УДК 336.647/.648:004.9
JEL: G32; O33; M21
DOI: https://doi.org/10.32983/2222-4459-2026-8-401-415

ЦИФРОВІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ ПІДПРИЄМСТВА: ТЕХНОЛОГІЧНА АРХІТЕКТУРА, БАР'ЄРИ ВПРОВАДЖЕННЯ ТА СТРАТЕГІЧНІ НАПРЯМИ

© 2026 **ЗВЕРУК Л. А.**

УДК 336.647/.648:004.9
JEL: G32; O33; M21

Зверук Л. А. Цифровізація системи управління фінансовими ризиками підприємства: технологічна архітектура, бар'єри впровадження та стратегічні напрями

Статтю присвячено комплексному вивченню процесів цифровізації системи управління фінансовими ризиками підприємства. Наявні наукові праці присвячені переважно окремим цифровим технологіям (RegTech, штучний інтелект, блокчейн, Big Data) або певним категоріям фінансових ризиків, тоді як цифровий ризик-менеджмент як цілісна системна архітектура залишається малодослідженим; недостатньо розробок, які б враховували специфіку вітчизняних підприємств в умовах воєнно-економічних викликів та євроінтеграційних вимог. Метою статті є розробка комплексної науково-аналітичної концепції цифровізації системи управління фінансовими ризиками підприємства, що інтегрує методологічний, технологічний і практично-прикладний виміри проблеми. В процесі дослідження використано системний підхід, критичний та порівняльний аналіз (зіставлення традиційних і цифрових підходів за критеріями точності, оперативності, витратності й масштабованості), класифікаційний підхід, синтез і узагальнення. У статті обґрунтовано чотиривимірну модель цифрової трансформації ризик-менеджменту (когнітивний, аналітичний, операційний та архітектурний виміри). Систематизовано п'ять інструментальних груп цифрового фінансового ризик-менеджменту підприємства: RegTech, штучний інтелект і машинне навчання, Big Data та предиктивну аналітику, блокчейн і кіберзахист, виходячи із функцій, результатів використання й обмежень застосування кожного з інструментів. Кіберризик ідентифіковано як новий системний фінансовий ризик підприємства в умовах цифровізації. Виявлено технологічні, методологічні, організаційні та регуляторні бар'єри впровадження цифрових технологій у сфері управління фінансовими ризиками. Визначено шість стратегічних напрямів для побудови цифрової системи управління фінансовими ризиками. Висновок дослідження полягає в тому, що цифровізація – не автоматизація наявних процедур, а зміна парадигми управління ризиками: від ретроспективного, людиноцентричного та дискретного підходу до перспективного, гібридного («людина + алгоритм») і безперервного. Новизна полягає в системному поданні цифрового ризик-менеджменту як інтегрованої цілісної системи та у формулюванні парадоксу цифровізації, коли технології, покликані знижувати фінансові ризики, самі стають джерелом кіберризиків, алгоритмічних помилок і залежності від постачальників. Практична цінність дослідження полягає у систематизації інструментарію і окресленні стратегічних напрямів, які можуть слугувати для підприємств дорожньою картою цифровізації ризик-менеджменту та підготовки до вимог DORA і CSRD.

Ключові слова: *фінансовий ризик-менеджмент; цифрова трансформація підприємства; RegTech-комплаєнс; штучний інтелект; Big Data та предиктивна аналітика; блокчейн; кіберризик; ESG-ризики.*

Табл.: *2.* ***Бібл.:*** *20.*

Зверук Людмила Анатоліївна *– кандидат економічних наук, доцент, доцент кафедри фінансів і обліку, Київський кооперативний інститут бізнесу і права (вул. Юлії Здановської, 18, Київ, 03022, Україна)*
E-mail: *lyudmila.zveruk@gmail.com*
ORCID: *https://orcid.org/0000-0001-6531-5896*

UDC 336.647/.648:004.9
JEL: G32; O33; M21

Zveruk L. A. Digitalization of the Enterprise Financial Risk Management System: Technological Architecture, Implementation Barriers and Strategic Directions

The article provides a comprehensive study of the digitalization of the enterprise financial risk management system. Existing research is devoted mainly to individual digital technologies (RegTech, artificial intelligence, blockchain, Big Data) or to particular categories of financial risk, whereas digital risk management as an integral system architecture remains under-researched; there is a shortage of studies that take into account the specifics of domestic enterprises under wartime economic challenges and European integration requirements. The aim of the article is to develop a comprehensive scientific and analytical conception of the digitalization of the enterprise financial risk management system that integrates the methodological, technological and applied dimensions of the problem. The research employs the system approach, critical and comparative analysis (a comparison of traditional and digital approaches by the criteria of accuracy, timeliness, cost and scalability), a classification approach, synthesis and generalization. The article substantiates a four-dimensional model of the digital transformation of risk management (the cognitive, analytical, operational and architectural dimensions). Five instrumental groups of digital financial risk management of an enterprise are systematized – RegTech, artificial intelligence and machine learning, Big Data and predictive analytics, blockchain, and cybersecurity – on the basis of the functions, outcomes of use and application limitations of each instrument. Cyber risk is identified as a new systemic financial risk of the enterprise under digitalization. Technological, methodological, organizational and regulatory barriers to the implementation of digital technologies in the field of financial risk management are revealed. Six strategic directions for building a digital financial risk management system are determined. The study concludes that digitalization is not the automation of existing procedures but a change of the risk management paradigm: from a retrospective, human-centred and discrete approach to a forward-looking, hybrid («human + algorithm») and continuous one. The novelty lies in presenting digital risk management as an integrated and holistic system and in formulating the paradox of digitalization, whereby technologies intended to reduce financial risks themselves become a source of cyber risks, algorithmic errors and dependence on vendors. The practical value of the study lies in the systematization

of the tools and the outlining of strategic directions, which may serve enterprises as a roadmap for the digitalization of risk management and for preparing to meet DORA and CSRD requirements.

Keywords: *financial risk management; digital transformation of the enterprise; RegTech compliance; artificial intelligence; Big Data and predictive analytics; blockchain; cyber risk; ESG risks.*

Tabl.: *2.* ***Bibl.:*** *20.*

Zveruk Liudmyla A. *– PhD (Economics), Associate Professor, Associate Professor of the Department of Finance and Accounting, Kyiv Cooperative Institute of Business and Law (18 Yulii Zdanovskoi Str., Kyiv, 03022, Ukraine)*
E-mail: *lyudmila.zveruk@gmail.com*
ORCID: *https://orcid.org/0000-0001-6531-5896*

ВСТУП

Сучасне підприємство функціонує в середовищі багатовимірної ризикогенності, де традиційні межі між фінансовими, операційними та стратегічними ризиками стрімко розмиваються під тиском цифрової трансформації. Цифровізація економіки, що набуває дедалі більш всеохоплюючого характеру, не лише генерує принципово нові категорії ризиків: кіберризики, ризики алгоритмічних рішень, операційні ризики цифрових платформ, а й фундаментально змінює природу та динаміку вже існуючих фінансових ризиків.

Традиційна парадигма ризик-менеджменту, що ґрунтується на ретроспективному аналізі даних, статистичних моделях із жорсткими припущеннями про нормальний розподіл і лінійні залежності, а також людському судженні як центральному механізмі прийняття рішень, демонструє критичну недостатність в умовах, коли фінансові ризики миттєво матеріалізуються, а їх міжсистемна взаємозалежність досягає безпрецедентного рівня складності.

Особливої гостроти ця проблема набуває для підприємств, що працюють у сучасних складних умовах, а саме: в умовах воєнного стану, глобальної фінансової нестабільності, геополітичної фрагментації та одночасного тиску євроінтеграційних вимог щодо відповідності стандартам корпоративного управління та розкриття ризиків. Вітчизняні підприємства опиняються перед подвійним викликом.

З *одного боку*, існує необхідність імплементації передових цифрових рішень у сферу ризик-менеджменту, з *іншого* – бракує достатнього методологічного та практичного підґрунтя для такої імплементації. Зазначене вище актуалізує потребу в критичному переосмисленні концептуальних засад і технологічного інструментарію управління фінансовими ризиками підприємства з урахуванням можливостей та загроз, що несе в собі цифровізація. Саме це й зумовлює необхідність проведення цього дослідження.

ОГЛЯД ЛІТЕРАТУРИ

Проблематика управління фінансовими ризиками в умовах цифровізації перебуває на перетині кількох наукових напрямів, які активно розвиваються. Варто зазначити, що попри наявність значного масиву наукових розробок, питання комплексного впровадження цифрових інструментів у систему фінансового ризик-менеджменту підприємств залишається дискусійним.

У міжнародній науковій літературі значна увага направлена на дослідження ролі RegTech та FinTech технологій у трансформації ризик-менеджменту. Систематичний огляд Olaiya O. P. та інших у 2024році [1] показав, що RegTech-рішення суттєво скорочують витрати на комплаєнс, підвищують точність ідентифікації ризиків та прискорюють адаптацію до регуляторних змін. Водночас автори критично фіксують значне відставання практики впровадження від теоретичних можливостей технологій.

Фундаментальне дослідження конвергенції RegTech та FinTech, проведене міжнародним колективом авторів у 2025 році [2], довело, що інтеграція штучного інтелекту в регуляторні технології формує принципово новий рівень прозорості та безпеки фінансових екосистем. Автори констатують, що ані технологічна перевага, ані регуляторна підтримка самі по собі не є достатніми, тому виникає необхідність у системній інституційній трансформації.

Результати дослідження використання Big Data у фінансовому ризик-менеджменті, опубліковані у Frontiers in Artificial Intelligence у 2025 році [3], показали, що гібридні моделі машинного навчання, такі як Random Forest, XGBoost та їх селективні комбінації, домінують у виявленні шахрайства, кредитному скорингу та управлінні операційними ризиками над класичними однофакторними підходами. Однак автори також підкреслюють, що такі системи вимагають значних ресурсів для попередньої обробки даних і формування ознак, що обмежує їхню доступність для ресурсно-обмежених підприємств.

У сфері кредитного ризику важливим є дослідження авторів Gu Z. Lv J., Wu B., Hu Z., Yu X. [4], що демонструє ефективність МН-алгоритмів для оцінки кредитних ризиків малого та середнього бізнесу. Ключовим методологічним внеском є застосування алгоритмів обробки незбалансованих вибірок, що дозволяє адекватно оцінювати ризики для підприємств без достатньої кредитної історії.

Дослідження Lozić J. та Fotova Čiković K. (2024) [5], що стосується цифрової трансформації бізнес-діяльності, встановило, що підприємства, які системно впроваджують цифрові технології, демонструють не лише підвищену операційну ефективність, а й суттєво вищу стійкість до ризиків. Це підтверджує принципову важливість цифрового ризик-менеджменту як конкурентної переваги.

Серед вітчизняних наукових розробок заслуговують на увагу праці в галузі цифрової трансформації ризик-менеджменту підприємства [6; 7; 8]. Дослідження Танклевської Н. С. та Мірошниченка В. О. [6] охоплює трансформацію підходів до оцінки фінансового стану підприємства в умовах цифрової економіки. Кульчицький І. І. (2024) [7] аналізує стратегії управління економічною безпекою підприємств в умовах цифрової економіки, а Разумова Г. В. та Курносова О. І. (2024) [8] досліджують управління ризиками інвестиційної діяльності в умовах цифрової трансформації.

Критичний огляд наукової літератури дозволяє ідентифікувати ряд проблемних зон: по-перше, більшість досліджень зосереджена на окремих технологіях або категоріях ризиків, а не на системній архітектурі цифрового ризик-менеджменту; по-друге, практично відсутні дослідження, що враховують специфіку вітчизняних підприємств в умовах воєнно-економічних викликів; по-третє, недостатньо опрацьованими залишаються питання збалансування ефективності цифрових рішень та нових ризиків, генерованих ними. Ці прогалини і визначають дослідницький фокус даної статті.

МЕТА ДОСЛІДЖЕННЯ

Метою статті є розробка комплексної науково-аналітичної концепції цифровізації системи управління фінансовими ризиками підприємства, що інтегрує методологічні, технологічні та практично-прикладні виміри досліджуваної проблеми.

Реалізація поставленої мети передбачає вирішення таких завдань: розкрити теоретико-методологічні засади цифрової трансформації систем фінансового ризик-менеджменту підприємства; критично проаналізувати обмеженість традиційних підходів до ідентифікації та оцінки фінансових ризиків в умовах цифрової економіки; систематизувати ключові технологічні інструменти цифрового ризик-менеджменту та оцінити їх функціональні можливості; виявити проблеми та бар'єри практичного впровадження цифрових рішень; визначити стратегічні напрями побудови сучасної системи управління фінансовими ризиками підприємства.

МЕТОДИ ДОСЛІДЖЕННЯ

Методологічну основу дослідження становлять комплекс загальнонаукових та спеціальних методів. Системний підхід реалізовано в розгляді управління фінансовими ризиками як інтегрованої системи взаємопов'язаних елементів, а саме: методів ідентифікації, оцінки, моніторингу та контролю ризиків, де цифрові технології виступають трансформуючим чинником для кожного з цих елементів.

Критичний аналіз застосовано для виявлення методологічних обмежень існуючих підходів та суперечностей між теоретичними можливостями цифрових рішень і практикою їх впровадження. Порівняльний аналіз дозволив зіставити традиційні та цифрові підходи до управління фінансовими ризиками різних категорій за критеріями точності, оперативності, витратності та масштабованості. Класифікаційний підхід використано для систематизації технологічних інструментів цифрового ризик-менеджменту. Методи синтезу та узагальнення застосовані для формулювання стратегічних рекомендацій щодо побудови цифрової системи управління фінансовими ризиками підприємства.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Традиційна система управління фінансовими ризиками підприємства, що сформувалася протягом XX століття та базується на роботах Марковіца з портфельної теорії, концепції Value-at-Risk (VaR) і методологіях Basel, демонструє фундаментальні методологічні недоліки, які стають критичними в умовах цифрової економіки.

По-перше, переважання ретроспективної орієнтації, за якої більшість традиційних моделей оцінки ризиків є статистичними моделями, регресійним аналізом чи кредитними скоринговими картами, що ґрунтуються на аналізі минулих даних і недостатньо готові передбачати нові типи ризиків, що виникають унаслідок цифрових трансформацій і не мають аналогів в історії [3].

По-друге, існують проблеми структурованих даних. Традиційні методи оцінки ризиків оперують обмеженим набором структурованих фінансових

показників, а саме: коефіцієнтами ліквідності, рентабельності, боргового навантаження. При цьому ігнорується колосальний масив неструктурованих даних: транзакційні патерни в реальному часі, новинні потоки, інформація з соціальних мереж, геолокаційні та поведінкові дані, що несуть у собі суттєву ризик-інформацію [3; 9].

По-третє, людський чинник і когнітивні упередження. Традиційні системи ризик-менеджменту значною мірою спираються на людське судження, яке є вразливим до когнітивних упереджень (надмірної самовпевненості, ефекту підтвердження та ретроспективних спотворень) [2].

По-четверте, проблема недостатньої швидкості аналізу. Ручний збір та обробка даних, підготовка звітності, прийняття рішень через ієрархічні бюрократичні процедури, які є елементами традиційного ризик-менеджменту, генерують критичні тимчасові лаги, протягом яких ризикова ситуація може кардинально змінитися. Ці структурні обмеження традиційної парадигми й формують методологічне обґрунтування переходу до цифрового ризик-менеджменту.

Цифровізація системи управління фінансовими ризиками підприємства — це не просто автоматизація наявних процесів, а концептуальна зміна парадигми, що охоплює чотири взаємопов'язані виміри трансформації.

Перший вимір – когнітивний, коли здійснюється перехід від людського судження до гібридної моделі «людина + алгоритм», де системи штучного інтелекту беруть на себе рутинні аналітичні функції, звільняючи людських фахівців для розв'язання стратегічних і нестандартних завдань.

Другий вимір – аналітичний, який полягає у розширенні інформаційної бази ризик-менеджменту від структурованих фінансових показників до мультиджерельного потоку даних у режимі реального часу.

Третій вимір – операційний, за якого відбувається перехід від дискретних, переривчастих процесів оцінки ризику до безперервного, автоматизованого моніторингу.

Четвертий вимір – архітектурний, спрямований на формування інтегрованої цифрової екосистеми ризик-менеджменту, де різні технологічні рішення функціонують як компоненти єдиної системи. Таким чином, чотиривимірна модель цифрової трансформації ризик-менеджменту підприємства включає: когнітивний, аналітичний, операційний та архітектурний виміри. Сучасні дослідження [5; 9] підкреслюють, що успішна цифрова трансформація ризик-менеджменту вимагає синхронізованих змін не лише в технологічній площині, а й в організаційній культурі, компетентностях персоналу та корпоративному управлінні.

Оцінка рівня цифровізації фінансового ризик-менеджменту підприємства, в першу чергу, пов'язана з розглядом необхідного технологічного інструментарію (табл. 1).

Регуляторні технології (RegTech) являють собою клас цифрових рішень, що автоматизують процеси забезпечення відповідності регуляторним вимогам та управління ризиками комплаєнсу. У контексті фінансового ризик-менеджменту підприємства, RegTech виконує дві ключові функції: по-перше, операційну, яка включає автоматизацію збору, обробки та подання регуляторної звітності; по-друге, аналітичну, тобто забезпечення безперервного моніторингу відповідності бізнес-процесів нормативним вимогам та раннє попередження про можливі порушення. Аналіз емпіричних досліджень [10] дозволив встановити, що RegTech-рішення демонструють значне скорочення витрат на комплаєнс, вищу точність та швидкість виявлення порушень і покращений внутрішній кон-троль порівняно з традиційними підходами.

Ключовими функціональними модулями сучасних RegTech-систем є: автоматизований моніторинг транзакцій для протидії відмиванню коштів (AML); системи ідентифікації клієнтів (KYC) на основі цифрових ідентифікаторів та біометричного аналізу; платформи автоматизованої регуляторної звітності; інструменти управління ризиком відповідності в режимі реального часу [1]. Критично важливим у контексті євроінтеграційних прагнень України є те, що у сфері RegTech відбувається активна стандартизація вимог на рівні ЄС. Регламент DORA (Digital Operational Resilience Act), що набув чинності у 2025 році, встановлює жорсткі вимоги до цифрової операційної стійкості фінансових суб'єктів та управління ризиками інформаційно-комунікаційних технологій [10].

Однак, критичний погляд на RegTech-рішення виявляє, що є істотні обмеження. Так, фрагментарність регуляторного середовища, коли різні юрисдикції мають різні вимоги, ускладнює стандартизацію рішень. Особливо актуальною для вітчизняних підприємств із застарілою IT-інфраструктурою є технічна складність інтеграції. Певні обмеження пов'язані з ризиками залежності від постачальника рішень, що можуть перерости в системний ризик у разі кібератаки чи збоїв у роботі RegTech-провайдера [1; 2].

Найбільш технологічно зрілим та практично дієвим напрямом цифровізації у сфері фінансового ризик-менеджменту є застосування технологій

Таблиця 1

Технологічний інструментарій цифрового фінансового ризик-менеджменту підприємства

№	Технологія / Інструмент	Категорії ризиків, що охоплюються	Ключові функції у ризик-менеджменті	Результати застосування	Обмеження та ризики
1	2	3	4	5	6
RegTech — технологічна основа цифрового комплаєнсу та ризик-контролю					
1	RegTech-платформи (комплаєнс та моніторинг)	– Ризик комплаєнсу; – операційний ризик; – ризик регуляторних санкцій (AML/CFT)	– Автоматизований моніторинг транзакцій (AML); – ідентифікація клієнтів (KYC/KYB); – генерація регуляторної звітності; – відстеження змін у нормативній базі	– Скорочення витрат на комплаєнс; – підвищення точності виявлення порушень; – прискорення адаптації до регуляторних змін	– Фрагментарність регуляторного середовища; – складність інтеграції із застарілими (legacy)-системами; – залежність від постачальника
Штучний інтелект та машинне навчання (ШІ/МН) — ідентифікація та прогнозування ризиків					
2	Алгоритми ML (XGBoost, Random Forest, LSTM, ансамблеві моделі)	– Кредитний ризик; – ризик шахрайства; – ринковий ризик; – операційний ризик	– Кредитний скоринг на основі альтернативних даних; – виявлення шахрайських транзакцій (>97% точності); – прогнозування дефолту позичальника рішень; – оцінка операційних збоїв	– Точність виявлення шахрайства понад 97%; – скорочення хибнопозитивних сигналів у 3–5 разів; – підвищення точності кредиту. оцінки на 15–20%	– Ризик надмірної оптимізації (overfitting); – проблема «чорного ящика» (XAI); – відтворення дискримінаційних патернів
3	NLP та аналіз настроїв (Sentiment Analysis)	– Ринковий ризик; – репутаційний ризик; – ризик ESG	– Аналіз новинних потоків, соціальних медіа та корпоративних звітів у реальному часі; – виявлення ринкових та репутаційних ризиків до їх відображення у фінансових показниках	– Проактивне виявлення ризиків; – врахування неструктурованих даних; – підвищення оперативності ризик-рішень	– Залежність від якості медіа-даних; – складність інтерпретації у кроскультурному контексті
Big Data та предиктивна аналітика — нова інформаційна основа ризик-менеджменту					
4	Big Data-платформи та аналітика великих даних	– Кредитний ризик; – ринковий ризик; – системний ризик	– Агрегація та аналіз різнорідних масивів даних у реальному часі; – альтернативний кредитний скоринг (транзакційні шаблони, дані ланцюгів постачання); – стрес-тестування з вищою деталізацією сценаріїв	– Аналіз нелінійних залежностей; – підвищення точності моделей кредитного ризику МСП; – безперервний моніторинг без часових лагів	– Критична залежність від якості вхідних даних; – вимоги GDPR та захист персональних даних; – висока вартість інфраструктури

Закінчення табл. 1

1	2	3	4	5	6
Блокчейн – цілісність даних та прозорість транзакцій					
5	Блокчейн і смарт-контракти	– Ризик шахрайства; – контрактний ризик; – ESG-комплаєнс ризик	– Незмінний реєстр транзакцій для верифікації контрагентів; – автоматичне виконання зобов'язань через смарт-контракти; – верифікація ESG-показників у режимі реального часу та протидія greenwashing («зелене прикриття»)	– Підвищення прозорості фінансових операцій; – зниження ризику шахрайства у ланцюгах постачання; – достовірна ESG-звітність	– Масштабованість при великих обсягах транзакцій; – регуляторна невизначеність смарт-контрактів; – вразливість до кібератак державного рівня
Інструменти кіберзахисту – управління кіберризиком як системним фінансовим ризиком					
6	Системи кіберзахисту (Zero Trust, SOAR, поведінковий AI)	– Кіберризик; – операційний ризик; – репутаційний ризик	– Реалізація архітектури «нульової довіри» (Zero Trust); – AI-моніторинг аномалій та автоматичне реагування на інциденти (SOAR); – шифрування даних та захист ланцюгів постачання ПЗ	– Зниження ймовірності реалізації кіберінциденту; – прискорення реагування на загрози; – захист репутації та довіри інвесторів	– Значні витрати впровадження; – дефіцит кваліфікованих фахівців; – неможливість повного усунення «людського фактору»

Джерело: складено автором на основі [1; 2; 3; 4; 5; 6; 7; 8].

Примітка: RegTech – регуляторні технології; AML – протидія відмиванню коштів; CFT – протидія фінансуванню тероризму; KYC/KYB – ідентифікація клієнтів/бізнесу; ML – машинне навчання; LSTM – довга короткострокова пам'ять (тип нейронної мережі); NLP – обробка природної мови; XAI – пояснюваний штучний інтелект; GDPR – Загальний регламент ЄС про захист даних; SOAR – управління, автоматизація та реагування на інциденти безпеки; ESG – екологічні, соціальні та управлінські критерії; Zero Trust – архітектура «нульової довіри».

штучного інтелекту (ШІ) та машинного навчання (МН). Їхнє проникнення охоплює всі ключові категорії фінансових ризиків підприємства. У сфері кредитного ризику МН-алгоритми, зокрема, градієнтний бустинг (XGBoost), нейронні мережі LSTM та моделі Random Forest, дозволяють аналізувати значно ширший спектр даних порівняно з традиційними кредитними скоринговими картами (від транзакційних патернів та активності в соціальних мережах до ланцюгових зв'язків в мережах постачальників) [4; 11]. Дослідження Gu Z. та ін. [4] показало, що застосування МН-моделей з алгоритмами обробки незбалансованих вибірок дозволяє підвищити точність оцінки кредитних ризиків малих та середніх підприємств на 15–20% порівняно з традиційними підходами.

У галузі виявлення операційних ризиків і шахрайства ансамблеві МН-моделі демонструють особливо вражаючі результати. За даними Frontiers in Artificial Intelligence [3], такі системи досягають точності ідентифікації шахрайських транзакцій понад 97%, водночас у 3–5 разів скорочуючи кількість хибнопозитивних сигналів, що є критичною проблемою для традиційних систем. Цей результат є принципово важливим, оскільки надмірна кількість хибнопозитивних сигналів призводить до «втоми від сповіщень» у аналітиків та фактичного зниження ефективності ризик-контролю.

Обробка природної мови (NLP) розширює аналітичні можливості ШІ-систем ризик-менеджменту у принципово новий спосіб. Дані системи, аналізуючи новинні потоки, корпоративні оголошення, протоколи засідань регуляторів та дискусії у соціальних медіа, дозволяють виявляти ринкові ризики та ризики репутації ще до того, як вони відобразяться у фінансових показниках [2; 3]. Алгоритми аналізу настроїв, що виявляють негативні сигнали у реальному часі, набувають особливого значення в умовах надзвичайної вола-

тильності ринків, коли традиційні лагові індикатори виявляються безнадійно запізнілими.

Водночас застосування ШІ та МН-моделей у ризик-менеджменті несе в собі низку критичних загроз. Проблема «чорного ящика» та непрозорості алгоритмів ускладнює пояснення рішень регуляторам і зацікавленим сторонам, особливо в контексті зростаючих вимог стандарту XAI (Explainable AI). Ризик надмірної оптимізації на історичних даних і, як наслідок, недооцінки «хвостових» ризиків (рідкісних, але катастрофічних подій) залишається системним методологічним обмеженням МН-підходів [3].

Технології великих даних (Big Data) революційно змінюють інформаційну основу фінансового ризик-менеджменту підприємства, розширюючи її від вузького набору структурованих фінансових показників до мультиджерельного масиву різноформатних даних. У практиці управління фінансовими ризиками Big Data забезпечує п'ять ключових аналітичних можливостей: безперервний моніторинг ризикових індикаторів у режимі реального часу без часових лагів, характерних для традиційної звітності; виявлення нелінійних зв'язків та складних взаємозалежностей у ризиковій поведінці, що не піддаються виявленню стандартними статистичними методами; альтернативний кредитний скоринг на основі нефінансових даних (транзакційні шаблони, поведінкові дані, дані ланцюгів постачання); ситуаційний аналіз і стрес-тестування з вищим рівнем деталізації та реалістичності сценаріїв; агрегація та аналіз системних ризиків фінансових екосистем [3; 9].

Аналіз альтернативних даних, таких як транзакції у ланцюгах постачання, дані онлайн-платформ, патерни комунікацій [4], дозволяє суттєво підвищити якість моделей щодо прогнозування кредитного ризику для малих і середніх підприємств, де традиційний аналіз балансових показників є обмеженим через непрозорість звітності.

Практичне впровадження Big Data у ризик-менеджменті підприємств, однак стикається із серйозними бар'єрами. Якість та достовірність даних залишаються критичними обмеженнями через «сміттєві» вхідні дані, які генерують помилкові ризикові сигнали і можуть бути більш небезпечними, ніж їх відсутність. Забезпечення відповідності вимогам GDPR та вітчизняного законодавства про захист персональних даних за одночасного підвищення аналітичної цінності великих даних є складним балансуючим процесом, що вимагає як технологічних, так і правових рішень [2; 10].

Якісно нові можливості у сфері управління фінансовими ризиками підприємства відкриває технологія блокчейн, і здійснюється це, через три ключові характеристики: незмінність записів, децентралізований консенсус, прозорість транзакцій. В архітектурі цифрового ризик-менеджменту блокчейн відіграє роль довіреного середовища зберігання та обміну даними. Дослідження Frontiers in Blockchain [12] доводить, що децентралізований незмінний реєстр блокчейну суттєво підвищує безпеку фінансових транзакцій і знижує потенціал кібератак та шахрайства порівняно з традиційними централізованими системами.

Практичне застосування блокчейну в управлінні фінансовими ризиками підприємства охоплює кілька ключових напрямів. Перший напрям, пов'язаний із верифікацією контрагентів та управлінням ризиком партнерства. Блокчейн-реєстри забезпечують незмінну хронологію комерційних відносин, що суттєво знижує ризики шахрайства в ланцюгах постачання. Другий напрям – використання смарт-контрактів як інструменту автоматичного виконання зобов'язань і мінімізації контрактних ризиків. Вбудовані в блокчейн програмні контракти автоматично виконують умови угод при настанні визначених подій, виключаючи ризик неналежного виконання. Третій напрям реалізується шляхом впровадження ESG-комплаєнсу та верифікації сталого розвитку. Результати сучасних досліджень [13] підтверджують, що блокчейн дозволяє відстежувати та верифікувати ESG-показники у режимі реального часу, забезпечуючи достовірність звітності про сталий розвиток та знижуючи ризики «зеленого камуфляжу». Проте критичний аналіз дозволяє виявляти і суттєві обмеження блокчейну у сфері ризик-менеджменту. Глобальний ринок безпеки блокчейн-систем, за даними Allianz Commercial [14], має зрости з 20 млрд дол. США у 2024 році до 250 млрд дол. США протягом наступних п'яти років, що свідчить про масштаб кіберзагроз, які супроводжують розповсюдження блокчейн-технологій. Кібератаки державного рівня (як-от атака на ByBit, що завдала збитків на 1,5 млрд дол. США) демонструють, що навіть криптографічно захищені системи є вразливими в контексті операційних і людських ризиків [14].

Отже, парадоксальна природа цифровізації ризик-менеджменту полягає в тому, що вона одночасно є засобом управління ризиками та джерелом принципово нових ризиків. Кіберризик можна охарактеризувати як ймовірність фінансових втрат, операційних збоїв і репутаційного збитку внаслідок кібератак, збоїв IT-систем або

несанкціонованого доступу до даних. Цей вид ризику трансформувався із суто технічної проблеми ІТ-департаментів у ризик стратегічного значення, що потребує уваги на рівні ради директорів і правління підприємства. Дослідження на основі аналізу банківського сектору [15], також переконливо підтверджують, що кіберризики вийшли за межі суто ІТ-проблематики і перетворилися на стратегічний чинник довгострокової ефективності бізнесу. Тому установи, що інвестують у надійні системи кіберзахисту, не лише захищають дані та виконують регуляторні вимоги, а й будують довіру з боку інвесторів та клієнтів, тобто управляють репутаційним ризиком. Allianz Risk Barometer ідентифікує кіберінциденти як ризик номер один у глобальному рейтингу на 2026 рік, з відривом 10% від наступної позиції [14], яку займає штучний інтелект. Таким чином, дві ключові технології цифровізації одночасно є і найбільшими джерелами ризику.

Кіберризик, у системі управління фінансовими ризиками підприємства, виявляється через кілька специфічних каналів. Перший – це прямі фінансові втрати, а саме: крадіжка коштів через компрометацію платіжних систем, вимагання через програми-шифрувальники, штрафи регуляторів за порушення захисту даних. Другий канал виявлення кіберризиків – це непрямі втрати, зокрема: операційні збої, що порушують виробничі процеси та ланцюги постачання; репутаційний збиток, що знижує ринкову вартість підприємства та ускладнює доступ до фінансування. Третій канал пов'язаний із системними ризиками, які проявляються у атаках на критичну фінансову інфраструктуру (платіжні системи, розрахункові платформи) і можуть мати каскадний ефект для всіх підприємств, що від неї залежать.

Отже, архітектура кіберстійкого фінансового ризик-менеджменту передбачає реалізацію принципу «нульової довіри», коли жоден користувач, пристрій або мережевий сегмент не вважається довіреним за замовчуванням, незалежно від їхнього місцезнаходження відносно мережевого периметра. Ключові технологічні елементи такої архітектури включають: поведінковий аналіз на основі ШІ для виявлення аномалій у реальному часі; автоматичне реагування на інциденти (SOAR); шифрування даних у стані спокою та в русі; криптографічний захист ланцюгів постачання програмного забезпечення [2; 14; 15].

Попри очевидний потенціал цифрових технологій у сфері управління фінансовими ризиками, практика їх впровадження стикається з комплексом системних бар'єрів, які потребують усвідомленого управління. Виділимо основні з них: технологічні бар'єри; методологічні та організаційні бар'єри; регуляторну невизначеність; проблему довіри та сприйняття цифрових рішень.

Проблема успадкованих (застарілих) систем є, мабуть, найбільш гострим технічним бар'єром, адже значна частина вітчизняних підприємств функціонує на застарілих корпоративних ІТ-системах, архітектура яких не передбачає інтеграції сучасних цифрових рішень. Вартість такої інтеграції або повної заміни систем може сягати десятків мільйонів гривень і потребувати значних витрат часу [7; 8]. Крім того, якість даних у таких системах нерідко є незадовільною. Дані можуть містити дублікати, пропуски та невідповідності, що підривають ефективність навіть найпередовіших МН-алгоритмів. Принцип «сміття на вході – сміття на виході» є особливо актуальним для ризик-менеджменту підприємства, де помилковий сигнал може спричинити неправильне управлінське рішення.

Дефіцит кваліфікованих кадрів, що поєднують компетентності у фінансовому ризик-менеджменті та цифрових технологіях, є критичним обмежувальним чинником. Технологічні рішення без відповідних людських компетентностей нефункціональні. Дослідження [10] фіксує, що навіть найбільш технологічно розвинені фінансові установи стикаються з «розривом компетентностей» між ІТ-спеціалістами, які розробляють цифрові рішення, та ризик-менеджерами, які їх використовують. Цей розрив призводить до неправильного трактування результатів алгоритмічного аналізу та субоптимальних рішень.

Регуляторна невизначеність також створює суттєві бар'єри. Чинне законодавство України у сфері захисту персональних даних, кіберзахисту та використання ШІ для фінансових рішень розвивається повільніше, ніж технологічні можливості, що створює правову невизначеність. Зокрема, питання відповідальності за рішення, прийняті ШІ-алгоритмами, регулятивного статусу смарт-контрактів та вимог до прозорості ШІ-моделей у фінансових рішеннях є вирішеними лише фрагментарно [6; 10].

Суттєвим нематеріальним бар'єром є скептичне ставлення до цифрових рішень з боку ризик-менеджерів з великим досвідом роботи в традиційній системі. Цифрова трансформація ризик-менеджменту вимагає не просто впровадження нових інструментів, а й зміни культури прийняття рішень, переходу від інтуїтивного до аналітично обґрунтованого підходу, а також готовності делегувати частину аналітичних функцій алгоритмам [5; 9]. Ці культурні та ментальні зміни є повільнішими та складнішими, ніж технологічні.

На підставі проведеного комплексного дослідження можна визначити стратегічні напрями, що формують дорожню карту цифровізації системи управління фінансовими ризиками сучасного підприємства (табл. 2).

Перший стратегічний напрям полягає у побудові інтегрованої цифрової платформи ризик-менеджменту. Сучасна концепція цифрового ризик-менеджменту передбачає перехід від набору ізольованих інструментів до єдиної інтегрованої

Таблиця 2

Стратегічні напрями побудови цифрової системи управління фінансовими ризиками підприємства

№	Стратегічний напрям	Зміст і ключові заходи	Технологічні рішення	Регуляторна основа	Очікуваний ефект для підприємства
1	2	3	4	5	6
1	Побудова інтегрованої цифрової платформи ризик-менеджменту	– Перехід від ізольованих інструментів до єдиної платформи управління всіма категоріями фінансових ризиків; – єдина база даних ризиків у реальному часі; – автоматизована генерація управлінської та регуляторної звітності; – API-first архітектура для інтеграції підсистем	– RegTech-платформи; – ERM-системи; – хмарні обчислення; – API-інтеграція	– DORA (ЄС); – Базель III (Pillar 2); – нормативи НБУ	– Цілісний погляд на ризик-профіль; – скорочення часу прийняття рішень; – зниження операційних витрат
2	Впровадження предиктивної аналітики ризиків на основі ШІ/МН	– Перехід від реактивного до проактивного ризик-менеджменту; – системи раннього попередження про фінансові ризики на основі ML-моделей; – NLP-моніторинг медіапростору для виявлення репутаційних та ринкових ризиків; – предиктивне стрес-тестування	– ML/DL алгоритми; – NLP/sentiment analysis; – AI Early Warning Systems; – сценарне моделювання (Монте-Карло)	– Базель III (ICAAP); – вимоги ESMA; – рекомендації FSB	– Випереджальне виявлення ризиків; – підвищення точності ризик-оцінок; – зниження резервів під очікувані збитки
3	RegTech-комплаєнс та підготовка до євроінтеграційних вимог	– Впровадження RegTech для автоматизації комплаєнсу з DORA, MiFID II, SFDR; – перетворення комплаєнсу з витратного центру на джерело конкурентної переваги; – підвищення прозорості та довіри інвесторів через ESG-ризик-звітність	– RegTech (AML, KYC); – автоматизована регуляторна звітність; – ESG-рейтингові платформи	– DORA (2025); – MiFID II; – SFDR; – FATF (AML/CFT)	– Зниження регуляторних штрафів; – доступ до пільгового «зеленого» фінансування; – підвищення ESG-рейтингу
4	Побудова кіберстійкої архітектури	– Реалізація принципу Zero Trust - жоден сегмент мережі	– Zero Trust архітектура;	– DORA (ICT risk); – NIS2 (ЄС);	– Зниження ймовірності кіберінциденту;

Закінчення табл. 2

1	2	3	4	5	6
	фінансового ризик-менеджменту	не вважається довіреним за замовчуванням; – запровадження AI-систем виявлення аномалій та SOAR; – формування культури кібербезпеки та регулярні навчання за кризовими сценаріями; – страхування кіберризиків	– Zero Trust архітектура; – SOAR-системи; – поведінковий AI (UEBA); – EDR/XDR рішення	– ISO 27001; – вимоги НБУ до кіберзахисту	– скорочення часу відновлення; – захист репутації та вартості бізнесу
5	Інтеграція ESG-ризиків у цифрову систему ризик-менеджменту	– Кількісна оцінка кліматичних (фізичних і перехідних) та соціальних ризиків; – блокчейн-верифікація ESG-даних для запобігання greenwashing; – AI-аналітика вуглецевого сліду та кліматичних сценаріїв; – автоматизація звітності за стандартами TCFD та CSRD	– ESG-скорингові AI-моделі; – блокчейн ESG-реєстри; – TCFD-сумісні сценарні інструменти; – платформи нефінансової звітності	– CSRD (ЄС); – TCFD; – SFDR; – таксономія ЄС	– Зниження вартості «зеленого» капіталу; – покращення ESG-рейтингу; – зменшення кліматичних збитків
6	Розвиток цифрових компетентностей персоналу ризик-менеджменту	– Навчання розуміння принципів роботи ШІ/МН-алгоритмів та критичного аналізу їх рекомендацій; – розвиток компетентностей у кіберзахисті, ESG-аналізі та роботі з великими даними; – формування гібридної культури «людина + алгоритм» в управлінні ризиками [2; 9]	– LMS-платформи; – симулятори ризик-сценаріїв; – цифрові навчальні середовища; – сертифікація FRM/CAMS	– Стратегія ЄС щодо ШІ; – вимоги XAI (Explainable AI); – Базель III (Model Risk Management)	– Підвищення якості ризик-рішень; – зниження «втоми від сповіщень»; – стійкість до маніпуляцій з алгоритмами

Джерело: складено автором на основі [1; 2; 3; 5; 6; 7; 8; 9; 10; 16; 18].

Примітка: DORA – Регламент ЄС про цифрову операційну стійкість (Digital Operational Resilience Act, набув чинності 2025 р.); MiFID II – Директива ЄС про ринки фінансових інструментів; SFDR – Положення ЄС про розкриття інформації зі сталого фінансування; FATF – Група з розробки фінансових заходів боротьби з відмиванням грошей; ICAAP – процедура внутрішньої оцінки достатності капіталу; FSB – Рада фінансової стабільності; ESMA – Європейський орган з цінних паперів та ринків; TCFD – Цільова група з питань фінансової звітності щодо клімату; CSRD – Директива про корпоративну звітність зі сталості; UEBA -аналіз поведінки користувачів та організацій; EDR/XDR – виявлення та реагування на кінцеві точки/розширені загрози; FRM – сертифікований менеджер фінансових ризиків (GARP); CAMS – сертифікований спеціаліст боротьби з відмиванням грошей.

платформи, що охоплює всі категорії фінансових ризиків і всі фази ризик-менеджменту (ідентифікацію, оцінку, моніторинг, контроль та звітність). Ключовими принципами такої платформи є: API-first архітектура, що забезпечує інтеграцію різних технологічних модулів; єдина база даних ризиків у режимі реального часу; автоматизована генерація управлінської та регуляторної звітності.

Другий напрям побудови цифрової системи управління фінансовими ризиками підприємства спрямований на впровадження предиктивної аналітики ризиків на основі ШІ/МН. Стратегічним

пріоритетом за цим напрямом буде перехід від реактивного (фіксація факту реалізації ризику) до проактивного (прогнозування ризиків до їх матеріалізації) ризик-менеджменту. Практична реалізація передбачає: впровадження систем раннього попередження про фінансові ризики на основі МН-моделей; застосування NLP-систем для моніторингу медіапростору та виявлення репутаційних та ринкових ризиків; використання інструментів предиктивної аналітики для сценарного планування та стрес-тестування.

Третій напрям передбачає впровадження RegTech-комплаєнсу та підготовку до виконання євроінтеграційних вимог. З огляду на євроінтеграційний курс України, стратегічно важливим є випереджальне приведення системи ризик-менеджменту у відповідність до вимог ЄС: DORA (цифрова операційна стійкість), MiFID II (ринкові ризики), SFDR (розкриття ризиків сталості). Впровадження RegTech-рішень дозволяє не лише забезпечити таку відповідність, а й перетворити комплаєнс із витратного центру на джерело конкурентної переваги через підвищену прозорість та довіру з боку інвесторів і партнерів.

Четвертий стратегічний напрям полягає у побудові кіберстійкої архітектури фінансового ризик-менеджменту. Стратегічна відповідь підприємства на зростаючу кіберзагрозу передбачає три взаємопов'язані елементи: технологічний, через впровадження Zero Trust-архітектури, ШІ-систем виявлення аномалій та автоматичного реагування на інциденти; організаційний, за допомогою формування культури кібербезпеки, навчання персоналу та регулярних тренувань за сценаріями кіберінцидентів; фінансовий, який включає страхування кіберризиків як частину комплексної стратегії управління фінансовими ризиками [14; 15].

П'ятий напрям побудови цифрової системи управління фінансовими ризиками підприємства спрямований на інтеграцію ESG-ризиків у цифрову систему ризик-менеджменту. Регуляторний тиск ЄС та зростаючі очікування інвесторів щодо сталого розвитку перетворюють ESG-ризики (кліматичні, соціальні, управлінські) на центральний елемент корпоративного ризик-менеджменту. Цифрові технології відіграють тут ключову роль через те, що: блокчейн-системи забезпечують верифікацію ESG-даних і запобігають «зеленому камуфляжу»; ШІ-аналітика дозволяє кількісно оцінювати кліматичні ризики та їх фінансовий вплив; RegTech-рішення автоматизують звітність відповідно до стандартів TCFD та CSRD.

Шостий стратегічний напрям передбачає розвиток цифрових компетентностей персоналу ризик-менеджменту. Технологічна досконалість систем ризик-менеджменту нівелюється, якщо персонал не здатний ефективно їх використовувати та інтерпретувати результати. Стратегічна програма розвитку компетентностей має охоплювати: глибоке розуміння принципів роботи ШІ/МН-алгоритмів та їх обмежень; навички критичного аналізу алгоритмічних рекомендацій; компетентності у сфері кіберзахисту та управління кіберризиками; здатність до роботи з великими масивами даних та інструментами візуалізації ризиків.

ОБГОВОРЕННЯ

Обґрунтована чотиривимірна модель цифрової трансформації ризик-менеджменту, представлена у дослідженні, узгоджується з висновком Lozić J. та Fotova Čiković K. [5] про вищу ризикостійкість підприємств із системним упровадженням цифрових технологій, проте конкретизує цей висновок. Зазначені автори фіксують кореляцію між цифровою зрілістю та стійкістю на рівні бізнес-діяльності загалом, тоді як запропонована модель пояснює механізм цієї залежності через одночасну трансформацію способу прийняття рішень, інформаційної бази, режиму моніторингу та архітектури системи. Дослідження Танклевської Н. С. і Мірошниченка В. О. [6] розкриває трансформацію підходів до оцінки фінансового стану підприємства, але залишає поза увагою архітектурну інтеграцію оцінних інструментів у єдину систему. Показовим є зіставлення з висновком [2] про недостатність як технологічної переваги, так і регуляторної підтримки самі по собі. Проведене дослідження пояснює причину цього, адже жоден із ідентифікованих інструментів не є самодостатнім, а ефект досягається виключно за їхньої системної інтеграції зі змінами в організаційній культурі та компетентностях персоналу, що узгоджується із зафіксованим в огляді 59 досліджень [10] «розривом компетентностей» між розробниками рішень і ризик-менеджерами.

Виявлена результативність ШІ- та МН-інструментів корелює з емпіричними даними попередніх робіт, а саме, підвищення точності оцінки кредитних ризиків малих і середніх підприємств на 15–20 % за рахунок алгоритмів обробки незбалансованих вибірок [4] та точність ідентифікації шахрайських транзакцій понад 97 % за скорочення хибнопозитивних сигналів у 3–5 разів [3], що підтверджує перевагу гібридних і ансамблевих моделей над однофакторними підходами. Проте представлена інтерпретація цих даних є стриманішою, ніж у публікаціях, орієнтованих на демонстрацію технологічних можливостей [11; 19; 20]. Високі показники точності отримано на

ретроспективних вибірках, і вони не гарантують адекватної поведінки моделей у зоні «хвостових» ризиків (рідкісних, але катастрофічних подій, де концентрується основна загроза фінансовій стійкості); приріст точності на типових спостереженнях і надійність моделі в критичних сценаріях є різними за властивостями, що в літературі нерідко ототожнюють.

Щодо регуляторних технологій, результати представленого дослідження частково розходяться з оптимістичною тональністю попередніх оцінок [1; 10]. Погоджуючись із зафіксованим скороченням витрат на комплаєнс і підвищенням точності виявлення порушень, в дослідженні вказано, що залежність від постачальника RegTech-рішень є не операційною незручністю, а системним ризиком. Концентрація критичних функцій комплаєнсу в невеликій кількості провайдерів створює єдину точку відмови, реалізація якої через кібератаку чи збій одночасно вражає всіх їхніх клієнтів. Схожу логіку закладено в Регламенті DORA щодо ризиків третіх сторін, однак у літературі цей аспект залишається недостатньо концептуалізованим. Результати дослідження щодо блокчейну узгоджуються з висновками [12; 13] про підвищення безпеки транзакцій і прозорості ESG-звітності, проте представлена позиція вказує на певні обмеження, адже блокчейн доцільно розглядати як інфраструктурний рівень довіри до даних, а не як інструмент оцінки ризику, оскільки незмінність запису гарантує цілісність даних, але не їх достовірність у момент внесення.

Обґрунтований парадокс цифровізації, за якого дві ключові технології цифровізації водночас є й найбільшими джерелами ризику, підтверджується даними Allianz Risk Barometer [14]. Кіберінциденти визначено як ризик номер один на 2026 рік, а штучний інтелект посідає другу позицію. На відміну від розробок, які трактують кіберризик як окрему категорію операційного ризику [17], в представленому дослідженні обґрунтовано його інтеграцію в систему фінансового ризик-менеджменту через три канали матеріалізації: прямі та непрямі фінансові втрати і системні ефекти. Такий підхід узгоджується з висновками щодо зв'язку кібербезпеки, ESG та операційного ризику з результативністю банків [15], але поширює його на підприємства реального сектору.

Вітчизняні дослідження охоплюють важливі, проте фрагментарні аспекти: стратегії управління економічною безпекою [7], ризики інвестиційної діяльності [8], цифрові технології в ризик-менеджменті агросфери [9]. Виявлені в процесі дослідження бар'єри: успадковані системи, дефіцит кадрів на стику фінансів і технологій, регуляторна невизначеність, культурний спротив зводяться окремі спостереження цих авторів у єдину класифікацію. Відмінністю представленого підходу є висновок про інституційну природу бар'єрів, що потребує скоординованих зусиль на всіх рівнях (підприємства, галузевих об'єднань, держави), тоді як більшість наявних досліджень зосереджена на рівні окремого підприємства. Слід також зауважити, що предметна сфера характеризується високою швидкістю технологічних і регуляторних змін. Набуття чинності Регламенту DORA, розгортання вимог CSRD, поява генеративних моделей та великих мовних моделей у фінансовій аналітиці [19] означають, що часова валідність окремих висновків є обмеженою і потребує періодичного перегляду.

ВИСНОВКИ

Проведене дослідження дає змогу сформулювати низку ключових висновків щодо цифровізації системи управління фінансовими ризиками підприємства.

По-перше, цифровізація не є простим доповненням до традиційної системи ризик-менеджменту, а виступає її концептуальною трансформацією, пов'язаною зі зміною самої парадигми управління ризиками – від ретроспективного, людиноцентричного, дискретного підходу до проспективного, гібридного (людина + алгоритм), безперервного. Традиційні методи оцінки ризиків на основі структурованих фінансових показників та ретроспективних даних принципово не здатні адекватно реагувати на виклики цифрової економіки, де ризики виникають і матеріалізуються на принципово вищих швидкостях.

По-друге, технологічний арсенал цифрового ризик-менеджменту включає п'ять ключових інструментальних груп: RegTech (автоматизація комплаєнсу та регуляторного контролю), ШІ та МН (ідентифікація та прогнозування ризиків), Big Data та предиктивна аналітика (розширення інформаційної бази), блокчейн (цілісність даних і верифікація транзакцій) та кіберзахист (управління кіберризиками). Жоден із цих інструментів не є самодостатнім, а лише їхня системна інтеграція формує ефективну цифрову архітектуру ризик-менеджменту.

По-третє, критичний аналіз виявив ключовий парадокс цифровізації ризик-менеджменту. Технології, покликані знижувати фінансові ризики, самі є джерелами нових системних ризиків: кіберризиків, ризиків алгоритмічних помилок, ризиків залежності від постачальників технологій. Управ-

ління цим парадоксом вимагає балансуючого підходу, що поєднує максималізацію аналітичних можливостей цифрових технологій із жорстким контролем ризиків, породжуваних ними.

По-четверте, практичне впровадження цифрових рішень у систему ризик-менеджменту вітчизняних підприємств гальмується комплексом взаємопов'язаних технологічних, методологічних, організаційних та регуляторних бар'єрів, подолання яких потребує скоординованих зусиль на рівні підприємства, галузевих об'єднань і держави.

По-п'яте, визначено шість стратегічних напрямів побудови цифрової системи управління фінансовими ризиками: інтегрована цифрова платформа ризик-менеджменту; предиктивна аналітика; RegTech-комплаєнс і підготовка до євроінтеграційних вимог; кіберстійка архітектура на засадах Zero Trust; інтеграція ESG-ризиків; розвиток компетентностей персоналу.

Наукова новизна у наступному. Обґрунтовано чотиривимірну концептуальну модель цифрової трансформації системи управління фінансовими ризиками підприємства (когнітивний, аналітичний, операційний, архітектурний виміри), яка розглядає цифровізацію не як сукупність окремих технологічних упроваджень, а як цілісну зміну архітектури системи. Сформульовано парадокс цифровізації ризик-менеджменту як методологічну проблему, що потребує окремого управлінського контуру. Удосконалено класифікацію інструментарію за категоріями охоплюваних ризиків, функціями, результатами застосування та обмеженнями. Набули подальшого розвитку положення щодо кіберризику як складника системи фінансових ризиків підприємства (три канали матеріалізації у фінансові наслідки) та щодо систематизації бар'єрів цифровізації з урахуванням специфіки вітчизняних підприємств.

Практична цінність результатів полягає в тому, що запропонована систематизація інструментарію та стратегічні напрями можуть використовуватися підприємствами як дорожня карта поетапної цифровізації ризик-менеджменту з урахуванням рівня їх цифрової зрілості, а виявлені обмеження кожної групи технологій дають змогу формувати реалістичні очікування щодо ефектів упровадження. Прив'язка напрямів до регуляторних вимог (DORA, MiFID II, SFDR, CSRD, нормативів НБУ) робить результати придатними для підготовки підприємств до виконання євроінтеграційних зобов'язань.

Перспективи подальших досліджень пов'язані з розробкою кількісних методик оцінки ефективності цифрових систем ризик-менеджменту та окупності відповідних інвестицій; дослідженням впливу євроінтеграційних регуляторних вимог (DORA, CSRD) на архітектуру цифрового ризик-менеджменту вітчизняних підприємств; розробкою методологічних засад управління ризиками алгоритмічних рішень у системах ШІ-орієнтованого фінансового аналізу. ■

БІБЛІОГРАФІЯ

1. Olaiya O. P., Adesoga T. O., Pieterson K., Obani O. Q., Adebayo J. O., Ajayi O. O. RegTech solutions: enhancing compliance and risk management in the financial sector. *GSC Advanced Research and Reviews*. 2024. Vol. 20, No. 2. P. 8–15. DOI: https://doi.org/10.30574/gscarr.2024.20.2.0295
2. Abbas Anwar, Zeeshan Umer. RegTech and FinTech convergence: leveraging artificial intelligence for transparent and secure financial ecosystems. *World Journal of Advanced Research and Reviews*. 2025. Vol. 27, No. 3. P. 1796–1808. DOI: https://doi.org/10.30574/wjarr.2025.27.3.3356
3. Theodorakopoulos L., Theodoropoulou A., Bakalis A. Big data in financial risk management: evidence, advances, and open questions: a systematic review. *Frontiers in Artificial Intelligence*. 2025. Vol. 8. Art. 1658375. DOI: https://doi.org/10.3389/frai.2025.1658375 (
4. Gu Z., Lv J., Wu B., Hu Z., Yu X. Credit risk assessment of small and micro enterprise based on machine learning. *Heliyon*. 2024. Vol. 10. № 5. Art. e27096. DOI: https://doi.org/10.1016/j.heliyon.2024.e27096
5. Lozić J., Fotova Čiković K. Digital transformation: the fundamental concept of transformation of business activities. *107th International Scientific Conference on Economic and Social Development – Economic and Social Survival in Global Changes*, Zagreb. P. 326–337. Танклевська Н. С., Мірошниченко В. О. Фінансова стійкість підприємств в умовах цифрової економіки. *Бізнес Інформ*. 2024. № 3. С. 249–255. DOI: https://doi.org/10.32983/2222-4459-2024-3-249-255
6. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. *Актуальні питання економічних наук*. 2024. № 6. DOI: https://doi.org/10.5281/zenodo.14575016
7. Разумова Г. В., Курносова О. І. Управління ризиками інвестиційної діяльності в умовах цифрової трансформації. *Бізнес Інформ*. 2024. № 3. С. 96–101. DOI: https://doi.org/10.32983/2222-4459-2024-3-96-101
8. Птащенко О., Крисоватий І., Федорович І. Фінансові ризики в агросфері: страхові стратегії та цифрові технології у контексті ефективного використання людського капіталу. *Світ фінансів*.

2025. № 4 (85). С. 162–175. URL: https://sf.wunu.edu.ua/index.php/sf/article/view/1886

9. Bagherifam N., Naghdi S., Ahmadian V., Fazlzadeh A., Baghalzadeh Shishehgarkhaneh M. Digital regulatory governance: the role of RegTech and SupTech in transforming financial oversight and administrative capacity. *International Journal of Financial Studies*. 2025. Vol. 13 (4). Art. 217. DOI: https://doi.org/10.3390/ijfs13040217
10. Mensah D. L. Machine learning based credit evaluation and risk control in digital finance platforms. *The American Journal of Engineering and Technology*. 2025. № 7 (11). С. 235–241. URL: https://www.theamericanjournals.com/index.php/tajet/article/view/7417
11. Ali Eyadat A., Alamaren A. S., Almomani S. L. The influence of blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks. *Frontiers in Blockchain*. 2025. Art. 1657110. DOI: https://doi.org/10.3389/fbloc.2025.1657110
12. Almadadha R. Blockchain technology in financial accounting: enhancing transparency, security, and ESG reporting. *Blockchains*. 2024. No. 2 (3). С. 312–333. DOI: https://doi.org/10.3390/blockchains2030015
13. Allianz Risk Barometer 2026. *Allianz Commercial*. 2026. URL: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
14. Bruno E., Pistolesi F., Teti E. Cybersecurity policy, ESG and operational risk: a virtuous relationship to improve banks' performance. *International Review of Financial Analysis*. 2025. Vol. 99. Art. 104053. DOI: https://doi.org/10.1016/j.iref.2025.104053
15. Zhao B. FinTech and risk management: exploring opportunities, challenges, and regulatory implications. *SHS Web of Conferences: International Conference on Financial Management and Digital Economy (ICFMDE 2025)*. 2025. Vol. 225. Art. 02024. DOI: https://doi.org/10.1051/shsconf/202522502024
16. Прокоф'єва О. В., Беспалова Ю. Ю. Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. *Ефективна економіка*. 2024. № 5. DOI: https://doi.org/10.32702/2307-2105.2024.5.87
17. Dong J. Study on the identification of financial risk path under the digital transformation of enterprise based on DEMATEL-ISM-MICMAC. 2023. *arXiv:2305.04216*. DOI: https://doi.org/10.48550/arXiv.2305.04216
18. Cao B., Wang S., Lin X., Wu X., Zhang H., Ni L. M., Guo J. From deep learning to LLMs: a survey of AI in quantitative investment. 2025. *arXiv:2503.21422*. DOI: https://doi.org/10.48550/arXiv.2503.21422
19. Paccagnini A., Iannario M., Osterrieder J., Perrotta A., Parla F., Skaftadottir. Editorial: applications of AI and machine learning in finance and economics. *Frontiers in Artificial Intelligence*. 2025. Vol. 8. Art. 1715929. DOI: https://doi.org/10.3389/frai.2025.1715929

REFERENCES

Abbas Anwar & Zeeshan Umer (2025). RegTech and FinTech convergence: leveraging artificial intelligence for transparent and secure financial ecosystems. *World Journal of Advanced Research and Reviews*, *3*(27), 1796–1808. https://doi.org/10.30574/wjarr.2025.27.3.3356

Ali Eyadat A., Alamaren A. S. & Almomani S. L. (2025). The influence of blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2025.1657110

Allianz Commercial. (2026). Allianz Risk Barometer 2026. https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Almadadha R. (2024). Blockchain technology in financial accounting: enhancing transparency, security, and ESG reporting. *Blockchains*, *2 (3)*, 312–333. https://doi.org/10.3390/blockchains2030015

Bagherifam N., Naghdi S., Ahmadian V., Fazlzadeh A. & Baghalzadeh Shishehgarkhaneh M. (2025). Digital regulatory governance: the role of RegTech and SupTech in transforming financial oversight and administrative capacity. *International Journal of Financial Studies*, *4*(13). https://doi.org/10.3390/ijfs13040217

Bruno E., Pistolesi F. & Teti E. (2025). Cybersecurity policy, ESG and operational risk: a virtuous relationship to improve banks' performance. *International Review of Financial Analysis*, 99. https://doi.org/10.1016/j.iref.2025.104053

Cao B., Wang S., Lin X., Wu X., Zhang H., Ni L. M. & Guo J. (2025). From deep learning to LLMs: a survey of AI in quantitative investment. *arXiv*. https://doi.org/10.48550/arXiv.2503.21422

Dong J. (2023). Study on the identification of financial risk path under the digital transformation of enterprise based on DEMATEL-ISM-MICMAC. *arXiv*. https://doi.org/10.48550/arXiv.2305.04216

Gu Z., Lv J., Wu B., Hu Z. & Yu X. (2024). Credit risk assessment of small and micro enterprise based on machine learning. *Heliyon*, *5*(10). https://doi.org/10.1016/j.heliyon.2024.e27096

Kulchytskyi I. I. (2024). Tsyfrova ekonomika ta ekonomichna bezpeka pidpryiemstva: stratehii upravlinnia [Digital economy and economic security of the enterprise: management strategies]. *Aktualni pytannia ekonomichnykh nauk*, *6*. https://doi.org/10.5281/zenodo.14575016

Lozić J. & Fotova Čiković K. Digital transformation: the fundamental concept of transformation of business activities. *107th International Scientific Conference on Economic and Social Development – Economic and Social Survival in Global Changes, Zagreb* (pp. 326–337).

Mensah D. L. (2025). Machine learning based credit evaluation and risk control in digital finance platforms. *The American Journal of Engineering and Technology*.

https://www.theamericanjournals.com/index.php/tajet/article/view/7417

Olaiya O. P., Adesoga T. O., Pieterson K., Obani O. Q., Adebayo J. O. & Ajayi O. O. (2024). RegTech solutions: enhancing compliance and risk management in the financial sector. *GSC Advanced Research and Reviews*, *2*(20), 8–15. https://doi.org/10.30574/gscarr.2024.20.2.0295

Paccagnini A., Iannario M., Osterrieder J., Perrotta A., Parla F. & Skaftadottir (2025). Editorial: applications of AI and machine learning in finance and economics. *Frontiers in Artificial Intelligence*, 8. https://doi.org/10.3389/frai.2025.1715929

Prokofieva O. V. & Bespalova Yu. Yu. (2024). Kiber-ryzyky ta upravlinnia nymy v umovakh hlobalizatsii ta tsyfrovoi transformatsii [Cyber risks and their management in the conditions of globalization and digital transformation]. *Efektyvna ekonomika*, *5*. https://doi.org/10.32702/2307-2105.2024.5.87

Ptashchenko O., Krysovatyi I. & Fedorovych I. (2025). Finansovi ryzyky v ahrosferi: strakhovi stratehii ta tsyfrovi tekhnolohii u konteksti efektyvnoho vykorystannia liudskoho kapitalu [Financial risks in the agricultural sphere: insurance strategies and digital technologies in the context of effective use of human capital]. *Svit finansiv*. https://sf.wunu.edu.ua/index.php/sf/article/view/1886

Razumova H. V. & Kurnosova O. I. (2024). Upravlinnia ryzykamy investytsiinoi diialnosti v umovakh tsyfrovoi transformatsii [Management of investment activity risks in the conditions of digital transformation]. *Biznes Inform*, *3*, 96–101. https://doi.org/10.32983/2222-4459-2024-3-96-101

Tanklevska N. S. & Miroshnychenko V. O. (2024). Finansova stiikist pidpryiemstv v umovakh tsyfrovoi ekonomiky [Financial stability of enterprises in the conditions of the digital economy]. *Biznes Inform*, *3*, 249–255. https://doi.org/10.32983/2222-4459-2024-3-249-255

Theodorakopoulos L., Theodoropoulou A. & Bakalis A. (2025). Big data in financial risk management: evidence, advances, and open questions: a systematic review. *Frontiers in Artificial Intelligence*, 8. https://doi.org/10.3389/frai.2025.1658375

Zhao B. (2025). FinTech and risk management: exploring opportunities, challenges, and regulatory implications. *SHS Web of Conferences: International Conference on Financial Management and Digital Economy (ICFMDE 2025)*. https://doi.org/10.1051/shsconf/202522502024

Дослідження не отримувало зовнішнього фінансування.
Автор заявляє про відсутність конфлікту інтересів.
Інструменти ШІ у підготовці цієї роботи не використовувалися.

Стаття надійшла до редакції / Received: 28.07.2026
Статтю прийнято до публікації / Accepted: 13.08.2026
Оприлюднено / Published: 08.10.2026