АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

УДК 005.334:004.056

DOI https://doi.org/10.5281/zenodo.18059737

Економічна оцінка ризиків кіберзагроз для цифрових бізнес-моделей

Левченко Олександр Миколайович,
доктор економічних наук, професор, завідувач кафедри менеджменту та підприємництва, Центральноукраїнський державний університет імені Володимира Винниченка, м. Кропивницький, Україна,
https://orcid.org/0000-0001-5452-7420

Довгенко Яна Олексіївна,
кандидат економічних наук, доцент, доцент кафедри менеджменту та підприємництва, Центральноукраїнський державний університет імені Володимира Винниченка, м. Кропивницький, Україна,
https://orcid.org/0000-0002-3254-8746

Яременко Людмила Іванівна,
кандидат педагогічних наук, доцент, доцент кафедри менеджменту та підприємництва, Центральноукраїнський державний університет імені Володимира Винниченка, м. Кропивницький, Україна,
https://orcid.org/0000-0002-1167-8744

Прийнято: 09.12.2025 | Опубліковано: 26.12.2025

Анотація. Упровадження інноваційних бізнес-моделей дає змогу суттєво підвищити ефективність діяльності підприємств, проте їхня зростаюча ІТ-залежність генерує нові ризики, які можуть спричинити значні економічні

збитки. **Метою статті** є дослідження специфіки економічної оцінки кіберзагроз в умовах цифрових бізнес-моделей та визначення їх реального економічного впливу на функціонування підприємств. **Методи.** У роботі застосовано методи критичного аналізу наукових джерел, синтезу, систематизації та абстрагування для виявлення основних підходів до економічної оцінки кіберризиків, класифікації типів загроз та встановлення їх економічного впливу на цифрові бізнес-моделі. **Результати.** З'ясовано, що цифровізація суттєво поліпшує ефективність бізнес-процесів, забезпечуючи швидший обмін інформацією та автоматизацію операцій, проте водночас збільшує вразливість компаній до кібератак, оскільки зростає залежність від IT-інфраструктури та цифрових активів. Підкреслено важливість використання комплексного підходу до оцінки кіберризиків, який поєднує кількісні, імовірнісні та експертні методи, даючи змогу враховувати як технічні характеристики загроз, так і контекст бізнес-процесів. Показано, що застосування моделей очікуваних втрат, FAIR, стохастичних та гібридних підходів допомагає не лише трансформувати технічні загрози у фінансові метрики, а й визначати можливі сценарії економічних витрат, порівнювати альтернативні ризики та пріоритезувати інвестиції в заходи кіберзахисту. Окрім того, інтеграція цих підходів сприяє більш точному плануванню бюджету безпеки, підвищенню операційної стійкості підприємств та обґрунтованому ухваленню рішень щодо фінансування залишкових ризиків, включно з використанням страхових механізмів. **Висновки.** Встановлено, що економічна оцінка кіберризиків – це головний інструмент стратегічного управління цифровими бізнес-моделями, що забезпечує стійкість, ефективне розподілення ресурсів і підтримку нормативної відповідності в умовах зростаючих кіберзагроз.

Ключові слова: кіберризики, економічна оцінка, інформаційний менеджмент, цифрові бізнес-моделі, кібербезпека, стратегічне управління, інвестиції в кіберзахист.

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Economic assessment of cyber threat risks for digital business models

Oleksandr Levchenko,
Doctor of Economic Sciences, Professor, Head of the Department of Management and Entrepreneurship, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, Ukraine,
https://orcid.org/0000-0001-5452-7420

Yana Dovhenko,
PhD of Economics, Associate Professor, Department of Management and Entrepreneurship, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, Ukraine,
https://orcid.org/0000-0002-3254-8746

Liudmyla Yaremenko,
PhD of Pedagogical Sciences, Associate Professor, Department of Management and Entrepreneurship, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, Ukraine,
https://orcid.org/0000-0002-1167-8744

Abstract. The implementation of innovative business models significantly increases enterprise efficiency; however, their growing IT dependence generates new risks that can cause significant economic losses. The **article aims** to examine the specifics of the economic assessment of cyber risks in the context of digital business models and to determine their actual economic impact on enterprise activities. **Methods**. The study used methods of critical analysis of scientific sources, synthesis, systematization, and abstraction to identify key approaches to the economic assessment of cyber risks, classify threat types, and establish their economic impact on digital business models. **Results**. It was found that digitalization

significantly increases the efficiency of business processes, enabling faster information exchange and the automation of operations. Still, it also increases companies' vulnerability to cyberattacks as their reliance on IT infrastructure and digital assets grows. The importance of using a comprehensive approach to cyber risk assessment, combining quantitative, probabilistic, and expert methods to consider both the technical characteristics of threats and the context of business processes, is emphasized. It is shown that the use of expected loss models, FAIR, stochastic, and hybrid approaches allows not only to transform technical threats into financial metrics, but also to determine probable scenarios of economic losses, compare alternative risks, and prioritize investments in cyber protection measures. In addition, integrating these approaches contributes to more accurate security budget planning, increases operational resilience, and supports informed decision-making on financing residual risks, including through insurance mechanisms. **Conclusions**. It has been established that the economic assessment of cyber risks is a key tool for the strategic management of digital business models, ensuring sustainability, efficient resource allocation, and supporting regulatory compliance in the face of growing cyber threats.

Keywords: cyber risks, economic assessment, information management, digital business models, cybersecurity, strategic management, investments in cyber defence.

Постановка проблеми. Стрімка цифровізація бізнес-процесів та перехід підприємств до використання цифрових бізнес-моделей значно підвищують їх ефективність, але водночас роблять більш вразливими до кіберзагроз. Зростання кількості кібератак, витоку даних, порушення роботи цифрових сервісів та блокування інформаційних систем призводить до суттєвих економічних втрат, які охоплюють прямі фінансові збитки, репутаційні ризики, штрафи за порушення регуляторних вимог та відплив клієнтів.

Попри актуальність проблеми, підприємства нерідко применшують масштаби кіберризиків або визначають їх лише за допомогою технічних методів, не враховуючи економічних наслідків для бізнес-моделі. Відсутність уніфікованого підходу до економічної оцінки кіберзагроз ускладнює ухвалення управлінських рішень та формування ефективної стратегії кіберзахисту. У результаті виникає суперечність між потребою бізнесу в гарантуванні цифрової безпеки та недостатньою розробленістю методичного інструментарію для комплексної економічної оцінки ризиків кіберзагроз. Саме ця неузгодженість окреслює наукову проблему дослідження – необхідність розроблення економічно обґрунтованого підходу до ідентифікації, оцінки та мінімізації кіберризиків у цифрових бізнес-моделях.

Аналіз останніх досліджень і публікацій. Проблему кіберризиків у цифрових бізнес-моделях активно вивчають сучасні науковці, які намагаються розробити дієві підходи до їх оцінки та мінімізації. Так, Ю. Смоляк аналізує питання гарантування кібербезпеки під час використання дистанційних комунікацій у процесі цифрової трансформації підприємства. Автор підкреслює, що ефективне управління кіберризиками є головним фактором стабільності бізнесу та забезпечення безперервності операційних процесів [1]. Роль кіберзахисту у формуванні бізнес-моделі підприємства в умовах цифрової економіки вивчають Л. Шостак, А. Федонюк та О. Помазун. Вони зазначають, що кіберризики мають прямий вплив на економічну ефективність і конкурентоспроможність підприємств [2]. Метод комплексної оцінки ризиків кібербезпеки для розподілених інформаційних систем пропонують Д. Палко та Л. Мирутенко. Їхній підхід дає змогу інтегрувати різні моделі оцінки, підвищуючи точність прогнозування потенційних загроз [3]. Науковці О. Пташенко, О. Кириленко та О. Курцев досліджують, як цифрові трансформації кардинально змінюють сучасний економічний простір, зосереджуючись на їх впливі на людський капітал, інклюзію та безпеку. Автори наголошують, що для максимізації позитивних змін треба розробити

 ISSN 3041-2129

стратегії з поліпшення цифрових навичок, гарантування рівного доступу до технологій та укріплення кібербезпеки [4]. Роль диджиталізації як основного фактору, що породжує нові внутрішні та зовнішні загрози для економічної безпеки України, вивчають А. Кудінова, О. Маслій, А. Буряк. На основі проведеного аналізу вони пропонують алгоритм формалізованого управління цими ризиками та обґрунтовують необхідність інтеграції технічних, організаційних і освітніх заходів для гарантування належного рівня безпеки [5]. Нейромережевий підхід для оцінки кіберризиків у великих динамічних мережах рекомендує В. Крундишев (V. Krundyshev). Метод дає змогу враховувати численні взаємодіючі пристрої, проте потребує великих обсягів навчальних даних і складний у реалізації [6]. Науковці С. Горбаченко та Н. Клєвцєвич узагальнюють підходи до координації економічного розвитку, доводячи, що перехід від традиційної лінійної до циркулярної економіки є критично важливим для світової стійкості, причому він неможливий без відповідної цифрової бази. Хоча впровадження цифрових технологій створює нові ризики (від втрати даних до втрати робочих місць), гарантування дієвої кібербезпеки є основним, оскільки вона нерозривно пов’язана з подальшим становленням циркулярної економіки та реалізацією її переваг [7]. Учені П. Фісуненко та Ю. Булєєв досліджують спектр ризиків, які виникають у процесі цифрової трансформації підприємств і загрожують їхній стійкості, та визначають вагомі загрози для фінансової, інформаційної, технічної та кадрової сфер. Результатом роботи є авторська класифікація ризиків, на основі якої запропоновано концептуальний підхід до їх систематизації, що слугує інструментом для посилення антикризової та адаптивної спроможності суб’єктів господарювання [8]. Науковці Дж. Ван (J. Wang), М. Ніл (M. Neil) та Н. Фентон (N. Fenton) використовують баєсівські мережі для прогнозування ризиків у корпоративних мережах. Метод показав високу ефективність у моделюванні сценаріїв атак, проте потребує значних обчислювальних ресурсів для навчання моделей [9]. Колектив науковців під керівництвом М. Екстедт

 ISSN 3041-2129

(M. Ekstedt) визначає гібридний підхід до оцінки кіберризиків, що поєднує декілька моделей і дає змогу динамічно коригувати рівень ризику відповідно до змін у конфігурації системи. Такий метод покращує підтримку ухвалення рішень і допомагає ефективніше мінімізувати негативний вплив кіберзагроз [10].

Виділення невирішених раніше частин загальної проблеми. Попри наявність численних наукових праць, окремі аспекти проблеми економічної оцінки кіберризиків у цифрових бізнес-моделях залишаються мало опрацьованими. Зокрема, більшість досліджень зосереджені на технічній характеристиці загроз, тоді як економічний вплив на бізнес-моделі часто ігнорується.

Невирішеним є питання формалізованої оцінки непрямих втрат, пов'язаних із підривом довіри клієнтів та зменшенням ринкової вартості компанії після кіберінциденту. Окрім того, значна частина моделей обмежено враховують адаптивний характер цифрових бізнес-моделей, де ризики швидко мігрують між партнерами по ланцюгу створення вартості. Також недостатньо гібридних методологій, здатних інтегрувати якісні управлінські параметри з кількісним прогнозуванням, необхідним для підтвердження інвестицій у кіберзахист.

Формулювання цілей статті (постановка завдання). Основною метою статті є дослідження теоретико-методичних засад економічного вимірювання кіберризиків та обґрунтування їх впливу на стійкість функціонування цифрових бізнес-моделей. У рамках цієї роботи поставлено такі завдання:

1. Вивчити специфіку кіберзагроз та їх економічний вплив на цифрові бізнес-моделі.

2. Проаналізувати сучасні методи економічної оцінки кіберризиків і визначити їх ефективність для підтримки стратегічного управління та інвестицій у кібербезпеку.

Виклад основного матеріалу дослідження. Сучасний бізнес нерозривно пов'язаний із цифровими технологіями, що є основою цифрових бізнес-моделей, які забезпечують створення, надання та отримання цінності в електронному вигляді. Однак ця залежність спричиняє значну вразливість перед кіберзагрозами, які можуть мати катастрофічні економічні наслідки. Економічна оцінка цих ризиків стає критично важливим складником стратегічного управління кіберзахистом та стійкістю цифрових бізнес-моделей. У цьому контексті актуальним є формування цілісного інформаційного менеджменту цифрової економіки, де стратегічний аспект управління базується на ефективній візуалізації даних для підтримки ухвалення рішень [11].

На теперішній час економіка України потребує дієвих інструментів підтримки новаторської діяльності, які можуть гарантувати сталий розвиток національного механізму генерування новацій [12]. Упровадження нових технологій у виробництво є вагомим кроком для інтеграції наукових досягнень у реальний сектор економіки [13; 14]. Цей процес не лише стимулює появу інноваційних продуктів, але й значно підвищує ефективність виробничих процесів, сприяючи економічному зростанню. Цифровізація суттєво трансформує сучасний економічний ландшафт, висуваючи нові вимоги до бізнесу щодо адаптації до динамічних ринкових умов [15, с. 856]. Сучасні дослідження підтверджують, що використання штучного інтелекту та передових цифрових інструментів стає визначальним фактором зростання капіталізації підприємств у довгостроковій перспективі [16]. Проте цифровізація бізнес-процесів неминуче посилює залежність діяльності компаній від їх IT-інфраструктури, що зумовлює їхню чутливість до кіберризиків та потребує вдосконалення рівня кіберзахисту як обов'язкової умови та невід'ємного елементу сталого інноваційного розвитку [1; 17; 18].

Кібербезпека є складним, але важливим компонентом ефективної роботи сучасного бізнесу. В епоху стрімкого використання інтернету будь-яка

організація поступово перетворюється на цифрову, впроваджуючи нові технології, інструменти та форми організації праці. Так кожний бізнес-процес стає лише окремою ланкою у великому ланцюзі взаємопов'язаних елементів. Тому компаніям дедалі важче визначати критично важливі точки власної розгалуженої інфраструктури, через яку здійснюється взаємодія із зовнішнім середовищем. Зростання цієї залежності неодмінно підвищує вразливість систем, сприяючи успішній реалізації хакерських атак [2, с. 5].

На сьогодні кіберзагрози є головними викликами для бізнесу. У країнах Європи за останні п'ять років частка компаній, що постраждали від кібератак, зросла з 28% до 80% [19]. В Україні лише за перше півріччя 2025 року Державний центр кіберзахисту зафіксував 3 018 інцидентів, тоді як у другому півріччі 2024 року їх було 2 575, відзначаючи приріст на 17% лише за шість місяців [20].

Така динаміка свідчить про те, що інтенсивність атак невпинно зростає, а отже, підприємства опиняються під дедалі більшим цифровим тиском. Для ефективної протидії кіберризикам важливо усвідомити, з якими саме типами загроз найчастіше стикається український бізнес. У табл. 1 систематизовано й охарактеризовано найпоширеніші з них.

Таблиця 1

Поширені кіберзагрози для українського бізнесу

Вид загрози	Опис
Злом простих паролів (наприклад, 1234)	Зловмисники часто підбирають елементарні паролі, що дає їм змогу отримати доступ до важливої корпоративної інформації
Вимагальне програмне забезпечення (malware, ransomware)	Шифрує дані користувачів і вимагає викуп за їх відновлення. Злочинці можуть погрожувати оприлюднити конфіденційну інформацію в разі несплати
DDoS-атака	Велика кількість заражених комп'ютерів перевантажує сервер трафіком, що призводить до зупинки роботи сайтів або додатків
Фішинг	Спроби отримати конфіденційні дані (логіни, паролі, фінансову інформацію) через підроблені електронні листи або сайти
Wiper-атаки	Вірус, який знищує дані. Без резервних копій компанія може втратити їх назавжди

Вид загрози	Опис
Неліцензоване ПЗ зі шкідливим кодом	Встановлення піратського програмного забезпечення може надати зловмисникам доступ до корпоративної інформації. Часто поширюється через сумнівні торент-трекери
Соціальна інженерія	Використання психологічних маніпуляцій для отримання доступу до систем або конфіденційної інформації
Загрози зсередини організації	Ризики виникають від співробітників, які свідомо чи несвідомо розкривають або передають закриту інформацію

Джерело: узагальнено авторами за [1, с. 2]

Представлений перелік кіберзагроз яскраво демонструє широкий спектр потенційних уразливостей, з якими стикається український бізнес. Однак простої ідентифікації цих загроз недостатньо для ефективного управління інформаційною безпекою. Щоб ухвалювати зважені рішення щодо інвестицій у захист та пріоритезації заходів безпеки, компаніям необхідно не лише знати про існування загроз, а й оцінювати їх економічний вплив на діяльність бізнесу.

Особливо важливою економічна оцінка кіберризиків є для цифрових бізнес-моделей, де значна частина цінності створюється завдяки інформаційним технологіям та даним.

У цьому контексті саме бізнес-модель підприємства має вагоме значення, оскільки є основою для коректної економічної оцінки [21, с. 2]. Розуміння бізнес-моделі дає змогу точно визначити найбільш критичні активи (наприклад, платформи, унікальні торгові пропозиції чи бази даних клієнтів), охарактеризувати залучені ресурси й потенційні витрати на реалізацію бізнес-процесів, які стануть об’єктами атаки. Це забезпечує можливість адекватно обчислити розмір потенційних збитків у разі порушення цілісності, доступності чи конфіденційності цих головних елементів.

Економічна оцінка – це процес, який перекладає технічні сценарії інцидентів у грошові показники (наприклад, очікувані щорічні витрати, втрати виручки за період простою, вартість відновлення). Це дає змогу зіставляти ризики між собою, пріоритезувати інвестиції в заходи захисту та розраховувати оптимальні моделі фінансування залишкового ризику (включно

зі страхуванням). Такий підхід сприяє узгодженню кібербезпеки з бізнес-цілями та бюджетом компанії.

Основні складники економічної оцінки кіберризиків систематизовано на рис. 1.

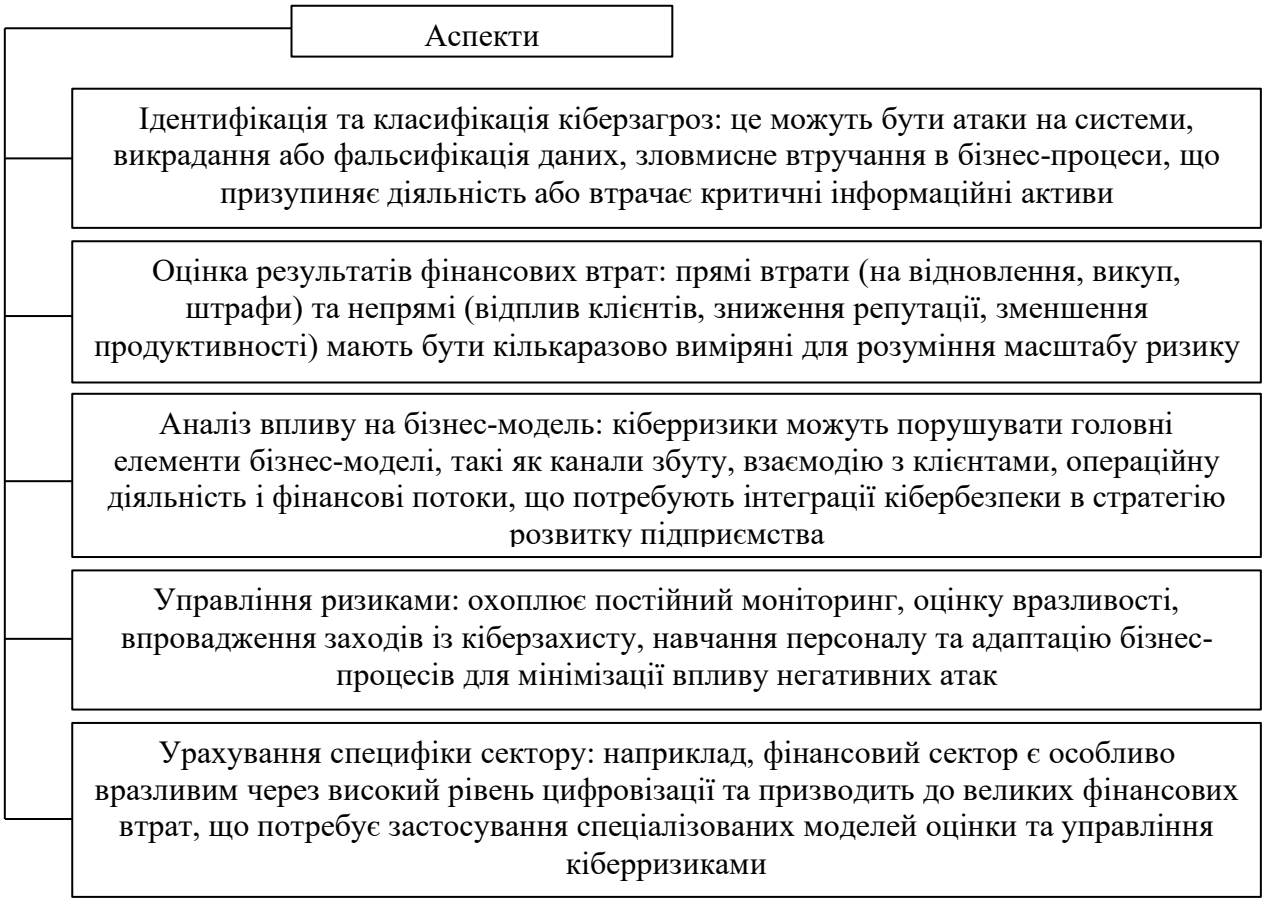

Рис. 1. Основні елементи економічної оцінки кіберризиків

Джерело: складено авторами

Оцінка кіберризиків у цифрових бізнес-моделях ґрунтується на поєднанні кількісних, імовірнісних та гібридних методів, які дають змогу перетворювати технічні параметри загроз на економічно значущі показники. Сучасні підходи різняться за рівнем формалізації, вимогами до даних і точністю прогнозування, проте всі вони спрямовані на отримання об’єктивного аналізу можливих втрат для бізнесу.

Однією з базових груп методів є *моделі очікуваних втрат (Expected Loss / Annualized Loss Expectancy)*. Вони поєднують оцінку ймовірності кіберінциденту з розрахунком грошового збитку, даючи змогу визначати

очікуваний рівень втрат на рік [20]. Цей підхід є корисним для порівняння альтернативних ризиків та оптимізації інвестицій у кіберзахист.

Більш структурованим та формалізованим методом є *FAIR (Factor Analysis of Information Risk).* Фреймворк допомагає кількісно оцінювати частоту подій та масштаб втрат, формуючи розподіл економічних наслідків ризику. FAIR став одним із найпоширеніших інструментів для переведення технічних параметрів у бізнес-метрики та підтримки фінансово обґрунтованих рішень [22].

Для врахування невизначеності широко застосовують стохастичні методи, зокрема моделювання Монте-Карло та сценарний аналіз. Вони дають змогу оцінити діапазон можливих втрат та проаналізувати завершальні події – малоймовірні, але потенційно катастрофічні інциденти. Ефективність цих методів, як зазначають Т. Фагаде (T. Fagade), К. Мараслiс (K. Maraslis) і Т. Трифонас (T. Tryfonas) [23], значною мірою залежить від точності вихідних даних та обчислювальних можливостей.

У відповідь на обмеженість класичних методів сучасні дослідники пропонують гібридні моделі, які поєднують експертні оцінки з аналізом машинного навчання та статистичними техніками [24]. Це підвищує точність оцінювання через адаптивне калібрування параметрів ризику. Використання машинного навчання дає змогу об’єктивно скоригувати суб’єктивні судження експертів на основі аналізу фактичних історичних інцидентів та фінансових втрат, що забезпечує не лише вищу прогностичну точність, але й перетворює ризики на кількісні фінансові показники, необхідні для ефективного ризик-орієнтованого ухвалення рішень. Отже, гібридна модель стає гнучким і надійним інструментом, що адаптується до швидких змін у ландшафті цифрових загроз.

Важливу роль у практиці управління вразливостями відіграє загальна система їх оцінювання – CVSS (Common Vulnerability Scoring System), розроблена FIRST (Forum of incident response and security teams) [25]. Отже, у

сучасному цифровому середовищі для оцінки ризиків потрібне використання комплексних та адаптивних методологій, які виходять за рамки класичних моделей. Так, перший підхід [26] пропонує інтеграцію детальних особливостей активів та специфіки вразливостей, що їм притаманні, для створення обґрунтованої моделі оцінки. Замість загальної характеристики методологія надає вагові коефіцієнти, які залежать від критичності конкретного активу (наприклад, сервер із даними клієнтів проти публічного вебсайту) та складності експлуатації виявленої вразливості, забезпечуючи в такий спосіб релевантність кінцевої оцінки ризику.

Моделі, засновані на баєсівських мережах [9], використовують для прогнозування ризиків у складних корпоративних мережах. Баєсівська мережа – це спрямований ациклічний граф, який представляє множину випадкових величин та їхні умовні залежності. Це дає змогу моделювати складні сценарії кібератак, де успіх наступного кроку залежить від результату попереднього. Їх цінність полягає в здатності оновлювати ймовірності подій (ризиків) при надходженні нових даних (доказів). Основним обмеженням є потреба в значних обчислювальних ресурсах та високоякісних даних для визначення умовних імовірностей.

Для ситуацій із високою невизначеністю та неточною вихідною інформацією ефективними є методи, що використовують нечітку логіку [27]. На відміну від класичної бінарної логіки (ризик або є, або його немає), нечіткі моделі дають змогу працювати з лінгвістичними змінними (наприклад, «висока важливість», «середня ймовірність»). Це створює можливість брати до уваги контекст середовища, рівень важливості активів та неточність вихідних даних, забезпечуючи механізм оцінки ризику, що ближчий до людського сприйняття невизначеності.

Активно розвивається напрям застосування машинного навчання (МН), зокрема нейромережевих моделей [6]. Нейромережі здатні враховувати складну нелінійну структуру взаємодій у великих розподілених системах,

 ISSN 3041-2129

виявляючи приховані залежності, які не помітні для класичних методів. Вони використовуються для автоматичного виявлення аномалій та прогнозування ризику. Однак, як зазначається [3], такі рішення є складними у впровадженні, потребують висококваліфікованого персоналу та великих, ретельно розмічених масивів навчальних даних для досягнення необхідної точності.

Ігрові моделі [28] розглядають взаємодію між атакувальником та захисником як стратегічну гру з обмеженим або необмеженим числом ходів. Цей підхід унікальним тим, що дає змогу аналізувати оптимальні стратегії захисту, оцінювати економічні вигоди та витрати сторін, а також моделювати поведінку противника в умовах конфлікту. Основним його обмеженням є складність точного опису мотивацій атакувальника та потреба у великій кількості параметрів для адекватного моделювання.

Комплексні гібридні системи поєднують сильні сторони кількісних, логічних та емпіричних методів (наприклад, експертну думку, статистичні моделі та МН-прогнозування). Така інтеграція забезпечує динамічне оновлення параметрів ризику відповідно до змін у конфігурації середовища, створюючи цілісний та адаптивний інструмент для підтримки ухвалення рішень.

Отже, різноманітність сучасних підходів свідчить, що економічна оцінка кіберризиків виходить за межі суто технічних методів і перетворюється на міждисциплінарний інструмент стратегічного управління. Вона дає змогу цифровим бізнес-моделям ухвалювати обґрунтовані рішення щодо інвестицій у безпеку, підтримувати операційну стійкість та гарантувати відповідність нормативним вимогам у сфері кіберзахисту.

Водночас економічна оцінка кіберризиків допомагає цифровим бізнес-моделям перетворити технічні загрози на зрозумілі для менеджменту фінансові метрики, що дає можливість ефективніше розподіляти ресурси та вибирати стратегії фінансування ризику. Однак точність таких оцінок обмежена доступністю даних і швидкістю змін у загрозливому ландшафті.

 ISSN 3041-2129

Тому найкраща практика поєднує кількісні моделі (FAIR, Monte Carlo), навчання моделей машинного навчання та персоналу на реальних інцидентах та активну співпрацю між компаніями, індустрією та регуляторами.

Висновки. Підсумовуючи проведене дослідження, можна констатувати, що економічна оцінка кіберризиків є невід'ємною та важливою частиною стратегічного управління сучасними цифровими бізнес-моделями.

Упровадження цифрових технологій, хоча й підвищує ефективність бізнес-процесів та сприяє інноваційному розвитку, одночасно значно збільшує залежність компаній від IT-інфраструктури та їхню вразливість до кібератак. У цьому контексті економічна оцінка ризиків розв'язує основну управлінську проблему: вона дає змогу трансформувати складні технічні загрози в зрозумілі фінансові метрики, роблячи питання кібербезпеки інтегрованим компонентом бізнес-стратегії, а не лише технічним викликом.

Аналіз сучасних методів оцінки, включно з кількісними моделями (зокрема, FAIR), стохастичними, гібридними та ігровими підходами, демонструє, що її точність залежить від комплексного критерію. Ефективна методологія повинна поєднувати кількісні (фінансові), імовірнісні (прогнозування атак) та експертні (оцінка унікальних активів) методи для гарантування адекватності результатів.

Економічне вимірювання ризиків надає підприємствам інструмент для пріоритезації інвестицій у кіберзахист за принципом співвідношення витрат та вигод (Cost-Benefit Analysis), підтримки операційної стійкості та забезпечення відповідності нормативним вимогам. Це є критично важливим для стабільного функціонування, конкурентоспроможності та сталого розвитку цифрових бізнес-моделей у мінливих ринкових умовах.

Подальші наукові дослідження можуть спрямовуватися на розроблення більш точних та адаптивних методик економічної оцінки кіберризиків, здатних ураховувати швидкі зміни в цифровому середовищі та появу нових загроз.

 ISSN 3041-2129

Список використаних джерел

1. Смоляк Ю. Забезпечення кібербезпеки при використанні дистанційних комунікацій у процесі цифрової трансформації підприємства. *Молодий вчений.* 2025. № 6 (137). С. 45–53. DOI: https://doi.org/10.32839/2304-5809/2025-6-137-8.

2. Шостак Л., Федонюк А., Помазун О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. *Економіка та суспільство*. 2024. № 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-37.

3. Палко Д., Мирутенко Л. Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах. *Кібербезпека: освіта, наука, техніка.* 2024. Т. 2, № 26. С. 487–502. DOI: https://doi.org/10.28925/2663-4023.2024.26.731.

4. Пташенко О. В., Кириленко О. П., Курцев О. Ю. Вплив цифрових трансформацій на розвиток сучасного економічного простору: людський капітал, інклюзія, безпека. *Бізнес Інформ*. 2024. № 7. С. 180–190. DOI: https://doi.org/10.32983/2222-4459-2024-7-180-190.

5. Кудінова А., Маслій О., Буряк А. Формалізація ризиків і загроз економічній безпеці України в умовах цифровізації. *Управління змінами та інновації*. 2024. № 12. С. 25–31. DOI: https://doi.org/10.32782/CMI/2024-12-4.

6. Krundyshev V. Neural network approach to assessing cybersecurity risks in large-scale dynamic networks. 13th International Conference on Security of Information and Networks. 2020. Article 32. P. 1–8. DOI: https://doi.org/10.1145/3433174.3433603.

7. Горбаченко С. А., Клєвцєвич Н. А. Роль кібербезпеки у впровадженні циркулярних економічних моделей: аналіз ризиків та можливостей. *Вісник Херсонського національного технічного університету*. 2024. № 1 (88). С. 342–348. DOI: https://doi.org/10.35546/kntu2078-4481.2024.1.48.

8. Фісуненко П., Булєєв Ю. Класифікація ризиків цифрової трансформації підприємств у контексті економічної безпеки. *Цифрова економіка та економічна безпека: науково-практичний журнал*. 2025. Т. 3, № 18. С. 203–213. DOI: https://doi.org/10.32782/dees.18-31.

9. Wang J., Neil M., Fenton N. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*. 2020. Vol. 89. 101659. DOI: https://doi.org/10.1016/j.cose.2019.101659.

10. Ekstedt M., Afzal Z., Mukherjee P., Hacks S., Lagerström R. Yet another cybersecurity risk assessment framework. *International Journal of Information Security.* 2023. Vol. 22. P. 1713–1729. DOI: https://doi.org/10.1007/s10207-023-00713-y.

11. Левченко О. М., Довгенко Я. О., Яременко Л. І. Інформаційний менеджмент цифрової економіки на основі візуалізації даних: стратегічний аспект. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки».* 2025. № 11. DOI: https://doi.org/10.25313/2520-2294-2025-11-11659.

12. Ilina A. Special fund as a driver of national innovation system development. *Наука і техніка сьогодні. Серія: Економіка.* 2025. № 9 (50). С. 276–296. DOI: https://doi.org/10.52058/2786-6025-2025-9(50)-276-296.

13. Ільїна А. О. Інновації як інструмент модернізації національної інноваційної системи. *Наукові інновації та передові технології. Серія: Економіка*. 2025. № 2 (42). С. 894–909. DOI: https://doi.org/10.52058/2786-5274-2025-2(42)-894-909.

14. Kaptosv L. RESTful API design for geospatial logistics platforms using type script and laravel. *Journal of Information, Technology and Policy*. 2025. P. 1–13. DOI: https://doi.org/10.62836/jitp.2025.515.

15. Alazzam F. A. F., Kiblyk D., Kardashevskyy Y., Yaremenko L., Rodchenko S. Determination of optimal administrative, legal and economic methods for managing artificial intelligence in the context of information security.

International Journal of Religion. 2024. Vol. 5, № 10. P. 856–866. DOI: https://doi.org/10.51751/ijor.v5i10.5154.

16. Левченко О. М., Довгенко Я. О., Замуренко Д. В. Вплив штучного інтелекту та сучасних цифрових технологій на капіталізацію підприємств: регресійний аналіз. *Актуальні проблеми розвитку економіки регіону*. 2025. Т. 2, № 21. С. 344–359. DOI: https://doi.org/10.15330/apred.2.21.344-359.

17. Опірський І. Р., Хохлачова Ю. Є., Стефанків А. В., Шевчук Ю. А. Аналіз технічних особливостей реалізації шифрування даних на SD-картах в Android. *Сучасний захист інформації.* 2025. № 1 (61). С. 219–228. DOI: https://doi.org/10.31673/2409-7292.2025.016526.

18. Poperehnyak S., Syvachenko I., Shevchuk Y. Enhancing pseudorandom number generation using environmental sensor-based entropy sources. *Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)*: proc. of the Workshop. 2025. Vol. 3991. P. 363–380. URL: https://ceur-ws.org/Vol-3991/paper26.pdf (дата звернення: 11.10.2025).

19. Основи кібербезпеки для бізнесу. *Westelecom.ua:* вебсайт. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa (дата звернення: 11.10.2025).

20. Російські кібероперації: аналітика за І півріччя 2025. Державний центр кіберзахисту Держспецзв'язку, Київ. 2025. 24 с. URL: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=71278&embedded=true&a=bi (дата звернення: 11.10.2025).

21. Зибарева О., Лопащук І., Бивших І. Концептуалізація та економічний зміст поняття «бізнес-модель». *Економіка та суспільство*. 2025. № 74. DOI: https://doi.org/10.32782/2524-0072/2025-74-69.

22. Orlando A. Cyber risk quantification: investigating the role of cyber value at risk. *Risks.* 2021. Vol. 9, № 10. 184. DOI: https://doi.org/10.3390/risks9100184.

23. Fagade T., Maraslis K., Tryfonas T. Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach. *International*

Journal of Critical Infrastructures. 2017. Vol. 13, № 2–3. P. 152–167. URL: https://scispace.com/pdf/towards-effective-cybersecurity-resource-allocation-the-14cyqd0ydb.pdf (дата звернення: 11.10.2025).

24. Nwafor C., Nwafor O. Z., Brahma S., Acharyya M. A hybrid FAIR and XG Boost framework for cyber-risk intelligence and expected loss prediction', Expert Systems with Applications. 2026. Vol. 299. 129920. DOI: https://doi.org/10.1016/j.eswa.2025.129920.

25. FIRST. Common Vulnerability Scoring System (CVSS). Official Documentation. 2021. URL: https://www.first.org/cvss/specification-document (дата звернення: 11.10.2025).

26. Aksu M. U., Dilek M. H., Tatlı E. İ., Bicakci K., Dirik H. I., Demirezen M. U., Aykır T. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. *2017 International Carnahan Conference on Security Technology (ICCST)*: proc. 2017. P. 1–8. DOI: https://doi.org/10.1109/CCST.2017.8167819.

27. Alali M., Almogren A., Hassan M. M., Rassan I. A., Bhuiyan M. Z. A. Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*. 2018. Vol. 74. P. 323–339. DOI: https://doi.org/10.1016/j.cose.2017.09.011.

28. Do C. T., Tran N. H., Hong C. S., Kamhoua C. A., Kwiat K. A., Blasch E., Ren S., Pissinou N., Iyengar S. S.. Game theory for cyber security and privacy. *ACM Computing Surveys (CSUR)*. 2017. Vol. 50, № 2. P. 1–37. DOI: https://doi.org/10.1145/3057268.