

DOI: <https://doi.org/10.32782/2524-0072/2024-62-22>

УДК 338.24.01

# БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ В УКРАЇНІ: ВИКЛИКИ ТА МОЖЛИВОСТІ В УМОВАХ ВІЙНИ

## BUSINESS CONTINUITY IN UKRAINE: CHALLENGES AND OPPORTUNITIES IN WARTIME

**Ситайло Уляна Василівна**доктор філософії, асистент кафедри,  
Київський національний університет імені Тараса Шевченка  
ORCID: <https://orcid.org/0000-0001-6013-2580>**Sytailo Uliana**

Taras Shevchenko National University of Kyiv

У статті досліджено питання безперервності бізнесу в умовах загострення глобальних викликів, зокрема збройної агресії РФ проти України. Уточнено сутність поняття «стійкість бізнесу» та його компоненти. Наведено ключову відмінність між стійкістю та безперервністю бізнесу у розрізі підходу до реагування на виклики. Визначено чотири основні категорії загроз, що перешкоджають безперебійному функціонуванню українських підприємств, серед яких: антропогенні (випадкові та навмисні), технологічні, біологічні та стихійні лиха. Проаналізовано поточний стан вразливості України щодо актуальних загроз відповідно до рейтингів «Індекс крихких держав» та INFORM Ризик. На основі потенційних загроз запропоновано перелік інструментів їх мінімізації та забезпечення безперебійної роботи бізнесу в умовах воєнної агресії РФ.

**Ключові слова:** стійкість, безперервність бізнесу, загрози, російська військова агресія.

The article is devoted to highlighting the current state of Ukraine in the context of vulnerability to current challenges and identifying key tools to minimize threats to business continuity in the context of Russian military aggression. The essence of the concept of 'business resilience' and its components, including risk management, adaptability and flexibility, and business continuity planning for critical functions, are clarified. The key difference between business resilience and business continuity in terms of the approach to tackling challenges is elucidated. The article identifies four main categories of threats that impede the uninterrupted functioning of Ukrainian enterprises, including anthropogenic (accidental and intentional), technological, biological, and natural disasters. The current state of Ukraine's vulnerability to current threats according to the Fragile States Index and INFORM Risk ratings is analyzed. It has been noted that in 2023, Ukraine was classified as having a 'high' risk level. Thus, the author notes a significant deterioration in the level of state stability in the overall Fragile States Index rating in 2023. The key threats to business continuity in Ukraine are identified, including loss of personnel due to dismissal, illness or death, loss of fixed assets or access to them, power outages, disruptions and interference with information technology systems, and disruption of supply chain integrity. Based on the potential threats, the author proposes a list of tools for minimizing them and ensuring continuous business operations in the context of Russia's military aggression. It is noted that the specific choice of tools depends on the specifics of the enterprise, its industry, and market conditions. The positive effect of the implementation of the proposed tools for minimizing threats to business continuity on the sustainability and long-term development of Ukrainian enterprises is determined. The author has emphasized that the key factors for the successful implementation and maintenance of an effective business continuity system are a systematic approach, synergy of efforts, and continuous investment.

**Key words:** sustainability, business continuity, threats, Russian military aggression.

**Постановка проблеми.** Трансформація світу від формату VUCA (нестабільний, невизначений, складний, неоднозначний) до нового SHIVA (розщепленого, жахливого, незбагненного, жорстокого, такий, що зароджується) ставить перед організаціями по всьому світу низку серйозних викликів, зму-

шуючи їх керівництво переглядати стратегії та адаптуватися до нових реалій. Особливо це стосується України, яка з 2014 року зіткнулася з низкою викликів, таких як війна на Донбасі, анексія Криму, пандемія COVID-19 та повномасштабне вторгнення Росії у 2022 році. Останнє загострило не тільки геополітичну та

економічну поляризацію, але й суттєво посилює загрози для глобальної стабільності у цілому. Відтак, український бізнес стикається з необхідністю пошуку та впровадження дієвих інструментів безперервності бізнесу, які б враховували поточні виклики та могли б забезпечити стабільне функціонування підприємств у мінливих умовах.

#### **Аналіз останніх досліджень і публікацій.**

Дослідженню актуальних викликів та можливостей стійкості бізнесу в часи турбулентності присвячено працю Х. Руко, П. Фігейредо [1]. Разом з тим, питання забезпечення безперервності бізнесу (ББ) актуалізувалась у контексті впливу COVID-19 на глобальні операції та економіку загалом. Так, у праці М. Барського [2] приділено увагу питанню управління безперервністю бізнесу у контексті ланцюгів постачання з висвітленням впливу ключових ризиків на діяльність компаній. Дж. Баз та С. Руель [3] емпірично доводять, що ефективні практики ББ покращують стійкість до перебоїв в ланцюзі поставок та фінансових труднощів. У свою чергу, Т. Хол [4] розкриває проблему «ілюзії готовності» організацій до раптових викликів, підкреслюючи важливість не лише формальних планів, але й гнучкої адаптації та культури стійкості. У науковій праці

**Виділення невирішених раніше частин загальної проблеми.** Проте, попри значний науковий внесок у розуміння стійкості бізнесу в часи турбулентності, існує дефіцит досліджень, які б фокусувалися на важливості безперервності бізнесу в Україні в умовах викликів, спричинених вторгненням росії на територію держави.

**Формулювання цілей статті.** Метою дослідження є висвітлення поточного стану України в контексті вразливості щодо актуальних викликів та визначення ключових інструментів мінімізації загроз безперервності бізнесу в умовах воєнної агресії рф.

**Виклад основного матеріалу дослідження.** Згідно з результатами щорічного дослідження BCI Horizon Scan 2023 [5], що проводиться Інститутом безперервності бізнесу, до потенційних ризиків, з якими організація можуть зіткнутися у 2024 році, відносяться кібератаки, екстремальні погодні явища, ІТ та телекомунікаційні збої, збільшення вартості життя, а також перебоїв в енергопостачанні. Будь-яка комбінація вище зазначених ризиків може загрожувати критично важливим бізнес-операціям, що, у свою чергу, актуалізує необхідність розроблення та впровадження

комплексних стратегій стійкості для мінімізації ризиків та забезпечення безперебійної роботи.

Відповідно до Стандарту ISO 22301:2019 [6] стійкість бізнесу (СБ) визначається як здатність організації адаптуватися до середовища загроз, що постійно змінюється, і надавати продукти чи послуги під час збоїв, які загрожують статус-кво. З точки зору довгострокової перспективи, стійкість бізнесу виступає як стратегія, спрямована на підготовку суб'єкта господарювання до протистояння можливим потрясінням у майбутньому у розрізі таких основних компонентів:

- управління ризиками, що включає в себе ідентифікацію потенційних ризиків та вразливостей, оцінку їх ймовірності та впливу, а також розробку та впровадження відповідних стратегій реагування. Це дає змогу організаціям проактивно готуватися до потенційних збоїв та мінімізувати їх негативні наслідки;
- адаптивність і гнучкість. У динамічному бізнес-середовищі постійна готовність до прийняття нових ідей, технологій та методів роботи зумовлює підвищення ефективності та конкурентоспроможності;
- планування безперервності критично важливих функцій під час збоїв, надзвичайних ситуацій чи стихійних лих.

Слід зазначити, що основною відмінністю між стійкістю та безперервністю бізнесу є підхід до реагування на кризу. Безперервність бізнесу реалізує реактивний підхід, який фокусується на швидкому реагуванні на фактичні збої в роботі організації в режимі реального часу. У свою чергу, стійкість бізнесу полягає в проактивній здатності суб'єкта господарювання протистояти, відновлюватися та адаптуватися до широкого кола проблем, збоїв і змін.

Таким чином, управління безперервністю бізнесу полягає у реагуванні на фактичні перебої, у той час як стійкість бізнесу вимагає послідовного планування сценаріїв і регулярного навчання, щоб підготуватися до ймовірних типів порушень.

Безперервність бізнесу спрямована на підготовку організації до протистояння потенційним загрозам, які можуть загрожувати її основній місії та здатності безперебійно постачати продукти та послуги протягом прийнятних часових рамок із заздалегідь визначеною потужністю.

Таким чином, можна визначити чотири основні категорії загроз, що перешкоджають безперебійному функціонуванню українських підприємств, а саме:

– антропогенні (випадкові та навмисні). Деякі загрози антропогенного характеру зводяться до людської помилки, як-от руйнування конструкцій, дефіцит ресурсів, розлив матеріалів, транспортні інциденти, вибухи/пожежі або відсутність основних працівників. Однак, інколи загрози, спричинені людиною, є навмисними, на кшталт підпалів, переслідувань, крадіжок, вандалізму, терористичних актів та воєнних дій. Більшість випадкових антропогенних ризиків можна уникнути або пом'якшити за допомогою комплексного моніторингу і ретельного використання стандартів, тоді як навмисні антропогенні ризики, як правило, важче передбачити та мінімізувати.

– Технологічні загрози. Зростаюча залежність суспільства від технологій зумовлює появу та поширення низки ризиків, серед яких: кібератаки, поломки обладнання, переривання з'єднання з мережею, збої програмного забезпечення, електропостачання тощо.

– Стихійні лиха (геологічного та метеорологічного характеру). Так, геологічні ризики включають обвали, зсуви, землетруси, а метеорологічні – зливи, сильні снігопади, повені тощо. Оскільки природні явища неможливо контролювати, підприємства повинні бути готові до будь-якого сценарію.

– Біологічні загрози. Ця категорія включає інфекційні хвороби/пандемії, які зазвичай вимагають широкомасштабної та всеосяжної відповіді щодо обмеження їх поширення. Тривалі наслідки даної категорії ризику можуть вплинути на бізнес на всіх рівнях, від ланцюга постачань і персоналу до спожива-

чів і торгових посередників. Так, пандемія COVID-19 є актуальним прикладом великомасштабної події під назвою «Чорний лебідь», яка поставила під загрозу майже кожен бізнес у більшості галузей. Варто зазначити, що на початку 2020 року відповідно до звіту Всесвітнього економічного форуму «Глобальні ризики 2020» [7] ризик поширення інфекційних захворювань за ймовірністю виникнення посідав 27 сходинку у загальному рейтингу глобальних ризиків і тільки 10 позицію – за своїх негативним впливом.

Тенденції вразливості до загроз відображені у щорічному рейтингу Фонду миру (FFP) «Індекс крихких держав» (FSI) [8], що формується на основі чотирьох груп індикаторів – згуртованості, економічній, політичній та соціальній. Так, у загальному рейтингу 178 країн світу Україна посіла 18 сходинку (значення індексу – 95,9), суттєво піднявшись на 74 позиції у порівнянні з 2022 роком (індекс – 68,6). Зазначимо, що оцінки FSI слід інтерпретувати за принципом «чим нижча оцінка, тим краще», тому зростання оцінки вказує на погіршення стабільності. Індекс крихких держав є критично важливим інструментом для висвітлення не лише нормального тиску, який відчувають усі держави, але й для визначення того, коли цей тиск переважає здатність держави справлятися з ним.

У свою чергу, згідно з індексом INFORM [9] позиції України значно погіршилися після 2014 року внаслідок початку війни на сході країни, і відтоді не опускались нижче 60 сходинки серед рейтингу 191 країн світу.

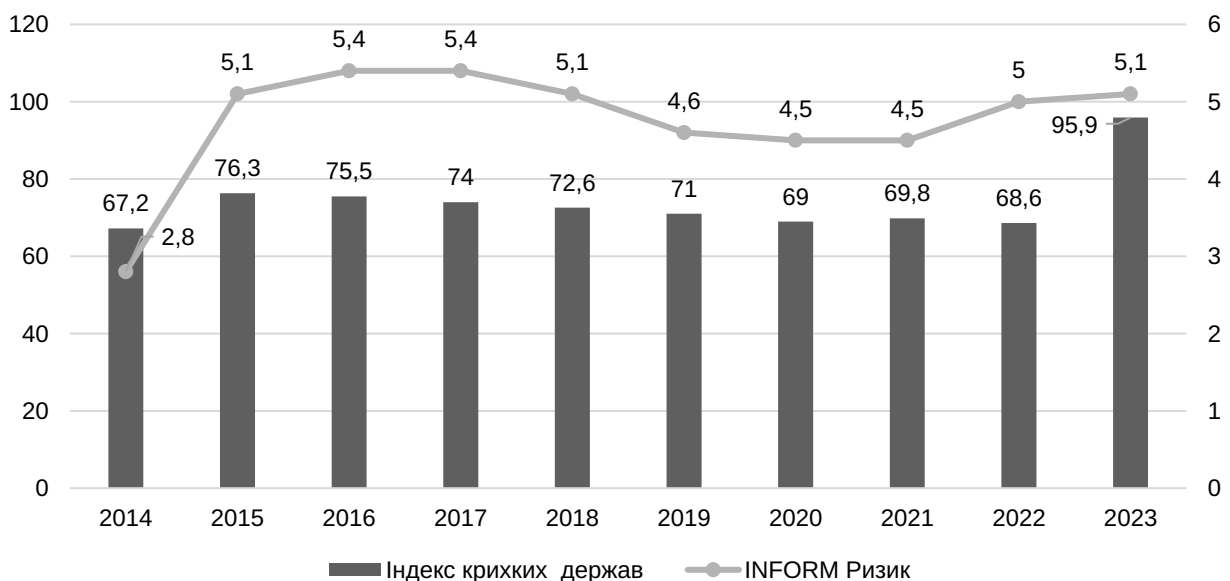


Рис. 1. Україна у рейтингах «Індекс крихких держав» та INFORM Ризик

Джерело: складено автором на основі [8; 9]

У 2023 році Україна класифікована із «високим» рівнем ризику, що підтверджується 33 місцем у рейтингу (значення індексу – 5,1). Для порівняння, Румунія посідає 132 сходинку (індекс 2,6), а Польща – 139 позицію (індекс 2,5). Зазначимо, що індекс INFORM враховує 143 фактори, що групуються в 11 категорій, та надає оцінку ризиків в п'яти сферах: політичній, економічній, фінансовій, соціальній та екологічній. Зрештою, він врівноважує дві основні сили: небезпеки та ризику (природного та антропогенного походження), з одного боку, і вразливість спільноти та відсутність здатності країни їх долати з точки зору офіційних, організованих заходів і зусиль уряду.

Таким чином, сучасні умови ведення бізнесу в Україні характеризуються високим рівнем невизначеності та динамічністю зовнішнього середовища. Це обумовлено виникненням низки загроз, які можуть суттєво вплинути на безперервну роботу суб'єктів господарювання. Для ефективної протидії

цим загрозам українським підприємствам рекомендується застосовувати інструменти з їх мінімізації (табл. 1), конкретний вибір яких залежить від специфіки підприємства, його галузі діяльності та ринкових умов.

Впровадження запропонованих інструментів мінімізації загроз безперервності бізнесу може мати значний позитивний вплив на стійкість та довгостроковий розвиток українських підприємств, зокрема, шляхом:

- мінімізації простою та фінансових втрат (полягає у розробці планів, процесів і технологій для швидкого відновлення критичних операцій (виробництво, постачання, обслуговування клієнтів, фінансові транзакції тощо), запобігаючи тривалим перервам);

- захисту даних, систем і активів (регулярне резервне копіювання даних, резервна інфраструктура та заходи кібербезпеки є критично важливими для зменшення втрати даних і підтримки операційної цілісності);

- збереження репутації (безперервність бізнесу підтримує зобов'язання та рівень

Таблиця 1

## Інструменти мінімізації загроз безперервності бізнесу в Україні

Загроза	Інструмент мінімізації загрози	Опис
1	2	3
Втрата персоналу внаслідок звільнення, захворювання або смерті	Інвентаризація навичок персоналу	Збір та аналіз інформації про навички, знання та досвід співробітників для виявлення потенційних резервів
	Перехресне навчання	Навчання декількох співробітників виконувати одні й ті ж завдання.
	Документування процесів	Систематичний запис та опис послідовних кроків, необхідних для виконання певного завдання чи досягнення певного результату.
	Планування спадкоємності	Підготовки організації до заміни ключових співробітників
	Використання сторонньої підтримки	Залучення зовнішніх компаній або фахівців, підкріплене контрактними угодами, для виконання певних завдань чи функцій
Втрата основних засобів чи доступу до них	Внутрішнє переміщення персоналу	Переміщення персоналу в інше приміщення, що належить організації
	Віддалена робота	Забезпечення можливості роботи персоналу з дому або інших місць (коворкінги, антикризові центри)
	Релокація бізнесу	Переміщення суб'єкта господарювання (повне або часткове) в більш сприятливе географічне середовище з метою продовження його функціонування
Перебої енергопостачання	Забезпечення резервного електропостачання	Встановлення джерел безперебійного живлення (ДБЖ) та генераторів

Продовження Таблиці 1

1	2	3
Збої та втручання в інформаційно-технологічні системи	Підтримка тієї самої технології в різних місцях	Використання однакових технологічних рішень, таких як програмне забезпечення, обладнання та інфраструктура, в декількох локаціях
	Зберігання старого обладнання	Створення резерву старого обладнання для екстреної заміни або запасних частин
	Кібербезпека	Заходи, спрямовані на захист комп'ютерних систем, мереж та даних від несанкціонованого доступу, використання, порушення їх роботи або знищення (хмарне резервне копіювання, шифрування, контроль доступу тощо)
Порушення цілісності ланцюгів постачання	Диверсифікація постачальників	Співпраця з декількома постачальниками для отримання товарів або послуг
	Визначення резервних маршрутів	Пошук альтернативних логістичних сполучень та способів доставки
	Створення резервних запасів	Зберігання запасів ключових товарів або компонентів
	Вимога підтвердження здатності безперервності	Заохочення або вимога до постачальників мати підтвержену здатність безперервності бізнесу

Джерело: складено автором

обслуговування, зміцнюючи впевненість та довіру стейкхолдерів. У свою чергу, своєчасна комунікація та прозорість демонструють готовність до подальшої співпраці);

– забезпечення конкурентної переваги (здатність швидко адаптуватися до мінливих умов ринку та нових викликів є запорукою успіху в довгостроковій перспективі).

Однак, важливо зазначити, що впровадження та підтримка ефективної системи безперервності бізнесу – це комплексний процес, що потребує системного підходу та синергії зусиль з боку всіх зацікавлених сторін – як керівництва, так і персоналу, зокрема. Це зумовлено багатогранністю системи ББ, яка охоплює широкий спектр елементів, від ідентифікації ризиків до навчання персоналу та тестування планів реагування. Успішне впровадження та підтримка ББ вимагають чіткої стратегії, інтеграції з іншими системами

управління та постійного вдосконалення. Системний підхід, синергія зусиль та постійні інвестиції є ключовими факторами успішного впровадження та підтримки дієвої системи ББ, яка може допомогти підприємствам протистояти надзвичайним ситуаціям та забезпечити безперервну роботу.

**Висновки.** Сучасні реалії ведення бізнесу в Україні вимагають системного підходу до формування та впровадження комплексної стратегії стійкості, яка ґрунтується на плануванні безперервності роботи. Управління безперервністю бізнесу відіграє фундаментальну роль у цій стратегії, гарантуючи економічну безпеку, внутрішню координацію та підкреслюючи соціальну відповідальність компанії. Перспективи подальших наукових досліджень полягають у проведенні аналізу впливу російсько-української війни на рівень стійкості європейських держав.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Rouco J. C., Figueiredo P. C. Business Continuity Management and Resilience: Theories, Models, and Processes. IGI Global, 2024. 360 p.
2. Барський М. В. Безперервність бізнесу в контексті ланцюгів постачання. *Сталий розвиток економіки*. 2024. № 1(48). С. 302–308. DOI: <https://doi.org/10.32782/2308-1988/2024-48-42>
3. Baz J. E., Ruel S. Investigating the role of business continuity during COVID-19: an empirical examination. *Supply Chain Forum*. 2023. P. 1–14. DOI: 10.1080/16258312.2023.2199127.
4. Hall T. Business continuity beyond COVID-19: Lessons learned and the 'illusion of preparedness'. *Journal of Business Continuity & Emergency Planning*, 2022. Volume 16. Number 1. P. 45–52.

5. BCI Horizon Scan Report 2023. *The Business Continuity Institute (BCI)*. URL: <https://www.thebci.org/resource/bci-horizon-scan-report-2023.html>
6. ISO 22301. Security and resilience – Business continuity management systems – Requirements. URL: [https://pttweb7.pttplc.com/pttbcm/upload/media/878\\_ISO22301\\_2019.pdf](https://pttweb7.pttplc.com/pttbcm/upload/media/878_ISO22301_2019.pdf)
7. The Global Risks Report 2020. *The World Economic Forum*. URL: [https://www3.weforum.org/docs/WEF\\_Global\\_Risk\\_Report\\_2020.pdf](https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf)
8. Fragile States Index. *The Fund for Peace*. URL: <https://fragilestatesindex.org/>
9. INFORM Risk. *European Commission*. URL: <https://drmkc.jrc.ec.europa.eu/inform-index/INFORM-Risk>

#### REFERENCES:

1. Rouco J. C., Figueiredo P. C. Business Continuity Management and Resilience: Theories, Models, and Processes. IGI Global, 2024. 360 p.
2. Barskyi M. V. (2024) Bezperervnist biznesu v konteksti lantsiuhiv postachannia [Business continuity in the context of supply chain]. *Stalyi rozvytok ekonomiky*, no. 1(48), pp. 302–308. DOI: 10.32782/2308-1988/2024-48-42 (in Ukrainian).
3. Baz J. E., Ruel S. (2023) Investigating the role of business continuity during COVID-19: an empirical examination. *Supply Chain Forum*, pp. 1–14. DOI: 10.1080/16258312.2023.2199127.
4. Hall T. (2022) Business continuity beyond COVID-19: Lessons learned and the ‘illusion of preparedness’. *Journal of Business Continuity & Emergency Planning*. Volume 16. Number 1, pp. 45–52.
5. BCI Horizon Scan Report 2023. *The Business Continuity Institute (BCI)*. Available at: <https://www.thebci.org/resource/bci-horizon-scan-report-2023.html>
6. ISO 22301. Security and resilience – Business continuity management systems – Requirements. Available at: [https://pttweb7.pttplc.com/pttbcm/upload/media/878\\_ISO22301\\_2019.pdf](https://pttweb7.pttplc.com/pttbcm/upload/media/878_ISO22301_2019.pdf)
7. The Global Risks Report 2020. *The World Economic Forum*. Available at: [https://www3.weforum.org/docs/WEF\\_Global\\_Risk\\_Report\\_2020.pdf](https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf)
8. Fragile States Index. *The Fund for Peace*. Available at: <https://fragilestatesindex.org/>
9. INFORM Risk. *European Commission*. Available at: <https://drmkc.jrc.ec.europa.eu/inform-index/INFORM-Risk>