

РИЗИК-ОРІЄНТОВАНЕ УПРАВЛІННЯ В КОНТЕКСТІ ЦИФРОВОЇ ЕКОНОМІКИ:  
СУТНІСТЬ, ЦІЛІ, ІНСТРУМЕНТИRISK-BASED MANAGEMENT IN THE CONTEXT OF THE DIGITAL ECONOMY:  
ESSENCE, GOALS, TOOLS

У статті досліджено концептуальні засади ризик-орієнтованого управління (РОУ) у контексті цифрової трансформації економіки. Обґрунтовано, що зміна природи ризиків – від зовнішніх до внутрішньоорганізаційних – зумовлює потребу перегляду традиційного ризик-менеджменту на користь проактивного, системного підходу. РОУ розглядається як інтегрована стратегічна функція, що охоплює виявлення, оцінку, моніторинг і використання ризиків на всіх рівнях управління. Здійснено аналіз наукових підходів до РОУ, уточнено його місце в управлінській системі підприємства та запропоновано авторське визначення цього поняття. У дослідженні окреслено архітектуру ризиків цифрової економіки (мікро-, мезо- та макрорівень) і проаналізовано відповідні цифрові інструменти управління – AI, Big Data, IoT, Blockchain тощо. Побудовано інтегровану модель РОУ, яка відображає логіку переходу від ідентифікації загроз до реалізації адаптивних управлінських рішень. Особливу увагу приділено специфіці впровадження РОУ на промислових підприємствах. Визначено перспективи подальших досліджень у напрямі розробки методик оцінки ефективності РОУ в умовах цифрової турбулентності.

**Ключові слова:** ризик-орієнтоване управління, цифрова економіка, стійкість підприємства, архітектура цифрових ризиків, проактивне реагування на ризики, штучний інтелект в управлінні ризиками.

*The purpose of this study is to conceptualize risk-based management as a fundamental component of enterprise governance in the context of digital economic transformation. The relevance of the research lies in the growing complexity and multidimensionality of risks that arise in digital environments, where conventional approaches to risk management prove insufficient. As digital technologies become deeply integrated into business processes, organizations face the challenge of ensuring resilience, adaptability, and continuity through proactive and systemic risk-oriented strategies. The study aims to explore how risk-based management can be adapted to meet the specific demands of a fast-changing digital economy and how it contributes to the strategic sustainability of industrial enterprises. The methodological framework of the research is based on systems thinking, logical modeling, synthesis and analysis of management processes, as well as conceptual generalization. The author employed a structural-functional approach to model the architecture of digital risks and their correlation with managerial decision-making cycles. Scenario-based reasoning and abstraction were applied to identify the relationships between risk sources, control instruments, and the stages of enterprise risk response. Additionally, methods of classification and typology were used to systematize types of digital risks and tools for mitigating them at different organizational levels. As a result, the research presents a comprehensive model of risk-based management tailored to the digital economic environment. The model outlines the integration of digital risk architecture (micro, meso, and macro levels) with core risk management stages such as identification, assessment, mitigation planning, monitoring, and corrective action. The findings demonstrate the importance of digital tools – including artificial intelligence, big data analytics, blockchain, and IoT – in enhancing the responsiveness and efficiency of risk management systems. The study highlights how these technologies transform risk management from a reactive process to a proactive and strategic function of the enterprise. The practical value of the article lies in its applicability to modern enterprises seeking to maintain operational stability and competitiveness in volatile digital markets. By offering a structured and technology-integrated approach to managing digital risks, the study provides a useful framework for decision-makers to develop adaptive and sustainable risk management systems. This enables organizations not only to protect their assets but also to convert emerging risks into new opportunities for growth and innovation.*

**Keywords:** Risk-based management, digital economy, enterprise resilience, digital risk architecture, proactive risk response, AI in risk management.

УДК 005.334:005.21:330.46:004

DOI: <https://doi.org/10.32782/dees.18-32>

**Аберніхіна І.Г.<sup>1</sup>**

к.е.н., доцент,  
ННІ «Дніпровський  
металургійний інститут»  
Українського державного університету  
науки та технологій

**Abernikhina Iryna**

SEI Dnipro Metallurgical Institute  
Ukrainian  
State University of Science  
and Technologies

**Постановка проблеми.** Сучасна економіка стрімко трансформується під впливом цифрових технологій, що зумовлює радикальні зміни у структурі ризиків: з'являються кіберзагрози, технологічна залежність, регуляторна невизначеність, ризики цифрової нерівності та втрати конфіденційності. Такі ризики є взаємопов'язаними, динамічними й мають потенційно масштабні наслідки для підприємств. У цьому контексті традиційні підходи до ризик-менеджменту втрачають ефективність, а отже, актуалізується потреба у створенні нових теоретико-методичних засад ризик-орієнтованого

управління (РОУ), яке відповідає викликам цифрової економіки.

Проблема полягає у відсутності уніфікованих моделей, які б інтегрували цифрову інфраструктуру, багаторівневу архітектуру ризиків і сучасні інструменти прийняття управлінських рішень. Для підприємств надзвичайно важливим є формування гнучких систем управління ризиками, здатних до адаптації, оперативного реагування та стратегічного використання ризиків як джерела розвитку. Це зумовлює необхідність уточнення сутності РОУ в цифровому контексті, визначення його цілей,

<sup>1</sup> ORCID: <https://orcid.org/0000-0003-0692-1276>

функцій і обґрунтування доцільності впровадження цифрових інструментів нового покоління.

#### **Аналіз останніх досліджень і публікацій.**

У сучасній науковій літературі ризик-орієнтоване управління (РОУ) трактується як стратегічний інструмент корпоративного управління в умовах зростання невизначеності та цифрової трансформації. Arena M., Arnaboldi M., Azzone G. (2010) [1] розглядають РОУ як інтеграцію процесів прийняття рішень, контролю та підзвітності, що еволюціонують під впливом зовнішнього середовища. Shin I., Park S. (2017) [4] підкреслюють важливість РОУ як елемента управлінського контролю, особливо в структурі великих компаній. Yasmin S., Ghafran C. (2019) [2] наголошують на формуванні ризикоорієнтованої культури, що передбачає залучення всіх підрозділів підприємства до процесу управління ризиками. Вітчизняні дослідження, зокрема Співак С. і Мариняк Б. (2022) [7], пропонують адаптацію РОУ до специфіки промислових підприємств, орієнтуючись на процесно-операційний підхід.

Цифрова трансформація створює нові ризики, що потребують переосмислення класичних моделей. Tura J., Simota J., Steiner F. (2017) [5] вказують на зростання кіберзагроз і потребу у використанні великих даних, IoT та інтелектуальної автоматизації. Kholod V. et al. (2020) [6] пропонують системно-кібернетичний підхід до РОУ із застосуванням математичних моделей для оптимізації ризикового портфеля. Sotamaa T., Reiman A. Kauprila O., (2025) [8] узагальнюють цифрові практики РОУ у малих та середніх промислових підприємствах, акцентуючи на використанні штучного інтелекту, хмарних технологій та аналітики в умовах криз і нестабільності. Vasylyshyna L. et al. (2022) [9] розробили матричну модель, що поєднує цифрову зрілість підприємства з рівнем ризикованості його діяльності, виокремлюючи три стратегії управління ризиками: «новатор», «послідовник» і «спостерігач».

Незважаючи на прогрес у дослідженні РОУ, залишається низка нерозв'язаних проблем: відсутність уніфікованої інтегрованої моделі управління ризиками (стратегічного, операційного й цифрового рівнів), обмежена IT-інтеграція у системи ризик-менеджменту, дефіцит емпіричних досліджень щодо ефективності цифрових інструментів (AI, blockchain, big data), а також нестача адаптованих моделей для МСП у країнах із перехідною економікою. Це обумовлює необхідність подальших досліджень у сфері цифрового РОУ як важливого напрямку розвитку економіки та управлінської практики.

Формулювання цілей статті (постановка завдання). Метою статті є теоретичне обґрунтування сутності ризик-орієнтованого управління в умовах цифрової економіки, визначення його ключових цілей і принципів, а також систематизація сучасних інструментів управління ризиками з урахуванням цифрових трансформацій.

Для досягнення поставленої мети в статті передбачено вирішення таких наукових завдань:

- розкрити особливості формування ризиків у цифровій економіці та визначити їхню відмінність від традиційних ризиків підприємницької діяльності;

- уточнити понятійно-категоріальний апарат ризик-орієнтованого управління, обґрунтувати його зміст у стратегічному та операційному вимірах;

- проаналізувати цілі й функціональні завдання ризик-орієнтованого управління в контексті цифрової трансформації бізнес-процесів;

- запропонувати інтегровану модель ризик-орієнтованого управління, яка поєднує архітектуру цифрових ризиків, управлінський цикл і технологічну підтримку управлінських рішень.

#### **Виклад основного матеріалу дослідження.**

У сучасних умовах цифрової трансформації ризики змінюють свою природу, набуваючи як зовнішнього, так і внутрішнього характеру, що зумовлює перегляд класичних підходів до управління. З огляду на це, ризик-орієнтоване управління (РОУ) розглядається як сучасна управлінська парадигма, орієнтована на забезпечення гнучкості та стійкості підприємства в умовах цифрової економіки. Його метою є не лише мінімізація загроз, але й проактивне виявлення можливостей, що відкриваються внаслідок ризику. Такий підхід передбачає системну інтеграцію ідентифікації, оцінки, моніторингу та контролю ризиків у всі бізнес-процеси підприємства.

Теоретичні засади РОУ ґрунтуються на поєднанні кількох концепцій. Теорія ризику Ф. Найта [10] розмежовує вимірювану невизначеність (ризик) і неможливість кількісної оцінки (невизначеність). Теорія очікуваної корисності [11] дала змогу формалізувати вибір в умовах ризику, а система теорія управління – інтегрувати ризики у всі функціональні блоки управління. У цьому контексті важливою стає також теорія резильєнтності, що акцентує увагу на адаптації до змін як ключовій управлінській здатності. В українському науковому дискурсі РОУ дедалі частіше розглядається як основа побудови адаптивних і динамічних систем управління в умовах цифровізації [6; 7].

Зміст РОУ полягає в постійній роботі з ризиками на всіх етапах життєвого циклу підприємства: від стратегічного планування до операційного управління. Ключовими його ознаками є орієнтація на можливість, використання як кількісних, так і якісних методів оцінки, а також формування культури управління ризиками. В умовах цифрової економіки зростає потреба в оновленні методологічного апарату РОУ, який враховує ризики, пов'язані з IT-інфраструктурою, автоматизацією, IoT, AI та іншими цифровими технологіями. У цьому контексті цифрове РОУ перетворюється на системоутворюючий елемент стратегічного управління, що забезпечує підприємствам здатність до адаптації та розвитку [9].

Аналіз наукових джерел (табл. 1) свідчить, що поняття «ризик-орієнтоване управління» не має єдиного усталеного трактування. У різних підходах воно асоціюється: з процесним управлінням ризиками в межах окремих функціональних підрозділів; з елементом внутрішнього контролю; з частиною загальної корпоративної стратегії або системи управління якістю.

З огляду на сучасні виклики, доцільно запропонувати власне визначення поняття, яке б відобразило його багатовимірну природу.

Ризик-орієнтоване управління в цифровій економіці – це цілісна система стратегічного й операційного управління підприємством, заснована на проактивному виявленні, оцінюванні, контролі та використанні ризиків як факторів впливу на досягнення цілей організації, із застосуванням цифрових технологій для прийняття рішень у високоневизначеному середовищі (авторське визначення).

Зміст ризик-орієнтованого управління, на думку автора, розкривається у двох взаємопов'язаних вимірах:

– у стратегічному вимірі РОУ слугує механізмом підвищення адаптивності підприємства до змін зовнішнього середовища, формування

сценаріїв сталого розвитку, інтеграції управління ризиками в довгострокову бізнес-стратегію, а також прийняття управлінських рішень, що враховують імовірність і наслідки потенційних загроз;

– в операційному вимірі РОУ передбачає реалізацію процедур виявлення, класифікації, моніторингу, аналізу та реагування на ризики у межах поточних бізнес-процесів. У цифровому контексті це втілюється через використання автоматизованих систем контролю, модулів прогнозування ризиків, цифрових панелей управління (dashboard) та інструментів кіберзахисту.

Таким чином, уточнений понятійно-категоріальний апарат РОУ відображає його еволюцію від допоміжної функції до центральної складової стратегічного управління підприємством у цифрову епоху (рис. 1).

Цифрова економіка створює нове середовище для реалізації ризик-орієнтованого управління, водночас генеруючи специфічні загрози: кіберризик, втрату конфіденційності, цифрову нерівність, залежність від технологічних платформ тощо. Це зумовлює потребу у впровадженні цифрових інструментів управління ризиками, таких як штучний інтелект, Big Data, блокчейн, хмарні

Таблиця 1

**Порівняння підходів до ризик-орієнтованого управління в наукових дослідженнях**

Автор (рік)	Підхід до РОУ	Ключові ознаки	Рівень застосування	Цифровий вимір
Arena M., Arnaboldi M., Azzone G. (2010)	РОУ як частина корпоративної стратегії	Інтеграція з прийняттям рішень, підзвітністю, організаційною культурою	Організаційний / стратегічний	Не розглянуто
Shin I., Park S. (2017)	РОУ як елемент системи управлінського контролю	Моніторинг дочірніх компаній, делегування ризик-менеджменту, стратегічне охоплення	Група компаній / корпорація	Обмежений (корпоративні політики)
Voronko R., Vovchuk N. (2018)	РОУ як внутрішній контроль бізнес-ризиків	Фокус на запобіганні ризикам, визначенні їх допустимості, епізодичність управлінських рішень	Підприємство / операційний рівень	Не розглянуто
Співак С., Мариняк Б. (2022)	Процесно-операційний підхід	Виявлення ризиків у функціональній діяльності, моделювання	Функціональний / виробничий	Обмежено
Tupa J., Simota J., Steiner F. (2017)	РОУ у контексті Industry 4.0	Інтеграція з IoT, автоматизація, необхідність нових фреймворків, аналіз даних у реальному часі	Виробництво / цифрові системи	Високий: IoT, кіберризик, аналітика
Kholod, Borys et al. (2020)	Математичне моделювання РОУ на промислових підприємствах	Оптимізація портфеля страхування, моделі на основі Excel, кібернетичний підхід	Промислове підприємство	Частково: електронні таблиці, оптимізація
Sotamaa, T., Reiman, A., Kauppi, O., (2025)	РОУ у МСП + цифрові технології / AI	Систематизація факторів ризику в макро/мікросередовищі, адаптація цифрових ресурсів	Малі і середні підприємства (МСП)	Високий: AI, CRM, DSS, хмарні сервіси
Vasylyshyna L. et al. (2022)	РОУ через фінансову діагностику та цифрову трансформацію	Категоризація фінансових ризиків, рівні цифрового управління, цифрові стратегії (новатор, послідовник)	Промислове підприємство	Високий: аналітика, фінансове моделювання

Джерело: систематизовано автором за [1, 2, 3, 4, 5, 6, 7, 8, 9]



**Рис. 1. Модель трансформації РОУ в часовому та управлінському вимірі**

Джерело: авторська розробка

сервіси. Ефективне управління ризиками вимагає постійного оновлення карт ризиків, моніторингу змін та реагування в реальному часі, що досягається через інтегровані платформи з аналітичною підтримкою управлінських рішень.

У таких умовах ризик-орієнтоване управління постає як багаторівнева система, що поєднує класичні теорії ризику з цифровими технологіями. Його впровадження забезпечує адаптивність, стійкість і конкурентоспроможність підприємств. Для кращого розуміння специфіки РОУ в цифровій економіці доцільно дослідити практики його застосування в різних галузях, узагальнивши ці дані в табличній формі з урахуванням галузевих ризиків та особливостей цифрових бізнес-моделей. Такий формат дозволяє узагальнити ключові види ризиків, проілюструвати напрями їхнього управління та окреслити використувані інструменти ризик-менеджменту (табл. 2).

Приклади застосування ризик-орієнтованого управління в різних галузях цифрової економіки демонструють його актуальність і багатовимірність. Ефективність цього підходу залежить від здатності управлінської системи враховувати специфіку нового цифрового середовища, яке змінює як бізнес-моделі, так і природу ризиків. Цифрова економіка базується на створенні, обробці та використанні даних як головного ресурсу, активно впроваджуючи штучний інтелект, Big Data, IoT, блокчейн та інші технології, що трансформують принципи організації бізнесу.

Ключовими особливостями цифрової економіки є зростаюча взаємозалежність між учасниками

ринку та висока динаміка змін. Це створює нові ризики, які можуть швидко поширюватися в межах цифрових екосистем та мають каскадний ефект. Стрімкий розвиток технологій призводить до появи нових типів загроз, які важко виявити традиційними інструментами. У таких умовах ризик-менеджмент потребує трансформації у гнучку, адаптивну систему з елементами прогнозного моделювання та цифрової аналітики.

Цифрова економіка також породжує нові типи ризиків, зокрема:

- кіберризики (несанкціонований доступ, зловмисне програмне забезпечення, DDoS-атаки);
- ризики цифрової нерівності (відсутність доступу до інфраструктури або компетенцій);
- ризики залежності від технологій (постачальників ПЗ/обладнання, хмарних сервісів);
- репутаційні ризики у соціальних мережах та цифровому медіапросторі.

Крім того, цифрова економіка відзначається високим рівнем прозорості та відстежуваності операцій, що, з одного боку, підвищує вимоги до безпеки даних, а з іншого – відкриває можливості для побудови більш ефективних систем контролю та управління ризиками.

З урахуванням вищезазначених характеристик, ризик-орієнтоване управління в цифровій економіці має базуватися на таких принципах:

- безперервний моніторинг середовища в режимі реального часу;
- використання передових цифрових інструментів (AI, аналітика великих даних, блокчейн);

Приклади застосування ризик-орієнтованого управління в цифровій економіці

Сфера/галузь	Види цифрових ризиків	Приклади	Інструменти ризик-менеджменту	Очікуваний ефект від впровадження РОУ
Фінансові технології (FinTech)	Кіберризики, шахрайство, витік даних	Виявлення підозрілих транзакцій у банках (Revolut, Monobank)	Штучний інтелект (AI), машинне навчання, автоматизовані фільтри	Зменшення збитків від шахрайства, підвищення довіри клієнтів
Аграрний сектор (AgriTech)	Кліматичні ризики, ризики неврожаю, технічні збої	Моніторинг стану полів з використанням супутникових даних та IoT	Геоаналітика, супутниковий моніторинг, системи підтримки прийняття рішень	Оптимізація агротехнологій, мінімізація втрат урожаю
Електронна комерція (E-commerce)	Операційні ризики, логістичні, репутаційні	Контроль повернень, скарг і поведінки клієнтів (Amazon, Rozetka)	CRM-системи, аналіз поведінки клієнтів, алгоритми big data	Підвищення лояльності клієнтів, зниження операційних витрат
Охорона здоров'я (eHealth)	Конфіденційність, недоступність систем, помилки введення	Захист електронних медичних записів, кібербезпека телемедицини	Блокчейн, багатофакторна автентифікація, системи резервного копіювання	Підвищення захисту даних пацієнтів, зменшення юридичних ризиків
Міське управління (Smart City)	Інфраструктурні збої, збої в транспорті та енергетиці	Прогнозування навантаження на транспортну інфраструктуру або електромережі	IoT-сенсори, автоматизовані панелі управління, прогнозна аналітика	Підвищення безпеки, зменшення витрат на аварійне реагування
Освіта (EdTech)	Порушення доступу до платформ, втрата даних	Управління ризиками у цифрових освітніх середовищах, зокрема захист персональних даних студентів	Хмарні сервіси з резервуванням, шифрування даних	Підвищення надійності доступу до освітніх ресурсів, довіра користувачів
Промисловість (Industry 4.0)	Збої в роботі цифрового обладнання, хакерські атаки	Управління ризиками в системах автоматизованого виробництва	SCADA-системи, кіберзахист виробничих мереж	Безперервність виробництва, зниження технологічних простоїв

Джерело: систематизовані автором на основі критичного аналізу наукових [1, 5, 9]

– орієнтація не лише на мінімізацію збитків, а й на забезпечення цифрової стійкості підприємства (cyber resilience).

Таким чином, цифрова економіка формує нову багаторівневу архітектуру ризиків (мікро-, мезо- та макрорівень), що вимагає трансформації управлінських практик і впровадження інтегрованого ризик-орієнтованого підходу. В умовах цифрової трансформації ризик-менеджмент перестає бути окремою функцією контролю та набуває стратегічного характеру, охоплюючи всі рівні управління підприємством. Ефективне реагування на цифрові виклики потребує комплексної моделі, яка поєднує класичні управлінські інструменти з новітніми цифровими технологіями, забезпечуючи адаптивність, системність та аналітичну підтримку управлінських рішень.

На рисунку 2 нижче представлено графічну інтерпретацію інтегрованої моделі ризик-орієнтованого управління в умовах цифрової економіки.

Враховуючи специфіку цифрової економіки, яка характеризується високим рівнем динаміки, технологічною складністю та зростаючою

взаємозалежністю суб'єктів ринку, істотно змінюється не лише структура економічних процесів, а й природа ризиків. Ці зміни обумовлюють виникнення нових типів ризиків, які є складнішими за своєю сутністю та швидшими за темпами прояву, ніж у традиційних економічних умовах.

Цифрове середовище породжує як технологічні ризики (збої в платформах, кіберзагрози, втрати даних), так і системні ризики (залежність від інфраструктури провайдерів, нестабільність регуляторного середовища, цифрова нерівність). Ці ризики мають багаторівневий, взаємопов'язаний характер і часто проявляються каскадно – від проблем на рівні окремого підприємства до порушень у роботі цілих галузей чи ринків.

В умовах такої складності ефективно управління ризиками вимагає переходу від фрагментарних чи реактивних дій до проактивного, інтегрованого ризик-орієнтованого підходу з використанням сучасних цифрових технологій. Систематизація інструментів ризик-менеджменту відповідно до видів цифрових ризиків (табл. 3) дозволяє



**Рис. 2. Концептуальна модель ризик-орієнтованого управління в умовах цифрової економіки**

Джерело: авторська розробка

Таблиця 3

### Види ризиків у цифровій економіці та відповідні інструменти управління

Тип ризику	Суть ризику / Приклади прояву	Інструменти управління ризиком	Приклади цифрових технологій
Кіберризики	Несанкціонований доступ, DDoS-атаки, витік персональних даних	Системи кібербезпеки, багатофакторна автентифікація, моніторинг подій	SIEM-системи (IBM QRadar, Splunk), Firewalls, MFA
Технологічна залежність	Збої в хмарних платформах, монополія провайдерів цифрових послуг	Диверсифікація постачальників, бекапи, мультихмарна стратегія	AWS, Microsoft Azure, Google Cloud, Kubernetes
Ризики конфіденційності	Витік даних користувачів, недотримання GDPR	Шифрування даних, політики доступу, аудит безпеки	SSL/TLS, Blockchain, системи управління даними (DLP)
Репутаційні ризики	Негатив у соцмережах, відкриті відгуки про сервіс	Моніторинг соціальних мереж, PR-реагування в реальному часі	AI-моніторинг (Brandwatch, Talkwalker), чат-боти
Операційні ризики	Відмова цифрової інфраструктури, помилки в автоматизованих системах	Контроль якості процесів, тестування IT-рішень, резервні канали	ERP-системи (SAP, Oracle), CI/CD-системи
Ризики цифрової нерівності	Відсутність доступу до інтернету чи цифрових навичок у частини користувачів	Освітні програми, інвестиції в інфраструктуру, UX-адаптація	LMS-платформи, мобільні інтерфейси, інтернет речей
Регуляторні ризики	Зміна законодавства (GDPR, цифрові податки), невідповідність нормам	Юридичний аудит, гнучке оновлення політик, інтеграція нормативних вимог	LegalTech-рішення, смарт-контракти, системи контролю відповідності
Стратегічні ризики	Застарілість бізнес-моделі через нові цифрові продукти конкурентів	Бізнес-аналітика, цифрова трансформація, стратегічне моделювання	BI-системи (Power BI, Tableau), цифрові близнюки

Джерело: систематизовано автором на основі [3, 7, 12]

створити гнучку цифрову архітектуру управління, яка забезпечує нейтралізацію загроз на різних рівнях – від операційного до стратегічного – та перетворення ризиків на джерела нових можливостей.

Цифрове середовище породжує два основні типи ризиків: технологічні (збої в платформах, кіберзагрози, втрати даних) і системні (залежність від провайдерів, нестабільність регуляторного середовища, цифрова нерівність). Ці ризики мають багаторівневий та взаємопов'язаний характер і часто викликають каскадні ефекти – від проблем окремого підприємства до збоїв у роботі цілих галузей чи ринків.

У таких умовах традиційні реактивні методи управління ризиками виявляються недостатніми. Необхідний проактивний, інтегрований підхід, що базується на ризик-орієнтованому управлінні із застосуванням сучасних цифрових технологій.

Систематизація інструментів ризик-менеджменту відповідно до типів цифрових ризиків (див. табл. 3) дає змогу побудувати гнучку цифрову архітектуру управління. Вона забезпечує ефективну нейтралізацію загроз на всіх рівнях – від операційного до стратегічного – та створює умови для перетворення ризиків на джерела нових можливостей.

**Висновки.** Дослідження показало, що цифрова економіка суттєво змінює умови ведення бізнесу та підходи до управління ризиками. Ризики в цифровому середовищі стають більш комплексними, динамічними та взаємозалежними, що вимагає переходу від традиційних методів до ризик-орієнтованого управління (РОУ). Цей підхід інтегрує проактивне виявлення, кількісну та якісну оцінку ризиків, стратегічне планування дій з нейтралізації загроз і використання цифрових інструментів контролю й моніторингу, що сприяє підвищенню стійкості підприємства та розвитку інновацій.

Ключовою складовою сучасного РОУ є застосування цифрових технологій – штучного інтелекту, аналітики великих даних, блокчейну та систем автоматизованого моніторингу. Вони дозволяють виявляти ризики на ранніх стадіях, прогнозувати їх еволюцію та швидко обирати ефективні заходи реагування. Запропонована інтегрована модель РОУ поєднує багаторівневу архітектуру ризиків, управлінський цикл і цифрові інструменти підтримки рішень, що забезпечує комплексне управління ризиками, адаптивність і довгострокову стійкість підприємств у цифровому середовищі.

Подальший розвиток ризик-орієнтованого управління в умовах цифрової економіки вимагає поглибленого аналізу як на теоретичному, так і на прикладному рівні. Насамперед перспективним є створення методик емпіричної оцінки ефективності застосування РОУ на конкретних підприємствах, зокрема шляхом використання кейс-аналізу, моделювання ризиків та діагностики управлінської поведінки в умовах цифрової турбулентності.

#### БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Arena M., Arnaboldi M., Azzone G. The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*. 2010. Vol. 35, no. 7. P. 659–675. DOI: <https://doi.org/10.1016/j.aos.2010.07.003> (date of access: 14.07.2025).
2. Yasmin S., Ghafran C. The problematics of accountability: Internal responses to external pressures in exposed organisations. *Critical Perspectives on Accounting*. 2019. Vol. 64. P. 102070. DOI: <https://doi.org/10.1016/j.cpa.2019.01.002> (date of access: 14.07.2025).
3. Voronko R., Vovchuk N. Risk management and the concept of risk-based internal control. *The institute of accounting, control, and analysis in the globalization circumstances*, 2018. No. 1. P. 49–58. URL: <https://euro-pub.co.uk/articles/risk-management-and-the-concept-of-risk-based-internal-control-A-662481>
4. Shin I., Park S. Integration of enterprise risk management and management control system: based on a case study. *Investment Management and Financial Innovations*. 2017. Vol. 14, no. 1. P. 19–26. DOI: [https://doi.org/10.21511/imfi.14\(1\).2017.02](https://doi.org/10.21511/imfi.14(1).2017.02) (date of access: 14.07.2025).
5. Tupa J., Simota J., Steiner F. Aspects of Risk Management Implementation for Industry 4.0. *Procedia Manufacturing*. 2017. Vol. 11. P. 1223–1230. DOI: <https://doi.org/10.1016/j.promfg.2017.07.248> (date of access: 14.07.2025).
6. Kholod Borys and Danyliuk Olena and Pavlova Valentyna and Bakulina Nataliia and Shtepa Olena and Orlova Victoria. Risk Management System Development at an Industrial Enterprise (May 13, 2020). *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 11(4), 2020, pp. 439–451. Available at: <https://ssrn.com/abstract=3599861>
7. Співак С., Мариняк Б. Моделювання ризику в системі управління промисловим підприємством. *Економічний аналіз*. 2022. Vol. 6, № 4. С. 298–304. DOI: <https://doi.org/10.35774/econa2022.04.298>.
8. Sotamaa T., Reiman A. Kauppila O. Manufacturing SME risk management in the era of digitalisation and artificial intelligence: a systematic literature review. *Continuity & Resilience Review*, 2025. Vol. 7 No. 1, pp. 1–28. DOI: <https://doi.org/10.1108/CRR-12-2023-0022>
9. Assessment of the impact of digitalized management on the financial risks of industrial enterprises / L. Vasylyshyna et al. *Eastern-European Journal of Enterprise Technologies*. 2022. Vol. 6, no. 13 (120). P. 87–95. DOI: <https://doi.org/10.15587/1729-4061.2022.268024> (date of access: 14.07.2025).
10. Frank H. Knight. Risk, Uncertainty and Profit. 1921. URL: [https://econlib.org/library/Knight/knRUP.html?chapter\\_num=8#book-reader?utm\\_source=chatgpt.com](https://econlib.org/library/Knight/knRUP.html?chapter_num=8#book-reader?utm_source=chatgpt.com)
11. Neumann J. v., Morgenstern O. Theory of Games and Economic Behavior. URL: [https://dwulff.github.io/\\_Goodchoices/Literature/Von%20NeumannMorgenstern1944TheoryOfGamesAndEconomicBehaviour.pdf](https://dwulff.github.io/_Goodchoices/Literature/Von%20NeumannMorgenstern1944TheoryOfGamesAndEconomicBehaviour.pdf)
12. Вепрал К. Ю. Загрози та ризики цифрової трансформації економіки. *Вісник Хмельницького національного університету*. 2020. Т. 3, № 4. С. 294–298. URL: <https://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/03/2020-4t3-53.pdf>

## REFERENCES:

1. Arena M., Arnaboldi M. & Azzone G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, 35(7), 659–675. DOI: <https://doi.org/10.1016/j.aos.2010.07.003>
2. Yasmin S. & Ghafran C. (2019). The problematics of accountability: Internal responses to external pressures in exposed organisations. *Critical Perspectives on Accounting*, 64, 102070. DOI: <https://doi.org/10.1016/j.cpa.2019.01.002>
3. Voronko R. & Vovchuk N. (2018). Risk management and the concept of risk-based internal control. *The Institute of Accounting, Control, and Analysis in the Globalization Circumstances*, (1), 49–58. <https://europub.co.uk/articles/risk-management-and-the-concept-of-risk-based-internal-control-A-662481>
4. Shin I. & Park S. (2017). Integration of enterprise risk management and management control system: Based on a case study. *Investment Management and Financial Innovations*, 14(1), 19–26. DOI: [https://doi.org/10.21511/imfi.14\(1\).2017.02](https://doi.org/10.21511/imfi.14(1).2017.02)
5. Tupa J., Simota J. & Steiner F. (2017). Aspects of risk management implementation for Industry 4.0. *Procedia Manufacturing*, 11, 1223–1230. DOI: <https://doi.org/10.1016/j.promfg.2017.07.248>
6. Kholod B., Danyliuk O., Pavlova V., Bakulina N., Shtepa O. & Orlova V. (2020). Risk management system development at an industrial enterprise. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 11(4), 439–451. Available at: <https://ssrn.com/abstract=3599861>
7. Spivak S. & Maryniak B. (2022). Modeliuvannia ryzyku v systemi upravlinnia promyslovym pidpriemstvom [Modeling risk in the management system of an industrial enterprise]. *Ekonomichnyi analiz – Economic Analysis*, 32(4), 298–304. DOI: <https://doi.org/10.35774/econa2022.04.298>
8. Sotamaa T., Reiman A. & Kauppila O. (2025). Manufacturing SME risk management in the era of digitalisation and artificial intelligence: A systematic literature review. *Continuity & Resilience Review*, 7(1), 1–28. DOI: <https://doi.org/10.1108/CRR-12-2023-0022>
9. Vasylyshyna L., et al. (2022). Assessment of the impact of digitalized management on the financial risks of industrial enterprises. *Eastern-European Journal of Enterprise Technologies*, 6(13[120]), 87–95. DOI: <https://doi.org/10.15587/1729-4061.2022.268024>
10. Knight F. H. (1921). *Risk, uncertainty and profit*. Available at: [https://www.econlib.org/library/Knight/knRUP.html?chapter\\_num=8#book-reader?utm\\_source=chatgpt.com](https://www.econlib.org/library/Knight/knRUP.html?chapter_num=8#book-reader?utm_source=chatgpt.com)
11. Von Neumann J. & Morgenstern O. (1944). *Theory of games and economic behavior*. Available at: [https://dwulff.github.io/\\_Goodchoices/Literature/Von%20NeumannMorgenstern1944TheoryOfGamesAndEconomicBehaviour.pdf](https://dwulff.github.io/_Goodchoices/Literature/Von%20NeumannMorgenstern1944TheoryOfGamesAndEconomicBehaviour.pdf)
12. Verhal K. Yu. (2020). Zahrozy ta ryzyky tsyfrovoy transformatsii ekonomiky [Threats and risks of the digital transformation of the economy]. *Visnyk Khmelnytskoho natsionalnoho universytetu – Bulletin of Khmelnytskyi National University*, 3(4), 294–298. Available at: <https://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/03/2020-4t3-53.pdf>