УДК 005.334:005.591.6:316.4
DOI: https://doi.org/10.32782/CMI/2026-20-10

Костін І.Д.
аспірант кафедри економіки підприємства та організації бізнесу,
Харківський національний економічний університет
імені Семена Кузнеця
ORCID: https://orcid.org/0009-0001-5111-808X

АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ РИЗИКІВ УПРОВАДЖЕННЯ СОЦІАЛЬНО ОРІЄНТОВАНИХ ЦИФРОВИХ ІННОВАЦІЙ У КОРПОРАТИВНОМУ СЕКТОРІ

У статті систематизовано підходи до моніторингу ризиків упровадження соціально орієнтованих цифрових інновацій у корпоративному секторі та обґрунтовано склад індикаторів, джерел даних і механізмів управлінського реагування. Методику побудовано як інтегративний аналітичний огляд рецензованих джерел 2021–2026 років із прозорою процедурою відбору та тематичним синтезом на основі матриці синтезу. Основним результатом є цілісний контур аналітичного забезпечення, що пов'язує контекст інновації, групу ризику, випереджальні й запізнілі індикатори, джерело даних, критерій ескалації та управлінську реакцію на операційному, управлінському й стратегічному рівнях, а також матриця моніторингу основних груп ризику. Практична значущість полягає в ранньому виявленні ризиків, інтеграції розрізнених показників у єдину систему та узгодженні цифрових інновацій із соціальними зобов'язаннями підприємства.

Ключові слова: *соціально орієнтовані цифрові інновації, корпоративний сектор, моніторинг ризиків, аналітичне забезпечення, корпоративний ризик-менеджмент, індикатори ризику, відповідальна інновація, соціальний вплив.*

Kostin Illia
Simon Kuznets Kharkiv National University of Economics

ANALYTICAL SUPPORT FOR MONITORING THE RISKS OF IMPLEMENTING SOCIALLY ORIENTED DIGITAL INNOVATIONS IN THE CORPORATE SECTOR

The rapid diffusion of digitally enabled products, processes and business models with a pronounced social effect for employees, consumers, partners and local communities has outpaced the development of coherent instruments for monitoring the risks that such innovations generate. In corporate practice these risks are still addressed in isolation: cybersecurity is treated separately from ethical consequences, environmental, social and governance considerations separately from operational risk management, and social outcomes separately from the metrics of digital transformation. As a result, a company may hold a set of disconnected control indicators yet lack an integrated analytical loop that links a risk to its indicator, data source, threshold, responsible function and management response. This article conceptualises analytical support for risk monitoring of socially oriented digital innovation and proposes a reproducible way of building it. The design is an integrative analytical review of peer-reviewed and normative sources published in 2021–2026, with an explicit search-and-selection procedure and a thematic synthesis organised around a synthesis matrix rather than a sequential summary of publications. The review advances a working definition that distinguishes digital innovation, digital transformation and socially oriented digital innovation through two criteria, the use of a digital technology as a mechanism of change and the presence of a measurable social effect for at least one stakeholder group. On this basis a corporate-oriented typology of risks is derived by mechanism of harm rather than by technology, and the interdependence of the risk groups is demonstrated. The central result is an integrated monitoring contour that connects six elements, the context of the innovation, the risk group, leading and lagging indicators, the data source, the evaluation criterion and the management response, and distributes them across three levels of control, operational for current signals, managerial for aggregated trends and strategic for alignment with corporate goals, social commitments and risk appetite. A risk-monitoring matrix operationalises the synthesis, and practical conditions for company-level implementation, including thresholds, ownership and integration with corporate information systems, are specified. The framework supports early detection, escalation and response, and provides a transparent basis for aligning digital innovation with the social obligations of the enterprise.

Keywords: *socially oriented digital innovation, corporate sector, risk monitoring, analytical support, enterprise risk management, risk indicators, responsible innovation, social impact.*

Постановка проблеми. Цифрові інновації дедалі частіше набувають вираженого соціального виміру. HR-аналітика, персоналізовані клієнтські сервіси, відповідальний штучний інтелект, цифрові інструменти безпеки праці та інклюзії змінюють не лише продукти й процеси компаній, а й безпосередньо впливають на працівників, споживачів, партнерів і локальні спільноти. Поєднання цифрової технології як механізму змін із вимірюваним соціальним ефектом для стейкхолдерів визначає окремий клас нововведень, який можна розглядати як соціально орієнтовані цифрові інновації. Розширення цифрової відповідальності підприємства за наслідки використання технологій і даних, зокрема ризики виключення користувачів і порушення приватності, обґрунтоване концепцією корпоративної цифрової відповідальності [1]. Водночас цифрова трансформація змінює профіль корпоративного ризику, посилюючи значення внутрішнього контролю й стра-

© Костін І.Д., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

тегічної узгодженості та зумовлюючи «парадокс цифровізації», за якого нарощування технологій без належного управління ризиками знижує результативність [2].

Соціальні наслідки цифрових інновацій дедалі тісніше переплітаються з екологічно-соціально-управлінським (далі – ESG) контуром, а отже, потребують не ізольованого, а інтегрованого ризик-менеджменту, що пов'язує соціальні ризики з операційними, фінансовими й репутаційними [3]. Проте на практиці ці виміри залишаються роз'єднаними. Кібербезпека відокремлена від етичних наслідків, ESG-підходи – від операційного ризик-менеджменту, а соціальні ефекти – від метрик цифрової трансформації. Через це компанія має набір розрізнених показників, але не має інтегрованого контуру, який пов'язував би ризик, індикатор, джерело даних, порогове значення, відповідального суб'єкта й управлінську реакцію. Наукова та практична проблема полягає у відсутності цілісного аналітичного забезпечення моніторингу ризиків саме для соціально орієнтованих цифрових інновацій у корпоративному секторі.

Аналіз останніх досліджень і публікацій. Теоретико-методологічну основу дослідження становлять концепція корпоративної цифрової відповідальності, підходи до корпоративного ризик-менеджменту та відповідального врядування штучного інтелекту. З огляду на це, наукові праці згруповано за чотирма взаємопов'язаними напрямами, аналіз яких дає змогу окреслити наукову прогалину. Перший напрям охоплює цифрові та соціально орієнтовані інновації. Зокрема, Л. Лобшат та співавтори обґрунтовують, що корпоративна цифрова відповідальність визначає цінності й норми, які спрямовують створення технологій і збір даних, їх використання та оцінювання впливу, і прямо фіксує ризик виключення користувачів [1]. Розвиваючи цю тезу, Б. Мюллер показує, що така відповідальність потребує операційного, а не декларативного втілення через управлінські структури й процеси [4], а П. Копалле та співавтори наголошують на залежності ефекту споживчих інновацій від локального регуляторного й культурного контексту, що ускладнює перенесення універсальних рішень [5]. Спільним для напряму є висновок про те, що соціальний вимір цифрових інновацій є вимірюваним, але досі слабко пов'язаним з інструментами контролю ризику.

Другий напрям продовжує цю логіку в площині корпоративного ризик-менеджменту в умовах цифровізації. Так, Н. Сюй та колеги емпірично показують, що цифрова трансформація впливає на результативність через стратегічну ефективність і внутрішній контроль, тобто через складники корпоративного ризик-менеджменту [2], а С. Шах та співавтори демонструють, що розширення предмета enterprise risk management на ESG-ризики дає змогу систематизовано оцінювати соціальні та управлінські ризики в межах єдиної рамки [3]. Водночас Р. Манн і Д. Мироненко зазначають, що управління ризиками інноваційного підприємства традиційно зосереджене на фінансово-виробничій сфері, а алгоритмічні, приватнісні та інклюзивні аспекти залишаються недостатньо охопленими [6]. Отже, наявні підходи до ризик-менеджменту загалом придатні для оцінювання корпоративних ризиків, проте недостатньо адаптовані до специфіки соціально орієнтованих цифрових інновацій, що обґрунтовує потребу в їх розширенні.

Третій напрям поглиблює попередній, зосереджуючись на відповідальній інновації, соціальному впливі та алгоритмічному врядуванні. Зокрема, М. Мустак та колеги фіксують, що організаційна неготовність і фрагментація важать не менше за технічні обмеження, а етичні питання й приватність даних стають самостійним джерелом ризику [7]. У цьому ж контексті С. Верма та співавтори наголошують на переході до гібридних моделей «людина + штучний інтелект» і керуванні етичними наслідками [8]. Далі Д. Хорнебер і С. Лаумер операціоналізують алгоритмічну підзвітність через відповідність вимогам, нагляд і забезпечення виконання, пов'язуючи технічний і управлінський погляди [9], а колектив авторів на чолі з К. Новеллі уточнює, хто, перед ким і за що відповідає [10]. Спільним висновком напряму є те, що принципи відповідальності сформульовано, однак їх недостатньо переведено в регулярні вимірювані процедури контролю.

Четвертий напрям безпосередньо стосується моніторингу цифрових та алгоритмічних ризиків, даних і приватності, тобто інструментального забезпечення, якому в попередніх напрямах приділено недостатньо уваги. Рамка управління ризиками штучного інтелекту NIST (Е. Табассі) описує безперервний цикл «врядування – картування – вимірювання – керування» й узгоджується з корпоративним ризик-менеджментом [11], а ризик-орієнтоване регулювання ЄС класифікує системи за рівнями ризику та задає правовий контекст порогів [12]. На цій основі С. Кобернюк та співавтори пропонують трирівневу систему метрик моніторингу з ієрархічною агрегацією показників, пороговими значеннями та джерелами даних [13]. Окремий аспект цієї проблематики С. Кобернюк розкриває через співвідношення між предиктивною цінністю даних та їх приватнісною вразливістю, визначаючи «персоналізаційний відтік» як індикатор ризику [14]. Цей підхід доповнюють А. Таранич і Д. Пелехацький, показуючи, що застосування штучного інтелекту у стратегічному управлінні розширює контур спостереження [15], І. Соснов і Є. Іпполітов, акцентуючи на кіберзагрозах і управлінні ризиками даних [16], а також І. Іванова та колеги, В. Бондаренко й О. Омельяненко, підкреслюючи залежність ефекту від якості інтеграції інструментів у бізнес-процеси [17; 18].

Узагальнення чотирьох напрямів засвідчує фрагментарність наявних підходів та недостатній зв'язок між ними. Соціальний вимір цифрових інновацій, корпоративний ризик-менеджмент, відповідальне врядування та моніторинг цифрових ризиків розглядаються переважно окремо, без єдиної системи їх аналітичного поєднання. У наявних дослідженнях недостатньо чітко визначено взаємозв'язок між групами ризиків, індикаторами, джерелами даних, пороговими значеннями, відповідальними суб'єктами та управлінськими реакціями на різних рівнях контролю. Це зумовлює необхідність формування цілісного аналітичного контуру для моніторингу ризиків соціально орієнтованих цифрових інновацій.

Формування цілей статті (постановка завдання). Метою статті є систематизація підходів до моніторингу ризиків упровадження соціально орієнтованих цифрових інновацій у корпоративному секторі та обґрунтування структури індикаторів, джерел даних і механізмів управлінського реагування.

Відповідно до мети сформульовано такі завдання: 1) уточнити понятійне поле дослідження та систематизувати сучасні підходи до моніторингу ризиків соціально орієнтованих цифрових інновацій; 2) сформувати типологію ризиків і визначити відповідні для них індикатори, джерела даних та критерії оцінювання; 3) побудувати інтегровану аналітичну модель моніторингу ризиків і визначити механізми управлінського реагування та умови її застосування на рівні підприємства.

Методичну основу дослідження становить інтегративний аналітичний огляд із прозорою процедурою пошуку, відбору та тематичного опрацювання джерел. Повний протокол і подвійний відбір не застосовувалися, тому дослідження не позиціонується як систематичний огляд. Основний пошук проведено в базах Scopus і Web of Science Core Collection, додатково використано Google Scholar і Crossref для перевірки цифрових ідентифікаторів. Нормативні матеріали залучалися лише для уточнення регуляторних, етичних і ризикових аспектів.

Пошукові запити формували з використанням термінів digital innovation, responsible innovation, social innovation, corporate digital transformation, social impact, ESG, enterprise risk management, risk monitoring, responsible AI, algorithmic governance, digital inclusion, data privacy та cybersecurity, а для національного сегмента доповнювали їх україномовними відповідниками. До огляду включали праці, присвячені цифровим інноваціям, соціальному ефекту або моніторингу ризиків у корпоративному секторі, а виключали суто технічні та виняткова публічно-секторні дослідження без можливості застосування їхніх висновків у корпоративному контексті. Відібрані джерела систематизовано в робочій матриці за параметрами авторства й року публікації, типу інновації, корпоративного контексту, групи ризику, показника, джерела даних, рівня аналізу, механізму контролю та обмежень. Матриця стала основою для тематичного аналізу й узагальнення результатів за окремими напрямами. З огляду на відсутність універсальних порогових значень їх доцільно визначати з урахуванням специфіки та ризик-профілю конкретного підприємства.

Виклад основного матеріалу дослідження. Побудова системи моніторингу ризиків потребує насамперед чіткого визначення того, які саме інновації є предметом аналізу. У дослідженні розмежовано поняття цифрової інновації, цифрової трансформації та соціально орієнтованої цифрової інновації. Цифрову інновацію розуміємо як використання цифрової технології для зміни продукту, процесу або бізнес-моделі, а цифрову трансформацію – як ширший організаційно-стратегічний процес перебудови діяльності. Соціально орієнтованою цифровою інновацією пропонуємо вважати цифрову інновацію, яка має дві основні ознаки, а саме: використовує цифрову технологію для зміни та забезпечує вимірюваний соціальний ефект принаймні для однієї групи стейкхолдерів. Таке визначення дає змогу відмежувати суто технологічні нововведення без соціального ефекту й водночас охопити персоналізовані сервіси, HR-аналітику, інструменти доступності та відповідальний штучний інтелект.

Визначення предмета дослідження дає змогу перейти до уточнення самого ризику та принципів його моніторингу. Ризик розглядаємо як можливість відхилення, що може мати негативні наслідки для компанії та/або її стейкхолдерів, а моніторинг – як регулярне зіставлення індикаторів із визначеними критеріями. Для соціально орієнтованих інновацій важливим є співвідношення між предиктивною цінністю даних та ризиками для приватності й довіри. Глибший профіль користувача розширює можливості персоналізації, але водночас підвищує ризик порушення приватності й втрати довіри [14]. Відповідно, врядування, безпеку й інклюзивність варто розглядати не як додаткові характеристики, а як умови, за яких розширення цифрових і комерційних можливостей не ототожнюється зі зрілістю всієї системи [1; 4].

Спираючись на наведені визначення, типологію доцільно будувати не за назвами технологій, а за механізмами потенційної шкоди та управлінськими наслідками. Це запобігає дублюванню категорій і робить типологію придатною для корпоративного моніторингу. Пропонуємо одинадцять взаємопов'язаних груп: стратегічні (невідповідність цілям і ризик-апетиту); операційні (збої, недоведені до впровадження рішення); фінансово-економічні (перевитрати, невизначеність окупності); правові та регуляторні (невідповідність вимогам, зокрема ризик-орієнтованій класифікації систем [12]); кібербезпекові (вразливості й атаки на дані та моделі [16]); ризики даних і приватності (надмірний збір, витік, повторне використання даних [1; 14]); алгоритмічні та етичні (зміщення рішень, непрозорість, дискримінація [9; 10]); кадрові (перевантаження, втрата компетенцій, спротив [7]); репутаційні (втрата довіри до практик роботи з даними й алгоритмами); цифрової нерівності та доступності (виключення користувачів [1]); ризики недосягнення заявленого соціального ефекту (розрив між декларованим і фактичним впливом).

Ризики взаємозалежні, а тому їх не можна контролювати ізольовано. Помилка алгоритмічного рішення здатна одночасно зумовити правовий, репутаційний, кадровий і фінансовий ризик; надмірний збір даних посилює приватнісний і кібербезпековий ризики; недосягнення соціального ефекту може посилювати репутаційні втрати. Саме ця взаємозалежність обґрунтовує єдиний контур, у межах якого для кожної групи визначають механізм виникнення, типові ранні сигнали, можливі наслідки та спосіб вимірювання. Це дає змогу перейти від переліку загроз до операціоналізованої системи, у якій алгоритмічні та приватнісні ризики вимірюються так само послідовно, як традиційні операційні чи фінансові [2; 3].

Для того щоб окреслені групи ризику стали керованими, потрібні вимірювані показники, тому аналітичний перехід від абстрактних ризиків ґрунтується на розмежуванні випереджальних (early-warning) і запізнілих індикаторів. Випереджальні фіксують ранні сигнали до настання шкоди, зокрема частоту збоїв і незавершених процесів (операційні); частку користувачів без доступу, індекс доступності та динаміку скарг (цифрова нерівність та доступність); цифрове навантаження й потребу в перенавчанні (кадрові); розрив показників між групами та частку рішень, переданих на ручний перегляд (алгоритмічні). Запізнілі відображають реалізований наслідок: час відновлення, обґрунтовані скарги, приписи регулятора, відтік клієнтів, штрафи, недосягнення соціальних цілей.

Джерела даних охоплюють внутрішні транзакційні системи, журнали подій платформ, HR-системи, CRM і служби підтримки, опитування працівників і клієнтів, комплаєнс-звіти, реєстри кіберінцидентів та аудити, а також зовнішні регуляторні й репутаційні дані. Для соціально орієнтованих інновацій особливого значення набувають зважений збір персональних даних із дотриманням згоди й мінімізації [14] та інтеграція показників довіри й доступності, які традиційно перебувають поза технічним моніторингом. Це зіставлення узагальнено в матриці моніторингу ризиків (табл. 1), що поєднує для кожної групи механізм прояву, випереджальний і запізнілий індикатори, джерело даних, критерій ескалації та реакцію. Для компактності споріднені класичні групи ризиків (стратегічні, операційні, фінансово-економічні, правові) об'єднано в один рядок, а специфічні для соціально орієнтованих інновацій ризики подано окремо.

Отже, матриця демонструє, що для кожної групи ризику можна визначити узгоджений ланцюжок «механізм – індикатори – джерело даних – критерій ескалації – реакція», а не окремі розрізнені показники. Це підтверджує можливість переведення різнорідних ризиків соціально орієнтованих інновацій у єдиний вимірюваний формат, придатний для регулярного моніторингу.

Узгоджене використання індикаторів і джерел даних можливе в межах цілісного контуру, що об'єднує шість послідовно пов'язаних елементів, зокрема контекст інновації, групу ризику, індикатори, джерела даних, оцінювання та управлінське реагування. Такий контур узгоджується з логікою «врядування – картування – вимірювання – керування» [11] і з поділом корпоративного ризик-менеджменту на стратегічну ефективність і внутрішній контроль [2], але конкретизує їх для соціально орієнтованих інновацій, додаючи соціальні індикатори, показники довіри й доступності. Він придатний не лише для опису ризику, а й для регулярного циклу контролю зі зворотним зв'язком від реагування до контексту та індикаторів.

У контурі доцільно виокремити три рівні моніторингу відповідно до рівня управління та часового горизонту рішень. Операційний рівень призначений для поточних сигналів та інцидентів (керівник підрозділу, день/тиждень); управлінський – для агрегованих тенденцій і відхилень (керівник напряму, тиждень/місяць); стратегічний – для оцінювання відповідності інновації корпоративним цілям, соціальним зобов'язанням і ризик-апетиту (вище керівництво, місяць/квартал). Поділ спирається на ієрархічну агрегацію, за якої дані нижчого рівня є вхідними для вищого [13], і на розширення контуру спостереження засобами штучного інтелекту в стратегічному управлінні [15]. Послідовність елементів контуру та трьох рівнів контролю узагальнено на рисунку 1.

Таблиця 1

Матриця моніторингу ризиків соціально орієнтованих цифрових інновацій

Група ризику	Механізм прояву	Індикатори (випереджальні / запізнілі)	Джерело даних	Критерій ескалації та реакція
Алгоритмічні та етичні	Систематичне зміщення рішень моделі щодо груп стейкхолдерів	Розрив показників між групами, частка рішень на ручний перегляд / обґрунтовані скарги, випадки дискримінації	Логи моделі; журнали рішень; аудит	Перевищення порогу розриву – донавчання моделі, посилення людського контролю
Дані та приватність	Надмірний збір, витік чи повторне використання персональних даних	Частка обробки без згоди, аномалії доступу / інциденти витоку, приписи регулятора	DPIA; журнали доступу; комплаєнс-звіти	Порушення політики згоди чи мінімізації – посилення захисту, звуження збору
Кібербезпекові	Уразливості сервісу; атаки на дані й моделі	Частота вразливостей, спроби вторгнення / час відновлення, збитки від інцидентів	Журнали подій; звіти CSIRT	Критичний інцидент – реагування на інцидент, сегментація доступу
Кадрові	Цифрове перевантаження, втрата компетенцій, спротив	Цифрове навантаження, звернення щодо інструментів / плинність, потреба перенавчання	HR-системи; опитування; служба підтримки	Стійке зростання навантаження чи плинності – перенавчання, перегляд процесів
Репутаційні	Недовіра до практик роботи з даними й алгоритмами	Тональність згадок, частка негативних відгуків / відтік клієнтів, медіакризи	Соцмоніторинг; CRM; опитування довіри	Різке падіння індексу довіри – комунікація, коригування практик
Цифрова нерівність і доступність	Виключення частини користувачів із сервісу	Частка користувачів без доступу, індекс доступності/ скарги, відтік уразливих груп	Журнали платформ; аудит доступності	Зниження доступності нижче норми – редизайн сервісу, альтернативні канали
Недосягнення соціального ефекту	Заявлений ефект не підтверджується фактом	Розрив «план–факт» соціальних метрик / відсутність задекларованого впливу	Моніторинг соціальних KPI; звітність	Стійке відхилення від цілі – перегляд дизайну й цілей ініціативи
Стратегічні, операційні, фінансово-економічні, правові	Збої, невідповідність цілям, витрати, регуляторна невизначеність	Частота збоїв, відхилення від бюджету чи стратегії / час відновлення, штрафи	Транзакційні системи; фінзвіти; реєстр вимог	Перевищення допустимих меж – корекція процесу, аудит, призупинення функціоналу

Джерело: авторська розробка

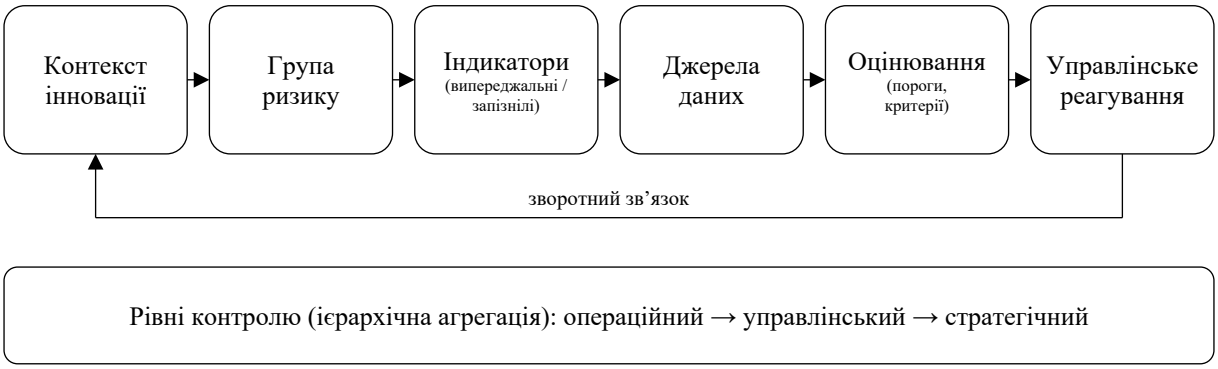

Рис. 1. Контур аналітичного забезпечення моніторингу ризиків соціально орієнтованих цифрових інновацій

Джерело: авторська розробка

Як видно з рисунка, контур утворює замкнений цикл, у якому елементи послідовно пов'язані, а зворотний зв'язок від управлінського реагування дає змогу уточнювати контекст, індикатори й пороги. Розподіл контуру на операційний, управлінський і стратегічний рівні забезпечує узгодженість поточного реагування з тактичними тенденціями та стратегічними цілями підприємства. У такий спосіб розрізнене спостереження перетворюється на інтегроване управління ризиками.

Критично важливим є перехід від даних до рішення. Для кожного значущого індикатора визначають періодичність спостереження, спосіб нормування, критерій ескалації, відповідальну функцію та тип реакції, зокрема корекцію процесу, аудит, навчання персоналу, перегляд чи донавчання алгоритму, посилення захисту даних, зміну дизайну сервісу або призупинення функціоналу. Нормування доцільно виконувати за фіксованими реперами (наприклад, $z = (x - L) / (U - L)$, де L і U – нижня та верхня межі), що забезпечує часову порівнянність і придатність до агрегації [13]. За відсутності універсальних порогів їх встановлюють на рівні компанії з урахуванням її ризик-апетиту, галузевої специфіки й регуляторного середовища. Практична реалізація передбачає інтеграцію показників у наявні системи (CRM, BI), закріплення відповідальних функцій та забезпечення алгоритмічної підзвітності через відповідність вимогам, нагляд і забезпечення виконання [9; 10], прозорість за замовчуванням у роботі з даними стейкхолдерів [14] і якісну інтеграцію інструментів у бізнес-процеси [17; 18]. Контур не замінює галузевих стандартів і технічних бенчмарків, а узгоджує їх у єдину систему раннього попередження й реагування.

Висновки. Фрагментація підходів до моніторингу ризиків пов'язана з багатовимірністю соціально орієнтованих цифрових інновацій, які мають технологічні, соціальні, організаційні та регуляторні наслідки. Уточнено понятійне поле та визначено соціально орієнтовану цифрову інновацію як таку, що поєднує використання цифрової технології для зміни продукту, процесу або бізнес-моделі з вимірюваним соціальним ефектом для стейкхолдерів. На цій основі виокремлено одинадцять взаємопов'язаних груп ризиків, розмежованих за механізмами потенційної шкоди та управлінськими наслідками.

Для визначених груп ризиків систематизовано випереджальні й запізнілі індикатори та джерела даних, які об'єднано в матрицю моніторингу. Її використання дало змогу побудувати інтегровану аналітичну модель у формі контуру, що поєднує контекст інновації, групу ризику, індикатори, джерела даних, оцінювання та управлінське реагування. Контур охоплює три рівні контролю – операційний, управлінський і стратегічний – та забезпечує послідовний перехід від фіксації сигналу до відповідної управлінської реакції.

Практичне застосування моделі передбачає нормування показників за фіксованими реперами, встановлення порогів з урахуванням ризик-апетиту, галузевої специфіки й регуляторного середовища, інтеграцію даних у корпоративні інформаційні системи та закріплення відповідальності за реагування. Наукова новизна полягає в поєднанні соціального виміру цифрових інновацій із корпоративним моніторингом ризиків у єдиному аналітичному контурі, що дає змогу одночасно враховувати кібербезпекові, фінансові, алгоритмічні, приватнісні, кадрові, інклюзивні та репутаційні ризики. Практична цінність запропонованого підходу полягає у створенні основи для раннього виявлення ризиків і узгодження цифрових інновацій із соціальними зобов'язаннями підприємства. Подальші дослідження доцільно спрямувати на емпіричну апробацію моделі, розроблення галузевих порогів і профілів індикаторів та її інтеграцію з інструментами предиктивної аналітики.

СПИСОК ЛІТЕРАТУРИ

1. Corporate digital responsibility / L. Lobschat et al. *Journal of Business Research.* 2021. Vol. 122. P. 875–888. DOI: https://doi.org/10.1016/j.jbusres.2019.10.006

2. Xu N., Lv W., Wang J. The impact of digital transformation on firm performance: a perspective from enterprise risk management. *Eurasian Business Review.* 2024. Vol. 14. P. 369–400. DOI: https://doi.org/10.1007/s40821-024-00264-9

3. Shah S. Q. A., Lai F.-W., Shad M. K., Hamad S., Ellili N. O. D. Exploring the effect of enterprise risk management for ESG risks towards green growth. *International Journal of Productivity and Performance Management.* 2024. Vol. 74, № 1. DOI: https://doi.org/10.1108/IJPPM-10-2023-0582

4. Mueller B. Corporate digital responsibility. *Business & Information Systems Engineering.* 2022. Vol. 64. P. 689–700. DOI: https://doi.org/10.1007/s12599-022-00760-0

5. Examining artificial intelligence (AI) technologies in marketing via a global lens: current trends and future research opportunities / P. K. Kopalle et al. *International Journal of Research in Marketing.* 2022. Vol. 39, № 2. P. 522–540. DOI: https://doi.org/10.1016/j.ijresmar.2021.11.002

6. Манн Р. В., Мироненко Д. Ю. Управління ризикостійкістю інноваційного підприємства. *Управління змінами та інновації.* 2023. № 5. С. 69–73. DOI: https://doi.org/10.32782/CMI/2023-5-12

7. Mustak M., Salminen J., Plé L., Wirtz J. Artificial intelligence in marketing: topic modeling, scientometric analysis, and research agenda. *Journal of Business Research.* 2021. Vol. 124. P. 389–404. DOI: https://doi.org/10.1016/j.jbusres.2020.10.044

8. Verma S., Sharma R., Deb S., Maitra D. Artificial intelligence in marketing: systematic review and future research direction. *International Journal of Information Management Data Insights.* 2021. Vol. 1, № 1. Art. 100002. DOI: https://doi.org/10.1016/j.jjimei.2020.100002

9. Horneber D., Laumer S. Algorithmic accountability. *Business & Information Systems Engineering.* 2023. Vol. 65. P. 723–730. DOI: https://doi.org/10.1007/s12599-023-00817-8

10. Novelli C., Taddeo M., Floridi L. Accountability in artificial intelligence: what it is and how it works. *AI & Society.* 2024. Vol. 39. P. 1871–1882. DOI: https://doi.org/10.1007/s00146-023-01635-y

11. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0) : NIST AI 100-1. Gaithersburg : National Institute of Standards and Technology, 2023. DOI: https://doi.org/10.6028/NIST.AI.100-1

12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *Regulations.ai.* URL: https://regulations.ai/regulations/RAI-EU-NA-E2AIXXX-2024 (дата звернення: 18.08.2026).

13. Кобернюк С. О., Ільченко Т. В., Якубенко Ю. Л. Методичні підходи до побудови комплексної системи метрик моніторингу впровадження та ефективності інструментів штучного інтелекту в маркетингу. *Ефективна економіка.* 2026. № 3. DOI: https://doi.org/10.32702/2307-2105.2026.3.105

14. Кобернюк С. О. Цифровий портрет та персоналізація комунікації з сучасним споживачем. *International Security Studies: managerial, technical, legal, environmental, informational, economic and psychological aspects : international collective monograph.* Vol. II. Lublin : ISAP, 2026. С. 106–142. DOI: https://doi.org/10.5281/zenodo.19385630

15. Таранич А. В., Пелехацький Д. О. Використання штучного інтелекту в процесах стратегічного управління підприємствами. *Економіка України.* 2024. Т. 67, № 1 (746). С. 54–65. DOI: https://doi.org/10.15407/economyukr.2024.01.054

16. Соснов І. І., Іпполітов Є. М. Стратегічне забезпечення інформаційної безпеки підприємства. *Підприємництво і торгівля.* 2025. № 47. С. 141–149. DOI: https://doi.org/10.32782/2522-1256-2025-47-16

17. Іванова І. В., Боровик Т. М., Залозна Т. Г., Руденко А. Ю. Використання штучного інтелекту в маркетингу. *Маркетинг і цифрові технології.* 2023. Т. 7, № 2. С. 32–42. DOI: https://doi.org/10.15276/mdt.7.2.2023.3

18. Бондаренко В., Омельяненко О. Вплив штучного інтелекту (AI) на розвиток інтернет-маркетингу. *Вісник Хмельницького національного університету. Серія: Економічні науки.* 2024. Т. 334, № 5. С. 319–324. DOI: https://doi.org/10.31891/2307-5740-2024-334-47

REFERENCES

1. Lobschat L., Mueller B., Eggers F., Brandimarte L., Diefenbach S., Kroschke M. & Wirtz J. (2021) Corporate digital responsibility. *Journal of Business Research,* vol. 122, pp. 875–888. DOI: https://doi.org/10.1016/j.jbusres.2019.10.006

2. Xu N., Lv W. & Wang J. (2024) The impact of digital transformation on firm performance: A perspective from enterprise risk management. *Eurasian Business Review,* vol. 14, pp. 369–400. https://doi.org/10.1007/s40821-024-00264-9

3. Shah S. Q. A., Lai F. W., Shad M. K., Hamad S. & Ellili N. O. D. (2024) Exploring the effect of enterprise risk management for ESG risks towards green growth. *International Journal of Productivity and Performance Management,* vol. 74, no. 1. DOI: https://doi.org/10.1108/IJPPM-10-2023-0582

4. Mueller B. (2022) Corporate digital responsibility. *Business & Information Systems Engineering*, vol. 64, pp. 689–700. DOI: https://doi.org/10.1007/s12599-022-00760-0

5. Kopalle P. K., Gangwar M., Kaplan A., Ramachandran D., Reinartz W. & Rindfleisch A. (2022) Examining artificial intelligence (AI) technologies in marketing via a global lens: Current trends and future research opportunities. *International Journal of Research in Marketing,* vol. 39, no. 2, pp. 522–540. DOI: https://doi.org/10.1016/j.ijresmar.2021.11.002

6. Mann R. V. & Myronenko D. Yu. (2023) Upravlinnia ryzykostiikistiu innovatsiinoho pidpryiemstva [Management of risk resilience of an innovative enterprise]. *Upravlinnia zminamy ta innovatsii,* no. 5, pp. 69–73. DOI: https://doi.org/10.32782/CMI/2023-5-12 (in Ukrainian)

7. Mustak M., Salminen J., Plé L. & Wirtz J. (2021) Artificial intelligence in marketing: Topic modeling, scientometric analysis, and research agenda. *Journal of Business Research,* vol. 124, pp. 389–404. DOI: https://doi.org/10.1016/j.jbusres.2020.10.044

8. Verma S., Sharma R., Deb S. & Maitra D. (2021) Artificial intelligence in marketing: Systematic review and future research direction. *International Journal of Information Management Data Insights,* vol. 1, no. 1, art. 100002. DOI: https://doi.org/10.1016/j.jjimei.2020.100002

9. Horneber D. & Laumer S. (2023) Algorithmic accountability. *Business & Information Systems Engineering,* vol. 65, pp. 723–730. DOI: https://doi.org/10.1007/s12599-023-00817-8

10. Novelli C., Taddeo M. & Floridi L. (2024) Accountability in artificial intelligence: What it is and how it works. *AI & Society,* vol. 39, pp. 1871–1882. DOI: https://doi.org/10.1007/s00146-023-01635-y

11. Tabassi E. (2023) Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.AI.100-1

12. Regulations.ai. (2024) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available at: https://regulations.ai/regulations/RAI-EU-NA-E2AIXXX-2024 (accessed August 18, 2026).

13. Koberniuk S. O., Ilchenko T. V. & Yakubenko Yu. L. (2026) Metodychni pidkhody do pobudovy kompleksnoi systemy metryk monitorynhu vprovadzhennia ta efektyvnosti instrumentiv shtuchnoho intelektu v marketynhu [Methodological approaches to building

a comprehensive metrics system for monitoring the implementation and effectiveness of artificial intelligence tools in marketing]. *Efektyvna ekonomika* no. 3. DOI: https://doi.org/10.32702/2307-2105.2026.3.105 (in Ukrainian)

14. Koberniuk S. O. (2026) Tsyfrovyi portret ta personalizatsiia komunikatsii z suchasnym spozhyvachem [Digital portrait and personalisation of communication with the modern consumer]. In: *International Security Studies: managerial, technical, legal, environmental, informational, economic and psychological aspects: international collective monograph,* vol. II, pp. 106–142. Lublin: ISAP. DOI: https://doi.org/10.5281/zenodo.19385630 (in Ukrainian)
15. Taranych A. V. & Pelekhatskyi D. O. (2024) Vykorystannia shtuchnoho intelektu v protsesakh stratehichnoho upravlinnia pidpryiemstvamy [Use of artificial intelligence in strategic management of enterprises]. *Ekonomika Ukrainy,* vol. 67, no. 1(746), pp. 54–65. DOI: https://doi.org/10.15407/economyukr.2024.01.054 (in Ukrainian)
16. Sosnov I. I. & Ippolitov Ye. M. (2025) Stratehichne zabezpechennia informatsiinoi bezpeky pidpryiemstva [Strategic ensuring of enterprise information security]. *Pidpryiemnytstvo i torhivlia,* no. 47, pp. 141–149. DOI: https://doi.org/10.32782/2522-1256-2025-47-16 (in Ukrainian)
17. Ivanova I. V., Borovyk T. M., Zalozna T. H. & Rudenko A. Yu. (2023) Vykorystannia shtuchnoho intelektu v marketynhu [The use of artificial intelligence in marketing]. *Marketynh i tsyfrovi tekhnolohii,* vol. 7, no. 2, pp. 32–42. DOI: https://doi.org/10.15276/mdt.7.2.2023.3 (in Ukrainian)
18. Bondarenko V. & Omelianenko O. (2024) Vplyv shtuchnoho intelektu (AI) na rozvytok internet-marketynhu [The impact of artificial intelligence (AI) on the development of internet marketing]. *Visnyk Khmelnytskoho natsionalnoho universytetu. Seriia: Ekonomichni nauky*, vol. 334, no. 5, pp. 319–324. DOI: https://doi.org/10.31891/2307-5740-2024-334-47 (in Ukrainian)

Дата надходження статті: 02.09.2026
Дата прийняття статті до публікації: 15.10.2026
Дата публікації статті: 24.11.2026