DOI 10.31558/2307-2318.2026.1.8

УДК 330.131.7:658.5
JELClassification: G32, M21, O33.

Козловський С. В.
д.е.н., професор кафедри підприємництва,
корпоративної та просторової економіки
Донецький національний університет імені Василя Стуса, м. Вінниця
ORCID: https://orcid.org/0000-0003-0707-4996
s.kozlovskyy@donnu.edu.ua
Чеботок В. В.
аспірант
Донецький національний університет імені Василя Стуса, м. Вінниця
ORCID: https://orcid.org/0009-0003-6987-8698
v.chebotok@donnu.edu.ua

РИЗИК-МЕНЕДЖМЕНТ ЯК СТРАТЕГІЯ УПРАВЛІННЯ ЕКОНОМІЧНОЮ ДІЯЛЬНІСТЮ ПІДПРИЄМСТВА

У статті досліджено ризик-менеджмент як стратегічну основу управління економічною діяльністю підприємства в умовах воєнної нестабільності, макроекономічної турбулентності та цифрової трансформації. Актуальність теми зумовлена зростанням рівня невизначеності зовнішнього середовища, посиленням конкуренції, появою нових цифрових і воєнних ризиків, що потребують формування інтегрованої системи стратегічного управління ризиками. Метою статті є обґрунтування теоретичних засад і розроблення практичних підходів до формування системи ризик-менеджменту як стратегічного інструменту управління економічною діяльністю підприємства. У роботі систематизовано основні інструменти управління ризиками (прийняття, уникнення, передача, мінімізація), визначено структурні елементи процесу ризик-менеджменту та запропоновано модель організації бізнес-процесу в межах реалізації стратегії управління ризиками. Розкрито концепцію зон ризику (безризикова, допустима, критична, катастрофічна), що дозволяє оцінити рівень концентрації ризику та забезпечити своєчасне коригування управлінських рішень. Особливу увагу приділено цифровим ризикам, які виникають у процесі впровадження наскрізних цифрових технологій, зокрема штучного інтелекту, великих даних, робототехніки та систем розподіленого реєстру. Запропоновано авторську класифікацію ризиків цифрової трансформації підприємства, виокремлено економічні, технічні, організаційні та воєнні ризики, а також визначено ключові ризики використання технологій штучного інтелекту (ризик конфіденційності, інфраструктурний, ризик статистичної дискримінації, ухвалення некоректних управлінських рішень, кадровий дисбаланс тощо). Обґрунтовано необхідність інтеграції цифрових ризиків у систему корпоративного ризик-менеджменту (ERM). Розглянуто сучасні стратегічні підходи до управління ризиками – модель «трьох ліній захисту», метод визначення ризик-апетиту та толерантності до ризику, а також формування ризик-культури та ефективних комунікацій. Доведено, що їх комплексне застосування створює цілісну архітектуру управління ризиками, орієнтовану на превентивне реагування, збалансування прибутковості та стійкості, підвищення рівня економічної безпеки підприємства.

Зроблено висновок, що ризик-менеджмент у сучасних умовах виступає не лише механізмом мінімізації загроз, а стратегічною концепцією забезпечення довгострокової стабільності, інноваційного розвитку та конкурентоспроможності підприємства в умовах цифрової економіки та воєнних викликів.

Ключові слова: ризик-менеджмент, стратегічне управління, економічна діяльність підприємства, цифрова трансформація, цифрові ризики, управління економічною безпекою, корпоративний ризик-менеджмент, ризик-апетит, ризик-культура, штучний інтелект, інформаційна безпека, воєнні ризики, інноваційний розвиток.

Рис. 6, Табл. 2, Літ. 20.

Kozlovskyi Serhii
Doctor of Economics, Professor of the Department of Entrepreneurship,
Corporate and Spatial Economics
Vasyl' Stus Donetsk National University, Vinnytsia
ORCID: https://orcid.org/0000-0003-0707-4996
s.kozlovskyy@donnu.wdu.ua
Chebotok Vasyl
postgraduate student of Vasyl' Stus Donetsk National University, Vinnytsia
ORCID: https://orcid.org/0009-0003-6987-8698
v.chebotok@donnu.edu.ua

RISK MANAGEMENT AS A STRATEGY FOR MANAGING THE ECONOMIC ACTIVITY OF AN ENTERPRISE

The article examines risk management as a strategic foundation for managing the economic activity of an enterprise under conditions of wartime instability, macroeconomic turbulence, and digital transformation. The relevance of the topic is driven by the growing level of environmental uncertainty, intensified competition, and the emergence of new digital and war-related risks that require the formation of an integrated system of strategic risk management. The purpose of the article is to substantiate the theoretical foundations and develop practical approaches to the formation of a risk management system as a strategic tool for managing the economic activity of an enterprise.

The paper systematizes the main risk management instruments (risk acceptance, avoidance, transfer, and mitigation), identifies the structural elements of the risk management process, and proposes a model for organizing business processes within the framework of a risk management strategy. The concept of risk zones (risk-free, acceptable, critical, and catastrophic) is disclosed, enabling the assessment of risk concentration levels and ensuring timely adjustments of managerial decisions.

Special attention is paid to digital risks arising from the implementation of cross-cutting digital technologies, including artificial intelligence, big data, robotics, and distributed ledger systems. The authors propose an original classification of digital transformation risks at the enterprise level, distinguishing economic, technical, organizational, and war-related risks, as well as identifying key risks associated with the use of artificial intelligence technologies (data privacy risk, infrastructure risk, statistical discrimination risk, incorrect managerial decision-making risk, workforce imbalance risk, etc.). The necessity of integrating digital risks into the corporate risk management system (ERM) is substantiated.

The article also considers modern strategic approaches to risk management, including the "three lines of defense" model, the method of defining risk appetite and risk tolerance, and the development of risk culture and effective communication. It is proved that their integrated

application creates a holistic risk management architecture aimed at preventive response, balancing profitability and sustainability, and enhancing the economic security of the enterprise. It is concluded that under modern conditions, risk management acts not only as a mechanism for minimizing threats but also as a strategic concept for ensuring long-term stability, innovative development, and competitiveness of an enterprise in the context of the digital economy and wartime challenges.

Keywords: risk management, strategic management, economic activity of an enterprise, digital transformation, digital risks, economic security management, corporate risk management, risk appetite, risk culture, artificial intelligence, information security, wartime risks, innovative development.

Fig. 6, Tab. 2, Ref. 20.

Вступ. У сучасних умовах воєнних викликів, макроекономічної нестабільності та трансформаційних процесів в Україні особливої актуальності набуває ризик-менеджмент як стратегія управління економічною діяльністю підприємства. Динамічність зовнішнього середовища, посилення конкурентного тиску, розриви логістичних ланцюгів, коливання фінансових ринків і зміни регуляторної політики формують багаторівневе поле невизначеності, у межах якого підприємства змушені функціонувати та розвиватися. За таких умов стратегічне управління більше не може обмежуватися лише плануванням і контролем ресурсів – воно має ґрунтуватися на системному передбаченні, ідентифікації, оцінці та мінімізації ризиків.

Ризик-менеджмент стає інтегрованою складовою економічної стратегії підприємства, спрямованою на забезпечення фінансової стійкості, підвищення адаптивності бізнес-моделі та формування довгострокових конкурентних переваг. Для топменеджменту ключовим завданням є створення ефективної системи управління ризиками, яка поєднує аналітичні інструменти, сучасні методи прогнозування та механізми оперативного реагування. Така система повинна не лише мінімізувати втрати, а й трансформувати ризики у можливості розвитку, сприяти оптимізації бізнес-процесів та підвищенню рентабельності діяльності.

Разом із тим цифровізація породжує нові види ризиків – кіберзагрози, витоки конфіденційної інформації, технологічні збої, залежність від зовнішніх цифрових платформ, правові ризики, пов’язані з інтелектуальною власністю та захистом персональних даних. Інтелектуальні системи, які приймають або підтримують управлінські рішення, формують додаткові виклики щодо відповідальності, етичності та безпеки їх використання. Таким чином, стратегічний ризик-менеджмент має охоплювати не лише традиційні фінансові чи операційні ризики, а й цифрові, інформаційні та репутаційні загрози.

Отже, ризик-менеджмент у сучасних умовах виступає не лише інструментом захисту від небезпек, а комплексною стратегічною концепцією управління економічною діяльністю підприємства, що забезпечує його стійкість, інноваційний розвиток і конкурентоспроможність у середньо- та довгостроковій перспективі.

Постановка проблеми. В умовах воєнної нестабільності, макроекономічної турбулентності, цифрової трансформації та структурних змін у національній економіці підприємства функціонують у середовищі підвищеної невизначеності та багаторівневих ризиків. Традиційні підходи до управління економічною діяльністю, орієнтовані переважно на короткострокове планування та реагування на вже наявні проблеми, втрачають ефективність і не забезпечують належного рівня фінансової стійкості та конкурентоспроможності. Відсутність інтегрованої системи стратегічного ризик-менеджменту, здатної поєднувати інструменти прогнозування, цифрові аналітичні технології та механізми превентивного управління, зумовлює зростання втрат, зниження

інвестиційної привабливості та погіршення економічних результатів діяльності підприємств. У зв'язку з цим постає необхідність теоретичного обґрунтування та розроблення практичних підходів до формування ризик-менеджменту як стратегічної основи управління економічною діяльністю підприємства в умовах сучасних викликів.

Аналіз останніх досліджень і публікацій. Дослідженням проблем ризик-менеджменту та стратегічного управління присвячені праці відомих вчени: Адамів М. Є., Гейдор А. П., Герасименко О. М., Данілова Е. І., Демиденко К. О., Дуднєва Ю., Дороніна О. А., Заремба К. В., Калетнік Г. М., Карпенко Н. В., Коцин А. Р., Кочін І. В., Криков'язюк І. В., Кузьмін О. Є., Кулик Ю. М., Лавров Р. В., Мельник О. Г., Мирошниченко Г., Морщенюк Т. С., Мушникова С. А., Пасєка С. Р., Пушненко А. С., Ревуцька Н. В., Скомаровський В. В., Соболь О. М., Тьопа В., Хаджинова І., Швиданенко Г. О., A. Smith, A. Hamscher, A. Osterwalder, A. Hanelt, A.-W. Scheer, F. Knight, G. Kane, H. Markowitz, I. Jacobson, J. Jeston, J. Martin, J. Nelles, K. Ishikawa, K. Stensrud, L. Pfeffer, L. Buntic, M. Kirchmer, M. Champy, M. E. Porter, M. Hammer, M. Sugeno, M.-F. Hsu, N. Fenton, R. L. Katz, R. S. Kaplan, T. H. Davenport, T. Takagi, W. E. Deming, W. F. Sharpe та ін., які досліджували питання переходу підприємств до процесного та ризик-орієнтованого управління, теорію та практику реінжинірингу бізнес-процесів. Однак вони не розглядають принципові відмінності між аналітичними та виконуваними моделями, застосовуючи традиційні підходи, розроблені для аналітичного моделювання.

Водночас, незважаючи на значний науковий доробок зазначених авторів, у їхніх працях переважно акцентується увага на загальнотеоретичних аспектах управління ризиками, фінансовому аналізі або реінжинірингу бізнес-процесів без належного врахування трансформаційних змін цифрової економіки та воєнно-кризового контексту функціонування підприємств. Зокрема, недостатньо дослідженим залишається питання інтеграції ризик-менеджменту в стратегічну архітектуру управління економічною діяльністю підприємства з урахуванням відмінностей між аналітичними моделями, що використовуються для прогнозування та оцінювання ризиків, і виконуваними (операційними) моделями, які безпосередньо імплементуються в бізнес-процеси та цифрові системи управління. Таким чином, актуальним є формування концептуальних засад ризик-менеджменту як комплексної стратегії управління економічною діяльністю підприємства, що поєднує процесний підхід, цифрові інструменти, аналітичне моделювання та практичну імплементацію у систему корпоративного управління.

Мета статті – обґрунтувати теоретичні засади і розробити практичні підходи до формування системи ризик-менеджменту як стратегічного інструменту управління економічною діяльністю підприємства.

Виклад основного матеріалу. Основною метою ризик-менеджменту є максимізація стійкості всіх видів діяльності підприємства в поточному періоді та забезпечення стабільного розвитку у довгостроковій перспективі. Своєчасно виявляючи та оптимізуючи ризики, підприємство може збалансувати позитивні й негативні наслідки їх настання для забезпечення стійкого функціонування в умовах невизначеності.

Завданням ризик-менеджменту є пошук стратегії, яка забезпечує прийнятне для організації поєднання потенційного ризику та доходу.

Серед додаткових завдань ризик-менеджменту можна виокремити [1]:

- побудову ризикової моделі для конкретної організації;
- виявлення всіх потенційних внутрішніх і зовнішніх ризиків, включно з визначенням того, як одні ризики можуть впливати на появу інших або на вже існуючі;
- визначення ймовірності виникнення, небезпеки, можливого збитку та наслідків кожного ризику;

– оцінку допустимого для організації рівня ризику.

Допустимий рівень ризику показує, наскільки значними можуть бути наслідки ризику для системи управління підприємством. Реалізовані ризики не враховуються під час цієї оцінки, оскільки вони є поточними проблемами організації – такі ризики вже враховані підприємством.

Під час розв'язання завдань, спрямованих на забезпечення економічної безпеки підприємства, використовують один із чотирьох основних інструментів управління ризиками – див. рис. 1 [2, 3].

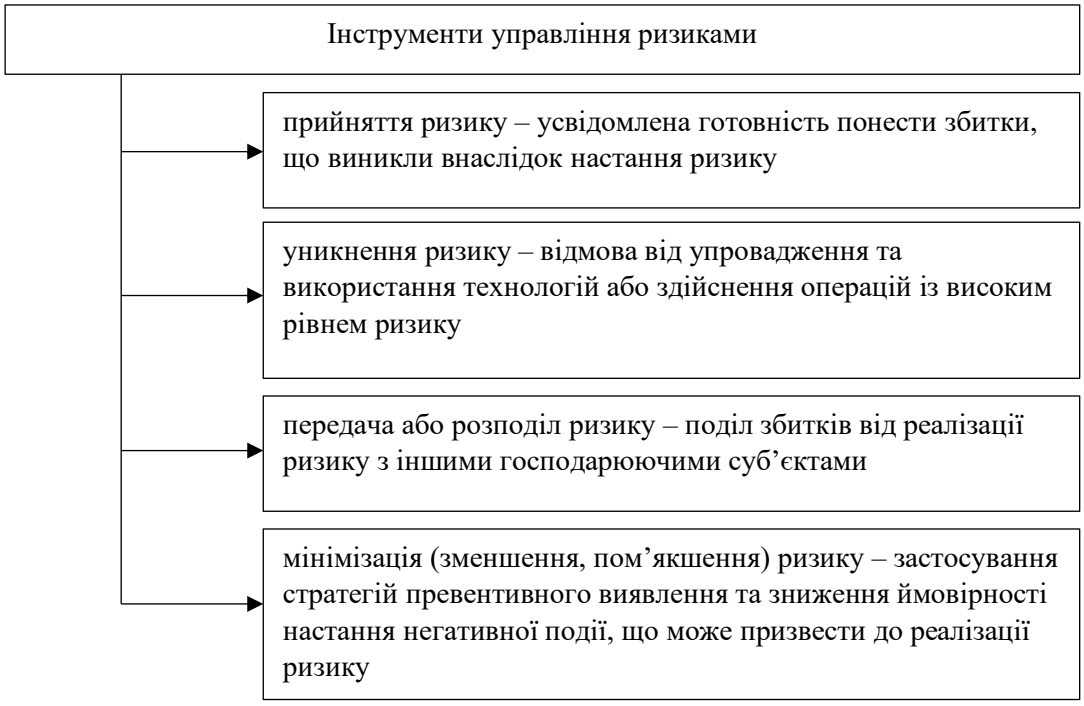

Рисунок 1 – Інструменти управління ризиками

Розроблено з використанням [2, 3]

Базова модель організації бізнес-процесу в межах реалізації стратегії ризик-менеджменту виглядає наступним чином – див. рис. 2.

Структурними елементами процесу управління ризиками є [**Ошибка! Закладка не определена.**, **Ошибка! Закладка не определена.**, **Ошибка! Закладка не определена.**]:

– взаємодія та консультування зовнішніх і внутрішніх учасників господарського процесу на кожному етапі;
– визначення зовнішніх характеристик підприємницького середовища, внутрішніх характеристик організації та параметрів управління ризиками, у межах яких буде реалізовано процес;
– визначення вимог до діяльності організації, на основі яких формуються структура та методи аналізу ризиків;
– визначення ризикових ситуацій;
– аналіз наслідків виникнення ризикових ситуацій, імовірності їх появи, а також причин і факторів виникнення;
– оцінка ризиків: порівняння рівня ризику з раніше встановленими критеріями, визначення балансу між потенційними вигодами та негативними наслідками;

– ухвалення та реалізація ризикового рішення: визначення й упровадження доцільних стратегій і планів заходів;
– контроль та аналіз ефективності всіх етапів процесу управління ризиками.

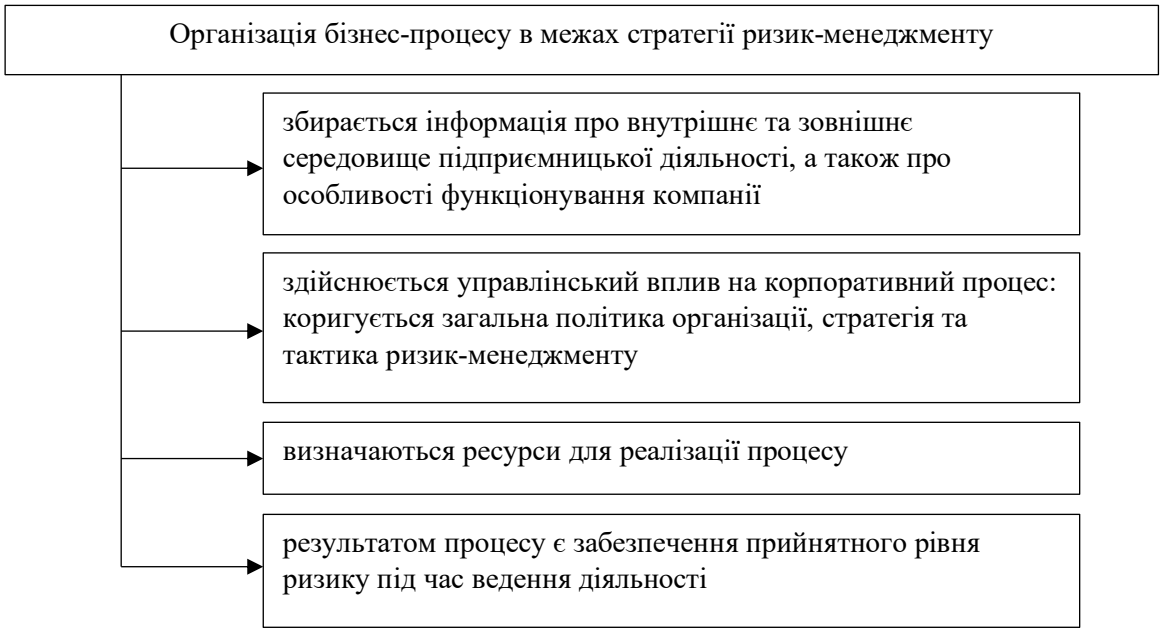

Рисунок 2 – Модель організації бізнес-процесу в межах стратегії ризик-менеджменту

Розроблено з використанням [4]

Сукупність наведених елементів визначає межі процесу ризик-менеджменту [5, 6]:
– безризикова зона – знаходиться між точками повного розрахункового прибутку та мінімального розрахункового прибутку;
– зона допустимого ризику – між точкою мінімального розрахункового прибутку та точкою беззбитковості;
– зона критичного ризику – між точкою беззбитковості та точкою бездоходності;
– зона катастрофічного ризику – між точкою беззбитковості та точкою банкрутства з втратою всього капіталу.

Розподіл операцій за зонами ризику дозволяє оцінити рівень концентрації ризику у відповідних зонах залежно від розміру можливих збитків. Перебування операцій у небезпечних зонах ризику є сигналом до більш ретельного контролю на наступних етапах ризик-менеджменту. Таке підвищене увага зумовлене посиленням конкуренції, ускладненням умов підприємницької діяльності та, відповідно, появою нових типів ризиків, не характерних для попередніх етапів функціонування підприємств і організацій.

Таким чином, з позиції інформаційного суспільства, можна зробити такий висновок: цифрова трансформація сучасного підприємства передбачає управління ризиками на всіх етапах його функціонування – від постановки цілей і оцінки готовності підприємства до впровадження нових технологій до реалізації практичних моделей ризик-менеджменту та періодичного перегляду самої корпоративної системи управління ризиками. Управління «цифровими» ризиками та запобігання їх наслідкам є важливим елементом корпоративного управління підприємством. Водночас, крім розроблення загальної корпоративної стратегії ризик-менеджменту на рівні підприємства, необхідно реалізовувати стратегії на рівні конкретних проєктів і підрозділів, з урахуванням їх специфіки та унікальності.

Зростання ролі інформаційно-комунікаційних технологій, автоматизації, штучного інтелекту та великих даних створює нові можливості для підвищення ефективності бізнес-процесів, але водночас формує і нову групу ризиків – цифрові ризики, які мають бути інтегровані у загальну систему ризик-орієнтованого управління підприємством.

Ризик-орієнтоване управління передбачає ідентифікацію, оцінювання, моніторинг та мінімізацію ризиків, що впливають на досягнення стратегічних цілей організації. У цьому контексті цифрові ризики розглядаються не як окрема категорія загроз, а як невід'ємна складова комплексної системи управління ризиками (ERM – Enterprise Risk Management). Їхня природа пов'язана з процесами цифровізації, які охоплюють усі рівні функціонування підприємства – від виробничих операцій і фінансових розрахунків до взаємодії з клієнтами та партнерами.

Інтеграція управління цифровими ризиками у систему ризик-менеджменту дозволяє підприємству збалансувати потенціал інновацій із рівнем прийнятного ризику. Це означає, що кожне цифрове рішення (впровадження штучного інтелекту, хмарних сервісів, блокчейн-систем чи IoT-рішень) має оцінюватися не лише з позиції технічної ефективності, а й з погляду можливих загроз інформаційній безпеці, репутаційних втрат, фінансових збитків або порушення безперервності бізнес-процесів.

Ключовими принципами ризик-орієнтованого управління цифровими ризиками є:

- системність – врахування взаємозв'язку між технологічними, економічними та організаційними ризиками;
- проактивність – прогнозування ризикових подій до моменту їх виникнення;
- адаптивність – гнучке реагування на зміни технологічного середовища;
- безперервність – постійний моніторинг і вдосконалення процедур управління ризиками.

Таким чином, цифрові ризики є не лише викликом, а й невід'ємним елементом стратегічного ризик-орієнтованого підходу, який дозволяє забезпечити стійкість і конкурентоспроможність підприємства в умовах цифрової економіки. Ефективне управління цими ризиками вимагає поєднання технічних, організаційних і управлінських рішень, що дозволяють зберігати баланс між інноваційністю та безпекою бізнесу.

«Цифрові» ризики стають дедалі гострішою проблемою для сучасного підприємства, оскільки традиційні стратегії ризик-менеджменту можуть допомагати управляти цими ризиками лише до певного моменту. Розвиток інформаційно-комунікаційних технологій призвів до суттєвих змін у традиційних концепціях корпоративного ризик-менеджменту: цифрові технології створюють якісно нові небезпеки та загрози для підприємства. Вплив сучасних «цифрових» ризиків не обмежується межами самої компанії, а дедалі частіше поширюється на всю екосистему взаємодії з клієнтами, партнерами та конкурентами [7].

До ризиків цифрової трансформації підприємства належать економічні, технічні та організаційні ризики.

Економічні ризики, що виникають унаслідок імплементації нових технологій у господарську діяльність компанії, виділяють в окрему категорію ризиків. З одного боку, інвестиції в нові технології «мають величезний економічний потенціал і відкривають можливості для постійного вдосконалення різних процесів та підприємства загалом», з іншого – подібне інвестування «визначає необхідність оцінки ризиків, пов'язаних із доцільністю та своєчасністю інвестицій у конкретні технології з позиції довгострокових перспектив і бар'єрів для їх використання» [8]. Економічні ризики також пов'язані зі складністю оцінювання ефектів від упровадження технологій та інтелектуалізації бізнес-процесів, обґрунтуванням доцільності інвестицій в інноваційні технології,

функціонування яких нерозривно пов'язане з уже наявними «зрілими» інформаційно-комунікаційними технологіями.

Технічні ризики пов'язані з ресурсним потенціалом і інфраструктурною базою підприємства. Багато компаній не можуть самостійно інтегрувати цифрові інновації у свою господарську діяльність. Однак наявність необхідних компетенцій і матеріально-технічної бази не є гарантією успішного функціонування інтелектуальних систем і підвищення ефективності бізнесу. Самі по собі цифрові системи, що взаємодіють із об'єктами фізичного світу, несуть у собі чимало загроз. У випадках, коли відбувається розширення технологічних ланцюгів у результаті процесів кооперації чи злиття, і при цьому відсутні міжнаціональні (міжгалузеві, міжкорпоративні) стандарти, здатні синхронізувати ці процеси, технічні ризики масштабуються та якісно ускладнюються.

Існування організаційних ризиків зумовлене впливом технологій на кадрове забезпечення підприємства, рівнем інноваційної активності та «цифрової» грамотності персоналу, ускладненням господарських завдань і зростанням ступеня відповідальності, вимогами до рівня кваліфікації та внутрішньокорпоративної взаємодії, наявністю професійних компетенцій і вмінням їх застосовувати, а також здатністю гнучко реагувати на зміни.

Ризиками цифровізації на глобальному рівні є [9]:

– технологічні,
– геополітичні,
– геоекономічні,
– макроекономічні,
– екологічні,
– кліматичні,
– біологічні ризики.

Існують й інші підходи до класифікації «цифрових» ризиків. Ризики цифрових технологій підприємства можуть бути класифіковані крізь призму наскрізних цифрових технологій (НЦТ) (табл. 1).

Таблиця 1 – Ризики цифрових технологій бізнесу при використанні наскрізних цифрових технологій

НЦТ	Ризики
Великі дані (ВД)	- конфіденційність - втрата даних - переповнення сховища - зниження ефективності ВД - формування неефективного набору даних - помилки ВД - економічна недоцільність ВД - неготовність до змін - шахрайство
Промисловий інтернет	- протиправні дії та маніпуляції - злам системи - помилки у конфігуруванні, адмініструванні та використанні - втрати електроживлення, комунікацій або сервісів - форс-мажор - виведення пристрою з ладу - вразливість ПЗ - правовий ризик

НЦТ	Ризики
Штучний інтелект	- втрата контакту з клієнтом - нестача кваліфікованих фахівців - інформаційно-технологічна інфраструктура - помилки в управлінні виробництвом
Технології бездротового зв'язку	- неавторизований доступ до корпоративної мережі - нефіксована природа зв'язку - вразливість мереж і пристроїв - нові загрози та атаки - витоки інформації з дротової мережі - проблеми функціонування бездротових мереж
Робототехніка	- недотримання техніки безпеки - кібербезпека
Квантові технології	- квантова загроза кібербезпеці
Системи розподіленого реєстру	- смарт-контракти - інфраструктурні - криптографічні - майнінг/консенсус - конфіденційність і безпека даних - правові

Авторська розробка

Цифровізація кадрових аспектів господарської діяльності підприємства, зокрема переведення працівників на віддалений формат роботи, підвищує вразливість компаній до ризиків, пов'язаних із конфіденційністю, захистом даних та кібератаками. Ризики кібератак зумовлюють необхідність адаптації корпоративних стратегій ризик-менеджменту до стрімко мінливої технологічної кон'юнктури. Ризики кібератак часто пов'язані з ключовими загрозами діяльності сучасних підприємств.

Класифікація «цифрових» ризиків з точки зору бізнесу представлена в табл. 2.

За результатами аналізу наукової літератури не було виявлено загальноприйнятого сталого підходу до класифікації «цифрових» ризиків як у науково-дослідному середовищі, так і у бізнес-сфері. Різноманіття класифікаційних підходів може бути зумовлене технологічною багатогранністю та унікальністю інноваційних систем, що впроваджуються на підприємствах, специфікою стратегій ризик-орієнтованого управління залежно від галузі або конкретного підприємства, а також складністю виявлення зв'язку між причинами виникнення «цифрових» ризиків і настанням негативних наслідків для підприємства.

Цифрова трансформація компаній, імплементація сучасних технологічних рішень – це неповністю передбачуваний процес, нерозривно пов'язаний із невизначеністю та новими, «цифровими» ризиками, що потребує спеціальної кадрової підготовки.

Упровадження штучного інтелекту у різні сфери діяльності підприємства може стати причиною появи якісно нових викликів і загроз, з якими компанія може зіткнутися в процесі здійснення своєї господарської діяльності. Варіативність напрямів використання технологій ШІ зумовлює проблеми застосування відповідного програмного забезпечення та алгоритмів. Упровадження технологій на базі ШІ в господарську діяльність підприємства супроводжується виникненням низки юридичних

і технічних проблем, пов'язаних із конфіденційністю даних, безпекою та відповідальністю користувачів, а також питаннями інтелектуальної власності.

Таблиця 2 – Ризики цифрової трансформації з позицій консалтингових компаній

Джерело	Види ризиків
Аудиторсько-консалтингова компанія KPMG	- операційні - правові - інфраструктурні - нестача компетенцій - вразливе програмне забезпечення - технологічна залежність
Аудиторсько-консалтингова компанія Deloitte	- ризик шахрайства - ризик масштабування - ризик використання «цифрових» інструментів - ризик затримки змін (неявний результат за значних інвестицій) - ризик корпоративного управління
Аудиторсько-консалтингова компанія EY	- упередженість алгоритмів - перебільшення можливостей - програмні помилки - ризик кібератак - правові - репутаційні

Розроблено з використанням [10, 11, 12]

У межах дослідження було виокремлено п'ять основних укрупнених груп ризиків, зумовлених упровадженням і використанням технологій ШІ у господарській діяльності підприємства (рис. 3).

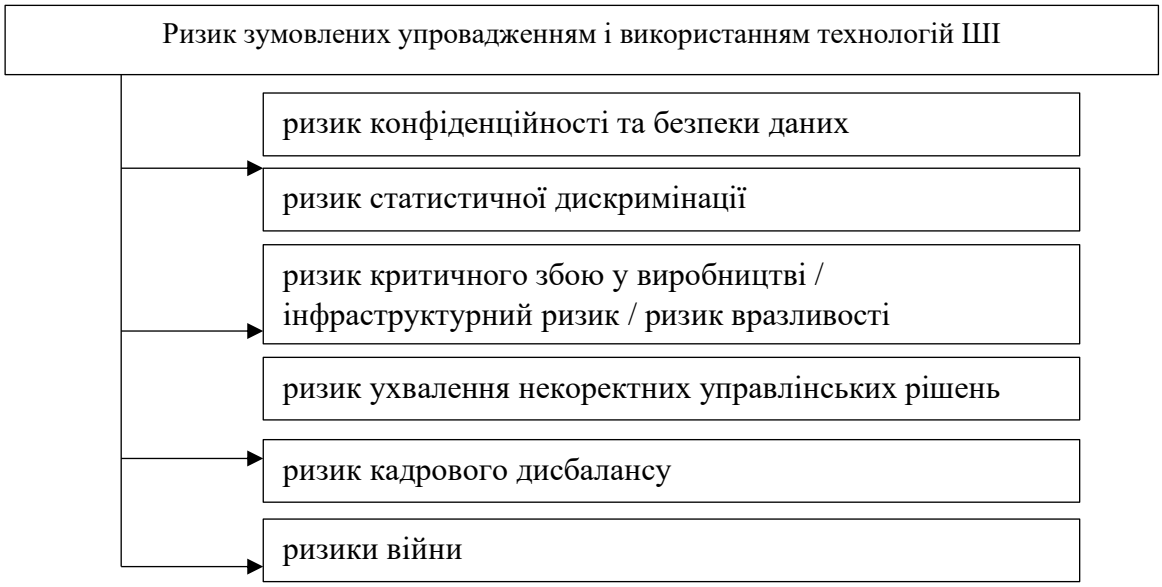

Рисунок 3 – Класифікація ризику зумовлених упровадженням і використанням технологій штучного інтелекту

Авторська розробка

Розглянемо детально ці ризики з позиції механізмів ризик-орієнтованого управління:

1. Ризик конфіденційності та безпеки даних.

Технології штучного інтелекту активно застосовуються в управлінні автомобільними засобами, поїздами, фабриками та виробництвами, інтегруються в міське середовище, використовуються у банківській сфері – усе це стає можливим завдяки накопиченню та аналізу масивів великих даних. Дані, що збираються та використовуються системами ШІ, часто є персональними, зокрема біометричними. Напрями діяльності ШІ, пов'язані з використанням таких даних, потенційно небезпечні через уразливість баз даних і цифрових сховищ інформації, які можуть бути зламані або викрадені внаслідок кібератак.

Окрім викрадення конфіденційної персональної інформації, цифровим крадіжкам піддається також інтелектуальна власність підприємств, яка фактично є їхнім технологічним активом.

Небезпеки використання технологій ШІ можуть також критися у системах навчання, якщо інформація, яка подається для навчання системи, є неповною або недостовірною. Це може призвести до деструктивної поведінки системи та викривлення результатів її функціонування, що негативно вплине на діяльність підприємства, якість прогнозів і управлінських рішень, оперативність реагування на зміни. Сукупність таких негативних проявів може завдати шкоди репутації компанії, підірвати лояльність клієнтів і контрагентів, а також знизити рівень довіри до систем ШІ.

Забезпечення безпеки користувача та його даних є одним із першочергових завдань, які потребують вирішення під час упровадження та використання технологій ШІ.

У листопаді 2020 року була запущена база даних інцидентів штучного інтелекту (AIID), що містить повідомлення про збої ШІ, які призвели до завдання шкоди [14]. Ця база використовується для фіксації інцидентів – так званих «збоїв» ШІ. Метою створення подібної інформаційної платформи є надання розробникам можливості, проаналізувавши зафіксовані випадки, врахувати потенційні ризики та проблеми й усунути їх до введення системи в експлуатацію [15].

2. Ризик статистичної дискримінації.

Якість даних визначається їхньою структурою, розмірністю, наявністю випадкових викидів, відсутніх даних та дисбалансом класів даних. На якість даних також впливає достовірність джерела. Одним із наслідків неякісних даних є поява упередженої системи – тобто системи, яка може бути несправедливою щодо певної досліджуваної групи.

Система штучного інтелекту, що зазнає впливу внутрішніх упереджень конкретного джерела даних, піддається ризику прийняття рішень, які можуть призвести до несправедливих або некоректних результатів. Наслідком недостатньої якості даних також є системні помилки, що виникають у результаті неправильно організованого процесу відбору та зважування даних.

Описуваний ризик також має етичний вимір взаємодії з технологіями ШІ у процесі господарської діяльності підприємства. Він полягає в тому, що дані, які використовуються для ухвалення рішень, можуть бути неповними або упередженими, що призводить до статистичної дискримінації у межах системи, негативно впливає на рівень довіри до технологій ШІ загалом і до конкретної системи зокрема.

У дослідженні [16] 41% опитаних респондентів розглядають якість даних як суттєву або значну перешкоду для впровадження ШІ; забезпечення доступу до даних і систематичне викривлення даних як проблему відзначили відповідно 35% і 17% респондентів.

3. Ризик критичного збою у виробництві / інфраструктурний ризик / ризик вразливості технологічних систем.

Некоректна робота системи штучного інтелекту може спричинити збої у функціонуванні пов'язаної з нею інфраструктури, зокрема тієї, що є критично важливою для реалізації та підтримання господарської діяльності підприємства. Подібні збої можуть бути викликані низкою факторів: обмеженістю обчислювальних потужностей, відносно низькою швидкістю інтернет-з'єднання, складністю підтримання функціонування системи ШІ, проблемами її обслуговування та високою вартістю енергоспоживання.

Після інциденту, який призвів до загибелі людини, компанія Uber Technologies повністю зупинила тестування безпілотних автомобілів у Піттсбурзі, Сан-Франциско та Торонто [17]. Причиною стали збої в роботі алгоритмів ШІ [18].

Окрім внутрішніх технологічних збоїв у господарських процесах підприємства, інфраструктурний ризик може бути спровокований і реалізований зовнішніми силами – шляхом кібератак. Так, багатомільйонні збитки стали наслідком кібератаки на металургійне підприємство в Німеччині: впровадження шкідливої програми у програмне забезпечення, яке керувало доменною піччю компанії, призвело до її перегріву та виходу обладнання з ладу – критичного збою у виробничому процесі [19].

4. Ризик ухвалення некоректних управлінських рішень.

Чим глибше цифрові рішення інтегровані у господарські процеси компанії, яка використовує неякісні дані, тим вищим є ризик ухвалення помилкового управлінського рішення, що може спричинити низку негативних наслідків для функціонування підприємства, його технологічної та фінансово-економічної стійкості. Неякісні дані стають причиною некоректної роботи системи, що знижує ефективність використання технологій штучного інтелекту та породжує недовіру з боку споживачів. Вплив цього фактора може бути зменшений як шляхом ручної підготовки даних, так і за допомогою використання вже підготовлених баз даних.

5. Ризик кадрового дисбалансу.

Кадрова проблема зумовлена складністю інтелектуальних систем – з одного боку, та низьким рівнем «цифрової» кваліфікації працівників підприємства – з іншого. Залучення зовнішніх висококваліфікованих фахівців для розв'язання нетипових техніко-технологічних завдань часто може бути неможливим власними силами та ресурсами компанії у конкретний момент часу.

7. Ризики війни.

Війна в Україні з 2022 року зумовлює появу нових ризиків. Зрив постачань інноваційного іноземного обладнання, блокування технологічної інфраструктури, розміщеної за межами України (сервери, центри обробки даних), розрив технологічних ланцюгів постачання та усталених контрактів – усе це є проявами ризику війни. Реалізація цього ризику завдає шкоди ІТ-інфраструктурі підприємств, підриває стабільність їхньої господарської діяльності та змушує оперативно перебудовувати технологічні ланцюги, заміщуючи елементи, які вибули внаслідок війни та військових руйнувань.

На основі проведеного аналізу представлено авторську класифікацію ризиків цифрової трансформації (ЦТ) підприємства, а також подано характеристику виявлених ризиків за такими критеріями:

- вид збитків від реалізації ризику (прямі або непрямі);
- можливість страхування ризику (нестраховий, важкостраховий, страховий);
- сфера виникнення ризику (внутрішня або зовнішня);
- можливість регулювання ризику (некерований, умовно керований, керований);
- рівень втрат (мінімальний, допустимий, критичний).

Також запропоновано заходи щодо запобігання (до настання ризику – превентивні) та пом'якшення наслідків (після його реалізації) виявлених ризиків (див. додаток В, табл. В.1).

Описані вище підходи окреслюють зміст і структуру ризиків, однак для практичної реалізації необхідна системна стратегія їхнього управління, інтегрована у корпоративне планування та операційні процеси.

Розглянемо стратегії корпоративного управління ризиками в умовах цифрової трансформації підприємства:

1. Модель «трьох ліній захисту» (див. рис. 4) – це концепція, що використовується у системі управління ризиками та внутрішнього контролю для розмежування відповідальності між різними рівнями управління. Її мета – забезпечити ефективну координацію заходів контролю, управління ризиками та незалежного нагляду.

Перша лінія захисту – операційний рівень. Вона включає керівників і працівників підрозділів, які безпосередньо управляють ризиками у своїй діяльності. Їх завдання — виявляти, оцінювати та контролювати ризики у межах повсякденних процесів.

Друга лінія захисту – функції моніторингу та контролю ризиків, що забезпечують методичну підтримку, розробку політик, процедур, стандартів, а також перевірку їх виконання. До неї належать відділи комплаєнсу, управління ризиками, фінансового контролю тощо.

Третя лінія захисту – незалежний аудит, який здійснює перевірку ефективності двох попередніх ліній. Внутрішній або зовнішній аудит оцінює, чи відповідають дії компанії затвердженим політикам і чи забезпечується належний рівень контролю.

Рисунок 4 – Модель «трьох ліній захисту»

Авторська розробка

Перевага моделі полягає у тому, що вона забезпечує прозорість, чіткий розподіл повноважень та ефективне виявлення слабких місць у системі контролю. Вона є базовою структурою для побудови інтегрованої системи управління ризиками (ERM) у відповідності до міжнародних стандартів (COSO, ISO 31000).

2. Ризик-апетит та толерантність до ризику [20]. Ризик-апетит – це рівень ризику, який організація або особа готові прийняти для досягнення своїх стратегічних цілей. Він визначається у межах загальної політики управління ризиками та залежить від культури управління, фінансової стійкості, досвіду керівництва й зовнішнього середовища. Толерантність до ризику (risk tolerance) – це допустимі відхилення від

установленого рівня ризик-апетиту, тобто межі, в яких ризик може змінюватися без порушення стабільності функціонування (див. рис. 5).

Метод оцінки базується на поєднанні кількісних (аналіз сценаріїв, VaR, стандартне відхилення, коефіцієнт варіації) та якісних (експертні оцінки, шкали ризиків, матриці пріоритетів) підходів. Процес формування ризик-апетиту передбачає:

1. Ідентифікацію ключових ризиків – визначення подій, що можуть вплинути на досягнення цілей.
2. Оцінку впливу та ймовірності кожного ризику.
3. Встановлення меж прийнятності – визначення діапазону толерантності (наприклад, «низький», «помірний», «високий» ризик).
4. Узгодження ризик-апетиту з корпоративною стратегією – співвідношення ризику й очікуваної вигоди.
5. Моніторинг і перегляд – періодичне оновлення рівнів толерантності відповідно до змін середовища.

Таким чином, метод «Ризик-апетит та толерантність до ризику» дозволяє сформувати оптимальний баланс між прагненням до прибутку і допустимим рівнем невизначеності, забезпечуючи узгодженість рішень на всіх рівнях управління.

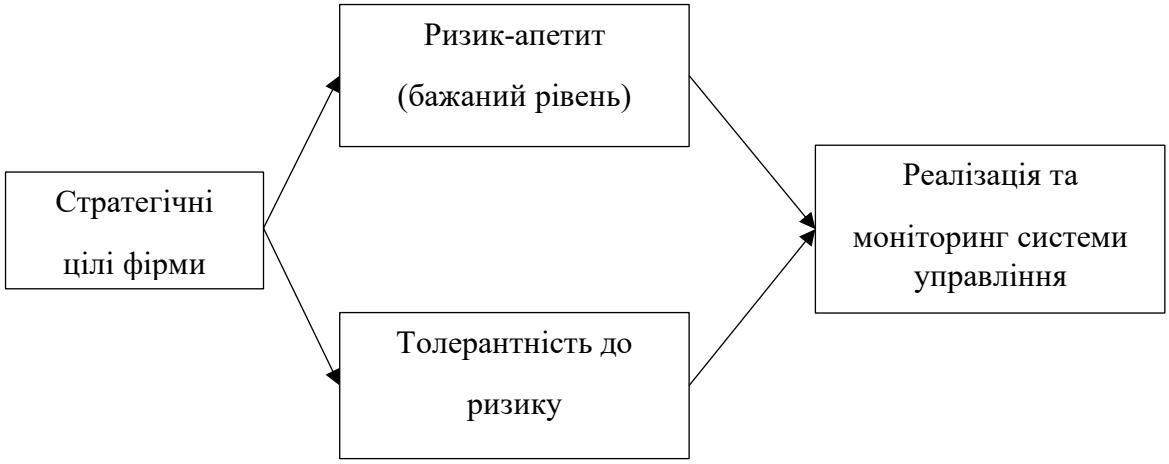

Рисунок 5 – Структура взаємозв'язку ризик-апетиту та толерантності до ризику
Авторська розробка

3. Метод «Ризик-культура та комунікації» [**Ошибка! Закладка не определена.**]. Ризик-культура – це сукупність цінностей, переконань, знань і поведінкових норм, які визначають ставлення працівників до ризиків та впливають на процес прийняття управлінських рішень. Вона формує спосіб мислення організації щодо ризику – від повної обережності до контрольованої готовності приймати ризик заради розвитку (рис. 6).

Метод базується на створенні системи ефективних комунікацій між усіма рівнями управління, що забезпечує відкритий обмін інформацією про ризики, навчання персоналу, підвищення відповідальності та своєчасне реагування на потенційні загрози.

Основні етапи формування ризик-культури:

1. Визначення цінностей та принципів управління ризиками (етика, прозорість, підзвітність).
2. Навчання та підвищення обізнаності персоналу щодо ризиків.
3. Впровадження каналів комунікації – звіти, зустрічі, платформи обміну інформацією.
4. Зворотний зв'язок і моніторинг – виявлення проблем і удосконалення поведінкових стандартів.

5. Підтримка керівництва – демонстрація прикладу «зверху вниз» (tone at the top).

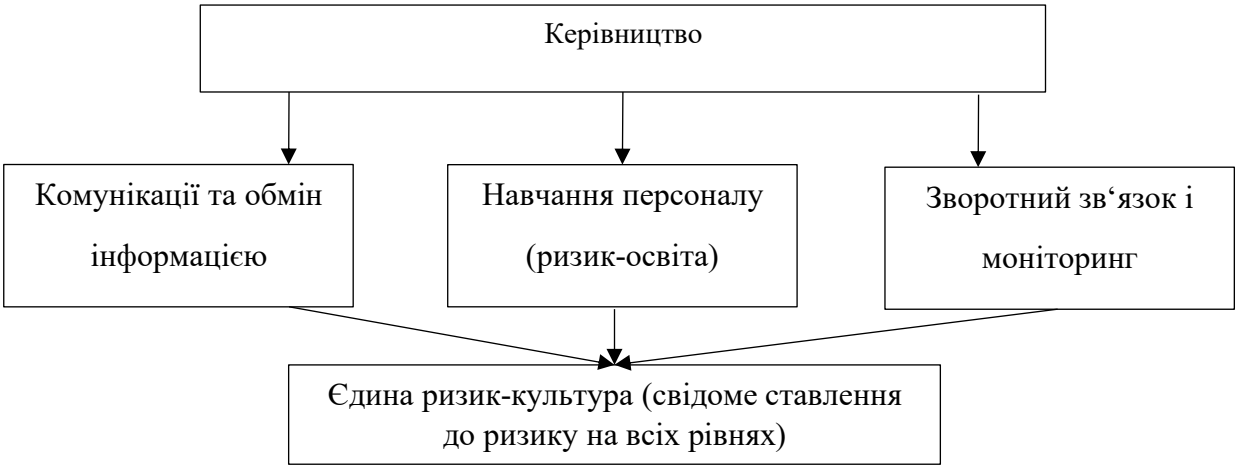

Рисунок 6 – Структура ризик-культури та комунікацій в організації
Авторська розробка

Метод ризик-культури та комунікацій сприяє створенню прозорого середовища, у якому всі учасники організації розуміють свою роль у процесі управління ризиками, а рішення приймаються на основі достовірної інформації, що знижує імовірність помилок і кризових ситуацій.

Узагальнюючи суть трьох розглянутих методів можна зазначити, що вони утворюють єдину систему стратегічного управління ризиками підприємства. Перший метод визначає межі прийнятного ризику та формує основу для прийняття рішень із урахуванням балансу між можливостями та загрозами. Модель трьох ліній захисту забезпечує чіткий розподіл відповідальності та багаторівневий контроль ефективності управлінських дій. Натомість розвиток ризик-культури та налагоджена комунікація сприяють усвідомленому ставленню до ризику, прозорості та швидкому обміну інформацією між усіма рівнями управління. У комплексі ці методи створюють цілісну архітектуру управління ризиками, що поєднує стратегічне бачення, операційну відповідальність і корпоративну свідомість, підвищуючи стійкість організації до внутрішніх і зовнішніх викликів.

Висновки. У результаті дослідження обґрунтовано, що ризик-менеджмент є стратегічною основою управління економічною діяльністю підприємства, яка забезпечує його стійкість, безперервність функціонування та конкурентоспроможність у нестабільному середовищі. Доведено необхідність інтеграції управління ризиками у всі етапи життєвого циклу бізнес-процесів – від стратегічного планування до контролю результатів. Запропоновано концептуальний підхід, що поєднує кількісні та якісні методи оцінювання ризиків і спрямований на оптимізацію співвідношення «прибутковість – допустимий рівень ризику». Встановлено, що цифрова трансформація підприємства актуалізує потребу у формуванні системи управління як традиційними, так і «цифровими» ризиками. Розвинуто підхід до їх комплексної ідентифікації, оцінювання та моніторингу з урахуванням технологічних, економічних і організаційних чинників. Обґрунтовано доцільність реалізації ризик-менеджменту не лише на корпоративному рівні, а й у межах окремих підрозділів і проєктів, що підвищує адаптивність, інноваційність та рівень економічної безпеки підприємства в умовах цифрової невизначеності. Доведено необхідність інтеграції сучасних інструментів стратегічного управління ризиками в єдину систему корпоративного ризик-менеджменту. Використання підходів визначення ризик-апетиту, моделі «трьох ліній захисту» та формування ризик-культури створює цілісну архітектуру управління,

орієнтовану на превентивне реагування, збалансування прибутковості та стійкості, а також підвищення ефективності внутрішнього контролю. Комплексне застосування цих інструментів забезпечує довгострокову стабільність і стратегічний розвиток підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kalina, I., Khurdei, V., Shevchuk, V., Vlasiuk, T., Leonidov, I. Introduction of a Corporate Security Risk Management System: The Experience of Poland. Journal of Risk and Financial Management. 2022. Vol. 15(8): 335.
2. Zurich Resilience Solutions. (n.d.). Risk management strategies: How to build a robust risk management framework. URL: https://zurichresilience.com/knowledge-and-insights-hub/articles/risk-management-strategies
3. Managing Information Security Risk. Organization, Mission, and Information System View. Special Publication 800-39. National Institute of Standards and Technology, U.S. Department of Commerce. 2011. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
4. Lavrentieva, L., Anisimova, O. Strategic Approaches to the Risk Management and their Influence on Economic Security of the Enterprise. Journal of Modern Science. 2018. Vol. 37(2), pp. 127-144.
5. Cassano, R. Corporate global responsibility and reputation risk management. Symphonya. Emerging Issues in Management. 2019. Vol. 1, pp. 129-142.
6. Hsu, Ming-Fu, Ying-Shao Hsin, Fu-Jiing Shiue. Business analytics for corporate risk management and performance improvement. In Annals of Operations Research. Berlin and Heidelberg: Spinger. 2021, pp. 1-41.
7. Buntić, L., Damić, M., Dužević, I. Artificial intelligence in business models as a tool for managing digital risks in international markets. SHS Web of Conferences 92. 2021, pp. 1-7.
8. Raul L. Katz. Social and economic impact of digital transformation on the economy. International Telecommunication Union. Report. 2017, pp. 2-41.
9. Fritzen, M. P. Remote working and Cyber Security threats in Ireland. Challenges and Prospective Solutions. School of Computing National College of Ireland. 2021, pp.1-37.
10. KPMG. Digital risk: A new security frontier. 2019. URL: https://kpmg.com/jm/en/home/insights/2019/03/digital-risk-a-security-new-frontier.html
11. Deloitte LLP. Beyond the hype: Global Digital Risk Survey 2019. URL: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-digital-risk-survey.pdf
12. EY. Why AI is both a risk and a way to manage risk. 2018. URL: https://www.ey.com/en_gl/insights/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk
13. AI Incident Database. AI Incident Database. 2025. URL: https://incidentdatabase.ai
14. Partnership on AI. Annual Report 2020. URL: https://www.partnershiponai.org/wp-content/uploads/2021/02/PAI-2020-Annual-Report-Final.pdf
15. Ryll, L., Barton, M. E., Zhang, B., McWaters, J. Transforming Paradigms: A Global AI in Financial Services Survey. Cambridge Centre for Alternative Finance & World Economic Forum. 2020. URL: https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf
16. National Transportation Safety Board. Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona. March 18, 2018. (Highway Accident Report NTSB/HAR-19/03). URL: https://www.ntsb.gov/investigations/accidentreports/reports/har1903.pdf

17. Kohli, P., Chadha, A. Enabling Pedestrian Safety using Computer Vision Techniques: A Case Study of the 2018 Uber Inc. Self-driving Car Crash. arXiv. 2018. URL: https://arxiv.org/abs/1805.11815
18. Liu, P. People's biased responses to traffic accidents involving self-driving vehicles. Accident Analysis & Prevention, 124. 2019. URL: https://www.sciencedirect.com/science/article/abs/pii/S0001457518310492
19. Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrating with Strategy and Performance. Durham, NC: COSO. 2017.
20. International Organization for Standardization. ISO 31000:2018 Risk management – Guidelines. Geneva: ISO. 2018.

REFERENCES

1. Kalina, I., Khurdei, V., Shevchuk, V., Vlasiuk, T., & Leonidov, I. (2022). Introduction of a Corporate Security Risk Management System: The Experience of Poland. *Journal of Risk and Financial Management*, Vol. 15(8), 335. [in English].
2. Zurich Resilience Solutions. (n.d.). Risk management strategies: How to build a robust risk management framework. URL: https://zurichresilience.com/knowledge-and-insights-hub/articles/risk-management-strategies [in English].
3. National Institute of Standards and Technology (NIST). (2011). *Managing Information Security Risk: Organization, Mission, and Information System View*. Special Publication 800-39. U.S. Department of Commerce. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf [in English].
4. Lavrentieva, L., & Anisimova, O. (2018). Strategic Approaches to the Risk Management and their Influence on Economic Security of the Enterprise. *Journal of Modern Science*, Vol. 37(2), Pp. 127-144. [in English].
5. Cassano, R. (2019). Corporate global responsibility and reputation risk management. *Symphonya. Emerging Issues in Management*, Vol. 1, Pp. 129-142. [in English].
6. Hsu, M.-F., Hsin, Y.-S., & Shiue, F.-J. (2021). Business analytics for corporate risk management and performance improvement. *Annals of Operations Research*. Berlin and Heidelberg: Springer. Pp. 1-41. [in English].
7. Buntić, L., Damić, M., & Dužević, I. (2021). Artificial intelligence in business models as a tool for managing digital risks in international markets. *SHS Web of Conferences*, 92. Pp. 1-7. [in English].
8. Katz, R.L. (2017). *Social and economic impact of digital transformation on the economy*. International Telecommunication Union. Report. Pp. 2-41. [in English].
9. Fritzen, M.P. (2021). *Remote working and Cyber Security threats in Ireland: Challenges and Prospective Solutions*. School of Computing, National College of Ireland. Pp. 1-37. [in English].
10. KPMG. (2019). Digital risk: A new security frontier. URL: https://kpmg.com/jm/en/home/insights/2019/03/digital-risk-a-security-new-frontier.html [in English].
11. Deloitte LLP. (2019). Beyond the hype: Global Digital Risk Survey 2019. URL: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-digital-risk-survey.pdf [in English].
12. EY. (2018). Why AI is both a risk and a way to manage risk. URL: https://www.ey.com/en_gl/insights/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk [in English].
13. AI Incident Database. (2025). AI Incident Database. URL: https://incidentdatabase.ai [in English].

14. Partnership on AI. (2020). Annual Report 2020. URL: https://www.partnershiponai.org/wp-content/uploads/2021/02/PAI-2020-Annual-Report-Final.pdf [in English].
15. Ryll, L., Barton, M.E., Zhang, B., & McWaters, J. (2020). Transforming Paradigms: A Global AI in Financial Services Survey. Cambridge Centre for Alternative Finance & World Economic Forum. URL: https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf [in English].
16. National Transportation Safety Board. (2019). Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona. March 18, 2018 (Highway Accident Report NTSB/HAR-19/03). URL: https://www.ntsb.gov/investigations/accidentreports/reports/har1903.pdf [in English].
17. Kohli, P., & Chadha, A. (2018). Enabling Pedestrian Safety using Computer Vision Techniques: A Case Study of the 2018 Uber Inc. Self-driving Car Crash. *arXiv*. URL: https://arxiv.org/abs/1805.11815 [in English].
18. Liu, P. (2019). People's biased responses to traffic accidents involving self-driving vehicles. *Accident Analysis & Prevention*, 124. URL: https://www.sciencedirect.com/science/article/abs/pii/S0001457518310492 [in English].
19. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise Risk Management – Integrating with Strategy and Performance*. Durham, NC: COSO. [in English].
20. International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Risk management – Guidelines*. Geneva: ISO. [in English].

Стаття надійшла до редакції 23.12.2025
Стаття прийнята до друку після рецензування 08.01.2026