INDEX COPERNICUS INTERNATIONAL

№70
MAY, 2026

ISSN 2710-3056

The issue of journal contains:

Proceedings of the XI Correspondence International Scientific and Practical Conference

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

to be held on June 12th, 2026 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

GRAIL OF SCIENCE
PERIODICAL SCIENTIFIC JOURNAL

ISSN 2710–3056

INTERNATIONAL SCIENTIFIC JOURNAL

GRAIL OF SCIENCE

№ 70 (May 2026)

featuring papers to be presented at the:

XI Correspondence International Scientific and Practical Conference

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

to be held on June 12th, 2026 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

МІЖНАРОДНИЙ НАУКОВИЙ ЖУРНАЛ

ГРААЛЬ НАУКИ

№ 70 (травень, 2026)

із працями, що будуть представлені на:

XI Міжнародної науково-практичної конференції

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

що відбудеться 12.06.2026

ГО «Європейська наукова платформа» (Вінниця, Україна)
ТОВ «International Centre Corporative Management» (Відень, Австрія)

Вінниця – Відень, 2026

DOI 10.36074/grail-of-science.31.05.2026

ГРААЛЬ НАУКИ : міжнар. наук. журнал. – Вінниця : ГО «Європейська наукова платформа»; НУ «Інститут науково-технічної інтеграції та співпраці», 2026. – No 70. – 990 с.

Видання розраховане на науковців, викладачів, аспірантів, студентів, усіх, хто прагне отримати ґрунтовні знання теоретичного і прикладного характеру.

Рекомендовано до видання Вченою Радою Наукової установи «Інститут науково-технічної інтеграції та співпраці». Протокол № 21 від 30.05.2026.

Верстальник: *Білоус Тетяна (Україна).* ***Дизайнер:*** *Казьміна Надія (Україна).* ***Коректор:*** *Дудник Григорій (Україна).*

«Грааль науки» є офіційно зареєстрованим мультидисциплінарним науковим виданням з міжнародною сферою поширення, що підтримує політику відкритого доступу. **Ідентифікатор медіа R30-02704** (рішення № 430 від 22.02.2024 Національної Ради України з питань телебачення і радіомовлення).

Наказом МОН України № 582 від 24.04.2024 виданню «Грааль науки» присвоєно Категорію Б фахових видань України з питань економіки (051 «Економіка»).

«Грааль науки» індексується в міжнародних реферативних та наукометричних базах даних:
Index Copernicus Journals Master List; «Наукова періодика України» (Національна бібліотека України імені В.І. Вернадського НАН України); Національний репозитарій академічних текстів; Google Scholar; WorldCat; Open Ukrainian Citation Index; CrossRef; Mendeley; Scite; Semantic Scholar; Scilit; OpenAIRE, PubPeer.

Конференція зареєстрована УкрІНТЕІ (Посвідчення № 88 від 26.01.2026) та сертифікована Euro Science Certification Group (Сертифікат № 23312 від 28.04.2026).

За точність викладених фактів та правильність цитування відповідальність несе автор.

DOI 10.36074/grail-of-science.31.05.2026

GRAIL OF SCIENCE : inter. scientific journal. – Vinnytsia : NGO «European Scientific Platform»; SI «Institute of Scientific and Technical Integration and Cooperation», 2026. – No 70. – 990 p.

The publication is intended for scientists, teachers, graduate students, students, all those who seek to obtain thorough knowledge of a theoretical and applied nature.

Recommended for publication by the Academic Council of the Institute of Scientific and Technical Integration and Cooperation. Protocol № 21 from May 30, 2026.

Responsible for e-layout: *Tetiana Bilous (Ukraine).* ***Designer:*** *Nadiia Kazmina (Ukraine).* ***Proofreader:*** *Hryhorii Dudnyk (Ukraine).*

The journal «Grail of Science» is an officially registered in Ukraine multidisciplinary and internationally disseminated scientific edition that supports the policy of open access for scientific publications. **Media identifier R30-02704** (decision № 430 dated 22.02.2024 of the National Council of Ukraine on Television and Radio Broadcasting).

By order of the Ministry of Education and Culture of Ukraine № 582 of April 24, 2024, the journal «Grail of Science» was assigned Category B of specialized publications of Ukraine on economics (051 «Economics»).

The journal «Grail of Science» is indexed in international reference and scientometric databases:
Index Copernicus Journals Master List; «Наукова періодика України» (Національна бібліотека України імені В.І. Вернадського НАН України); Національний репозитарій академічних текстів; Google Scholar; WorldCat; Open Ukrainian Citation Index; CrossRef; Mendeley; Scite; Semantic Scholar; Scilit; OpenAIRE, PubPeer.

The conference is approved by UKRISTEI (Certificate № 88 dated January 26th, 2026) and certified by Euro Science Certification Group (Certificate № 23314 dated April 28th, 2026).

The author is responsible for the accuracy of the facts presented and the correctness of citations.

ЗМІСТ

РОЗДІЛ І.
ЗАГАЛЬНА ЕКОНОМІЧНА ТЕОРІЯ (Категорія Б)

РОЗДІЛ ІІ.
ПОВЕДІНКОВА ЕКОНОМІКА (Категорія Б)

РОЗДІЛ ІІІ.
ІННОВАЦІЙНА ЕКОНОМІКА (Категорія Б)

РОЗДІЛ IV.
ЦИФРОВА ЕКОНОМІКА, МАТЕМАТИЧНІ І ІНСТРУМЕНТАЛЬНІ МЕТОДИ ЕКОНОМІКИ (Категорія Б)

ISSN 2710–3056 | Категорія Б (Наказ МОН України № 582 від 24.04.2024)
DOI 10.36074/grail-of-science.31.05.2026.035

УПРАВЛІННЯ БІЗНЕС-РИЗИКАМИ В ЦИФРОВІЙ ЕКОНОМІЦІ: КАСКАДНИЙ ХАРАКТЕР ЗАГРОЗ ТА АЛГОРИТМ ДЛЯ ПІДПРИЄМСТВ РІЗНОГО МАСШТАБУ

Марущак Світлана Миколаївна
кандидат економічних наук, доцент,
доцент кафедри економіки та цифрового бізнесу
Національний університет кораблебудування імені адмірала Макарова, Україна

Анотація. *Цифрова трансформація формує якісно новий ризиковий ландшафт, що виходить за межі класичного Enterprise Risk Management. У статті запропоновано дев'ятигрупову класифікацію бізнес-ризиків цифрової економіки, структуровану у два блоки – зовнішні та внутрішні ризики. Виокремлення внутрішніх ризиків (поведінкових, компетентнісних, залежності) як метаризиків – ендогенних підсилювачів зовнішніх загроз, є авторським внеском. Каскадний характер цифрових загроз обґрунтовано через конвергенцію трьох наукових традицій та верифіковано на прецедентах SolarWinds (2020) і CrowdStrike (2024). Розроблено scoring framework оцінювання зрілості ризик-менеджменту та диференційований алгоритм для підприємств різного масштабу.*
Ключові слова: *цифрові ризики, ризик-менеджмент, каскадний ефект, метаризики, scoring framework, кібербезпека, ERM, цифрова економіка, МСБ.*

Постановка проблеми. Цифрова трансформація докорінно змінює умови функціонування підприємств, породжуючи якісно нові класи загроз, які не мають аналогів у традиційній господарській діяльності. За даними Allianz Risk Barometer 2026, кіберінциденти залишаються найбільшим глобальним ризиком для бізнесу п'ятий рік поспіль – з відривом від наступного ризику у 10 відсоткових пунктів. [22]. Водночас традиційні концепції управління ризиками – зокрема COSO ERM 2017 та ISO 31000:2018 – розроблялися до сучасного етапу масштабної цифрової трансформації і не передбачають ані каскадного характеру цифрових загроз, ані специфіки внутрішніх організаційних чинників, що підсилюють зовнішні ризики [4; 6].

Практична гострота проблеми підтверджується масштабом реалізованих цифрових ризиків. Інцидент CrowdStrike у липні 2024 р. спричинив збій 8,5 млн пристроїв [20]; за оцінкою страхової компанії Parametrix, лише 500 найбільших американських компаній (за винятком Microsoft) зазнали прямих збитків на суму близько 5,4 млрд дол. США, значна частина яких не покривалася кіберстрахуванням [23]. Це явище принципово недостатньо враховане класичними ERM-моделями. Для України проблема набуває додаткової гостроти: вітчизняний бізнес проходить цифрову трансформацію в умовах

повномасштабного збройного вторгнення, яке надає кіберзагрозам геополітичного виміру [12].

Аналіз останніх досліджень і публікацій. Наукова спільнота активно досліджує проблематику управління ризиками в умовах цифровізації, однак більшість публікацій охоплює лише окремі виміри цієї трансформації. Jazairy et al. (2024) верифікували каскадний характер кіберризиків у цифрових ланцюгах постачання, показавши, що атака на одного учасника здатна безпосередньо або опосередковано вражати пов'язаних партнерів у спосіб, що потребує адаптації класичного ERM [11]. Afifi et al. (2026) у систематичному огляді 175 праць підтвердили, що управління каскадними кіберризиками трансформується із суто технічної функції у стратегічний управлінський імператив [10]. Zhu et al. (2026) довели, що каскадні відмови є визначальною характеристикою цифрових ланцюгів постачання і принципово відрізняються від традиційних ризиків швидкістю поширення та транскордонним масштабом [18].

Серед вітчизняних дослідників Прокоф'єва та Беспалова (2024) підтверджують подвійну природу кіберзагроз – загальноцифрову та специфічно воєнну [12]. Захаркін та ін. (2023) систематизували цифрові інструменти забезпечення фінансової безпеки бізнесу [13]. Sotamaa et al. (2025) підтвердили, що МСБ в умовах цифровізації потребує адаптованого алгоритму управління ризиками [15].

Виділення невирішених раніше частин загальної проблеми. Попри значний масив публікацій, залишаються невирішеними три ключові проблеми: відсутня класифікація, що одночасно охоплює зовнішні та внутрішні цифрові ризики підприємства; внутрішні організаційні чинники системно не розглядаються як підсилювачі зовнішніх загроз; бракує практичного диференційованого інструментарію, адаптованого до масштабу підприємства.

Мета дослідження. Метою даного дослідження є розроблення комплексної системи управління бізнес-ризиками цифрової економіки, що охоплює: (1) дев'ятигрупову класифікацію цифрових ризиків підприємства з виокремленням внутрішніх метаризиків; (2) теоретичне обґрунтування каскадного характеру цифрових загроз та його верифікацію на документованих прецедентах; (3) scoring framework оцінювання зрілості ризик-менеджменту; (4) диференційований алгоритм управління для підприємств різного масштабу.

Наукова новизна дослідження полягає у: (1) введенні концепту «метаризиків» як ендогенних підсилювачів зовнішніх цифрових загроз та розробленні двоблокової класифікації бізнес-ризиків цифрової економіки; (2) теоретичному обґрунтуванні каскадного характеру цифрових загроз через конвергенцію теорії системних аварій, мережевої теорії системного ризику та досліджень каскадних збоїв у цифрових ланцюгах постачання; (3) адаптації scoring framework оцінювання зрілості ризик-менеджменту до специфіки цифрових загроз. Практичну цінність має диференційований п'ятикроковий алгоритм управління цифровими ризиками для підприємств малого, середнього та великого масштабу.

Виклад основного матеріалу. Досліджуючи еволюцію концепцій ризик-менеджменту, можна виокремити п'ять етапів, кожен із яких формувався як реакція на обмеження попереднього (рис. 1).

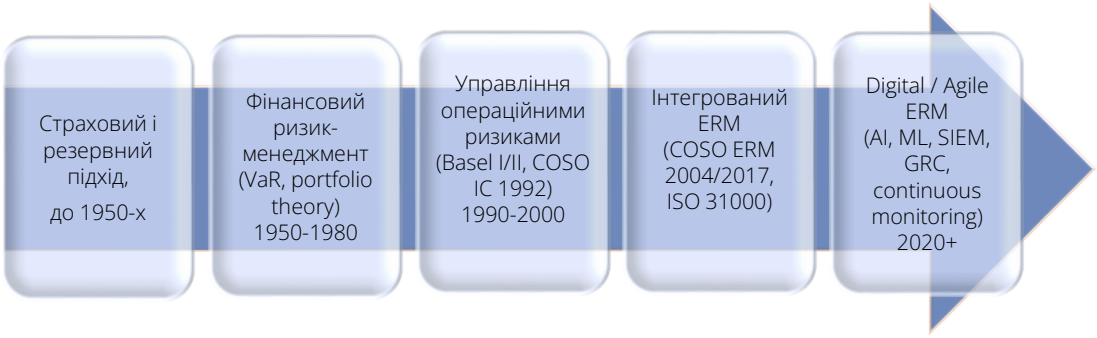

Рис. 1. Еволюція підходів до управління бізнес-ризиками в цифровій економіці
Джерело: авторська розробка на основі [1-7]

До 1950-х рр. домінував страховий і резервний підхід: основними інструментами були страхування майна та резервні фонди. Найт (1921) обґрунтував, що страхуванню піддаються лише кількісно вимірювані ризики, тоді як фундаментальна невизначеність не може бути повністю формалізована [1]. У 1950-1980-х рр. ризик-менеджмент набув кількісної складової завдяки портфельній теорії Марковіца, моделі CAPM та інструментам хеджування, проте у фокусі залишалися переважно фінансові ризики [2]. Корпоративні скандали 1990-х рр. (Enron, WorldCom, Barings Bank) та посилення регулювання (Basel I, COSO 1992, Закон Сарбейнса-Окслі) стимулювали розвиток операційного ризик-менеджменту, проте підходи залишалися ретроспективними та силосними [3; 4; 5]. Концепція інтегрованого ERM (COSO 2004/2017, ISO 31000:2018) охопила всі класи ризиків і формалізувала роль CRO [3; 4]. Проте на сучасному етапі цифрової трансформації традиційні ERM-підходи потребують адаптації до нових реалій – кіберзагроз, платформної залежності, AI-систем [6; 7].

ISO/TS 31050:2023 та NIST CSF 2.0 (2024) акцентують на необхідності адаптації традиційних підходів до зростання цифрових загроз [8; 9]. Цифрова трансформація породжує принципово нові класи ризиків, які вирізняються високою швидкістю поширення, міжорганізаційним характером та складністю кількісного вимірювання. Зростаюча взаємозалежність організацій у цифрових ланцюгах постачання зумовлює каскадне поширення кіберзагроз, що потребує системної класифікації (табл. 1).

Таблиця 1

Класифікація бізнес-ризиків цифрової економіки

Група ризиків	Характеристика	Типові прояви
I. Зовнішні цифрові ризики – загрози, що формуються поза підприємством		
Кіберризики	Несанкціонований доступ, злам або знищення цифрових активів	DDoS-атаки, ransomware, витоки даних, соціальна інженерія
Платформні	Залежність від цифрових екосистем та хмарних провайдерів	Vendor lock-in, збої SaaS-сервісів, каскадні відмови постачальників
Ризики даних	Порушення конфіденційності, цілісності та доступності даних	Витоки персональних даних, маніпуляції з даними, низька якість датасетів

Продовження табл. 1

Група ризиків	Характеристика	Типові прояви
Регуляторні	Невідповідність мінливому цифровому законодавству	Санкції GDPR, вимоги AI Act 2024/1689; для України – ЄС-гармонізація
Операційні	Збої автоматизованих процесів та цифрової інфраструктури	Помилки алгоритмів, відмова цифрових сервісів, вразливості хмари
Стратегічні	Довгострокові загрози конкурентним позиціям та репутації підприємства	Цифрова дезрупція бізнес-моделі, репутаційні кризи, упередженість ШІ
II. Внутрішні цифрові ризики – ендогенні чинники, що знижують ефективність управління зовнішніми загрозами		
Поведінкові	Систематичні когнітивні упередження осіб, що приймають рішення в умовах цифрової невизначеності	Overconfidence, ефект статус-кво, confirmation bias при оцінці загроз
Компетентнісні	Дефіцит цифрових знань, навичок та організаційної спроможності	Цифрова неграмотність менеджменту, брак фахівців з IT-безпеки
Залежності	Втрата стійкості внаслідок повної переорієнтації на цифрові системи без резервних механізмів	Неможливість функціонування при збої, відсутність аналогових резервних процедур

Джерело: авторська розробка на основі [1; 3; 4; 7-9; 11-14]

Запропонована класифікація охоплює дев'ять груп, структурованих у два блоки за критерієм джерела виникнення. До першого блоку віднесено шість груп зовнішніх загроз, до другого – три групи ендогенних ризиків. Двоблокова структура розширює традиційні класифікації, що обмежуються зовнішніми технічними загрозами, не враховуючи внутрішніх чинників, які детермінують якість реакції підприємства [15].

Внутрішні ризики виокремлено як метаризики – ендогенні підсилювачі всіх зовнішніх загроз. Під метаризиками у дослідженні розуміються ризики другого порядку, які не створюють загроз безпосередньо, але системно підсилюють вразливість підприємства до зовнішніх цифрових ризиків. Поведінкові ризики (overconfidence, confirmation bias) знижують якість управлінської реакції в умовах цифрової невизначеності [16]. Компетентнісні ризики унеможливлюють своєчасне виявлення та нейтралізацію загроз навіть за наявності відповідних інструментів [17]. Ризики залежності відображають системну вразливість підприємств, що повністю перейшли на цифрові процеси без резервних аналогових механізмів [8; 9].

Класифікацію доповнено двома аналітичними параметрами (табл. 2): швидкістю поширення ризику – для обґрунтування каскадного характеру загроз [8-11], та специфікою прояву залежно від масштабу підприємства [10-12; 15].

Таблиця 2

Класифікація бізнес-ризиків цифрової економіки за критеріями швидкості поширення та масштабу підприємства

Група ризиків	Швидкість поширення	Платформа	Корпорація	МСБ
I. Зовнішні цифрові ризики				
Кіберризики	Висока хв.-год.	Каскадний вплив на всю екосистему партнерів	Часткові втрати, але висока вартість відновлення	Відсутність резервування – повна зупинка
Платформні	Середня год.-дні	Ризик у точках інтеграції API	Диверсифікована інфраструктура знижує ризик	Критична залежність (1-2 платформи = весь бізнес)
Ризики даних	Середня год.-тижні	Агрегація даних мільйонів – системна загроза	Пропорційний обсягу та чутливості оброблюваних даних	Ресурсів для виявлення витоку часто немає
Регуляторні	Низька міс.-роки	Транскордонна діяльність = множинні юрисдикції	Є compliance-служба, але висока вартість адаптації	Брак юридичної експертизи
Операційні	Висока хв.-год.	SLA перед тисячами клієнтів – репутаційний мультиплікатор	Резервні системи знижують вплив	Збій одного сервісу = зупинка всього ланцюга
Стратегічні	Повільна міс.-роки	Мережеві ефекти можуть посилювати або нівелювати загрозу	Ресурси є, але інерція заважає адаптації	Слабкий моніторинг – ризик непомітної дезрупції
II. Внутрішні цифрові ризики				
Поведінкові	Повільна міс.-роки	Системні помилки в стратегії реагування	Overconfidence сповільнює реакцію команд	Ефект статус-кво гальмує цифрову адаптацію
Компетентнісні	Повільна міс.-роки	Дефіцит спеціалістів обмежує масштабування	Цифрова неграмотність блокує нові інструменти	Відсутність IT-компетенцій унеможливлює самостійну оцінку загроз
Залежності	Середня год.-дні	Збій інфраструктури = зупинка всієї екосистеми	Глибока інтеграція ускладнює резервні режими	Відсутність аналогових резервних процедур

Джерело: авторська розробка на основі [4; 7-13; 15-17]

Систематизація класів цифрових ризиків створює підґрунтя для розроблення практичного інструменту самодіагностики підприємств. Запропонований scoring framework (система бального оцінювання зрілості) містить вісім індикаторів за чотирма вимірами і дозволяє оцінити рівень зрілості ризик-менеджменту порівняно з вимогами COSO ERM 2017 [4], ISO/TS 31050:2023 [8] та NIST CSF 2.0 [9] (табл. 3).

Таблиця 3

Scoring framework: індикатори оцінювання зрілості ризик-менеджменту цифрового підприємства

Вимір	Критерій	Традиційний ERM	Цифровий підхід
Методологічний	Частота оновлення реєстру загроз	1 раз на рік	Безперервно
	Частка кількісно вимірюваних ризиків	≥ 70 %	≤ 40 %
Технологічний	Частка ризиків поза периметром	≤ 20 %	≥ 60 %
	Наявність SIEM/SOC	Рідко	Норма (СП/ВП)
Організаційний	CRO з доступом до ради директорів	Рідко	Так (ВП)
	Культура ризику (% залучених)	≤ 40 %	≥ 70 %
Нормативний	Цикл оновлення внутрішніх стандартів	1-2 роки	≤ 6 місяців
	Відповідність GDPR, AI Act, NIS2	Часто часткова	Систематична

Джерело: авторська розробка на основі [3-5; 8; 9; 11]

Scoring framework дозволяє підприємству самостійно діагностувати рівень зрілості за кожним виміром і визначати пріоритетні напрями розвитку. Зміни в одному вимірі без адаптації інших є недостатніми [11; 18]. Framework не передбачає жорсткої уніфікованої шкали, а використовується як інструмент порівняльної діагностики зрілості, що дозволяє адаптувати оцінювання до масштабу, галузі та рівня цифровізації підприємства. Цифровий підхід також породжує нові ризики алгоритмічної непрозорості та технологічної залежності, що самі по собі є проявами метаризиків другого блоку класифікації [7; 16]. Запропонований scoring framework має концептуально-аналітичний характер та розглядається як основа для подальшої емпіричної апробації на вибірці українських підприємств.

Ресурсний потенціал і профіль загроз суттєво різняться між підприємствами різного масштабу, що зумовлює необхідність диференційованого підходу [15]. Sotamaa et al. (2025) підтверджують, що МСБ потребує спрощеного, але системного алгоритму управління ризиками [15] (табл. 4).

Таблиця 4

Диференційований алгоритм управління цифровими ризиками для підприємств різного масштабу

Масштаб підприємства	Пріоритет	Алгоритм (5 кроків)
Мале (до 49 осіб)	Базовий захист	1. MFA і антивірус/EDR 2. Резервування за правилом 3-2-1 3. Навчання персоналу: фішинг, кібергігієна – 2 рази на рік 4. Базова IT-гігієна за матеріалами CERT-UA 5. Реєстр 5–10 ризиків із KRI та відповідальними
Середнє (50–249 осіб)	Системний ERM	1. Ризик-реєстр + KRI + Risk Owner 2. SIEM / SOC або MSSP-аутсорс 3. GDPR / ISO 27001 / DPO 4. Incident Response Plan (5 фаз) 5. Аудит цифрових постачальників (SLA, NDA, exit-план)
Велике та платформа (250+ осіб)	Інтегрований ERM	1. GRC-платформа (ServiceNow, MetricStream) 2. Threat Intelligence + UEBA + SOC 24/7 3. Стрес-тести / Pentest / сценарний аналіз 4. CRO з розширеними повноваженнями + Three Lines of Defence 5. EU AI Act – реєстр ШІ-систем (2025–2027)

Джерело: авторська розробка на основі [4; 8; 9; 11; 15]

Незалежно від масштабу, ефективне управління цифровими ризиками ґрунтується на чотирьох наскрізних принципах: проактивність – превентивні заходи є значно дешевшими за усунення наслідків реалізованих ризиків [8; 9]; культура ризику – понад 80 % успішних кібератак реалізуються через людський фактор, що підтверджує критичну роль поведінкових метаризиків [16]; безперервний моніторинг – статичні щорічні оцінки є недостатніми [8; 9]; адаптивність – система потребує регулярного перегляду з урахуванням змін регуляторного середовища [7; 9].

Теоретичне обґрунтування принципу проактивності спирається на концепцію каскадного характеру цифрових загроз, що принципово відрізняє їх від традиційних загроз і обумовлює недостатність реактивних підходів до управління ризиками. Введення поняття «каскадного характеру» цифрових загроз у контексті управління бізнес-ризиками спирається на три взаємопов'язані наукові традиції.. Перша – теорія системних аварій (Normal Accident Theory) – обґрунтовує, що у щільно інтегрованих технічних системах локальні збої поширюються на суміжні підсистеми через саму архітектуру високої взаємозалежності [10; 11]. Хмарні платформи, API-інтеграції та SaaS-екосистеми утворюють саме таке середовище. Друга – мережева теорія системного ризику – доводить, що в умовах асиметричної взаємозалежності збої у вузлових елементах мережі спричиняють непропорційно масштабні системні кризи [19]. Платформні компанії є такими вузлами, а тисячі підприємств, інтегрованих через них, — периферійними учасниками,

уразливими до чужих збоїв. Третя – сучасні дослідження каскадних збоїв – підтверджує, що каскадні відмови є визначальною характеристикою цифрових екосистем і принципово відрізняються від традиційних ризиків швидкістю поширення та транскордонним масштабом [18]. Синтез цих трьох традицій формує теоретичне підґрунтя для виокремлення «каскадного характеру» як самостійної концептуальної характеристики цифрових ризиків підприємства.

Механізм каскадного поширення цифрових ризиків ілюструє рис. 2.

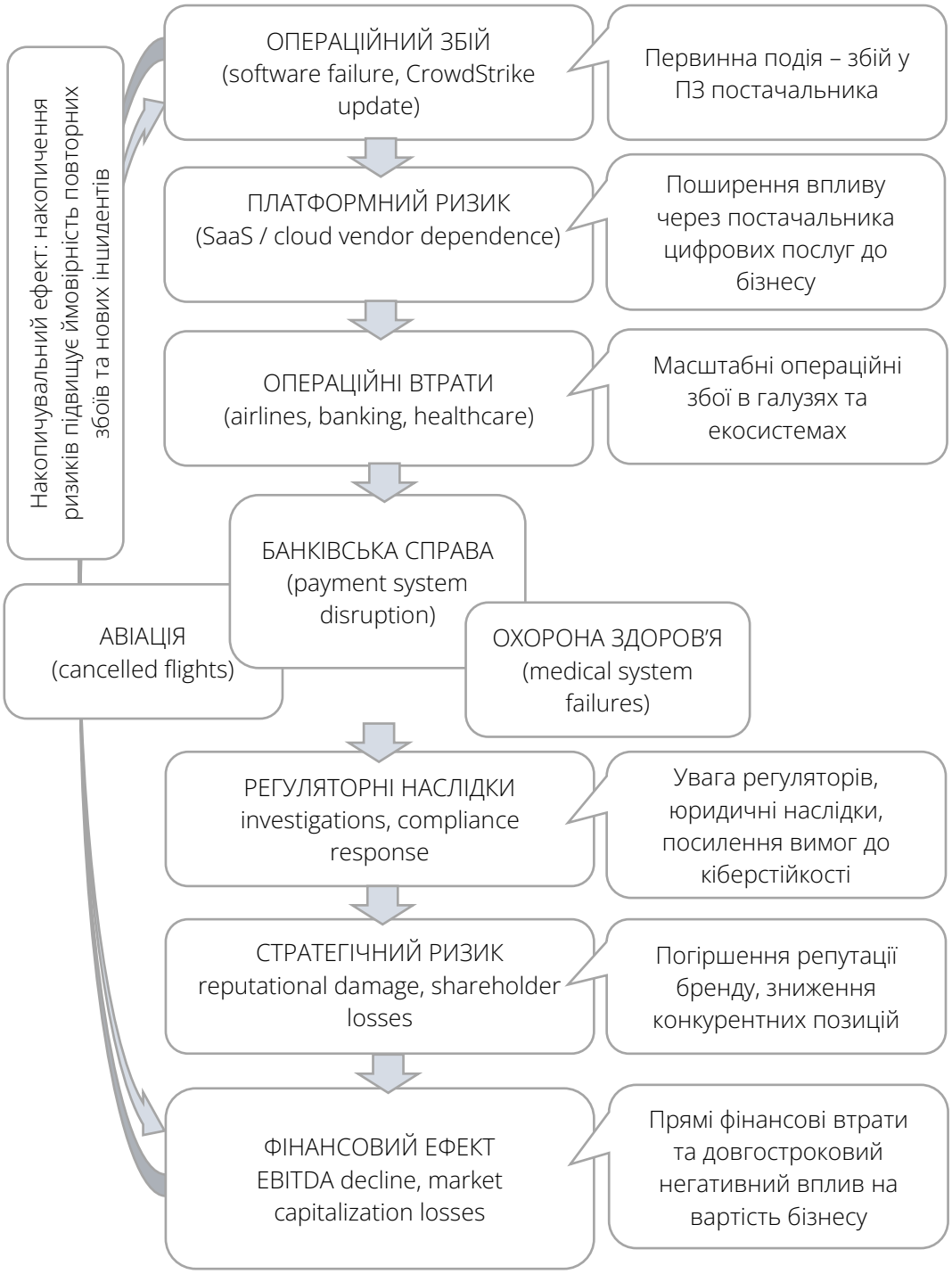

Рис. 2. Каскадний механізм поширення цифрових бізнес-ризиків у платформній економіці

Джерело: авторська розробка на основі [10; 11; 18; 19]

Теоретичні тези верифіковано на двох задокументованих прецедентах (рис. 3). Прецедент 1. SolarWinds (грудень 2020 р.): впровадження шкідливого коду у оновлення ПЗ мережевого моніторингу Orion призвело до компрометації близько 18000 клієнтів. Атака залишалася прихованою понад вісім місяців; вартість акцій SolarWinds знизилася утричі; SEC порушила розслідування. Ризик охопив одночасно операційний, платформний, регуляторний та стратегічний виміри [10; 11]. Прецедент 2. CrowdStrike (19 липня 2024 р.): програмна помилка у оновленні ПЗ безпеки призвела до збою близько 8,5 млн комп'ютерів. За оцінками Parametrix прямі фінансові втрати компаній Fortune 500 склали близько 5,4 млрд дол. США, значна частина яких не покривалася кіберстрахуванням [23].

	SolarWinds (грудень 2020)	CrowdStrike (липень 2024)
Рівень 1 Тригер	**Кіберризик (атака)** Зловмисний код SUNBURST впроваджено в оновлення ПЗ Orion (лютий 2020)	**Операційний ризик (помилка)** Хибне оновлення Falcon Sensor: невідповідність полів даних → збій 8,5 млн пристроїв Windows
Рівень 2 Платформний ризик	**Ризик даних / платформний** ~18000 організацій завантажили заражене оновлення; бекдор у мережах клієнтів SolarWinds	**Платформний / операційний** Збій поширився на авіалінії, банки, лікарні, держагенції у 150+ країнах світу
Рівень 3 Операційні втрати підприємств	**Операційний ризик** Корпорації: компрометація Microsoft, Intel, Cisco, Deloitte, держагенцій США; середні витрати на відновлення ~$12 млн	**Операційний ризик** Delta: збитки $500+ млн, скасовано ~16900 рейсів; МСБ без резервних процедур – повна зупинка на години/дні
Рівень 4 Стратегічні ризики та регуляторні наслідки	**Регуляторний / стратегічний** Слухання Конгресу США; нові вимоги CISA до software supply chain security; судові позови	**Репутаційний / регуляторний** Акції CrowdStrike -32% за 12 днів (-$25 млрд капіталізації); позов Delta; розслідування FCC
Спільна архітектура	Єдина точка довіри (постачальник ПЗ) → компрометація/збій платформного рівня → операційні втрати тисяч підприємств → регуляторні, репутаційні та ринкові наслідки МСБ постраждав непропорційно: відсутність резервних процедур дорівнює повній зупинці діяльності	

Рис. 3. Каскадний характер цифрових ризиків на прикладі SolarWinds (2020) та CrowdStrike (2024)

Джерело: авторська розробка на основі [20; 21]

Обидва прецеденти підтверджують: атака або збій одного вузла ланцюга постачання ініціює ланцюгову реакцію у масштабах всієї цифрової екосистеми, охоплюючи чотири виміри ризику одночасно – явище, що потребує адаптації класичного ERM [10; 11; 18; 19].

Висновки та перспективи. Цифрова трансформація формує якісно новий ризиковий ландшафт, що принципово виходить за межі класичного Enterprise Risk Management. Традиційні концепції COSO ERM та ISO 31000 не повною мірою враховують специфіку цифрових загроз, зокрема їх каскадний характер та роль внутрішніх організаційних чинників, що системно підсилюють зовнішні ризики. Запропонована дев'ятигрупова класифікація бізнес-ризиків цифрової економіки розширює наявні типології завдяки виокремленню внутрішніх метаризиків як ендогенних підсилювачів зовнішніх цифрових загроз. Запровадження параметрів швидкості поширення та специфіки прояву залежно від масштабу підприємства дозволяє диференціювати ризики за пріоритетністю реагування та рівнем потенційного впливу.

Обґрунтування каскадного характеру цифрових загроз та аналіз задокументованих прецедентів дозволили поглибити розуміння природи сучасних ризиків у цифровій економіці й підтвердили, що цифрові збої здатні швидко поширюватися між взаємопов'язаними суб'єктами, одночасно охоплюючи операційний, платформний, регуляторний і репутаційний виміри. Це створює підґрунтя для більш ефективного, адаптивного та диференційованого управління цифровими ризиками залежно від масштабу підприємства.

Запропонований диференційований алгоритм та scoring framework мають концептуально-аналітичний характер і розглядаються як основа для подальшої емпіричної апробації на вибірці українських підприємств. Перспективою подальших досліджень є кількісне тестування scoring framework на панельних даних підприємств різного масштабу, а також розробка програмного інструменту самодіагностики на основі запропонованих індикаторів.

Список використаних джерел:

[1] Dimand, R. W. (2021). Keynes, Knight, and fundamental uncertainty: A double centenary 1921-2021. *Review of Political Economy, 33*(4), 570-584. https://doi.org/10.1080/09538259.2021.1924470

[2] Kayahan, C., & Murat, T. (2022). The evolution of financial risk management. *Journal of Corporate Governance, Insurance, and Risk Management, 9*(Special Issue 1), 155-168. https://doi.org/10.51410/jcgirm.9.1.10

[3] Bromiley, P., McShane, M., Nair, A. K., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265-276. https://doi.org/10.1016/j.lrp.2014.07.005

[4] Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO. https://www.coso.org/guidance-erm

[5] Gleißner, W., & Romeike, F. (2024). Enterprise risk management: Improving embedded risk management and risk governance. *Risks, 12*(12), Article 196. https://doi.org/10.3390/risks12120196

[6] International Organization for Standardization. (2018). *ISO 31000:2018 Risk management – Guidelines*. https://www.iso.org/standard/65694.html

[7] Wang, X. (2024). The risk and challenges in digital economy. *Advances in Economics, Business and Management Research, 287*, 358-364. https://doi.org/10.2991/978-94-6463-441-9_46

[8] International Organization for Standardization. (2023). *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*. https://www.iso.org/standard/54224.html

[9] National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

[10] Afifi, Y. A. M., Hashem, A. E. A. E., & Ahmed Younis, R. A. (2026). The anatomy of a good concept: A systematic review on cyber supply chain risk management. *Sustainability, 18*(3), Article 1151. https://doi.org/10.3390/su18031151

[11] Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: Toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management, 54*(11), 1-29. https://doi.org/10.1108/IJPDLM-12-2023-0445

[12] Прокоф'єва, О. В., & Беспалова, Ю. Ю. (2024). Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. *Ефективна економіка*, (5). https://doi.org/10.32702/2307-2105.2024.5.87

[13] Захаркін, О. О., Бойко, А. В., & Сокол, Л. В. (2023). Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу. *Проблеми сучасних трансформацій*, (10). https://doi.org/10.54929/2786-5738-2023-10-08-02

[14] Леонов, С., & Семко, О. (2023). Інформаційна технологія управління інформаційними ризиками для проєктів цифрової трансформації бізнесу. *Управління розвитком складних систем*, (56), 64-69. https://doi.org/10.32347/2412-9933.2023.56.64-69

[15] Sotamaa, T., Reiman, A., & Kauppila, O. (2025). Manufacturing SME risk management in the era of digitalisation and artificial intelligence: A systematic literature review. *Continuity & Resilience Review*. https://doi.org/10.1108/CRR-12-2023-0022

[16] Berthet, V. (2022). The impact of cognitive biases on professionals' decision-making: A review of four occupational areas. *Frontiers in Psychology, 12*, Article 802439. https://doi.org/10.3389/fpsyg.2021.802439

[17] World Economic Forum. (2023). *The future of jobs report 2023*. https://www.weforum.org/publications/the-future-of-jobs-report-2023

[18] Zhu, X., Zhu, J., Regan, D., & Wen, Z. (2026). Exploring cascading failures in supply chain risk management: A systematic review, 2013-2024. *Journal of Safety Science and Resilience, 7*(2), Article 100234. https://doi.org/10.1016/j.jnlssr.2025.100234

[19] Acemoglu, D., Ozdaglar, A., & Tahbaz-Salehi, A. (2015). Systemic risk and stability in financial networks. *American Economic Review, 105*(2), 564-608. https://doi.org/10.1257/aer.20130456

[20] CrowdStrike. (2024). *Technical details: Falcon content update issue*. https://lnk.ua/2lxOkvdsN

[21] IBM. (2024). *Cost of a data breach report 2024*. https://www.ibm.com/reports/data-breach

[22] Allianz Commercial. (2026). *Cyber incidents, business interruption and natural catastrophes top business risks for 2026: Allianz risk barometer 2026*. https://lnk.ua/kDX7wlmyr

[23] Parametrix loses Fortune 500 firms: $5.4 billion in CrowdStrike losses. (2024). *Reuters*. https://lnk.ua/XiJSGVrl

BUSINESS RISK MANAGEMENT IN THE DIGITAL ECONOMY: CASCADE NATURE OF THREATS AND ALGORITHM FOR ENTERPRISES OF DIFFERENT SCALE

Svitlana Marushchak
Candidate of Economic Sciences, Associate Professor,
Associate Professor of the Department of Economics and Digital Business
Admiral Makarov National University of Shipbuilding, Ukraine

Summary. *Digital transformation is fundamentally reshaping the risk landscape for enterprises, creating qualitatively new classes of threats that fall outside the scope of traditional Enterprise Risk Management (ERM) frameworks. While existing ERM models – including COSO ERM 2017 and ISO 31000:2018 – were designed prior to the current stage of large-scale digital transformation, their limited adequacy for managing digital risks has become increasingly evident in the context of cyber threats, platform dependencies, AI systems, and the high dynamics of the digital environment. This gap between existing risk management tools and the realities of the digital economy constitutes the central problem addressed in this article. The article proposes a nine-group classification of digital business risks structured into two blocks: external digital risks (cyber, platform, data, regulatory, operational, and strategic) and internal digital risks (behavioral, competency-based, and dependency risks). The identification of internal risks as a separate block – functioning as meta-risks, i.e., endogenous amplifiers of all external threats – is an original contribution that extends traditional classifications focused solely on external technical threats. The cascade nature of digital threats is theoretically substantiated through the convergence of three scientific traditions: Normal Accident Theory (Perrow), network theory of systemic risk (Acemoglu et al.), and contemporary research on cascading failures in digital supply chains (Zhu et al., 2026; Jazairy et al., 2024). This theoretical framework is empirically verified through comparative analysis of two documented cases – SolarWinds (December 2020) and CrowdStrike (July 2024). A scoring framework comprising eight indicators across four dimensions (methodological, technological, organizational, and normative) is developed to assess digital risk management maturity, with threshold values validated against COSO ERM 2017, ISO/TS 31050:2023, and NIST CSF 2.0. A differentiated five-step algorithm is proposed for enterprises of different scales, ranging from basic cybersecurity hygiene for SMEs to integrated GRC platforms and EU AI Act compliance for large corporations.*

Keywords: *digital risks, risk management, cascade effect, meta-risks, scoring framework, cybersecurity, Enterprise Risk Management, digital economy, SME.*

Дата публікації: 31.05.2026

Дата першого надходження статті до видання: 29.04.2026
Дата прийняття статті до друку після рецензування: 20.05.2026