

DOI: <https://doi.org/10.37634/efp.2026.6.11e>
 УДК 005.334:658(477)

Андрій Едуардович **ЛОЗАН**

здобувач, Національний університет "Одеська політехніка"

ORCID: <https://orcid.org/0009-0009-2808-6217>

e-mail: andlozedd@gmail.com

ГЛОБАЛЬНІ РИЗИКИ ДЛЯ ПІДПРИЄМСТВ УКРАЇНИ: ОЦІНЮВАННЯ ТА ПЕРСПЕКТИВИ УПРАВЛІННЯ

Досліджено вплив глобальних ризиків на стійкість українських підприємств. Мета статті – систематизація загроз та обґрунтування підходів до управління ними за допомогою цифрових технологій. На основі методології COSO ERM та ISO 31000 побудовано ризик-реєстр і виокремлено 8 груп ризиків. Найвищу критичність мають геополітичні, енергетичні та кіберризики. Запропоновано напрями їх мінімізації через застосування систем підтримки рішень, моніторингу та кіберзахисту. Наукова новизна полягає в інтеграції оцінки ризиків воєнного стану з групуванням цифрових інструментів їх нейтралізації.

Ключові слова: глобальні ризики, управління ризиками, підприємства України, цифрові технології, ризик-реєстр, стійкість бізнесу, стратегічна адаптація

Стаття надійшла 29.04.2026

Статтю прийнято 18.05.2026

Статтю опубліковано 29.05.2026

ВСТУП

Сучасні українські підприємства функціонують у надзвичайно турбулентному глобальному середовищі, яке визначається одночасною дією військових загроз, енергетичних і кліматичних викликів, фінансової нестабільності, регуляторних бар'єрів та стрімкої цифровізації. У таких умовах традиційні підходи до стратегічного планування й управління втрачають ефективність, оскільки вони не враховують комплексного та динамічного характеру глобальних ризиків. Відсутність систематизованого інструментарію для оцінювання та моніторингу ризиків знижує стійкість бізнесу та обмежує його здатність до інноваційного розвитку. Це зумовлює необхідність розроблення підходів, що поєднують кількісне оцінювання ймовірності та впливу ризиків із сучасними цифровими рішеннями для їх своєчасного виявлення та управління.

Аналіз останніх досліджень і публікацій

Проблеми впливу глобальних ризиків на діяльність підприємств та їх цифрової трансформації активно досліджуються у світовій і вітчизняній науці. Зокрема, еволюцію систем ризик-менеджменту та застосування стандартів COSO досліджували К. Прюетт та А. Террі [1]. Вплив цифрових технологій (ЦТ) на управління ризиками ланцюгів постачання розкрито у працях Д. Іванова, А. Долгуї та Б. Соколова [2]. Зв'язок між управлінням ризиками та фінансовою результативністю підприємств обґрунтовано Л. Сировою та співавторами [3]. Вітчизняні дослідники, зокрема І. Чмутова, А. Гайналій, В. Алькема фокусують увагу на специфіці управління безпекою та стійкістю українських підприємств в умовах тривалого військового конфлікту [4; 5; 10].

МЕТА статті – систематизація ключових глобальних ризиків для підприємств України, формалізація методології їх кількісного оцінювання та обґрунтування комплексної системи управління ризиками на основі функціонального застосування ЦТ.

МЕТОДИ ДОСЛІДЖЕННЯ

У дослідженні застосовано такі методи, як: аналіз та синтез, порівняння, пояснення та узагальнення.

РЕЗУЛЬТАТИ

Глобальний ризик визначається як ймовірність настання події або ситуації, яка матиме негативний вплив на значну частину світового ВВП, населення або бізнес-середовища [6].

Для розуміння специфіки загроз, що впливають на українські підприємства, доцільно проаналізувати наявні підходи до класифікації ризиків. Узагальнення підходів провідних міжнародних інституцій та дослідників наведено у табл. 1.

Як свідчить аналіз табл. 1, наявні підходи мають різний фокус. Міжнародні звіти (WEF, Allianz) акцентують на глобальних макроекономічних та кібернетичних трендах, тоді як національні звіти (RDNA4) та вітчизняні дослідження зосереджені на фізичній інфраструктурі та наслідках війни. Запропонована у цій статті класифікація заповнює наявну прогалину, інтегруючи глобальні технологічні та екологічні тренди зі специфічними українськими реаліями (енергетичний дефіцит, порушення логістики), створюючи єдину комплексну номенклатуру ризиків для рівня окремого підприємства.

На основі цього синтезу виокремлено вісім ключових категорій ризиків у табл. 2, які формують основу для подальшого оцінювання.

Логічним продовженням класифікації є кількісне оцінювання виявлених загроз. Методологія оцінювання у цьому дослідженні базується на принципах міжнародних стандартів ISO 31000:2018 та концептуальній основі COSO ERM. Для оцінювання застосовано метод побудови ризик-реєстру із застосуванням матриці «ймовірність × вплив».

Вибір мультиплікативного підходу (де інтегральний показник є добутком балів ймовірності та впливу) зумовлено його здатністю чітко диференціювати ризики з високою ймовірністю/низьким впливом від ризиків з низькою ймовірністю/катастрофічним впливом, що дає підприємствам змогу раціонально розподіляти ресурси на реагування [11; 12].

Оцінювання ризиків здійснювалося за п'ятибальною шкалою з окремим визначенням рівнів ймовірності та впливу. Зокрема, для оцінювання ймовірності настання ризикової події застосовано таку градацію: 1 бал – вкрай

Таблиця 1 – Порівняння підходів до класифікації ризиків (складено автором на основі [4-9])

Основні групи ризиків	Джерело	Критерій фокусування	Рівень деталізації технологічних/цифрових ризиків
Економічні; політичні; технологічні; соціальні; екологічні	І. Чмутова, А. Гайналій, Н. Пагуліна	Специфіка воєнного стану та стійкість підприємств	Середній (технологічні ризики розглядаються як похідні від інфраструктурних)
Економічні; геополітичні; соціальні; технологічні; екологічні	WEF (Global Risks Report)	Макроекономічний та глобальний вплив	Високий (виділено кібернетичні ризики, ІІІ, дезінформацію)
Фінансові; інфраструктурні; соціальні; управлінські	Світовий банк (RDNA4)	Оцінка збитків та потреб відбудови	Низький (акцент на фізичній інфраструктурі та енергетиці)
Політичні; економічні; комерційні	Allianz	Вплив на безперервність бізнесу	Високий (кіберінциденти визнано ризиком №1 у світі)
Кадрові; фінансові; логістичні; технологічні	UNDP (МСП)	Фокус на операційних ризиках та життєздатності малого бізнесу	Середній (цифровізація розглядається як інструмент виживання)

Таблиця 2 – Класифікація глобальних ризиків для підприємств України (складено автором на основі [4-7])

Категорія ризику	Ризики	Потенційний вплив на підприємства
Економічні	інфляція; девальвація валюти; рецесія; неплатежі контрагентів	зниження платоспроможності клієнтів; проблеми ліквідності
Політичні та геополітичні	війна; санкції; нестабільність політичних режимів; регіональні конфлікти	втрата ринків збуту; перебої у співпраці з міжнародними партнерами
Енергетичні	дефіцит потужностей; пошкодження інфраструктури; перебої постачання е/е, газу	простої виробництва; зростання витрат на енергоресурси
Логістичні	блокування коридорів; перебої у портах; зростання страхових премій; обмеження експорту	затримки постачання; зрив контрактів; зростання собівартості
Кібернетичні	кібератаки; витік даних; блокування виробничих систем	фінансові збитки; репутаційні втрати; ризики безпеки даних
Регуляторні	вимоги ЄС (CBAM, GDPR, ETS); зміни податкового законодавства; бюрократія	штрафи; втрата доступу до ринків; додаткові витрати на комплаєнс
Кліматичні та екологічні	посухи; повені; підвищення витрат на декарбонізацію; ESG-вимоги інвесторів	збитки від стихійних лих; підвищення витрат; втрата інвестицій
Кадрові та соціальні	дефіцит робочої сили; мобілізація; плинність кадрів; дефіцит кваліфікації	зниження продуктивності; зрив проєктів; зростання зарплатного тиску

малоймовірна подія (менше 10 % імовірності протягом року); 2 бали – низька ймовірність (11–30 %); 3 бали – середня ймовірність (31–50 %); 4 бали – висока ймовірність (51–80 %); 5 балів – майже неминуха подія (понад 80 %).

Оцінювання впливу ризику також проводилося за п'ятибальною шкалою: 1 бал відповідає незначному впливу, що зумовлює зниження маржинальності менш ніж на 5 %; 2 бали – помірному впливу в межах 5–15 %; 3 бали – суттєвому впливу, який може спричинити втрати на рівні 16–30 % і тимчасові перебої в діяльності; 4 бали – критичному впливу, що характеризується втратами в межах 31–50 % та можливим скороченням частки ринку; 5 балів – катастрофічному впливу, який створює загрозу банкрутства підприємства або повного припинення його діяльності.

Оскільки дослідження має макрорівневий характер стосовно українського бізнесу загалом, бали присвоювалися не на основі первинних опитувань конкретного підприємства, а шляхом узагальнення вторинних аналітичних даних: звітів Світового банку, аналітики НБУ, звітів стосовно кіберзагроз та баз даних міжнародних страхових компаній. Результати розрахунку інтегрального показника наведено у табл. 3.

Оцінювання ризиків здійснювалося з урахуванням двох ключових параметрів – ймовірності їх настання та сили впливу на функціонування підприємства. Визначення рівнів ризику ґрунтувалося на аналізі актуальних аналітичних матеріалів, статистичних даних і прогностичних оцінок міжнародних та національних інституцій.

Таблиця 3 – Ймовірність, вплив та рівень критичності глобальних ризиків для підприємств України (складено автором на основі [4-7])

Код ризику	Категорія	Ймовірність (1–5)	Вплив (1–5)	Інтегральний бал	Рівень критичності
R-001	Геополітичні	5	5	25	високий
R-002	Енергетичні	4	5	20	високий
R-003	Логістичні	4	4	16	середній
R-004	Фінансово-економічні	4	4	16	середній
R-005	Кібернетичні	5	4	20	високий
R-006	Регуляторні	3	3	9	низький
R-007	Кліматичні та екологічні	3	3	9	низький
R-008	Кадрові та соціальні	4	4	16	середній

Геополітичні ризики (R-001) віднесено до категорії ризиків з найвищим рівнем ймовірності та впливу. Така оцінка зумовлена тривалим характером бойових дій, їх системним впливом на економічне середовище, руйнуванням виробничих активів, інфраструктури та порушенням господарських зв'язків. Катастрофічний характер наслідків підтверджується, зокрема, результатами оцінювання збитків і потреб на відновлення України, наведеними у звіті RDNA4 [7].

Енергетичні ризики (R-002) оцінено як високі за ймовірністю реалізації та критичні за ступенем впливу. Це пояснюється системним дефіцитом генеруючих потужностей, нестабільністю енергопостачання та високою залежністю виробничих процесів від безперервного доступу до енергоресурсів. За окремих умов їх вплив може набувати катастрофічного характеру, особливо для енергоємних видів діяльності [5].

Кібернетичні ризики (R-005) визначено як такі, що мають високу ймовірність настання та критичний рівень впливу. За оцінками Allianz, кібератаки залишаються одним з найбільш значущих глобальних ризиків для бізнесу. В умовах посилення цифровізації управлінських, комунікаційних і виробничих процесів реалізація таких ризиків може спричиняти суттєві порушення операційної діяльності, втрату даних, зниження рівня інформаційної безпеки та фінансові втрати [8].

Логістичні ризики (R-003) характеризуються високою ймовірністю виникнення, що зумовлено ускладненням транспортного сполучення, затримками постачання та зростанням витрат на перевезення. Водночас ступінь їхнього впливу оцінено нижче порівняно з геополітичними та енергетичними ризиками, оскільки частина підприємств адаптувала логістичні моделі шляхом диверсифікації маршрутів і переорієнтації на альтернативні напрями постачання [4].

Фінансові ризики (R-004) оцінено як значущі, проте відносно прогнозовані. Їх формування пов'язане з інфляційними процесами, валютними коливаннями, зміною вартості кредитних ресурсів і загальною макрофінансовою нестабільністю. Водночас наявність прогнозів Національного банку України, а також застосування

підприємствами інструментів часткового хеджування й адаптації фінансової політики дає змогу певно знижувати негативний вплив цієї групи ризиків.

Кадрові ризики (R-008) оцінено як суттєві за впливом, оскільки дефіцит трудових ресурсів, зумовлений міграційними процесами, мобілізацією та структурними дисбалансами на ринку праці, безпосередньо обмежує операційну стійкість підприємств. Їх реалізація ускладнює підтримання безперервності бізнес-процесів, знижує адаптивність організації та стримує інноваційний розвиток.

Регуляторні ризики (R-006) визначено як помірні за силою впливу. Це пояснюється поступовим характером імплементації європейських норм і стандартів, що надає суб'єктам господарювання певний час для організаційної та ресурсної адаптації. У короткостроковому періоді вплив цієї групи ризиків на ліквідність і поточну стабільність підприємств не є визначальним, однак у середньо- та довгостроковій перспективі їх значення зростатиме.

Кліматичні ризики (R-007) у короткостроковому часовому горизонті оцінено як відносно обмежені для більшості видів економічної діяльності. Водночас для окремих секторів, насамперед агропромислового комплексу, їх вплив є значно вищим через пряму залежність результатів діяльності від природно-кліматичних умов. Отже, сила впливу кліматичних ризиків має галузево диференційований характер [6].

Результати оцінювання ризиків (табл. 3) свідчать, що пріоритетним напрямом управлінського впливу для підприємств має бути нейтралізація ризиків високої критичності, зокрема геополітичних, енергетичних та кібернетичних. Оскільки уникнення таких макроризиків є об'єктивно неможливим, основний акцент має бути зміщено у площину зниження інтенсивності їх негативного впливу через підвищення рівня організаційної гнучкості, адаптивності та резильєнтності підприємства. В цих умовах цифрова трансформація набуває значення стратегічного інструменту забезпечення безперервності діяльності та підвищення ефективності ризик-орієнтованого управління. У цьому зв'язку мето-

дично доцільним є групування цифрових інструментів не за ознакою конкретних програмних рішень, а за їх функціональним призначенням, що дає змогу вибудувати комплексну архітектуру безпеки підприємства незалежно від вибору окремих технологічних платформ. До основних функціональних груп таких інструментів належать:

1. *Системи підтримки прийняття рішень та прогностичної аналітики.* Для управління геополітичними та фінансовими ризиками принципове значення має перехід від реактивного до випереджального управління. Сучасні аналітичні системи та інструменти на основі штучного інтелекту забезпечують можливість сценарного моделювання, аналізу значних масивів макроекономічних даних і проведення стрес-тестування фінансових моделей підприємства. Це дає змогу завчасно виявляти потенційні касові розриви, оцінювати альтернативні сценарії розвитку подій та оптимізувати розподіл фінансових ресурсів в умовах невизначеності [3].

2. *Платформи інтеграції та прозорості ланцюгів постачання.* Зниження логістичних ризиків (R-003) значно забезпечується завдяки впровадженню сучасних цифрових рішень, зокрема хмарних платформ управління логістикою та технологій розподілених реєстрів. Зазначені інструменти формують наскрізну прозорість руху товарів, підвищують рівень контролю над постачальницькими процесами та дають змогу оптимізувати маршрути в режимі реального часу з урахуванням геополітичних обмежень. У результаті знижується ймовірність поширення негативних наслідків порушень постачання на суміжні ланки логістичної системи [2].

3. *Засоби моніторингу та децентралізації інфраструктури.* Управління критичними енергетичними ризиками (R-002) потребує застосування комплексних апаратно-програмних рішень. Застосування інтелектуальних датчиків забезпечує детальний моніторинг параметрів енергоспоживання, а інтеграція отриманих даних із системами енергоменеджменту підвищує оперативність і точність управлінського реагування. Водночас перехід до локальних енергомереж із використанням відновлюваних джерел енергії створює умови для автоматичного балансування навантаження та підтримання автономності функціонування підприємства в умовах перебоїв електропостачання [5].

4. *Системи інформаційної безпеки та кіберстійкості.* Високий рівень кіберризиків (R-005) зумовлює необхідність переходу від фрагментарних засобів захисту до комплексної архітектури інформаційної безпеки, побудованої на принципах «нульової довіри». Важливу

роль у цій системі відіграють рішення з управління подіями інформаційної безпеки, які забезпечують централізований збір і аналіз даних з усієї IT-інфраструктури, а також автоматизовані центри реагування, що дають змогу своєчасно виявляти, локалізувати та нейтралізувати кіберзагрози на ранніх етапах їх реалізації [8].

5. *Системи нормативної відповідності та управління персоналом.* Для зниження кадрових (R-008) і регуляторних (R-006) ризиків доцільним є використання спеціалізованих цифрових платформ. Системи управління персоналом забезпечують автоматизацію процесів підбору, перекваліфікації, утримання працівників і координації роботи розподілених команд. Одночасно платформи екологічного, соціального та управлінського спрямування забезпечують автоматизований збір даних і формування звітності відповідно до нових європейських вимог, що сприяє зниженню ризику фінансових санкцій, репутаційних втрат і втрати доступу до зовнішніх ринків [13].

Так, логіка побудови системи управління полягає в тому, що результати кількісного оцінювання ризиків безпосередньо диктують пріоритетність інвестицій у відповідні функціональні групи ЦТ, формуючи цілісний механізм стійкості підприємства [14].

ВИСНОВКИ

У результаті проведеного дослідження систематизовано ключові глобальні ризики для українських підприємств. Встановлено, що в сучасних умовах бізнес стикається з багатовимірною системою загроз, де найвищий рівень критичності демонструють геополітичні, енергетичні та кібернетичні ризики.

Запропоновано комплексний підхід до управління глобальними ризиками підприємств України, що базується на впровадженні п'яти функціональних груп ЦТ: систем прогностичної аналітики, платформ прозорості ланцюгів постачання, IoT-моніторингу інфраструктури, архітектури кіберрезилієнтності та систем комплаєнсу. Доведено, що цифрова трансформація є не просто інструментом оптимізації, а базовою передумовою виживання та збереження безперервності бізнесу в умовах воєнного стану.

Обмеженням дослідження є макрорівневий характер оцінювання, що не враховує галузеву специфіку. Перспективи подальших досліджень пов'язані з проведенням емпіричних опитувань підприємств для формування галузевих профілів ризику та оцінювання ефективності впровадження цифрових антиризикових інструментів.

Список використаних джерел

1. Prewett K., Terry A. COSO's Updated Enterprise Risk Management Framework – A Quest for Depth and Clarity. *Journal of Corporate Accounting & Finance*. 2018. Vol. 29, No. 3. pp. 16–23. DOI: 10.1002/jcaf.22346
2. Ivanov D., Dolgui A., Sokolov B. The Impact of Digital Technology and Industry 4.0 on the Ripple Effect and Supply Chain Risk Analytics. *International Journal of Production Research*. 2019. Vol. 57, No. 3. pp. 829–846. DOI: 10.1080/00207543.2018.1488086
3. Лозан А.Е. Digital enabling of innovation management: implementation at the enterprise. *Modern Digital Technologies and Developments: Problems of Their Use and Challenges: Abstracts of VII International Scientific and Practical Conference (Stockholm, February 16-18, 2026)*. URL: <https://eu-conf.com/wp-content/uploads/2025/12/MODERN-DIGITAL-TECHNOLOGIES-AND-DEVELOPMENTS-PROBLEMS-OF-THEIR-USE-AND-CHALLENGE.pdf>
4. Чмутова І., Гайналій А. Оцінка глобальних ризиків з позицій управління безпекою підприємств України. *Вісник Хмельницького національного університету. Серія: Економічні науки*. 2024. Т. 336, № 6. С. 506–514. DOI: 10.31891/2307-5740-2024-336-77
5. Лозан А.Е. Адаптація цифрових інструментів менеджменту в умовах глобальної нестабільності. *Evolving Science: Theories, Discoveries and Practical Outcomes: матеріали наук.-практ. конф.*, (Цюріх, 8 верес. 2025 р.). Цюріх, 2025. URL: https://www.eoss-conf.com/wp-content/uploads/2025/09/Zurich_Switzerland_08.09.25.pdf
6. The Global Risks Report 2024. 19th ed. Geneva: World Economic Forum, 2024. URL: <https://www.weforum.org/publications/global-risks-report-2024/>

7. Ukraine Fourth Rapid Damage and Needs Assessment (RDNA4): February 2022–December 2024. Washington, DC: World Bank, 2025. URL: <https://openknowledge.worldbank.org/entities/publication/0f04dfe0-41ea-410f-bdd9-4d2bc9d40569>
8. Allianz Risk Barometer 2024. Allianz Commercial, 2024. URL: <https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>
9. Assessment of the Impact of the War on Micro-, Small-, and Medium-sized Enterprises in Ukraine. United Nations Development Programme in Ukraine, 2024. URL: <https://www.undp.org/ukraine/publications/assessment-wars-impact-micro-small-and-medium-enterprises-ukraine>
10. Alkema V., Hryhoruk P., Skhidnytska H., Sylkin O. Resilience and Strategic Management: Ways to Ensure Economic and Social Security of Ukrainian Enterprises during Long-Term Warfare. *Clio. Revista de Historia, Ciencias Humanas y Pensamiento Crítico*. 2025. Vol. 5, No. 9. pp. 740–767. DOI: 10.5281/zenodo.14567109
11. Lemmens S.M.P. et al. The Risk Matrix Approach: A Helpful Tool Weighing Probability and Impact when Deciding on Preventive and Diagnostic Interventions. *BMC Health Services Research*. 2022. Vol. 22, No. 1. Article 218. DOI: 10.1186/s12913-022-07484-7
12. Efe A. A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31000, COBIT. *Denetim ve Gvence Hizmetleri Dergisi*. 2023. Vol. 3, No. 2. pp. 185–205. URL: <https://dergipark.org.tr/en/pub/audas/article/1291915>
13. Moreira A., Rodrigues A.C., Ferreira M.R. Where Is Human Resource Management in Sustainability Reporting? ESG and GRI Perspectives. *Sustainability*. 2025. Vol. 17, No. 7. Article 3033. DOI: 10.3390/su17073033
14. Лозан А.Е. Інтеграція цифрових рішень в управління інноваційним розвитком підприємств. *Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії: матеріали наук.-практ. конф.* 2025. URL: https://duikt.edu.ua/uploads/p_2779_50068458.pdf

References

1. Prewett K., Terry A. COSO's Updated Enterprise Risk Management Framework – A Quest for Depth and Clarity. *Journal of Corporate Accounting & Finance*. 2018. Vol. 29, No. 3. pp. 16–23. DOI: 10.1002/jcaf.22346
2. Ivanov D., Dolgui A., Sokolov B. The Impact of Digital Technology and Industry 4.0 on the Ripple Effect and Supply Chain Risk Analytics. *International Journal of Production Research*. 2019. Vol. 57, No. 3. pp. 829–846. DOI: 10.1080/00207543.2018.1488086
3. Лозан А.Е. Digital enabling of innovation management: implementation at the enterprise. *Modern Digital Technologies and Developments: Problems of Their Use and Challenges: Abstracts of VII International Scientific and Practical Conference (Stockholm, February 16-18, 2026)*. URL: <https://eu-conf.com/wp-content/uploads/2025/12/MODERN-DIGITAL-TECHNOLOGIES-AND-DEVELOPMENTS-PROBLEMS-OF-THEIR-USE-AND-CHALLENGE.pdf>
4. Chmutova I., Hainalii A. Otsinka hlobalnykh ryzykiv z pozytsii upravlinnia bezpekoiu pidpriemstv Ukrainy. *Herald of Khmelnytskyi National University. Economic Sciences*. 2024. Vol. 336, No. 6. pp. 506–514. DOI: 10.31891/2307-5740-2024-336-77 (in Ukrainian).
5. Lozan A.E. Assessment of global risks from the perspective of security management of Ukrainian enterprises. *Evolving Science: Theories, Discoveries and Practical Outcomes: proceedings of the scientific and practical conference*. (Zurich, September 8, 2025). Zurich, 2025. URL: https://www.eoss-conf.com/wp-content/uploads/2025/09/Zurich_Switzerland_08.09.25.pdf (in Ukrainian).
6. The Global Risks Report 2024. 19th ed. Geneva: World Economic Forum, 2024. URL: <https://www.weforum.org/publications/global-risks-report-2024/>
7. Ukraine Fourth Rapid Damage and Needs Assessment (RDNA4): February 2022–December 2024. Washington, DC: World Bank, 2025. URL: <https://openknowledge.worldbank.org/entities/publication/0f04dfe0-41ea-410f-bdd9-4d2bc9d40569>
8. Allianz Risk Barometer 2024. Allianz Commercial, 2024. URL: <https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>
9. Assessment of the Impact of the War on Micro-, Small-, and Medium-sized Enterprises in Ukraine. United Nations Development Programme in Ukraine, 2024. URL: <https://www.undp.org/ukraine/publications/assessment-wars-impact-micro-small-and-medium-enterprises-ukraine>
10. Alkema V., Hryhoruk P., Skhidnytska H., Sylkin O. Resilience and Strategic Management: Ways to Ensure Economic and Social Security of Ukrainian Enterprises during Long-Term Warfare. *Clio. Revista de Historia, Ciencias Humanas y Pensamiento Crítico*. 2025. Vol. 5, No. 9. pp. 740–767. DOI: 10.5281/zenodo.14567109
11. Lemmens S.M.P. et al. The Risk Matrix Approach: A Helpful Tool Weighing Probability and Impact when Deciding on Preventive and Diagnostic Interventions. *BMC Health Services Research*. 2022. Vol. 22, No. 1. Article 218. DOI: 10.1186/s12913-022-07484-7
12. Efe A. A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31000, COBIT. *Denetim ve Gvence Hizmetleri Dergisi*. 2023. Vol. 3, No. 2. pp. 185–205. URL: <https://dergipark.org.tr/en/pub/audas/article/1291915>
13. Moreira A., Rodrigues A.C., Ferreira M.R. Where Is Human Resource Management in Sustainability Reporting? ESG and GRI Perspectives. *Sustainability*. 2025. Vol. 17, No. 7. Article 3033. DOI: 10.3390/su17073033
14. Lozan A.E. Integration of digital solutions in the management of innovative development of enterprises. *Modern aspects of digitalization and informatization in software and computer engineering*. 2025. URL: https://duikt.edu.ua/uploads/p_2779_50068458.pdf (in Ukrainian).

Andrii LOZAN

applicant, Odesa Polytechnic National University

ORCID: <https://orcid.org/0009-0009-2808-6217>

e-mail: andlozedd@gmail.com

GLOBAL RISKS AFFECTING UKRAINIAN ENTERPRISES: ASSESSMENT AND PROSPECTS FOR MANAGEMENT

Under conditions of global instability, Ukrainian enterprises operate in an environment shaped by the simultaneous influence of military, energy, financial, logistical, climatic, regulatory and digital risks. The interaction of these factors forms a multidimensional system of threats that directly affects business resilience, competitiveness, operational continuity, and the capacity for innovative development. The purpose of the paper is to systematize the key global risks faced by Ukrainian enterprises, formalize approaches to their quantitative assessment, and substantiate directions for effective management through the functional application of digital technologies. The methodological basis of the study is the development of a risk register using the “probability × impact” matrix, grounded in the principles of COSO ERM and ISO 31000, as well as a comparative analysis of international reports, analytical materials, and scientific literature. The study identifies 8 groups of risks: geopolitical, energy, logistical, financial and economic, cyber, regulatory, climatic and environmental, and personnel and social risks. The highest level of criticality is attributed to geopolitical, energy, and cyber risks, since their realization may cause systemic disruptions to production, infrastructure, data security, and business continuity. The paper proposes a comprehensive approach to risk mitigation based on five groups of digital tools: decision-support and predictive analytics systems, supply chain transparency platforms, infrastructure monitoring and decentralization tools, cybersecurity and cyber-resilience systems, and compliance and human resource management platforms. The practical value of the study lies in the formation of an integrated risk register that supports managerial decision-making and strengthens business-model resilience. The scientific novelty consists in the development of a comprehensive approach to the quantitative assessment of Ukraine-specific wartime risks with the functional grouping of digital instruments for their mitigation, thereby forming a holistic mechanism for ensuring the economic security and strategic adaptability of enterprises.

Keywords: global risks, risk management, Ukrainian enterprises, digital technologies, risk register, business resilience, strategic adaptation