https://www.sworldjournal.com/index.php/swj/article/view/swj35-03-050
DOI: 10.30888/2663-5712.2026-35-03-050

УДК 005.334:338.2:004.056

A MODEL FOR MANAGING BUSINESS ECONOMIC SECURITY IN THE DIGITAL ECONOMY: A RISK-CONTROL MATRIX AND A KRI/KPI INDICATOR SYSTEM

МОДЕЛЬ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕПЕКОЮ БІЗНЕСУ В ЦИФРОВІЙ ЕКОНОМІЦІ: МАТРИЦЯ РИЗИКІВ І КОНТРОЛІВ ТА СИСТЕМА ІНДИКАТОРІВ (KRI/KPI)

Ventsuryk A. M. / Венцурик А. М.
Ph.D. / к. е. н.
ORCID ID: 0000-0002-1583-664X
National University of Water and Environmental Engineering, Rivne
Національний університет водного господарства та природокористування, м. Рівне

Анотація. *Цифрова економіка змінює природу економічної безпеки бізнесу: критичними стають дані, цифрові платформи, інтеграції, хмарні та аутсорсингові сервіси, а також здатність компанії підтримувати безперервність ключових процесів під час інцидентів. За таких умов традиційні підходи до переліку загроз є недостатніми, оскільки не формують операційного зв'язку між ризиком, управлінським контролем і вимірюваними індикаторами виконання. Метою статті є розроблення прикладної моделі управління економічною безпекою бізнесу в цифровій економіці через: контур управління, матрицю «ризик - контроль» та систему індикаторів KRI/KPI для моніторингу рівня ризику й результативності контролів. Методологічну основу становлять принципи ризик-менеджменту, вимоги до системи управління інформаційною безпекою, підхід до забезпечення стійкості та відновлюваності, а також рамка NIST CSF 2.0, що інституціоналізує управління кіберризиками як управлінську функцію. У результаті запропоновано логіку циклічного управління (ідентифікація активів і залежностей → оцінювання ризиків → добір контролів → реалізація → моніторинг і аудит → коригування), наведено приклад матриці ризиків і контролів та мінімально достатній набір KRI/KPI з правилами встановлення порогових значень відповідно до прийнятного (допустимого) рівня ризику, визначеного керівництвом. Практична цінність роботи полягає в можливості швидкого впровадження моделі в компаніях різних секторів як каркаса внутрішньої політики економічної безпеки в умовах цифрової трансформації.*

Ключові слова: *економічна безпека бізнесу, цифрова економіка, ризик-менеджмент, матриця ризиків і контролів, індикатори KRI/KPI, ISMS, безперервність бізнесу, NIST CSF.*

Вступ

Під впливом цифрової трансформації бізнес дедалі більше залежить від IT-ландшафту, зовнішніх провайдерів, цифрових платформ і якості даних. Відповідно, економічна безпека починає визначатися не лише фінансовою стійкістю, а й цифровою стійкістю (resilience), керованістю залежностей і здатністю відновлювати критичні процеси після збоїв чи атак. В українських дослідженнях наголошується на циклічності управління економічною безпекою та інтеграції цього процесу в загальну систему управління підприємством [1], а

також на необхідності системного моніторингу, оцінювання ризиків і постійного вдосконалення механізмів захисту [2].

У цифровій економіці проблема загострюється через «ефект каскаду»: інцидент у постачальника сервісу, збій інтеграції або компрометація облікового запису можуть швидко трансформуватися у фінансові втрати, простій, репутаційний шок і юридичні санкції. Дослідники ризик-менеджменту в умовах цифровізації підкреслюють необхідність поєднання організаційних, технічних і фінансових заходів, а також створення інструментальної бази для контролю ризиків [3]. Паралельно з цим у наукових роботах про економічну безпеку в цифровій економіці посилюється акцент на інституціоналізації управлінських процедур і вимірюваності результатів [4], включно з фінансовим виміром ризиків цифрового середовища [5].

Міжнародні рамки (OECD, ISO, NIST) пропонують розглядати управління ризиками цифрової безпеки (digital security risk management) як управлінську категорію та інтегрувати її в прийняття рішень на рівні керівництва [6] - [10]. Однак на практиці у багатьох компаній зберігається розрив між переліком загроз, набором формальних політик та відсутністю зрозумілих індикаторів виконання контролів. Саме тому потрібна модель, яка «зшиває» ризики, управлінські дії та вимірюваний контроль результату.

Мета статті розробити прикладну модель управління економічною безпекою бізнесу в цифровій економіці через контур управління, матрицю ризиків і контролів та систему індикаторів KRI/KPI. **Завдання:** уточнити логіку управління економічною безпекою як циклу; запропонувати структуру матриці «ризик - контроль»; визначити мінімально достатню систему KRI/KPI та підхід до порогових значень.

1. Огляд зовнішнього оточення та постановка проблеми

Економічна безпека підприємства традиційно пов’язується із захистом ресурсів і стабільністю функціонування в умовах загроз. У роботах, присвячених моделям управління економічною безпекою, підкреслюється необхідність стратегічного планування, діагностики загроз і заходів з мінімізації, а також

безперервного характеру оцінювання рівня безпеки [1]. Окремо виділяється набір базових завдань системи економічної безпеки: моніторинг і прогнозування загроз; оцінювання ризиків кількісними та якісними методами; розробка інструментів нівелювання загроз; постійне вдосконалення механізму управління [2].

У цифровій економіці вказані завдання ускладнюються трьома чинниками:

1. **зростанням цифрових активів** (дані клієнтів, алгоритми, цифрові канали продажу);

2. **залежністю від третіх сторін** (хмара, платіжні провайдери, маркетплейси, SaaS);

3. **прискоренням інцидентів** (швидкість розвитку події стає фактором збитків).

Підходи OECD пропонують інтегрувати цифрові ризики в загальну управлінську логіку та пов'язувати їх із довірою, економічною та соціальною цінністю цифрового середовища [6]. У фінансовому вимірі ризики цифровізації прямо впливають на стійкість компаній і потребують управлінських інструментів, здатних фіксувати трансформаційні зміни [5]. Отже, ключова проблема формулюється як **відсутність єдиного операційного ланцюжка**: **ризик → контроль (управлінська дія) → індикатор → управлінське рішення → перевірка ефекту → коригування**.

2. Вхідні дані та методи

Методологія статті ґрунтується на поєднанні:

- **ризик-орієнтованого підходу** ISO 31000 (ідентифікація, аналіз, оцінювання, обробка, моніторинг і комунікація ризиків) [7];
- **вимог до ISMS** як організаційної системи управління інформаційною безпекою та ризиками (ISO/IEC 27001) [8];
- **принципів безперервності бізнесу** (ISO 22301) як інституційної рамки готовності до збоїв і відновлення [9];
- **рамки NIST CSF 2.0**, що структурує результати управління кіберризиками за функціями Govern – Identify – Protect – Detect – Respond - Recover [10].

Інструментально використано підхід **матриці ризиків** як способу пріоритизації (ймовірність × вплив, із практичним застосуванням у менеджменті) [11], а також наукові напрацювання щодо економічної безпеки підприємств та ролі цифрових компонентів у системі безпеки [4].

Ключові визначення для цієї роботи:

- **KRI (Key Risk Indicators)** - індикатори, що сигналізують про зростання ризику або наближення до небезпечного стану (передінцидентні/провісники).
- **KPI (Key Performance Indicators)** - індикатори результативності контролів/процесів (післядія або підтвердження виконання).
- **Порогові значення** KRI/KPI встановлюються компанією відповідно до **прийнятного (допустимого) рівня ризику, визначеного керівництвом** (аналог того, що в англомовній літературі називають risk appetite).

3. Результати дослідження

Запропонований контур управління (рис. 1) відображає безперервний цикл, у якому економічна безпека досягається через керованість цифрових активів і залежностей, узгоджений набір контролів та регулярне вимірювання індикаторів. Логіка циклу узгоджується з ідеєю постійної оцінки економічної безпеки та її інтеграції в управління підприємством [1], а також із принципами ризик-менеджменту [7].

Логіка циклу узгоджується з позицією, що управління економічною безпекою має бути постійним і циклічним, інтегрованим у загальний менеджмент підприємства.

Матриця ризиків і контролів (таблиця 1) потрібна для того, щоб перейти від загальних формулювань до керованих управлінських дій. У наукових підходах до управління економічною безпекою наголошується на необхідності механізмів нівелювання загроз і системності заходів [2]. У цифровізації цей механізм доцільно конкретизувати через зв'язку «ризик → контроль», де контроль має власника, частоту виконання, доказ виконання та вимірюваний ефект [3], [8].

Перед поданням прикладу матриці зауважимо: перелік ризиків формується від критичних процесів і цифрових активів (дані, платформи, інтеграції, облікові

записи), а не від технологій загалом. Пріоритизація ризиків виконується за комбінацією ймовірності, впливу та швидкості розвитку інциденту, що краще відображає цифрову динаміку (коли швидкість ескалації безпосередньо збільшує збитки).

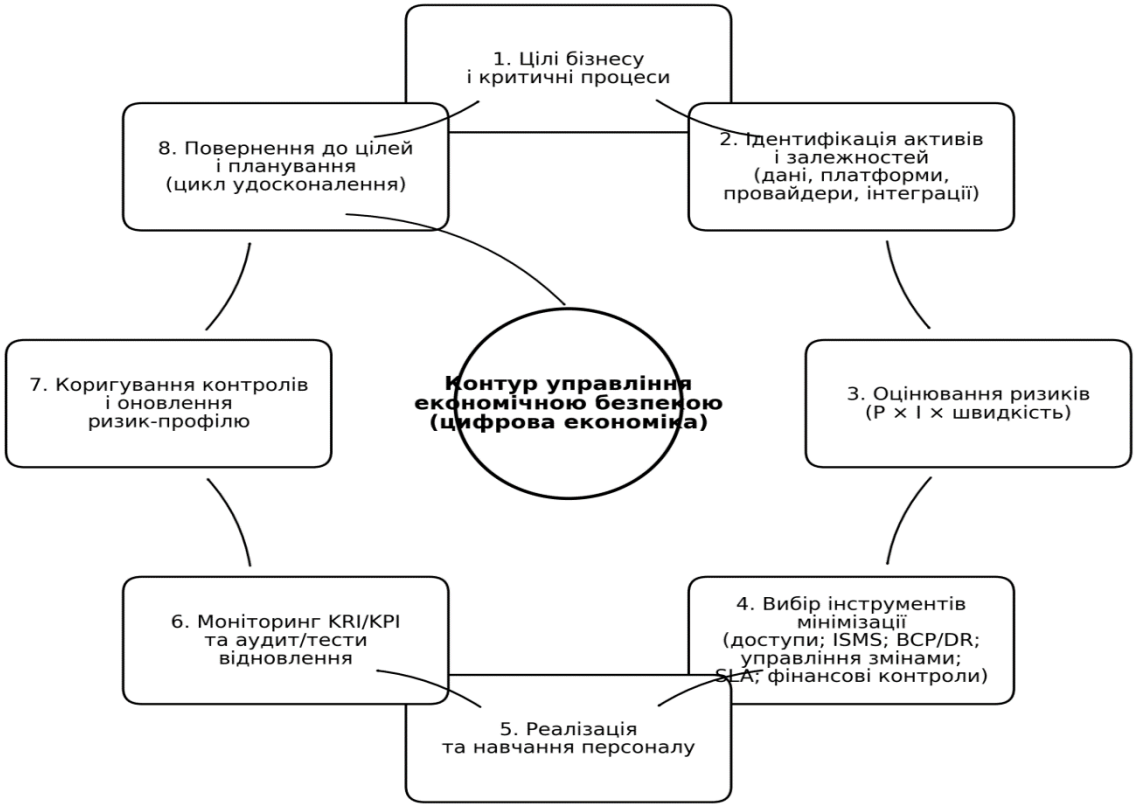

Рисунок 1 - Контур управління економічною безпекою бізнесу в цифровій економіці

Джерело: авторська розробка на основі [6] - [9].

Щоб матриця «ризик - контроль» працювала як інструмент менеджменту, кожен ключовий контроль має бути підкріплений індикаторами. Доцільно розводити KRI (сигнали ризику) і KPI (результативність виконання контролів), аби уникнути змішування причин і наслідків.

Принципи побудови індикаторів:

1. Однозначність (індикатор має «читатися» без додаткових трактувань).

2. Регулярність (частота вимірювання прив’язана до швидкості розвитку ризику).

3. Власник та реакція (для кожного порога визначається, хто й що робить).

4. Пороги встановлюються відповідно до прийнятного (допустимого) рівня ризику, визначеного керівництвом, та мають бути зафіксовані в політиках/регламентах.

Таблиця 1 - Фрагмент матриці ризиків і контролів для управління економічною безпекою бізнесу в цифровій економіці

Ризик (подія)	Цифровий актив/ залежність	Ймовірність	Вплив	Ключовий контроль (управлінська дія)	Власник контролю	Доказ виконання
Компрометація облікового запису адміністрування	IAM / адмін-доступи	Середня	Високий	MFA для привілейованих акаунтів; принцип найменших привілеїв; ревізія доступів	CISO / IT Security	Звіт IAM; журнал змін прав
Простій критичної платформи продажу	Платформа/ хмара/SaaS	Середня	Високий	План безперервності (BCP), план відновлення (DR), тестування RTO/RPO; угода про рівень сервісу (SLA) та план виходу (exit plan)	COO / IT Ops	Протоколи тестів; умови SLA; звіт DR
Витік персональних даних клієнтів	Бази даних / DLP	Низька-середня	Високий	Класифікація даних; шифрування; DLP; реагування на інциденти	DPO / CISO	Реєстр даних; політики; журнал інцидентів
Збій інтеграції з платіжним провайдером	API/інтеграції/ провайдер	Середня	Середній	Управління змінами; моніторинг API; резервний провайдер	CIO / Product	Change log; метрики API; договори
Шахрайські транзакції	Платежі/ антифрод	Середня	Середній	Антифрод-правила; ліміти; сегментація; розслідування	CFO / Risk	Антифрод-звіти; кейси розслідувань

Джерело: авторська розробка.

Приклади KRI:

- частка привілейованих акаунтів без MFA;
- кількість критичних вразливостей, що перевищили термін усунення (SLA на патчинг);
- частота збоїв інтеграцій та середній час деградації сервісу;
- частка «невідомих» цифрових активів (невідповідність реєстру активів фактичному стану).

Приклади KPI:

- відсоток успішно завершених тестів відновлення (DR) за планом;
- фактичні RTO/RPO у тестах проти цільових значень;
- частка контролів, виконаних у строк (за календарем контролів);
- час виявлення/реагування на інцидент (MTTD/MTTR) у межах встановлених норм.

У термінах міжнародних рамок така логіка підтримує інтеграцію управління цифровими ризиками в управлінські рішення (OECD) [6], відповідає процесності ризик-менеджменту (ISO 31000) [7], підсилює вимоги до ISMS (ISO/IEC 27001) [8], а також узгоджується з орієнтацією NIST CSF 2.0 на безперервність функцій управління та готовність до реагування/відновлення [10].

4. Обговорення і аналіз результатів

Запропонована модель має прикладну цінність для бізнесу, який: швидко масштабується в онлайні; значною мірою покладається на провайдерів; має високі вимоги до безперервності продажів/обслуговування. Її впровадження доцільно проводити етапно:

1. **Картування критичних процесів і цифрових залежностей** (активи, інтеграції, провайдери, дані).

2. **Формування реєстру ризиків** із зазначенням швидкості розвитку інциденту та ланцюжків залежностей.

3. **Проєктування контролів**: політики доступу, управління змінами, BCP/DR, угода про рівень сервісу (SLA) та план виходу (exit plan), фінансові контроли (ліміти, резерви, антифрод).

4. **Побудова KRI/KPI** та регламенту реагування на порогові значення.

5. **Аудит і тестування** (включно з відновленням), коригування ризик-профілю.

Важливим є те, що модель не підміняє собою стандарти, а виступає «операційним каркасом», який дозволяє узгодити вимоги та рекомендації ISO/NIST/OECD із внутрішніми процедурами компанії. При цьому матриця ризиків, як інструмент управління, забезпечує наочність пріоритетів і

дисциплінує прийняття рішень (що підтверджується практиками використання risk matrix у менеджменті).

Обмеження. Запропонований приклад матриці є універсалізованим; у реальному впровадженні потрібна адаптація до галузі, регуляторних вимог і конкретних ланцюжків створення цінності. Окремого посилення потребує фінансово-економічна частина (оцінка втрат, резервування, страхування), що є перспективним напрямом подальших досліджень у контексті ризиків цифрової економіки.

Висновки

Запропонована модель управління економічною безпекою бізнесу в цифровій економіці дає можливість перейти від декларативного опису загроз до керованого процесу, у якому ризики пов'язані з конкретними управлінськими контролями та вимірюваними індикаторами. Логіка моделі побудована як безперервний цикл: від формулювання бізнес-цілей і визначення критичних процесів - до ідентифікації цифрових активів і залежностей, оцінювання ризиків, добору та впровадження контролів, навчання персоналу, моніторингу показників, проведення аудитів і тестування відновлення, а також регулярного коригування контрольного середовища й оновлення ризик-профілю. Такий підхід підсилює узгодженість управління безпекою з операційним і фінансовим менеджментом, зменшує фрагментацію відповідальності та робить управлінські рішення відтворюваними.

Структурування ризиків через матрицю «ризик - контроль» забезпечує практичну придатність моделі для різних типів підприємств: ризики формуються від критичних процесів і цифрових залежностей (дані, платформи, провайдери, інтеграції), для кожного ризику визначається набір мінімально необхідних контролів і відповідальний власник, а пріоритетність заходів обґрунтовується не лише ймовірністю та впливом, але й швидкістю ескалації інциденту. Це дозволяє раціонально розподіляти ресурси, концентруючи їх на найбільш швидких і дорогих за наслідками подіях, та уникати ситуації, коли контрольні заходи існують формально, але не знижують реальних втрат.

Розмежування індикаторів на KRI та KPI підвищує керованість: KRI виконують роль ранніх сигналів погіршення ризикового стану, тоді як KPI фіксують результативність контролів і процесів. Порогові значення індикаторів доцільно встановлювати відповідно до прийнятного (допустимого) для компанії рівня ризику, затвердженого керівництвом, із наперед визначеними реакціями на відхилення (відповідальний, термін, коригувальна дія). У такій конфігурації модель може застосовуватися як «каркас» внутрішньої політики економічної безпеки: вона створює основу для системного моніторингу, підвищує прозорість контролю виконання рішень, зменшує імовірність простоїв і непрямих втрат та підтримує довіру клієнтів і партнерів у цифровому середовищі.

Подальший розвиток підходу доцільно спрямувати на кількісне обґрунтування порогів KRI/KPI для різних галузей і масштабів підприємств та на поглиблення фінансового блоку оцінювання наслідків цифрових інцидентів (вартість простою, очікувані збитки, резервування, страхування). Це посилить точність пріоритизації ризиків і дасть змогу приймати ще більш обґрунтовані управлінські рішення в межах запропонованої моделі.

Література

1. Загородня А. С. Підвищення рівня управління економічною безпекою підприємств в умовах ризиків та загроз // Економіка та суспільство. 2023. Вип. 54. DOI: 10.32782/2524-0072/2023-54-12. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2727/2644 (дата звернення: 12.01.2026).

2. Сергеєва Д. О., Нагорна І. І. Модель управління економічною безпекою підприємства в умовах нестабільного зовнішнього середовища // Бізнес, інновації, менеджмент: проблеми та перспективи : матеріали VI Міжнар. наук.-практ. конф. 2025. С. 121-122. URL: https://confmanagement-proc.kpi.ua/article/view/329462/318995 (дата звернення: 12.01.2026).

3. Гудзь О. Є., Захаржевська А. А. Управління ризиками підприємств в умовах цифровізації : навч. посіб. Кропивницький : Видавець Лисенко В. Ф.,

2023. 176 с. URL: https://duikt.edu.ua/uploads/l_2322_63313494.pdf (дата звернення: 12.01.2026).

4. Organisation for Economic Co-operation and Development (OECD). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Paris : OECD, 2015. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc/9789264245471-en.pdf (дата звернення: 12.01.2026).

5. International Organization for Standardization (ISO). ISO 31000:2018 Risk management - Guidelines : [Електронний ресурс]. URL: https://www.ler.uam.mx/Calidad-UAML/wp-content/uploads/2025/02/ISO-31000-2018.pdf (дата звернення: 12.01.2026).

6. International Organization for Standardization (ISO). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements : [Електронний ресурс]. URL: https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf (дата звернення: 12.01.2026).

7. International Organization for Standardization (ISO). ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements : [Електронний ресурс]. URL: https://cdn.standards.iteh.ai/samples/75106/d11801a9bab045a88d59cd321519ecf1/ISO-22301-2019.pdf (дата звернення: 12.01.2026).

8. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. 2024 : [Електронний ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 12.01.2026).

9. FlexiProject. Матриця ризиків: ключовий інструмент в управлінні проєктними ризиками : [Електронний ресурс]. URL: https://flexi-project.com/uk/%D0%BC%D0%B0%D1%82%D1%80%D0%B8%D1%86%D1%8F-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA%D1%96%D0%B2-

%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%B2%D0%B8%D0%B9-%D1%96%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82/ (дата звернення: 12.01.2026).

10. Сосновська О. О. Система економічної безпеки підприємств зв'язку : монографія. Київ : Центр учбової літератури, 2019. 440 с. URL: https://elibrary.kubg.edu.ua/id/eprint/28946/1/O_Sosnovska_SEBPZ_FITU.pdf (дата звернення: 12.01.2026).

References (for international indexing)

1. Zahorodnia, A. S. (2023). Pidvyshchennia rivnia upravlinnia ekonomichnoiu bezpekoiu pidpryiemstv v umovakh ryzykiv ta zahroz. *Ekonomika ta suspilstvo*, (54). URL: https://economyandsociety.in.ua/index.php/journal/article/view/2727/2644 (accessed: 12 Jan 2026).

2. Serheieva, D. O., & Nahorna, I. I. (2023). Model upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva v umovakh nestabilnoho zovnishnoho seredovyshcha. In *Business, Innovations, Management: Problems and Prospects: Proceedings of the VI International Scientific and Practical Conference* (pp. 121-122). URL: https://confmanagement-proc.kpi.ua/article/view/329462/318995 (accessed: 12 Jan 2026).

3. Hudz, O. Ye., & Zakharzhevska, A. A. (2023). *Upravlinnia ryzykamy pidpryiemstv v umovakh tsyfrovizatsii* [Risk management of enterprises in the context of digitalization] (Study guide). Kropyvnytskyi: Vydavets Lysenko V. F. URL: https://duikt.edu.ua/uploads/l_2322_63313494.pdf (accessed: 12 Jan 2026).

4. OECD. (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris: OECD. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc/9789264245471-en.pdf (accessed: 12 Jan 2026).

5. ISO. (2018). *ISO 31000:2018 Risk management - Guidelines*. URL: https://www.ler.uam.mx/Calidad-UAML/wp-content/uploads/2025/02/ISO-31000-2018.pdf (accessed: 12 Jan 2026).

6. ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. URL: https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf (accessed: 12 Jan 2026).

7. ISO. (2019). *ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements*. URL: https://cdn.standards.iteh.ai/samples/75106/d11801a9bab045a88d59cd321519ecf1/ISO-22301-2019.pdf (accessed: 12 Jan 2026).

8. NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed: 12 Jan 2026).

9. FlexiProject. (n.d.). Matrytsia ryzykiv: kliuchovyi instrument v upravlinni proiektnymy ryzykamy [Risk matrix as a key tool in project risk management]. URL: https://flexi-project.com/uk/%D0%BC%D0%B0%D1%82%D1%80%D0%B8%D1%86%D1%8F-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA%D1%96%D0%B2-%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%B2%D0%B8%D0%B9-%D1%96%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82/ (accessed: 12 Jan 2026).

10. Sosnovska, O. O. (2019). *Systema ekonomichnoi bezpeky pidpryiemstv zviazku* [Economic security system of telecommunications enterprises] (Monograph). Kyiv: Tsentr uchbovoi literatury. URL: https://elibrary.kubg.edu.ua/id/eprint/28946/1/O_Sosnovska_SEBPZ_FITU.pdf (accessed: 12 Jan 2026).

Abstract

Introduction. *Digital transformation changes the nature of business economic security: data, digital platforms, integrations, cloud and outsourced services become critical assets, while incident-driven disruptions increasingly translate into direct and indirect financial losses. Traditional "lists of threats" are insufficient because they do not establish an operational link between risks, managerial controls, and measurable monitoring indicators.*

External environment and problem statement. *The digital economy amplifies dependency risk and the "cascade effect": a provider incident, integration failure, or account compromise can quickly escalate into downtime, reputational damage, and compliance exposure. Therefore, a practical governance gap emerges-companies often have fragmented policies and controls without a unified, measurable chain connecting risk identification, mitigation actions, and evidence of effectiveness.*

Data and methods. *The paper relies on a risk-based management logic and integrates approaches from ISO 31000 (risk management process), ISO/IEC 27001 (information security management system), ISO 22301 (business continuity management), and NIST CSF 2.0 (govern – identify – protect – detect – respond - recover). Risk prioritization is proposed using a combined assessment of likelihood, impact, and incident escalation speed. A risk matrix approach is used as an instrumental tool to structure and prioritize managerial responses.*

Results. *A continuous management loop is proposed: defining objectives and critical processes; identifying digital assets and dependencies; assessing risks; selecting and implementing controls; staff training; monitoring KRI/KPI; audit and recovery testing; and iterative adjustment of controls and the risk profile. A risk–control matrix template is provided to translate key risk events into specific controls with assigned owners and evidence requirements. A minimal but sufficient KRI/KPI set is specified to distinguish early risk signals (KRI) from control/process performance (KPI), including rules for setting thresholds aligned with the organization's acceptable risk level determined by top management.*

Discussion. *The model is practically applicable to businesses with high reliance on digital channels and third-party services and with strict continuity requirements. It does not replace international standards; rather, it operationalizes them into an executable internal governance framework. Implementation is recommended as a staged rollout from critical processes and dependencies toward full coverage, with attention to industry and regulatory specifics.*

Conclusions. *The proposed model enables a measurable and repeatable chain "risk → control → indicator → decision → verification → adjustment," improving accountability, prioritization discipline, and continuity readiness in the digital economy. Future work should refine quantitative threshold setting for KRI/KPI across sectors and strengthen the financial estimation block (downtime cost, expected losses, reserving, and insurance).*

Keywords: *business economic security; digital economy; risk management; risk-control matrix; KRI; KPI; ISMS; business continuity; NIST CSF.*

Article sent: 16.01.2026