Андрій О. Якобчук[1], Дмитро М. Дзюбук[2]

СУЧАСНІ БІЗНЕС-РИЗИКИ В УМОВАХ НЕСТАБІЛЬНОСТІ: СТРАТЕГІЇ МІНІМІЗАЦІЇ ТА УБЕЗПЕЧЕННЯ ПІДПРИЄМНИЦТВА

У статті досліджено сутність сучасних бізнес-ризиків та визначено ефективні стратегії їх мінімізації підприємствами в умовах глобальної нестабільності та війни в Україні. Встановлено необхідність переходу підприємств до проактивних моделей ризик-менеджменту на основі інтегрованих систем управління у зв'язку із прискоренням цифровізації бізнес-процесів та змінами геоекономічного ландшафту. Розглянуто особливості формування бізнес-ризиків під впливом невизначеності зовнішнього та внутрішнього середовища. Запропоновано класифікацію ризиків за джерелом походження з виокремленням зовнішніх та внутрішніх загрозах. Проведено комплексний аналіз ключових етапів процесу управління ризиками відповідно до міжнародного стандарту ISO 31000:2018 та представлено п'ять базових стратегій ризик-менеджменту. Визначено основні інструменти убезпечення підприємств від ризиків та наведено їх характеристики, що дозволяє розробити оптимальні стратегії протидії негативним факторам в конкурентних просторово-часових умовах. Особливу увагу приділено кіберризикам як домінуючій загрозі сучасного бізнес-середовища та сформовано систему превентивних заходів проактивної стратегії кіберзахисту. Доведено, що ефективна інтеграція систем ризик-менеджменту на всіх рівнях управління підприємством разом із впровадженням європейських стандартів кібербезпеки забезпечує безперервність бізнес-процесів і підвищення конкурентоспроможності в довгостроковій перспективі.

Ключові слова: *бізнес-ризик; невизначеність; управління ризиками; стратегії мінімізації; безпека бізнесу; сценарне планування; кіберризики.*

Рис. 3. Літ. 21.

DOI: 10.32752/1993-6788-2026-1-297-680-696

[1] ORCID: https://orcid.org/0009-0006-5382-6000

[2] ORCID: https://orcid.org/0009-0000-3037-9785

Andrii Yakobchuk, Dmytro Dziubuk

MODERN BUSINESS RISKS UNDER INSTABILITY: STRATEGIES FOR MINIMIZATION AND ENTREPRENEURIAL RESILIENCE

The article examines the nature of modern business risks and identifies effective strategies for minimizing them for enterprises in the context of global instability and the war in Ukraine. The need for enterprises to transition to proactive risk management models based on integrated management systems is established in connection with the acceleration of digitalization of business processes and changes in the geoeconomic landscape. The features of the formation of business risks under the influence of uncertainty of the external and internal environment are considered. A classification of risks by source of origin is proposed, with the separation of external and internal threats. A comprehensive analysis of the key stages of the risk management process is carried out in accordance with the international standard ISO 31000:2018, and five basic risk management strategies are presented. The main tools for protecting enterprises from risks are identified, and their characteristics are given, which allows for developing optimal strategies for countering negative factors in competitive spatial and temporal conditions. Special attention is paid to cyber risks

[1] Private Higher Education Establishment «European University», Kyiv, Ukraine.
[2] Private Higher Education Establishment «European University», Kyiv, Ukraine.

as the dominant threat of the modern business environment, and a system of preventive measures of a proactive cyber defense strategy has been formed. It has been proven that effective integration of risk management systems at all levels of enterprise management, together with the implementation of European cybersecurity standards, ensures the continuity of business processes and increases competitiveness in the long term.

Keywords: *business risk; uncertainty; risk management; mitigation strategies; business security; scenario planning; cyber risks.*

Peer-reviewed, approved and placed: *22.03.2026*

Постановка проблеми. Сучасне бізнес-середовище характеризується істотним рівнем невизначеності, пов'язаним із турбулентністю міжнародної економічної системи, геополітичними конфліктами, технологічними трансформаціями та інтенсифікацією цифровізації. Підприємства змушені функціонувати на національному та глобальному рівнях за умови браку повної та достовірної інформації щодо майбутнього впливу комплексу найістотніших факторів. Для української економіки проблема виникнення сучасних бізнес-ризиків посилюється у зв'язку із військовими діями на території країни, знищенням інфраструктури, міграцією населення та дефіцитом фінансових ресурсів. Одним із прикладів стала масштабна хакерська атака 12 грудня 2023 р. на мережу «Київстар», яку пов'язують з російським військовим угрупованням Sandworm. Впродовж чотирьох діб відмічалися перебої зі зв'язком у 24 млн абонентів компанії, а сукупні втрати склали близько 95 млн дол. США [1].

Турбулентність зовнішнього середовища створює передумови для значного зростання ризиків прояву несприятливих подій, що можуть призвести до збільшення прямих збитків, а також виникнення непрямих втрат (зниження конкурентоспроможності, втрати ділової репутації тощо). Окреслені обставини створюють стимул для підприємств переорієнтовуватись із традиційних управлінських підходів в умовах сталого розвитку зовнішнього середовища на системи оперативної ідентифікації ризиків, визначення їх потенційного впливу на бізнес-процеси та створення системи ефективних управлінських рішень на довгостроковий період.

Для сучасних підприємств стратегічно важливим є створення інтегрованих систем управління ризиками, що дозволяє мінімізувати ймовірність виникнення потенційних загроз у майбутньому та трансформувати ідентифіковані негативні чинники у потенційні переваги. Завдяки оптимізації використання організаційних, фінансових та технологічних інструментів підприємства отримують можливість забезпечити фінансову стійкість та ефективне функціонування у довгостроковій перспективі. Отже, дослідження комплексу питань щодо систематизації сучасних бізнес-ризиків та визначення ефективних стратегій мінімізації їхнього впливу на діяльність підприємств є напрочуд актуальним.

Аналіз останніх досліджень і публікацій. Дослідженню проблематики управління бізнес-ризиками в умовах невизначеності присвячено праці багатьох іноземних та вітчизняних вчених, а також провідних міжнародних інституцій, які розробляють стандарти та методичні підходи щодо ризик-

менеджменту. Зокрема, заслуговує на увагу публікація О. В. Гаврилюка (2026 р.), присвячена ідентифікації глобальних ризиків та напрямів їх мінімізації [2].

У науковій праці І. Аберніхіної з'ясовано еволюцію теорій управління ризиками в бізнесі в умовах глобалізації, цифровізації економіки та зростання невизначеності зовнішнього середовища [3]. Проведено систематизацію основних етапів розвитку теоретичних концепцій управління ризиками та ідентифіковано їх вплив на сучасні управлінські підходи. Автором виокремлено п'ять ключових етапів еволюції ризиків: класичний, кількісний, інтегрований, поведінковий та цифрово-ESG-орієнтований; для кожного з етапів наведено особливості визначення ризиків, їх оцінювання та управління. Справедливо наголошено на доцільності використання концептуальних основ розвитку управління ризиками в умовах цифрової економіки та сталого розвитку для підприємств у різних видах економічної діяльності.

Колектив авторів (Дж. Фрезер та ін.) здійснив комплексний аналіз проблем впровадження корпоративного управління ризиками, наголошуючи на доцільності підвищення ефективності реалізації даного підходу у практичній діяльності підприємств [4]. Авторами було встановлено сім основних проблем використання корпоративного управління ризиками. На противагу стандартному процесу збору даних для формування звітів керівництву, виникає потреба у використанні корпоративного управління ризиками як проактивного інструменту при розробці оптимальних рішень в умовах невизначеності. Було наведено приклади ефективного запровадження даного підходу такими компаніями, як Hydro One, Mars, Statoil та Bank of Tokyo-Mitsubishi. На основі даних підприємств встановлено, що ефективне управління ризиками вимагає інтеграції в бізнес-процеси та стратегічне планування.

С. Романовскі та Е. Саєрс вивчили особливості інтеграції сучасними підприємствами кіберризиків у свої практики управління корпоративними ризиками [5]. На основі напівструктурованих опитувань було отримано дані щодо особливостей управління корпоративними ризиками та особливостей інтеграції кіберризиків в існуючі процеси. Автори встановили наявність істотних відмінностей у підходах та практиках управління ризиками підприємства. Найчастіше кіберризики розглядаються як операційні ризики, а не як стратегічні ризики, що виникли внаслідок технологічних інновацій. Наголошено на доцільності реалізації стандартних процедур щодо обробки інформації чи процесів для відстеження кіберризиків на рівні підприємства.

І. Чен показав взаємозв'язок між фінансовою інформатизацією та управлінням ризиками підприємств [6], приділив значну увагу опису особливостей використання фінансових технологій для покращення ідентифікації, оцінки та стратегій реагування на ризики в різних видах економічної діяльності. Автор підкреслив доцільність використання таких сучасних інструментів, як великі дані, штучний інтелект, хмарні обчислення та блокчейн, що трансформують фінансові процеси та дозволяють підприємствам реагувати на ризики точніше та гнучкіше. Важливість публікації полягає і в розкритті подвійної сутності фінансової інформатизації,

яка, поряд із забезпеченням обробки великих даних у реальному часі та формуванням ефективних управлінських рішень, призводить до виникнення нових складних ризиків. Інтеграція фінансової інформатизації з управлінням ризиками є стратегічним пріоритетом для розвитку підприємств у волатильному бізнес-середовищі, враховуючи автоматизацію моніторингу та прогнозування ризиків у реальному часі.

Я. Дворскій розкрив вплив штучного інтелекту на управління ризиками малих та середніх підприємств як ефективного інструменту забезпечення стійкого зростання у висококонкурентному середовищі [7]. Ідентифіковано ринкові, фінансові, кадрові та операційні ризики і їх коригування на базі сучасних алгоритмів штучного інтелекту. Оцінювання впливу даної технології на фактори ризику підприємств здійснено за допомогою кореляційно-регресійного аналізу. Інформаційною базою дослідження слугувало онлайн-опитування керівників малих та середніх підприємств у Словаччині впродовж грудня 2024 р. На основі проведеного статистичного аналізу встановлено, що штучний інтелект має найбільший вплив на управління кадровими та фінансовими ризиками, покращуючи ефективність функціонування відповідних напрямів підприємства.

Незважаючи на наявність великої кількості ґрунтовних публікацій, динамічність розвитку зовнішнього середовища та поява нових ризиків (кіберзагрози, кліматичні ризики та трансформація геополітичного середовища) детермінують необхідність проведення нових поглиблених досліджень щодо систематизації сучасних бізнес-ризиків та розробки інноваційних стратегій їх мінімізації на основі принципів динамічності та адаптивності.

Метою статті є вирішення наступних завдань:

- висвітлення сутності та ключових характеристик бізнес-ризиків у сучасному турбулентному середовищі;
- обґрунтування ефективних інструментів підвищення стійкості підприємств і мінімізації негативного впливу зовнішніх та внутрішніх загроз в умовах нестабільності, зокрема в контексті війни в Україні.

Основні результати дослідження. Формування сучасних бізнес-ризиків відбувається під впливом невизначеності зовнішнього та внутрішнього середовища, що істотно впливає на особливості функціонування сучасних підприємств. Регуляторну основу для управління ризиками становить стандарт якості ISO 31000:2018, який розкриває двоїстість цього явища, тобто негативні наслідки (загрози) та позитивні результати (можливості). У зв'язку з турбулентністю глобального економічного середовища та непередбачуваністю виникнення несприятливих подій в Україні існує нагальна потреба посилення систематичного управління ризиками.

Для вітчизняних підприємств нестабільність бізнес-середовища формується як під впливом війни в країні, так і внаслідок геополітичних загроз (торговельних воєн, збройних конфліктів, санкційних обмежень і фрагментації глобальних ринків). Макроекономічна нестабільність проявляється у високому рівні інфляції, волатильності валютних курсів, недостатньому рівні розвитку економіки тощо. Ринкові чинники насамперед

виявляються у скороченні платоспроможного попиту, зростанні рівня конкуренції та ціновій волатильності. Серед технологічних загроз, які характеризуються значним рівнем інноваційності, доцільно виокремити кіберзагрози та високу ймовірність швидкого застарівання бізнес-моделей. Окремо слід звернути увагу на форс-мажорні обставини (пандемії, кліматичні зміни, природні катаклізми), які характеризуються високим рівнем непередбачуваності та здатні завдавати суттєвих збитків національним економічним системам упродовж короткого періоду часу. Одним із прикладів технологічних ризиків у сучасних умовах став глобальний збій CrowdStrike 19 липня 2024 р. внаслідок помилкового оновлення програмного забезпечення, що призвело до відмов у роботі 8,5 млн комп'ютерів та порушило роботу авіакомпаній, банків, медичних установ і медіаорганізацій. Завдані збитки оцінюються компаніями у понад 5 млрд дол. США [8]. Катастрофічна повінь 29 жовтня 2024 р. у Валенсії (Іспанія) є прикладом природно-кліматичних ризиків. Стихійне лихо призвело до загибелі 230 осіб, а економічні збитки оцінюються у понад 20 млрд євро [9].

Для ефективного управління ризиками виникає потреба у розробці науково обґрунтованих класифікацій. Відповідно до наведених вище факторів доцільно виокремити зовнішні та внутрішні ризики, які представлені у вигляді класифікації на рисунку 1.

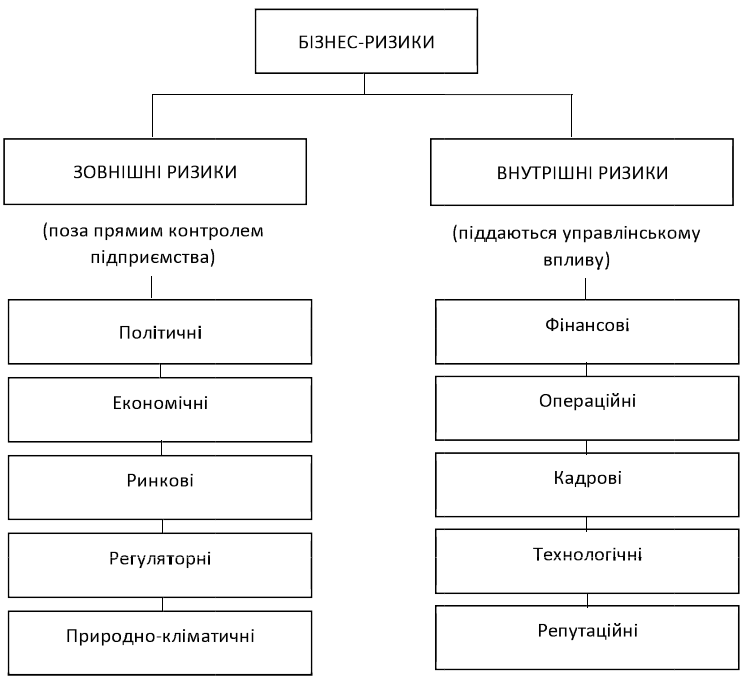

Рис. 1. **Класифікація бізнес-ризиків за джерелом походження,** *побудовано авторами на основі [10, 11]*

Міжнародний стандарт ISO 31000 дозволяє реалізовувати процес управління ризиками відповідно до послідовно розташованих та взаємопов'язаних етапів. Ідентифікація ризиків орієнтована на своєчасне виявлення можливих загроз. Комплексний аналіз інформації передбачає визначення ймовірності настання відповідних негативних явищ, оцінювання їх негативного впливу на бізнес-процеси, ранжування ризиків за силою негативного впливу тощо. Безперервне відстеження динаміки ризиків проводиться для коригування спеціалізованих заходів, орієнтованих на пом'якшення негативних наслідків. Оптимізація управлінських стратегій впливу на ризики створює передумови для мінімізації втрат ресурсів.

На основі систематизації теоретико-методичних підходів було розроблено концептуальну схему управління бізнес-ризиками в умовах турбулентності (рисунок 2). Наведена схема дозволяє оцінити взаємозв'язки між джерелами нестабільності, процесом ризик-менеджменту, стратегіями мінімізації, інструментами убезпечення та кінцевими результатами для підприємств.

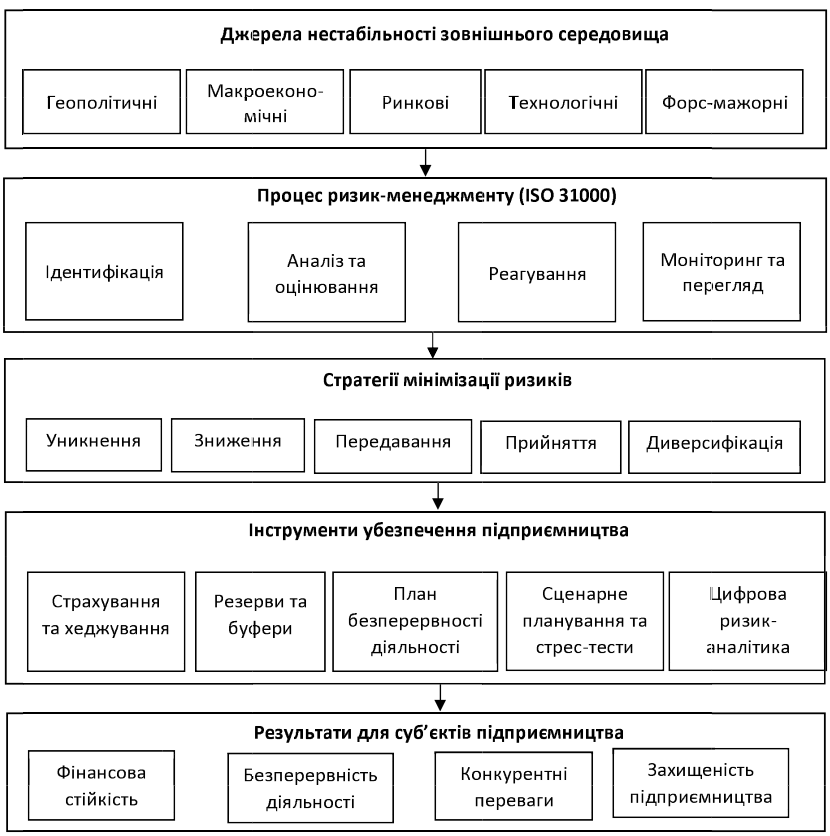

Рис. 2. **Концептуальна схема управління бізнес-ризиками підприємництва в умовах нестабільності,** *розроблено авторами*

Основним елементом системи управління ризиками є вибір оптимальної стратегії їх мінімізації, яку доцільно обирати серед п'яти базових стратегій ризик-менеджменту. Стратегія уникнення передбачає припинення підприємством бізнес-процесів, які характеризуються високим рівнем ризиковості. Зниження ймовірності виникнення ризиків досягається завдяки впровадженню превентивних заходів, які підприємство може реалізувати відповідно до наявних ресурсів та особливостей впливу факторів зовнішнього середовища. Передавання ризиків здійснюється шляхом перекладання фінансової відповідальності на спеціалізовані підприємства у сфері аутсорсингу, страхування та хеджування фінансових інструментів тощо. Стратегію прийняття доцільно застосовувати за умови можливого виникнення прийнятних для підприємства ризиків, оскільки затрати на управління витратами істотно перевищують потенційні збитки. Завдяки диверсифікації підприємства отримують можливість знизити залежність від певного джерела ризику.

Для реалізації наведених стратегій підприємства використовують інструменти, які дозволяють досягти оптимальних економічних результатів. Страхування та хеджування забезпечуються спеціалізованими інституціями, що дозволяє отримати компенсацію збитків за умови виникнення несприятливих для підприємства наслідків. Формування фінансових резервів та операційних буферів створює передумови для пом'якшення шоків без катастрофічних наслідків для функціонування підприємств. Планування безперервності діяльності регламентується відповідним переліком заходів у критичних ситуаціях та забезпечує оперативність відновлення критичних процесів. Данський логістичний концерн A.P. Moller-Maersk у червні 2017 р. став однією з жертв кібератаки шкідливого програмного забезпечення NotPetya, що порушило функціонування портових терміналів і судноплавних операцій у багатьох країнах світу. Maersk втратила близько 49 тис. комп'ютерів та можливість використовувати 1200 критично важливих бізнес-додатків. Завдяки злагодженій роботі співробітників компанії вдалося відновити основні бізнес-процеси впродовж двох тижнів. Прямі втрати Maersk склали 350 млн дол. США, що вважається відносно невеликими збитками у порівнянні з сукупними глобальними втратами інших компаній у розмірі понад 10 млрд дол. США [12, 13].

В умовах турбулентності зовнішнього середовища значного розповсюдження набули сценарне планування та стрес-тестування, які дають можливість оцінити стійкість підприємств за умови виникнення різних подій та розробити ефективні стратегії реагування на ймовірні ризики. Наявність великих даних та можливість їх обробки за допомогою алгоритмів машинного навчання стимулюють використання цифрової ризик-аналітики з метою оперативної ідентифікації ризикових сценаріїв та прийняття ефективних управлінських рішень у короткі терміни. Завдяки поєднанню представлених інструментів в системі управління ризиками досягається синергетичний ефект протистояння підприємствами комплексних шоків.

Убезпечення підприємств від ризиків передбачає формування організаційної стійкості шляхом забезпечення можливостей адаптуватись до

змін зовнішнього середовища, швидко відновлюватись від негативних наслідків та ефективно використовувати нові можливості. Стійкість бізнесу формується на засадах гнучкості бізнес-моделі, диверсифікації джерел доходу, фінансової забезпеченості та розвиненої корпоративної культури управління ризиками. Завдяки інтеграції ризик-менеджменту на всіх рівнях управління підприємства дана функція починає відігравати роль стратегічного фактора забезпечення високого рівня конкурентоспроможності.

За умови системного впровадження наведеного підходу підприємство забезпечить економічну ефективність, високий рівень конкурентоспроможності та загальний рівень захищеності у довгостроковій перспективі. Важливою умовою є забезпечення зворотного зв'язку між процесом управління ризиками та отриманими результатами, що сприяє постійному вдосконаленню системи та її адаптації до факторів зовнішнього середовища.

На рисунку 3 представлено глобальні масштаби кіберризиків: прогноз збитків від кіберзлочинності у 2025 р. та світових витрат на кібербезпеку до 2028 р.

Рис. 3. **Глобальні масштаби кіберризиків: прогноз збитків від кіберзлочинності у 2025 р. та світових витрат на кібербезпеку до 2028 р.,** *[14]*

У сучасних умовах глобальної економічної нестабільності питання забезпечення стійкості підприємств набуває особливої ваги. Світове бізнес-середовище характеризується високим рівнем турбулентності, що зумовлено поєднанням геополітичних конфліктів, економічних криз, інфляційних процесів, розривів логістичних ланцюгів та стрімких технологічних змін. У таких умовах традиційні підходи до управління ризиками виявляються недостатніми, що актуалізує потребу в пошуку нових інструментів мінімізації глобальних загроз та підвищення адаптивності підприємств.

Сучасні виклики стимулюють трансформацію бізнес-моделей, впровадження інноваційних підходів до управління ризиками та формування нових стратегій забезпечення економічної безпеки підприємств. У цих умовах особливого значення набуває концепція стійкості (resilience), яка передбачає здатність підприємств не лише протистояти кризовим явищам, але й

адаптуватися до змін, зберігати функціональність і забезпечувати подальший розвиток. Таким чином, дослідження інструментів мінімізації глобальних ризиків та підвищення стійкості підприємств у турбулентному середовищі є вкрай актуальним як з теоретичної, так і з практичної точки зору, особливо в умовах воєнного стану та післявоєнного відновлення економіки України.

Численні сучасні ризики не існують ізольовано, а формують складну систему взаємозалежностей, що значно ускладнює процес управління ними. У таких умовах підприємства повинні переходити від реактивного до проактивного управління ризиками (у т.ч. з використанням алгоритмів предиктивної аналітики), впроваджуючи сучасні підходи до забезпечення стійкості, гнучкості та адаптивності бізнесу.

Одна з найбільших і найвпливовіших у світі страхових компаній Allianz SE (Німеччина) з-поміж глобальних ризиків поточного 2026 року вже п'ятий рік поспіль на першому місці ранжувала кіберризики/кіберінциденти – в результаті масштабних кібератак у поєднанні з проблемами, що викликані прискоренням цифровізації та переходом великої кількості підприємств, персоналу та населення на дистанційну працю [15]. Причому кіберризики продовжують розвиватися. Фірми дедалі більше залежать від сторонніх постачальників критично важливих даних та послуг, тоді як штучний інтелект посилює загрози, збільшуючи поверхню атаки та посилюючи існуючі вразливості.

Нові ризики створює штучний інтелект (ШІ), який різко піднявся на друге місце серед світових бізнес-проблем – з десятого місця у 2025 р. Оскільки впровадження ШІ прискорюється та глибше інтегрується в основні бізнес-операції, цілком імовірно можна і в подальшому очікувати посилення ризиків, пов'язаних з ним, позаяк все більше фірм намагатимуться масштабуватися у 2026 р. і зіткнуться з більшою схильністю до проблем із надійністю систем, обмеженнями якості даних, перешкодами в інтеграції та нестачею кваліфікованих фахівців. Виникають і нові ризики відповідальності, що пов'язані з автоматизованим прийняттям рішень, упередженими або дискримінаційними моделями, зловживанням інтелектуальною власністю та невизначеністю щодо того, хто несе відповідальність, коли результати, створені ШІ, завдають шкоди.

Глобальні збитки від кіберзлочинності у 2025 р., згідно з даними дослідницької компанії Cybersecurity Ventures (США), склали близько 10,5 трлн дол. [16]. За прогнозом компанії IDC (США), провідного світового постачальника ринкової аналітики, даних і галузевих заходів для ринків інформаційних технологій, телекомунікацій та споживчих технологій, до 2028 р. світові витрати на кібербезпеку сягнуть 377 млрд дол. [17]. Сам по собі цей контраст пояснює дуже багато: кіберзлочинність як індустрія зростає швидше, ніж сектор кіберзахисту.

Український бізнес функціонує в безпрецедентному кіберландшафті: в 2025 р. національна команда реагування CERT-UA (Computer Emergency Response Team of Ukraine) опрацювала 5927 кіберінцидентів – на 37% більше, ніж у 2024 р. Але дана цифра не здатна продемонструвати реального масштабу, що детерміновано виникненням нового, ще більш небезпечного тренду:

практичного переходу зловмисників від швидких разових крадіжок до прихованої довготривалої присутності в цифрових каналах своїх жертв. Зазначений тренд фундаментально трансформує правила гри не лише для критичної інфраструктури, а й усього середнього бізнесу.

За 2025 рік звіт містить два числа, які варто читати разом: перше – вже вищевідзначені 5927 опрацьованих інцидентів, друге – +37,4% до 4 315 справ у 2024 р. Окремо аналітичний звіт оперативного центру Держспецзв'язку фіксує 17,3 тис. подій безпеки та 730 повноцінних кіберінцидентів у його системі моніторингу. Найбільша частка інцидентів спрямована на зараження шкідливим програмним забезпеченням з головною мотивацією – встановленням прихованого контролю над інформаційними системами.

Звідси можна констатувати тренд: посилення інтересу до комерційного сегмента бізнесу з можливістю ідентифікації найважливішої зміни – не в кількості, а в природі атак. Мотивація зловмисників дедалі частіше спрямована не на заволодіння певною інформацією, а насамперед – на забезпечення можливості повторного входу і закріплення в мережі бізнес-екосистеми з поверненням у раніше скомпрометовані системи через місяці після першого вторгнення.

У зв'язку з цим варто наголосити, що лише базового відновлення роботи після кібератаки вже недостатньо. Без повного очищення систем та впровадження жорстких превентивних заходів безпеки установи залишаються відкритими для повторних, часто більш руйнівних ударів, через що можливо дійти висновку, що традиційні алгоритми реагування – знаходження, видалення, відновлення з бекапу, подальше функціонування – вже не варто розглядати як інструмент закриття ризику. Саме тому на повістці денній команди реагування дедалі частіше працюють не за моделлю «реакція на інцидент», а за моделлю «глибока перевірка інфраструктури після кожного підозрілого сигналу».

Для українського бізнесу важлива не глобальна цифра, а її локальне відлуння: ринок кібершкоди – це ринок постійних послуг, а не разових інцидентів. Ransomware-операції (операції з використанням програм-вимагачів) здаються в оренду, фішингові кампанії запускаються як SaaS (хмарне програмне забезпечення за підпискою), дані з витоків купуються пакетами. Інакше кажучи: те, що раніше робила команда хакерів за два тижні роботи, у 2026 р. робить один скрипт за годину і за 50 дол. на тиждень за підписку на phishing-as-a-service (готові платформи для проведення фішингових атак за підпискою) платформу.

На основі цього можливо сформулювати ряд превентивних заходів проактивної стратегії зменшення негативних наслідків від настання ризиків:

1. Управління ризиком. Ідентифікація відповідальних осіб за кібербезпеку у компанії, розпорядників бюджету, фахівців із вибору стандартів. Відсутність виконання зазначеної умови закономірно генеруватиме хаотичні витрати.

2. Інвентаризація та аудит наявних активів з виділенням критичних із них, визначення їхнього розташування з окресленням осіб, які мають доступ до них.

3. Формулювання превентивних засобів за рахунок контролю доступу, шифрування, навчання персоналу, патчів. На даному етапі мінімізація ризику обійдеться найдешевше.

4. Виявлення – запровадження безперервного спостереження за інфраструктурою (моніторинг 24/7). До ключових елементів його слід віднести:

- наявність/створення центру операційної безпеки SOC (Security Operations Center) – підрозділу або зовнішньої служби, що цілодобово відстежує події безпеки. Може бути власним або аутсорсинговим;
- поведінкова аналітика (Behavioral analytics) – технологія, що виявляє аномалії, порівнюючи поточну активність користувачів і систем зі звичною «нормою» поведінки;
- розвідка кіберзагроз (Threat intelligence) – збір і аналіз даних про актуальні загрози, тактики й інструменти зловмисників.

Дана рекомендація належить до критичних, позаяк в умовах моделі персистентності, тобто здатності атакувальника надовго закріпитися в системі, без цього елемента існує ризик не дізнатися про злам, доки не стане пізно.

5. Реагування на інцидент – передбачає підготовку плану заздалегідь із чітко визначеними відповідальними, контактами та процедурами комунікації, готовими сценаріями (покроковими інструкціями на конкретні типи атак) і регулярним навчанням команди з реагуванням за відпрацьованим алгоритмом, а не імпровізацією під час реальної атаки.

6. Відновлення – створення бекапів (резервних копій даних), які реально відновлюються і регулярно тестуються на фактичне відновлення, а не просто розробляються.

Непересічне значення має регуляторне питання. Український бізнес, який працює з європейськими партнерами, дедалі частіше отримує запити щодо відповідності вимогам NIS2 – оновленої Директиви Європейського Союзу з кібербезпеки. Технічні рекомендації Агентства Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity (ENISA)), опубліковані у 2025 р., визначають мінімальний перелік заходів з управління кіберризиками (risk-management measures), які мають бути впроваджені в організації. До них належать:

- реагування на інциденти (incident handling);
- забезпечення безперервності бізнесу (business continuity);
- безпека ланцюга постачання (supply chain security);
- навчання персоналу;
- контроль доступу;
- управління активами;
- використання криптографічних засобів захисту [18].

Для українського малого та середнього бізнесу, який не є прямим суб'єктом NIS2, зазначені рекомендації не становлять юридичного зобов'язання, але стають ринковою вимогою. Великі європейські клієнти дедалі частіше включають у договори вимоги «cyber-due diligence» (перевірки рівня кібербезпеки та управління кіберризиками), і компанія без базової кібергігієни просто не пройде відбір.

Резюмуючи, можна констатувати, що зловмисники перейшли до моделі довготривалої прихованої присутності. У середньому в світі організації виявляють компрометацію через 200+ днів після факту, і в плані кіберзахисту вже назріла критична необхідність у можливості виявлення «чужого», який уже всередині.

Окреме питання полягає в убезпеченні підприємництва в умовах воєнного стану, за якого український бізнес стикається з обмеженими ресурсами, проблемами логістики, нестачею кадрів та фінансів, що загрожує економічній безпеці. Попри ці виклики, адаптивність стала головною стратегією виживання. Підприємці змушені переглядати звичні ланцюги постачання у пошуках нових партнерів усередині країни або за кордоном, що генерує розвиток горизонтальних зв'язків. Забезпечення гнучкості у прийнятті рішень дозволяє бізнесу не лише утримувати позиції на ринку, а й освоювати нові ніші, зокрема у сфері оборонних технологій, енергоефективності та гуманітарного забезпечення.

До важливих факторів убезпечення належать цифрова трансформація та релокація потужностей у безпечніші регіони. Використання хмарних сервісів та автоматизація процесів допомагають мінімізувати ризики втрати даних та фізичних активів. Водночас держава та міжнародні донори намагаються підтримувати приватний сектор через грантові програми та пільгове кредитування, що створює необхідний фінансовий «буфер» для відновлення операційної діяльності [3]. Зрештою, стійкість українського бізнесу є фундаментом національної безпеки, оскільки саме він забезпечує робочі місця та податкові надходження до бюджету. Соціальна відповідальність компаній, яка проявилася у масштабній волонтерській підтримці армії та цивільних, зміцнює довіру всередині суспільства. Збереження економічної активності сьогодні це не лише питання прибутку, а й запорука швидкого відновлення країни в післявоєнний період.

Цифровізація дозволяє оптимізувати процеси, підвищити гнучкість та конкурентоспроможність, вона проникає в усі сфери: від застосунку «Дія» до електронного врядування та бізнес-платформ. Її результативність спричинює наступні наслідки:

- зростання ефективності бізнес-процесів через автоматизацію та AI, що зменшує витрати на 20-30% [19];
- розширення ринків за допомогою цифрових платформ і залучення клієнтів онлайн;
- підвищення інформаційної безпеки: моніторинг процесів, захист даних.

Прикладом слугує впровадження Дія.City для IT-бізнесу спеціального правового та податкового простору для IT-компаній в Україні з метою підвищення обороноздатності країни, забезпечення її конкурентоспроможності на світовому рівні та виведення індустрії з «тіні» [20]. Стисло це можна ідентифікувати як «цифровий офшор» всередині країни із прозорими правилами гри ПДФО 5%, ЄСВ 22% від мінімальної заробітної плати з фокусом на оборонні технології.

Водночас існують і ризики та загрози: кібератаки, залежність від імпортного програмного забезпечення (ПЗ), брак цифрових навичок. Задля їх

мінімізації необхідно проводити регулярний аудит безпеки, навчання персоналу (digital skills), перехід на українське ПЗ, інтеграцію з державними платформами. У даному контексті слід керуватися положеннями Закону України «Про стимулювання розвитку цифрової економіки в Україні» № 1667-IX від 15 липня 2021 року [21].

Вважається доцільним окреслити ряд інших напрямів убезпечення бізнесу.

Першочергове завдання полягає в убезпеченні персоналу. Ще за часів пандемії багато підприємств встигло перепрофілюватися за рахунок запровадження нових форм організації праці, велику кількість працівників було переведено на дистанційний графік роботи; з початком війни цей досвід особливо став у нагоді. Даний перехід не повинен викликати багато проблем, оскільки питання віддаленої (дистанційної та надомної) роботи давно широко практикуються і врегульовані на законодавчому рівні. Причому при можливості варто не скорочувати штат позаяк збереження команди є надважливим кроком, адже після перемоги для швидкого відновлення будуть потрібні досвідчені та перевірені кадри.

Антикризове управління підприємством у воєнний час передбачає набуття та застосування нових (у т. ч. лідерських) якостей менеджменту як однієї із запорук успішності убезпечення. Наявність злагодженого та скоординованого персоналу становить напрочуд важливий чинник стабільності за будь-яких обставин, а особливо коли оперативність прийняття рішень і вжиття дієвих заходів здатні врятувати життя та забезпечити збереження активів фірми. Здатність взяти на себе відповідальність та забезпечити професійну комунікацію з персоналом (часто вельми розгубленим) належить до ще однієї запоруки дієвого антикризового управління. Саме нові лідерські якості керівників підприємств, їхня реакція на зміни ситуації, уміння прогнозувати та швидко розв'язувати задачі, вчасно вживати дієві стратегічні рішення виступають запорукою успішності ведення бізнесу в умовах воєнного стану.

Ще один ризик зводиться до «втрати» керівника або його можливості виконувати свої функції. Очевидно, що цей факт є головним. Однак слід констатувати, що бізнесмени часто про це забувають та більше уваги приділяють персоналу та активам. З одного боку, аксіоматично, керівник повинен безпосередньо управляти своїм бізнесом, але з іншого правильно розставляти пріоритети та організовувати роботу. У випадку, якщо керівник має найманий статус, цілком реальним є виникнення ряду проблем: останній може піти на службу у Збройні сили України або через інші об'єктивні причини не перебувати на робочому місці. Виходячи з цього, не потрібно додаткових аргументів на користь наявності «у доступі» підписанта, а отже необхідно мати варіант «Б», наприклад, за рахунок додавання інших підписантів.

Наступна проблема, що потребує вирішення перехід на електронний документообіг. Це процес неминучий у будь-якому випадку, і за умови якомога оперативнішого його впровадження корпоративні документи стануть доступними будь-де і будь-коли особам, яким буде надано до них доступ;

документи ніколи не зникнуть, знищити їх фізично або вкрасти буде неможливо. Крім того, це заощаджує час, який витрачається на пошук документів та їх доставку, і дає змогу фокусуватись на важливіших питаннях. Налагодження постійного зв'язку з персоналом теж є вкрай важливим: це можуть бути як групи в месенджерах, так і корпоративні чати для оперативного інформування та координації дій.

Непересічне значення для збереження бізнесу має страхування активів. Російська війна проти України та пов'язані з нею фізичні втрати, пошкодження чи захоплення майна та вантажу, поранення чи загибель працівників тощо складають основні ризики. Деякі підприємства, такі як металургія та гірничодобувна промисловість, сільське господарство, логістика, особливо поблизу лінії фронту, хоча й перебувають у зоні підвищеного ризику, але фізично не можуть бути передислоковані, а захист від воєнних ризиків є пріоритетом для підприємців. Тому до вищезазначених напрямів убезпечення можна віднести і страхування політичних (військових) ризиків, нещасних випадків і збитків від переривання бізнесу. З одного боку, внаслідок вторгнення Росії переважна більшість постачальників страхових послуг призупинили свою діяльність в Україні, з іншого ряд установ все ще пропонують варіанти страхування, зокрема MIGA (Група Світового банку), DFC (США), UKEF (Великобританія), KUKE (Польща), SACE (Італія) та ряд інших. Їхніми послугами цілком реально скористатися. В ідеалі ж компанії повинні мати резервне обладнання та запаси сировини, палива, матеріалів, здійснювати моніторинг щодо розвитку безпекової ситуації в Україні, проводити заходи з кібербезпеки.

Висновки. Підсумовуючи, можна констатувати, що стратегія убезпечення підприємництва в умовах війни трансформувалася з моделі пасивного виживання у модель активної адаптивності. Ключовим інструментом цієї трансформації виступає синергія технологічних інновацій та управлінської гнучкості. Впровадження цифрових інструментів, перехід на електронний документообіг та використання спеціальних правових режимів, як-от Дія.City, не лише мінімізують фізичні ризики втрати активів, а й створюють фундамент для прозорого та конкурентоспроможного бізнесу. Водночас критичне значення має інституціоналізація «плану Б» у системі менеджменту, що передбачає дублювання функцій управління та юридичну підготовку до можливої відсутності керівних осіб, що є специфічним, але життєво необхідним викликом воєнного часу.

Економічна стійкість України безпосередньо залежить від здатності приватного сектору інтегрувати механізми страхування воєнних ризиків та зберігати людський капітал як найцінніший актив. Попри складність залучення міжнародних страхових інструментів (MIGA, DFC та інших), їх використання стає вагомим чинником інвестиційної привабливості навіть у кризових умовах. Зрештою, успішне антикризове управління сьогодні базується на принципі відповідального лідерства та здатності бізнесу бути частиною системи національної безпеки.

Мінімізація глобальних бізнес-ризиків у сучасному турбулентному середовищі потребує комплексного застосування стратегічних,

організаційних та технологічних інструментів, спрямованих на підвищення адаптивності та стійкості підприємств. До ключових із них належать впровадження системи ризик-менеджменту з елементами раннього попередження, диверсифікація постачальників і ринків збуту, цифровізація бізнес-процесів, розвиток кібербезпеки, створення фінансових резервів і страхових механізмів, а також сценарне планування та антикризове управління. Особливої актуальності ці інструменти набувають в умовах російсько-української війни, коли підприємства змушені оперативно реагувати на високий рівень невизначеності, забезпечуючи безперервність діяльності та збереження конкурентоспроможності.

1. Kyivstar Completes Preliminary Assessment of the Financial Impact of the Cyberattack. VEON. URL: https://www.veon.com/newsroom/press-releases/kyivstar-completes-preliminary-assessment-of-the-financial-impact-of-the-cyberattack

2. Havryliuk, O. (2026). Global business risks and directions for their minimization. In A. Zadoia & S. Fedulova (Eds.), European Security Architecture in the 21st Century: Monograph (pp. 90–105). Dnipro: Alfred Nobel University. https://doi.org/10.32342/eurosec/9789664346266

3. Abernikhina, I. (2025). The evolution of risk management theories in business. Економіка розвитку систем, 7(2), 13–19. https://doi.org/10.32782/2707-8019/2025-2-2

4. Fraser, J., Quail, R., & Simkins, B. (2024). What's wrong with enterprise risk management? Journal of Risk and Financial Management, 17(7), 274. https://doi.org/10.3390/jrfm17070274

5. Romanosky, S., & Petrun Sayers, E. L. (2024). Enterprise risk management: how do firms integrate cyber risk? Management Research Review, 47(1), 1–17. https://doi.org/10.1108/MRR-10-2021-0774

6. Chen, Y. (2026). The role of financial informatization in enhancing enterprise risk management. Journal of Computer Technology and Applied Mathematics, 3(1), 63–70. https://doi.org/10.70393/6a6374616d.333633

7. Dvorsky, J. (2025). Impact of artificial intelligence on enterprise risk management: A case study from the Slovak SME segment. Journal of Business Sectors, 3(1), 96–103. https://doi.org/10.62222/CAJA0666

8. What the 2024 CrowdStrike glitch can teach us about cyber risk. Harvard Business Review. URL: https://hbr.org/2025/01/what-the-2024-crowdstrike-glitch-can-teach-us-about-cyber-risk

9. Valencia floods: lessons in claims and recovery, one year on. Zurich. URL: https://www.zurich.com/commercial-insurance/sustainability-and-insights/commercial-insurance-risk-insights/valencia-floods-lessons-in-claims-and-recovery-one-year-on

10. Semenova, S. M. (2020). Klasyfikatsiia ryzykiv: systematyzovanyi pidkhid z metoiu upravlinnia [Risk classification: a systematicized management approach]. Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky, 4(2), 42–51.

11. Kovtun, O. (2024). Pidkhody do klasyfikatsii ryzykiv stiikoho rozvytku pidpryiemstv [Approaches to the classification of sustainable development risks of enterprises]. Transformatsiina ekonomika, 3(08), 79–82. https://doi.org/10.32782/2786-8141/2024-8-11

12. Rebuilding after NotPetya: How Maersk moved forward. CSO Online. URL: https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html

13. Friendly cyber fire: How much did NotPetya cost Russia? Irregular Warfare Initiative. URL: https://www.irregularwarfare.org/notpetya-cost-russia/

14. 2025 Data Breach Investigations Report. Verizon Business. URL: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

15. Allianz Risk Barometer 2026 results appendix. The most business risks in 2026: global. Allianz Commercial. URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/allianz-risk-barometer-2026-appendix.pdf

16. Cybercrime to cost the world $12.2 trillion annually by 2031. (2025, May 28). Cybersecurity Ventures. URL: https://cybersecurityventures.com/official-cybercrime-report-2025/

17. Global security spending continues to rise. (2025, March 21). IT Pro. URL: https://www.itpro.com/security/global-security-spending-continues-to-rise

18. European Union Agency for Cybersecurity (ENISA). European Union. URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en

19. Tsyfrova transformatsiia ekonomiky Ukrainy v umovakh viiny [Digital transformation of Ukraine's economy under war]. (2024). National Institute for Strategic Studies (NISS). URL: https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-sichen-2024

20. Diia.City v umovakh voiennoho stanu [Diia.City under martial law]. Faculty of Law of Yuriy Fedkovych Chernivtsi National University. URL: https://law.chnu.edu.ua/diia-city-v-umovakh-voiennoho-stanu/

21. Zakon Ukrainy «Pro stymuliuvannia rozvytku tsyfrovoi ekonomiky v Ukraini» № 1667-IX vid 15 lypnia 2021 roku [Law of Ukraine «On stimulating the development of the digital economy in Ukraine» No. 1667-IX of July 15, 2021]. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text

---

1. Kyivstar Completes Preliminary Assessment of the Financial Impact of the Cyberattack. VEON. URL: https://www.veon.com/newsroom/press-releases/kyivstar-completes-preliminary-assessment-of-the-financial-impact-of-the-cyberattack

2. Havryliuk, O. (2026). Global business risks and directions for their minimization. In A. Zadoia & S. Fedulova (Eds.), European Security Architecture in the 21st Century: Monograph (pp. 90–105). Dnipro: Alfred Nobel University. https://doi.org/10.32342/eurosec/9789664346266

3. Abernikhina, I. (2025). The evolution of risk management theories in business. Економіка розвитку систем, 7(2), 13–19. https://doi.org/10.32782/2707-8019/2025-2-2

4. Fraser, J., Quail, R., & Simkins, B. (2024). What's wrong with enterprise risk management? Journal of Risk and Financial Management, 17(7), 274. https://doi.org/10.3390/jrfm17070274

5. Romanosky, S., & Petrun Sayers, E. L. (2024). Enterprise risk management: how do firms integrate cyber risk? Management Research Review, 47(1), 1–17. https://doi.org/10.1108/MRR-10-2021-0774

6. Chen, Y. (2026). The role of financial informatization in enhancing enterprise risk management. Journal of Computer Technology and Applied Mathematics, 3(1), 63–70. https://doi.org/10.70393/6a6374616d.333633

7. Dvorsky, J. (2025). Impact of artificial intelligence on enterprise risk management: A case study from the Slovak SME segment. Journal of Business Sectors, 3(1), 96–103. https://doi.org/10.62222/ CAJA0666

8. What the 2024 CrowdStrike glitch can teach us about cyber risk. Harvard Business Review. URL: https://hbr.org/2025/01/what-the-2024-crowdstrike-glitch-can-teach-us-about-cyber-risk

9. Valencia floods: lessons in claims and recovery, one year on. Zurich. URL: https://www.zurich.com/commercial-insurance/sustainability-and-insights/commercial-insurance-risk-insights/valencia-floods-lessons-in-claims-and-recovery-one-year-on

10. Semenova, S. M. (2020). Klasyfikatsiia ryzykiv: systematyzovanyi pidkhid z metoiu upravlinnia [Risk classification: a systematicized management approach]. Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky, 4(2), 42–51.

11. Kovtun, O. (2024). Pidkhody do klasyfikatsii ryzykiv stiikoho rozvytku pidpryiemstv [Approaches to the classification of sustainable development risks of enterprises]. Transformatsiina ekonomika, 3(08), 79–82. https://doi.org/10.32782/2786-8141/2024-8-11

12. Rebuilding after NotPetya: How Maersk moved forward. CSO Online. URL: https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html

13. Friendly cyber fire: How much did NotPetya cost Russia? Irregular Warfare Initiative. URL: https://www.irregularwarfare.org/notpetya-cost-russia/

14. 2025 Data Breach Investigations Report. Verizon Business. URL: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

15. Allianz Risk Barometer 2026 results appendix. The most business risks in 2026: global. Allianz Commercial. URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/allianz-risk-barometer-2026-appendix.pdf

16. Cybercrime to cost the world $12.2 trillion annually by 2031. (2025, May 28). Cybersecurity Ventures. URL: https://cybersecurityventures.com/official-cybercrime-report-2025/

17. Global security spending continues to rise. (2025, March 21). IT Pro. URL: https://www.itpro.com/security/global-security-spending-continues-to-rise

18. European Union Agency for Cybersecurity (ENISA). European Union. URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en

19. Tsyfrova transformatsiia ekonomiky Ukrainy v umovakh viiny [Digital transformation of Ukraine's economy under war]. (2024). National Institute for Strategic Studies (NISS). URL: https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-sichen-2024

20. Diia.City v umovakh voiennoho stanu [Diia.City under martial law]. Faculty of Law of Yuriy Fedkovych Chernivtsi National University. URL: https://law.chnu.edu.ua/diia-city-v-umovakh-voiennoho-stanu/

21. Zakon Ukrainy «Pro stymuliuvannia rozvytku tsyfrovoi ekonomiky v Ukraini» № 1667-IX vid 15 lypnia 2021 roku [Law of Ukraine «On stimulating the development of the digital economy in Ukraine» No. 1667-IX of July 15, 2021]. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text