Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2025. № 12.

DOI: http://doi.org/10.32702/2307-2105.2025.12.101
УДК 330.131.52:004.056:519.246

Т. П. Гринчук,
к. е. н., доцент, в.о. завідувачки кафедри гуманітарних, економічних та фінансово-облікових дисциплін,
Вінницький кооперативний інститут
ORCID ID: https://orcid.org/0000-0002-0008-4764
Ю. Б. Ільніцька,
викладач кафедри гуманітарних, економічних та фінансово-облікових дисциплін, Вінницький кооперативний інститут
ORCID ID: https://orcid.org/0009-0008-9961-6070
Ю. А. Кашпрук,
к. е. н., доцент, доцент кафедри гуманітарних, економічних та фінансово-облікових дисциплін, Вінницький кооперативний інститут
ORCID ID: https://orcid.org/0000-0002-2196-2001

СТОХАСТИЧНІ МОДЕЛІ УПРАВЛІННЯ КІБЕРРИЗИКАМИ В УМОВАХ ЦИФРОВІЗАЦІЇ БІЗНЕСУ

T. Hrynchuk,
PhD in Economics, Associate Professor, Acting Head of the Department of Humanities, Economics, and Financial and Accounting Disciplines, Vinnytsia Cooperative Institute
Yu. Ilnitska,
Lecturer of the Department of Humanities, Economics, and Financial and Accounting Disciplines, Vinnytsia Cooperative Institute
Yu. Kashpruk,
PhD in Economics, Associate Professor, Associate Professor of the Department of Humanities, Economics, and Financial and Accounting Disciplines, Vinnytsia Cooperative Institute

STOCHASTIC MODELS FOR CYBER RISK MANAGEMENT IN THE CONTEXT OF BUSINESS DIGITALIZATION

У статті досліджено застосування стохастичних моделей для управління кіберризиками в умовах інтенсивної цифровізації бізнесу. Проаналізовано переваги й обмеження традиційних підходів до оцінки кіберризиків та обґрунтовано доцільність використання ймовірнісних методів, зокрема марковських ланцюгів для моделювання динаміки атак, теорії масового обслуговування для аналізу навантаження на системи безпеки та байєсівських мереж для врахування залежностей між різними типами загроз. На основі аналізу сучасних досліджень запропоновано інтегровану стохастичну модель оцінки кіберризиків, яка враховує динамічну природу загроз, залежність компонентів системи та вплив зовнішніх факторів. Модель дозволяє кількісно оцінити ймовірність реалізації кіберзагроз, масштаб потенційних збитків та оптимізувати вибір заходів захисту на основі аналізу вартості впровадження та очікуваного ефекту. Окрім того, розглянуто практичні аспекти впровадження запропонованого підходу для українських підприємств з урахуванням специфіки їх функціонування в умовах воєнного стану та відбудови економіки.

The article presents a comprehensive investigation into the application of advanced stochastic models for enhancing cyber risk management frameworks within the rapidly evolving context of intensive business digitalization. It begins with a critical analysis of the inherent advantages and significant limitations of traditional, often qualitative, approaches to cyber risk assessment, which frequently rely on static matrices and expert judgment. These conventional methods are shown to be inadequate for capturing the dynamic, probabilistic, and interconnected nature of modern cyber threats in complex digital ecosystems. The study substantiates the critical need for a paradigm shift towards sophisticated probabilistic methods to achieve a more resilient and predictive security posture.

The research provides a detailed rationale for employing specific stochastic techniques, each addressing a unique facet of cyber risk. The use of Markov chains

is justified for modeling the temporal evolution and multi-stage progression of cyber-attacks, illustrating how systems transition between different states of security compromise. Queuing theory is proposed to analyze the performance and potential bottlenecks of security incident response systems under fluctuating loads of attack attempts, allowing for the optimization of resource allocation. Furthermore, the integration of Bayesian networks is highlighted as a powerful tool for reasoning under uncertainty, enabling the quantification of conditional dependencies between various threat vectors, system vulnerabilities, and the effectiveness of existing security controls, while also allowing for continuous updating of risk probabilities as new evidence emerges.

Building upon this analytical foundation, the article proposes a novel, integrated stochastic model for a holistic assessment of cyber risks. This model is specifically designed to account for the dynamic and non-stationary nature of the threat landscape, the critical interdependencies among system components where a failure in one node can cascade through the entire network, and the significant impact of external macroeconomic, geopolitical, and regulatory factors. The proposed framework enables organizations to move beyond simplistic risk scores and towards a quantitative financial valuation of cyber exposure. It facilitates the calculation of key metrics such as the probability of a successful breach within a given timeframe, the distribution of potential financial losses including direct costs, operational disruption, and reputational damage, and the Return on Security Investment (ROSI) for various countermeasures.

Finally, the study addresses the crucial practical aspects of implementing this proposed analytical approach, with a specific focus on Ukrainian enterprises. It carefully considers the unique operational challenges posed by the conditions of martial law and the subsequent period of economic recovery. This includes adapting the model to account for heightened state-level cyber threats, resource constraints that prioritize cost-effective solutions, and the critical need for business continuity planning. The research outlines a pathway for integrating this data-driven, stochastic methodology into the national cybersecurity strategy,

empowering Ukrainian businesses to build digital resilience and safeguard their assets during a critical period of transformation and rebuilding.

Ключові слова: *стохастичні моделі, кіберризики, управління ризиками, цифровізація бізнесу, марковські ланцюги, теорія масового обслуговування, байєсівські мережі.*

Keywords: *stochastic models, cyber risks, risk management, business digitalization, Markov chains, queuing theory, Bayesian networks.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Стрімка цифровізація бізнесу, зростання складності інформаційних систем та посилення кіберзагроз зумовлюють необхідність розробки ефективних методів управління кіберризиками. Традиційні детерміновані підходи, засновані на якісних оцінках, часто виявляються недостатніми для адекватного відображення динамічної та невизначеної природи кіберзагроз. У рамках досліджуваної проблеми стохастичні моделі, що враховують ймовірнісний характер кіберінцидентів, пропонують нові можливості для побудови більш точних і адаптивних систем управління ризиками.

Аналіз останніх досліджень і публікацій. Сучасна наукова література з кібербезпеки демонструє зростаючий інтерес до застосування стохастичних моделей для аналізу та прогнозування кіберзагроз. Дослідження останніх років пропонують різноманітні підходи до вирішення цієї проблеми. У роботі [1] представлено модель оцінки кіберризиків, що базується на аналізі взаємозалежності компонентів IoT-систем. Хоч автори й використовують графові моделі для відтворення взаємозв'язків між пристроями та сервісами, що дає змогу оцінити каскадний ефект від реалізації загроз, запропонована модель має переважно якісний характер і недостатньо враховує ймовірнісну природу кіберінцидентів. У дослідженні [2] розглядається динамічна оцінка ризиків для медичних IoT-мереж із застосуванням імітаційного моделювання. Незважаючи на ефективність дискретно-подієвого моделювання для аналізу

потоків даних, цей підхід вимагає значних обчислювальних ресурсів і ускладнює адаптацію для масштабних гетерогенних систем. Наукова праця [3] демонструє ефективність марковських ланцюгів і теорії масового обслуговування для вдосконалення систем виявлення вторгнень, досягаючи високих показників точності (92%) та відгуку (91%). Вагомий внесок у розвиток кількісних методів оцінки ризиків зроблено в роботі [4], де запропоновано комплексну аналітичну рамку з інтеграцією методів прогнозної аналітики, моделювання Монте-Карло та машинного навчання. Їх підхід дозволяє оптимізувати баланс між превентивними заходами та трансфером ризиків через страхування, використовуючи такі метрики, як Annual Loss Expectancy та Return on Security Investment.

У рамках досліджень А. Вербійської, Т. Азової [5] та В. Кифяк [6] висвітлюються інституційні та управлінські складові цифрової трансформації. А. Вербійська, Т. Азова акцентують увагу на основних факторах успішної цифровізації, тоді як В. Кифяк пропонує класифікацію інституцій управління ризиками та коефіцієнт цифровізації для оцінки вразливості бізнес-процесів.

Незважаючи на значний прогрес, більшість сучасних досліджень зосереджено на окремих аспектах проблеми. Відсутніми залишаються інтегровані рішення, що поєднують різні стохастичні методи для комплексної оцінки та управління кіберризиками в умовах цифровізації бізнесу, що відкриває перспективи для подальших наукових розвідок у цьому напрямі.

Формулювання цілей статті (постановка завдання). Метою даної роботи є розробка інтегрованої стохастичної моделі управління кіберризиками, яка поєднує марковські ланцюги, теорію масового обслуговування та байєсівські мережі для кількісної оцінки ймовірності реалізації загроз, масштабу збитків та оптимізації вибору заходів захисту в умовах цифровізації бізнесу.

Виклад основного матеріалу дослідження. Стохастичні моделі в управлінні кіберризиками базуються на принципі ймовірнісного опису поведінки складних систем у умовах невизначеності. На відміну від детермінованих підходів, які передбачають однозначну відповідність між

вхідними та вихідними параметрами, стохастичні моделі враховують випадковий характер кіберзагроз та їх наслідків. Математичний апарат стохастичного моделювання охоплює теорію ймовірностей для кількісної оцінки невизначеності, випадкові процеси для моделювання динаміки змін у часі, статистичне моделювання для аналізу емпіричних даних та оптимізаційні методи для прийняття рішень в умовах ризику.

Підхід до аналізу кіберризиків через призму стохастичного моделювання відкриває нові можливості для прогнозування та запобігання загрозам у кіберпросторі. Особливе місце серед стохастичних інструментів займають марковські процеси, які пропонують математичний апарат для опису динамічної поведінки систем безпеки.

Марковські моделі демонструють особливу ефективність для аналізу послідовностей кібератак та оцінки ймовірностей переходу між станами системи. Розглядаючи розширену модель марковського ланцюга для кібербезпеки, система може перебувати в станах нормальної роботи, виявленої підозрілої активності, активної атаки, компрометації системи, відновлення та критичного збою.

Основу марковського підходу складає матриця переходів, яка визначає ймовірності переходу системи між станами за одиницю часу. Для системи з N станами безпеки матриця переходів $P = [p_{ij}]$ описує динаміку змін, де p_{ij} визначає ймовірність переходу зі стану i до стану j. Для кожного стану визначається функція збитків, що дозволяє розрахувати очікуваний збиток за період часу T. Стаціонарний розподіл $\pi = (\pi_1, \pi_2, ..., \pi\_N)$, який задовольняє умові $\pi P = \pi$, дозволяє визначити довгострокові тенденції в безпековому стані системи та оцінити стійкість до тривалих кібератак.

Використання марковських процесів у кібербезпеці дозволяє перейти від реактивного до проактивного підходу в управлінні ризиками. Моделі дають змогу не лише оцінити поточний стан безпеки, але й прогнозувати майбутні загрози, оптимізувати розподіл ресурсів для захисту та обґрунтувати інвестиції в заходи кібербезпеки на основі кількісних оцінок ризиків.

Теорія масового обслуговування знаходить ефективне застосування для аналізу навантаження на системи захисту та оцінки ефективності реагування на інциденти. Розглядаючи систему масового обслуговування з пуассонівським потоком кібератак та експоненційним розподілом часу обслуговування, можна визначити оптимальну кількість каналів обслуговування та місткість системи для мінімізації втрат.

Стаціонарні ймовірності станів системи розраховуються через суми комбінацій інтенсивностей потоків атак та обслуговування, що дозволяє визначити ймовірність втрати виклику та середній час очікування в черзі. Ці параметри мають критичне значення для планування ресурсів відділів кібербезпеки та оцінки їх здатності протистояти масовим атакам.

Стаціонарні ймовірності станів системи p_o, p_k розраховуються за формулами (1), (2):

$$p_o = \left[\sum_{k=0}^{c} \frac{(\frac{\lambda}{\mu})^k}{k!} + \sum_{k=c+1}^{K} \frac{(\frac{\lambda}{\mu})^k}{c! \cdot c^{k-c}}\right]^{-1}, \quad (1)$$

$$p_k = \begin{cases} \frac{\left(\frac{\lambda}{\mu}\right)^k}{k!} p_o, \text{ якщо } 0 \le k \le \text{c} \\ \frac{(\frac{\lambda}{\mu})^k}{c! \cdot c^{k-c}}, \text{ якщо c} \le k \le \text{K} \end{cases}, \quad (2)$$

де λ – інтенсивність потоку кібератак (пуассонівський потік); μ – інтенсивність обслуговування атак (експоненційний розподіл); c – кількість каналів обслуговування (спеціалістів з кібербезпеки); K – місткість системи (максимальна кількість атак, що можуть оброблятися одночасно).

Ймовірність втрати виклику P_{loss} (відмови в обслуговуванні) розраховується за формулою:

$$P_{loss} = p_k. \quad (3)$$

Середній час очікування в черзі W_q:

$$W_q = \frac{\sum_{k=c}^{K}(k-c)p_k}{\lambda(1-P_{loss})}. \quad (4)$$

Запропоновані формули (1)-(4) дозволяють кількісно оцінити стаціонарні стани системи та прийняти обґрунтовані рішення щодо планування потужностей відділів кібербезпеки, особливо в умовах масових атак. Це забезпечує баланс між витратами на захист та рівнем ризику для організації.

Байєсівські мережі пропонують потужний інструмент для моделювання складних причинно-наслідкових зв’язків між різними факторами ризику. Моделюючи взаємозв'язки між наявністю вразливостей, рівнем захисту, мотивацією атакуючого, складністю атаки, успішністю атаки та фінансовими збитками, можна побудувати комплексну картину кіберризиків організації.

Умовні ймовірності в байєсівській мережі дозволяють врахувати залежність між різними факторами ризику. За допомогою байєсівського виводу розраховується ймовірність великих фінансових збитків через підсумовування усіх можливих комбінацій станів вузлів мережі, що забезпечує комплексну оцінку ризиків з урахуванням усіх взаємозв'язків.

Розглянемо приклад мережі для оцінки ризику успішної кібератаки з такими вузлами: A – Наявність вразливостей; B – Рівень захисту; C – Мотивація атакуючого; D – Складність атаки; E – Успішність атаки; F – Фінансові збитки.

Умовні ймовірності: P(A = високий) = 0,3; P(B = низький) = 0,4; P(C = висока) = 0,2; P(D = висока | A = високий) = 0,8; P(D = висока | A = низький) = 0,1; P(E = так | B = низький, D = висока) = 0,9; P(E = так | B = високий, D = висока) = 0,3; P(F = великі | E = так) = 0,7.

За допомогою байєсівського виводу можна розрахувати ймовірність великих фінансових збитків:

$$\text{P(F = великі)} = \sum_{A,B,C,D,E} P(F \mid E)P(E \mid B,D)P(D \mid A)P(C)P(B)P(A). \quad (4)$$

У наведеному прикладі мережа з шести вузлів демонструє, як різні фактори – від наявності вразливостей до мотивації атакуючих – послідовно впливають на ймовірність успішної атаки та величину фінансових збитків. Застосування байєсівського виводу через маргіналізацію всіх можливих станів системи (формула 4) забезпечує комплексну ймовірнісну оцінку ризику, що є цінним інструментом для прийняття обґрунтованих рішень щодо інвестицій у кібербезпеку.

Розглянемо запропоновану інтегровану стохастичну модель управління кіберризиками, що складається з чотирьох фаз (рис. 1-4).

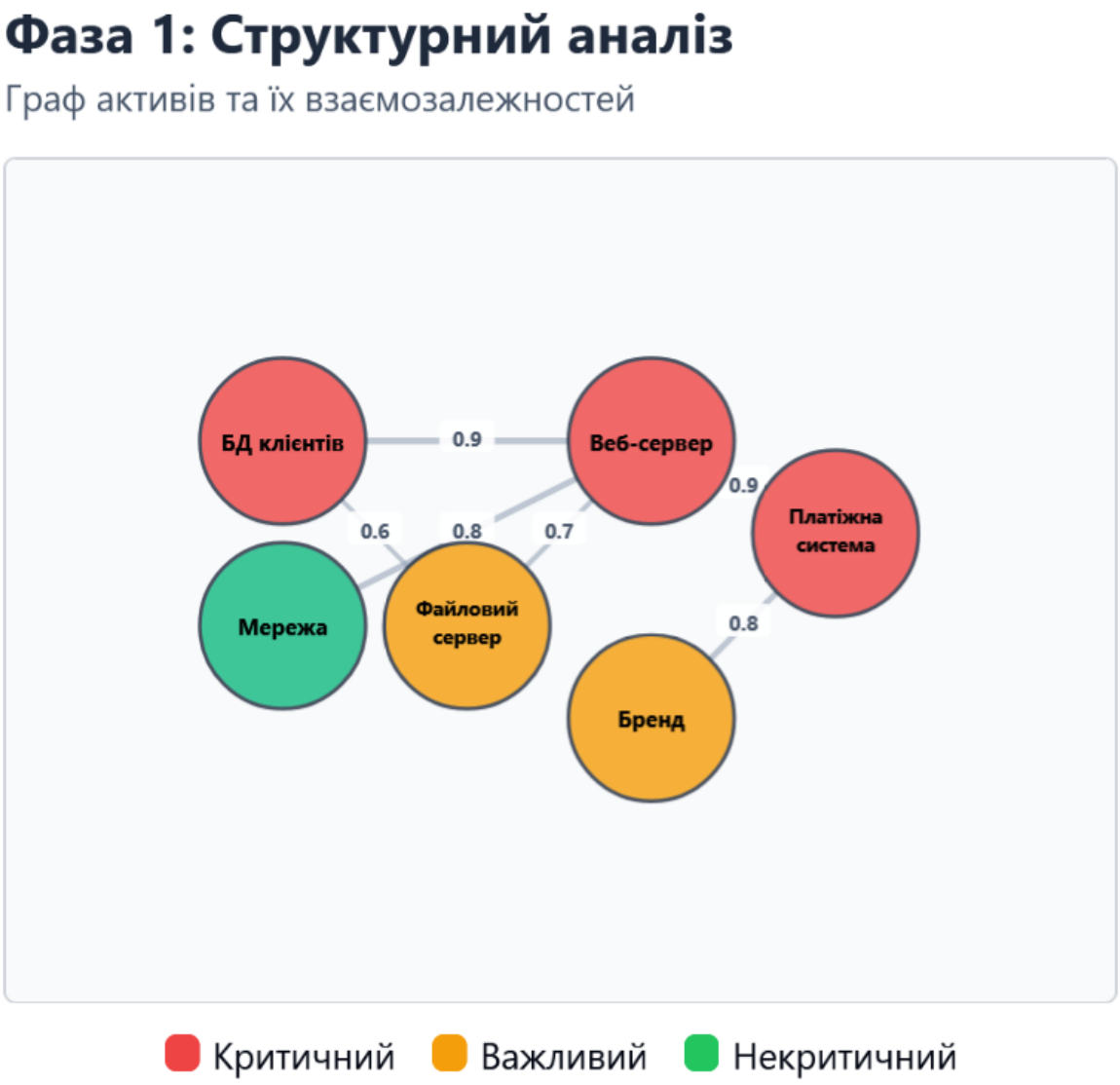


Рис. 1. Фаза 1 – Структурний аналіз

Джерело: складено автором.

Фаза 2: Кількісна оцінка ризиків

Матриця ризиків та ймовірності загроз

Теплова матриця ризиків

Загроза	БД	Веб	Файл	Плат	Бренд	Мереж
DDoS	0.3	0.9	0.4	0.7	0.6	0.8
Malware	0.7	0.6	0.8	0.5	0.3	0.4
Phishing	0.8	0.4	0.5	0.9	0.7	0.2
SQL Injection	0.9	0.7	0.2	0.8	0.4	0.1
Insider	0.6	0.5	0.7	0.6	0.8	0.5

Ймовірності загроз

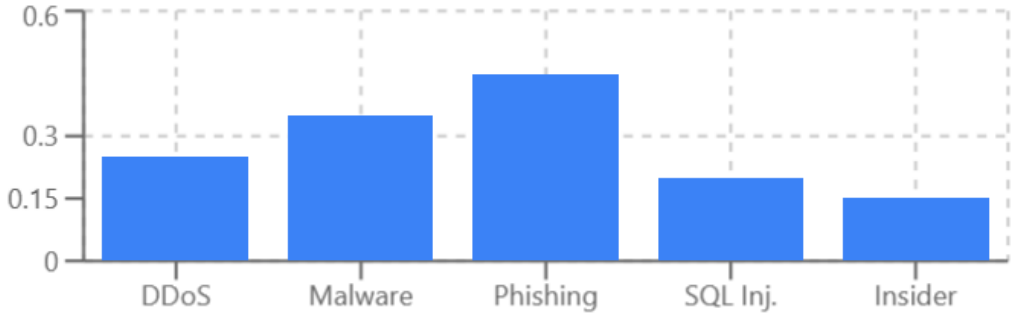


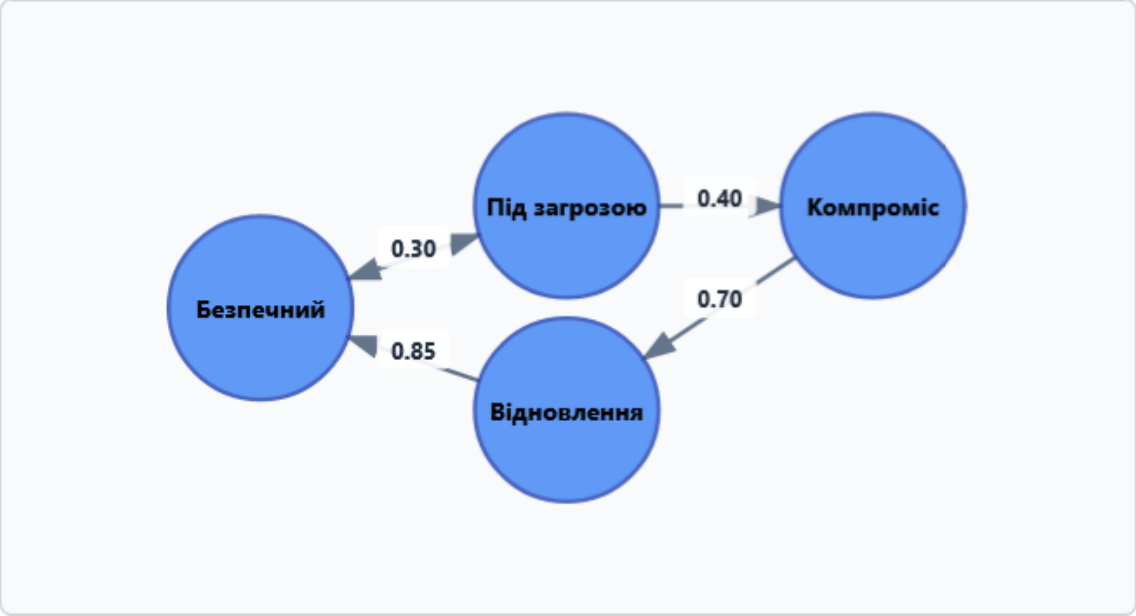
Рис. 2. Фаза 2 – Кількісна оцінка ризиків

Джерело: складено автором.

Фаза 3: Динамічне моделювання

Марковська модель та еволюція станів

Діаграма станів



Еволюція ймовірностей

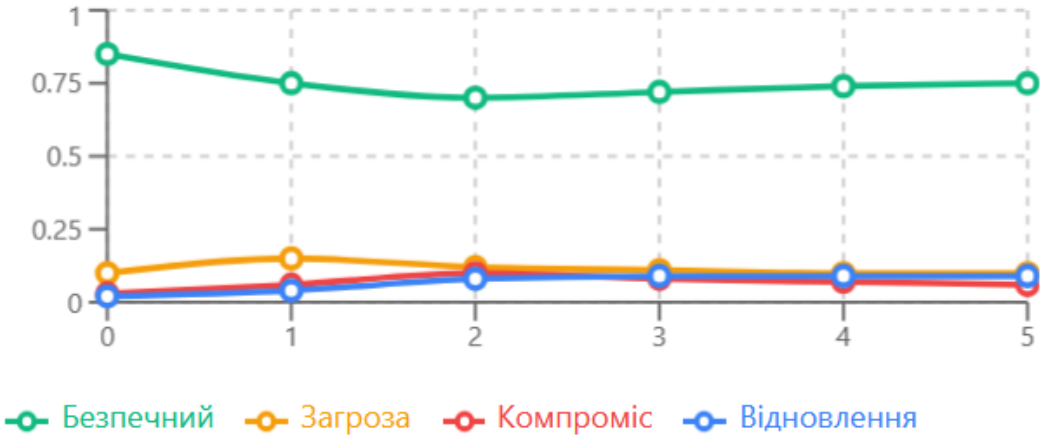


Рис. 3. Фаза 3 – Динамічне моделювання

Джерело: складено автором.

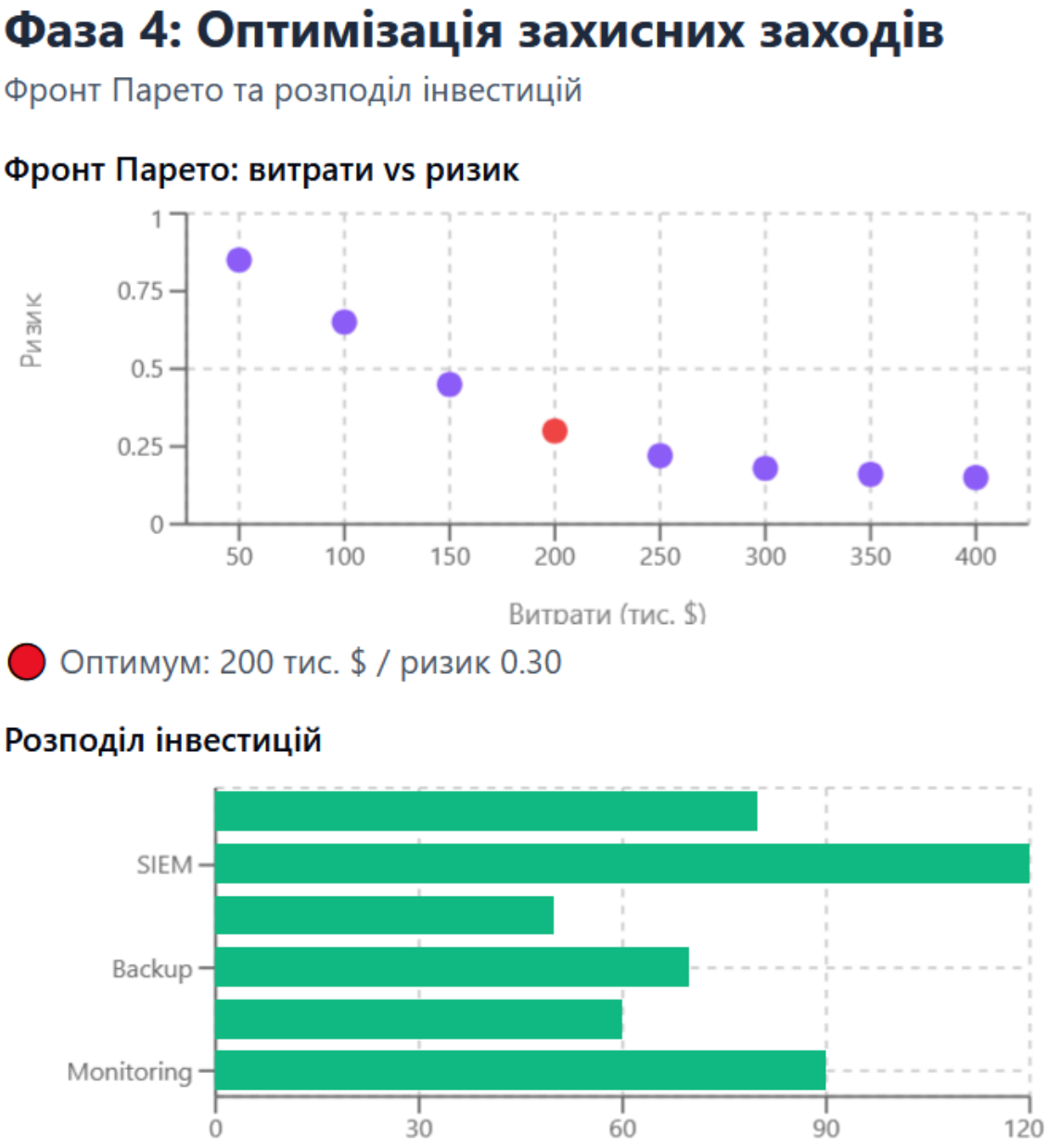


Рис. 4. Фаза 4 – Оптимізація захисних заходів

Джерело: складено автором.

Запропонована модель поєднує різні стохастичні методи в єдину framework, починаючи зі структурного аналізу системи. На етапі ідентифікації критичних активів визначаються дані, системи, процеси та репутація як ключові об'єкти захисту. Побудова графа залежностей з

вершинами-активами та ребрами-функціональними залежностями формує основу для аналізу каскадних ефектів при реалізації загроз.

Кількісна оцінка ризиків включає оцінку ймовірностей реалізації загроз на основі історичних даних, експертних оцінок, даних з Threat Intelligence платформ та аналізу вразливостей. Для кожної пари актив-загроза оцінюється рівень вразливості, що характеризує ефективність заходів захисту, а для кожного активу визначається функція збитків, що залежить від інтенсивності впливу.

Динамічне моделювання реалізується через побудову марковської моделі з дискретним часом і станами, що описують різні сценарії розвитку кіберінцидентів. Аналіз стійкості системи здійснюється через розрахунок граничних ймовірностей станів системи, що дозволяє оцінити довгострокову стійкість системи до кіберзагроз.

Оптимізація заходів захисту формулюється як задача мінімізації суми вартості заходів захисту та очікуваного збитку після їх впровадження. Для розв'язку цієї задачі використовуються методи лінійного програмування для лінійних моделей, цілочисельного програмування для дискретних рішень, генетичні алгоритми для складних нелінійних задач та метод Монте-Карло для оцінки стохастичних моделей.

Для українських підприємств особливе значення має адаптація моделі до специфічних умов функціонування. Використання даних з національних баз кіберзагроз забезпечує релевантність оцінок, а врахування геополітичної ситуації та активності ворожих кібергруп дозволяє адекватно оцінити рівень загроз. Поетапне впровадження моделі, починаючи з найкритичніших бізнес-процесів, забезпечує практичну реалізацію без значних одноразових інвестицій [7-12].

Ефективність запропонованого підходу підтверджується результатами практичного застосування, де використання стохастичних моделей дозволило підвищити точність виявлення кібератак та оптимізувати витрати на заходи захисту. Інтеграція різних стохастичних методів у єдину модель забезпечує

комплексний підхід до управління кіберризиками в умовах цифровізації бізнесу, що є особливо актуальним для українських підприємств у сучасних умовах.

Висновки та перспективи подальших розвідок у даному напрямі. Проведене дослідження довело ефективність застосування стохастичних моделей для управління кіберризиками в умовах цифровізації бізнесу. Запропонована інтегрована модель, що поєднує марковські ланцюги, теорію масового обслуговування та байєсівські мережі, дозволяє перейти від якісних оцінок до кількісного аналізу кіберризиків. Це забезпечує об'єктивну основу для прийняття управлінських рішень щодо розподілу ресурсів та інвестицій у заходи безпеки.

У рамках дослідження було розроблено комплексну методологію оцінки кіберризиків, яка враховує динамічну природу загроз, залежність компонентів інформаційних систем та вплив зовнішніх факторів. Запропоновано математичний апарат для кількісної оцінки ймовірності реалізації кіберзагроз та потенційних збитків, що створює основу для оптимізації вибору заходів захисту шляхом аналізу вартості їх впровадження та очікуваного ефекту. Важливим результатом стала адаптація моделі до специфічних умов функціонування українських підприємств, зокрема з урахуванням геополітичних ризиків та обмеженості ресурсів.

Перспективним напрямом є вдосконалення адаптивних стохастичних моделей шляхом інтеграції методів штучного інтелекту та машинного навчання. Це дозволить автоматизувати оцінку ризиків у режимі реального часу, зокрема за рахунок використання глибоких байєсівських мереж для прогнозування складних каскадних атак. Актуальною є інтеграція моделей кіберризиків із фінансовими моделями для оцінки впливу кіберінцидентів на ринкову вартість компанії, кредитні рейтинги та вартість страхування.

Також варто зосередитись на розробці спеціалізованих моделей для критичної інфраструктури, враховуючи особливості енергетичних, фінансових та транспортних систем в умовах гібридних загроз. Важливим

напрямом є дослідження міжгалузевих ефектів поширення кіберризиків з використанням мережевих моделей для аналізу каскадних наслідків кіберінцидентів у економіці.

Перспективним також є розвиток методів квантіфікації нефінансових ризиків, таких як репутаційні збитки, втрата інтелектуальної власності та порушення конфіденційності даних. Необхідною є адаптація моделей до вимог нормативно-правової бази з кібербезпеки, зокрема Директиви NIS2, GDPR та національних стандартів безпеки. Окремий інтерес становить дослідження впливу квантових обчислень на криптографічні системи та розробка стохастичних моделей для оцінки ризиків переходу до постквантової криптографії.

Для української науки та практики особливе значення має розвиток методологій, адаптованих до умов воєнного стану та відбудови економіки. Перспективним напрямом є створення національної платформи для збору та аналізу даних про кіберінциденти, що дозволить удосконалювати стохастичні моделі на основі релевантної статистики.

Реалізація запропонованих напрямів досліджень сприятиме розвитку теорії управління кіберризиками та створенню практичних інструментів для підвищення стійкості бізнесу в умовах цифрової трансформації.

Література

1. Radanilev P., De Roure D., Maple C., Nurse J. R. C., Nicolescu R., Ani U. AI security and cyber risk in IoT systems. *Front. Big Data*. 2024. Vol. 7.

2. 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*. 2025. Vol. 29.

3. Murti R. K., Joshi V. V., Wagh R., Jangale M. S., Chaudhari A. C., Wagh M. Stochastic Models for Cyber Attack Detection and Response: A Mathematical Approach to Intrusion Detection Systems. *Communications on Applied Nonlinear Analysis*. 2024. Vol. 31. P. 488–502.

4. Dan T., City A., Okunola A., Dreafer C. Quantifying Cyber Risk: Developing a Business Analytics Framework for Proactive Investment in Cybersecurity Measures and Insurance. *AOIJ*. 2024. 14 p. URL: https://surl.li/yhbbca (дата звернення: 25.11.2025).

5. Вербівська Л. В., Дзюба Т. В. Цифрова трансформація підприємництва: стратегічні виклики та управлінські рішення. *Інвестиції: практика та досвід*. 2025. № 12. С. 60-65.

6. Кифяк В. І. Інституційне забезпечення управління ризиками бізнесу в умовах цифровізації. *Проблеми інноваційно-інвестиційного розвитку*. 2022. № 28. С. 85-98.

7. Гринчук Т. П., Ціхановська А. М., Чичкалюк Д. О. Удосконалення методик фінансового планування в системі фінансової безпеки підприємства. *Приазовський економічний вісник.* 2021. № 1 (24).

8. Ільніцька Ю. Б., Медведська В. Б. Інноваційні підходи до професійної підготовки фахівців в умовах цифрової трансформації суспільства. *Виклики та потенційні шляхи розвитку освіти та технологій в Україні та світі*: матеріали ІІІ Всеукраїнської науково-практичної конференції, ВСП "Сумський фаховий коледж Національного університету харчових технологій", 14.05.2025 р. С. 52-56.

9. Гріщенко І. В., Гринчук Т. П. Основні аспекти фінансового планування в системі фінансової безпеки підприємства. *Економіка та суспільство*. 2020. № 22.

10. Ільніцька Ю. Б. Інтеграція технологій штучного інтелекту в сучасних освітніх практиках. *Освіта, наука і практика: інноваційні підходи до вирішення глобальних викликів*: матеріали міжнародної науково-практичної конференції, м. Вінниця, 30 квітня 2025 року. Вінниця, 2025. С. 47-49.

11. Ilnitska Yulia, Medvedska Victoria. Innovations in computer science education through blockchain technology. *Mathematics and Informatics in Science and Education: Challenges of Modernity*: V international Scientific Internet Conference, Vinnytsia, 2025. P. 85-89.

12. Гринчук Т. П., Гусак Л. П. Використання криптовалюти у злочинних цілях та пріоритетні напрями її правового регулювання. *Фінансовий простір.* 2022. № 2 (46). С. 6-18.

References

1. Radanilev, P. De Roure, D. Maple, C. Nurse, J.R.C. Nicolescu, R. and Ani, U. (2024), "AI security and cyber risk in IoT systems", *Front. Big Data*, vol. 7.

2. Czekster, R.M. Webber, T. Furstenau, L.B. and Marcon, C. (2025), "Dynamic risk assessment approach for analysing cyber security events in medical IoT networks", *Internet of Things*, vol. 29.

3. Murti, R.K. Joshi, V.V. Wagh, R. Jangale, M.S. Chaudhari, A.C. and Wagh, M. (2024), "Stochastic Models for Cyber Attack Detection and Response: A Mathematical Approach to Intrusion Detection Systems", *Communications on Applied Nonlinear Analysis*, vol. 31, pp. 488-502.

4. Dan, T. City, A. Okunola, A. and Dreafer, C. (2024), "Quantifying Cyber Risk: Developing a Business Analytics Framework for Proactive Investment in Cybersecurity Measures and Insurance", *AOIJ*, 14 p., available at: https://surl.li/yhbbca (Accessed 30 November 2025).

5. Verbivska, L.V. and Dziuba, T.V. (2025), "Digital Transformation of Entrepreneurship: Strategic Challenges and Management Decisions", *Investytsii: praktyka ta dosvid*, vol. 12, pp. 60-65.

6. Kyfiak, V.I. (2022), "Institutional Support for Business Risk Management in the Conditions of Digitalization", *Problemy innovatsiino-investytsiinoho rozvytku*, vol. 28, pp. 85-98.

7. Hrynchuk, T.P. Tsikhanovska, A.M. and Chychkaliuk, D.O. (2021), "Improvement of Financial Planning Methods in the Enterprise Financial Security System", *Priazovskyi ekonomichnyi visnyk*, vol. 1 (24).

8. Ilnitska, Yu.B. and Medvedska, V.B. (2025), "Innovative Approaches to Professional Training of Specialists in the Conditions of Digital Transformation

of Society", *Materialy III Vseukrainskoi naukovo-praktychnoi konferentsii "Vyklyky ta potentsiini shliakhy rozvytku osvity ta tekhnolohii v Ukraini ta sviti"* [Proceedings of the III All-Ukrainian Scientific-Practical Conference "Challenges and Potential Ways of Development of Education and Technologies in Ukraine and the World"], Sumy, Ukraine, pp. 52-56.

9. Hrinenko, I.V. and Hrynchuk, T.P. (2020), "Main Aspects of Financial Planning in the Enterprise Financial Security System", *Ekonomika ta suspilstvo*, vol. 22.

10. Ilnitska, Yu.B. (2025), "Integration of Artificial Intelligence Technologies in Modern Educational Practices", *Materialy mizhnarodnoi naukovo-praktychnoi konferentsii "Osvita, nauka i praktyka: innovatsiini pidkhody do vyrishennia hlobalnykh vyklykiv"* [Proceedings of the International Scientific-Practical Conference "Education, Science and Practice: Innovative Approaches to Solving Global Challenges"], Vinnytsia, Ukraine, pp. 47-49.

11. Ilnitska, Yu. and Medvedska, V. (2025), "Innovations in computer science education through blockchain technology", *Mathematics and Informatics in Science and Education: Challenges of Modernity: V International Scientific Internet Conference*, Vinnytsia, Ukraine, pp. 85-89.

12. Hrynchuk, T.P. and Husak, L.P. (2022), "The Use of Cryptocurrency for Criminal Purposes and Priority Areas of Its Legal Regulation", *Finansovyi prostir*, vol. 2 (46), pp. 6-18.

Стаття надійшла до редакції 02.12.2025 р.