованого стороннього програмного забезпечення |
| | | Factor_8 | Використання неліцензованих програмних рішень з незадекларованими функціональними можливостями |
| | | Factor_9 | Уразливості "нульового дня" (0-day) та помилки, пов’язані з розвитком інформаційних технологій |
| | | Factor_10 | Недостатнє управління доступом [1] |
| | **Фізичні (апаратні)** | Factor_11 | Використання застарілого обладнання та компонентів із відомими вразливостями |
| | | Factor_12 | Неправильне налаштування безпеки серверів і мережевих пристроїв |
| | | Factor_13 | Низька надійність комплексу апаратно-програмних компонентів, відсутність плану відновлення та регулярних резервних копій |
| | | Factor_14 | Слабкий захист кінцевих точок і мережевого периметру |
| | | Factor_15 | Неконтрольовані IoT-пристрої та мобільні пристрої |
| | | Factor_16 | Недосконаліть організаційної структури інформаційної системи, необхідність частих переналаштувань системи або її окремих частин |
| | | Factor_17 | Можливість витоку інформації та компрометації конфіденційних даних через технічні канали |
| | | Factor_18 | Недостатній контроль фізичного доступу |
| | | Factor_19 | Несанкціоноване використання активів організації |
| | | Factor_20 | Відсутність механізмів захисту від зовнішніх мережевих атак |
| **Фактори організаційного характеру** | | Factor_21 | Відсутність політики кібербезпеки |
| | | Factor_22 | Невиконання вимог стандартів на етапі проєктування системи |
| | | Factor_23 | Порушення вимог інформаційної безпеки під час експлуатації системи |
| | | Factor_24 | Відсутність контролю за інцидентами інформаційної безпеки |
| | | Factor_25 | Брак підтримки, залученості та уваги з боку топ-менеджменту |
| | | Factor_26 | Відсутність аудитів безпеки |
| | | Factor_27 | Відсутність політики антивірусного захисту |
| | | Factor_28 | Слабкий потенціал використання існуючих технологій захисту |
| | | Factor_29 | Невідповідність між інфраструктурою та впровадженими заходами безпеки |
| | | Factor_30 | Нездатність забезпечити належний рівень підтримки та розвитку систем захисту |

*Продовження таблиці 2.3*

| | | |
|---|---|---|
| **Фактори пов' язані з людським чинником** | Factor_31 | Дії ненадійних співробітників |
| | Factor_32 | Ненавмисні помилки обслуговуючого персоналу |
| | Factor_33 | Зловживання привілеями |
| | Factor_34 | Надмірна кількість осіб, які мають доступ до захищеної інформації, надмірні права доступу для облікових записів |
| | Factor_35 | Низький рівень обізнаності персоналу (особливо щодо фішингу/соціальної інженерії) |
| | Factor_36 | Відсутність навчання з питань інформаційної безпеки |
| | Factor_37 | Значний дефіцит професіоналів у сфері кібербезпеки |
| | Factor_38 | Недостатній рівень гігієни паролів |
| | Factor_39 | Доступ персоналу до потенційно небезпечних ресурсів у зовнішній мережі |
| | Factor_40 | Відсутність контролю за втратою чи крадіжкою даних |

1 Відсутність розмежування доступу до контрольованої зони та розподілу прав користувачів

Відповідно до NIST SP 800-37 Risk Management Framework не слід забувати й про такі категорії ризику як: фінансові, юридичні, політичні, проєктні, репутаційні, бізнес-ризики та ризики стратегічного планування. Вони не були враховані в рамках даного дослідженні проте становлять важливу частину будь-якого процесу ризик-менеджменту [57].

**Ключові контролі безпеки та заходи ризик менеджменту.** Як результат аналізу вищезазначених чинників, експертній групі пропонуються можливі категорії заходів по мінімізації ризиків інформаційної безпеки, що включають в себе організаційно-правовий захист інформації, інженерно-технічні та програмно-апаратні засоби, криптографічні механізми, а також заходи фізичного захисту.

В якості ефективних мір забезпечення безпеки розподілених систем підготовленими штатними фахівцями або ж за допомогою аутсорсингу інформаційної безпеки можуть бути впроваджені наступні рішення (як окремо, так і в сукупності):

- Системи резервного копіювання;
- Системи захисту від несанкціонованого доступу;
- Системи захисту від атак на прикладному рівні (WAF);
- Системи управління інцидентами і подіями ІБ (SIEM);
- Системи управління ідентифікаційними даними і доступом (IAM);

- Системи управління відповідністю вимогам ІБ (Compliance Management);
- Системи захисту від витоку конфіденційної інформації (DLP);
- Системи управління доступом до інформації (IRM);
- Рішення з мережевої безпеки та мережевого екранування;
- Системи антивірусного захисту;
- Системи захисту електронної пошти від спаму, вірусів і інших загроз;
- Системи контентної фільтрації web-трафіку;
- Системи контролю доступу до периферійних пристроїв і додатків;
- Системи контролю цілісності програмних середовищ (FIM);
- Системи криптографічного захисту при зберіганні інформації.

Основою для розроблених анкет по можливим контролям та заходам ризик-менеджменту виступив стандарт ISO/IEC 27001 та безпосередньо Додаток А (Appendix A) даного стандарту, що становить собою важливий інструмент для управління інформаційною безпекою [58]. Він містить список заходів безпеки, які повинні застосовуватись для підвищення захищеності інформації, та за своєю структурою сумарно вміщує перелік із 93 контролів безпеки, класифікованих на 4 розділи. Не всі з цих контролів є обов'язковими для впровадження – компанія може обрати самостійно, які елементи управління вона вважає застосовними при даних обставинах в залежності від напрямку бізнесу, стану інфраструктури чи існуючого профілю зовнішніх загроз, та в подальшому реалізувати їх (зазвичай розглядаються по крайній мірі 90% контролів). Розширене тлумачення кожного елементу керування додатку А з поясненням того, як його необхідно застосовувати, описом та прикладами механізмів реалізації подано в стандарті ISO/IEC 27002 [59].

Окремо слід відмітити міжнародний стандарт ISO/IEC 27005, що містить рекомендації по управлінню ризиками інформаційної безпеки. Цей документ підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для надання рекомендацій при впровадженні заходів інформаційної безпеки на основі ризик-орієнтовного підходу [60].

В рамках опитування респондентам запропоновано оцінити 14 основних груп контролів інформаційної безпеки в сучасних розподілених інформаційних системах з точки зору частоти та ефективності їх застосування, промарковані від Control_1 до Control_14 (Таблиця 2.4).

*Таблиця 2.4*

*Основні контролі безпеки сучасних розподілених інформаційних систем*

| № | Категорія контролів | Опис |
|---|---|---|
| Control_1 | Information security policies | контролі, що відповідають за впровадження та перевірку дотримання політик інформаційної безпеки; |
| Control_2 | Organization of information security | контролі, що відповідають за організаційну складову заходів з інформаційної безпеки та розподіл обов'язків; створення системи управління для ініціювання та контролю впровадження та функціонування процесів інформаційної безпеки в організації; |
| Control_3 | Personnel and human resources security | контролі, що призначені для регулювання роботи персоналу та підрядників, визначення їх обов'язків щодо дотримання інформаційної безпеки як на етапі робочого процесу так і при звільненні; |
| Control_4 | Asset management | контролі, пов'язані з інвентаризацією активів компанії, класифікацією оброблюваної інформації та управлінням медіа-носіями; |
| Control_5 | Logical access control | контролі, що відповідають за обмеження доступу до інформації та засобів обробки інформації, політику контролю доступу (Access control policy), менеджмент прав доступу авторизованих користувачів до систем і додатків; |
| Control_6 | Cryptography | контролі, що відповідають за належне та ефективне використання криптографії та інфраструктури відкритих ключів (PKI) для захисту конфіденційності, достовірності та цілісності інформації; |
| Control_7 | Physical and environmental security | контролі, пов'язані з керуванням та запобіганням несанкціонованого фізичного доступу, втрати, пошкодження, крадіжки або компрометації активів та перериванню діяльності організації, а також визначенням безпечних зон, засобами контролю входу, безпекою обладнання, політиками «clear desk» та «clear screen»; |
| Control_8 | Operational security | сукупність контролів забезпечення правильної та безпечної роботи засобів обробки інформації, що об'єднують такі активності як керування змінами, резервне копіювання, моніторинг, логування та ведення журналів активності, відслідковування встановленого програмного забезпечення та детектування шкідливого ПЗ, контроль та усунення виявлених вразливостей; |
| Control_9 | Communications security | контролі, пов'язані з мережевою безпекою, мережевими послугами, передачею інформації та обміном повідомленнями; |
| Control_10 | System acquisition, development and maintenance | засоби керування, що визначають вимоги безпеки та механізми захисту в процесах розробки і підтримки; |

*Продовження таблиці 2.4*

| | | |
|---|---|---|
| Control_11 | Supplier relationships | контролі, що стосуються взаємовідносин з третіми сторонами та підрядниками, захистом цінних активів організації, що доступні для них, та забезпеченням узгодженого рівня інформаційної безпеки і надання послуг у відповідності до угод з постачальниками; |
| Control_12 | Information security incident management | засоби керування, пов'язані з управлінням інцидентами, подіями та вразливостями інформаційної безпеки, звітуванням про виявлені факти порушень, визначенням відповідальності, процедурами реагування і збору доказів; |
| Control_13 | Information security aspects of business continuity management | контролі, що необхідні для забезпечення планування неперервності бізнесу, процедур верифікації та постійного аудиту, доступності ресурсів та засобів обробки інформації, використання принципів відмовостійкості та надійності для забезпечення безпеки; |
| Control_14 | Compliance | засоби керування, що вимагають дотримання законодавчих та договірних вимог, уникнення порушень статутних, регулятивних або договірних зобов'язань, пов'язаних з інформаційною безпекою, процедур захисту інтелектуальної власності, персональних даних та перевірки стану інформаційної безпеки на всіх етапах життєвого циклу; |

Таким чином, запропоновані варіанти охоплюють весь спектр найбільш поширених механізмів та заходів ризик менеджменту, що застосовуються в сучасних розподілених системах, та можуть бути рекомендовані для подальшого аналізу в рамках поточного дослідження.

**Визначення рівня важливості факторів ризику в життєвому циклі сучасних розподілених інформаційних систем.** В процесі аналізу результатів опитування рекомендується проведення попередньої обробки отриманих даних. На цьому етапі здійснюється:

1. Видалення відповідей із високою варіативністю або підозрілими шаблонами, ідентифікація та видалення аномальних або відсутніх значень (методами середнього заповнення, лінійної інтерполяції тощо).

2. Нормалізація значень та приведення шкал до єдиного формату для забезпечення коректності подальшого статистичного аналізу.

На наступному етапі проводиться статистичний аналіз отриманих даних та ранжування досліджуваних показників за ступенем критичності та важливості:

1. Розрахунок **середніх значень** кожного фактора ризику та контрольного механізму, як середнього значення оцінки кожного показника.

2. Визначення **стандартного відхилення** як показника дисперсії, що дозволяє зрозуміти варіативність думок експертів.

3. Формування **ранжованого списку** факторів ризику за рівнем загрози та контрольних механізмів за рівнем ефективності при впровадженні.

Для проведення статистичного аналізу та моделювання використано інструментарій програмного забезпечення IBM SPSS Statistics.

Нескореговане стандартне відхилення (standard deviation) вибірки $S$ обчислено (2.1) для чотирьох груп факторів, кожна з яких містить по 10 факторів ризику.

$$S = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \tilde{x})^2}, \tag{2.1}$$

де $\{x_1, x_2, \dots, x_n\}$ – середні значення елементів вибірки, $n = 10$ – розмір вибірки (кількість факторів у кожній групі: Factor_1 – Factor_10, Factor_11 – Factor_20, Factor_21 – Factor_30, Factor_31 – Factor_40), та $\tilde{x}$ – середнє значення цієї оцінки (2.2).

$$\tilde{x} = \frac{1}{n}\sum_{i=1}^{n} x_i. \tag{2.2}$$

Очевидно, що переважна більшість факторів технологічного характеру відіграють ключову роль при визначенні кінцевого рівня ризику (Таблиця 2.5). Аналіз та узагальнення відповідей опитування дав наступний рейтинг важливості перерахованих ризиків у порядку спадання: Factor_20, Factor_6, Factor_10, Factor_11, Factor_12, Factor_14, Factor_8, Factor_9, Factor_4, Factor_3, Factor_13, Factor_17, Factor_18, Factor_1, Factor_15, Factor_19, Factor_2, Factor_5, Factor_7, Factor_16.

Серед факторів організаційного характеру найбільшу вагу мають ризики, пов’язані з відсутністю політик кібербезпеки та антивірусного захисту. Рейтинг важливості ризиків даної категорії: Factor_21, Factor_27, Factor_30, Factor_28, Factor_29, Factor_25, Factor_23, Factor_24, Factor_22, Factor_26.

Окрім того, усі респонденти зазначили, що ризик зловживання привілеями є найвищим фактором ризику та дуже важливим серед факторів пов’язаних з людським чинником. Рейтинг важливості ризиків даної категорії: Factor_33, Factor_40, Factor_35, Factor_37, Factor_38, Factor_36, Factor_34, Factor_31, Factor_32, Factor_39.

Підсумовуючи, рейтинг важливості категорій факторів ризику можна подати наступним чином (у порядку критичності): фактори технологічного характеру (логічні та фізичні), фактори пов'язані з людським чинником, фактори організаційного характеру.

*Таблиця 2.5*

*Середнє значення для кожного фактору ризику*

| Категорія | | № | N | Mean | Std. Deviation | Відсоток (%) |
|---|---|---|---|---|---|---|
| Фактори технологічного характеру | Логічні (програмні) | Factor_1 | 23 | 3.043478 | 0.824525 | 60.8695 |
| | | Factor_2 | 23 | 2.826087 | 0.886883 | 56.5217 |
| | | Factor_3 | 23 | 3.695652 | 0.764840 | 73.9130 |
| | | Factor_4 | 23 | 3.739130 | 0.540824 | 74.7826 |
| | | Factor_5 | 23 | 2.782609 | 0.795243 | 55.6521 |
| | | Factor_6 | 23 | 4.217391 | 0.735868 | 84.3478 |
| | | Factor_7 | 23 | 2.695652 | 0.764840 | 53.9130 |
| | | Factor_8 | 23 | 3.869565 | 0.694416 | 77.3913 |
| | | Factor_9 | 23 | 3.826087 | 0.777652 | 76.5217 |
| | | Factor_10 | 23 | 4.173913 | 0.650327 | 83.4782 |
| | | **Total** | **23** | **3.4869564** | **0.7435418** | **69.7391** |
| | Фізичні (апаратні) | Factor_11 | 23 | 4.130435 | 0.625543 | 82.6087 |
| | | Factor_12 | 23 | 4.086957 | 0.668312 | 81.7391 |
| | | Factor_13 | 23 | 3.434783 | 0.895752 | 68.6956 |
| | | Factor_14 | 23 | 3.913043 | 0.792754 | 78.2608 |
| | | Factor_15 | 23 | 2.869565 | 0.868873 | 57.3913 |
| | | Factor_16 | 23 | 1.913043 | 0.733178 | 38.2608 |
| | | Factor_17 | 23 | 3.434783 | 0.843482 | 68.6956 |
| | | Factor_18 | 23 | 3.086957 | 0.733178 | 61.7391 |
| | | Factor_19 | 23 | 2.869565 | 0.757049 | 57.3913 |
| | | Factor_20 | 23 | 4.304348 | 0.634950 | 86.0869 |
| | | **Total** | **23** | **3.4043479** | **0.7553071** | **68.0869** |
| Фактори організаційного характеру | | Factor_21 | 23 | 4.391304 | 0.656376 | 87.8260 |
| | | Factor_22 | 23 | 2.434783 | 0.787752 | 48.6956 |
| | | Factor_23 | 23 | 2.608696 | 0.782718 | 52.1739 |
| | | Factor_24 | 23 | 2.521739 | 0.845822 | 50.4347 |
| | | Factor_25 | 23 | 2.739130 | 0.810016 | 54.7826 |
| | | Factor_26 | 23 | 2.391304 | 0.838783 | 47.8260 |
| | | Factor_27 | 23 | 3.956522 | 0.824525 | 79.1304 |
| | | Factor_28 | 23 | 2.913043 | 0.596432 | 58.2608 |
| | | Factor_29 | 23 | 2.782609 | 0.795243 | 55.6521 |
| | | Factor_30 | 23 | 3.043478 | 0.638055 | 60.8695 |
| | | **Total** | **23** | **2.9782608** | **0.7575722** | **59.5652** |

*Продовження таблиці 2.5*

| | | | | | |
|---|---|---|---|---|---|
| **Фактори пов' язані з людським чинником** | Factor_31 | 23 | 2.782609 | 0.599736 | 55.6521 |
| | Factor_32 | 23 | 2.304348 | 0.764840 | 46.0869 |
| | Factor_33 | 23 | 4.000000 | 0.738549 | 80 |
| | Factor_34 | 23 | 2.869565 | 0.548083 | 57.3913 |
| | Factor_35 | 23 | 3.391304 | 0.782718 | 67.8260 |
| | Factor_36 | 23 | 3.000000 | 0.603023 | 60 |
| | Factor_37 | 23 | 3.347826 | 0.884652 | 66.9565 |
| | Factor_38 | 23 | 3.260870 | 0.688700 | 65.2174 |
| | Factor_39 | 23 | 2.086957 | 0.668312 | 41.7391 |
| | Factor_40 | 23 | 3.782609 | 0.599736 | 75.6521 |
| | **Total** | **23** | **3.0826088** | **0.6878349** | **61.6521** |

Таблиця 2.6 ілюструє перелік топ-10 ключових факторів ризику розподілених інформаційних систем на основі результатів опитування.

*Таблиця 2.6*

*Десять основних факторів ризику для розподілених інформаційних систем*

| № | N | Mean | Std. Deviation | Відсоток (%) |
|---|---|---|---|---|
| Factor_21 | 23 | 4.391304 | 0.656376 | 87.8260 |
| Factor_20 | 23 | 4.304348 | 0.634950 | 86.0869 |
| Factor_6 | 23 | 4.217391 | 0.735868 | 84.3478 |
| Factor_10 | 23 | 4.173913 | 0.650327 | 83.4782 |
| Factor_11 | 23 | 4.130435 | 0.625543 | 82.6087 |
| Factor_12 | 23 | 4.086957 | 0.668312 | 81.7391 |
| Factor_33 | 23 | 4.000000 | 0.738549 | 80 |
| Factor_27 | 23 | 3.956522 | 0.824525 | 79.1304 |
| Factor_14 | 23 | 3.913043 | 0.792754 | 78.2608 |
| Factor_8 | 23 | 3.869565 | 0.694416 | 77.3913 |

Таким чином, практично всі респонденти виділили фактори, пов'язані з відсутністю політики кібербезпеки та механізмів захисту від мережевих атак, порушеннями автентифікації та управління сеансами, порушеннями контролю доступу та використанням компонентів з відомими вразливостями як найбільш важливі в життєвому циклі сучасних PIC [110].

**Частота використання контролів безпеки.** У Таблиці 2.7 наведено середнє значення та середньоквадратичне відхилення для кожної групи контролів безпеки. Аналіз найбільш поширених категорій механізмів та заходів ризик менеджменту, що

застосовуються в сучасних розподілених системах показав, що більшість контролів захисту використовуються часто та є важливими механізмами попередження та мінімізації потенційних ризиків.

*Таблиця 2.7*

*Середнє значення для кожного контролю безпеки*

| № | N | Mean | Std. Deviation | Відсоток (%) |
|---|---|---|---|---|
| Control_1 | 23 | 4.260870 | 0.619192 | 85.2174 |
| Control_2 | 23 | 3.391304 | 0.940944 | 67.82608 |
| Control_3 | 23 | 2.347826 | 1.070628 | 46.95652 |
| Control_4 | 23 | 3.782609 | 0.735868 | 75.65218 |
| Control_5 | 23 | 4.304348 | 0.634950 | 86.08696 |
| Control_6 | 23 | 4.478261 | 0.593109 | 89.56522 |
| Control_7 | 23 | 4.478261 | 0.665348 | 89.56522 |
| Control_8 | 23 | 4.260870 | 0.619192 | 85.2174 |
| Control_9 | 23 | 4.130435 | 0.625543 | 82.6087 |
| Control_10 | 23 | 3.000000 | 1.044466 | 60 |
| Control_11 | 23 | 2.086957 | 0.900154 | 41.73914 |
| Control_12 | 23 | 2.130435 | 0.757049 | 42.6087 |
| Control_13 | 23 | 2.478261 | 0.845822 | 49.56522 |
| Control_14 | 23 | 2.782609 | 0.951388 | 55.65218 |

Узагальнення відповідей опитування, щодо основних груп контролів інформаційної безпеки сучасних розподілених інформаційних системах з точки зору частоти та ефективності їх застосування, продемонструвало що більша частина опитаних виділили контролі, що відповідають за дотримання політик інформаційної безпеки, належне та ефективне використання криптографії та інфраструктури відкритих ключів (PKI), логічний і фізичний контроль доступу, а також операційну безпеку як найважливіші та найбільш поширені в практиці застосування.

### 2.2.2. Моделювання взаємозв’язків між факторами ризику

На наступному етапі виконано перевірку гіпотези про зв’язки між ключовими факторами ризику з використанням коефіцієнтів кореляції.

Відповідно до запропонованого підходу цей етап включає:

1. Перевірку нормальності розподілу:
   – Критерії Колмогорова-Смірнова та Шапіро-Вілка.

– Побудова гістограм частотного розподілу.

2. Кореляційний аналіз:

– Розрахунок коефіцієнтів кореляції (Пірсона, Спірмена, Кендалла тощо).

– Визначення сили взаємозв’язку (слабкий, середній, сильний).

– Аналіз значущості залежностей.

Коефіцієнт кореляції є статистичним показником ймовірності зв’язку між двома змінними, вимірюваними в кількісній шкалі, що дозволяє відповісти на питання про ступінь і напрямок зв’язку між значеннями цих змінних.

В залежності від розмірів досліджуваної вибірки даних та результатів перевірки її розподілу приймається рішення про вибір методу кореляційного дослідження. Коефіцієнт рангової кореляції Спірмена (r-Спірмена) застосовується для оцінки сили та напрямку монотонного зв’язку між двома змінними у випадках коли вибірка має невеликий обсяг, не відповідає нормальному розподілу, а дані представлені у вигляді рангів або порядкових шкал. Коефіцієнт кореляції Пірсона використовується для вимірювання лінійного зв’язку між двома змінними, та підходить для даних, що мають нормальний розподіл і лінійний зв’язок. Коефіцієнт кореляції Кендалла (tau-b Кендалла) використовується для оцінки сили та напрямку асоціації між двома змінними у випадках невеликих вибірок, коли необхідна менша чутливість до викидів у даних [64].

Перевірка кореляції між вхідними параметрами нейромережевої моделі є критично важливим кроком у науковому дослідженні, оскільки корельовані ознаки можуть впливати на продуктивність моделі та її інтерпретованість. В рамках проєктованих моделей оцінювання ризику кібербезпеки перевірка кореляції між вхідними параметрами дозволить забезпечити:

- **Усунення мультиколінеарності.** Якщо вхідні параметри сильно корельовані між собою, це може спричинити мультиколінеарність – ситуацію, коли модель не може чітко визначити вплив кожної змінної на вихідний результат.
- **Покращення узагальнюючої здатності моделей.** Зменшення кількості надмірно корельованих ознак допомагає уникнути перенавчання. Здатність нейромережевих моделей запам’ятовувати залежності між подібними ознаками,

призводить до погіршення узагальнення на нових даних. Видалення або об'єднання корельованих ознак (наприклад, за допомогою PCA) може покращити продуктивність моделі.

- **Оптимізацію процесу навчання.** Зайві корельовані параметри збільшують вимоги до обчислювальних ресурсів, оскільки модель витрачає час на навчання з дубльованими або надлишковими ознаками.
- **Поліпшення інтерпретованості результатів.** Видалення або трансформація корельованих ознак робить модель більш зрозумілою, а її результати більш інтерпретованими, особливо в контексті задач оцінювання ризику ІБ.

Для вибору правильного методу кореляційного дослідження необхідно відповісти на питання чи нормально розподілені досліджувані фактори (Рис. 2.3). Висунуто дві гіпотези (2.3) для перевірки:

- Нульова гіпотеза ($H_0$): дані підпадають під зазначений розподіл.
- Альтернативна гіпотеза ( $H_1$ ): принаймні одне значення не відповідає вказаному розподілу.

$$H_0: P = P_0, H_1: P \neq P_0, \tag{2.3}$$

де $P$ – розподіл тестової вибірки та $P_0$– нормальний розподіл.

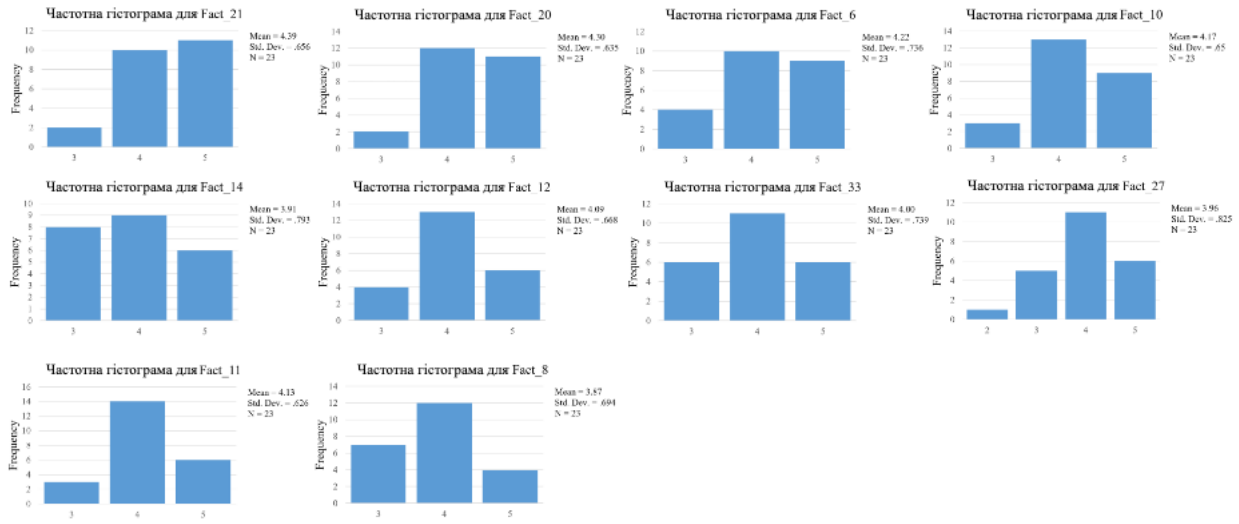


*Рис. 2.3. Частотні гістограми для ключових факторів ризику.*

Незважаючи на те, що побудовані частотні гістограми на перший погляд достатньо симетричні та добре описуються параболічною кривою для обох тестів

Колмогорова-Смірнова (Kolmogorov-Smirnov Test, K-S Test) та Шапіро-Вілка (Shapiro-Wilk Test) значення значимості менше 0,05, що означає, що дані не мають нормального розподілу (Рис. 2.4). Отже, нульова гіпотеза про те, що дані розподілені нормально відхиляється.

| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| | Statistic | df | Sig. | Statistic | df | Sig. |
| Fact_21 | .301 | 23 | <.001 | .760 | 23 | <.001 |
| Fact_20 | .293 | 23 | <.001 | .771 | 23 | <.001 |
| Fact_6 | .248 | 23 | <.001 | .798 | 23 | <.001 |
| Fact_10 | .301 | 23 | <.001 | .788 | 23 | <.001 |
| Fact_11 | .322 | 23 | <.001 | .778 | 23 | <.001 |
| Fact_12 | .291 | 23 | <.001 | .798 | 23 | <.001 |
| Fact_33 | .239 | 23 | .001 | .815 | 23 | <.001 |
| Fact_27 | .260 | 23 | <.001 | .857 | 23 | .004 |
| Fact_14 | .223 | 23 | .004 | .807 | 23 | <.001 |
| Fact_8 | .270 | 23 | <.001 | .804 | 23 | <.001 |

a. Lilliefors Significance Correction

*Рис. 2.4. Перевірка нормальності для ключових факторів ризику.*

Оскільки об’єм досліджуваної вибірки невеликий ($n<30$), всі дані мають ранговий характер (представлені у вигляді рангів або порядкових шкал) та розподіл їх значень не відповідає нормальному, то приймається рішення про вибір коефіцієнта рангової кореляції r-Спірмена (2.4).

$$r = 1 - \frac{6\sum d_i^2}{n(n^2-1)}, \tag{2.4}$$

де $n = 10$ – кількість факторів, $d_i$ – різниця між двома рангами кожного оцінювання.

Приймаючи рішення про вибір типу кореляції, при інтерпретації результатів важливо пам’ятати і враховувати, що лінійні кореляції є більш точними, ніж рангові. Ранжування значень при використанні r-Спірмена природним чином знижує міру індивідуальної мінливості виміряного показника.

Для оцінювання обґрунтованості використання вищеописаного інтрументарію дослідження було обраховано коефіцієнти кореляції для ключових факторів ризику сучасних розподілених інформаційних систем.

**Correlations**

| | | | Fact_21 | Fact_20 | Fact_6 | Fact_10 | Fact_11 | Fact_12 | Fact_33 | Fact_27 | Fact_14 | Fact_8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Spearman's rho | Fact_21 | Correlation Coefficient | 1.000 | .065 | -.095 | .056 | -.055 | .207 | .000 | .118 | .340 | -.251 |
| | | Sig. (2-tailed) | . | .770 | .665 | .801 | .803 | .344 | 1.000 | .592 | .112 | .248 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_20 | Correlation Coefficient | .065 | 1.000 | .119 | .244 | .134 | .110 | .107 | -.164 | .066 | -.528** |
| | | Sig. (2-tailed) | .770 | . | .588 | .262 | .544 | .616 | .628 | .453 | .765 | .010 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_6 | Correlation Coefficient | -.095 | .119 | 1.000 | .005 | .262 | .071 | -.069 | .123 | -.019 | -.132 |
| | | Sig. (2-tailed) | .665 | .588 | . | .983 | .227 | .749 | .755 | .577 | .932 | .548 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_10 | Correlation Coefficient | .056 | .244 | .005 | 1.000 | .423* | -.234 | .388 | -.094 | -.309 | -.157 |
| | | Sig. (2-tailed) | .801 | .262 | .983 | . | .044 | .283 | .067 | .668 | .152 | .476 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_11 | Correlation Coefficient | -.055 | .134 | .262 | .423* | 1.000 | -.145 | .193 | .089 | .040 | -.038 |
| | | Sig. (2-tailed) | .803 | .544 | .227 | .044 | . | .510 | .377 | .685 | .856 | .863 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_12 | Correlation Coefficient | .207 | .110 | .071 | -.234 | -.145 | 1.000 | .086 | .183 | .354 | -.361 |
| | | Sig. (2-tailed) | .344 | .616 | .749 | .283 | .510 | . | .695 | .404 | .098 | .091 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_33 | Correlation Coefficient | .000 | .107 | -.069 | .388 | .193 | .086 | 1.000 | -.200 | -.401 | .270 |
| | | Sig. (2-tailed) | 1.000 | .628 | .755 | .067 | .377 | .695 | . | .360 | .058 | .214 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_27 | Correlation Coefficient | .118 | -.164 | .123 | -.094 | .089 | .183 | -.200 | 1.000 | .177 | -.026 |
| | | Sig. (2-tailed) | .592 | .453 | .577 | .668 | .685 | .404 | .360 | . | .418 | .906 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_14 | Correlation Coefficient | .340 | .066 | -.019 | -.309 | .040 | .354 | -.401 | .177 | 1.000 | -.415* |
| | | Sig. (2-tailed) | .112 | .765 | .932 | .152 | .856 | .098 | .058 | .418 | . | .049 |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| | Fact_8 | Correlation Coefficient | -.251 | -.528** | -.132 | -.157 | -.038 | -.361 | .270 | -.026 | -.415* | 1.000 |
| | | Sig. (2-tailed) | .248 | .010 | .548 | .476 | .863 | .091 | .214 | .906 | .049 | . |
| | | N | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

*Рис. 2.5. Перевірка гіпотези про зв'язки між змінними з використанням коефіцієнту кореляції Спірмена.*

Інтерпретація коефіцієнта кореляції проводиться виходячи з рівня сили зв'язку:

*r> 0,01≤0,29* – слабкий позитивний зв'язок,

*r> 0,30≤0,69* – помірний позитивний зв'язок,

*r> 0,70≤1,00* – сильний позитивний зв'язок,

*r> -0,01≤-0,29* – слабкий негативний зв'язок,

*r> -0,30≤-0,69* – помірний негативний зв'язок,

*r> -0,70≤-1,00* – сильний негативний зв'язок.

Інтерпретація рівня значимості (*p*-рівня) коефіцієнта кореляції проводиться аналогічно тому, як це робилося для параметричних і непараметричних критеріїв:

– якщо *p*-рівень≤*0,05*, то зв'язок між змінними є статистично значущим;

– якщо *p*-рівень>*0,05*, то зв'язок між змінними є статистично незначущим.

Також при інтерпретації *p*-рівня коефіцієнта кореляції важливим є не тільки сам факт значимості, а й її рівень. Традиційно *p*-рівень кореляції диференціюється на три категорії:

– $p \leq 0,05 > 0,01$ – низька статистична значимість (одна зірочка – *),

– $p \leq 0,01 > 0,001$ – середня сила статистичної значимості (дві зірочки – **),

– $p \leq 0,001$ – висока статистична значимість (три зірочки – ***).

Рисунок 2.5 ілюструє взаємозв'язок між ключовими факторами ризику розподіленого середовища.

В процесі кореляційного аналізу було виявлено помірний негативний зв'язок середнього ступеня статистичної значущості між факторами Factor_20 та Factor_8 – *r*-Спірмена = -0,528 при $p \leq 0,01$, а також помірний негативний зв'язок низького ступеня статистичної значущості між факторами Factor_14 та Factor_8 – *r*-Спірмена = -0,415 при $p \leq 0,05$.

Аналізуючи результати кореляційного аналізу можна дійти висновку, що серед досліджуваних факторів ризику існує помірний позитивний зв'язок низького ступеня статистичної значущості для кореляції змінних Factor_10 та Factor_11 – *r*-Спірмена = 0,423 при $p \leq 0,05$ [68, 70].

Отримані результати свідчать про те, що фактори ризику мають значний ступінь взаємозв'язку, часто є взаємопов'язаними і діють в комплексі, що обумовлює їх комбінований вплив на безпеку PIC. Це підкреслює необхідність застосування комплексного та багатокритеріального підходу до їх аналізу, із врахуванням усіх можливих залежностей.

Отже, результати дослідження демонструють, що всі фактори ризику в процесі життєвого циклу сучасної розподіленої системи є надзвичайно важливими та потребують детального аналізу та врахування при побудові профілю потенційних загроз та здійсненні оцінювання ризиків інформаційної безпеки.

Попередній статистичний аналіз відіграє важливу роль у виборі та підготовці ознак для оптимізації глибинної нейромережевої архітектури, що розглядатиметься в наступних параграфах. Окрім цього, це сприяє якісному плануванню процедури інжинірингу ознак та нормалізації даних на підставі виявлених кореляцій для підвищення точності та стабільності класифікаційних моделей глибинного навчання.

## 2.3. Розробка нейромережевої моделі оцінювання ризику на основі багатокритеріального аналізу розподілених метрик активу

Проведений у попередньому розділі аналіз продемонстрував доцільність застосування алгоритмів машинного навчання, штучних нейронних мереж та парадигми глибинного навчання для вирішення задач оцінювання ризиків кібербезпеки в комплексних, розподілених, та велико-масштабованих інформаційних системах. Організація такої оцінки в РІС передбачає вирішення комплексу задач пов'язаних в першу чергу з наявністю значної невизначеності, обумовленої складністю архітектури та потоків даних розподілених інформаційних систем, неповнотою або ж повною відсутністю інформації про її компоненти та їх стан, а також необхідністю в режимі часу близькому до реального аналізувати великі, часто неповні та різнорідні набори параметрів та метрик, що описують стан захищеності активів та вузлів такої системи. Необхідність витягнення з «сирих» гетерогенних за структурою та походженням метаданих про роботу розподіленої системи невідомих, але практично корисних знань, які можуть бути певним чином інтерпретовані і використані для прийняття рішень про рівень ризику, придає даній проблемі нетривіального трактування.

Експериментальна частина дослідження спрямована на розробку, апробацію та валідацію моделей оцінювання ризику для розподілених інформаційних систем на основі методів інтелектуального аналізу даних та алгоритмів машинного навчання, зокрема глибоких нейронних мереж. Вона передбачає побудову, навчання та тестування комплексу моделей класифікації ризиків на основі багатокритеріального аналізу гетерогенних метаданих та метрик про стан мережевих активів РІС, що можуть бути агреговані на етапі інвентаризації [63, 65].

Узагальнення результатів анкетування та кореляційного аналізу, визначення переліку найважливіших факторів ризику та контролів безпеки, а також формування «карти» взаємозв'язків між чинниками ризику слугує основою для подальшого вибору ознак та адаптивного налаштування нейромережевої моделі з урахуванням виявлених закономірностей.

### 2.3.1. Особливості та ключові принципи машинного аналізу даних мережевих інформаційних активів

Розподілені інформаційні системи характеризуються великою кількістю різнорідних компонентів (сервери, клієнтські, мережеві та IoT-пристрої, тощо), які генерують величезний обсяг даних, що може бути використаний для аналізу ризиків ІБ [117]. Ці дані зазвичай включають числові, категоріальні, булеві метрики, часові штампи, а також агреговані масиви показників. Унікальність цих даних полягає у високій гетерогенності, що зумовлена різноманітністю джерел інформації, методів збору даних та особливостями кожного компоненту системи.

Завдання машинного аналізу таких даних передбачає вирішення низки проблем, які мають як теоретичне, так і прикладне значення. До основних викликів відносяться:

- **Неповнота та низька якість даних**: У розподілених системах часто спостерігається відсутність значень для певних метрик, що значно ускладнює побудову надійної моделі.
- **Невизначеність у даних**: Частина метрик може бути представленою з низькою точністю, або їх значення можуть суттєво варіюватися залежно від контексту.
- **Високий рівень гетерогенності**: Дані для аналізу можуть надходити з різних джерел та мати концептуально різну природу (окремі метрики та показники зібрані автоматизованим шляхом, журнали подій та системні логи, дані опитувань персоналу, аудитів ІБ тощо), що значною мірою пов’язано з широким інструментарієм механізмів збору та агрегації, а також значною диференціацією у використовуваних апаратних та програмних засобах для побудови сучасний розподілених екосистем. Окрім цьому такі дані характеризуються різними форматами представлення, що потребує складної попередньої обробки для забезпечення узгодженості та стандартизації процесу аналізу та опрацювання.
- **Необхідність забезпечення масштабованості**: Дані для аналізу можуть охоплювати записи про сотні тисяч активів, і будь-яка запропонована модель повинна бути здатною працювати із такими обсягами інформації з можливістю забезпечення оперативного аналізу, подальшої адаптації та масштабування.

На рівні дисертаційного дослідження особливий акцент зроблено на тому, що інформаційні активи мають багатовимірну структуру опису. Для кожного активу в системі можуть бути представлені такі типи даних метрик:

- **Числові метрики**: наприклад, кількість відкритих портів, кількість виявлених вразливостей, кількість зареєстрованих інцидентів тощо.
- **Булеві показники**: наявність антивірусного захисту, шифрування дисків, наявність механізмів резервного копіювання, застосування політик ІБ тощо.
- **Категоріальні дані**: тип пристрою, операційна система, рівень критичності активу тощо.
- **Дата-часові метрики**: дата останньої активності / сканування / оновлення / інциденту тощо.
- **Агреговані дані**: зведені показники стану захищеності (наприклад, дані по інстальованому програмному забезпеченню, категоризація відкритих портів, агреговані показники по різним системам антивірусного захисту тощо).

Слід зазначити, що предметом дослідження на даному етапі є виключно мережеві активи та апаратні компоненти розподіленої системи. В рамках дисертаційного роботи не досліджуються сервіси обробки даних, комунікаційні механізми, організаційні та операційні компоненти.

Інтеграція та об’єднання даних із різних джерел є ключовим завданням на початковому етапі оцінки стану захищеності будь-якої інфраструктури РІС. Агрегація даних на етапі інвентаризації мережевих активів у розподіленій інформаційній системі – це процес збору, упорядкування та інтеграції інформації про всі мережеві компоненти, які входять до складу системи. Цей процес передбачає застосування різних механізмів для отримання актуальної та цілісної картини мережевої інфраструктури [67, 69].

Основні механізми агрегації даних включають:

1. **Автоматизоване сканування мережі** – збір даних про активні пристрої у мережі автоматизованими інструментами сканування (наприклад, Nmap, SolarWinds, Lansweeper, Open-AudIT), які автоматично ідентифікують мережеві пристрої, їх IP-адреси, MAC-адреси, відкриті порти, протоколи, типи пристроїв тощо.

2. **Використання протоколів управління**

SNMP (Simple Network Management Protocol): Отримання інформації про конфігурацію, стан, та параметри роботи пристроїв.

ICMP (Internet Control Message Protocol): Використовується для перевірки доступності пристроїв у мережі.

WMI (Windows Management Instrumentation): Для збору даних із Windows-пристроїв.

3. **Збір даних із конфігураційних файлів** – зчитування даних (IP-адреси, маршрутизаційні таблиці, правила брандмауера, VPN-конфігурації) із файлів конфігурації мережевих пристроїв (маршрутизаторів, комутаторів, серверів тощо). Приклад інструментів: RANCID, Oxidized, Ansible.

4. **Використання логів та журналів подій –** аналіз даних про активність мережевих пристроїв, виявлення аномалій або подій. Джерела: Syslog, журнали подій Windows, інструменти SIEM (Splunk, ELK, QRadar).

5. **Агрегація даних із систем керування** – збір актуальних метрик про мережеві активи з використанням API. До цієї категорії можна віднести інтеграцію із системами керування мережевою інфраструктурою (наприклад Cisco DNA Center, HPE IMC, Aruba Central), системи управління хмарними ресурсами (Azure, AWS, Google Cloud) тощо.

6. **Агентний збір** – що передбачає встановлення спеціалізованих агентів на кінцевих пристроях для моніторингу їх стану та конфігурацій. Приклади інструментів: Microsoft System Center Configuration Manager (SCCM), Agent-based Discovery Tools (наприклад Osquery).

7. **Централізовані бази даних активів** – використання баз даних інвентаризації (наприклад CMDB – Configuration Management Database) для побудови повної моделі мережевої інфраструктури та автоматичної синхронізації даних із різних джерел.

8. **Використання інструментів для топологічного аналізу** – збір інформації про взаємозв’язки між пристроями та побудова топології мережі через інструменти візуалізації (NetBrain, SolarWinds Network Topology Mapper тощо).

9. **Інтеграція даних із зовнішніх джерел** – наприклад із системами закупівлі, технічної підтримки чи обслуговування обладнання (дані про вендора, серійні номери, гарантії, дати оновлення тощо).

Для вирішення задачі агрегації метрик розподіленої системи у дисертації розглядається використання програмного комплексу **ITS Inventory**, роботою над розробкою та покращенням якого займається здобувач. Додаток перевірено, схвалено компанією **IBM** та опубліковано в офіційному магазині застосунків **IBM X-Force Exchange / App Exchange**. ITS Inventory є комерційним продуктом, що широко використовується для інвентаризації мережевих активів не лише багатьма українськими компаніями, а й закордонними клієнтами.

Додаток ITS Inventory надає компаніям можливість централізовано організувати швидкий доступ до розрізненої інвентаризаційної інформації про всі елементи IT-інфраструктури організації. Завдяки цьому IT-фахівці, аналітики SOC та спеціалісти з кібербезпеки можуть оперативно отримувати деталізовані дані про сервери, робочі станції, мережеве обладнання та інші компоненти складних IT-систем. Це суттєво полегшує виконання завдань моніторингу та реагування, підвищує ефективність аналізу інцидентів і сприяє виявленню конфігураційних помилок та слабких місць в IT-інфраструктурі.

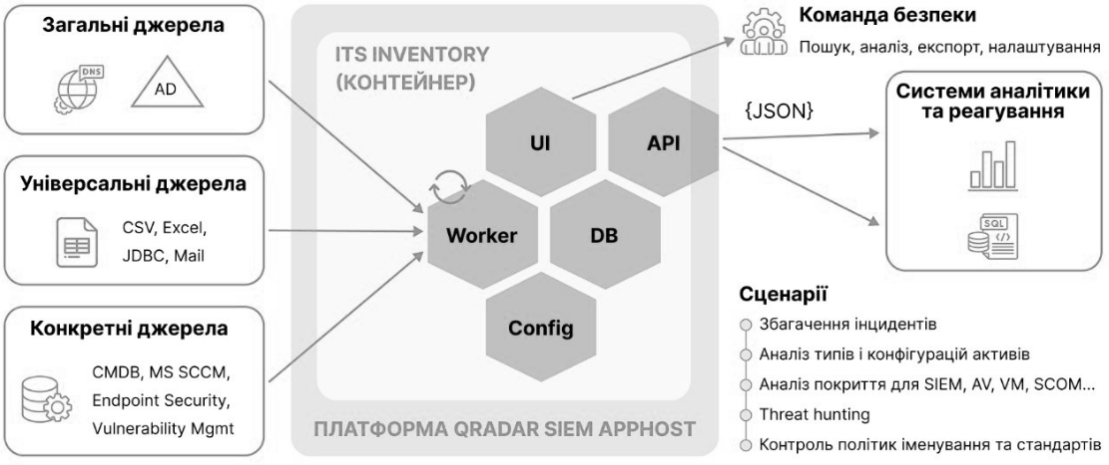


*Рис. 2.6. Схематичне представлення потоків даних застосунку ITS Inventory.*

Worker-процес здійснює безперервний моніторинг підключених джерел даних, збираючи актуальну інформацію про активи, виконуючи її аналіз, кореляцію та структурування за допомогою графової моделі взаємозв’язків для подальшого

відображення в графічному інтерфейсі (Рис. 2.6). Завдяки оптимізованому циклу аналізу, додаток гарантує доступ до актуалізованих інвентаризаційних даних в режимі часу, близькому до реального.

ITS Inventory повністю покриває всі вищеописані механізми агрегації даних та підтримує інтеграцію з хмарними сервісами, системами віртуалізації, системами моніторингу інфраструктури та управління мережею. На сьогоднішній день застосунок забезпечує підтримку всіх базових та універсальних механізмів агрегації на основі стандартних протоколів та технологій, а також понад 60 конекторів для зовнішніх пропрієтарних систем від сторонніх вендорів, перелік яких постійно розширюється.

Завдяки вбудованому REST API, програмний продукт може виконувати роль джерела даних для зовнішніх систем, наприклад Business Intelligence (BI), Business Process Automation, IT Accounting, Security orchestration, automation and response (SOAR), IT Process Management, Service Desk та систем управління змінами. Окрім цього вказаний механізм може бути використаний в задачах автоматизованого збору диференційованих даних PIC, та подальшого аналізу за допомогою проєктованих моделей оцінювання ризику кібербезпеки (Рис. 2.7).

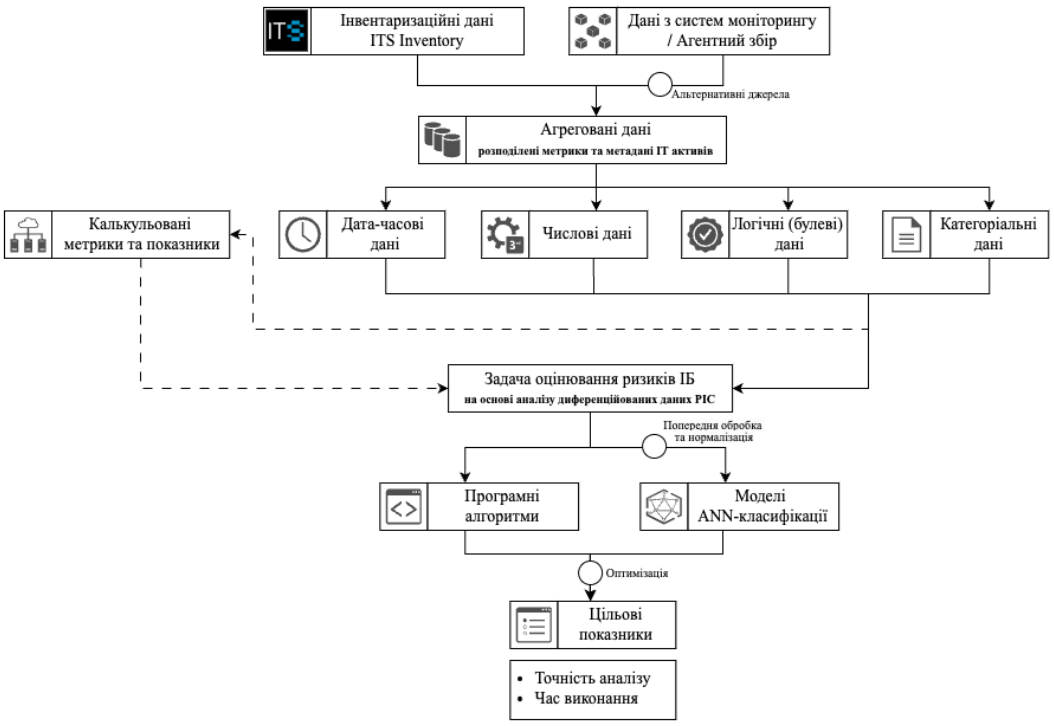


*Рис. 2.7. Концептуальна схема комплексної системи машинного аналізу гетерогенних даних PIC в задачах оцінювання ризику ІБ.*

Таким чином, програмний комплекс ITS Inventory вже виконує функції безагентного збору, уніфікації, попередньої обробки та консолідації всіх фактичних даних PIC про IT-активи в єдиному середовищі, що значною мірою спрощує задачу проєктування комплексної системи машинного аналізу диференційованих даних PIC та моделювання процесу оцінювання ризику в розподіленому середовищі.

### 2.3.2. Підготовка та аналіз вхідних наборів даних для оцінки стану інфраструктури PIC

Вхідний масив даних репрезентує дані типової розподіленої інформаційної системи корпоративного рівня, та містить близько 220 тисяч записів про мережеві активи. Початковий набір містив близько 350 параметрів та ознак, що комплексно описують поточний стан інформаційного активу. Виявлено, що розподілені метрики потребують попереднього аналізу через високий рівень гетерогенності та наявність незаповнених значень.

На основі результатів проведення багатокритеріального аналізу та кореляції даних ознак із побудованим профілем ключових факторів ризику, що був виконаний у попередніх параграфах, здійснено оптимізацію простору вхідного вектору розподілених метрик про роботу інформаційних активів PIC, а їх перелік скорочено до 75 інформативних параметрів, що певним чином відображать стан захищеності активу та можуть бути асоційовані з рівнем ризику.

Відносно предметної області даний перелік параметрів можна згрупувати на наступні логічні класи:

- Загальні параметри мережевих активів (наприклад тип пристрою, операційна система, середовище, тип підключення, характеристики критичності та поточного статусу активу тощо);
- Активність та моніторинг (наприклад метрики останньої активності мережевого активу, дані SIEM та лог-моніторингу тощо);
- Політики безпеки та управління (дані по застосовуваним політикам, парольний менеджмент тощо);

- Захист кінцевих точок та конфіденційності (дані щодо антивірусного захисту та DLP систем, шифрування дисків тощо);
- Сканування та оцінка вразливостей (дані відносно проведених та запланованих сканувань, відомості по відкритим портам та задетектованим вразливостям тощо);
- Резервне копіювання та відновлення (дані щодо наявності та режиму виконання бекапів);
- Інциденти безпеки та попередній досвід (ретроспективна історія подій та інцидентів для поточного активу);

Програмна платформа ITS Inventory проводить уніфікацію та стандартизацію більшості категорій метрик на основі попередньо встановлених рекомендацій та алгоритмів обрахунку.

Для подальшого опрацювання серед представленого набору ознак аналітичним шляхом виокремлено 42 показники, що відповідають найбільш релевантним характеристикам для задачі аналізу ризиків на основі оцінки значущості та корисності даних. Відбір здійснено на основі ряду наступних критеріїв:

- **Збереження інформативності**: залишені лише ті змінні, які мають високу варіативність та безпосередньо впливають на оцінювання ризиків ІБ.
- **Виключення надлишкової інформації**: ознаки, що дублюють інформацію або не несуть цінності для аналізу (як-от специфікації версій ПЗ та окремих модулів), були видалені. Проте наявність цих даних сигналізувала щодо наявності певних характеристик, тому попередньо використовувалась для формування агрегованих параметрів.
- **Зниження кількості пропусків**: змінні з великою кількістю пропусків, які складно заповнити без втрати якості даних, були виключені.
- **Фокус на ключових показниках**: пріоритет на вплив ознак на результативність моделі.

Приклад розподілених метаданих і метрик мережевих активів в умовах типової інфраструктури PIC представлено в **Додатку В**.

З метою уніфікації, об’єднання даних та уникнення надлишковості, як уже було сказано, для ряду параметрів додатково виконано формування агрегованих показників (наприклад метрики антивірусного захисту та сканування вразливостей, що представлені широким спектром ознак для окремих вендорів). Узгодження даних із різних джерел дозволяє отримати повний та багатовимірний опис кожного активу, що є основою для подальшого оцінювання ризику.

У Таблиці 2.8 на прикладі метрик Asset category та Device type подано зразок профілювання IT-активів за типами та рівнем критичності для функціонування розподіленої системи та потенційних наслідків для бізнес-процесів.

*Таблиця 2.8*

*Приклад профілювання IT-активів за типами*

| **Device type** | **Asset category** | **Опис** | **Рівень критичності** |
|---|---|---|---|
| PC | Workstation | Робочі станції / персональні комп’ютери | Низький |
| NB | Workstation | Ноутбуки | Низький |
| TAB | Workstation | Планшети | Низький |
| TC | Workstation | Тонкі клієнти | Середній |
| MB | Workstation | Моноблоки | Середній |
| SRV | Server | Сервери | Високий |
| SRVNI | Server | Неідентифіковані сервери | Середній |
| SRC | Server | Віртуальні машини | Середній |
| DB | Server | Сервери баз даних | Високий |
| Router | Network | Мережеві маршрутизатори | Середній |
| Switch | Network | Мережеві комутатори | Середній |
| NET | Network | Мережеве обладнання | Середній |
| AP | Network | Точки доступу | Середній |
| Video | Device | Пристрої системи корпоративного відеонагляду | Низький |
| IP Phone | Device | Пристрої системи IP-телефонії | Низький |
| PRN | Device | Принтери / сканери / багатофункціональні пристрої | Низький |
| IOT | Device | Пристрої / сенсори Інтернету речей | Низький |
| Cash | Finance | Касові апарати | Критичний |
| POS | Finance | Платіжні термінали | Критичний |
| PPO | Finance | Реєстратори розрахункових операцій | Критичний |

1 Приставка «**D» вкінці регламентує пристрої, що на поточний момент виведені з експлуатації (рівень критичності - Низький)
2 Приставка «**A» вкінці регламентує аліаси

Додатково здійснено аналіз розподілу даних за типом та категорією мережевого пристрою (Рис. 2.8).

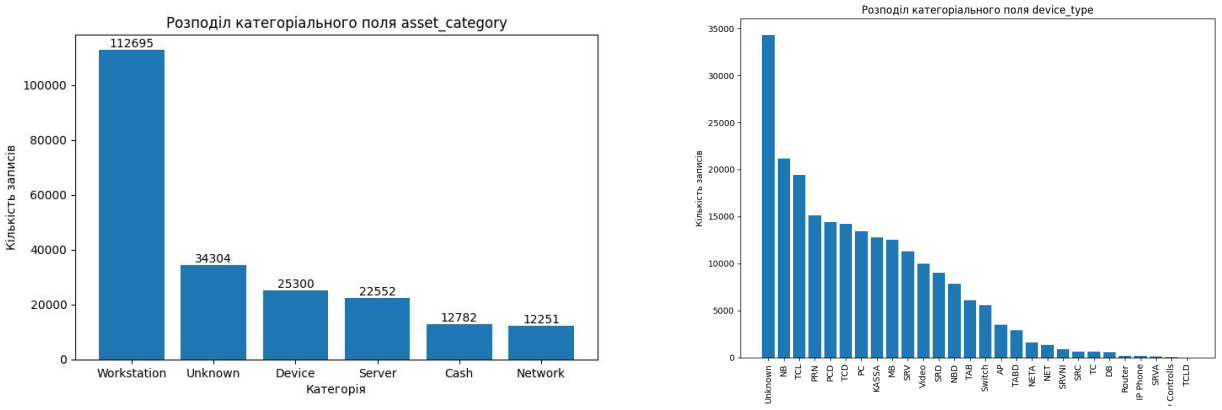


*Рис. 2.8. Розподіл даних за типом та категорією мережевого пристрою.*

Результати аналізу свідчать про велику кількість неідентифікованих активів, для яких відсутня інформація про тип та категорію асету.

Для перевірки гіпотези $H_{(2)}$ про вплив ступеню інформаційної наповненості та міри якості і повноти вхідних даних на показник достовірності результатів класифікації рівнів ризику, проведено аналіз загальної заповненості даних, що дозволило визначити граничні значення. Для цього проаналізовано динаміку розподілу незаповнених значень (Рис. 2.9).


*Рис. 2.9. Динаміка розподілу даних в залежності від кількості незаповнених метрик.*

Позначимо кількість незаповнених ознак для конкретного екземпляру набору даних як $M_i$ при загальній кількості досліджуваних метрик $N$. Проведений аналіз демонструє, що досліджуваний набір даних має суттєві сплески в сторону збільшення кількості незаповнених метрик та погіршення наповненості на межі:

- близько 86 тисяч записів (20 незаповнених ознак ( $M_i > 19$) та різке погіршення якості вхідних даних після цього порогового значення);

- близько 173 тисяч записів (24 незаповнена ознака ( $M_i > 23$), значний локальний сплеск та велика кількість записів представлення для наступної незаповненої метрики);

Несуттєвий сплеск присутній на рівні декількох тисяч записів ($M_i = [5,6]$), проте він не є значним за амплітудою, а тому не має прикладного значення на результуючі показники моделювання. Фактично до рівня 19 незаповнених метрик ($M_i \leq 19$) включно вхідні дані демонструють чудову динаміку заповненості з малою кількістю представлених зразків для кожного досліджуваного значення $M_i$.

У результаті підготовки даних було створено три експериментальні вибірки різного розміру, які дозволять дослідити вплив повноти даних на якість моделювання. Характеристики сформованих наборів представлено у Таблиці 2.9.

*Таблиця 2.9*

*Характеристики сформованих наборів даних*

| **Позначення** | **Набір даних** | **Кількість записів** | **Кількість незаповнених параметрів $M_i$** | **Індекс повноти даних (%)** |
|---|---|---|---|---|
| $D_{full}$ | Повний | 219884 | $M_i \leq 27$ | 35,71% |
| $D_{ext}$ | Розширений / збалансований | 173103 | $M_i \leq 23$ | 45,24% |
| $D_{core}$ | Найбільш насичений | 86660 | $M_i \leq 19$ | 54,76% |

В подальшому для кожного набору дані розділені на навчальну (80%) та тестову (20%) вибірки для тренування проєктованих моделей класифікації, та оцінки їх якісних характеристик і точності залежно від кількості та наповненості даних у кожному з датасетів.

На наступному етапі виконано попередню обробку та нормалізацію вхідних масивів даних. Попередня обробка є критичною для забезпечення якості вхідних даних і зменшення впливу «шуму», що суттєво підвищує точність моделей класифікації рівня ризику. Реалізація автоматизованих алгоритмів нормалізації, стандартизації та попередньої обробки значень в залежності від типу даних досліджуваних параметрів є важливим кроком на шляху їх подальшого представлення для навчання моделей.

Більшість метрик мають категоріальний характер тому на даному етапі необхідна їх векторизація. Для інтерпретації категоріальних змінних з нечислового формату в цілочисловий застосовано методи **LabelEncoder** та **OneHotEncoder**. Перший 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 бібліотеки Scikit Learn (або ж методу get_dummies бібліотеки pandas). Він перетворює кожну категорію на окрему бінарну ознаку, що нівелює вищеописані проблеми та дозволяє ефективно використовувати ці дані у моделях, не створюючи упередженості через числове ранжування категорій, але в свою чергу спричиняє розростання простору вхідних змінних. Для випадків, коли значення були відсутні вводилась категорія за замовчуванням [93-94].

Для числових ознак було використано метод **Min-Max Scaling**, який масштабує значення в межах заданого діапазону (зазвичай [0, 1] або [−1, 1]). Цей метод вибрано з кількох причин:

1. Підвищення стабільності моделей: масштабування даних до одного діапазону допомагає уникнути домінування ознак із великими значеннями над іншими. Це особливо важливо для алгоритмів, чутливих до масштабу, таких як метод опорних векторів (SVM), нейронні мережі та градієнтний бустинг.

2. Збереження пропорційності даних: На відміну від інших методів, Min-Max Scaling не змінює розподіл даних і зберігає відносні пропорції між значеннями ознаки, що важливо для інтерпретації результатів.

$$x' = \frac{x - min(x)}{max(x) - min(x)} \tag{2.5}$$

де $x$ – початкове значення;

$min(x)$ – мінімальне значення ознаки;

$max(x)$ – максимальне значення ознаки.

Для ознак пов’язаних з дата-часовими метриками відбувається модифікація шляхом **динамічного визначення зрізу часу $\Delta t$**, що минув з моменту події $t_i$ до поточного часу $t$ (часу виконання аналізу).

$$\Delta t = | t_i - t | \tag{2.6}$$

де $\Delta t$ – різниця часу, для подальшого аналізу;

$t_i$ – дата-час події, що відображена метрикою $i$;

$t$ – поточний час.

Таким чином, навчальна вибірка буде оперувати значеннями різниці часу (тривалості), що минув замість використання статично прописаних абсолютних значень – для прикладу, чим менше часу минуло з моменту останнього оновлення сигнатур антивірусного ПЗ, тим відповідно кращою є безпекова ситуація для активу. Для нормалізації отриманих дата-часових параметрів та числових метрик було розглянуто декілька підходів: можливість та доцільність заповнення пропусків медіаною, модою, введення додаткового значення (наприклад -1 як фінального значення після нормалізації). Останній підхід на практиці показав найгірші результати ефективності, оскільки введене значення вносить дисбаланс в розподіл даних, а модель акцентує увагу на незаповнених параметрах. Емпірична перевірка ефективності моделей для різних підходів продемонструвала найкращі показники точності при заповненні таких значень нулем.

Таким чином, комплексний аналіз різноманітних типів даних потребує спеціалізованих підходів, таких як комбіновані моделі обробки категоріальних, числових, бінарних та дата-часових ознак. Такий підхід до нормалізації забезпечив коректну підготовку даних з використанням інструментарію автоматизованих алгоритмів обробки даних для подальшого використання у задачах машинного навчання.

### 2.3.3. Архітектура моделі оцінювання ризику кібербезпеки на основі нейромережевого аналізу гетерогенних даних РІС

Для проведення емпіричної перевірки висунутих гіпотез та моделювання процесу оцінювання ризику в розподіленому середовищі РІС пропонується

використовувати інструментарій глибоких нейронних мереж. Переваги підходу побудованого на принципах машинного навчання та алгоритмів ГНМ описано в попередніх розділах дисертаційного дослідження та полягають в першу чергу в чудовій здатності до узагальнення та нелінійного моделювання складних внутрішніх залежностей і взаємозв'язків, гарних апроксимуючих можливостях та високому рівні адаптивності до структури даних, гнучкості архітектури та потенціалі для роботи з великими обсягами часто неповних неоднорідних за структурою даних, що створює передумови для побудови більш адаптивних прогностичних систем ризик-менеджменту в умовах функціонування сучасних РІС. Задача ідентифікації рівня ризику інформаційної безпеки по суті зводиться до вирішення класичного завдання класифікації. У статистичному моделюванні аналіз класифікацією – це сукупність статистичних процесів для оцінки зв'язків між залежною змінною (часто її називають «змінною результату») та однією або декількома незалежними змінними (часто їх називають «предикторами», або «коваріатами»), при якому результуюча змінна може приймати дискретний набір значень [72, 74].

Як вже було сказано вище, для задач моделювання використано набори даних різного об'єму, що включають 219884, 173103 та 86660 екземпляри даних та 43 атрибути, останнім з яких є рівень ризику – промаркований цільовий атрибут, прогнозування якого є метою даного етапу. Перші 42 атрибути, які являють собою розподілені метадані та метрики інформаційної системи після проведення попереднього аналітичного опрацювання – це предиктори, на основі яких відбувається обрахунок цільового атрибуту. Цільова ознака може бути представлена 5 основними категоріями, що відображені у Таблиці 2.10.

*Таблиця 2.10*

*Перелік значень цільового атрибуту*

| **Позначення** | **Рівень ризику** | **Представлення в датасеті** | **Кількість записів** | **Відсоток (%)** |
|---|---|---|---|---|
| $R_4$ | Критичний | Critical | 9851 | 4,48% |
| $R_3$ | Високий | High | 26009 | 11,83% |
| $R_2$ | Середній | Medium | 46578 | 21,18% |
| $R_1$ | Низький | Low | 62884 | 28,6% |
| $R_0$ | Інформаційний | Moderate | 74562 | 33,91% |

Процес тренування нейронної мережі вимагає розбиття набору даних на дві підмножини: навчальну та тестову вибірки. Зразки з навчального датасету слугують для тренування моделі класифікатора, тоді як зразки з тестової вибірки використовуються для незалежної та об’єктивної оцінки її точності. Окрім цього, тестова вибірка має забезпечувати репрезентативність і відповідність умовам реальних прикладних застосувань.

Таким чином, початкові набори даних було розділено на датасети для тренування (80% від початкових) та тестування (20%). При цьому навчальні дані представляють собою числову матрицю розмірності $m \times (n + 1)$, в якій кількість рядків $m$ відповідає обсягу навчальної вибірки, перші $n$ стовпців – значенням вхідних змінних моделі, а останній – значенню вихідної змінної. Хоча за кількістю рядків матриці навчальної вибірки не існує формальних рекомендацій (у проведеному експерименті це 80%), прийнято вважати, що якість навчання нейронної мережі, а, отже, і точність одержуваних результатів пропорційно залежить від обсягу навчальної вибірки. Що стосується кількості стовпців, то у даному випадку для аналізу рівня ризику вона дорівнює 42 на початковому етапі та змінюється динамічно в залежності від кількості категоріальних метрик, число яких пропорційно зростає зі збільшенням об’єму навчального набору даних.

Враховуючи специфіку досліджуваного явища та природу поняття ризику в цілому, на етапі підготовки та аналізу даних доцільно припустити, що будь-який вхідний набір, що репрезентує характеристики типової розподіленої інформаційної системи, за своєю суттю завжди буде містити нерівномірний розподіл даних між класами за цільовою метрикою. Ризик інформаційної безпеки має нерівномірний розподіл через статистичну рідкість подій із високим впливом. Ризики високого рівня менш імовірні, оскільки їх реалізація потребує складної комбінації умов, значних ресурсів і часу, тоді як низькі ризики виникають частіше через простіші механізми їх реалізації. Крім того, багаторівневий захист критичних активів знижує ймовірність ризиків високого рівня, залишаючи більш вразливими низькопріоритетні активи.

Таблиця 2.10 демонструє нерівномірний розподіл даних між цільовими класами у досліджуваній вибірці. Очікувано, домінуючими класами будуть «інформаційний»

та «низький» ($R_0$ та $R_1$), тоді як «високий» та «критичний» класи ($R_3$ та $R_4$) будуть представлені меншою мірою.

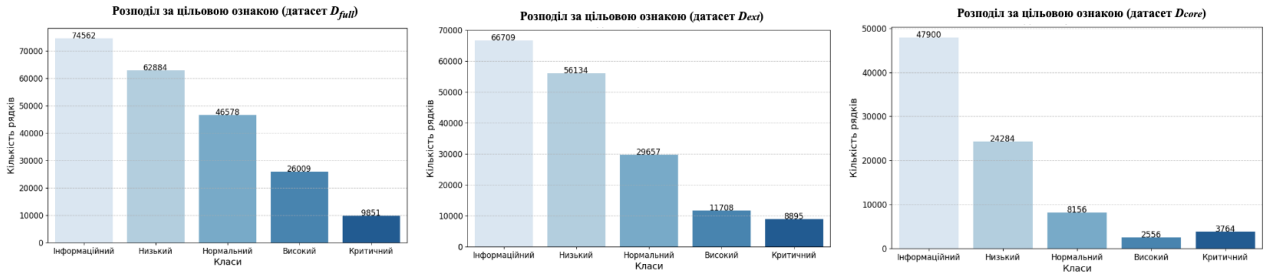


*Рис. 2.10. Розподіл даних за цільовою ознакою рівня ризику.*

Загальний вид розподілу дає змогу побудувати декілька гіпотез та сформувати подальший план:

1. Вплив дисбалансу на модель: Можна припустити, що моделі без балансування матимуть схильність до переваги домінуючих класів ($R_0$ та $R_1$), що може негативно вплинути на точність ідентифікації «високого» та «критичного» рівня ризику.

2. Збалансування датасету: Оскільки спостерігається суттєва нерівномірність у представленні класів цільової метрики, доцільно дослідити можливість застосування технік оверсемплінгу найменш представлених класів, зокрема підходів на основі алгоритмів SMOTE, ADASYN та методів вагових коефіцієнтів, щоб покращити ефективність моделі при визначенні малорепрезентованих класів.

3. Аналіз чутливості моделі: Доцільно дослідити, як різні методи балансування впливають на точність класифікації окремих класів та загальну продуктивність моделі в цілому.

З метою дослідження впливу архітектури багатошарового перцептрона на здатність інтерпретації прихованих залежностей та взаємозв’язків у вхідних даних та якість вирішення задачі класифікації прийнято рішення провести оцінку ефективності декількох варіантів архітектури. Для нейронної мережі використовувались наступні конфігурації гіперпараметрів:

- 1 прихований шар з 64 нейронами (Dropout 0.3);

- 2 приховані шари з 128 і 32 нейронами в кожному шарі (Dropout 0.3 для кожного);
- 3 приховані шари з 128, 64 та 32 нейронами у кожному шарі відповідно, (Dropout 0.3 для кожного).

Емпірично проведено підбір оптимальних значень гіперпараметрів, зокрема функцій активації. Як функцію активації для прихованих шарів було обрано ReLU (Rectified Linear Unit), для вихідного шару – softmax. Модель на основі функції ReLU демонструє нижчі помилки класифікації. Окрім цього, встановлено, що найвищу точність забезпечує класифікатор штучної нейронної мережі із наступними параметрами: алгоритм навчання (оптимізатор) – Adam, швидкість навчання – 0,001, розмір пакету (batch) – 32, функція втрат – категоріальна перехресна ентропія (Categorical Cross-Entropy, CCE).

$$L(y, \tilde{y}) = -\sum_{i=1}^{c} y_i log\ (\tilde{y}_i), \quad (2.7)$$

де $L(y, \tilde{y})$ – функція втрат для категоріальної перехресної ентропії*;*

$y_i$– справжня мітка (0 або 1 для кожного класу) закодованого цільового вектора;

$\tilde{y}_i$ – прогнозована ймовірність для класу *i*;

$c$ – кількість класів.

Експериментальна перевірка методів оптимізації SGD, RMSProp, Adagrad та Adadelta надала нижчі показники точності. Детальніше порівняння ефективності алгоритмів навчання для задач мультикласової класифікації під час оцінювання ризиків ІБ представлено в [63, 72] роботах здобувача.

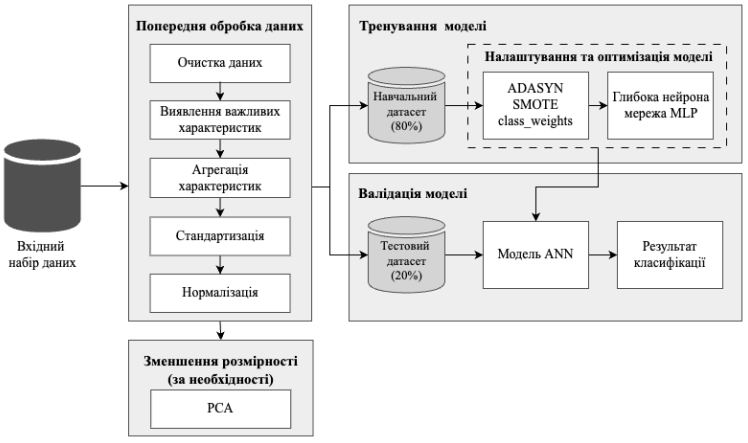


*Рис. 2.11. Структурна* схема *нейромережевого алгоритму оцінювання ризиків ІБ на основі архітектури ГНМ.*

Кількість епох на етапі навчання встановлюється автоматично, оскільки використано стратегію ранньої зупинки навчання (Early Stopping) за умови що відстежуваний показник перестає покращуватись (наприклад зміна функції втрат стає незначною, помилка навчання падає експоненціально до тих пір, поки вплив збільшення кількості епох на цю помилку не перестане бути значущим, а помилка валідації навпаки зі збільшенням кількості епох показує зворотню динаміку та починає з якогось моменту зростати). Такий механізм дозволяє поліпшити продуктивність моделі, скоротити час навчання та навантаження на обчислювальні ресурси, а також запобігти проблемам перенавчання, коли модель запам’ятовує тренувальні дані, до такої міри, що це негативно впливає на її здатність узагальнювати нові залежності.

### 2.3.4. Критерії оцінювання ефективності проєктованих моделей

В задачах машинного навчання для оцінювання ефективності класичного класифікатора використовується низка критеріїв, що обраховуються на основі так званої матриці невідповідностей або помилок (Confusion Matrix), основні принципи обчислення якої зображено на Рисунку 2.12.

| | | **Реальний клас** | |
|---|---|---|---|
| | | Позитивний | Негативний |
| **Прогнозований результат** | Позитивний | Істинно-позитивний | Хибно-позитивний |
| | Негативний | Хибно-негативний | Істинно-негативний |

*Рис. 2.12. Матриця невідповідностей класифікатора у машинному навчанні.*

Для задач бінарної класифікації наведені на рисунку величини можна охарактеризувати наступним чином:

True Positive (TP) – число істинно-позитивних результатів, коли передбачене значення збігається з реальним (тобто нейромережева модель коректно прогнозує позитивний результат).

True Negative (TN) – число істинно-негативних рішень класифікатора, коли модель правильно передбачає негативний клас.

False Positive (FP) – число хибно-позитивних результатів або помилка 1-го роду, коли істинна гіпотеза помилково відкидається (тобто нейромережева модель неправильно передбачає позитивний клас, коли насправді він негативний).

False Negative (FN) – число хибно-негативних рішень або помилка 2-го роду, коли помилково приймається хибна гіпотеза (тобто модель неправильно передбачає негативний клас, при умові що він позитивний).

Загальна кількість дослідів ($N$) буде обраховуватись як сумарне значення вищеописаних метрик (2.8).

$$N= TP+TN+FP+FN \tag{2.8}$$

Ці величини є ключовими для оцінки ефективності моделі та розрахунку низки критеріїв, які кількісно оцінюють ті чи інші аспекти роботи класифікатора у машинному навчанні (зокрема таких показників, як точність, чутливість та специфічність).

1. Позитивна умовна точність (Positive Predictive Value, PPV) або ж Precision – частка правильних позитивних передбачень серед усіх передбачених позитивних випадків:

$$PPV=TP/(TP+ FP) \tag{2.9}$$

Позитивна умовна точність показує, наскільки імовірно, що зразок, який модель класифікувала як позитивний, дійсно є позитивним.

2. Негативна умовна точність (Negative Predictive Value, NPV) – частка правильних негативних передбачень серед усіх передбачених негативних випадків:

$$NPV=TN/(TN+ FN) \tag{2.10}$$

Негативна умовна точність показує, наскільки імовірно, що зразок, який модель класифікувала як негативний, дійсно є негативним.

3. Повнота (Recall) або чутливість (Sensitivity) – частка правильних позитивних передбачень серед усіх реальних позитивних випадків (True Positive Rate):

$$TPR=TP/(TP+FN) \tag{2.11}$$

Чутливість показує, наскільки добре модель виявляє позитивні випадки.

4. Специфічність (Specificity) – частка правильних негативних передбачень серед усіх реальних негативних випадків (True Negative Rate):

$$TNR=TN/(TN+FP) \quad (2.12)$$

Специфічність показує, наскільки добре модель виявляє негативні випадки.

5. Точність (Accuracy) – частка правильних передбачень (як позитивних, так і негативних) серед усіх випадків, тобто імовірність одержати правильну відповідь:

$$ACC=(TP+TN)/(TP+TN+FP+FN) \quad (2.13)$$

Точність показує, наскільки добре модель класифікує всі зразки.

6. Площа під кривою ROC (Area Under The Curve of Receiver Operating Characteristics, AUC-ROC) – кількісний показник, що дає можливість інтерпретувати значення ROC та являє собою площу, обмежену кривою похибок. Крива ROC – це візуальне представлення якості бінарної класифікації та ефективності моделі в цілому, що відображає співвідношення між показниками TPR та TNR при різних порогових значеннях прийняття рішення. Для побудови кривої ROC, слід обчислити коефіцієнт істиннопозитивних (TPR) та істинно-негативних (TNR) результатів за кожним можливим пороговим значенням (на практиці беруться числа через вибрані інтервали), та нанести їх на графік – (TPR вздовж осі ординат, а TNR – вздовж осі абсцис).

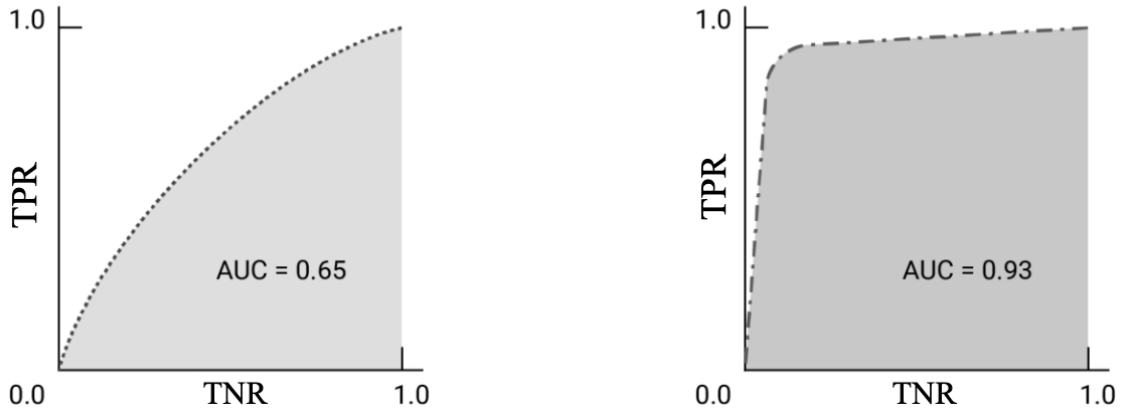


*Рис. 2.13. Порівняння ROC та AUC для двох гіпотетичних моделей класифікатора.*

Критерій AUC – корисний показник для порівняння ефективності двох різних моделей, якщо набір даних приблизно збалансований. Площа області під кривою

пропорційна предиктивній силі моделі. Модель із більшою площею під кривою зазвичай демонструє кращу класифікаційну здатність.

Криві ROC зазвичай використовуються в бінарній класифікації, де TPR і FPR можна визначити однозначно. У випадку багатокласової класифікації значення TPR або FPR отримується лише після бінарного представлення виводу моделі. Це можна зробити двома способами:

- схема One-vs-Rest порівнює кожен клас з усіма іншими (представленими як один);
- схема One-vs-One порівнює кожну унікальну попарну комбінацію класів.

В рамках дисертаційного дослідження використано перший підхід, що полягає в обчисленні кривої ROC для кожного з $i$ класів, при цьому на кожному кроці даний клас розглядається як позитивний, а решта цільових класів представляють негативний результат.

Окрім параметру AUC ROC, решта вищеописаних критеріїв також можуть бути застосовані для задач небінарної класифікації, але з певними модифікаціями. Для мультикласової ідентифікації використовуються підходи, які дозволяють оцінити загальну ефективність моделі для кожного класу окремо або в середньому по всіх класах. Для цього обраховуються усереднені показники значення кожної метрики (Precision, Recall або F1-score) для всіх класів – середнього значення (Macro Average) або зваженого середнього значення (Weighted Average), що дозволяють більш об’єктивно оцінити ефективність класифікатора.

Оцінка середнього значення (Macro Average) репрезентативна, якщо всі класи мають однакову важливість:

$$Macro\ Avg = \frac{1}{N}\sum_{i=1}^{N} K_i, \tag{2.14}$$

де $N$ – кількість класів, а $K_i$ – значення вимірюваної метрики для класу $i$.

Показник зваженого середнього значення (Weighted Average) враховує вагу (кількість зразків) кожного класу, а тому корисний для незбалансованих наборів даних:

$$Weighted\ Avg = \frac{\sum_{i=1}^{N} w_i K_i}{\sum_{i=1}^{N} w_i}, \tag{2.15}$$

де $w_i$ – ваговий коефіцієнт для класу $i$, що обраховується як відношення кількості екземплярів для даного класу до загального числа зразків.

Обчислення показника точності (Accuracy) з врахуванням всіх цільових класів набуде наступного вигляду:

$$ACC = \frac{\sum_{i=1}^{k}(TP_i+TN_i)}{\sum_{i=1}^{k}(TP_i+TN_i+FP_i+FN_i)}, \quad (2.16)$$

де $TP_i$ – кількість правильних передбачень для класу $i$, а $k$ - кількість класів.

Позитивна умовна точність (Precision) у випадку мультикласової ідентифікації вимірює, яка частка з передбачених зразків для певного класу є коректною:

$$Precision_i = \frac{TP_i}{TP_i+FP_i}, \quad (2.17)$$

де $FP_i$ – кількість помилково передбачених зразків для класу $i$.

Показник повноти (Recall) оцінює, яка частка зразків конкретного класу була правильно ідентифікована:

$$Recall_i = \frac{TP_i}{TP_i+FN_i}, \quad (2.18)$$

де $FN_i$ – кількість зразків класу $i$, які модель класифікувала неправильно.

Значення повноти та умовної точності дозволяють обрахувати показник критерію F1-міри (F1-score) – середнього гармонійного між Precision та Recall для кожного класу:

$$F1_i = 2 * \frac{Precision_i * Recall_i}{Precision_i+Recall_i}, \quad (2.19)$$

F1-міра є корисною при роботі з незбалансованими даними, оскільки вона враховує як Precision, так і Recall. Високий показник F1-score, що наближається до 1 ($F1_i \rightarrow 1$) означає баланс між цими метриками та ідеальну продуктивність моделі.

В процесі тренування нейромережевої моделі з метою уникнення перенавчання та забезпечення більш надійної оцінки застосовано метод крос-валідації, що передбачає поділ вхідних даних на декілька підмножин та тренування моделі на кожному з них, зі змінною динамічною вибіркою для тестування. Це дозволяє виділити ряд додаткових показників для аналізу, що будуть описані нижче.

Таким чином, в рамках дисертаційного дослідження для оцінки продуктивності проєктованих моделей за основу взято наступний перелік критеріїв:

**Базові показники ефективності**

1. Accuracy (test accuracy) – точність моделі на валідаційному наборі даних.

2. Average Accuracy (average accuracy) – середня точність моделі на різних підмножинах даних (за результатами крос-валідації), що надає більш комплексний показник з урахуванням всієї диференціації можливих значень.

3. Standard Deviation (standard deviation) – середнє квадратичне відхилення або ж стандартна похибка моделі, що показує наскільки результати варіюються між різними підмножинами даних (за результатами крос-валідації), і допомагає зрозуміти стабільність моделі: низьке значення вказує на те, що модель дає стабільні результати на різних підмножинах даних, тоді як високе значення може свідчити про значну диференціацію результатів та меншу стабільність.

**Метрики ефективності для кожного класу**

4. Precision (precision) – позитивна умовна точність, що показує наскільки модель точна при передбаченні правильного результату.

5. Recall (recall) – повнота показує, наскільки добре модель може ідентифікувати фактичні позитивні випадки.

6. F1-score (F1) – збалансований критерій для комплексної оцінки попередніх показників.

7. Macro Average (macro avg) – середнє значення, що обраховується для кожного критерію по класам.

8. Weighted Average (weight avg) – зважене середнє значення, що також обраховується для кожного критерію по класам та враховує коефіцієнт його важливості.

9. AUC-ROC – візуальне представлення та числовий показник ефективності моделі при порогових значеннях.

Варто зазначити, що в умовах дисбалансу цільових класів додатково варто опиратись на аналіз матриць невідповідностей, а також оцінювати метрики для кожного класу окремо з подальшим обрахунком середніх значень.

Запропонований підхід на основі комплексного обрахунку широкого ряду критеріїв забезпечує можливість проведення поглибленого аналізу достовірності

прогнозування та ефективності роботи класифікатора на основі нейромережевої архітектури, що суттєво знижує ризик підлаштування під конкретну метрику, забезпечує адаптацію до різних умов та збалансовану оцінку проєктованих моделей. Отримані моделі відзначатимуться вищою надійністю та матимуть кращу здатність до узагальнення, що є надзвичайно важливим при роботі з великими обсягами даних розподілених систем. Таким чином, використання широкого ряду критеріїв для валідації результатів нейромережевого моделювання є не лише доцільним, але й необхідним для забезпечення високої якості та надійності прогностичних моделей. Це дозволяє отримати більш точні та стабільні результати, що є критично важливим в умовах практичного застосування.

### 2.3.5. Експериментальні дослідження та інтерпретація отриманих результатів

Для досягнення максимально об’єктивної та реалістичної оцінки класифікаційних можливостей проєктованих моделей здійснено крос-валідацію методом k-fold ($k=5$). Метод крос-валідації k-fold застосовується для оцінювання продуктивності моделі та її здатності до узагальнення. Його суть полягає в розбитті вихідного набору даних на $k$ підмножин і послідовному використанні $k-1$ фолдів для навчання моделі, залишаючи один фолд для перевірки. Цей процес повторюється $k$ разів, так що кожна частина вхідного набору даних виступає в ролі валідаційної вибірки лише 1 раз (Рис. 2.14).

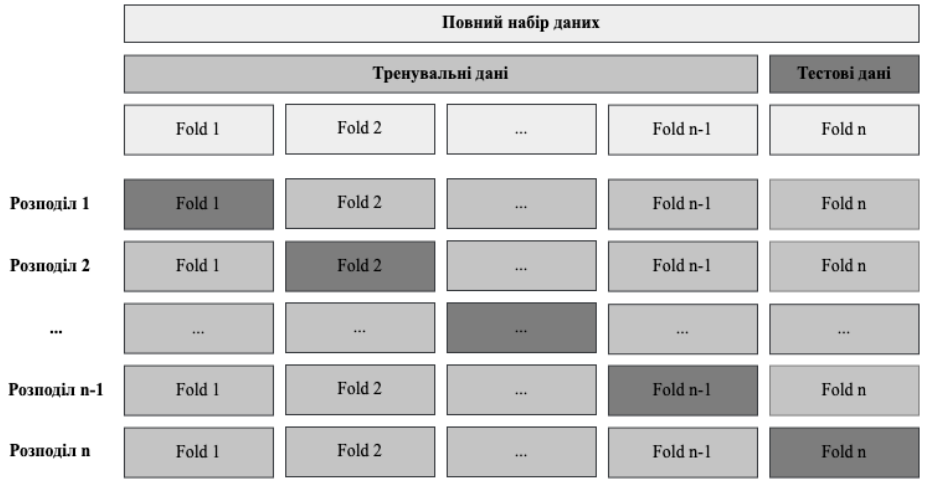


*Рис. 2.14. Схематичне зображення механізму крос-валідації методом k-fold.*

Такий підхід сприяє уникненню перенавчання та забезпечує більш об'єктивну оцінку ефективності моделі, у порівнянні з разовим розділенням на тренувальну та тестову вибірки. Таким чином, в рамках експерименту, проведено ітеративний поділ досліджуваних наборів даних випадковим чином (5 ітерацій, *k=5*), після чого розраховано середні значення точності навчання моделі для кожної підмножини.

У рамках початкової фази дослідження проведено аналіз результатів моделювання для різних наборів даних. На даному етапі дані для всіх вибірок $D_{full}$, $D_{ext}$ та $D_{core}$ подаються на навчальні моделі без додаткових механізмів балансування та оптимізації. Оскільки є явно домінуючі класи цільового параметру, що пов'язано з природою ризику, то очікувано що загальна точність буде достатньо висока за рахунок найкраще представлених класів $R_1$ (низький рівень ризику) та $R_0$ (інформаційний рівень ризику), тому доцільно детально розглянути альтернативні показники ефективності (в тому числі аналіз матриць невідповідностей), щоб зрозуміти як моделі справляються з найменш репрезентованими класами (критичний та високий рівні ризику − $R_4$ та $R_3$ відповідно), що є більш пріоритетним в контексті мети роботи.

*Таблиця 2.11*

*Результати навчання на повному датасеті $D_{full}$*

| **Показник** | **MLP (1 hidden layer)** | | | **MLP (2 hidden layer)** | | | **MLP (3 hidden layer)** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **support** |
| $R_0$ | 0.97 | 0.96 | 0.97 | 0.97 | 0.97 | 0.97 | 0.97 | 0.96 | 0.97 | 14912 |
| $R_1$ | 0.90 | 0.96 | 0.93 | 0.93 | 0.95 | 0.94 | 0.92 | 0.96 | 0.94 | 12577 |
| $R_2$ | 0.95 | 0.89 | 0.92 | 0.95 | 0.96 | 0.93 | 0.97 | 0.91 | 0.94 | 9316 |
| $R_3$ | 0.95 | 0.93 | 0.94 | 0.94 | 0.93 | 0.94 | 0.93 | 0.95 | 0.94 | 5202 |
| $R_4$ | 0.96 | 0.95 | 0.95 | 0.97 | 0.93 | 0.95 | 0.94 | 0.95 | 0.94 | 1970 |
| **macro avg** | 0.95 | 0.94 | 0.94 | 0.95 | 0.94 | 0.95 | 0.94 | 0.95 | 0.94 | 43977 |
| **weight avg** | 0.94 | 0.94 | 0.94 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 | 43977 |
| **test accuracy** | 94.26% | | | 94.98% | | | 94.82% | | | |
| **average accuracy** | 0.9428 | | | 0.9430 | | | 0.9439 | | | cross-valid. |
| **standard deviation** | 0.0019 | | | 0.0041 | | | 0.0022 | | | |

Результати аналізу навчання моделей з різною кількістю шарів на повному датасеті $D_{full}$ показують, що збільшення кількості прихованих шарів до трьох

дозволяє досягти найвищої продуктивності за показником середньої точності (average accuracy) за результатами крос-валідації на рівні 94.39% (Таблиця 2.11). Зокрема, тришарова архітектура демонструє високі середні значення F1-score для більшості класів, що свідчить про здатність глибших моделей краще адаптуватися до складних закономірностей у даних. Окрім того, слід відзначити, що усі 3 моделі демонструють високу точність, проте вона більшою мірою зумовлена домінуванням класів $R_0$ і $R_1$, що підтверджується вищим показником F1-score для відповідних класів на всіх досліджуваних моделях.

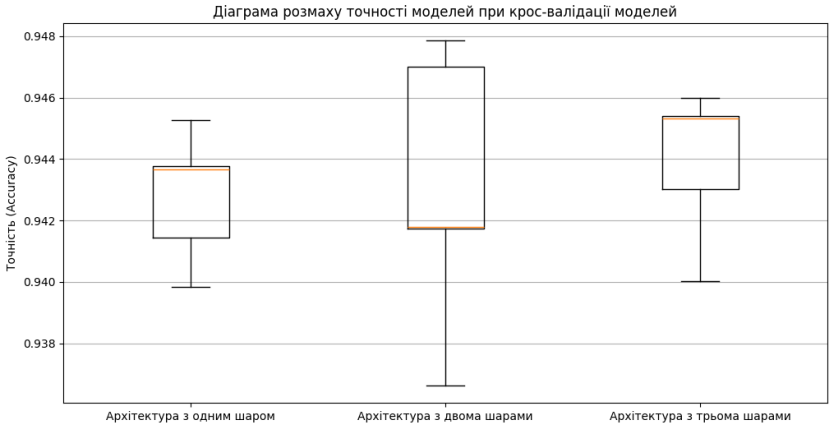


*Рис. 2.15. Діаграма розмаху точності моделей при крос-валідації (для датасету $D_{full}$).*

Варіант архітектури з 2 прихованими шарами демонструє найвищий показник стандартної похибки моделі на рівні 0.0041, що свідчить про нижчу стабільність в розрізі варіативності наборів даних між різними ітераціями крос-валідації (Рис. 2.15).

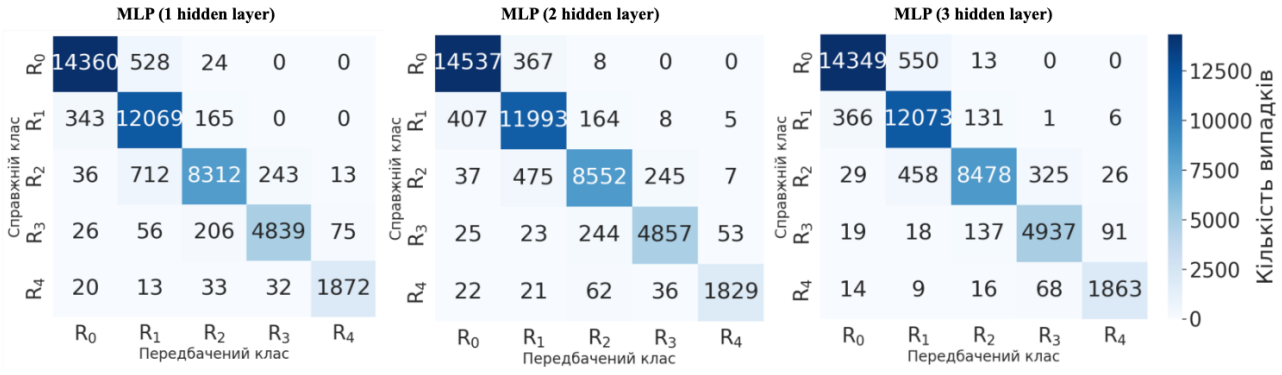


*Рис. 2.16. Матриці невідповідностей для навчання на повному датасеті $D_{full}$.*

Аналітичний огляд матриць невідповідностей також вказує на проблему з класифікацією слабко представлених класів ($R_3$ і $R_4$), для яких моделі демонструють нижчі значення точності та повноти, навіть у випадку тришарової архітектури (Рис. 2.16). Ця проблема виникає через сильний дисбаланс у розподілі цільової змінної, де домінують класи $R_0$ і $R_1$. Окрім цього, на матрицях невідповідностей можна спостерігати наступну закономірність, що актуальна для всіх архітектур незалежно від кількості прихованих шарів – якщо у випадку добре репрезентованих класів похибки прогнозування в основному відбуваються на рівні суміжних класів (наприклад детектування «низького» рівня ризику замість «інформаційного»), то для слабко представлених класів можна спостерігати значну диференціацію між прогнозованим значенням і реальним показником, що є критичним в розрізі предметної області забезпечення кібербезпеки.

Візуалізацію кривих навчання та динаміки значень функції втрат для датасету $D_{full}$ наведено на Рисунках 2.17 та 2.18.

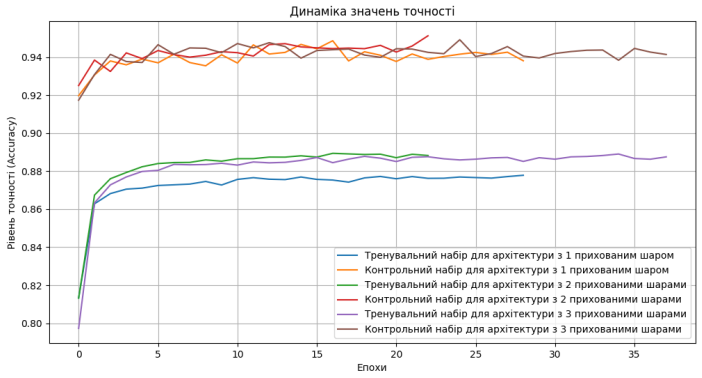


*Рис. 2.17. Приклад кривих навчання для датасету $D_{full}$.*

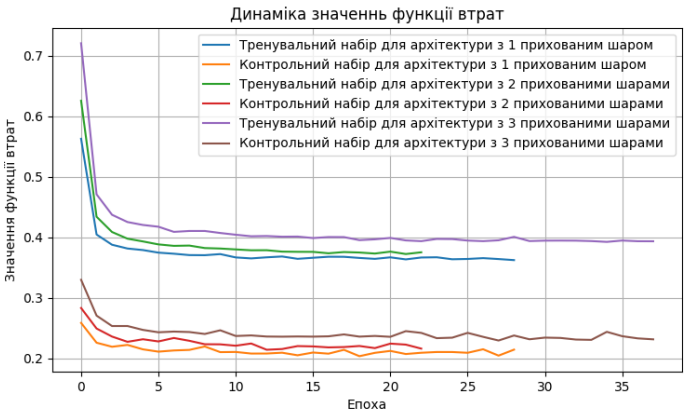


*Рис. 2.18. Динаміка значень функції втрат для датасету $D_{full}$.*

На наступному етапі розглянено ці ж показники на датасеті $D_{ext}$ (45,24% наповненості) з кількістю незаповнених метрик до 23 включно ($M_i \leq 23$). В цьому випадку розмір датасету значно зменшується (з 219884 записів до 173103), проте і змінюється кількість незаповнених метрик. Використання датасету з меншою кількістю пропусків дозволяє уникнути втрати інформації та зменшити потенційний вплив шуму в даних.

*Таблиця 2.12*

*Результати навчання на розширеному датасеті $D_{ext}$*

| **Показник** | **MLP (1 hidden layer)** | | | **MLP (2 hidden layer)** | | | **MLP (3 hidden layer)** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **support** |
| $R_0$ | 0.96 | 0.97 | 0.96 | 0.98 | 0.95 | 0.96 | 0.97 | 0.96 | 0.97 | 13342 |
| $R_1$ | 0.92 | 0.94 | 0.93 | 0.90 | 0.96 | 0.93 | 0.91 | 0.95 | 0.93 | 11227 |
| $R_2$ | 0.88 | 0.91 | 0.90 | 0.89 | 0.92 | 0.91 | 0.92 | 0.89 | 0.90 | 5931 |
| $R_3$ | 0.97 | 0.78 | 0.87 | 0.98 | 0.77 | 0.86 | 0.96 | 0.82 | 0.88 | 2342 |
| $R_4$ | 0.96 | 0.95 | 0.95 | 0.93 | 0.97 | 0.95 | 0.94 | 0.96 | 0.95 | 1779 |
| **macro avg** | 0.94 | 0.91 | 0.92 | 0.94 | 0.91 | 0.92 | 0.94 | 0.92 | 0.93 | 34621 |
| **weight avg** | 0.93 | 0.93 | 0.93 | 0.94 | 0.93 | 0.93 | 0.94 | 0.94 | 0.94 | 34621 |
| **test accuracy** | 93.41% | | | 93.45% | | | 93.84% | | | |
| **average accuracy** | 0.9363 | | | 0.9384 | | | 0.9389 | | | cross-valid. |
| **standard deviation** | 0.0016 | | | 0.0037 | | | 0.0032 | | | |

Розподіл цільової ознаки як і в попередньому випадку показав значний дисбаланс: домінують класи інформаційного ($R_0$) та низького ($R_1$) рівнів, тоді як класи «середній» ($R_2$), «високий» ($R_3$) та «критичний» ($R_4$) представлені низькою кількістю екземплярів (Рис. 2.10).

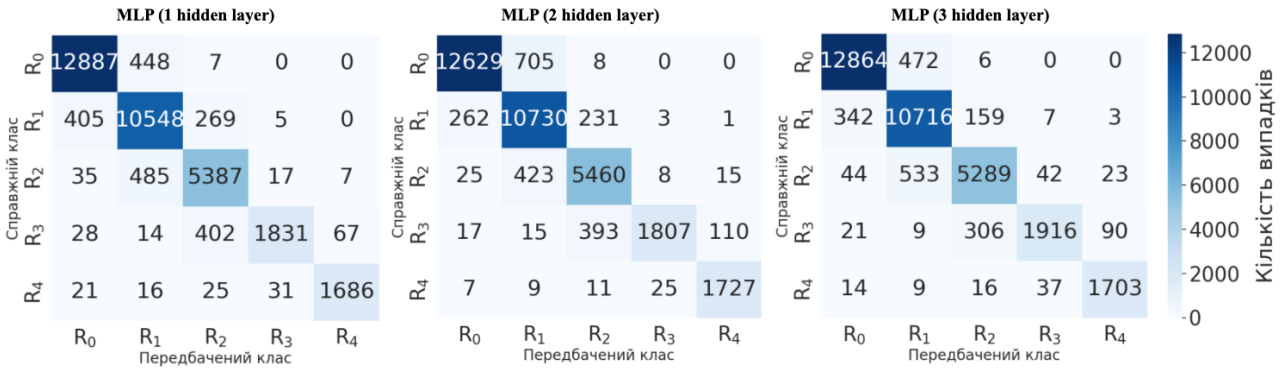


*Рис. 2.19. Матриці невідповідностей для навчання на розширеному датасеті $D_{ext}$*

Як і для попереднього набору даних найкращу ефективність за результатами крос-валідації показала модель з трьома прихованими шарами – точність на рівні 93.89%, що є найкращим показником серед усіх трьох варіантів архітектур. При цьому усі 3 моделі демонструють труднощі з класифікацією елементів класів $R_3$ та $R_4$, проте добре справляються з домінуючими класами (Таблиця 2.12).

На найбільш концентрованому датасеті $D_{core}$ (54,76% наповненості) з кількістю незаповнених метрик до 19 включно ($M_i \leq 19$) в даних також спостерігається суттєвий дисбаланс (Рис. 2.10).

*Таблиця 2.13*

*Результати навчання на найбільш насиченому датасеті $D_{core}$*

| **Показник** | **MLP (1 hidden layer)** | | | **MLP (2 hidden layer)** | | | **MLP (3 hidden layer)** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **support** |
| $R_0$ | 0.96 | 0.96 | 0.96 | 0.97 | 0.95 | 0.96 | 0.96 | 0.97 | 0.96 | 9580 |
| $R_1$ | 0.87 | 0.93 | 0.90 | 0.86 | 0.94 | 0.90 | 0.88 | 0.92 | 0.90 | 4857 |
| $R_2$ | 0.88 | 0.77 | 0.82 | 0.86 | 0.79 | 0.82 | 0.85 | 0.79 | 0.82 | 1631 |
| $R_3$ | 0.86 | 0.60 | 0.71 | 0.83 | 0.60 | 0.70 | 0.84 | 0.56 | 0.67 | 511 |
| $R_4$ | 0.91 | 0.92 | 0.92 | 0.90 | 0.92 | 0.91 | 089 | 0.94 | 0.91 | 753 |
| **macro avg** | 0.90 | 0.84 | 0.86 | 0.88 | 0.84 | 0.86 | 0.88 | 0.83 | 0.85 | 17332 |
| **weight avg** | 0.92 | 0.92 | 0.92 | 0.92 | 0.92 | 0.92 | 0.92 | 0.92 | 0.92 | 17332 |
| **test accuracy** | 92.36% | | | 92.33% | | | 92.21% | | | |
| **average accuracy** | 0.9230 | | | 0.9236 | | | 0.9237 | | | cross-valid. |
| **standard deviation** | 0.0041 | | | 0.0034 | | | 0.0035 | | | |

Результати моделювання на найбільш насиченому датасеті $D_{core}$ та аналізу матриць невідповідностей демонструють схожі закономірності – модель з трьома прихованими шарами демонструє найвищий показник середньої точності за результатами крос-валідації серед усіх протестованих на рівні 92.37%, що знову ж таки підтверджує перевагу глибоких архітектур у розв'язанні складних задач нейромережевого аналізу розподілених гетерогенних даних PIC.

Інтерпретація результатів крос-валідації демонструє, що всі 3 моделі мають достатньо високий показник стандартного відхилення 0.0034 – 0.0041 у порівнянні із моделями для попередніх наборів даних, що свідчить про відносно низьку стабільність між різними розрізами і високу чутливість до змін у даних (Таблиця 2.13).

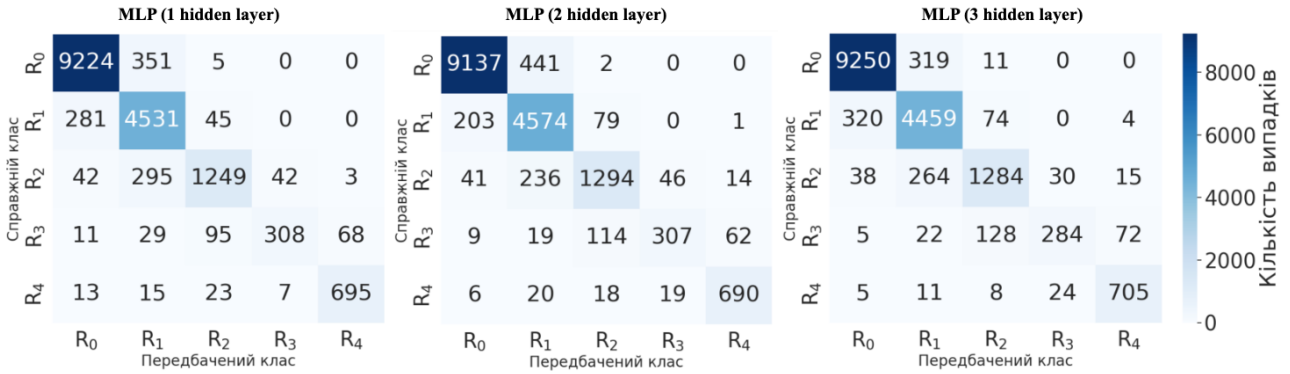


*Рис. 2.20. Матриці невідповідностей для навчання на концентрованому датасеті* $D_{core}$.

Аналіз матриць невідповідностей ще раз підтверджує тенденцію до покращення точності класифікації зі збільшенням кількості прихованих шарів, особливо для переважаючих класів $R_0$ та $R_1$.

Підсумовуючи, можна зробити наступні висновки:

1. **Глибина архітектури моделі позитивно впливає на її продуктивність та стабільність**: Зі збільшенням кількості прихованих шарів зростає точність класифікації, що свідчить про те, що складніші архітектури краще моделюють залежності в складних даних, які відображають процеси розподіленого середовища. Для всіх трьох наборів даних архітектура з 3 прихованими шарами продемонструвала найкращі показники точності передбачення рівня ризику та F1-міри за результатами крос-валідації. Окрім цього, моделі на основі архітектури з трьома прихованими шарами в середньому демонструють чудову стабільність в умовах дисбалансу цільових класів, що робить їх оптимальним вибором у цьому випадку.

2. **Компроміс між складністю та продуктивністю**: Якщо враховувати час навчання та обчислювальні ресурси, модель з двома шарами також є конкурентоспроможним варіантом, забезпечуючи високу точність при нижчій складності. Для сценаріїв, де критичною є стабільність і точність, доцільно обирати модель з трьома шарами. У випадках обмежених ресурсів можна зупинитися на моделі з двома прихованими шарами.

3. **Баланс між ступенем наповненості навчальної вибірки та її розміром**: Аналіз результатів тренування моделей на різних навчальних наборах демонструє

необхідність дотримання балансу між ступенем інформаційної наповненості датасету та його розміром. Прослідковуються наступні тенденції – збільшення якості та міри наповненості вхідних даних позитивно впливають на здатність моделі розпізнавати навіть слабко репрезентовані класи, що добре помітно по представленим матрицям невідповідності для вибірки $D_{core}$. Проте зменшення розмірності вхідного набору навчальних даних дещо погіршує показники F1-score та загальної точності average accuracy за результатами крос-валідації, для всіх трьох архітектур падіння цього показника досягає близько 2% (до 92% в середньому) у порівнянні із початковим набором даних $D_{full}$. Чітко прослідковується тенденція до зниження ефективності моделей при вирішенні задач класифікації зі зменшенням об'єму навчального набору даних, при цьому якість та міра наповненості датасету відіграє другорядну роль. Таким чином, гіпотеза $H_{(2)}$ про те, що ступінь інформаційної наповненості та міра повноти вхідних даних має суттєвий вплив на показник достовірності результатів класифікації рівнів ризику відкидається.

Окрім цього, Таблиця 2.10 демонструє, що дані мають нерівномірний розподіл за цільовою ознакою, а отже присутній ефект дисбалансу за рахунок найкраще представлених класів, що може впливати на якісні характеристики моделей, і підтверджується порівнянням показників специфічності, чутливості та F1-score для кожного класу проєктованих моделей і відповідними матрицями невідповідностей.

Результати емпіричної перевірки доводять, що незалежно від архітектури моделі та якісних характеристик вхідного набору даних зберігається проблема дисбалансу класів. Класи з невеликою кількістю зразків ($R_3$ та $R_4$) мають низьку точність і відтворюваність, що свідчить про те, що модель неефективно навчається на малих класах. Клас $R_0$, який є найбільшим за кількістю представлених екземплярів у всіх датасетах, має домінуючий вплив на метрики точності, оскільки більшість зразків належать до цього класу.

На даному етапі можна запропонувати методичні рекомендації щодо покращення проєктованих моделей:

1. Застосування підходів для усунення дисбалансу класів:

- Oversampling: методи SMOTE, ADASYN або їх комбінації можуть допомогти зменшити вплив дисбалансу і покращити результати для найменш представлених класів;
- Undersampling: зменшення кількості даних для великих класів;
- Використання вагових коефіцієнтів для втрат (weighted loss function);

2. Аналіз важливості класів – використання зважування класів та методу class_weights дозволить моделі зосередитись на важливих, але слабко представлених класах ($R_3$ та $R_4$).

3. Використання для нерепрезентативних класів спеціальних метрик оцінювання – наприклад, середньозважена F1-міра (weighted avg F1-score) або макро F1-міру (macro avg F1-score) як основного критерію оцінки моделі.

4. Тонке налаштування гіперпараметрів – наприклад, зміна порогів прийняття рішень (threshold tuning) для покращення балансу між показниками precision і recall, зменшення темпу навчання (learning rate) або додаткове налаштування регуляризації (наприклад, L2-регуляризація) для запобіганню перенавчанню.

5. Аугментація даних – штучне розширення розміру і різноманітності наявного навчального набору даних для класів з малою кількістю зразків.

Таким чином, використання моделей із складнішою архітектурою виявилось ефективним для домінуючих класів, але вимагає вдосконалення підходу для слабко представлених класів цільової метрики ризику. Залучення технік балансування даних, зважування класів та інженерії ознак є раціональним кроком для покращення загальної продуктивності. Це дозволить створити універсальну модель, яка буде більш ефективною для класифікації найменш представлених, проте критичних з огляду безпеки, класів, що мають вирішальне значення в практичних сценаріях використання.

Для перевірки гіпотези $H_{(1)}$ про можливість подолання проблеми дисбалансу класів і підвищення ефективності вирішення задач класифікації та оцінювання ризику для проєктований моделей проведено застосування вагових коефіцієнтів та технік оверсемплінгу найменш представлених класів на основі методів SMOTE та ADASYN.

Додатково проаналізовано доцільність застосування технік андерсемплінгу для зменшення кількості даних широко представлених класів, проте їх ефективність на практиці виявилась нижчою ніж вищеописані підходи. Окрім цього, такий підхід породжує додаткові ризики зниження якості навчання моделі та її здатності до узагальнення, а також втрати важливої інформації та цінних екземплярів даних, що несуть вагомі характеристики в розрізі модельованого явища.

Перевірку ефективності технік балансування даних проведено на повному наборі даних $D_{full}$, оскільки моделі спроєктовані на його основі демонструють найвищі показники середньої точності за результатами крос-валідації.

*Таблиця 2.14*

*Результати порівняння ефективності технік балансування даних на повному датасеті $D_{full}$ для архітектури з 3 прихованими шарами*

| **Показник** | **MLP (3 hidden layer) SMOTE** | | | **MLP (3 hidden layer) ADASYN** | | | **MLP (3 hidden layer) class_weights** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **support** |
| $R_0$ | 0.98 | 0.94 | 0.96 | 0.67 | 0.40 | 0.50 | 0.98 | 0.95 | 0.97 | 14854 |
| $R_1$ | 0.91 | 0.89 | 0.90 | 0.60 | 0.75 | 0.67 | 0.91 | 0.95 | 0.93 | 12559 |
| $R_2$ | 0.85 | 0.89 | 0.87 | 0.80 | 0.94 | 0.86 | 0.96 | 0.89 | 0.92 | 9409 |
| $R_3$ | 0.86 | 0.93 | 0.89 | 0.94 | 0.91 | 0.92 | 0.91 | 0.95 | 0.93 | 5209 |
| $R_4$ | 0.96 | 0.93 | 0.95 | 0.98 | 1.00 | 0.99 | 0.87 | 0.99 | 0.93 | 1946 |
| **macro avg** | 0.91 | 0.92 | 0.91 | 0.80 | 0.80 | 0.79 | 0.93 | 0.95 | 0.94 | 43977 |
| **weight avg** | 0.92 | 0.91 | 0.92 | 0.96 | 0.96 | 0.96 | 0.94 | 0.94 | 0.94 | 43977 |
| **test accuracy** | 93.05% | | | 91.45% | | | 94.08% | | | |
| **average accuracy** | 0.9402 | | | 0.9169 | | | 0.9397 | | | cross-valid. |
| **standard deviation** | 0.0049 | | | 0.0071 | | | 0.0045 | | | |

За результатами емпіричної перевірки найкращі показники приросту точності класифікації за результатами крос-валідації забезпечила техніка оверсемплінгу на основі методу SMOTE (Таблиця 2.14).

Хоча формально показник точності моделі фактично не змінився та становить 94.02% за результатами крос-валідації (k-fold=5), спроєктована модель отримала здатність краще інтерпретувати слабко представлені, проте важливі в розрізі предметної області класи цільової ознаки ($R_3$ та $R_4$, що відповідно репрезентують значення рівнів ризику «високий» та «критичний»).

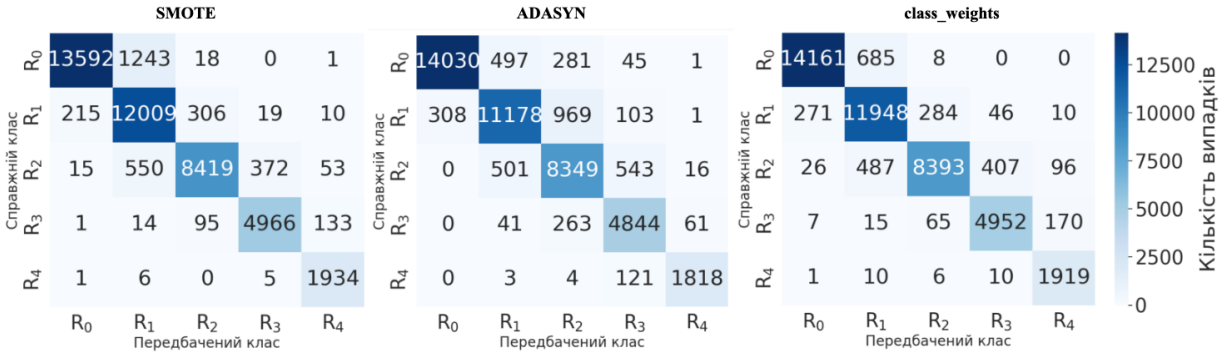


*Рис. 2.21. Матриці невідповідностей для порівняння методів оптимізації SMOTE, ADASYN та class_weights (датасет $D_{full}$).*

Таким чином, за результатами перевірки гіпотези $H_{(1)}$ можна підсумувати, що застосування вагових коефіцієнтів та технік оверсемплінгу на основі методів SMOTE та ADASYN дає можливість подолати проблему дисбалансу класів та оптимізувати ефективність вирішення задачі класифікації.

У якості фінального варіанту для подальшого дослідження обрано модель архітектури з 3 прихованими шарами, що тренувалась на повному наборі даних (датасет $D_{full}$) із застосуванням техніки балансування на основі алгоритму SMOTE. Вона продемонструвала найкращі якісні показники ефективності та середній рівень точності оцінювання ризику на рівні 94% за результатами крос-валідації.

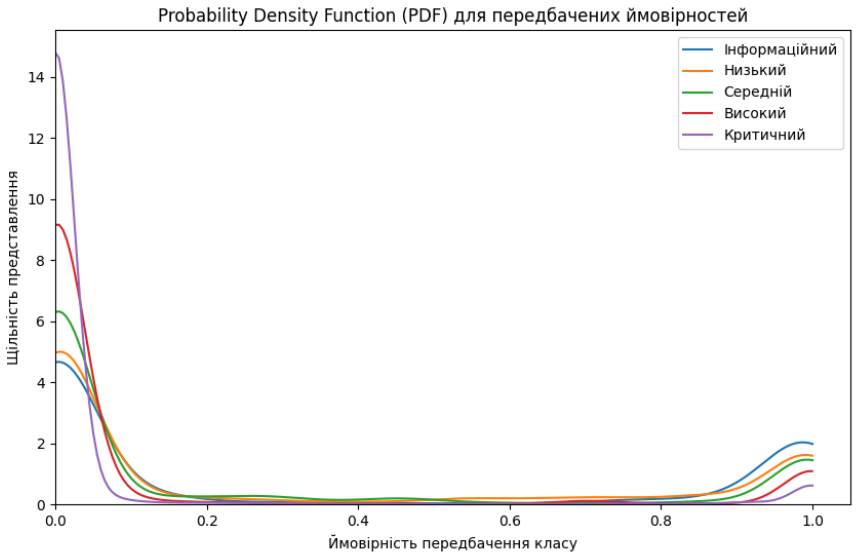


*Рис.2.22 Діаграми щільності ймовірностей (Probability Density Function, PDF) для ймовірностей передбачень рівнів ризику.*

Додатково для фінального варіанту моделі побудовано криві аналізу розподілу ймовірностей (Рисунки 2.22 – 2.23). Ймовірності передбачень зосереджені навколо 0 та 1, що сигналізує про те, що модель надто впевнена в своїх прогнозах.

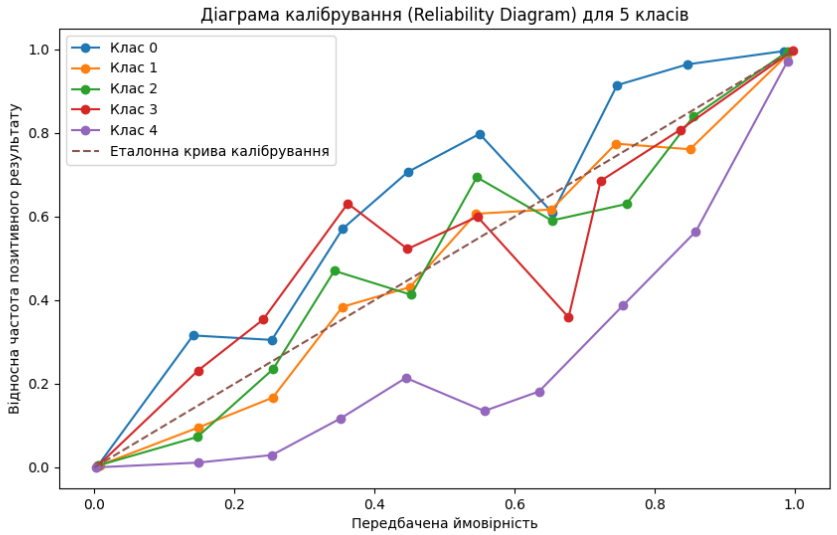


*Рис.2.23 Діаграми калібрування (Reliability Diagram) для класів.*

Підсумовуючи результати аналізу діаграми калібрування можна дійти висновку, що модель завищує ймовірності (занадто впевнена) для класу $R_4$, що відповідно репрезентує значення рівня ризику «критичний», і при цьому дещо занижує ймовірності для класу $R_0$ («інформаційний» рівень ризику).

### 2.3.6. Апробація та оцінка ефективності моделі багатокритеріального аналізу гетерогенних даних розподіленого середовища

З метою обґрунтування методології дослідження та підтвердження ефективності запропонованого рішення проведено навчання додаткової моделі, у якості контрольного зразка для порівняння. Тренування контрольної моделі проводилось на повному наборі даних (датасет $D_{full}$). У якості методу факторного аналізу для зменшення розмірності та вибору релевантних ознак початкового набору даних застосовано метод головних компонент (Principal component analysis, PCA). Такий підхід дозволить оцінити ефективність запропонованого рішення для оптимізації вибору ознак та виділення найсуттєвіших факторів ризику із використанням спроєктованого профілю ключових факторів ризику для сучасних PIC.

Вхідний набір даних розмірності [219884 x 341] після виділення методом головних компонент скорочується до аналізу 40 інформативних параметрів (що демонструє приблизно такий же рівень оптимізації вхідного простору, як і запропоноване рішення на основі профілю ключових факторів ризику, де цей показник становив 42 метрики).

*Таблиця 2.15*

*Результати навчання контрольної моделі на повному датасеті* $D_{full}$

| **Показник** | **MLP (1 hidden layer)** | | | **MLP (2 hidden layer)** | | | **MLP (3 hidden layer)** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **precision** | **recall** | **F1** | **support** |
| $R_0$ | 0.94 | 0.95 | 0.94 | 0.94 | 0.95 | 0.94 | 0.94 | 0.94 | 0.94 | 14912 |
| $R_1$ | 0.82 | 0.92 | 0.87 | 0.83 | 0.92 | 0.87 | 0.83 | 0.92 | 0.87 | 12577 |
| $R_2$ | 0.91 | 0.81 | 0.86 | 0.92 | 0.82 | 0.86 | 0.91 | 0.83 | 0.87 | 9316 |
| $R_3$ | 0.95 | 0.87 | 0.91 | 0.95 | 0.87 | 0.91 | 0.97 | 0.88 | 0.92 | 5202 |
| $R_4$ | 0.93 | 0.84 | 0.88 | 0.89 | 0.87 | 0.88 | 0.92 | 0.85 | 0.89 | 1970 |
| **macro avg** | 0.91 | 0.88 | 0.89 | 0.91 | 0.89 | 0.89 | 0.92 | 0.89 | 0.90 | 43977 |
| **weight avg** | 0.90 | 0.90 | 0.90 | 0.90 | 0.90 | 0.90 | 0.91 | 0.90 | 0.90 | 43977 |
| **test accuracy** | 89.64% | | | 89.93% | | | 90.29% | | | |
| **average accuracy** | 0.8978 | | | 0.8999 | | | 0.8996 | | | cross-valid. |
| **standard deviation** | 0.0018 | | | 0.0023 | | | 0.0017 | | | |

Побудована контрольна модель за результатами крос-валідації демонструє дещо кращі показники ефективності для архітектур з двома та трьома прихованими шарами, причому останній варіант має кращу стабільність та нижчу чутливість до варіативності вхідних параметрів за рахунок найнижчого показника середьоквадратичного відхилення (0.0017), що вказує на кращу узагальнювальну здатність. Проте загальні показники точності класифікації приблизно на 4% нижчі ніж запропоноване рішення на основі побудованого профілю ключових факторів ризику, де цей показник на рівні 94% за результатами крос-валідації (k-fold=5). Окрім цього критерій F1-score також демонструє дещо гіршу динаміку у порівнянні з моделлю із застосуванням техніки балансування на основі алгоритму SMOTE.

Аналіз класової ефективності за основними критеріями оцінки підтверджує кращі якісні характеристики запропонованого рішення у порівнянні з контрольною моделлю на основі методу головних компонент.

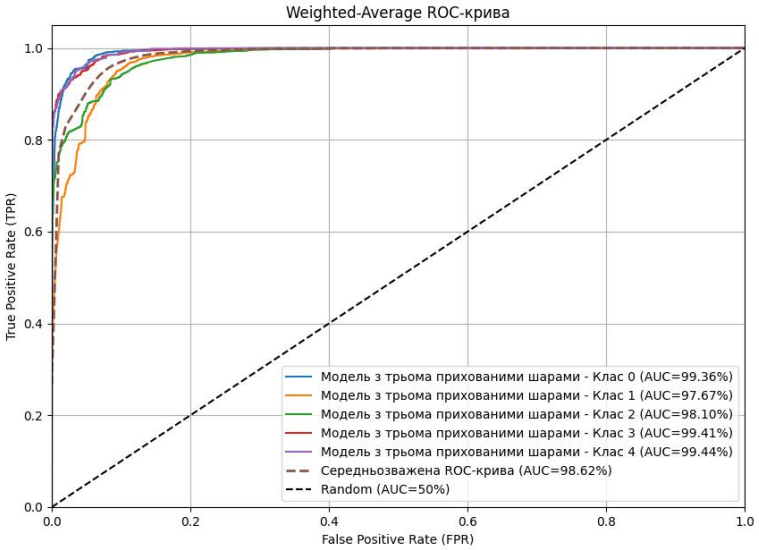


*Рис.2.24 Візуалізація кривої ROC-AUC (MLP+PCA)*

Додатково побудовано ROC-криві для кожного класу ризику за схемою One-vs-Rest та обчислено значення критерію ROC-AUC, що становить 99.46% для обраної конфігурації моделі та 98.62% для контрольного зразка (Рисунки 2.24 – 2.25).

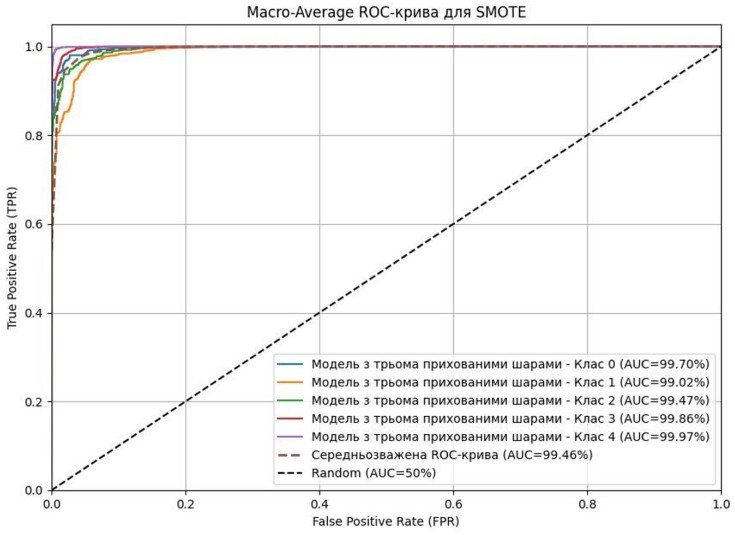


*Рис.2.25 Візуалізація кривої ROC-AUC (MLP+SMOTE)*

Таким чином, третя гіпотеза $H_{(3)}$ про застосування побудованого профілю ключових факторів ризику для оптимізації процесу вибору вхідного вектору ознак проєктованих моделей та покращення якісних характеристики оцінювання у порівнянні з класичним PCA підходом приймається.

## 2.4. Висновки до розділу 2

Другий розділ присвячено проєктуванню та побудові моделей глибинного навчання для вирішення класичної задачі класифікації та навчання з учителем з метою інтерпретації ризиків у розподіленому середовищі на основі багатокритеріального аналізу багатовимірних диференційованих метрик та метаданих про стан інфраструктури РІС. Такий підхід породжує необхідність ідентифікації та попереднього аналізу основних факторів ризику, встановлення їх взаємозв'язків та кореляційних залежностей, що безпосередньо пов'язано з оптимізацією вибору вхідного вектору ознак та ефективним налаштуванням гіперпараметрів нейромережевих моделей з урахуванням виявлених закономірностей.

В результаті проведеного дослідження та формалізації процедур машинного аналізу гетерогенних даних РІС поданих у форматі розподілених метрик та показників було вирішено наступні завдання:

1. **Здійснено вдосконалення методу побудови профілю ключових факторів ризику сучасних розподілених інформаційних систем**, виконано комплексне дослідження основних чинників ризику та проведено кореляційний аналіз та моделювання їх взаємозв'язків, а також **визначено та структуровано основні заходи та контролі інформаційної безпеки**, які демонструють найкращі показники ефективності в умовах розподіленості середовища, враховують як технологічні, так і організаційні аспекти, забезпечуючи системний підхід до управління ризиками, зменшення впливу загроз і підвищення стійкості розподілених систем до можливих атак. Проаналізовано та проведено ранжування 40 факторів ризику для типової РІС, а також 14 груп контролів безпеки відповідно до їх важливості та частоти виникнення на практиці. Запропонований підхід до оптимізації вибору вхідного набору ознак та виділення найсуттєвіших факторів ризику на основі спроєктованого профілю ключових факторів ризику для сучасних РІС продемонстрував тотожний результат по числовому показнику кількості відібраних для аналізу метрик у порівнянні з факторним аналізом за допомогою методу головних компонент (PCA) – 42 метрики у порівнянні із 40 для PCA, але при цьому приблизно **на 4% кращі загальні показники**

**точності класифікації** для проєктованих моделей оцінювання ризику кібербезпеки для РІС.

2. **Розроблено комплекс моделей оцінювання ризиків ІБ в розподілених інформаційних системах на основі інструментарію глибоких нейронних мереж** з кращими показниками зважених середніх значень точності (Average Accuracy), F1-міри (F1-score) та AUC-ROC, проведено порівняння їх ефективності та якісних характеристик при вирішенні задач класифікації, в тому числі в залежності від ступеня інформаційної наповненості та міри повноти вхідних даних, що демонструє здатність запропонованих моделей до масштабування та адаптації під різноманітні топології РІС та динамічні умови розподіленого середовища.

Проведено експериментальні дослідження, апробацію та оцінку ефективності моделей багатокритеріального аналізу гетерогенних даних розподіленого середовища, що довели доцільність та ефективність застосування нейромережевої парадигми для машинного аналізу ключових індикаторів безпеки розподіленого середовища з метою оцінювання ризиків кібербезпеки та продемонстрували достатньо високі показники середньої точності проєктованих моделей **на рівні 94%**.

Окрім цього, виявлено тенденцію до збільшення точності та стабільності моделей зі збільшенням складності архітектури та кількості прихованих шарів – на всіх досліджуваних наборах даних тришарова архітектура проєктованих моделей демонструвала кращі показники продуктивності за основними критеріями оцінки.

3. **Досліджено ефективність ряду підходів з підвищення точності побудованих моделей**, зокрема вирішення проблем якості і повноти вхідних даних, а також усунення дисбалансу цільових класів, із використанням вагових коефіцієнтів і технік оверсемплінгу навчальної вибірки за допомогою методів SMOTE та ADASYN, що покращує стійкість проєктованих моделей і підвищує достовірність результатів класифікації рівнів ризику, забезпечуючи ефективну обробку неструктурованих, значною мірою фрагментованих та частково відсутніх даних. В процесі емпіричної перевірки найкращі показники приросту точності класифікації за результатами крос-валідації забезпечила техніка оверсемплінгу на основі методу SMOTE. Хоча формально показник точності моделі фактично не змінився та залишився на рівні 94%

за результатами крос-валідації (k-fold=5), спроєктована модель, відповідно до результатів матриць невідповідності та ключових критеріїв оцінки для окремих класів, отримала здатність краще інтерпретувати слабко представлені, проте важливі в розрізі предметної області класи цільової ознаки $R_3$ та $R_4$ , що відповідно репрезентують значення рівнів ризику «високий» та «критичний».

4. **Здійснено дослідження ряду гіпотез**, за результатами емпіричної перевірки яких отримано наступні результати:

- Застосування вагових коефіцієнтів та технік оверсемплінгу найменш представлених класів на основі методів SMOTE та ADASYN на вході алгоритму класифікації дає можливість подолати проблему дисбалансу класів та оптимізувати ефективність вирішення задачі оцінювання ризику в розподіленому середовищі $H_{(1)}$ – **гіпотеза приймається**. Емпірично доведено ефективність технік оверсемплінгу, зокрема на основі методу SMOTE, для покращення інтерпретації моделлю слабко представлених класів рівня ризику.
- Ступінь інформаційної наповненості та міра повноти вхідних даних має суттєвий вплив на показник достовірності результатів класифікації рівнів ризику $H_{(2)}$ – **гіпотеза відхиляється**. Встановлено та емпірично доведено, що пріоритетнішу роль має розмір навчальної вибірки. Чітко прослідковується тенденція до зниження ефективності моделей при вирішенні задач класифікації зі зменшенням об’єму навчального набору даних, при цьому якість та міра наповненості датасету відіграє другорядну роль. Для розширеного датасету $D_{ext}$ (45,24% наповненості) з кількістю незаповнених метрик до 23 включно ($M_i \leq 23$) та зниженням розміру датасету з 219884 записів до 173103 – падіння загальної точності моделі з тришаровою архітектурою становило 0.5% із показником точності в 93.89%. Для найбільш концентрованого набору даних $D_{core}$ (54,76% наповненості) з кількістю незаповнених метрик до 19 включно ($M_i \leq 19$) та зниженням розміру датасету з 219884 записів до 86660 – падіння середньої точності моделі з тришаровою

архітектурою становило 2.02% із загальним показником в 92.37% за результатами крос-валідації.

- Застосування побудованого профілю ключових факторів ризику дозволяє оптимізувати процес вибору вхідного вектору ознак проєктованих моделей та покращити якісні характеристики оцінки у порівнянні з класичним PCA підходом $H_{(3)}$ – **гіпотеза приймається**. Запропоноване рішення дозволило підвищити точність проєктованих моделей в середньому на 4% у порівнянні з контрольною моделлю, що використовувала метод головних компонент (PCA) у якості підходу до факторного аналізу.

# РОЗДІЛ 3. МОДЕЛІ ОЦІНЮВАННЯ РИЗИКУ В РІС НА ОСНОВІ КОНТРОЛЮ ВІДПОВІДНОСТІ ВИМОГАМ СТАНДАРТІВ ІБ

В останньому розділі дисертаційного дослідження представлено підхід до оцінювання ризиків кібербезпеки, який синтезує кращі практики провідних міжнародних і національних стандартів інформаційної безпеки з інструментарієм інтелектуального аналізу даних. Такий підхід передбачає формалізацію контрольних заходів та вимог стандартів ІБ, та їх подальшу інтеграцію у моделі класифікації рівня ризику, засновані на методах глибинного навчання та класичних алгоритмах машинного навчання. Застосування стандарт-орієнтованого підходу є науково та практично обґрунтованим, оскільки стандарти ІБ відображають накопичений досвід у даній сфері, встановлюють зрілі контрольні механізми та узгоджені принципи безпеки, перевірені на практиці. Орієнтація на відповідність стандартам ІБ у процесі оцінювання ризиків забезпечує систематичність, прозорість та доказову основу для ухвалення управлінських рішень, так як ступінь впровадження контрольних заходів безпосередньо впливає на інтерпретацію рівня ризику та його можливу мінімізацію.

Подальша робота в рамках даного розділу має включати наступні завдання:

- Дослідження провідних стандартів ІБ та ідентифікація ключових технологічних контролів, орієнтованих на захист інформаційних активів;
- Формалізація контрольних заходів і вимог стандартів для їх представлення у вигляді вхідного вектору нейромережевих моделей;
- Аналіз теоретико-методологічних принципів застосування алгоритмів інтелектуального аналізу даних для вирішення задач підвищення ефективності процесу ризик-менеджменту в РІС та оптимізації прийняття управлінських рішень на основі контролю відповідності вимогам стандартів кібербезпеки;
- Розробка, порівняння та аналіз ефективності моделей оцінювання ризику в розподілених інформаційних системах на основі алгоритмів машинного навчання та глибоких нейронних мереж;
- Побудова адаптивного методологічного підходу до оцінювання ризиків, що враховуватиме як метрико-орієнтований, так і стандарт-орієнтований аспекти аналізу, інтегруючи переваги обох методів у єдиному аналітичному середовищі, та

забезпечуватиме комплексний обрахунок кількісного показника рівня ризику із урахуванням специфіки динамічного середовища РІС.

## 3.1. Обґрунтування концептуальних складових підходу до оцінювання ризиків на основі відповідності вимогам стандартів ІБ

Одним із ключових аспектів забезпечення сталого рівня кібербезпеки є відповідність вимогам провідних стандартів ІБ, що виконують роль еталонних орієнтирів під час формування й удосконалення політик, процесів та контролів безпеки. Дотримання вимог стандартів важливо не лише з точки зору проходження аудитів ІБ чи формальної сертифікації, але й для постійного моніторингу і відслідковування безпекової ситуації, підтримки безперервної ситуаційної обізнаності, своєчасного виявлення проблем в підходах до захисту та запобігання потенційним інцидентам в режимі реального часу.

### 3.1.1. Роль стандартів у формуванні політик інформаційної безпеки

Розвиток міжнародних стандартів та національних нормативно-правових актів у галузі ІБ є результатом колективного досвіду та знань фахівців з різних галузей, ІТ-компаній, наукових установ і державних організацій. Ці стандарти встановлюють систематизовані та формалізовані вимоги, рекомендації та найкращі практики для забезпечення належного рівня захищеності інформаційних активів та процесів. Значущість стандартів полягає у:

- **Розробці сталого каркасу політик безпеки**: Стандарти слугують джерелом еталонних вимог та контролів, які допомагають організаціям формувати політики й процедури інформаційної безпеки, що охоплюють широкий спектр загроз та вразливостей.
- **Міжнародній визнаності та сумісності**: Відповідність міжнародним стандартам дозволяє організаціям гармонізувати власні політики ІБ із загальноприйнятими світовими практиками, що сприяє сумісності процесів, підвищує довіру з боку клієнтів, партнерів та регуляторів.

- **Системності та повторюваності процесів**: Впровадження стандартів сприяє структуруванню процесу управління безпекою, забезпечує безперервний моніторинг та поліпшення, а також впроваджує циклічні процедури аналізу, оцінки, реагування та контролю ІБ.

Контролі, визначені стандартами, виступають практичними інструментами для зниження ризиків реалізації загроз. Відповідність стандартам передбачає не лише формальний критерій безпеки, а й формує культуру безпеки та підвищує загальну зрілість процесів ІБ в організації. Дотримання контролів має такі позитивні наслідки:

- **Мінімізація вразливостей**: Реалізація рекомендацій стандартів допомагає виявляти та своєчасно усувати слабкі місця у програмних комплексах, мережевій інфраструктурі, налаштуваннях систем та організаційних процедурах.
- **Зниження ймовірності інцидентів**: Ефективно впроваджені контролі зменшують ймовірність успішної реалізації атак, несанкціонованого доступу, витоків даних та інших небажаних подій.
- **Підвищення готовності до аудитів та оцінок**: Регулярні внутрішні та зовнішні аудити ІБ, не лише перевіряють відповідність вимогам стандартів, а й стимулюють безперервне вдосконалення системи ІБ. Аудити дозволяють виявляти прогалини, оцінювати ефективність впроваджених контролів і визначати напрями оптимізації.

Оцінювання ризиків на основі стандартизованих контролів дозволяє поєднати аналітичну складову ймовірнісної оцінки загроз з нормативною (вимоги до безпеки, що підкріплені світовою практикою). Це забезпечує більш зважений та обґрунтований підхід до прийняття управлінських рішень щодо розподілу ресурсів, впровадження додаткових заходів безпеки чи оптимізації конфігурацій засобів захисту та моніторингу.

### 3.1.2. Зв’язок між вимогами стандартів та рівнем ризику

Рівень ризику інформаційної безпеки у розподілених інформаційних системах визначається широким переліком факторів, що детально досліджувались в попередньому розділі дисертаційної роботи. Вимоги та контролі, передбачені

міжнародними й національними стандартами інформаційної безпеки (наприклад, ISO/IEC 27001, NIST SP 800-30, PCI-DSS тощо), виступають систематизованим набором рекомендацій для запобігання або зменшення впливу кіберзагроз. Тобто стандарти, будучи узагальненням кращих світових практик ІБ, безпосередньо впливають на імовірнісний та наслідковий компоненти ризику.

**Теоретичне підґрунтя впливу відповідності стандартам на рівень ризику.** Стандартизовані вимоги ІБ мають на меті мінімізацію можливості реалізації загроз та зниження масштабів потенційної шкоди. Застосування відповідних контролів, запропонованих стандартами, призводить до зменшення розмірності наявних векторів реалізації атак та підвищення рівня детектування інцидентів. Теоретично, кожен впроваджений контроль зменшує загальний простір вразливостей і перешкоджає прогресії загроз від «точки входу» до критичних вузлів системи. Таким чином, покращуючи стан ІБ завдяки дотриманню вимог, організація знижує ймовірність успішної атаки та / або обмежує масштаб потенційних збитків.

**Формалізація зв'язку між відповідністю стандартам та рівнем ризику.** Ризик ($R$) у сфері ІБ часто розглядається як функція від сукупностей ймовірностей реалізацій загроз та впливів від їх реалізації, що може бути представлено у вигляді 3.1:

$$R = f(P, I), \tag{3.1}$$

де $P = \{p_0, p_1 \dots p_n\}$ – сукупність ймовірностей реалізацій загроз;

$I = \{i_0, i_1 \dots i_n\}$ – сукупність відповідних впливів.

Припустимо, що рівень впроваджених контролів відповідності стандартам можна оцінити сукупністю індикаторів відповідності ($c_n$), тоді загальна відповідність стандартам може бути представлена як $C = \{c_0, c_1 \dots c_n\}$, $c_n \epsilon [0,1]$, де 0 відповідає повній відсутності контролю, а 1 – повній відповідності вимозі стандарту. За умови, що підвищення рівня відповідності стандартам зменшує кількість уразливостей та посилює захист системи, можна стверджувати:

- Зі збільшенням $C$ знижується ймовірність $P$ успішної реалізації певних сценаріїв загроз (наприклад, через вимоги щодо шифрування, контроль доступу, сегментацію мережі тощо).

- Зі збільшенням $C$ знижується можливий вплив $I$, оскільки організація краще підготовлена до реагування на інциденти, обмежує поширення атаки, захищає критичні дані та забезпечує безперервність сервісів.

Формально можна розглядати $P$ і $I$ як функції, що монотонно спадно залежать від $C$:

$$P = P(C), \tag{3.2}$$

$$I = I(C), \tag{3.3}$$

При чому $\frac{dP}{dC} < 0$ та $\frac{dI}{dC} < 0$, тобто зі збільшенням $C$ ймовірність реалізації загроз та потенційний негативний вплив зменшуються.

Отже, для певних сценаріїв кіберзагроз можна оцінити ризик як функцію залежності від відповідності стандартам:

$$R(C) = f(P(C), I(C)), \tag{3.4}$$

де $P(C)$ та $I(C)$ відповідають розглянутим законномірностям.

Таким чином, оскільки $P(C)$ та $I(C)$ зменшуються зі зростанням загального значення $C$, то й ризик $R$ також зменшується, що відображає формальну залежність: **більша відповідність вимогам стандартів → нижчий рівень ризику**.

### 3.1.3. Аналіз провідних стандартів та відбір ключових асет-орієнтовних контролів

У сучасних корпоративних розподілених інформаційних системах стандарти інформаційної безпеки виступають фундаментальною основою для побудови системного підходу до забезпечення захищеності інформаційних активів. Стандарти визначають загальні вимоги та підходи до забезпечення безпеки, що дозволяє знижувати ризики, пов’язані з інформаційними загрозами. Однак, зважаючи на складність РІС, реалізація всіх контролів, передбачених стандартами, часто є складною, недоцільною або ж неефективною.

У даному параграфі проведено аналітичний огляд провідних стандартів ІБ та здійснено відбір ключових технологічних асет-орієнтовних вимог, контроль виконання яких є релевантним для мережевих активів РІС, що досліджуються в рамках дисертаційного моделювання.

Ключовими стандартами, що формують основу сучасних підходів до ІБ, є:

1. **ISO/IEC 27001:2022 (Information security, cybersecurity and privacy protection – Information security management systems – Requirements)**: Сертифікаційний стандарт, який визначає вимоги до систем управління інформаційною безпекою (СУІБ), включаючи визначення контексту організації, оцінювання ризиків, впровадження контролів безпеки, моніторинг та безперервне вдосконалення. Каталог контролів безпеки (Annex A) охоплює вимоги до захисту інформації, управління активами, мережевої безпеки, моніторингу подій та реагування на інциденти.

2. **ISO/IEC 27002:2022 (Information security, cybersecurity and privacy protection – Information security controls)**: Стандарт є доповненням до ISO/IEC 27001, містить розширене тлумачення контролів з деталізованим описом механізмів реалізації та надає глибоку методологічну підтримку для їх впровадження на практиці. ISO 27001 та ISO 27002 є парними стандартами, що доповнюють один одного, так як додаток Annex A першого посилається на ISO/IEC 27002. У 2022 році обидва стандарти були оновлені, щоб синхронізувати структуру контролів – наразі вони ідентичні за назвою, номером і змістом, а їх кількість зменшено зі 114 до 93, та перегруповано у 4 розділи замість попередніх 14 доменів.

3. **PCI DSS v4 (Payment Card Industry Data Security Standard)**: PCI DSS розроблений для захисту платіжних систем і містить широкий перелік контролів, що охоплюють технічні, організаційні й процедурні заходи для захисту даних держателів платіжних карт. Контролі PCI DSS – суворо структуровані технічні вимоги для захисту даних платіжних карт, які повинні виконуватися без винятку або з формалізованими компенсуючими заходами. Вони не гнучкі, як у ISO 27001, і значно жорсткіші щодо технічної реалізації.

4. **SWIFT (Society for Worldwide Interbank Financial Telecommunication)**: SWIFT забезпечує стандарти безпеки для глобальної мережі фінансових транзакцій, орієнтуючись на захист від кіберзагроз та забезпечення цілісності операцій. Основним документом для безпеки є **SWIFT Customer Security Programme (CSP)**, що визначає обов’язкові та рекомендовані контролі для фінансових організацій.

5. **NBU-95 (Національний банк України – Постанова №95)**: Постанова №95 регламентує вимоги до забезпечення кіберзахисту інформаційних систем суб'єктів платіжного ринку України. Вона враховує міжнародні стандарти, такі як ISO/IEC 27001, та адаптує їх до специфіки національного фінансового сектору.

Загальний підхід до відбору контролів заснований на **принципі релевантності**, тобто врахування лише тих вимог, виконання яких є критично важливим для забезпечення безпеки інформаційних активів РІС у межах даного дослідження. Основні критерії відбору:

- Прямий вплив на рівень ризику активу.
- Можливість автоматизованого збору даних для контролю.
- Актуальність для оцінки стану мережевих активів (серверів, комутаторів, маршрутизаторів, робочих станцій тощо).

Таблиця 3.1 демонструє перелік відібраних контролів для основних стандартів ІБ.

*Таблиця 3.1*

*Перелік відібраних контролів для основних стандартів ІБ*

| Стандарт | Контролі організаційного характеру (Organizational controls) | Контролі пов'язані з людським чинником (People controls) | Фізичні контролі (Physical controls) | Технологічні контролі (Technological controls) | Сумарна кількість | Асет-орієнтовні контролі |
|---|---|---|---|---|---|---|
| **ISO 27001 / ISO 27002** | 37 | 8 | 14 | 34 | **93** | **11** |
| **PCI DSS v4** | 118 | 21 | 19 | 92 | **250** | **21** |
| **SWIFT** | 4 | 4 | 3 | 21 | **32** | **12** |
| **NBU-95** | 36 | 24 | 11 | 67 | **138** | **16** |

Для подальшого дослідження та моделювання процесу оцінки ризику в РІС для кожного стандарту відібрано наступні основні категорії асет-орієнтовних контролів:

- Інвентаризація активів, визначення їх критичності та статусу.
- Контроль та розмежування доступу.
- Мережева безпека.
- Моніторинг стану антивірусного захисту.

- Сканування на вразливості та управління виправленнями.
- Логування та журналювання подій, наявність процедур резервного копіювання.
- Виявлення інцидентів та моніторинг подій.

### 3.2. Методологічні аспекти застосування інструментарію машинного навчання в задачах оцінювання ризиків РІС на основі контролю відповідності стандартам ІБ

В умовах постійного зростання складності загроз та обсягів оброблюваних даних традиційні методи оцінювання ризиків, засновані на ручному аналізі, експертних оцінках або статичних моделях, втрачають свою ефективність. У зв'язку з цим, методи штучного інтелекту (ШІ) та машинного навчання (МН) стають перспективними інструментами для автоматизації, масштабування та підвищення точності процесів оцінювання ризиків ІБ. Як вже зазначалося в попередніх розділах дослідження, методи ШІ та МН пропонують низку переваг у порівнянні з традиційними підходами, до яких слід віднести здатність:

- Ефективно аналізувати значні обсяги даних, ідентифікувати складні залежності та приховані патерни;
- Підвищувати точність прогнозів завдяки адаптації моделей до нових даних;
- Працювати в режимі реального часу, що є критичним для виявлення та реагування на атаки;
- Прогнозувати майбутні загрози, що є важливим аспектом у динамічному середовищі сучасних РІС;

Однією з основних переваг застосування ШІ та МН є здатність до автоматизації процесів оцінювання ризиків, що значно знижує витрати часу та ресурсів, необхідних для їх виконання. Реалізація такого підходу дозволяє постійно моніторити інформаційні системи, забезпечуючи безперервний аналіз та оновлення оцінок ризиків у режимі реального часу. Крім того, ШІ та МН надають можливість підвищити точність оцінювання за рахунок зменшення людських помилок та суб'єктивності,

характерних для традиційних методів. Іншою суттєвою перевагою є здатність до адаптації та самонавчання. Алгоритми МН можуть вдосконалювати моделі на основі нових даних, що дозволяє системам оцінювання ризиків залишатися актуальними в умовах швидкоплинних змін і особливо важливо у контексті постійного розвитку методів кібератак та появи нових вразливостей.

Таким чином, методи штучного інтелекту та машинного навчання мають значний потенціал для покращення процесів оцінювання ризиків інформаційної безпеки. Вони пропонують можливості автоматизації, підвищення точності та адаптивності, що є важливим для ефективного управління ризиками в сучасних організаціях.

### 3.2.1. Критерії вибору алгоритмів для оцінювання ризиків розподіленого середовища

Штучний інтелект (AI) – це не нова концепція, але тільки в останні роки різноманітні компанії почали вивчати і розуміти її повний потенціал. Інтелектуальні системи відіграють все більш важливу роль в галузі аналізу даних та обчислень, що дозволяє застосункам діяти дедалі більш інтелектуально. Існує усталена класифікація алгоритмів навчання на чотири основні типи:

**Навчання з учителем або ж кероване навчання (supervised learning)**: Цей підхід полягає у формуванні відображення між вхідними та вихідними даними на основі пар «вхід-вихід», наданих під час етапу тренування. Модель, що використовує навчання під наглядом, отримує мітки для навчальних прикладів і, використовуючи їх, будує функцію, здатну коректно прогнозувати вихідний результат для нових вхідних даних. Таким чином, парадигма навчання з учителем полягає у створенні математичної моделі, що здатна прогнозувати вихідний результат (мітку або значення) на основі вхідних даних, використовуючи знання, отримані під час тренування. До типових задач, які вирішуються в рамках навчання з учителем, належать класифікація, у якій дані розподіляються за визначеними категоріями, та регресія, яка передбачає побудову функціональної залежності.

Класифікація є завданням визначення категорії (або класу), до якої належить об’єкт, представлений у вигляді набору характеристик (вектору ознак). У цьому контексті алгоритм моделює функцію, яка зіставляє кожному набору вхідних ознак дискретну мітку класу. Процес навчання включає мінімізацію помилок у передбаченнях класів шляхом аналізу шаблонів у навчальних даних.

Класифікація використовується, коли результат є дискретним, і її основними цілями є:

- Оптимізація коректного віднесення кожного об’єкта до відповідного класу.
- Мінімізація помилок хибнопозитивних і хибнонегативних рішень.
- Підвищення здатності моделі узагальнювати нові дані, що не зустрічались раніше.

Методи, які застосовуються для класифікації, включають як лінійні підходи (наприклад, логістична регресія), так і нелінійні (наприклад, дерева рішень, нейронні мережі). Основною проблемою у задачах класифікації є забезпечення балансу між високою точністю моделі на навчальних даних і здатністю моделі до узагальнення.

Регресія є завданням прогнозування безперервного числового значення на основі набору вхідних ознак. У цьому випадку модель навчається відображати залежність між незалежними змінними (вхідними даними) та залежною змінною (вихідним значенням), використовуючи методи мінімізації помилки передбачення.

Цілі задач регресії включають:

- Оцінку числових значень вихідної змінної на основі змін у вхідних параметрах.
- Визначення трендів і залежностей, які існують у навчальних даних.
- Узагальнення цих залежностей для точного передбачення на нових даних.

Регресія використовується, коли результат є безперервним числовим показником. Застосовуються різні підходи, починаючи від простих лінійних моделей до складних ансамблевих методів і глибоких нейронних мереж. Основною складністю задач регресії є адекватне моделювання залежностей у даних, враховуючи можливі нелінійності, взаємозв’язки між ознаками та присутність шуму.

Навчання з учителем є основою багатьох прикладних задач машинного навчання, а його ефективність визначається якістю навчальних даних, вибором алгоритму, налаштуванням параметрів моделі та врахуванням особливостей конкретного завдання.

**Навчання без учителя, неконтрольоване навчання або ж навчання без нагляду (unsupervised learning)**: Цей підхід ґрунтується на аналізі немаркованих даних, з метою виявлення прихованих закономірностей чи структури без необхідності людського втручання, тобто являє собою процес, керований даними. Неконтрольоване навчання широко використовується для виділення значущих ознак та тенденцій, групування результатів, а також виявлення закономірностей у даних, що дозволяє отримати нові знання або створити нові представлення інформації. Типові задачі навчання без учителя охоплюють кластеризацію, зменшення розмірності та виявлення аномалій.

Кластеризація є завданням групування об’єктів у кластери таким чином, щоб об’єкти в одному кластері були більш схожими між собою, ніж з об’єктами в інших кластерах. Цей процес дозволяє структурувати великі набори даних, виявляючи природні групи або сегменти.

Цілі задач кластеризації включають:

- Виявлення прихованих структур у даних.
- Групування об’єктів за спільними ознаками або характеристиками.
- Оптимізація представлення складних даних шляхом зменшення кількості груп.

Популярними методами кластеризації є алгоритми K-середніх, ієрархічна кластеризація, DBSCAN та алгоритми на основі глибинного навчання. Основною складністю в задачах кластеризації є визначення оптимальної кількості кластерів та вибір метрики, яка найкраще описує схожість між об’єктами.

Задача зменшення розмірності полягає у скороченні кількості ознак у даних при збереженні максимальної кількості інформації. Цей процес дозволяє спростити аналіз даних та підвищити ефективність роботи моделей машинного навчання.

Цілі зменшення розмірності включають:

- Виявлення прихованих змінних, які найкраще пояснюють варіативність у даних.
- Підготовка даних для візуалізації у зниженому вимірі (наприклад, у двовимірному або тривимірному просторі).
- Оптимізація обчислювальної складності для моделей, що працюють з великими обсягами даних.

Головною проблемою в задачах зменшення розмірності є вибір адекватної кількості збережених компонентів та забезпечення інтерпретованості нових представлень даних.

Виявлення аномалій є завданням ідентифікації об’єктів, які суттєво відрізняються від більшості представлених зразків. Аномалії можуть свідчити про різні події, такі як несправності, шахрайські дії або загрози ІБ.

Основні цілі включають:

- Виявлення відхилень у даних, які можуть мати критичне значення.
- Попередження про події або стан систем, що потребують уваги.
- Покращення якості даних шляхом ідентифікації та видалення шумів.

Основними викликами є високий рівень різноманітності аномалій та обмеженість даних для навчання моделей.

Таким чином, парадигма навчання без учителя забезпечує потужний інструментарій для роботи з немаркованими наборами даних. Його ефективність залежить від розуміння природи аналізованих даних та коректного налаштування моделей і їх параметрів.

**Напівкероване навчання (semi-supervised learning)**: Цей підхід поєднує характеристики попередніх двох, оперуючи одночасно маркованими та немаркованими даними. Він використовується у випадках, коли доступний великий обсяг немаркованих даних, але лише невелика частина має мітки. Типові задачі напівкерованого навчання охоплюють класифікацію, кластеризацію та прогнозування.

Особливо корисною перевагою такого гібридного підходу є покращення властивостей прогнозування в умовах обмежених даних, коли маркованих прикладів

недостатньо для повноцінного навчання. Немарковані дані використовуються для розширення інформації, яку може врахувати модель.

Цілі задач прогнозування:

- Створення моделі, здатної точно передбачати результати, використовуючи мінімальний обсяг маркованих даних.
- Підвищення стабільності та точності прогнозів за рахунок виявлення закономірностей у немаркованих даних.
- Зниження витрат на отримання маркованих даних при збереженні високої продуктивності моделі.

Напівкероване навчання має значні переваги при роботі з великими масивами даних, коли аналітичний аналіз та отримання міток є витратним. Методи напівкерованого навчання демонструють свою ефективність у багатьох прикладних задачах, зокрема у завданнях машинного перекладу, виявленні шахрайства (fraud detection), маркуванні даних або текстовій класифікації.

**Навчання з підкріпленням (reinforcement learning)**: Навчання з підкріпленням є підходом, у якому агент навчається взаємодіяти з середовищем, отримуючи підкріплення (винагороду або покарання) за свої дії, тобто підхід, керований середовищем. Основною метою такого підходу є знаходження оптимальної стратегії, яка максимізує кумулятивну винагороду. Цей підхід ефективно використовується у динамічних середовищах, де рішення агента впливають на майбутні стани. Типові задачі навчання з підкріпленням охоплюють оптимізацію стратегій, ігрове моделювання керування складними системами та прийняття рішень у реальному часі. Навчання з підкріпленням є потужним інструментом для вирішення задач, де потрібна адаптація, оптимізація та ефективне прийняття рішень у динамічних і невизначених середовищах. Такий підхід може допомогти підвищити автоматизацію або оптимізувати операційну ефективність складних систем.

Результативність рішень на основі машинного навчання залежить від природи, властивостей та якості вхідних даних, а також продуктивності обраних алгоритмів. Вибір підходу, що найкраще відповідає конкретній прикладній галузі та завданню, є надзвичайно складним і залежить від ряду факторів, що визначають специфіку

проблеми, доступні дані, вимоги до точності та продуктивності моделей, тому важливо досконало розуміти принципи роботи різних алгоритмів МН і сферу їх застосування [112].

Ключовою передумовою успішної побудови моделей машинного навчання є наявність якісних наборів даних. В залежності від впорядкованості структури, формату представлення та складності обробки програмними засобами такі дані можуть бути структурованими, напівструктурованими, неструктурованими, або ж мати форму метаданих («дані про дані»). Врахування цих аспектів є вирішальним для коректного вибору інструментарію і побудови ефективних систем інтелектуальної аналітики даних.

У контексті оцінювання ризиків кібербезпеки РІС, в рамках поточного дослідження йдеться про класичну задачу класифікації та навчання з учителем. При цьому вибір алгоритмів машинного навчання для аналізу відповідності вимогам стандартів ІБ повинен ґрунтуватись на низці науково-обґрунтованих критеріїв, що постають із необхідності врахувати характеристики вхідних даних, а також вимоги до точності й інтерпретованості результатів.

На відміну від метрико-орієнтованого підходу, описаного в попередньому розділі, що характеризується великою кількістю вхідних параметрів та складною структурою і форматом представлення гетерогенних даних РІС, стандарт-орієнтований підхід до оцінювання ризиків кібербезпеки передбачає дещо простіші вимоги, що пов’язано з достатньо простою варіативністю значень вхідних контролів, які можна інтерпретувати 3 станами – «контроль виконується», «контроль не виконується» або ж «дані відсутні». Однак доцільно розглянути загальні критерії вибору алгоритмів МН для оцінювання ризиків розподіленого середовища, що будуть актуальними для обох підходів:

- **Ефективний аналіз великих обсягів гетерогенних даних**: РІС генерують значні масиви різнорідних даних, що надходять із численних джерел: систем моніторингу, мережевих сенсорів, систем виявлення вторгнень, журналів безпеки, а також автоматизованих систем контролю показників відповідності вимогам стандартів ІБ. Обраний алгоритм повинен бути стійким до високої розмірності

вхідного простору та здатним ефективно інтегрувати дані різної природи без втрати продуктивності.

- **Адаптивність та стійкість до перенавчання**: З огляду на динамічний характер загроз у РІС, обраний інструментарій повинен забезпечувати високу узагальнювальну здатність та стійкість до перенавчання, а також мати здатність до адаптації, тобто навчатися на нових даних у реальному часі або з мінімальним оновленням моделі.
- **Інтерпретованість результатів та прозорість ухвалених рішень**: Задача оцінювання ризику кібербезпеки для РІС має не лише формальний, але й управлінський аспект: отриманий показник ризику буде використовуватися для прийняття управлінських рішень, оптимізації ресурсів та впровадження заходів забезпечення безпеки. Отже, важливо, щоб обраний алгоритм забезпечував певний рівень інтерпретованості результатів, зокрема можливість визначення найбільш впливових ознак. Це може бути реалізовано або шляхом вибору моделей з відносно прозорою структурою (наприклад, дерева рішень), або шляхом застосування методів інтерпретованості (LIME, SHAP) у разі використання більш складних моделей і нейронних мереж. Інтерпретованість особливо актуальна для другої підзадачі – оцінювання ризиків на основі відповідності стандартам, оскільки зацікавлені сторони (аудитори, менеджери ІБ) вимагатимуть аргументованих пояснень щодо ухвалених рішень.
- **Стійкість до шуму та аномалій у даних**: Дані, що описують стан активів та їх відповідність стандартам, можуть містити помилкові або суперечливі значення, зумовлені збоєм в обладнанні, людським фактором чи неточним збором метрик. Алгоритм повинен бути стійким до аномалій, здатним виявляти та ігнорувати некоректні дані без суттєвого погіршення якості класифікації. Для цього корисним є використання методів виявлення викидів або застосування алгоритмів, невразливих до шуму (наприклад, ансамблеві методи).
- **Оптимізація обчислювальної складності та можливість масштабування**: У міру зростання системи та обсягів даних модель повинна забезпечувати відповідну масштабованість без значного зниження продуктивності.

Враховуючи, що РІС можуть бути розподіленими на рівні великих корпоративних чи інфраструктурних середовищ, алгоритми повинні бути здатними масштабуватися та ефективно використовувати розподілені обчислювальні ресурси (хмарну інфраструктуру, кластери тощо). Перевагу слід надавати методам, що підтримують паралельну обробку даних або можуть бути розподіленими.

- **Інтеграція метрик різного формату та робота в умовах обмежених даних**: В залежності від джерела походження дані РІС можуть мати складну структуру представлення, що потребує алгоритмів, здатних працювати з різними форматами – кількісні, категоріальні, часові метрики тощо. З іншого боку, оцінювання ризиків часто засноване на даних, що мають обмежений або неповний характер. Обраний інструментарій повинен підтримувати роботу із заповненням прогалин або обробкою нечітких даних.
- **Часові обмеження**: Для завдань оцінювання ризиків у реальному часі алгоритми повинні забезпечувати швидку обробку даних та представлення результатів в терміни близькі до реальних.

До інших чинників, які слід враховувати при виборі інструментарію нейромережевого моделювання, належать якісні характеристики даних з якими повинна працювати модель – їх природу та формат представлення, надмірність та обсяг надлишкової інформації, кореляцію ознак та наявність складних прихованих залежностей (ідеальним сценарієм можна вважати ситуацію, коли кожна з ознак робить незалежний внесок в обрахунок виходу моделі). Ефективність алгоритмів машинного навчання варіюється в залежності від характеристик та особливостей вхідних даних, які найкраще відповідають вимогам конкретного алгоритму.

Отже, критерії вибору алгоритмів машинного навчання для задач класифікації ризиків кібербезпеки в РІС повинні враховувати здатність обраного інструментарію до узагальнення та оперативної обробки великих масивів гетерогенних даних, адаптивність, масштабованість, інтерпретованість результатів та стійкість до шуму. Дотримання цих вимог дозволить сформувати обґрунтований підхід до побудови ефективних моделей оцінювання кіберризиків.

### 3.2.2. SWOT-аналіз основних підходів до моделювання на основі алгоритмів машинного навчання

На основі описаних вимог та критеріїв доцільним є проведення детальнішого аналізу можливості застосування розглянутих алгоритмів машинного навчання до завдань класифікації в контексті оцінювання ризиків кібербезпеки сучасних РІС. В даному параграфі проведено аналіз популярних методів, які широко використовуються в різних сферах застосування. Розглянуті методи різняться за своєю теоретичною базою, вимогами до вхідних даних, здатністю інтерпретувати результати та адаптивністю до складних за структурою та гетерогенних за природою даних РІС.

**Логістична регресія (Logistic Regression)** є класичним і добре вивченим підходом, заснованим на статистичній теорії. Вона дає змогу моделювати ймовірність належності об’єкта до конкретного класу, маючи високий рівень інтерпретованості через вагові коефіцієнти [112]. Це робить логістичну регресію привабливою для використання у випадках, де необхідне чітке пояснення прийнятого рішення (наприклад, при аудиті ІБ). Однак логістична регресія є лінійною моделлю, а відтак ускладнюється її ефективне застосування при складних нелінійних взаємодіях між ознаками, характерних для багатовимірних гетерогенних даних у РІС. Припущення про лінійність між залежними та незалежними змінними вважається основним недоліком логістичної регресії. Її варто застосовувати в умовах, коли набір ознак попередньо ретельно відібрано, нормалізовано і змодельовано, а також коли пріоритетом є інтерпретованість та прозорість алгоритму. Класичною формулою логістичної регресії є формула 3.5

$$g(z) = \frac{1}{1+e^{-z}}, \tag{3.5}$$

Для багатокласової класифікації використовується мультикласова логістична регресія також відома як функція softmax:

$$\sigma(z)_i = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_k}}, \tag{3.6}$$

де $z_i$ – елемент вхідного вектора;

$k$ – загальна кількість класів об’єкту.

**Метод опорних векторів (Support Vector Machine, SVM)** забезпечує побудову гіперплощини, що максимізує відстань між класами, і за умови належного вибору математичних функцій, відомих як ядра, дозволяє моделювати складні нелінійні залежності. Лінійна, поліноміальна, радіальна базисна функція (RBF), сигмоїда тощо є популярними функціями ядра, які використовуються в класифікаторі SVM. Цей алгоритм добре працює у високорозмірному просторі та може проявляти різні характеристики в залежності від вибору математичних функцій, що є важливим для гнучкого аналізу великої кількості системних метрик PIC. Водночас велика обчислювальна вартість та складність параметризації (вибір ядер, налаштування параметрів) можуть стати перешкодою при аналізі дуже великих об'ємів даних та застосуванні в реальному часі. SVM доцільно застосовувати, коли є потреба у високій точності та узагальнювальній здатності, і коли обсяги даних дозволяють здійснити оптимізацію параметрів ядра [112].

**Лінійний дискримінантний аналіз (Linear Discriminant Analysis, LDA)** є статистичною моделлю, що ґрунтується на припущеннях про нормальність розподілів даних та однаковість коваріаційних матриць для класів. Цей метод також відомий як узагальнення лінійного дискримінанта Фішера, який проєктує заданий набір даних у простір нижчої розмірності, мінімізує складність моделі або зменшує витрати на обчислення кінцевої моделі. LDA працює для будь-якої кількості класів, на відміну від таких методів як логістична регресія, що в першу чергу використовуються для бінарної класифікації. Він дає простий та інтерпретований розподіл ознак і може бути застосований до відносно простих та лінійно роздільних задач. Однак у реаліях розподілених інформаційних систем, де структури залежностей часто є складними та нелінійними, ефективність LDA обмежена. Він є гарним відправним пунктом для попередньої оцінки даних або як модель порівняння, але для високорівневої оцінки його можливостей часто недостатньо [112].

**Наївний баєсів класифікатор (Naive Bayes, NB)** ґрунтується на застосуванні теореми Баєса з припущенням незалежності між кожною парою ознак. Цей метод є простим у реалізації та ефективним навіть на відносно великих наборах даних. Завдяки цьому NB може застосовуватися для швидкої побудови початкових моделей

оцінювання ризиків. Проте даний алгоритм демонструє низьку ефективність при наявності корельованих ознак, а тому може бути рекомендований лише на етапі первинної оцінки [112].

**Метод найближчих сусідів (k-Nearest Neighbor, k-NN)** є некласифікаційним методом, який не потребує попереднього навчання, адже рішення приймається на основі метрики відстані до найближчих сусідів у просторі ознак. Він не фокусується на побудові загальної внутрішньої моделі; замість цього він зберігає всі екземпляри, що відповідають навчальним даним, у n-вимірному просторі. KNN використовує дані та класифікує нові точки даних на основі показників подібності (наприклад, функції евклідової відстані). Класифікація обчислюється простою більшістю голосів k найближчих сусідів кожної точки. KNN досить стійкий до зашумлених навчальних даних, а точність залежить від їх якості [112]. Цей підхід називають «навчанням на основі екземплярів» або ж «лінивим навчання» оскільки він є інтуїтивно зрозумілим і може бути ефективним при помірних обсягах даних. Однак для великих, високо-вимірних, гетерогенних наборів даних, характерних для PIC, він виявляється надто повільним для задач прогнозування. Таким чином, k-NN може бути корисним на початкових етапах досліджень та як порівняльна модель, проте є малоефективним для практичного застосуваннях в умовах масштабованих PIC.

**Adaptive Boosting (AdaBoost)** – алгоритм з родини ансамблевих методів, який ітеративно комбінує прості базові класифікатори (наприклад, «слабкі» дерева рішень) шляхом навчання на їх помилках. Він здатний зосереджувати увагу на важких для класифікації випадках, підвищуючи точність та узагальнювальну здатність моделі. На відміну від алгоритм**у** Random Forest, який використовує паралельне ансамблювання, Adaboost застосовує послідовний ансамбль класифікаторів. У задачах оцінювання ризику в розподілених системах застосування AdaBoost виправдане, коли є потреба у підвищенні точності на основі простих, швидких, але нересурсоємких моделей. Недоліком є чутливість до шумів та викидів, а також інтерпретація результатів, яка ускладнюється внаслідок багаторівневого поєднання класифікаторів [112].

**Градієнтний бустінг (Extreme gradient boosting, XGBoost)** є одним із найпотужніших ансамблевих методів, що поєднує слабкі класифікатори у сильний за

рахунок ітеративного покращення помилок. Він ефективно працює з широким спектром типів ознак, добре себе проявляє на великих наборах даних, підтримує паралельні обчислення, механізми регуляризації та здатен досягати високої точності класифікації [112]. Недоліком є складність інтерпретації та потреба у досвіді для оптимального налаштування параметрів. Застосування XGBoost обґрунтовано в умовах, коли пріоритетом є висока точність й узагальнювальна здатність системи при великому обсязі гетерогенних даних, а інтерпретованість не є критичною [98].

**Дерева рішень (Decision Tree, DT)** є однією з найпрозоріших моделей, що заснована на послідовному розбитті простору ознак за умови максимізації інформаційного приросту (information gain) чи мінімізації ентропії (entropy).

Ентропія вимірює невизначеність, властиву даним. Цей показник використовується, щоб вирішити, як дерево рішень може розділити дані (3.7).

$$E(x) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i), \tag{3.7}$$

де $E(x)$ – ентропія;

$p(x_i)$ – імовірність настання класу $x_i$.

Інформаційний приріст – показник, що показує скільки «інформації» дає нам конкретна ознака / змінна про остаточний результат (3.8).

$$G = E(p) - E(c), \tag{3.8}$$

де $G$ – інформаційний приріст;

$E(p)$ – ентропія батьківського вузла;

$E(c)$ – середня ентропія дочірніх вузлів.

$$E(c) = \frac{n_{left}}{n_{total}} * e_{left} + \frac{n_{right}}{n_{total}} * e_{right}, \tag{3.9}$$

де $E(c)$ – середня ентропія дочірніх вузлів;

$n_{left}$ – кількість результатів у лівому дочірньому вузлі;

$n_{total}$ – загальна кількість результатів у батьківському вузлі;

$e_{left}$ – ентропія лівого вузла;

$n_{right}$ – кількість результатів у правому дочірньому вузлі;

$e_{right}$ – ентропія правого вузла.

Приріст інформації заснований на зменшенні ентропії після поділу набору даних на атрибут. Даний показник використовується, щоб прийняти рішення який атрибут обрати для поділу вибірки на кожному кроці побудови дерева рішень.

Інший важливий показник для аналізу – індекс Джині, який розраховується за формулою 3.10. Статистичний зміст цього показника полягає в тому, що він відображає, наскільки часто випадково вибраний приклад із навчальної вибірки буде розпізнаний неправильно за умови, що цільові значення в цій вибірці походять із певного статистичного розподілу. Таким чином, індекс Джині фактично демонструє відстань між двома розподілами – розподілом цільових значень та розподілом прогнозів моделі [112].

$$Gini(Q) = 1 - \sum_{i=1}^{c} p_i^2, \tag{3.10}$$

де $Q$ – результуюча множина;

$c$ – кількість класів;

$p_i$ – це ймовірність віднесення об’єкта до певного класу.

Застосування цього алгоритму у сфері оцінювання ризиків дозволяє легко інтерпретувати логіку прийняття рішень, що є важливим під час верифікації причин, котрі призвели до підвищеного ризику для конкретного активу. Дослідженням ефективності застосування алгоритмів дерев рішень для моделювання ризиків в розподілених середовищах було присвячено роботу [61] здобувача, де в цілому цей алгоритм продемонстрував гарний показник класифікації та точність моделі на рівні 80%. Однак одиничні дерева часто схильні до перенавчання та можуть втрачати точність на складних, високовимірних і гетерогенних даних. Їх доцільно застосовувати для швидкого отримання початкових результатів, прототипування або як частину ансамблевих методів.

**Random Forest (RF)** є ансамблевим методом, що об’єднує випадково побудовані дерева рішень. Підхід на основі алгоритму Random Forest надає високоякісні результати у більшості прикладних задач, є досить стійким до шуму, може оцінювати важливість ознак і зазвичай менш схильний до перенавчання, ніж одиничне дерево. RF добре працює із широким спектром типів ознак, не потребує складних налаштувань і часто слугує сильною базовою моделлю для оцінки складності

завдання. Проте, у порівнянні з лінійними моделями, інтерпретованість вихідного результату є нижчою. Для задач оцінювання ризиків у PIC, де необхідно поєднувати широкий спектр ознак, RF може бути одним із найбільш збалансованих варіантів [112].

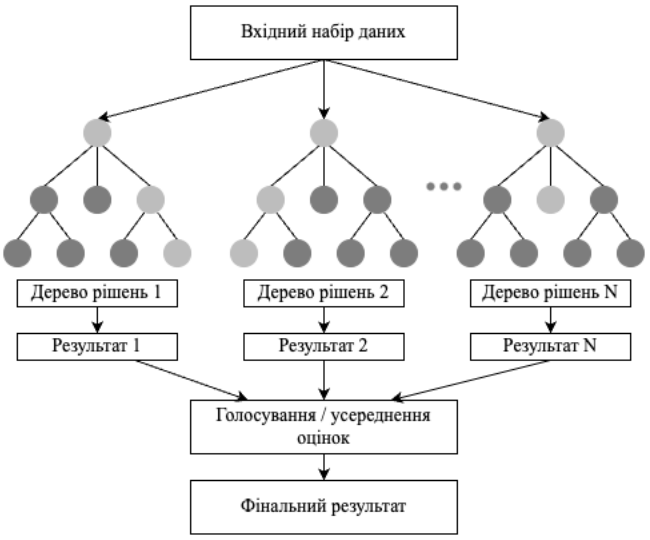


*Рис. 3.1. Приклад структури Random Forest (RF) з урахуванням кількох дерев рішень.*

**Stochastic Gradient Descent (SGD)** є варіантом алгоритму градієнтного спуску, який використовується для оптимізації моделей машинного навчання. Він усуває обчислювальну неефективність традиційних методів градієнтного спуску при роботі з великими наборами даних. Градієнтний спуск в свою чергу – це ітеративний процес оптимізації, який шукає оптимальне значення цільової функції (мінімум/максимум). Це один із найбільш використовуваних методів зміни параметрів моделі з метою зменшення функції витрат. У SGD замість використання всього набору даних для кожної ітерації вибирається лише один випадковий приклад навчання (або невелика партія – batch) для обчислення градієнта та оновлення параметрів моделі. Перевагою використання SGD є його обчислювальна ефективність, особливо при роботі з великими наборами даних. Завдяки використанню одного прикладу або невеликої партії обчислювальна вартість однієї ітерації значно знижується порівняно з традиційними методами градієнтного спуску, які потребують обробки всього набору даних [112].

У випадку, коли розглядається задача мінімізації цільової функції $Q(w)$, це можна представити виразом 3.11.

$$Q(w) = \frac{1}{n}\sum_{i=1}^{n} Q_i(w) \quad (3.11)$$

де $w$– параметр мінімізуючий $Q(w)$.

Для мінімізації цільової функції виконуються наступні ітерації:

$$w := w - \alpha \nabla Q(w) \quad (3.12)$$

де $\alpha$– розмір кроку, який називається швидкістю навчання.

У контексті класифікації ризиків кібербезпеки це дозволяє ефективно знаходити параметри моделі, особливо при великому обсязі даних та оптимізації великих розмірностей. Однак ефективність методу залежить від вибору параметрів (темпу навчання, розміру батчу) і попередньої обробки ознак.

**Нейронні мережі та глибинне навчання (Neural Networks, MLP)**. Парадигма глибинного навчання є частиною ширшого сімейства підходів машинного навчання на основі штучних нейронних мереж (ANN, ШНМ). Глибинне навчання забезпечує обчислювальну архітектуру шляхом поєднання кількох рівнів обробки, таких як вхідний (input), приховані (hidden) і вихідний рівні (output), для навчання з даних. Основною перевагою глибинного навчання перед традиційними методами машинного навчання є його здатність моделювати складні багатовимірні та нелінійні залежності, а також краща продуктивність, зокрема для навчання з великих наборів даних. Нейронні мережі навчаються налаштовувати ваги між шарами штучних нейронів, мінімізуючи функцію втрат. Для багатокласової класифікації на виході використовують функцію softmax, математичне представлення якої було надано раніше (3.6).

Нейронні мережі добре масштабуються та можуть адаптуватися під різні представлення даних. Водночас недоліками є значна обчислювальна вартість, складність у налаштуванні гіперпараметрів, необхідність великих обсягів даних для тренування та менша інтерпретованість. Проте, враховуючи сучасні тенденції в обчислювальній техніці, використання нейронних мереж стає дедалі привабливішим і потенційно найбільш ефективним для задач, де динамічність і складність середовища PIC відіграють ключову роль [112].

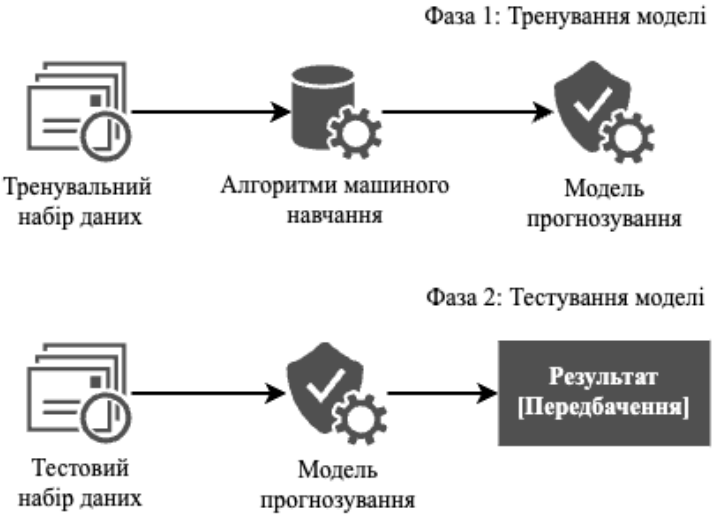


*Рис. 3.2. Концептуальна схема проєктування нейромережевих моделей на основі алгоритмів машинного навчання.*

Таким чином, вибір конкретного методу залежить від характеристик завдання, доступних обчислювальних ресурсів, вимог до інтерпретованості, обсягу та складності вхідних даних.

На наступному етапі пропонується провести SWOT-аналіз основних підходів до моделювання процесу оцінювання ризиків ІБ на основі алгоритмів машинного навчання. SWOT-аналіз допомагає зрозуміти сильні та слабкі сторони кожного підходу, а також оцінити потенційні можливості й ризики впровадження конкретних методів у реальній практиці оцінювання ризиків кібербезпеки.

Результати SWOT-аналізу основних підходів до моделювання процесу оцінювання ризиків кібербезпеки на основі алгоритмів машинного навчання представлено в **Додатку Г**. Підсумовуючи результати проведеного аналізу, можна зробити висновок, що логістична регресія, LDA, наївний Байєс та Decision Tree можуть бути корисними на початкових етапах чи для задач із відносно простими структурами даних та необхідністю інтерпретації результатів. Алгоритми SVM, SGD та k-NN доречні для помірних обсягів даних або специфічних умов. Нейронні мережі, AdaBoost, XGBoost та Random Forest рекомендовані при великих, складних масивах гетерогенних даних, де важлива висока точність, адаптивність та здатність до нелінійного моделювання, а рівень інтерпретованості може бути компенсований іншими підходами (наприклад, інструментами інтерпретації результатів).

### 3.2.3. Порівняльний аналіз програмних фреймворків машинного навчання

Для вибору ефективного інструментарію розробки моделей оцінювання ризиків в розподілених інформаційних системах доцільним є проведення огляду та порівняльного аналізу програмних фреймворків для машинного та глибинного навчання з урахуванням сучасних вимог до розробки моделей ШІ. Особливу увагу слід приділити вимогам здатності до обробки великих обсягів гетерогенних даних, оптимізації обчислювальної складності, можливості масштабування та сумісності роботи з різними апаратними платформами.

Стрімкий розвиток методів машинного навчання та технологій глибоких нейронних мереж привів до появи широкого спектра інструментів, бібліотек та програмних фреймворків від провідних вендорів та IT-гігантів. Найбільшою популярністю користуються такі інструменти як TensorFlow, PyTorch, scikit-lear, MXNet, JAX, CNTK тощо. Зазвичай, з метою досягнення найкращих показників оптимізації використання апаратних ресурсів, споживання пам’яті та швидкості виконання ядро таких фреймворків реалізовано на мовах програмування C/C++. Проте з метою зручності використання їх інтерфейс, як правило, обгортається високорівневими мовами програмування (Python, Lua, R, Matlab тощо). Вибір належного програмного оточення є критичним, оскільки він впливає на продуктивність, масштабованість, гнучкість, зручність інтеграції та підтримки моделей у продуктивних середовищах.

Зокрема, у задачах оцінки ризиків кібербезпеки в РІС важливі наступні критерії:

1. Продуктивність та масштабування: Здатність платформи ефективно навчати моделі на великих наборах гетерогенних даних із залученням різних обчислювальних ресурсів (CPU, GPU, TPU, кластери) для скорочення часу тренування.

2. Підтримка різних типів моделей: Можливість реалізовувати як класичні алгоритми МН (логістична регресія, SVM, дерева рішень) так і складні архітектури ГН (конволюційні, рекурентні мережі, трансформери) для адаптації до різнорідної природи даних РІС.

3. Зручність розробки та відлагодження: Інтуїтивний інтерфейс, наявність доступної документації, інструментів для візуалізації, оцінки продуктивності, відлагодження та спрощення процесу емпіричних досліджень.

4. Інтеграція з екосистемою сучасної IT-інфраструктури: Можливість розгортання моделей у хмарних середовищах, контейнеризація, підтримка мікросервісної архітектури, інтеграція з інструментами CI/CD, DevOps-практиками.

На сьогодні, на ринку домінують кілька ключових гравців:

- **TensorFlow** (Google): Один з найпоширеніших фреймворків глибинного навчання, що забезпечує потужний інструментарій для побудови нейромережевих архітектур, включно з Keras для швидкого прототипування. TensorFlow підтримує GPU, TPU, має інтеграцію з Google Cloud, інструменти для візуалізації (TensorBoard) та широкий спектр готових моделей.
- **PyTorch** (Meta, колишній Facebook): Відзначається гнучкою імперативною моделлю програмування, зручною для дослідницьких експериментів. PyTorch пропонує інтуїтивний синтаксис, інтеграцію з Python, ефективне навчання на GPU, а також широку спільноту користувачів і підтримку в академічній сфері.
- **MXNet** (Apache): Підтримує різні мови програмування (C++, Python, R), оптимізований для масштабування та розподіленого навчання, тісно інтегрований із хмарними платформами AWS. MXNet був початково популярний завдяки Amazon, але поступово поступився TensorFlow та PyTorch за популярністю.
- **JAX** (Google): Нова бібліотека від Google, що поєднує в собі можливості автоматичного диференціювання та векторизованих обчислень, добре працює з TPU і GPU, інтегрована зі стеком Google Cloud. JAX пропонує продуктивність і гнучкість, але поки має меншу спільноту користувачів.
- **CNTK** (Microsoft Cognitive Toolkit): Потужний і гнучкий фреймворк машинного навчання, розроблений компанією Microsoft для побудови та навчання глибоких нейронних мереж. Він орієнтований на розв’язання складних задач, таких як обробка природної мови, комп’ютерний зір та розпізнавання мовлення.
- **scikit-learn**: Широко відома бібліотека машинного навчання на мові Python, орієнтована здебільшого на класичні методи (лінійні моделі, дерева рішень,

ансамблі, методи зниження розмірності, кластеризації, тощо). Її перевагами є простота використання, уніфікований інтерфейс для різних алгоритмів, велика кількість документованих прикладів і можливість швидкого прототипування. Бібліотека оптимізована під CPU та менш орієнтована на використання GPU, проте чудово підходить для початкових етапів аналізу даних, створення еталонних моделей, проведення порівняння алгоритмів, а також для освітніх і наукових потреб. Має обмежені власні інструменти візуалізації, але ідеально поєднується з іншими Python-бібліотеками (matplotlib, seaborn, тощо).

*Таблиця 3.2*

*Порівняння основних програмних фреймворків машинного навчання*

| | **TensorFlow** | **PyTorch** | **MXNet** | **JAX** | **CNTK** | **scikit-learn** |
|---|---|---|---|---|---|---|
| Розробник / Вендор | Google | Meta (Facebook) | Apache (Amazon) | Google | Microsoft | Open Source |
| Мова програму-вання | Python, C++ Java, Go, JavaScript | Python, C++ | Python, C++, Go, Java, JavaScript, Scala, Julia, Perl, R | Python, C++ | Python, C#, C++ | Python |
| Дата релізу | 9 листопада 2015 року | Вересень 2016 р. | 10 травня 2022 р. | 30 липня 2024 р. | 25 січня 2016 р. | Червень 2007 р. |
| Ліцензія | Apache 2.0 | BSD-3 | Apache 2.0 | Apache 2.0 | MIT | New BSD |
| Апаратна підтримка | CPU, GPU, TPU, кластер | CPU, GPU, TPU, кластер | CPU, GPU, кластер | CPU, GPU, TPU, кластер | CPU, GPU, кластер | CPU |
| Спільнота та екосистема | Широка академічна спільнота, чудова оптимізація, промислові кейси застосування, Google Cloud інтеграція | Широка академічна спільнота, ідеальний для дослід-ницького етапу, швидкого прототипу-вання | Тісна інтеграція з AWS сервісами, менша кількість матеріалів | Активна академічна спільнота, Google Cloud інтеграція | Менша спільнота з огляду на припи-нення активної розробки, інтеграція з екосис-темою Microsoft | Відкрита спільнота, стандарт де-факто для класичних МН задач, ідеальна для початківців та навчання |

Таким чином, можна сформулювати наступні висновки щодо вибору інструментарію для задач дослідження. Для реалізації складних моделей глибинного навчання, що працюватимуть із гетерогенними, розподіленими даними й потребуватимуть масштабування, найбільш придатними будуть PyTorch або

TensorFlow/Keras, залежно від стадії проєкту (дослідницька чи виробнича). Бібліотека scikit-learn ідеально підходить для початкових експериментів, порівняння базових методів, побудови еталонних моделей та навчальних потреб, але менш придатна для важких задач глибинного чи розподіленого навчання великих мереж. Натомість, поєднання scikit-learn для початкового етапу й обраного фреймворку глибинного навчання (PyTorch чи TensorFlow) для більш складних завдань створює гнучкий багатоступеневий підхід, що оптимально відповідає вимогам комплексного дослідницького процесу.

## 3.3. Розробка та проєктування моделей оцінювання ризику на основі контролю відповідності вимогам стандартів кібербезпеки

Відповідність стандартам ІБ дозволяє мінімізувати ризики шляхом впровадження регламентованих заходів безпеки, проте традиційні підходи до аудиту та оцінки відповідності мають низку обмежень, зокрема низьку гнучкість, значні витрати часу та складність автоматизації процесів. Враховуючи ці виклики, актуальним є розроблення моделей оцінювання ризику, які інтегрують контроль відповідності стандартам ІБ у загальну систему управління кіберризиками. Такі моделі повинні не лише оцінювати рівень відповідності, а й дозволяти автоматизований моніторинг стану безпеки та динамічне корегування показників ризику відповідно до змін у конфігурації інфраструктури та загрозовому ландшафті.

### 3.3.1. Формалізація контролів ІБ як вхідних параметрів проєктованих моделей

Вимоги стандартів, виражені через контролі, можна перетворити на метрики (кількісні та / або якісні показники) для оцінки рівня зрілості ІБ. Разом із підходами ризик-менеджменту ці метрики формують основу для вимірювання ефективності та дієвості контрольних механізмів.

Для подальшого моделювання ризику з використанням алгоритмів інтелектуального аналізу та глибоких нейронних мереж необхідно формалізувати

якісні та описові вимоги стандартів у набір кількісних та категоріальних метрик. Така формалізація стандартів є критичною з наступних причин:

- **Автоматизація оцінювання**: Перетворення описових вимог у числові індикатори дозволяє автоматизувати процес оцінки ступеня відповідності, інтегрувати ці показники у системи моніторингу та управління ІБ, а також оновлювати оцінку ризику в реальному часі.
- **Порівняння та агрегація даних**: Числові метрики дають змогу порівнювати стан відповідності між різними активами, підрозділами або організаціями. Це сприяє кращому розподілу ресурсів, пріоритезації покращень та прийняттю управлінських рішень на підставі об’єктивних даних.
- **Модельне представлення та аналітика**: Чітко визначені метрики можна використовувати як вхідні параметри для моделей машинного навчання, що оцінюють ризик. Завдяки цьому стає можливим виявлення складних взаємозв’язків та прогнозування наслідків зміни рівня відповідності стандартам ІБ.

Таким чином, наявність формалізованих показників відповідності вимогам стандартів ІБ забезпечує сталу основу для інтеграції нормативних вимог у формальні математичні моделі ризику, створює умови для їх аналізу за допомогою ШІ-методів та сприяє побудові динамічних, адаптивних систем управління ризиками в розподілених середовищах.

### 3.3.2. Експериментальні дослідження та аналіз отриманих результатів

Контролі, що пройшли відбір, безпосередньо використовуються як основа для формування ознак у датасеті для моделювання. У якості джерела для агрегування даних відповідності стандартам ІБ розглядається використання програмного комплексу **ITS Inventory** та модулю **ITS Compliance**, що призначений для задач автоматизації контролю відповідності як внутрішнім політикам ІБ так і провідним стандартам ІБ та нормативно-правовим документам. ITS Compliance є важливим інструментом, що не тільки допомагає в процесі проведення аудитів інформаційної безпеки, а й забезпечує можливість постійного контролю і відслідковування стану відповідності регулюючим актам. Модуль містить ряд попередньо встановлених

шаблонів для ключових стандартів, що пропонують логіку автоматизації технологічних асет-орієнтованих контролів та не потребують додаткового налаштування. Окрім цього доступна можливість ручного контролю та фіксації стану метрик, що не можуть бути автоматизовані програмним шляхом.

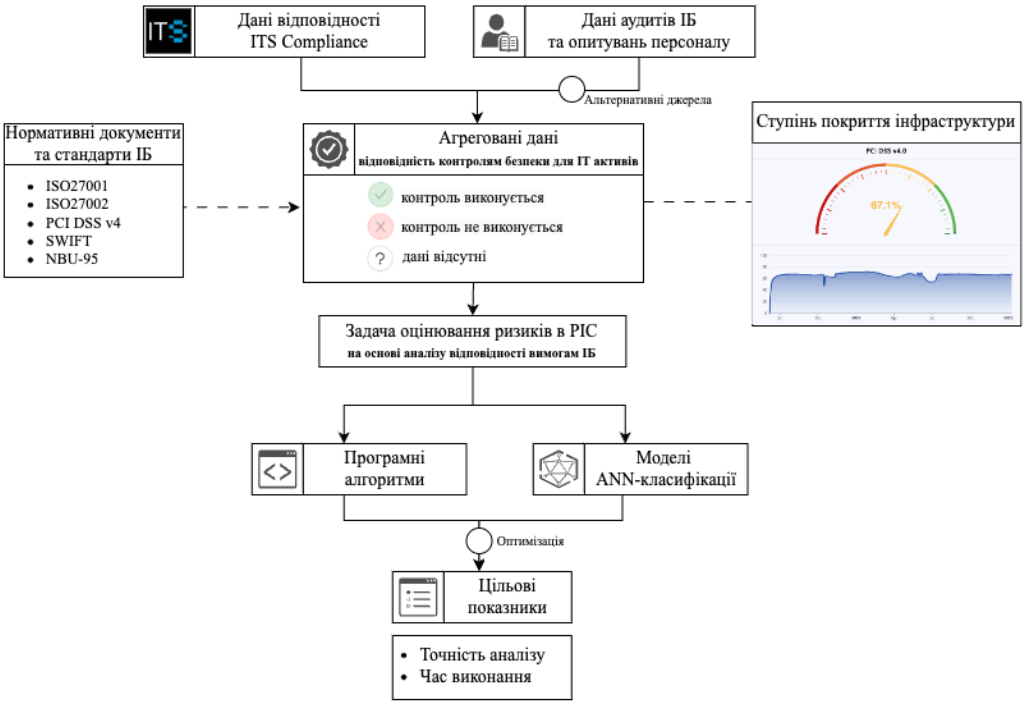


*Рис. 3.3. Концептуальна схема комплексної системи машинного аналізу відповідності вимогам стандартів ІБ в задачах оцінювання ризику РІС.*

Формат представлення даних відповідності носить стандартизований характер та може набувати наступних значень:

- Контроль виконується для даного мережевого активу (відповідність конкретній вимозі стандарту);
- Контроль не виконується для мережевого активу (невідповідність вимозі стандарту);
- Дані відсутні.

На етапі підготовки наборів даних сформовано навчальні вибірки для кожного із досліджуваних стандартів, що відображають дані типової розподіленої системи. Оскільки наявні набори даних мають невелику розмірність – прийнято рішення про застосування методів аугментації навчальної вибірки із застосуванням інструментарію генеративних змагальних мереж (Generative adversarial networks,

GANs), що дозволяє ефективно працювати зі «сирими» та неповними наборами, характерними для розподілених середовищ, і підвищує ефективність проєктованих моделей. В результаті сформовано навчальні датасети однакової розмірності, що містять по 5000 записів для кожного досліджуваного стандарту. Експериментальне моделювання передбачало розбиття навчальної та тестової вибірки у співвідношенні 0,8 до 0,2.

Для емпіричної перевірки було обрано вісім алгоритмів, які за результатами проведеного аналізу найкраще підходять для даного дослідження, а саме:

- логістична регресія (Logistic Regression);
- метод опорних векторів (Support Vector Machine);
- лінійний дискримінантний аналіз (Linear Discriminant Analysis);
- наївний Баєс (Naive Bayes);
- метод найближчих сусідів (K-Nearest Neighbor);
- градієнтний бустінг (Extreme Gradient Boosting, або xGboost);
- алгоритм Random Forest;
- нейронні мережі (Neural Networks or Multilayer Perceptron).

Для багатошарового перцептрона використовувались такі конфігурації гіперпараметрів: 1 прихований шар з 50 нейронами; 2 приховані шари з 50 і 30 нейронами в кожному шарі; та 3 приховані шари з 70, 50 та 30 нейронами у кожному шарі відповідно. ReLU було обрано як функцію активації для прихованих шарів, а softmax як функцію активації для вихідного шару. Алгоритм навчання (оптимізатор) – RMSprop, кількість епох на етапі навчання – 1000, швидкість навчання – 0,001, розмір пакету (batch) – 100, функція втрат – категоріальна перехресна ентропія (Categorical Cross-Entropy, CCE). Для інших алгоритмів використано конфігурацію за замовчуванням, рекомендовану фреймворком sklearn (наприклад, у випадку PCA кількість компонентів було встановлено на 30).

Класифікаційні моделі пройшли підготовку за двома різними сценаріями: з та без PCA компресії. Єдиним винятком стали нейронні мережі (MLP), оскільки вони є складними нелінійними моделями та менш чутливі до мультиколінеарності, оскільки здатні розпізнавати нелінійні залежності навіть у корельованих просторах. Таким

чином, не має сенсу використовувати PCA для цієї групи алгоритмів. Результати експериментів представлені у Таблиці 3.3.

*Таблиця 3.3*

*Результати точності класифікації для різних типів алгоритмів*

| | **ISO 27001 ISO 27002** | **PCI DSS v4** | **SWIFT** | **NBU-95** |
|---|---|---|---|---|
| **Logistic Regression** | 0.8650 | 0.8350 | 0.8702 | 0.8040 |
| **PCA+Logistic Regression** | 0.9046 | 0.8850 | 0.8940 | 0.8604 |
| **SVM classifier** | 0.7805 | 0.7650 | 0.8104 | 0.7303 |
| **PCA+SVM classifier** | 0.8255 | 0.8100 | 0.7877 | 0.7302 |
| **LDA classifier** | 0.8820 | 0.8750 | 0.9108 | 0.8306 |
| **PCA+LDA classifier** | 0.9303 | 0.9233 | 0.9104 | 0.8823 |
| **KNN classifier** | 0.5228 | 0.4160 | 0.5430 | 0.6120 |
| **PCA+KNN classifier** | 0.4914 | 0.5947 | 0.6336 | 0.5504 |
| **Naive Bayes** | 0.7082 | 0.6250 | 0.7406 | 0.6534 |
| **PCA+Naive Bayes** | 0.7505 | 0.7404 | 0.7907 | 0.7102 |
| **xgboost classifier** | 0.7500 | 0.5950 | 0.7804 | 0.6910 |
| **PCA+xgboost classifier** | 0.8030 | 0.7905 | 0.8373 | 0.7500 |
| **Random Forest** | 0.7200 | 0.5257 | 0.7508 | 0.7404 |
| **PCA+Random Forest** | 0.7702 | 0.7660 | 0.8060 | 0.7329 |
| **MLP (1 hidden layer)** | 0.8777 | 0.8603 | 0.8905 | 0.8320 |
| **MLP (2 hidden layer)** | 0.8801 | 0.7950 | 0.9398 | 0.8701 |
| **MLP (3 hidden layer)** | 0.9580 | 0.8589 | 0.9460 | 0.8934 |

Згідно з інформацією, представленою в Таблиці 3.3, загальні тренди залишаються сталими для всіх алгоритмів на кожному з наборів даних, що використовувалися для класифікації ризиків інформаційної безпеки. Лінійні моделі (логістична регресія, LDA, SVM), продемонстрували здатність досягати високої

точності в середньому на рівні 80-90% для всіх наборів даних досліджуваних стандартів ІБ, що робить їх привабливими для задач з обмеженими обчислювальними ресурсами. Натомість такі алгоритми як Naive Bayes, KNN, XGBoost та Random Forest, показали порівняно нижчі результати в точності. Варто зазначити, що використання PCA для компресії даних має неоднозначний ефект: в одних випадках спостерігається покращення точності, тоді як в інших – її зниження. Це свідчить про те, що застосування PCA не є універсальним підходом і може залежати від специфіки задачі та характеристик даних.

З точки зору обчислювальних витрат, MLP і xGBoost виявилися більш ресурсозатратними, що може обмежувати їх застосування у реальних системах із жорсткими обмеженнями на час обробки та енергоспоживання. У свою чергу, логістична регресія та LDA були одними з найшвидших алгоритмів, що робить їх ефективними для оперативного аналізу ризиків кібербезпеки.

Найвищу точність класифікації ризиків на рівні 90-95% було досягнуто за допомогою алгоритмів LDA та MLP на всіх чотирьох наборах даних. Нейронні мережі, очікувано демонструють дуже високу ефективність завдяки їх здатності моделювати складні залежності між вхідними ознаками ризиків ІБ (кращі показники для 3 з 4 досліджуваних наборів). При цьому чітко прослідковується наступна тенденція – ускладнення архітектури багатошарового перцептрону та збільшення кількості прихованих шарів позитивно впливає на продуктивність моделей. Найкращу ефективність прогнозовано продемонстрували моделі із 3 прихованими шарами із середнім рівнем точності на рівні 90,75% для всіх наборів даних.

### 3.4. Адаптивний метод комплексного кількісного оцінювання ризиків кібербезпеки в РІС з використанням спроєктованих моделей

Підсумовуючи результати попередніх досліджень, оцінювання ризиків кібербезпеки в умовах розподілених середовищ, є складним, багатофакторним процесом, оскільки передбачає вирішення комплексу проблем, що пов’язані з розподіленістю інфраструктури, динамічним характером загроз, зростанням вимог регуляторів та суттєвою обмеженістю існуючих методологій та підходів оцінки в

умовах масштабованих РІС. Це в свою чергу, вимагає розробки комплексної та адаптивної методики оцінювання кіберризиків в РІС, що на відміну від класичного підходу враховує динамічний характер розподіленого середовища і ймовірнісний характер кіберзагроз, сприяє підвищенню зрілості процесів кібербезпеки та дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних [118, 128, 132, 135].

Запропонована методика заснована на використанні ряду розроблених універсальних моделей оцінювання на основі класичних алгоритмів машинного навчання та глибоких нейронних мереж з кращими показниками зважених середніх значень критеріїв середньої точності (Average Accuracy), F1-міри (F1-score) та AUC-ROC, та дозволяє комплексно оцінити ризики кібербезпеки у розподілених системах, поєднуючи аналіз відповідності нормативним стандартам із глибокою обробкою технічних метрик, інтегруючи переваги метрико-орієнтовного та контроль-орієнтовного підходів. Це дозволяє створити масштабовану, адаптивну та динамічну систему управління кіберризиками, що ефективно реагує на сучасні загрози в РІС та перевершує традиційні методи аналізу ризиків.

Основні вимоги до запропонованого підходу можна узагальнити в наступних ключових положеннях та принципах:

- **Комплексність та універсальність.** Облік множинних факторів ризику, включаючи технічні та нормативно-правові аспекти; застосовність до різних типів IT-активів, що можуть значно диференціюватись за характером, призначенням та технічними аспектами функціонування (архітектура, обладнання, протоколи взаємодії тощо);
- **Масштабованість.** Здатність ефективно аналізувати масштабовані розподілені системи та асоційовані з їх функціонуванням великі масиви різнорідних даних;
- **Гнучкість та адаптивність.** Можливість динамічної корекції оцінювання ризику та адаптації до змін середовища без необхідності повторного навчання моделей; спроможність гнучко підлаштовуватись до змін умов функціонування, розмірів, топології та архітектури інфраструктури;

- **Кількісна оцінка.** Забезпечення кількісного підходу до оцінювання ризиків розподіленого середовища із врахуванням широкого спектру факторів впливу.
- **Автоматизованість та практична орієнтація.** Орієнтація на практичні аспекти імплементації та застосування з можливістю реалізації автоматизованих сценаріїв оцінювання.

Таким чином, розроблена методика [64] повинна бути побудована на принципах комплексного оцінювання із врахуванням всіх наявних даних та метрик безпеки, а також кореляції з існуючими факторами ризику, профілем потенційних загроз, та орієнтацією на аспекти практичної імплементації та застосування в корпоративному середовищі типової розподіленої інформаційної системи, створеної для забезпечення одного або декількох типів інформаційних процесів та / або надання інформаційних послуг. Окрім цього, запропонований підхід повинен враховувати факт функціонування інформаційної системи в умовах невизначеності, при невідомих законах і числових характеристиках розподілу кіберзагроз. Концептуальна схема архітектури системи комплексного оцінювання ризиків розподіленого середовища відображена на Рисунку 3.4.

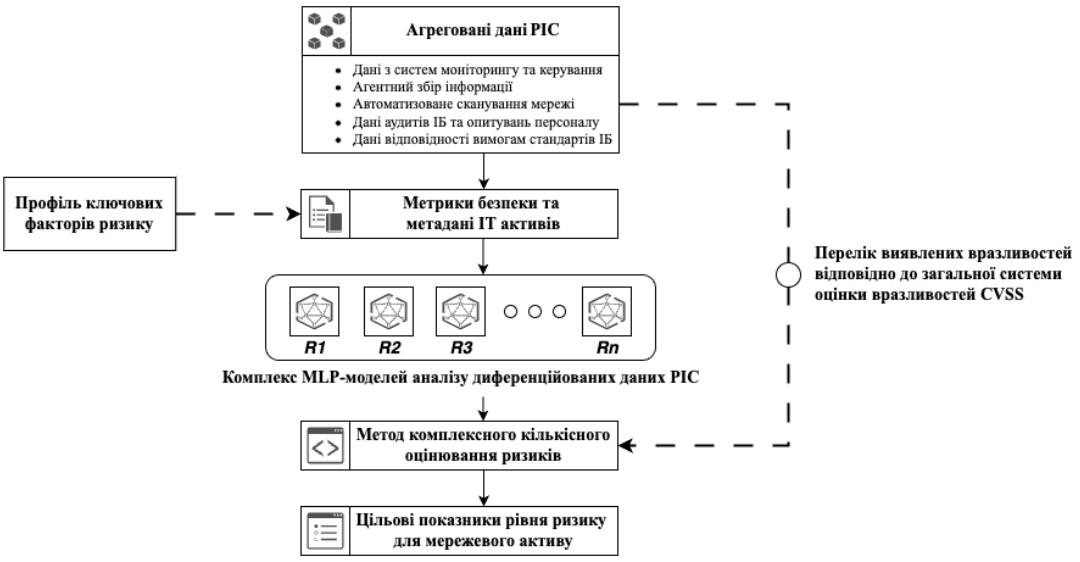


*Рис. 3.4. Концептуальна схема комплексної системи машинного аналізу даних PIC в задачах оцінювання ризику кібербезпеки.*

З метою вирішення поставлених завдань та обмежень, запропоноване рішення об’єднує декілька ключових аспектів:

1. Побудований профіль ключових факторів ризику сучасних РІС, на основі якого проведено оптимізацію вхідного простору метрик для проєктованих моделей;

2. Розроблені нейромережеві моделі оцінювання ризику на основі розподілених метрик про роботу мережевих активів;

3. Формалізовані вимоги та контролі безпеки провідних міжнародних та галузевих стандартів ІБ (ISO 27001, ISO 27002, PCI DSS v4, SWIFT, NBU-95 тощо), а також їх інтеграція у моделі оцінювання ризику, що спрощує процеси аудиту, полегшує виявлення критичних прогалин у безпеці та підвищує загальний рівень зрілості організації у сфері ІБ;

4. Розроблені нейромережеві моделі оцінювання ризику на основі аналізу відповідності вимогам стандартів ІБ та контролям безпеки;

5. Розроблений адаптивний метод комплексного кількісного оцінювання ризиків кібербезпеки в РІС з використанням спроєктованих моделей та загальної системи оцінки вразливостей CVSS.

Ключовим елементом запропонованого рішення, що забезпечує принцип комплексного аналізу та дослідження різних аспектів оцінки захищеності розподіленої системи є можливість використання комплексу розроблених нейромережевих моделей оцінювання ризику. Моделі на основі алгоритмів машинного навчання та глибоких нейронних мереж, у порівнянні із класичними підходами до оцінювання ризиків ІБ, демонструють чудові якісні показники ефективності. Комплексне застосування декількох моделей забезпечує ґрунтовний системний підхід до оцінювання стану безпеки, враховуючи всі фактори та аспекти функціонування РІС, аналізуючи всі доступні дані та об’єднуючи їх результати в єдиному аналітичному середовищі [111].

Виходячи із вимог універсальності застосування, гнучкості оцінювання та комплексності аналізу запропоновано адаптивний метод трансформації якісної шкали оцінювання ризику в кількісний показник, що на відміну від класичного підходу враховує динамічний характер розподіленого середовища, та дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних [130].

Відповідно до класичного підходу основними детермінантами ризику є множина кібернетичних загроз ($T$) та множина виявлених вразливостей ($V$). Також необхідно враховувати варіативний рівень збитку ($I$) при реалізації кібернетичних загроз для різних типів активів на основі проведеного профілювання за рівнем важливості та критичності об'єкту для інфраструктури ($W_i$). Подальше обґрунтування потребує попередньої математичної формалізації.

Позначимо множину факторів ризику $F = \{F_1, F_2, \dots, F_i\}$, де $F_i$ – фактор, який характеризує певний аспект стану безпеки інформаційної системи (наприклад, актуальність оновлень, наявність антивірусного захисту тощо). Кожен фактор описується певними безпековими метриками:

$$F_i = \{m_{i1}, m_{i2}, \dots, m_{ij}\}, \;\; m_{ij} \in [0,1] \tag{3.13}$$

де $m_{ij}$ – нормалізована метрика, яка характеризує фактор $F_i$.

Визначимо множину ризиків $R = \{R_1, R_2, \dots, R_m\}$. Кожен ризик може залежати від одного або декількох факторів $F_i$, при цьому кожен фактор може бути притаманним та формувати різні вектори загроз:

$$R_j = f_j(F_1, F_2, \dots, F_n), \tag{3.14}$$

де $f_j$ – функція залежності, що описує вплив факторів ризику на ризик $R_j$.

Розподілена система складається з компонентів $A = \{A_1, A_2, \dots, A_n\}$, де $A_i$ – окремий мережевий актив. Кожен актив $A_i$ має індивідуальний рівень ризику $R(A_i)$, який залежить від ідентифікованих для нього факторів ризику, загроз та вразливостей.

Ризик кібербезпеки в класичному розумінні можна визначити як функцію загроз, вразливостей та можливих наслідків. Формально це можна представити наступним чином:

$$R(A_i) = f(T, V, I), \tag{3.15}$$

де $R(A_i)$ – рівень ризику для активу $A_i$.

$T$ – множина потенційних загроз ($T = \{T_1, T_2, \dots, T_n\}$);

$V$ – множина потенційних вразливостей ($V = \{V_1, V_2, \dots, V_m\}$);

$I$ – можливий вплив загрози на систему ($I = \{I_1, I_2, \dots, I_k\}$).

В загальному випадку загрози можуть бути обраховані через ймовірності їх реалізації:

$$P(T_i) = \frac{N_{\text{успішних атак}}}{N_{\text{спроб атак}}} \quad (3.16)$$

де $N_{\text{успішних атак}}$ – кількість зафіксованих атак певного типу на подібні активи за певний період часу (тобто кількість реалізованих загроз);

$N_{\text{спроб атак}}$ – загальна кількість атак (за той же період).

Окрім цього, модель ризику може бути виражена як ймовірнісний продукт:

$$R(A_i) = P(T_n) \cdot P(V_m) \cdot I_k, \quad (3.17)$$

де $P(T_n)$ – ймовірність виникнення загрози;

$P(V_m)$ – ймовірність експлуатації вразливості;

$I_k$ – вплив загрози на актив.

Надане представлення можна ускладнити з врахуванням специфічних впливів кожного з аргументів. Загальна формула оцінки ризику для конкретного активу з урахуванням ймовірності загрози, впливу та критичності активу набуде наступного вигляду:

$$R(A_i) = W_i \cdot (P(T_n) \cdot I_T + P(V_m) \cdot I_V), \quad (3.18)$$

де $I_T$ – критичність впливу загрози (Threat Impact);

$I_V$ – серйозність впливу вразливості (Vulnerability Impact).

Таким чином, модель комплексного оцінювання рівня ризику для компонентів системи може бути обчислена як агрегована оцінка на основі врахування факторів ризику, загроз та вразливостей. Окрім цього, для розподілених систем важливо враховувати динаміку ризиків в часі:

$$R(A_i) = \sum_{j=1}^{h}\left[ w_j(t) \cdot f_j(F_1(t), F_2(t), \dots, F_n(t))\right] \cdot \sum_{j=1}^{n}\sum_{j=1}^{m} P(T_n \cdot V_m) \cdot I_k, \quad (3.19)$$

де $w_j$ – ваговий коефіцієнт для ризику $R_j$;

$f_j(F_1, F_2, \dots, F_n)$ – функція оцінки конкретного ризику;

$P(T_n \cdot V_m)$ – імовірність експлуатації вразливості $V_m$ загрозою $T_n$;

$t$ – час, а $w_j(t)$, $F_n(t)$ – значення, що змінюються в часі.

Обрахунок загального рівня ризику розподіленої інформаційної системи набуде наступного вигляду:

$$R_{total} = \sum_{i=1}^{N} R(A_i) \cdot W_i, \quad (3.20)$$

де $W_i$ – ваговий коефіцієнт активу $A_i$, що відображає міру його важливості у системі (наприклад, на основі критичності або функціональному навантаженні компонента).

Описані методологічні принципи обрахунку дозволяють сформувати комплексний адаптивний метод обчислення кількісного показника рівня ризику для розподіленого середовища. Запропонований метод ґрунтується на спроєктованих моделях як ключових критеріях оцінювання потенційних загроз, та враховує динамічний характер розподіленого середовища, використовуючи загальну систему оцінки вразливостей CVSS (Common Vulnerability Scoring System) для аналізу наявних вразливостей активу [129]. Окрім цього, запропонований підхід дозволяє врахувати параметри критичності активу на основі профілювання типів об'єктів та визначення їх важливості, а також ряд безпекових показників, пов'язаних із виявленим переліком вразливостей, що в свою чергу співвідноситься з класичною схемою обрахунку показника ризику, яка була описана раніше [119-120]. Запропонований метод, представлений формулою 3.21, є достатньо гнучким та універсальним, не залежить від типу, архітектури, топології чи розміру інформаційної системи, та дозволяє повністю автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

$$R_{Scaled} = \frac{\frac{1}{k}(R_{1+} R_2 + \cdots + R_k) + \alpha \cdot R_{old}}{1+\alpha} \cdot \frac{\sum_{j=1}^{N} CVSS_j}{2N} \cdot W_i + \beta, \quad (3.21)$$

де $R_k$ – показник рівня ризику обрахований відповідно до спроєктованих метрико-орієнтовних та стандарт-орієнтовних моделей оцінювання $R_k \in [1,5]$;

$k$ – кількість нейромережевих моделей оцінювання;

$R_{old}$ – усереднений показник рівня ризику обрахований за результатами $k$ моделей на попередній ітерації оцінювання (наявність зв'язку з ретроспективними даними);

$CVSS_j$ – показник CVSS-score $j$ вразливості $CVSS_j \in [1,10]$;

$N$ – кількість вразливостей задетектованих на мережевому активі;

$\alpha$ – коефіцієнт важливості врахування ретроспективних даних $\alpha \in [0,1]$;

β – коефіцієнт корегування для окремого активу;

$W_i$ – рівень критичності (важливості) активу $W\epsilon[1,4]$.

Відповідно до принципу, запропонованого в роботі [88], для систем з адитивними показниками ефективності окремих елементів (тобто таких систем, кожен з елементів яких вносить певний незалежний вклад в загальний результуючий ефект) сумарна ефективність може бути розрахована за формулою:

$$E(t) = \sum_{i=1}^{N} \sigma_i \cdot r_i(t), \quad (3.22)$$

де $\sigma_i$ – вклад, що вноситься $i$-м елементом в сумарний вихідний ефект;

$r_i(t)$ – досліджуваний показник.

Таким чином, запропонований механізм за рахунок наявності коефіцієнту $\sigma_i$ дозволяє врахувати зважені результати окремих моделей в залежності від їх пріоритету та важливості результату. Кожна з моделей здійснює якісну оцінку показника ризику відповідно до своєї предметної області за допомогою наступної шкали:

- Критичний – $r_i(t) = 5$;
- Високий – $r_i(t) = 4$;
- Середній – $r_i(t) = 3$;
- Низький – $r_i(t) = 2$;
- Інформаційний – $r_i(t) = 1$;

Окрім цього, за рахунок наявності коефіцієнт α, що набуває значень в діапазоні $\alpha\,\epsilon[0,1]$, можна гнучко налаштувати важливість врахування ретроспективного усередненого показника рівня ризику, обрахованого за результатами $k$ моделей на попередній ітерації оцінювання. Цей критерій може як повністю ігноруватись, так і вносити рівноцінний вклад до поточного результуючого значення оцінки моделей, таким чином збалансовуючи і зрівноважуючи результат та згладжуючи різкі динамічні зміни результатів.

Другий аргумент запропонованого методу трансформації якісної шкали оцінювання ризику в кількісний показник безпосередньо враховує критичність та число ідентифікованих вразливостей для кожного об’єкту відповідно до їх CVSS score відкритої системи класифікації та ранжування вразливостей Common Vulnerability

Scoring System. Обрахунок усередненого значення цього показника можна вдосконалити на основі середнього зваженого значення.

Зважене середнє – це статистична міра, яка враховує різну важливість (вагу) кожного елемента в наборі даних (вразливостей). Формула для обчислення зваженого середнього виглядає так:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i * w_i}{\sum_{i=1}^{n} w_i}, \quad (3.23)$$

де $x_i$ – значення елемента;

$w_i$– відповідна вага цього елемента.

У випадку зваженого середнього з квадратичними вагами, ваги $w_i$ визначаються як квадрати деяких величин, що відображають важливість або надійність відповідних значень $x_i$. Це означає, що ваги обчислюються як $w_i = {v_i}^2$, де $v_i$ – початкова вага або міра важливості елемента.

Таким чином, формула зваженого середнього з квадратичними вагами набуває вигляду:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i * {v_i}^2}{\sum_{i=1}^{n} {v_i}^2}, \quad (3.24)$$

Цей підхід дозволяє надавати більшої ваги елементам з вищими значеннями, що може бути корисним у випадках, коли важливість елементів зростає нелінійно.

Якщо розглянемо випадок де $w_i = x_i$, то середнє зважене набуватиме вигляду:

$$\bar{x} = \frac{\sum_{i=1}^{n} {x_i}^2}{\sum_{i=1}^{n} x_i}, \quad (3.25)$$

CVSS score вже розраховується як числова оцінка рівня критичності вразливості. Використання CVSS як ваги дозволяє автоматично враховувати серйозність кожної вразливості без необхідності додаткового масштабування. Вищий CVSS означає більшу критичність вразливості, тому її вплив на загальний рівень ризику має бути більшим. Наприклад, якщо є дві вразливості – одна з CVSS = 9.0, інша з CVSS = 4.0, то їх відносний вплив на ризик повинен бути пропорційним, що і забезпечує використання CVSS як ваги.

Якщо всі ваги рівні, то середнє зважене збігається з середнім арифметичним

$$\bar{x} = \frac{\sum_{i=1}^{n} k * x_i}{k * n} = \frac{\sum_{i=1}^{n} x_i}{n}, \quad (3.26)$$

де $x_i$ – значення елемента;

$k$ – вага елемента;

$n$ – кількість значень.

Ваговий коефіцієнт рівня критичності активу $W_i$ визначається на основі профілювання активів за типами та ранжуванням їх за важливістю для бізнес-процесів відносно шкали $W\epsilon[1,4]$. Такий підхід дозволяє врахувати потенційні наслідки та критичність настання інцидентів ІБ відносно категорії активу та ступеню його пріоритетності для інфраструктури.

Коефіцієнт β призначений для адаптивного та гнучкого корегування показника ризику для конкретного об'єкту у разі необхідності. Враховуючи наявність механізму врахування ретроспективних показників по активу це може бути корисним в умовах практичної експлуатації в корпоративних системах.

Таким чином, можна фіналізувати математичне представлення запропонованого методу із врахуванням всіх вищеописаних рекомендацій.

$$R_{Scaled} = \mu \cdot \frac{\frac{1}{K}\cdot\sum_{i=1}^{K}\sigma_i\cdot R_i(t)+\alpha\cdot R_{old}}{1+\alpha} \cdot \frac{\sum_{j=1}^{N} CVSS_j{}^2}{2\cdot\sum_{j=1}^{N} CVSS_j} \cdot W_i + \beta, \qquad (3.27)$$

де $\mu$ – коефіцієнт встановлення шкали оцінювання;

Основні аргументи запропонованого методу вносять рівнозважений вклад в кінцевий показник ризику. Оцінивши їх порогові значення можна констатувати, що запропонований підхід за замовчуванням надає 100-бальну шкалу оцінювання ризиків ІБ, проте вона може бути гнучко налаштована за допомогою коефіцієнту $\mu$ відповідно до пріоритетів та потреб ризик-менеджменту.

Проте запропонований варіант обрахунку має ряд недоліків, пов'язаних в першу чергу з двома ключовими аспектами – суттєвий вплив рівня критичності $W_i$ на кінцевий показник рівня ризику, та значний дисбаланс шкали оцінювання за рахунок нелінійного мультиплікативного зростання результуючого показника внаслідок операції добутку між основними аргументами (результати проєктованих моделей, кумулятивний показник оцінки вразливостей за шкалою CVSS та безпосередньо рівень критичності $W_i$ ). Описану проблему пропонується вирішити шляхом

застосування логарифмічної трансформації для нормалізації та масштабування результату до шкали оцінювання [0,100].

$$R_{normalized} = \frac{\log(a \cdot b)}{\log(100)} \cdot 100, \quad (3.28)$$

де $\log(100) \approx 2$.

Така трансформація передбачає зміну діапазонів можливих значень для основних аргументів математичного представлення до розмірності [0,10] (в тому числі шляхом введення додаткового коефіцієнту 2 для результуючого консолідованого аргументу оцінки проєктованих моделей), а також корегування можливих значень рівня критичності $W_i$ до діапазону [0, 1].

Аналіз граничних значень та балансу показників кінцевої шкали при різних варіаціях основних аргументів обрахунку (без врахування внеску додаткових параметрів $W_i$ та $\beta$) відповідно до підходу запропонованого в 3.28 наведено в Таблиці 3.4.

Запропонована шкала оцінювання демонструє нелінійне зростання нормалізованого результату в діапазоні від 0 до 100 зі збільшенням значень вхідних аргументів логарифмічної функції.

*Таблиця 3.4*

*Динаміка значень результуючого показника шкали оцінювання для логарифмічної трансформації (без врахування додаткових параметрів)*

| **a** | **b** | **Нормалізований результат** |
|---|---|---|
| 1 | 1 | 0 |
| 2 | 2 | 30.1 |
| 3 | 3 | 47.7 |
| 4 | 4 | 60.2 |
| 5 | 5 | 69.8 |
| 6 | 6 | 77.8 |
| 7 | 7 | 84.5 |
| 8 | 8 | 90.3 |
| 9 | 9 | 95.4 |
| 10 | 10 | 100 |

Із врахуванням нормалізації та корегування шкали кількісної оцінки кінцевий варіант математичного представлення рекомендований до впровадження набуде вигляду, представленого формулою 3.29.

$$R_{Normalized} = \mu \cdot \left[ \frac{\log\left( \frac{2 \cdot \left[ \frac{1}{K} \cdot \sum_{i=1}^{K} [\sigma_i \cdot R_i(t)] + \alpha \cdot R_{old} \right]}{1+\alpha} \cdot \frac{\sum_{j=1}^{N} CVSS_j^{\,2}}{\sum_{j=1}^{N} CVSS_j} \right)}{\log(100)} \cdot 100 \right] \cdot W_i + \beta, \qquad (3.29)$$

Відповідно до фінальної математичної інтерпретації описаного підходу можна запропонувати наступні значення вагового коефіцієнту рівня критичності активу $W_i$ – Таблиця 3.5.

*Таблиця 3.5*

*Профілювання IT-активів за рівнем критичності*

| **Рівень критичності** | **$W_i$** | **Приклад** |
|---|---|---|
| Низький | 0.7 | Пристрої системи корпоративного відео-спостереження та IP-телефонії, принтери / сканери / багатофункціональні пристрої / IoT тощо |
| Середній | 0.8 | Робочі станції / персональні комп'ютери, ноутбуки, планшети, тонкі клієнти, моноблоки, мережеве обладнання тощо |
| Високий | 0.9 | Фізичні та віртуальні сервери, бази даних тощо |
| Критичний | 1 | Касові апарати, платіжні POS-термінали, реєстратори розрахункових операцій (РРО) тощо |

Зниження рівня критичності для активу, в свою чергу, буде додатково збалансовувати та знижати результуючий показник комплексного оцінювання ризику відповідно до запропонованої шкали.

Як варіант модифікації розробленого адаптивного методу комплексного кількісного оцінювання ризиків для врахування впливу наявних вразливостей, як альтернативу, можна запропонувати використання CVSS Severity замість показника CVSS Score, що також буде методологічно правильним та дозволить узгодити шкалу оцінки вразливостей із результатами досліджуваних нейромережевих моделей.

Таким чином, описаний підхід дозволяє комплексно та методологічно обґрунтовано оцінити ризики кібербезпеки у розподілених системах на основі врахування результатів комплексу моделей оцінювання та ряду безпекових показників, при цьому забезпечуючи гнучкість та адаптивність налаштування, оперативність аналізу та можливість легкої практичної імплементації.

### 3.5. Висновки до розділу 3

Третій розділ присвячено проєктуванню та побудові комплексу моделей оцінювання ризику в РІС на основі контролю відповідності вимогам провідних стандартів кібербезпеки із застосуванням алгоритмів машинного навчання та глибоких нейронних мереж. Запропонований підхід забезпечує можливість гнучкої перевірки та контролю безпекової ситуації компанії в розрізі відповідності регулюючим нормативно-правовим документам та стандартам ІБ, та адаптивного кількісного підходу до оцінювання рівня ризику кібербезпеки в розподіленому середовищі, що поєднує переваги комплексного метрико-орієнтовного та стандарт-орієнтованого підходів.

В результаті проведеного дослідження та емпіричної перевірки запропонованого інструментарію було вирішено наступні завдання:

1. **Узагальнено теоретико-методологічні основи застосування алгоритмів ML та ANN** для вирішення задач підвищення ефективності процесу ризик-менеджменту в РІС, здійснено SWOT-аналіз основних підходів до моделювання на основі алгоритмів машинного навчання та порівняльний аналіз програмних фреймворків, в результаті чого обрано необхідний інструментарій для проведення емпіричного дослідження.

2. В рамках запропонованого підходу **вперше здійснено аналіз та формалізацію технологічних актив-орієнтованих вимог та контролів безпеки** провідних міжнародних та національних стандартів ІБ (ISO 27001, ISO 27002, PCI DSS v4, SWIFT, NBU-95), як багатовимірних вхідних метрик, сумісних з інструментами машинного навчання, що дозволяє врахувати кращі світові практики, забезпечити інтероперабельність, масштабованість та відповідність вимогам регуляторів, а також сприяє підвищенню зрілості процесів кібербезпеки. Відбір ключових асет-орієнтовних контролів та їх формалізація як вхідних параметрів проєктованих моделей забезпечила можливість в подальшому провести моделювання та перевірку ефективності алгоритмів машинного навчання в задачах оцінювання ризику розподіленого середовища.

3. **Розроблено комплекс моделей оцінювання ризику в РІС** на основі класичних алгоритмів машинного навчання та інструментарію глибоких нейронних мереж, емпірично досліджено їх якісні показники та ефективність в задачах аналізу даних відповідності вимогам стандартів. Емпірично доведено найвищі показники точності для глибоких нейронних мереж та LDA серед усіх досліджуваних алгоритмів при вирішенні задачі класифікації та аналізу ризиків розподіленого середовища. Моделі із 3 прихованими шарами прогнозовано продемонстрували найкращу ефективність для 3 з 4 досліджуваних наборів даних із середнім рівнем точності на рівні 90,75%. Доведено, що ускладнення архітектури багатошарового перцептрону та збільшення кількості прихованих шарів позитивно впливає на продуктивність проєктованих моделей.

4. **Розроблено адаптивний метод комплексного кількісного оцінювання** ризиків кібербезпеки в РІС з використанням спроєктованих моделей, що забезпечує гнучкий підхід до оцінювання розподілених ризиків та просту практичну імплементацію в системи корпоративної безпеки та програмні продукти ІБ.

Практична орієнтація запропонованого підходу до оцінювання ризиків в РІС створює передумови для ефективного впровадження та імплементації розробленого інструментарію в корпоративні рішення із забезпечення інформаційної безпеки та системи підтримки прийняття рішень (СППР), що відкриває широкі можливості для комплексного впровадження інтелектуальних систем управління інформаційною безпекою.

# ВИСНОВКИ

Дисертаційна робота присвячена вирішенню актуального **науково-прикладного завдання**, яке полягає в підвищенні ефективності процесу оцінювання ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем, та розробці відповідного науково-методичного апарату, що побудований на принципах комплексного аналізу безпекової ситуації РІС на основі синтезу метрико-орієнтованого та стандарт-орієнтованого підходів та використання парадигми нейронних мереж і машинного навчання, що на відміну від класичних методів враховує динамічний характер розподіленого середовища, та надає можливість автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

В рамках проведеного дослідження здійснено комплексний порівняльний аналіз сучасних підходів та методологій оцінювання ризиків кібербезпеки у розподілених системах, визначено їх недоліки і наявні прогалини в теорії та практиці управління ризиками, а також підкреслено науково-прикладну **актуальність подальших досліджень**, що визначається нагальною потребою у побудові комплексних методологічних та технологічних рішень для оцінювання ризиків кібербезпеки в РІС (з урахуванням специфіки функціонування динамічних розподілених середовищ), що здатні підвищити ефективність, точність та адаптивність аналізу, покращуючи здатність до протидії сучасним кіберзагрозам та забезпечуючи безперервне підвищення зрілості у сфері ІБ та сталий розвиток у цифровому середовищі.

Запропонований комплексний підхід до багатофакторного аналізу великих масивів складних і значною мірою диференційованих гетерогенних даних та безпекових метрик про стан інформаційних активів інфраструктури РІС, агрегованих в процесі їх моніторингу, з однієї сторони, та показників контролю відповідності нормативно-правовій базі і вимогам провідних стандартів ІБ з іншої, із застосуванням алгоритмів машинного навчання та інструментарію глибоких нейронних мереж дозволяє покращити точність і надійність оцінювання кіберризиків в розподіленому середовищі і сприяє підвищенню ефективності процесу ризик-менеджменту в цілому, забезпечує можливість вивчення, аналізу, моніторингу та прогнозування потенційних

загроз, а також своєчасного впровадженню економічно доцільних технічних та організаційних мір безпеки, та оцінювання ефективності вже існуючих заходів ІБ.

Відповідно до поставленої мети та сформульованих задач дослідження отримано **наступні наукові результати**:

1. На основі проведеного комплексного аналізу публікацій в предметній області, провідних стандартів ІБ, сучасних підходів і методологій оцінювання ризиків інформаційної безпеки, виявлено суттєві обмеження традиційних методів в умовах динамічного середовища РІС, що полягають в першу чергу в загальних та концептуальних аспектах оцінювання, браку узгодженості між різними підходами та суб'єктивності результатів, а також недостатній гнучкості, адаптивності та оперативності аналізу, що вимагається в умовах функціонування сучасних РІС. Відсутність універсальних та ефективних підходів до оцінювання ризиків в динамічних та масштабованих розподілених системах доводять актуальність обраного наукового завдання.

2. Вдосконалено метод побудови профілю ключових факторів ризику сучасних РІС за допомогою методів математичної статистики, проведено кореляційний аналіз та моделювання їх взаємозв'язків, а також визначено та структуровано основні заходи та контролі інформаційної безпеки, які демонструють найкращі показники ефективності в умовах розподіленості середовища, враховують як технологічні, так і організаційні аспекти, забезпечуючи системний підхід до управління ризиками ІБ, зменшення впливу загроз і підвищення стійкості розподілених систем до можливих атак. У ході дослідження здійснено аналіз та ієрархічне впорядкування 40 основних факторів ризику, характерних для типової розподіленої інформаційної системи, та 14 категорій контролів безпеки, оцінених за критеріями їх значущості та частоти виникнення у практичних сценаріях. Запропонований підхід до оптимізації вибору вхідного набору ознак та виокремлення найбільш вагомих факторів ризику, побудований на основі розробленого профілю ключових факторів ризику для сучасних РІС, продемонстрував тотожні результати щодо кількості відібраних метрик у порівнянні з факторним аналізом за допомогою методу головних компонент – 42 метрики у порівнянні із 40 для PCA. Водночас, розроблений підхід забезпечив

покращення загальних показників точності класифікації для проєктованих моделей оцінювання ризику кібербезпеки в РІС на 4% у порівнянні з контрольною моделлю, що використовувала метод головних компонент (PCA) у якості підходу до факторного аналізу, що підтверджує його ефективність у контексті адаптивного аналізу ризиків у розподілених середовищах.

3. Проведено аналіз теоретико-методологічних принципів застосування алгоритмів інтелектуального аналізу даних, машинного навчання та глибоких нейронних мереж для вирішення задач підвищення ефективності процесу оцінювання ризиків кібербезпеки в розподілених системах та покращення точності прийнятих управлінських рішень. Здійснено SWOT-аналіз основних підходів до моделювання на основі алгоритмів машинного навчання та порівняльний аналіз програмних фреймворків, в результаті чого обрано необхідний інструментарій для проведення емпіричної частини дослідження. Для практичної імплементації розроблених моделей використано засоби програмного фреймворку TensorFlow та бібліотеки scikit-learn.

4. Обґрунтовано концептуальну методику оцінювання ризиків ІБ в умовах розподілених інформаційних систем із врахуванням комплексного підходу, що на відміну від існуючих методів поєднує аспекти оцінки контролю відповідності нормативно-правовій базі і вимогам провідних стандартів ІБ, та метрико-орієнтований підхід на основі інтелектуального аналізу великих обсягів гетерогенних параметрів про стан інфраструктури РІС, з метою побудови гнучких та адаптивних рішень для управління інформаційною безпекою корпоративного середовища.

5. Розроблено комплекс моделей оцінювання ризиків ІБ в розподілених інформаційних системах на основі класичних алгоритмів машинного навчання та глибоких нейронних мереж з кращими показниками зважених середніх значень точності, F1-міри та AUC-ROC, проведено порівняння їх ефективності та якісних характеристик при вирішенні задач класифікації, в тому числі в залежності від ступеня інформаційної наповненості та міри повноти вхідних даних, що демонструє здатність запропонованих моделей багатокритеріального аналізу гетерогенних даних розподіленого середовища до масштабування та адаптації під різноманітні топології РІС та динамічні умови розподіленого середовища. Емпірично доведено ефективність

використання парадигми глибоких нейронних мереж в задачах машинного аналізу ключових індикаторів безпеки розподіленого середовища з метою оцінювання ризиків кібербезпеки в умовах динамічного середовища PIC (точність на рівні 94% для метрико-орієнтованого підходу, та 90,75% для контроль-орієнтованого підходу). Встановлено закономірність підвищення точності та стабільності моделей зі збільшенням складності їх архітектури та кількості прихованих шарів. Зокрема, на всіх досліджуваних наборах даних тришарова архітектура демонструвала перевагу за ключовими критеріями продуктивності, що свідчить про доцільність використання такого підходу для підвищення ефективності оцінювання ризиків кібербезпеки в розподілених системах. Окрім цього, емпірично доведено, що ключовим фактором, що визначає точність моделей, є розмір навчальної вибірки. Для розширеного набору даних $D_{ext}$ (45,24% наповненості) з кількістю незаповнених метрик до 23 включно ($M_i \leq 23$) та зниженням розміру датасету з 219884 записів до 173103 – падіння загальної точності моделі з тришаровою архітектурою склало лише 0,5%, при цьому кінцевий показник точності залишався високим – 93,89%. Для найбільш концентрованого набору даних $D_{core}$ (54,76% наповненості) з кількістю незаповнених метрик до 19 включно ($M_i \leq 19$) та скороченням вибірки з 219884 записів до 86660 – падіння середньої точності моделі з тришаровою архітектурою становило 2.02% із загальним показником в 92.37% за результатами крос-валідації. Спостерігається закономірна тенденція до зниження ефективності класифікаційних моделей зі зменшенням обсягу тренувального датасету, тоді як рівень його наповненості відіграє другорядну роль. Окрім цього, емпірично доведено найвищі показники точності для глибоких нейронних мереж серед усіх досліджуваних алгоритмів машинного навчання при вирішенні задач класифікації ризиків розподіленого середовища на основі аналізу даних відповідності вимогам провідних стандартів ІБ. Моделі із 3 прихованими шарами прогнозовано продемонстрували найкращу ефективність із середнім показником точності на рівні 90,75% для 3 з 4 досліджуваних наборів даних, що репрезентують контролі для основних регулюючих документів.

6. Досліджено ефективність ряду підходів з підвищення точності побудованих моделей, в тому числі для вирішення проблем якості і повноти вхідних даних, а також

усунення дисбалансу цільових класів, із використанням вагових коефіцієнтів і технік оверсемплінгу навчальної вибірки за допомогою методів SMOTE та ADASYN, що покращує стійкість проєктованих моделей і підвищує достовірність результатів класифікації рівнів ризику, забезпечуючи ефективну обробку погано структурованих, значною мірою фрагментованих та неповних даних. Емпірично доведено ефективність технік оверсемплінгу, зокрема на основі методу SMOTE, для покращення інтерпретації моделлю слабко представлених класів цільової метрики рівня ризику. Хоча загальний показник точності моделі залишився на рівні 94% за результатами крос-валідації (k-fold=5), аналіз матриць невідповідності та ключових критеріїв оцінювання ефективності для окремих класів засвідчив суттєве покращення здатності моделі до ідентифікації слабо представлених, проте критично важливих у контексті предметної області класів ризику $R_3$ та $R_4$, що відповідно репрезентують значення рівнів ризику «високий» та «критичний».

7. В рамках запропонованого підходу вперше здійснено аналіз та формалізацію технологічних актив-орієнтованих вимог та контролів безпеки провідних міжнародних та національних стандартів ІБ (ISO 27001, ISO 27002, PCI DSS v4, SWIFT, NBU-95), як багатовимірних вхідних метрик, сумісних з інструментами машинного навчання, що дозволяє врахувати кращі світові практики, забезпечити інтероперабельність, масштабованість та відповідність вимогам регуляторів, а також сприяє підвищенню зрілості процесів кібербезпеки. Відбір ключових асет-орієнтованих контролів та їх формалізація у вигляді вхідних параметрів для спроєктованих моделей створили основу для подальшого моделювання та оцінки ефективності алгоритмів машинного навчання у вирішенні задач оцінювання ризику в розподіленому середовищі. Емпірична перевірка запропонованого підходу у рамках експериментальних досліджень підтвердила його здатність адаптивно оцінювати рівень ризику в умовах динамічних змін інформаційної інфраструктури, що є критично важливим для ефективного управління безпекою сучасних РІС.

8. Вперше розроблено універсальний адаптивний метод комплексного кількісного оцінювання ризиків кібербезпеки в РІС з використанням спроєктованих моделей та загальної системи оцінки вразливостей, що на відміну від класичного

підходу враховує динамічний характер розподіленого середовища, забезпечує гнучкий підхід до оцінювання розподілених ризиків та просту практичну імплементацію, а також дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних. Запропонований метод дозволяє комплексно врахувати результати оцінки на основі спроєктованих моделей та пропонує ряд додаткових параметрів обрахунку кінцевого показника, до яких можна віднести критичність активу, перелік та рівень задетектованих вразливостей, ступінь врахування ретроспективних даних, а також додаткові коефіцієнти балансування. Запропонований підхід дозволяє підвищити ефективність оцінювання ризиків кібербезпеки в сучасних розподілених системах.

Таким чином, мета досліджень щодо підвищення ефективності процесу оцінювання ризиків в умовах сучасних масштабованих розподілених систем та побудови комплексних методологічних і технологічних рішень для оцінювання ризиків кібербезпеки в РІС з урахуванням специфіки функціонування динамічних розподілених середовищ, та всі поставлені завдання **вирішені в повному обсязі**.

Напрямками подальших досліджень є підвищення ефективності та вдосконалення спроєктованого комплексу нейромережевих моделей оцінювання ризику на основі інтелектуального аналізу гетерогенних даних про стан інфраструктури РІС, розширення переліку підтримуваних стандартів (наприклад NIST SP 800-30), впровадження додаткових механізмів підвищення інтерпретованості результатів, а також подальша інтеграція та практична імплементація описаного підходу кількісної оцінки в рамках існуючих програмних рішень забезпечення ІБ.

Результати дисертаційної роботи мають наукову та практичну цінність, апробовані та прийняті до впровадження у діяльність ТОВ «ІТ СПЕЦІАЛІСТ» (акт впровадження результатів дослідження від 13.02.2025 р.) та ТОВ «АПІ Коннект» (акт впровадження результатів дослідження від 13.02.2025 р.), а також, окрім цього, знайшли своє відображення та практичне застосування при розробці програмних продуктів **ITS Inventory**, **ITS Cybersecurity Awareness Tracker (ITS CSAT)**, **ITS Incident Management та ITS Compliance and Risk Management**.

Дисертаційне дослідження виконано відповідно до поточних та перспективних планів науково-дослідної діяльності кафедри кібербезпеки та захисту інформації, факультету інформаційних технологій Київського національного університету імені Тараса Шевченка та знайшли застосування в рамках науково-дослідних робіт: «Дослідження та розробка моделей, методів і засобів захисту від кібератак в інформаційних системах та мережах» №16 КП 064-03 (номер державної реєстрації НДР: 0116U007996), «Методи та моделі захисту персональних даних з урахуванням специфіки соціальних мереж» (номер державної реєстрації НДР: 0121U113248).

**Практичне значення отриманих результатів** полягає в реалізації цілісного та системного підходу до оцінювання ризиків кібербезпеки у РІС шляхом побудови комплексу моделей оцінювання ризику на основі алгоритмів машинного навчання та інструментарію глибоких нейронних мереж, що враховують особливості предметної області та надають ряд переваг у порівнянні з класичними підходами до аналізу ризиків ІБ в умовах розподілених інформаційних систем, а також розробки адаптивного методу комплексної кількісної оцінки ризиків кібербезпеки в РІС з використанням спроєктованих моделей, що забезпечує гнучкий підхід до оцінювання розподілених ризиків, просту практичну імплементацію в програмні продукти ІБ та системи корпоративної безпеки, а також відкриває можливості для комплексного впровадження інтелектуальних систем управління інформаційною безпекою.

Запропонований підхід на основі багатофакторного нейромережевого аналізу універсальних стандартизованих метрик та індикаторів безпеки розподілених систем, що враховує не лише технічні аспекти функціонування сучасних розподілених інфраструктур, а й показники відповідності вимогам регуляторів, дозволяє забезпечити комплексний, гнучкий та адаптивний аналіз безпекової ситуації, надає високий рівень точності, полегшує виявлення критичних прогалин в системах захисту та сприяє підвищенню ефективності процесів управління інформаційною безпекою та ризик-менеджменту в РІС. Це, в свою чергу, спрощує процеси аудиту ІБ, а також дозволяє організаціям оперативно розподіляти обмежені ресурси, забезпечувати пріоритетність заходів з посилення безпеки та приймати обґрунтовані управлінські рішення в режимі реального часу, що особливо актуально в умовах воєнного стану.

Розроблені моделі можуть бути рекомендовані для використання в розподілених інформаційних системах різної складності та масштабу для комплексного аналізу ризиків ІБ, а також оцінки ефективності наявних систем захисту та впроваджених заходів кібербезпеки. Результати дослідження демонструють здатність розроблених моделей до масштабування та адаптації під різні топології розподілених інформаційних систем, що забезпечує їх ефективне застосування в неоднорідних інфраструктурах та динамічних умовах середовища функціонування. Запропонований підхід дозволяє автоматизувати процеси моніторингу, аналізу та прогнозування кіберзагроз, що значно спрощує аудит систем безпеки та підвищує загальний рівень кіберзахищеності організації.

Таким чином, практичне значення розроблених рішень полягає у створенні необхідних передумов для практичної імплементації і впровадження описаних механізмів комплексного, масштабованого та динамічного оцінювання ризиків кібербезпеки в розподілених інформаційних системах. Практичне застосування результатів дослідження можливе у вигляді прикладних програмних модулів та систем підтримки прийняття рішень (СППР), що автоматично формують інтегральні показники ризику, виявляють приховані закономірності та аномалії, і як результат пропонують оптимальні стратегії зниження ризиків. Впровадження цих механізмів у засоби корпоративної безпеки, системи SIEM та SoC (Security Information and Event Management / Security Operations Center) дозволить суттєво розширити функціональні можливості сучасних платформ кіберзахисту, забезпечуючи ефективне виявлення, аналіз та попередження кіберзагроз у розподілених інформаційних системах. Це сприятиме підвищенню рівня кіберстійкості організацій, оптимізації процесів управління безпекою та впровадженню сучасних адаптивних підходів до захисту розподілених систем.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Measuring digital development: Facts and Figures 2024 [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://www.itu.int/itu-d/reports/statistics/facts-figures-2024.

2. DIGITAL 2023: GLOBAL OVERVIEW REPORT [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://datareportal.com/reports/digital-2023-global-overview-report.

3. Andrew S. Tanenbaum, Maarten Van Steen A brief introduction to distributed systems. / Computing, Vol. 98, No. 10, 2016, p. 967-1009 https://doi.org/10.1007/s00607-016-0508-7

4. Andrew S. Tanenbaum, Maarten Van Steen Distributed Systems: Principles and Paradigms, Prentice Hall of India; 2nd edition (January 1, 2007)

5. Andrew S. Tanenbaum, Maarten Van Steen Distributed systems, CreateSpace Independent Publishing Platform, 2017 p. 298-303.

6. Chandy, K. Mani, and Leslie Lamport. "Distributed snapshots: Determining global states of distributed systems." ACM Transactions on Computer Systems (TOCS) 3, no. 1, 1985, p. 63-75.

7. Leslie Lamport. Time, clocks, and the ordering of events in a distributed system. Concurrency: the Works of Leslie Lamport, 2019, p. 179-196.

8. Lynch, N. A. "Distributed Algorithms." (1996).

9. George Coulouris, Jean Dollimore, Tim Kindberg, Distributed systems : concepts and design / Wokingham; Sydney : Addison-Wesley (1994).

10. Kenneth Birman. Reliable distributed systems: technologies, web services, and applications. Springer Science & Business Media, 2006.

11. Kenneth P. Birman, and Thomas A. Joseph. Reliable communication in the presence of failures. ACM Transactions on Computer Systems (TOCS) 5.1 (1987): p. 47-76.

12. Kenneth P. Birman. The process group approach to reliable distributed computing. Communications of the ACM 36.12 (1993): p. 37-53.

13. Ross J. Anderson, Security engineering: a guide to building dependable distributed systems. John Wiley & Sons, 2010.

14. Neuman, B. Clifford. Proxy-based authorization and accounting for distributed systems. Proceedings. The 13th International Conference on Distributed Computing Systems. IEEE, 1993.

15. Neuman, B. Clifford. Scale in distributed systems. Readings in distributed computing systems, 1994.

16. Neuman, B. Clifford, and Santosh Rao. Resource management for distributed parallel systems. Proceedings The 2nd International Symposium on High Performance Distributed Computing. IEEE, 1993.

17. The Digitization of the World – From Edge to Core 2025. IDC White Paper [Електронний ресурс]. – Режим доступу до ресурсу: https://www.seagate.com/files/www-content/our-story/trends/files/dataage-idc-report-final.pdf

18. Машков О.А., Барабаш О.В. Топологічні критерії та показники функціональної стійкості складних ієрархічних систем / Збірник наукових праць НАН України, ІПМЕ – «Моделювання та інформаційні технології», 2003, Вип.. 25, с. 29-35.

19. Машков О.А., Дурняк Б.В., Усаченко Л.М., Сабат В.И. Методологія забезпечення функціональної стійкості ієрархічних організаційних систем управління / Збірник наукових праць: Інститут проблем моделювання в енергетиці, НАН України, вип. 48, 2008, с. 3-21.

20. Машков О.А., Коробчинський М.В., Косенко В.Р., Дурняк Б.В., Білак Ю.Ю. Застосування неформальних підходів до управління складними динамічними системами / Збірник наукових праць / Інститут проблем моделювання в енергетиці НАН України, вип. 60, Київ, 2011, с. 3-16.

21. Барабаш О.В. Забезпечення функціональної стійкості складних технічних систем / О.В. Барабаш, Б.В. Дурняк, О.А. Машков, Д.М. Обідін // Моделювання та інформаційні технології: Зб. наук. пр. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2012. – Вип. 64. – С. 36 – 41.

22. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. "Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки." (2018).

23. Герасимов, І.Ю. Субач, П.В. Хусаінов, В.О. Міщенко. Аналіз задач моніторингу інформаційних мереж та методів підвищення ефективності їх функціонування. // Сучасні інформаційні технології у сфері безпеки та оборони, 2008. − № 3 (3). – С. 24 − 27.

24. Лукова-Чуйко Н.В. Забезпечення функціональної стійкості інформаційних мереж на основі розробки методу протидії DDoS-атакам / О. В. Барабаш, Н. В. Лукова-Чуйко, А. П. Мусієнко, В. В. Собчук // Сучасні інформаційні системи. – 2018. –Т 2, № 1– С. 56 – 64.

25. Барабаш О.В. Побудова структури мережі передачі даних за критерієм максимуму функціональної стійкості // Проблеми інформатизації та управління: Збірник наукових праць.–К.: Національний авіаційний університет, 2003.–Вип.8. – С. 66-71.

26. Барабаш О.В. Построение функционально устойчивых распределенных информационных систем – К.: НАОУ, 2004. – 226 с. 54.

27. Кравченко Ю.В., Барабаш О.В. Функціональна стійкість – властивість складних технічних систем. Збірник наукових праць НАОУ. Бюл. №40. –К.: НАОУ, 2002. – С. 225 – 229.

28. Лукова-Чуйко Н.В. Подход к классификации состояния сети на основе статистических параметров для обнаружения аномалий в информационной структуре вычислительной системы / И.В. Рубан, В.А. Мартовицкий, Н.В. Лукова-Чуйко // Кибернетика и системный анализ. – 2018. – Том 54, № 2. – С. 142 – 150.

29. Лукова-Чуйко Н. В. Математична модель взаємовідносин загроз та комплексних систем захисту інформації / Н.В. Лукова-Чуйко // Вісник інженерної академії України. – № 3. – 2015 р. – С. 131–135.

30. Лукова-Чуйко Н.В. Застосування теорії нечітких множин для формалізації задачі оцінки рівня захищеності інформації // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави»: Зб. мат. наук.-практ. конф. студ., асп., викл. та науковців – 18 грудня, Київ, ДУТ, 2014. – С. 5.

31. Lukova-Chuiko N. Application game theory in constructing the mathematical model of threats and complex systems of information security / N. Lukova-Chuiko, Sergii Toliupa

// International Scientific and Practical Conference «WORLD SCIENCE». — ISSN 2413-1032.–№ 4(4), Vol.4. – 2015. – P. 12-15.

32. Лукова-Чуйко Н.В. Недоліки та переваги систем виявлення мережевих вторгнень і ознак кібератак на основі сигнатурного аналізу / С.В. Толюпа, Н.В. Лукова-Чуйко // Збірник наукових праць І Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційнотелекомунікаційних систем», 5-6 квітня 2018 р., м. Київ – С. 332-340.

33. Рубан І.В. Аналіз кібернетичних атак як істотних загроз інформаційній безпеці / І.В. Рубан, Є.С. Лошаков, Д.В. Прибильнов, О.П. Давікоза // Системи управління, навігації та зв'язку. – 2012. – № 4(24). – С. 102 – 105.

34. The State of Cybersecurity 2024 Report, Global Update on Workforce Efforts, Resources and Cyberoperations. ISACA [Електронний ресурс]. – Режим доступу до ресурсу: https://www.isaca.org/resources/reports/state-of-cybersecurity-2024

35. Cybersecurity Assessment Report 2024. Bitdefender [Електронний ресурс]. – Режим доступу до ресурсу: https://www.bitdefender.com/content/dam/bitdefender /business/campaign/2024-Assessment-Report.pdf

36. V. Zaslavsky, V. Ievgiienko Risk analyses and redundancy for protection of critical infrastructure. // Monographs of System Dependability, Oficyna Widawnicza Politechniki Wroclawskiej, Wroclaw, Poland, 2010, p. 161-173

37. Заславський В.А. Принцип разнотипности и проблемы обеспечения надежности сложных систем с высокой ценой отказа. // Радіоелектронні і комп'ютерні системи, Науково–технічний журнал, 2008, №6, с. 76-78

38. Zaslavskyi, V. (2017). System principles, mathematical models and methods to ensure high reliability of safety systems. Proceedings of SPIE, 10418, 1041803.

39. Norkin, V.I.; Gaivoronski, A.A.; Zaslavsky, V.A.; Knopov, P.S. Models of the Optimal Resource Allocation for the Critical Infrastructure Protection. Cybern. Syst. Anal. 2018, 54, 696–706.

40. Архипов А. Е. Экспертно-аналитическое оценивание информационных рисков и уровня эффективности системы защиты информации / А. Е. Архипов // «Радіоелектроніка. Інформатика. Управління». – 2009. – № 2. – С. 111 – 115.

41. Мохор В. В. Построение оценок рисков безопасности информации на основе динамического множества актуальных угроз / В. В. Мохор, А. М. Богданов, О. Н. Крук, В. В. Цуркан // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2010. – Вип. 56. – С. 87 – 99.

42. Замула О. А. Аналітичний підхід в методології оцінювання та управління ризиками інформаційної безпеки / О. А. Замула, Б. В. Волобуєв, В. І. Черниш, К. І. Іванов // Восточно-Европейский журнал передовых технологий. – 2011. – № 5/2 (53). – С. 19 – 22.

43. Качинський А. Б. Безпека загрози і ризик: наукові концепції та математичні моделі / А. Б. Качинський. – К., 2003. – 472.

44. Юдін О. К. Захист інформації в мережах передачі даних / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. – К.: Вид.-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

45. Корченко А. Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов / А. Г. Корченко, В. П. Щербина, С. В. Казмірчук // Захист інформації. – 2012. – № 1. – С. 126–139.

46. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

47. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К.: МК – Пресс, 2006. – 320 с

48. О. Г. Корченко, С. В. Казмірчук, Б. Б. Ахметов. Прикладні системи оцінювання ризиків інформаційної безпеки. (2017).

49. Цуркан В. В. Атестування ризику безпеки інформації в організаційно технічних системах об’єктів інформаційної діяльності / В. В. Мохор, В. В. Цуркан // Безопасность информации в информационно-телекоммуникационных системах (18-21 мая 2010 г.): XIII межд. науч.-практ. конф.: тезисы докл. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2010. – С. 106.

50. Потій О. В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу / О. В. Потій, А. В. Лєншин // Збірник наукових праць Харківського університету Повітряних Сил. – Харків, ХУПС, 2010. – № 2(24). – С. 85 – 91.

51. Хорошко В. О. Методика кількісно-якісного аналізу та визначення рівня інформаційної безпеки / В. О. Хорошко, В. С. Чередниченко // Інформаційні технології та комп'ютерна інженерія. – 2008. – № 3 (13). – С. 49 – 57.

52. Широчин В. П. Анализ рисков в задачах мониторинга безопасности компьютерных систем и сетей / В. П. Широчин, В. Е. Мухин, Д. И. Крамар // Захист інформації. – 2003. – № 1. – С. 28–34.

53. Henry K. Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton: Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321-329.

54. Rot A. IT Risk Assessment: Quantitative and Qualitative Approach // Proceedings of the World Congress on Engineering and Computer Science, 2008. – p. 1073-1078.

55. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2016. – 504 p.

56. James J. Cebula A Taxonomy of Operational Cyber Security Risks / James J. Cebula, Lisa R. Young. – Hanscom AFB, MA: Carnegie Mellon University. – 47 p.

57. National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

58. ISO/IEC 27001:2022. Information technology - Security techniques - Information security management systems - Requirements. 2022.

59. ISO/IEC 27002:2022. Information technology - Security techniques - Code of practice for information security controls. 2022

60. ISO/IEC 27005:2022. Information technology - Security techniques - Information security risk management. 2022.

61. Palko, D.; Babenko, T.; Bigdan, A.; Kiktev, N.; Hutsol, T.; Kuboń, M.; Hnatiienko, H.; Tabor, S.; Gorbovy, O.; Borusiewicz, A. Cyber Security Risk Modeling in Distributed Information Systems. Appl. Sci. 2023, 13, 2393. DOI: https://doi.org/10.3390/app13042393

62. Д.В. Палко, Л.В. Мирутенко «Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах», Кібербезпека: освіта, наука, техніка, Том 2 № 26 (2024), с. 487 – 502. DOI: https://doi.org/10.28925/2663-4023.2024.26.731

63. Д.В. Палко «Інтелектуальні моделі оцінки ризиків кібербезпеки в розподілених системах на основі нейромережевого підходу», Кібербезпека: освіта, наука, техніка, Том 3 № 27 (2025), с. 429 – 448. DOI: https://doi.org/10.28925/2663-4023.2025.27.764

64. Д.В. Палко, Л.В. Мирутенко «Метод побудови профілю ключових факторів ризику кібербезпеки сучасних розподілених інформаційних систем», Захист інформації, Том 26, № 2, липень-грудень 2024, с. 236 – 252. DOI: https://doi.org/10.18372/2410-7840.26.20014.

65. Д. Палко, Л. Мирутенко, О. Шайна «Протоколи безпеки в кіберфізичних системах», Безпека інформаційних систем і технологій («Information systems and technologies security»), № 2(8)/2024, с. 66 – 73. DOI: https://doi.org/10.17721/ISTS.2024.8.66-73

66. Д.В. Палко, Т.В. Бабенко, І.І. Пархоменко, Р.В. Зюбіна «Захист інформації та передачі даних в корпоративних мережах з використанням програмно-апаратних засобів», Вісник інженерної академії України випуск №3 – 2018, с. 68 – 72

67. Dmitry Palko, Tetiana Babenko, Larysa Myrutenko, Andrii Bigdan «Model of information security critical incident risk assessment» // Proceedings of the 2020 IEEE International Conference «Problems of infocommunications. Science and technology» PIC S&T′2020, pp. 157–161, 6-9 October 2020, Kharkiv, Ukraine DOI: https://doi.org/10.1109/PICST51311.2020.9468107

68. Dmytro Palko, Hrygorii Hnatienko, Tetiana Babenko, Andrii Bigdan «Determining Key Risks for Modern Distributed Information Systems» // IntSol-2021 Intelligent Solutions - CEUR Workshop Proceedings, Volume 3018, pp. 81–100, 28–30 September 2021, Kyiv, Ukraine

69. Dmytro Palko, Tetiana Babenko, Larysa Myrutenko, Andrii Bigdan «Intelligent risk assessment models in DIS based on the neural network approach» // IX International conference «Information Technology and Implementation (Satellite)» (IT&I-2022), ISBN 978-966-969-154-5 (e-book), pp. 118–120, 1 December, 2022, Kyiv, Ukraine

70. Dmytro Palko, Tetiana Babenko «Evaluation of key risk factors for modern distributed information systems» // V Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) 27-28 жовтня 2022 року

71. Dmytro Palko, Tetiana Babenko «Risk Assessment Driven Use Of Advanced Intelligent Solutions Approach In Modern Distributed Systems» // VI Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) 27 квітня 2023 року

72. Dmytro Palko, Tetiana Babenko, Hnatiienko Hryhorii, Larysa Myrutenko and Andrii Bigdan «Intelligent risk assessment models in distributed systems based on the neural network approach» // Next Generation Cybersecurity Systems and Applications NGSEC (NGSEC-2023) Conference Proceedings, 26-27 April, 2023, Kyiv, Ukraine

73. Dmytro Palko, Kateryna Mokliakova, Tetiana Babenko «Cybersecurity level assessment models» // Next Generation Cybersecurity Systems and Applications NGSEC (NGSEC-2023) Conference Proceedings, 26-27 April, 2023, Kyiv, Ukraine

74. Dmytro Palko, Vira Vialkova, Tetiana Babenko «Intellectual models for cyber security risk assessment» // Processing, transmission and security of information : Monografia. Tom 2. / Akademia Techniczno-Humanistyczna w Bielsku-Białej. –Bielsku-Biała : Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2019. – S. 284–288.

75. Д.В. Палко, Л.В. Мирутенко, В.І. Вялкова «Захист інформаційних ресурсів та транзакцій в корпоративних мережах» // І Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS), 5-6 квітня 2018 року, с. 268-272

76. Д. Палко, Т. Бабенко, Л. Мирутенко «Інтелектуальні моделі оцінки ризиків кібербезпеки» // III Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS). – 2020. – 4 с.

77. Д.В. Палко «Моделі інтелектуального аналізу кіберризиків у масштабованих розподілених середовищах» // VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем» (CPICS), 11 квітня 2025 року, – 4 с.

78. Бучик С.С., Шалаєв В.О. «Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем». Наукоємні технології 3 (2017): 215-225.

79. Jack Freund and Jack Jones. 2014. Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, USA.

80. A FAIR Framework for Effective Cyber Risk Management. The FAIR Institute. - January 3, 2025. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.fairinstitute.org/resources/a-fair-framework-for-effective-cyber-risk-management

81. FAIR Model Standard Artifact (V3.0). The FAIR Institute. - January 15, 2025. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.fairinstitute.org/ resources/fair-model-standard-artifact-v3.0

82. Cheimonidis P, Rantos K. Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. Future Internet. 2023; 15(10):324. https://doi.org/10.3390/fi15100324

83. A. Adebiyi, Johnnes Arreymbi and Chris Imafidon «Security Assessment of Software Design using Neural Network» // (IJARAI) International Journal of Advanced Research in Artificial Intelligence, Vol. 1, No. 4, 2012.

84. Бучик С. С. Методика оцінювання інформаційних ризиків в автоматизованій системі // С. С. Бучик, С. В. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир: ЖВІ ДУТ, 2015. – Вип. 11. – С. 33–43.

85. Risk analysis and risk management using MEHARI [Електронний ресурс] – Режим доступу до ресурсу: http://www.jabis.ro/2012/4/0304042012.pdf.

86. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process / Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. − Carnegie Mellon University, 2008. – 154 p.

87. A complete Information Risk Management solution For ISF Members using IRAM and STREAM [Електронний ресурс] // Jason Creasey, Simon Marvell – Режим доступу до ресурсу: https://acuitys3.s3.eu-west-2.amazonaws.com/s3fs-public/isf_congress_2013 _acuity_ jerakano_whitepaper_0_0.pdf.

88. А. Н. Новиков, А. Н. Родионов, А. А. Тимошенко Модели и методы кибернетической защиты информационно-коммуникационных систем на основе логико-вероятностного подхода: монография – К.: НТУУ "КПИ", 2015. – 274 с.

89. Ю. Геряк , А. Берко Система критеріїв оцінки якості даних у розподілених інформаційних системах / Вісник національного університету «Львівська політехніка», Інформаційні системи та мережі, SISN. 2024; Volume 16: pp. 191 - 202 https://doi.org/10.23939/sisn2024.16.191

90. Герасимов Б.М. Аналіз задач моніторингу інформаційних мереж та методів підвищення ефективності їх функціонування / Б.М. Герасимов Б.М., Дивизинюк М.М., И.Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. Севастополь: СНИЯЭиП. 2004.

91. Fatama Tuz Johora, Md Shahedul Islam Khan, Esrath Kanon, Mohammad Abu Tareq Rony, Md Zubair, Iqbal H Sarker A Data-Driven Predictive Analysis on Cyber Security Threats with Key Risk Factors, arXiv preprint arXiv:2404.00068, 2024 Mar 28.

92. State of Enterprise Risk Management 2020 Survey // ISACA, CMMI Institute. - 2019. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.isaca.org/-/media/info/state-of-enterprise-risk-management-survey/index.html

93. Haykin S. Neural networks / S. Haykin. − W.: Williams, 2006. − 1104 p. – Режим доступу до ресурсу: https://cours.etsmtl.ca/sys843/REFS/Books/ebook_Haykin09.pdf.

94. Rassel S. Artificial Intelligence: Modern approach / S. Rassel, P. Norvig. − W.: Williams, 2005. − 1424 p.

95. Zne Jung Lee, Zhao Yun Yang, Chou Yuan Lee, Zhi Hao Chen, Wen BingWu «Using improved neural network for the risk assessment of information security» // IOP Conference

Series Materials Science and Engineering 1113(1):012025, March 2021 DOI: 10.1088/1757-899X/1113/1/012025.

96. Sarker I. H. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective // SN Computer Science. - 2021. - Vol. 2. - №. 3. - p. 1-16.

97. Korneev, N.V.; Korneeva, J.V.; Yurkevichyus, S.P.; Bakhturin, G.I. An Approach to Risk Assessment and Threat Prediction for Complex Object Security Based on a Predicative Self-Configuring Neural System. Symmetry 2022, 14, 102.

98. Wilson A. C, Roelofs R., Stern M., Srebro N., Recht B. «The Marginal Value of Adaptive Gradient Methods in Machine Learning» // Proceedings of the 31st International Conference on Neural Information Processing Systems, pages 4151–4161, 2017.

99. Замула А. А., Черныш В. И., Землянко Ю. В. Математические методы оценивания информационных рисков компании. (2011)

100. Родін Є. С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки. Математические машины и системы, 1(4), 142-148. (2012)

101. Hnatiienko H., Hnatiienko O., Babenko T., Myrutenko L. Mathematical models and methods for decision coordination in critical infrastructure operations. (2024)

102. Zaslavskyi, Volodymyr A., and A. Horbunov. "The type-variety principle in ensuring the reliability, safety and resilience of critical infrastructures." Modern Optimization Methods for Decision Making Under Risk and Uncertainty. CRC Press, 2023. 245-274.

103. Мохор В. В., Гончар С. Ф. "Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури." Електронне моделювання 41.6 (2019): 65-76.

104. Мохор В. В., Гончар С. Ф., Дибач О. М. "Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури." Ядерна та радіаційна безпека 2 (2019): 4-8.

105. Мохор В. В., Гончар С. Ф. "Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури." Електронне моделювання 41.6 (2019): 65-76.

106. Гончар, С. Ф. "Моделі та метод оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури." // Актуальні питання

забезпечення кібербезпеки та захисту інформації, Київ, Лютий 2020 DOI: https://doi.org/10.5281/zenodo.4393667

107. Гончар, С. Ф. "Метод оцінювання ризиків кібербезпеки інформаційних систем Smart Grid." Інформатика, обчислювальна техніка та автоматизація. https://doi.org/10.32838/TNU-2663-5941/2020.3-1/15

108. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 – 435 с.

109. Архипов О. Є., Скиба А. В. "Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації." Захист інформації 15, № 4 (2013): 366-375.

110. Гончар С., Леоненк Г. "Аналіз факторів впливу на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури." Collection Information technology and security, December 2016, 4(2):262-268 https://doi.org/10.20535/2411-1031.2016.4.2.110098.

111. Honchar, Serhii, and Alexander Potenko. "Методологія оцінки суми ризиків кібербезпеки інформаційної системи об’єктів критичної інфраструктури." Ukrainian Information Security Research Journal 25.3 (2019): 159-165.

112. Sarker, I.H. Machine Learning: Algorithms, Real-World Applications and Research Directions. SN COMPUT. SCI. 2, 160 (2021). https://doi.org/10.1007/s42979-021-00592-x

113. Sarker, Iqbal H. "Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects." Annals of Data Science 10.6 (2023): 1473-1498. https://doi.org/10.1007/s40745-022-00444-2

114. Zhao, Dong-Mei, Jin-Xing Liu, and Ze-Hong Zhang. "Method of risk evaluation of information security based on neural networks." 2009 International Conference on Machine Learning and Cybernetics. Vol. 2. IEEE, 2009.

115. Тостоган Є. Г., Гальчинський Л. Ю. "Вибір інструментів оцінювання кіберризиків для організацій на основі багатокритеріального аналізу." (2024).

116. Загоруйко Л. В., Скирда А. В., Мартьянова Т. А. "Моделі аналізу ризику безпеки інформаційних технологій." Прикладні інформаційні технології (2021): 97-100.

117. Kotenko I.; Doynikova E. Security metrics for risk assessment of distributed information systems. In Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Berlin, Germany, 12–14 September 2013; Volume 2, pp. 646–650.

118. Kotenko, I., & Doynikova, E. Comprehensive Multilevel Security Risk Assessment of Distributed Information Systems. Комп'ютинг, 12(3), 217. (2013).

119. Kotenko I., Chechulin A. "A cyber attack modeling and impact assessment framework." 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE, 2013.

120. Doynikova E., Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. In 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), pp. 346-353, 2017, March, IEEE.

121. Kotenko I., Saenko I., Skorik F., Bushuev S. Neural network approach to forecast the state of the internet of things elements. In 2015 XVIII international conference on soft computing and measurements (SCM), pp. 133-135, 2015, May, IEEE.

122. Ferreira, Daniel Jorge, and Henrique São Mamede. "Predicting Cybersecurity Risk-A Methodology for Assessments." ARIS2-Advanced Research on Information Systems Security 2.2 (2022): 50-63. https://doi.org/10.56394/aris2.v2i2.23

123. Kure, Halima Ibrahim, Shareeful Islam, and Haralambos Mouratidis. "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection." Neural Computing and Applications 34.18 (2022): 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

124. Amin Z. M., Anwar N., Shoid M. S. M., Samuri, S. A Systematic Literature Review for Modeling a Cyber Risk Assessment Framework. Environment-Behaviour Proceedings Journal, 9(SI18), 189-195. (2024)

125. Sánchez-García, Isaac Daniel, Jezreel Mejía, and Tomás San Feliu Gilabert. "Cybersecurity risk assessment: a systematic mapping review, proposal, and validation." Applied Sciences 13.1 (2022): 395.

126. Федорін, І. В. Методи та технології обчислювального інтелекту. (2022)

127. Chivers, Howard, John A. Clark, and Pau-Chen Cheng. "Risk profiles and distributed risk assessment." Computers & Security 28.7 (2009): 521-535.

128. Richard, Andersson. Evaluation of the Security of Components in Distributed Information Systems. Technical Report LITH-ISY-EX-3430-2003, LinkÃűping University, Sweden, 2003.

129. Zhou, B., Sun, B., Zang, T., Cai, Y., Wu, J., & Luo, H. (2022). Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities. Entropy, 25(1), 47.

130. Ekstedt M., Afzal Z., Mukherjee P., Hacks S., Lagerström, R. Yet another cybersecurity risk assessment framework. International Journal of Information Security, 22(6), 1713-1729. (2023)

131. Wang J., Neil M., Fenton N. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security, 89, 101659. (2020)

132. Czekster R. M., Webber T., Furstenau L. B., Marcon C. Dynamic risk assessment approach for analysing cyber security events in medical IoT networks. Internet of Things, 29, 101437. (2025)

133. Ferreira D. J., Mateus-Coelho N., Mamede H. S. Methodology for predictive cyber security risk assessment (PCSRA). Procedia Computer Science, 219, 1555-1563. (2023)

134. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems. Computers & security, 56, 1-27. (2016) https://doi.org/10.1016/j.cose.2015.09.009

135. Naumov S., Kabanov I. "Dynamic framework for assessing cyber security risks in a changing environment." 2016 International Conference on Information Science and Communications Technologies (ICISCT). IEEE, 2016. https://doi.org/10.1109/ICISCT.2016.7777406

## Додаток А. Перелік наукових публікацій здобувача

**Статті в іноземних виданнях**

1. Palko, D.; Babenko, T.; Bigdan, A.; Kiktev, N.; Hutsol, T.; Kuboń, M.; Hnatiienko, H.; Tabor, S.; Gorbovy, O.; Borusiewicz, A. Cyber Security Risk Modeling in Distributed Information Systems. Appl. Sci. 2023, 13, 2393. DOI: https://doi.org/10.3390/app13042393 **[індексація в наукометричній базі SCOPUS, наукове періодичне видання віднесене до першого-третього квартилів (Q1 – Q3) відповідно до класифікації SCImago Journal and Country Rank / Journal Citation Reports]**

**Статті у наукових фахових виданнях України**

1. Д.В. Палко, Л.В. Мирутенко «Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах», Кібербезпека: освіта, наука, техніка, Том 2 № 26 (2024), с. 487 – 502. DOI: https://doi.org/10.28925/2663-4023.2024.26.731
2. Д.В. Палко «Інтелектуальні моделі оцінки ризиків кібербезпеки в розподілених системах на основі нейромережевого підходу», Кібербезпека: освіта, наука, техніка, Том 3 № 27 (2025), с. 429 – 448. DOI: https://doi.org/10.28925/2663-4023.2025.27.764
3. Д.В. Палко, Л.В. Мирутенко «Метод побудови профілю ключових факторів ризику кібербезпеки сучасних розподілених інформаційних систем», Захист інформації, Том 26, № 2, липень-грудень 2024, с. 236 – 252. DOI: https://doi.org/10.18372/2410-7840.26.20014
4. Д. Палко, Л. Мирутенко, О. Шайна «Протоколи безпеки в кіберфізичних системах», Безпека інформаційних систем і технологій («Information systems and technologies security»), № 2(8)/2024, с. 66 – 73. DOI: https://doi.org/10.17721/ISTS.2024.8.66-73
5. Д.В. Палко, Т.В. Бабенко, І.І. Пархоменко, Р.В. Зюбіна «Захист інформації та передачі даних в корпоративних мережах з використанням програмно-апаратних засобів», Вісник інженерної академії України випуск №3 – 2018, с. 68 – 72

**Публікації за матеріалами міжнародних науково-практичних конференцій та семінарів**

1. Dmitry Palko, Tetiana Babenko, Larysa Myrutenko, Andrii Bigdan «Model of information security critical incident risk assessment» // Proceedings of the 2020 IEEE International Conference «Problems of infocommunications. Science and technology» PIC S&T′2020, pp. 157–161, 6-9 October 2020, Kharkiv, Ukraine DOI: https://doi.org/10.1109/PICST51311.2020.9468107 **[індексація в наукометричній базі SCOPUS]**

2. Dmytro Palko, Hrygorii Hnatienko, Tetiana Babenko, Andrii Bigdan «Determining Key Risks for Modern Distributed Information Systems» // IntSol-2021 Intelligent Solutions - CEUR Workshop Proceedings, Volume 3018, pp. 81–100, 28–30 September 2021, Kyiv, Ukraine **[індексація в наукометричній базі SCOPUS]**

3. Dmytro Palko, Tetiana Babenko, Larysa Myrutenko, Andrii Bigdan «Intelligent risk assessment models in DIS based on the neural network approach» // IX International conference «Information Technology and Implementation (Satellite)» (IT&I-2022), ISBN 978-966-969-154-5 (e-book), pp. 118–120, 1 December, 2022, Kyiv, Ukraine

4. Dmytro Palko, Tetiana Babenko «Evaluation of key risk factors for modern distributed information systems» // V Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) 27-28 жовтня 2022 року

5. Dmytro Palko, Tetiana Babenko «Risk Assessment Driven Use Of Advanced Intelligent Solutions Approach In Modern Distributed Systems» // VI Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) 27 квітня 2023 року

6. Dmytro Palko, Tetiana Babenko, Hnatiienko Hryhorii, Larysa Myrutenko and Andrii Bigdan «Intelligent risk assessment models in distributed systems based on the neural network approach» // Next Generation Cybersecurity Systems and Applications NGSEC (NGSEC-2023) Conference Proceedings, 26-27 April, 2023, Kyiv, Ukraine

7. Dmytro Palko, Kateryna Mokliakova, Tetiana Babenko «Cybersecurity level assessment models» // Next Generation Cybersecurity Systems and Applications NGSEC (NGSEC-2023) Conference Proceedings, 26-27 April, 2023, Kyiv, Ukraine

8. Dmytro Palko, Vira Vialkova, Tetiana Babenko «Intellectual models for cyber security risk assessment» // Processing, transmission and security of information : Monografia. Tom 2. / Akademia Techniczno-Humanistyczna w Bielsku-Białej. –Bielsku-Biała : Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2019. – S. 284–288.

9. Д.В. Палко, Л.В. Мирутенко, В.І. Вялкова «Захист інформаційних ресурсів та транзакцій в корпоративних мережах» // I Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS), 5-6 квітня 2018 року, с. 268-272

10. Д. Палко, Т. Бабенко, Л. Мирутенко «Інтелектуальні моделі оцінки ризиків кібербезпеки» // III Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS). – 2020. – 4 с.

11. Палко Д.В., Губський О.Ю.«Захист інформації у поштових серверах» // III Міжнародна науково-практична конференція IT&I «Інформаційні технології та взаємодії» м. Київ, 8-10 листопада 2016 року.

12. Д.В. Палко «Моделі інтелектуального аналізу кіберризиків у масштабованих розподілених середовищах» // VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем» (CPICS), 11 квітня 2025 року, – 4 с.

# Додаток Б. Акти реалізації результатів досліджень

ТОВ «ІТ Спеціаліст», 03124, Україна, м.Київ
бул. Вацлава Гавела, 6, корпус 3
ЄДРПОУ 39230764, +38 044 390 81 90

Від 13.02.2025 № 196

**АКТ**
**впровадження результатів дисертаційної роботи**
на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека»
здобувача Кафедри кібербезпеки та захисту інформації
Факультету інформаційних технологій
Київського національного університету імені Тараса Шевченка
**Палко Дмитра Володимировича**
на тему «Моделі оцінки ризиків кібербезпеки в розподілених інформаційних системах»

Основні науково-прикладні положення, отримані в результаті дисертаційного дослідження Палко Дмитра Володимировича за напрямом: «Моделі оцінки ризиків кібербезпеки в розподілених інформаційних системах» на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека», мають наукову та практичну цінність, апробовані та впроваджені у діяльність ТОВ «ІТ СПЕЦІАЛІСТ». Результати дослідження знайшли своє відображення та практичне застосування при розробці програмних продуктів **ITS Inventory**, **ITS Cybersecurity Awareness Tracker (ITS CSAT)** та **ITS Incident Management**.

Запропонований підхід до організації процесу оцінки ризиків ІБ полягає у застосуванні комплексної та адаптивної методології оцінки кіберризиків в РІС, що враховує динамічний характер розподіленого середовища і ймовірнісний характер кіберзагроз, сприяє підвищенню зрілості процесів кібербезпеки та дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

Розроблений інструментарій та підходи знайшли застосування та практичну імплементацію в задачах оптимізації процесу оцінки ризиків ІБ та підтримки прийняття управлінських рішень щодо ризик-менеджменту. Інтеграція представленої в роботі концептуальної методології та комплексу прогностичних моделей в інформаційно-аналітичні системи підтримки прийняття рішень надає можливість підвищити ефективність аналізу ризиків для мережевих активів розподіленого середовища, покращити процес моніторингу стану ІБ, та впровадити економічно-доцільні заходи безпеки.

Сформульовані у дисертаційному дослідженні теоретичні положення та практичні рекомендації будуть в подальшому також враховані при проектуванні та розробці програмного продукту **ITS Compliance and Risk Management**.

Акт впровадження результатів дисертаційної роботи видано для подання до спеціалізованої вченої ради за місцем захисту дисертації.

Директор ТОВ “ІТ СПЕЦІАЛІСТ” _____ **Морозов О.Ю.**

**ТОВ «АПІ Коннект»**
*ЄДРПОУ 43808510*
*Україна, 03124, м. Київ, бульвар Вацлава Гавела, буд.6, корпус 3, літера У*
*Email: info@apiconnect.biz*
*Тел.: +38 044 390 03 00*

від 13.02.2025 № 197

**АКТ**
**впровадження результатів дисертаційної роботи**
на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека»
здобувача Кафедри кібербезпеки та захисту інформації
Факультету інформаційних технологій
Київського національного університету імені Тараса Шевченка
**Палко Дмитра Володимировича**
на тему «Моделі оцінки ризиків кібербезпеки в розподілених інформаційних системах»

Результати дисертаційного дослідження Палко Дмитра Володимировича за напрямом «Моделі оцінки ризиків кібербезпеки в розподілених інформаційних системах» на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека», мають наукову та практичну цінність, апробовані та впроваджені у діяльність ТОВ «АПІ Коннект». На основі результатів дослідження Палко Д.В. було розроблено комплексну систему підтримки управлінських рішень, що об'єднує аспекти прогнозного моделювання та розширеної аналітики для підвищення ефективності прийняття рішень на основі даних розподілених інформаційних систем, підвищення стабільності процесу оцінки ризиків кібербезпеки та зниження рівня потенційних загроз.

В процесі формування ефективної стратегії інформаційної безпеки, була впроваджена запропонована здобувачем комплексна методологія та ряд адаптивних моделей оцінки ризиків на основі багатокритеріального аналізу гетерогенних даних розподіленого середовища та контролю відповідності вимогам стандартів кібербезпеки. Запропонований комплекс прогностичних моделей на основі алгоритмів машинного навчання та глибоких нейронних мереж дозволив підвищити ефективність процесів оцінки корпоративних ризиків та прийняття управлінських рішень, сприяв попередженню потенційних атак, та надав можливість ідентифікувати оптимальний перелік заходів захисту із забезпеченням ефективного розподілу ресурсів.

Практичні рекомендації та сформовані принципи застосування представленої в роботі концептуальної методології забезпечили підвищення точності оцінки ризиків ІБ та надали можливість автоматизованого обрахунку показника ризику в умовах динамічних масштабованих розподілених систем.

Акт впровадження результатів дисертаційної роботи видано для подання до спеціалізованої вченої ради за місцем захисту дисертації.

**З повагою,**
**Директор ТОВ «АПІ Коннект»** _____ **ШАБЕЛЬНИК Д.М.**

# Додаток В. 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 / TC / TAB / NB / IOT / NET / DB… |
| Environment | environment | category | Тип середовища функціонування активу | Prod / Test / Dev … |
| OS type | os_type | category | Тип операційної системи | Windows Server 2019 / Windows 11 Pro / CentOS 7.3… |
| OS version | os_version | category | Версія операційної системи | SP1 / 10.0 / 6.1 / 7.5… |
| OS build number | os_build | number | Номер збірки операційної системи | 7601 / 19041 / 22621… |
| Asset status | asset_status | category | Узагальнений статус життєвого циклу об’єкту за інформацією з різних джерел | Operations / End of Live |
| 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 |
| Machine type | machine_type | category | Тип розгортання пристрою (фізичний/віртуалізація) | vm / hypervisor… |
| Location | host_location | category | Логічне розташування об’єкту та приналежність до сегменту корпоративної мережі | Inside / Outside |
| Backup status | backup_status | binary | Наявність механізмів резервного копіювання | Yes / No |
| DLP connection | dlp_connected | binary | Статус підключення DLP системи | Yes / No |
| Drive encryption | drive_encryption | binary | Наявність механізмів шифрування дисків | Yes / No |
| Open ports | open_ports | aggregated | Перелік відкритих портів та сервісів | Агрегований масив даних |
| Installed software | installed_software | aggregated | Перелік інстальованого ПЗ | Агрегований масив даних |
| Incidents count | incidents_count | number | Кількість зареєстрованих інцидентів | 4 |

| Назва метрики | Ідентифікатор у наборі даних | Тип | Опис | Приклад значення |
|---|---|---|---|---|
| First detected | first_scan | datetime | Дата-час першого сканування / ідентифікації об’єкту | 11.07.2022 11:35 |
| 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 |
| Last changed | last_changed | datetime | Дата-час останньої зміни об'єкту в Active Directory | 23.08.2024 15:21 |
| Antivirus installed | av_installed | binary | Чи встановлено антивірусне ПЗ | 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 |
| Antivirus last scan | last_av_scan | datetime | Дата-час останнього повного сканування | 13.07.2024 15:18 |
| Vulnerability scan status | vuln_scan_enabled | binary | Наявність пристрою у скоупі сканувань на вразливості | Yes / No |
| 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 |
| Critical vulnerabilities | critical_vulnerabilities | number | Кількість виявлених вразливостей рівня Critical | 2 |
| Vulnerabilities | vulnerabilities_list | aggregated | Перелік виявлених вразливостей | Агрегований масив даних |
| Policy status | policies_implemented | binary | Статус застосування політик ІБ | Yes / No |
| Last success policy | policy_success_date | datetime | Дата-час останнього успішного застосування політик | 13.11.2023 09:43 |
| Last failed policy | policy_errors_date | datetime | Дата-час останнього неуспішного застосування політик | 12.02.2024 13:51 |
| Laps exist | laps_exist | binary | Наявність LAPS на пристрої | Yes / No |
| Password expiration date | laps_password_expire | datetime | Дата завершення терміну дії паролю LAPS | 11.11.2024 14:13 |
| SIEM connected | siem_connected | binary | Чи підключено об’єкт до SIEM | Yes / No |
| Last event | last_siem_event | datetime | Дата-час останньої події в SIEM | 30.08.2024 15:13 |
| Log source status | log_source_status | category | Статус підключених джерел даних | SUCCESS / ERROR |
| Log source count | log_source_count | number | Кількість підключених джерел даних | 3 |
| Average EPS | average_eps | number | Середня кількість подій в секунду за останню хвилину | 12 |

# Додаток Г. SWOT-аналіз основних підходів до моделювання процесу оцінювання ризиків кібербезпеки на основі алгоритмів машинного навчання

| Алгоритм | S (Сильні сторони) | W (Слабкі сторони) | O (Можливості) | T (Загрози) |
|---|---|---|---|---|
| Logistic Regression (LR) | - Проста інтерпретація моделей і коефіцієнтів<br>- Низька обчислювальна складність<br>- Легке застосування регуляризації | - Обмежена здатність моделювати нелінійні залежності без розширення ознак<br>- Менша точність при складних структурах даних | - Можливість інтегрувати з інженерією ознак для покращення результатів<br>- Легке застосування в режимі реального часу завдяки швидкому передбаченню | - Непридатність при дуже складних нелінійних задачах<br>- Висока залежність від якості попередньої обробки та відбору ознак |
| Support Vector Machine (SVM) | - Висока узагальнювальна здатність<br>- Добре працює з високорозмірними просторами<br>- Використання ядерних функцій для нелінійних задач | - Висока обчислювальна вартість навчання на великих наборах<br>- Чутливість до вибору гіперпараметрів і ядерних функцій | - Налаштування ядер для складних структур даних<br>- Застосування в задачах з обмеженими ресурсами за умови зменшення розмірності | - Перенавчання при невідповідних параметрах<br>- Складнощі з інтерпретацією результатів |
| Linear Discriminant Analysis (LDA) | - Легко інтерпретувати<br>- Оптимальний для лінійно відокремлюваних класів<br>- Низька обчислювальна складність | - Погано справляється з нелінійними залежностями<br>- Обмежена здатність працювати з високорозмірними та складними даними | - Може бути ефективним на попередньо відфільтрованих та добре підготовлених даних<br>- Застосування для швидких оцінок | - Низька точність на складних множинах даних<br>- Втрата ефективності при порушенні припущень (нормальність, однаковість коваріаційних матриць) |
| Naive Bayes (NB) | - Швидкість навчання та прогнозування<br>- Стійкість до шуму<br>- Ефективність при текстовій класифікації<br>- Не потребує великого обсягу даних | - Використання сильно спрощеного припущення про незалежність ознак<br>- Може втрачати точність, коли ознаки взаємозалежні | - Може слугувати базовою моделлю для оцінки складності даних<br>- Швидка інтеграція в системи з обмеженими ресурсами | - Зниження точності при складних залежностях між ознаками<br>- Чутливість до вибору репрезентативних ознак |

| | | | | |
|---|---|---|---|---|
| K-Nearest Neighbor (k-NN) | - Проста реалізація<br>- Не потребує навчання моделей (зберігає вибірку) | - Висока обчислювальна вартість прогнозування<br>- Чутливість до шуму, масштабування ознак | - Можливість швидкої адаптації до нових даних (без перенавчання моделі)<br>- Легке додавання нових класів | - Зниження продуктивності при дуже великих наборах даних<br>- Проблеми з обчислювальною складністю та пам'яттю |
| Adaptive Boosting (AdaBoost) | - Покращує точність за рахунок комбінації слабких класифікаторів<br>- Автоматично акцентує увагу на складних зразках<br>- Добра узагальнювальна здатність | - Чутливість до даних з шумом<br>- Складніший процес інтерпретації порівняно з окремим деревом<br>- Вимагає налаштування ваг і параметрів | - Застосування до різних типів базових моделей<br>- Потенціал для паралельних або розподілених обчислень | - Може втрачати продуктивність на дуже неоднорідних наборах даних<br>- Ризик надмірної складності під час комбінування великої кількості слабких класифікаторів |
| Extreme Gradient Boosting (XGBoost) | - Висока точність<br>- Стійкість до шуму і перенавчання<br>- Добре працює з різноманітними типами ознак<br>- Підтримка паралельних обчислень | - Менш інтерпретований порівняно з простими моделями<br>- Тюнінг гіперпараметрів потребує досвіду | - Інтеграція з великими наборами даних і розподіленими системами<br>- Можливість удосконалення за рахунок функцій регуляризації | - Ризик надмірної складності моделі<br>- Обчислювальні витрати при дуже великих наборах даних |
| Decision Tree (DT) | - Висока інтер-претованість<br>- Простота візуалізації та пояснення рішень<br>- Швидке навчання на малих та середніх наборах даних | - Схильність до перенавчання без регуляризації<br>- Низька точність на складних нелінійних множинах<br>- Обмеженість у разі великої розмірності | - Використання як базового компонента у ансамблевих методах<br>- Швидкий прототип для попередньої оцінки даних | - Втрата ефективності у випадку складних, гетерогенних даних<br>- Можливість генерації великої кількості глибоких дерев без контролю якості |
| Random Forest (RF) | - Висока точність і стійкість до перенавчання<br>- Інтерпретованість через важливість ознак<br>- Здатність ефективно працювати з різними типами ознак | - Повільніше прогнозування в порівнянні з простими моделями<br>- Менша інтерпретованість, ніж у одного дерева | - Легке паралельне масштабування<br>- Поєднання з іншими методами, використання як базового класифікатора | - Обмеження в реальному часі при дуже великих наборах<br>- Чутливість до дуже високої розмірності без регуляризації |

| | | | | |
|---|---|---|---|---|
| Stochastic Gradient Descent (SGD) | - Ефективний на великих наборах даних<br>- Легко масштабувати та паралелізувати<br>- Використовується як метод оптимізації для різних моделей | - Чутливість до вибору параметрів темпу навчання<br>- Потреба в нормалізації даних | - Використання з нейронними мережами та великими даними<br>- Можливість швидкої адаптації до змін у реальному часі | - Недостатня точність на дуже складних задачах<br>- Можливе перенавчання або неповна збіжність за неправильного налаштування параметрів |
| Neural Networks (NN, MLP) | - Здатність моделювати складні нелінійні залежності<br>- Добра узагальнювальна здатність при великих даних<br>- Можливість адаптації через глибинне навчання | - Потребують значних обчислювальних ресурсів<br>- Складність налаштування гіперпараметрів<br>- Важка інтерпретованість результатів | - Гібридизація з іншими методами<br>- Використання попередньо навчених моделей, трансферне навчання | - Перенавчання при недостатній регуляризації<br>- Складність впровадження у середовищі з обмеженими ресурсами |