МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ

ННІ/факультет	Навчально-науковий інститут економіки та бізнес-освіти
Кафедра	міжнародних відносин
Спеціальність	292 Міжнародні економічні відносини
Форма навчання	денна

КВАЛІФІКАЦІЙНА РОБОТА

Гребенюк Анастасії Дмитрівни
(прізвище, ім'я, по батькові здобувача)

на тему **Економічна безпека міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності**

(повна назва теми)

за матеріалами _____

(повна назва бази дослідження)

науковий керівник **к.е.н., доцент** _____ **Єгорова І.Г.**
(наук. ступінь, вчене звання) *(підпис)* *(прізвище, ініціали)*

Робота допущена до захисту в ЕК
Протокол засідання кафедри
від «08» червня 2026р. № 12
Завідувач кафедри _____
(підпис)
д.е.н., доцент І. МАКСИМОВА

Кривий Ріг – 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ

ННІ/факультет	Навчально-науковий інститут економіки та бізнес-освіти
Кафедра	міжнародних відносин
Спеціальність	292 Міжнародні економічні відносини
Форма навчання	денна

«ЗАТВЕРДЖУЮ»
Завідувач кафедри _____ І. МАКСИМОВА
(підпис) (Ініціал, ПРІЗВИЩЕ)
«15» червня 2026 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ
Гребенюк Анастасії Дмитрівни

1. Тема роботи **Економічна безпека міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності**

Керівник роботи Єгорова Ірина Геннадіївна, к.е.н., доцент
затверджено наказом закладу вищої освіти від «06» квітня 2026 р. № 233-ст

2. Строк подання здобувачем роботи до «15» червня 2026 р.

3. Зміст кваліфікаційної бакалаврської роботи, об’єкт, предмет та мета дослідження:

Розділ 1.Теоретичне підґрунтя та методи забезпечення економічної безпеки міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності
1.1. Сутність та складові економічної безпеки міжнародного бізнесу
1.2.Кіберзагрози та геополітична нестабільність як чинники впливу на діяльність суб’єктів міжнародних економічних відносин
1.3.Методи забезпечення економічної та кібербезпеки міжнародного бізнесу
Розділ 2. Аналіз системи економічної безпеки міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності
2.1.Тенденції розвитку загроз та механізми протидії дій на економічній та кіберзлочинності у світовому господарстві
2.2.Оцінка впливу кіберінцидентів та воєнних функціонування суб’єктів міжнародної економічної діяльності в Україні
2.3.Аналіз стану економічної безпеки та інструментів кіберзахисту суб’єктів міжнародного бізнесу на території України
Розділ 3. Стратегічні напрями зміцнення економічної та кібербезпеки міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності
3.1.Міжнародний досвід компаній щодо підвищення рівня управління економічною безпекою та його прийнятність для українських реалій
3.2.Удосконалення державної політики України щодо зміцнення економічної безпеки підприємництва в умовах геополітичних ризиків та кіберзагроз
3.3.Стратегічні шляхи та ефективні інструменти посилення економічної безпеки українських компаній як суб’єктів міжнародного бізнесу у воєнний час та в період повоєнного відновлення країни

Об'єкт дослідження: процес забезпечення економічної безпеки міжнародного бізнесу в умовах глобальних економічних трансформацій

Предмет дослідження: формування системи економічної безпеки міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності

Мета кваліфікаційної бакалаврської роботи: аналіз системи економічної безпеки міжнародного бізнесу та визначення стратегічних напрямів й ефективних інструментів її зміцнення в умовах кіберзагроз та геополітичної нестабільності

5. Дата видачі завдання «06» квітня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної бакалаврської роботи	Строк виконання етапів роботи	Відмітка керівника про виконання етапів (дата)
1	Підготовка розділу 1	24.04.2026 р.	24.04.2026 р.
2	Підготовка розділу 2	11.05.2026 р.	11.05.2026 р.
3	Підготовка розділу 3	01.06.2026 р.	01.06.2026 р.
4	Перевірка кваліфікаційної бакалаврської роботи на наявність ознак академічного плагіату за допомогою програми StrikePlagiarism	до 04.06.2026 р.	04.06.2026 р.
5	Отримання відгуку від наукового керівника	до 12.06.2026 р.	12.06.2026 р.
6	Подання кваліфікаційної роботи на перегляд завідувачу кафедри	до 15.06.2026 р.	15.06.2026 р.
7	Реєстрація завершеної кваліфікаційної роботи	15.06.2026 р.	Реєстраційний № 3 «15» червня 2026 р.
8	Попередній захист кваліфікаційної роботи на кафедрі	15.06.2026 р.	15.06.2026 р.
9	Підготовка до захисту в ЕК	до 16.06.2026 р.	до 16.06.2026 р.

Завдання підготував науковий керівник _____ І. ЄГОРОВА
(підпис) (Ініціал, ПРІЗВИЩЕ)

Завдання одержав _____ А. ГРЕБЕНЮК
(підпис) (Ініціал, ПРІЗВИЩЕ)

АНОТАЦІЯ

Гребенюк Анастасія Дмитрівна. Економічна безпека міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності. – Рукопис. Кваліфікаційна бакалаврська робота за спеціальністю 292 Міжнародні економічні відносини. Державний університет економіки і технологій. Кривий Ріг, 2026.

96 с., 9 таблиць, 18 рисунків, 64 літ. джерела.

У кваліфікаційній бакалаврській роботі всебічно розглянуто теоретичні та практичні аспекти забезпечення економічної безпеки міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності.

Розкрито сутність економічної безпеки міжнародного бізнесу, її основні складові та функціональні елементи.

Проаналізовано вплив сучасних кіберзагроз, цифровізації економіки та геополітичних конфліктів на діяльність суб'єктів міжнародних фінансових відносин.

Узагальнено методи та шляхи забезпечення економічного захисту та кібербезпеки підприємств у глобальному бізнес-середовищі.

Особливу увагу приділено дослідженню тенденцій розвитку економічної та кіберзлочинності у світовому господарстві, оцінці впливу кіберінцидентів і воєнних дій на функціонування українських підприємств, а також аналізу сучасного стану економічної безпеки суб'єктів міжнародного бізнесу в Україні.

Проведено оцінювання ефективних шляхів кіберзахисту та визначено ключові ризики, які виникають унаслідок цифрових і геополітичних трансформацій.

Запропоновано стратегічні напрями зміцнення економічної безпеки міжнародного бізнесу на основі міжнародного досвіду управління ризиками.

Обґрунтовано шляхи удосконалення державної політики щодо забезпечення економічної безпеки підприємництва в умовах геополітичних викликів.

Наведено комплекс практичних заходів та інструментів підвищення стійкості українських компаній до кіберзагроз і зовнішніх ризиків у період воєнного стану та післявоєнного відновлення економіки України.

Ключові слова: економічна безпека, міжнародний бізнес, кібербезпека, кіберзагрози, кібератаки, геополітична нестабільність, кіберзлочинність, ризик-менеджмент, цифровізація, міжнародні економічні відносини, економічна стійкість, воєнний стан, повоєнне відновлення.

ЗМІСТ

ВСТУП

Функціонування міжнародного бізнесу в умовах глобалізації та середовищі підвищеної невизначеності, що супроводжується військовими конфліктами, стрімким розвитком цифрових технологій, загостренням геополітичної ситуації, трансформацією міжнародних економічних взаємозв'язків, суттєвим посиленням кіберзагроз, торговельними обмеженнями, кібератаками, інформаційними війнами та нестабільністю світових ринків суттєво впливають на діяльність компаній, створюючи кожного дня виклики для забезпечення їх економічної безпеки. За таких умов проблема формування ефективної системи економічної безпеки міжнародного бізнесу набуває особливої актуальності, оскільки саме від рівня захищеності підприємств залежить їхня конкурентоспроможність, фінансова стійкість та здатність адаптуватися до кризових змін зовнішнього середовища.

Особливо гостро цю проблему відчувають на собі українські підприємства після повномасштабного вторгнення, яке несе постійне руйнування критичної та соціальної інфраструктури, проблеми логістики, зменшення інвестування, валютні ризики, відсутність стабільності в сфері енергетичної системи та суттєвим збільшенням кібератак. Сучасні кіберзагрози стали одним із ключових факторів впливу на економічну безпеку бізнесу, оскільки цифровізація міжнародної економіки створює не лише нові можливості для розвитку, а також і нові джерела ризиків. Кібератаки призводять не тільки до втрат конфіденційних даних та інформації, а й до фінансових збитків, які блокують бізнес-процеси, погіршують репутацію компаній, що призводить до зменшення довіри міжнародних інвесторів та партнерів.

Геополітична нестабільність також істотно впливає на функціонування міжнародного бізнесу. Зміни у світовому балансі сил, загострення міжнародної конкуренції, торговельні війни, санкційна політика, регіональні конфлікти та порушення глобальних ланцюгів постачання формують нові ризики для суб'єктів господарювання. У таких умовах підприємства повинні не лише адаптуватися до

змін зовнішнього середовища, а й формувати комплексні механізми захисту власних економічних інтересів.

Актуальність теми кваліфікаційної бакалаврської роботи зумовлена необхідністю дослідження сучасних загроз економічній безпеці міжнародного бізнесу, аналізу впливу кіберзагроз та геополітичної нестабільності на діяльність компаній, а також розроблення ефективних стратегічних підходів та інструментів зміцнення економічної безпеки підприємств в умовах глобальних трансформацій. Значний внесок у дослідження проблем економічної безпеки, міжнародного бізнесу, ризик-менеджменту та кібербезпеки зробили як українські, так і зарубіжні науковці. Водночас сучасні умови розвитку світової економіки, цифровізація бізнес-середовища та зростання масштабів геополітичних ризиків потребують подальшого наукового осмислення механізмів забезпечення економічної безпеки міжнародного бізнесу.

Метою кваліфікаційної бакалаврської роботи аналіз системи економічної безпеки міжнародного бізнесу та визначення стратегічних напрямів й ефективних інструментів її зміцнення в умовах кіберзагроз та геополітичної нестабільності.

Для досягнення поставленої мети необхідно виконати такі **завдання**:

- розкрити сутність економічної безпеки міжнародного бізнесу та її основні складові;
- проаналізувати вплив кіберзагроз на діяльність міжнародних компаній;
- охарактеризувати геополітичну нестабільність як фактор ризику для міжнародного бізнесу;
- оцінити сучасний стан економічної безпеки українських компаній у воєнний період;
- проаналізувати вплив цифрових технологій на забезпечення економічної безпеки бізнесу;
- визначити стратегічні напрями зміцнення економічної безпеки міжнародного бізнесу;
- обґрунтувати ефективні інструменти посилення економічної безпеки українських компаній в умовах воєнного часу та повоєнного відновлення.

Об’єктом дослідження є процес забезпечення економічної безпеки міжнародного бізнесу в умовах глобальних економічних трансформацій.

Предметом дослідження є формування системи економічної безпеки міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності.

У процесі дослідження використано комплекс загальнонаукових і спеціальних **методів**. Зокрема, методи аналізу та синтезу застосовано для дослідження теоретичних основ економічної безпеки міжнародного бізнесу; метод порівняння – для зіставлення сучасних підходів до управління ризиками та кібербезпекою; статистичний метод – для аналізу впливу геополітичних та кібернетичних загроз на діяльність компаній; системний підхід – для формування комплексного бачення економічної безпеки підприємств; графічний та табличний методи – для наочного подання результатів дослідження.

Наукова новизна одержаних результатів полягає у розробленні комплексних стратегічних напрямів та практичних інструментів зміцнення економічної безпеки українських компаній у воєнний та повоєнний періоди.

Теоретичне значення роботи полягає у систематизації наукових підходів до визначення економічної безпеки міжнародного бізнесу, дослідженні сучасних факторів ризику та узагальненні механізмів забезпечення стійкості підприємств у кризових умовах.

Практичне значення одержаних результатів полягає у можливості використання запропонованих рекомендацій, стратегій та інструментів українськими компаніями для підвищення рівня економічної безпеки, мінімізації ризиків та забезпечення стабільного функціонування в умовах зовнішніх загроз.

Інформаційною базою дослідження послугували офіційні дані Державної служби статистики України та статистичного відомства ЄС, матеріали та звіти міжнародних організацій, таких як МВФ, Світового банку, офіційна статистика з міжнародної економіки, інновацій, ринку праці, торгівлі та цифровізації, аналітичні доповіді українських та міжнародних дослідницьких центрів, наукові публікації вітчизняних та зарубіжних авторів, матеріали періодичних видань та інформаційних ресурсів мережі інтернет.

РОЗДІЛ 1
ТЕОРЕТИЧНЕ ПІДҐРУНТЯ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ МІЖНАРОДНОГО БІЗНЕСУ В УМОВАХ КІБЕРЗАГРОЗ ТА ГЕОПОЛІТИЧНОЇ НЕСТАБІЛЬНОСТІ

1.1. Сутність та складові економічної безпеки міжнародного бізнесу

У сучасному економічному середовищі підприємницька діяльність здійснюється в умовах значно ускладненої глобальної взаємодії, де динаміка господарських процесів постійно прискорюється, рівень невизначеності зростає, а кількість чинників, здатних породжувати ризики, істотно збільшується. За таких обставин особливої ваги для будь-якого суб’єкта господарювання набуває створення ефективної системи економічного захисту. Разом із тим для підприємств, які відрізняються розмірами, сферою діяльності, галузевою належністю, а також національним чи міжнародним характером функціонування, зазначене питання поєднує як загальні, властиві всім організаціям ознаки, так і специфічні особливості, що визначаються траєкторією їхнього розвитку, структурою управління та умовами зовнішнього середовища.

Підприємства стикаються із небезпеками, які формуються не тільки під впливом зовнішніх змін, а також і через внутрішні організаційні процеси. Мова йде, про трансформації в управлінні, зміни в кадровому складі, розвиток корпоративної складової, реоргранізація менеджменту та модернізація технічної бази і технологічної основи. В такій багатофункціональній системі економічна безпека підприємства залежить від багатьох факторів таких, як персонал, фінансові ресурси, технологічні рішення та результати господарської діяльності, і часом передбачити та своєчасно виявити потенційні загрози і правильно на них відреагувати зберігаючи внутрішню цілісність, управлінську узгодженість та стратегічну орієнтацію буває дуже складно.

Економічну безпеку підприємства доцільно трактувати як цілісну сукупність взаємозалежних умов, управлінських інструментів і захисних засобів, які дають змогу підтримувати стабільність функціонування організації, забезпечувати

реалізацію інтересів її стейкхолдерів та зберігати здатність протидіяти ризикам внутрішнього й зовнішнього походження. Методологічне осмислення цієї категорії ґрунтується на міждисциплінарному підході, у межах якого поєднуються положення економічної теорії, політичної економії, інституціоналізму, теорії міжнародних економічних відносин, менеджменту, фінансів, економіки підприємства та наукових підходів до вивчення безпеки.

До визначальних ознак економічної безпеки підприємства належить низка фундаментальних характеристик. Надійність виявляється у здатності підтримувати необхідний рівень захисту завдяки наявності певного резерву стійкості, що дозволяє зменшувати або нейтралізувати руйнівний вплив загроз. Гнучкість означає спроможність підприємства використовувати різноманітні способи узгодження інтересів без втрати належного рівня безпеки. Результативність розкривається через досягнення поставлених цілей у процесі управління економічною захищеністю, тоді як керованість передбачає можливість свідомого й цілеспрямованого впливу на ефективність відповідних управлінських процесів [1].

Економічна безпека та розвиток підприємства перебувають у тісній взаємозалежності, тому їх не можна аналізувати як відокремлені або автономні явища. Підтримання стабільності й забезпечення довгострокової стійкості розвитку можливі лише за умови, що потенційні загрози, здатні ускладнити реалізацію стратегічних цілей, своєчасно виявляються, оцінюються та нейтралізуються. Звідси випливає, що успішний розвиток суб’єкта господарювання безпосередньо залежить від достатнього рівня його економічної захищеності. При цьому процес розпізнавання, аналізу й оцінювання ризиків слід розглядати як органічну складову загальної системи забезпечення економічної безпеки.

Розвиток підприємства, можливість впровадження інновацій, утримуючи стабільність і стійкість в сучасних умовах є основними індикаторами оцінки стану економічної безпеки. Позитивна динаміка результатів діяльності створює основу для зміцнення захисного потенціалу підприємства, тоді як погіршення параметрів економічної захищеності може породжувати загрози для сталого розвитку та звужувати можливості досягнення стратегічних орієнтирів. У зв’язку з цим

дослідження економічної безпеки має здійснюватися не ізольовано, а в поєднанні з аналізом розвитку підприємства як складової стратегічного управління. У такому трактуванні управління економічною безпекою постає як комплексна система цілеспрямованих дій, зорієнтованих на забезпечення стабільного функціонування та поступального розвитку підприємства в умовах впливу як внутрішніх, так і зовнішніх загроз.

Аналіз наукових праць [2, 3, 4] дає підстави визначити сукупність вихідних методологічних положень, на яких базується дослідження економічної безпеки як відносно самостійної категорії економічної науки. Передусім вагоме значення має системний принцип, згідно з яким економічну безпеку підприємства варто розглядати не як набір окремих запобіжних або захисних дій, а як цілісну багаторівневу конструкцію, що поєднує управлінські, фінансово-економічні, виробничі, кадрові, інформаційні та інші функціональні складові. Саме такий підхід дає змогу встановлювати джерела небезпек, які формуються на стику різних напрямів діяльності, забезпечувати узгодження інтересів стейкхолдерів, брати до уваги емерджентні ознаки підприємства як єдиного організаційно-економічного утворення та вибудовувати внутрішньо погоджену політику його захисту. Водночас суттєву роль відіграє принцип комплексності, відповідно до якого рішення, пов’язані з управлінням економічною безпекою, повинні охоплювати всі ключові сфери функціонування підприємства й бути інтегрованими як у його щоденну діяльність, так і в довгострокові управлінські процеси. Принцип детермінізму, у свою чергу, орієнтує дослідника на виявлення причинно-наслідкових зв’язків між подіями, процесами та факторами, що визначають умови діяльності суб’єкта господарювання. Принцип цілеспрямованості передбачає, що підтримання належного рівня економічної безпеки має ґрунтуватися на конкретизованих, досяжних і забезпечених ресурсами цілях, які не існують окремо від загальної стратегії підприємства, а становлять її невід’ємний елемент. З позиції превентивного підходу система економічної безпеки повинна бути зорієнтована не стільки на усунення наслідків уже наявних проблем, скільки на завчасне попередження, послаблення або нейтралізацію потенційних загроз фінансового, ринкового,

інформаційного, правового, техногенного та іншого характеру. Принцип адаптивності й гнучкості розкриває здатність підприємства своєчасно змінювати наявні механізми захисту відповідно до трансформацій зовнішнього середовища, виникнення нових ризиків і загального посилення нестабільності. Економічна обґрунтованість означає, що кожний захід у сфері безпекового управління має оцінюватися крізь призму співвідношення необхідних витрат і можливого обсягу втрат, оскільки витрати на його реалізацію не повинні бути більшими за ймовірну шкоду від настання загрози. Принцип правомірності вимагає, щоб усі дії, спрямовані на забезпечення економічної безпеки, здійснювалися відповідно до чинних норм національного законодавства та узгоджувалися з положеннями міжнародного права. Завершальним у цій логіці є принцип безперервності управління, який передбачає постійний моніторинг внутрішніх і зовнішніх умов функціонування підприємства, своєчасну модернізацію захисних процедур і системне впровадження заходів, спрямованих на тривале збереження його економічних інтересів.

Водночас наведений перелік принципів не слід сприймати як вичерпний або остаточно сформований, адже в науковому дискурсі існують різні підходи до їх групування, тлумачення та змістового розмежування. У цьому дослідженні увагу зосереджено насамперед на тих методологічних орієнтирах, які, на нашу думку, найповніше відображають сутнісну природу економічної безпеки підприємства та дозволяють розкрити її значення для підтримання стабільної діяльності суб’єкта господарювання.

Сутність економічної безпеки - це взаємодія ключових елементів системи, які забезпечують її функціонування, підтримання та подальший розвиток. Такими складовими є об’єкти, суб’єкти, цілі та завдання. Об’єктом наукового аналізу є підприємство, як цілісна економічна система, процес його життєдіяльності, можливість підтримувати стабільне функціонування, спроможність адаптуватися до змін і забезпечувати розвиток за умов безперервних змін, невизначеності, ризиків, що виникають унаслідок таких трансформацій.

До суб'єктного складу економічної безпеки належать як учасники внутрішнього середовища підприємства, так і зовнішні стейкхолдери, інтереси яких безпосередньо або опосередковано перетинаються з його господарською діяльністю. Цілі економічної безпеки мають багаторівневу й складну природу, оскільки вони одночасно повинні забезпечувати баланс інтересів усіх залучених сторін і створювати передумови для протидії реальним та ймовірним загрозам. При цьому такі орієнтири не можуть формуватися поза межами загальної управлінської системи підприємства: вони мають бути органічно інтегровані в її структуру, взаємно узгоджені у часовому й просторовому аспектах, позбавлені внутрішніх суперечностей і не повинні спонукати виконавців до дій, що взаємно заперечують одна одну або породжують конфліктність управлінських рішень [3]. Складові економічної безпеки міжнародного бізнесу відображені у таблиці 1.1.

Таблиця 1.1

Складові економічної безпеки міжнародного бізнесу

Функціональний компонент	**Суть складової економічної безпеки міжнародного бізнесу**	**Загрози**
Фінансовий	Ліквідність, платоспроможність, економічна стійкість	Фінансові ризики, інфляція, нестача ресурсів
Кадровий	Розвиток кадрового, інтелектуального та трудового потенціалу	Нестача кваліфікованих робітників, безперервна плинність робочої сили
Виробничий	Постійне виробництва продукції, підвищена конкурентоспроможність	Збій виробничого процесу, старе обладнання
Технологічний	Розвиток та модернізація інновацій	Аварія, відсутність технічної еволюції
Інформаційний	Захист комерційних даних, інформації та ресурсів	Витік даних, кібератаки
Правовий	Дотримання прав та законів держав, правовий захист підприємства	Судові процеси, ризики пов'язані із регуляторною політикою держави
Екологічний	Правильне використання ресурсів, дотримання екологічних норм	Техногенні виклики, штрафи через порушення екологічних норм
Інноваційний	Впровадження нових технологічних рішень	Втрата конкурентної переваги
Репутаційний	Створення позитивногго іміджу підприємства	Підрив репутації, інформаційний напад та тиск

Примітка.Джерело: складено автором на основі [1-5]

Е. Данілова [5, с. 142] наголошує, що «метою (загальною ціллю) управління економічною безпекою підприємства є забезпечення організаційної стійкості та часової стабільності процесів функціонування та розвитку економічних відносин підприємства шляхом формування системи захисту від сукупності зовнішніх та внутрішніх небезпек».

Загальна спрямованість управління економічною безпекою зазвичай розкривається через низку часткових цілей, кожна з яких відображає окремий напрям безпекового забезпечення підприємства. Захисний орієнтир передбачає завчасне розпізнавання, запобігання та нейтралізацію загроз внутрішнього й зовнішнього походження за допомогою безперервного моніторингу середовища, захисту інформаційних ресурсів, комерційних інтересів та інших внутрішніх активів, протидії проявам кібершпигунства, рейдерським ризикам, а також належного забезпечення безпеки працівників. Фінансовий напрям пов’язаний із підтриманням платоспроможності, стабільності та економічної самостійності підприємства, що досягається через контроль грошових потоків, раціоналізацію витрат, управління ризиками й забезпечення прибутковості господарської діяльності. Виробнича мета полягає у збереженні конкурентних переваг продукції та утриманні позицій підприємства у відповідних сегментах ринку. Техніко-технологічний аспект орієнтований на зменшення вразливості підприємства перед технологічними ризиками шляхом своєчасної модернізації основних фондів, реалізації результативної інноваційно-інвестиційної політики, посилення виробничого й ресурсного потенціалу та його ефективного використання. Соціальний вимір економічної безпеки охоплює підвищення кваліфікації персоналу, розвиток його інтелектуального ресурсу, формування зацікавленості всіх учасників у довгостроковому поступі підприємства та забезпеченні їхніх інтересів. Правова складова спрямована на захист інтересів підприємства в межах чинного правового поля, дотримання нормативних вимог і зниження ймовірності юридичних ризиків. Екологічний орієнтир, у свою чергу, пов’язується з довгостроковим плануванням, ощадливим і раціональним використанням ресурсної бази, адаптацією до змін

зовнішнього середовища та організацією господарювання з урахуванням засад сталого розвитку.

Цілі, через які конкретизується зміст економічної безпеки підприємства, мають спиратися на належне теоретичне осмислення й практичну доцільність, залишатися реалістичними, досяжними та узгодженими з фактичним потенціалом суб'єкта господарювання в конкретних умовах його діяльності. Водночас вони повинні відповідати раніше окресленим методологічним принципам. У процесі їх визначення необхідно враховувати не лише бажаний рівень захищеності підприємства, а й реальні ресурсні можливості, які можуть бути використані для досягнення та підтримання такого стану.

Виходячи з окреслених часткових цілей економічної безпеки, можна визначити основні напрями завдань, через які забезпечується її практична реалізація. Насамперед це стосується своєчасного розпізнавання, аналізу та запобігання загрозам, що потребує постійного вивчення як внутрішнього стану підприємства, так і умов його зовнішнього функціонування з метою виявлення можливих джерел уразливості, здатних активізуватися під впливом деструктивних факторів. У межах такого напряму особливого значення набувають ризик-оцінювання, дослідження змін ринкової кон'юнктури, а також систематичне спостереження за діями партнерів, конкурентного середовища та інших суб'єктів економічної взаємодії. Іншим важливим завданням є формування та регулярна модернізація комплексу заходів безпекового характеру. Його виконання передбачає виявлення недоліків у наявній організаційній моделі управління безпекою, періодичну діагностику стану економічної захищеності підприємства, а також подальше уточнення політик, процедур і стратегічних підходів до її забезпечення. До цього ж блоку належить розроблення інструментів раннього розпізнавання кризових сигналів, використання превентивних механізмів для послаблення чи нейтралізації потенційних ризиків, підготовка варіантів дій у надзвичайних ситуаціях з метою мінімізації можливих збитків, а також визначення ефективності вже реалізованих управлінських рішень.

Одним із ключових завдань у системі економічної безпеки виступає забезпечення фінансової рівноваги підприємства, що передбачає підтримання належного рівня ліквідності, платоспроможності та загальної фінансової стійкості. Реалізація цього напряму пов'язана з раціоналізацією витрат, ефективним використанням ресурсного потенціалу, запобіганням непередбаченим втратам і побудовою такої організаційної структури, яка сприятиме стабільності господарської діяльності. Самостійного значення набуває також зміцнення технологічної незалежності виробництва й підтримання конкурентоспроможності продукції. У цьому контексті йдеться про модернізацію виробничої бази та технологічних процесів шляхом інвестиційного забезпечення, впровадження інноваційних рішень, оперативного реагування на потреби ринку, переорієнтації на випуск високотехнологічної продукції споживчого призначення з належними якісними параметрами, освоєння нових ринків і розширення присутності в уже сформованих сегментах, а також адаптацію підприємства до цифровізаційних процесів і глобалізаційних трансформацій.

Суттєве місце серед завдань економічної безпеки посідає охорона матеріальних і нематеріальних ресурсів підприємства. Її зміст полягає у недопущенні неправомірного доступу до активів, запобіганні пошкодженню або втраті майна, протидії шахрайським діям, корупційним ризикам, рейдерським загрозам, кіберзлочинності, промисловому шпигунству та проявам недобросовісної конкуренції. У цій же площині важливого значення набуває захист конфіденційних відомостей, пов'язаних із комерційними, технологічними та ринковими аспектами діяльності підприємства, охорона прав інтелектуальної власності, забезпечення інтересів внутрішніх зацікавлених сторін, утримання кваліфікованих працівників і нарощування інтелектуального капіталу. Правова захищеність суб'єкта господарювання досягається через узгодження його діяльності з вимогами чинного національного та міжнародного права, дотримання принципів добросовісної конкуренції, відстоювання інтересів підприємства у правовому полі, а також організацію захисту персоналу від зовнішніх загроз і ризиків, зумовлених людським фактором. Окремим складником виступає екологічна безпека, яка за сучасних умов

розглядається не лише як вимога відповідального господарювання, а й як елемент корпоративної соціальної відповідальності та орієнтації на сталий розвиток. Її практичне забезпечення може здійснюватися, зокрема, через упровадження екологічно безпечних технологій виробництва та залучення відновлюваних енергетичних джерел.

Окреслені завдання не можуть розглядатися як ізольовані напрями діяльності, адже між ними існує стійка функціональна взаємозалежність. Їх практичне виконання потребує цілісного підходу, зорієнтованого на підтримання належного стану економічної захищеності підприємства та досягнення її достатнього рівня. Реалізація відповідних завдань разом із досягненням визначених цілей формує необхідні передумови для стабільного функціонування підприємства, збереження конкурентних позицій його продукції та пристосування до економічного середовища, яке постійно змінюється й характеризується посиленням ризиків. Водночас економічну безпеку не слід зводити лише до процесу ідентифікації загроз і ризиків та подальшого розроблення заходів для їх подолання. Її зміст є ширшим, оскільки охоплює здатність підприємства реально впроваджувати такі заходи, забезпечувати неперервність господарських процесів і послідовно досягати стратегічних цілей розвитку.

Дослідження показало, що економічна безпека підприємства має не лише складну, а й багатоступінчату природу у поєднанні із кількома різними аспектами. Згідно проведеного аналізу можна сказати, що економічна безпека - це стан захищеності від реальних та можливих загроз, швидка адаптація при непередбачуваних обставинах та підвищення конкурентно спроможності з урахуванням зовнішніх факторів та змін, таких як воєнний стан, світові фінансові кризи, цифрові метаморфози в економічній сфері. Визначено, що методологічне підґрунтя дослідження економічної безпеки формується на основі міждисциплінарного бачення, яке інтегрує базові положення економічної теорії, управлінської науки та суміжних галузей знань.

У межах проведеного аналізу розкрито провідні властивості економічної безпеки підприємства та показано її зв’язок із процесами розвитку суб’єкта

господарювання. На основі опрацювання наукових джерел виокремлено основні методологічні засади дослідження економічної безпеки як економічної категорії, а також проаналізовано її цільові орієнтири й завдання на рівні підприємства. Обґрунтовано, що сучасне розуміння структури економічної безпеки не може обмежуватися лише класичними складовими, серед яких фінансова, виробнича та кадрова, оскільки в умовах Industry 4.0 дедалі більшого значення набувають інформаційний, інноваційний та екологічний виміри. Забезпечення економічної безпеки передбачає не тільки реагування на загрози й мінімізацію їхнього впливу, а й цілеспрямоване управління ресурсним потенціалом, підтримку інноваційного поступу, захист інтелектуальної власності та формування високого рівня організаційної стійкості. Подальші дослідженні в перспективі слід пов’язати із розробкою інструментів оцінювання рівня економічної безпеки відповідно до її функціональних завдань, а також із вивченням можливостей впровадження цифрових технологій у систему управління безпекою підприємства.

1.2. Кіберзагрози та геополітична нестабільність як чинники впливу на діяльність суб’єктів міжнародних економічних відносин

Основні напрями світової системи часто перебувають в умовах постійних змін, особливо останнім часом на це дуже впливає політичний режим та напруження міжнародних взаємодій, що відображається на кон’юктурі ринків та спричиняє загрози в сфері кібербезпеки. У такому контексті геополітика постає як дослідницький напрям, що дає змогу пояснити взаємозалежність між просторово-географічними параметрами, політичною діяльністю та системою міжнародних відносин. Її предметне поле охоплює аналіз конфліктів і форм політичної взаємодії на глобальному рівні з урахуванням просторового чинника, оскільки поведінка держав у міжнародному середовищі значною мірою визначається їхніми фізико-географічними характеристиками [6].

Посилення геополітичної напруженості та зростання політичної непередбачуваності належать до тих факторів, які можуть запускати несприятливий інвестиційний цикл для багатонаціональних компаній. Політичне середовище

традиційно тісно пов’язане з рухом прямих іноземних інвестицій, оскільки інвестори оцінюють не лише макроекономічні показники, а й стійкість політичних інститутів, рівень міжнародної конфліктності та ймовірність регуляторних чи безпекових зрушень. З огляду на це геополітичний ризик посідає особливе місце в системі інвестиційного аналізу, адже його реалізація здатна суттєво змінювати кінцеву ефективність вкладеного капіталу [7].

Подальше дослідження доцільно зосередити на тому, у яких формах геополітичні ризики виявляються на макроекономічному рівні та яким чином вони впливають на побудову, структуру й результативність інвестиційного портфеля, що узагальнено в табл. 1.2.

Таблиця 1.2

Вплив геополітичних ризиків

Рівень	Значення
Макроекономічний рівень	Геополітичні чинники суттєво впливають на функціонування ринків капіталу, зокрема на темпи економічного зростання, рівень відсоткових ставок і загальну нестабільність фінансового середовища. Такі зміни формують нові умови для інвестування та визначають підходи до розподілу активів, включаючи вибір географічних напрямів вкладень.
Рівень інвестиційного портфеля	Геополітичні ризики можуть змінювати відповідність окремих фінансових інструментів чи стратегій цілям інвестора, його ризик-профілю та інвестиційному горизонту. Зростання рівня ризику впливає на очікувану дохідність активів, а також на умови діяльності галузей і компаній, що визначає їхню інвестиційну привабливість.

Примітка. Джерело: складено автором з використанням [8]

Нездатність державних інституцій результативно обмежувати поширення сепаратистських тенденцій, надмірне зосередження владних ресурсів, посилення управлінської централізації та інші споріднені процеси можуть бути віднесені до проявів геополітичної ризикогенності, оскільки за таких умов постає небезпека послаблення політичної самостійності держави, втрати суверенних повноважень і

незалежного статусу [9]. Геополітика у більшості випадків спрямована на дослідження політичної влади крізь призму її взаємозалежності з просторово-географічними параметрами, через що в розширеному трактуванні її нерідко пов'язують із вивченням міжнародних політичних відносин. У центрі її уваги перебувають політичні процеси, що розгортаються між державами або регіональними просторами, зокрема такі формати взаємодії, як відносини між США та Китаєм або між росією та Україною.

Під геополітичною напруженістю доцільно розуміти стан політичних протиріч, до яких безпосередньо або опосередковано залучаються дві чи більше держави та які здатні породжувати нестабільність, конфліктність і загострення суспільно-політичної ситуації. Сучасний етап світового розвитку характеризується інтенсифікацією таких явищ, що пояснюється накопиченням економічних, соціальних, релігійних, територіальних та ідеологічних суперечностей. Особливу загрозу становить тенденція, за якої подібні протиріччя дедалі частіше вирішуються не засобами дипломатичного діалогу чи економічного впливу, а через застосування воєнної сили [10].

На фінансових ринках невизначеність, як правило, підсилює прагнення інвесторів уникати ризикових інструментів і водночас збільшує волатильність. Досвід попередніх геополітичних потрясінь свідчить, що після первинного шоку ринки нерідко демонструють короткострокову нестабільність і негативну реакцію, проте надалі здатні досить швидко відновлювати позитивну динаміку. Зокрема, у 83% випадків через рік після геополітичної події ринки знову переходили до зростання, а середній приріст дорівнював 12,3% [11].

Отже, попередній історичний досвід дозволяє сформулювати певні узагальнення, однак не дає підстав для точного прогнозування майбутньої динаміки економічної активності чи поведінки фондових ринків, оскільки кожна геополітична подія має власну природу, масштаб впливу та наслідки. Водночас спостереження за минулими кризами показують, що військово-політичні конфлікти не в усіх випадках призводять до повноцінного формування ведмежого ринку. Здебільшого зниження після таких подій є відносно обмеженим і короткотривалим та не досягає позначки у

20%, яку традиційно розглядають як межу переходу ринку до ведмежої фази. Після проходження локального мінімуму ринки зазвичай демонструють прагнення до відновлення висхідної тенденції.

Світова економіка вразлива та не відрізняється стабільністю в наш час. США та держави Євросоюзу ризикують продовжити тенденцію економічного спаду. Китай має низкий темп приросту за осанні кілька років. З урахуванням цих факторів геополітична ситуація продовжує бути напруженою. Питання енергетики та кліматичні проблеми залишаються предметом політичної поляризації, тоді як глобальний поступ у напрямі протидії кліматичним загрозам усе ще є недостатнім. Разом із тим різке підвищення вартості енергоносіїв, спричинене вторгненням росії в Україну, може виступити додатковим чинником прискорення декарбонізаційних процесів. Однак цей можливий імпульс формується на тлі руйнування економічних систем, звуження можливостей зайнятості, падіння доходів населення та поширення бідності. Найбільш болісні соціальні наслідки війни пов'язані з втратою людського потенціалу країни внаслідок загибелі цивільного населення та масштабних міграційних процесів [12].

Світова реакція за пандемії COVID-19 досі виклакає дискусії, що відображається на економіці та соціальній сфері, тому що кожна держава прагне максимально зменшити залежність від зовнішніх стресів і зробити стабільною свою економічну систему. Одночасно з цим кібератаки стають частішими, масштабнішими й небезпечнішими, а також дедалі частіше використовуються як інструмент державного впливу. У міру цифровізації критичної інфраструктури зростають як людські, так і фінансові втрати, пов'язані з такими атаками. Посилення кіберзагроз щодо інформаційної інфраструктури створює ризики для конфіденційності, цілісності та доступності важливих даних і систем, що, своєю чергою, негативно впливає на фінансову, економічну й політичну стабільність держави [13].

Геополітичні конфлікти в наш час піддають небезпеці не тільки шляхи міжнародної торгівлі, а й в цілому погано впливають на стан суспільного добробуту. Проте для глибшого осмислення їхніх реальних наслідків доцільно застосовувати

багатогалузеву та багаторегіональну модель загальної рівноваги, здатну враховувати динамічне поширення знань усередині окремих секторів економіки. Саме такий аналітичний підхід дає можливість точніше показати, як торговельні конфлікти посилюють втрати добробуту. Передавання ідей у цьому випадку відбувається через структуру виробничих витрат і випуску, унаслідок чого секторальний розподіл витрат та частки імпортної торгівлі можуть розглядатися як індикатори джерел формування знань і напрямів їх подальшого поширення.

Ситуація 2022 року наочно показала геополітичну неясність і вразливі місця. Підприємства, які прагнули до максимальної реалізації скорочення витрат, намагаючись знайти нові шляхи збуту у різних куточках світу, ще більше ускладнили правила та умови ведення бізнесу. Підивщення геополітичної конкуренції показує, які саме регіони є критично значущими і посідають ключове місце в багатополярній світовій системі. Росія, Китай, Туреччина, Саудівська Аравія та Іран шляхом демонстрації політичної та військової сили дедалі погіршують і так вже наявні зіткнення. Конфлікт, спричинений вторгненням Росії на територію України, суттєво погіршив характер відносин між США та РФ, а також підвищив ризик ширшої ескалації на європейському континенті. Можна очікувати, що напруга між росією та сусідніми країнами - членами НАТО надалі посилюватиметься, тоді як Сполучені Штати, з огляду на свої союзницькі безпекові зобов'язання в межах Альянсу, ймовірно, залишатимуться залученими до цих процесів. Крім того, зазначений конфлікт матиме значно ширші наслідки для майбутньої міжнародної взаємодії з низки принципово важливих питань, серед яких доцільно виокремити такі напрями (рис. 1.1).

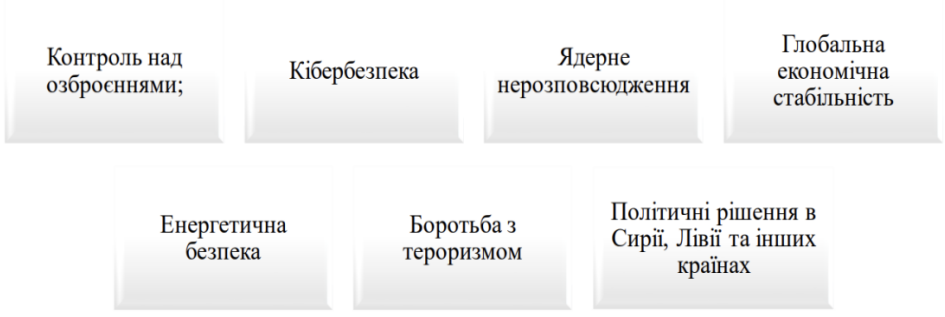

Рис. 1.1. Наслідки російсько-українського конфлікту

Примітка. Джерело: складено автором з використанням [14]

Світові потоки прямих іноземних інвестицій розвиваються нерівномірно та характеризуються значними коливаннями, що значною мірою пояснюється впливом глобальних економічних шоків і геополітичних протистоянь. Водночас інвестиційна динаміка в різних регіонах не має єдиного характеру, оскільки транснаціональні корпорації, що походять із розвинених економік, дедалі стриманіше підходять до нарощування капіталовкладень за кордоном [15].

За сучасних умов для підприємств дедалі важливішим стає не лише усвідомлення сутності геополітичних ризиків, а й формування дієвих механізмів реагування на виклики, пов’язані із зовнішньополітичними процесами. Якщо раніше локальні прояви нестабільності переважно сприймалися як чинники можливих порушень у ланцюгах постачання, то нині глобальні конкуренти значно активніше використовують санкційні режими, фінансові обмеження та торговельні ембарго. Такі інструменти виконують не тільки функцію регулювання міжнародної торгівлі, що ґрунтується на визначених правилах, а й дедалі частіше застосовуються як засоби реалізації зовнішньополітичних цілей. Унаслідок цього бізнес стає більш залежним від подій, які відбуваються на значній географічній відстані, а також від урядових рішень, ухвалених у відповідь на ці події.

Характерним прикладом такої трансформації є технологічне розмежування, зумовлене загостренням конкуренції між США та Китаєм. Воно може мати безпосередні практичні наслідки для європейських компаній, що здійснюють діяльність на китайському ринку, а також підвищує ймовірність перегляду та перебудови ланцюгів постачання. Одночасно часткові санкційні режими створюють нові й постійно змінювані ризики, пов’язані з необхідністю дотримання регуляторних вимог і можливими збоями у глобальних постачальних зв’язках. За таких обставин політичні чинники неминуче співвідносяться з комерційними інтересами, оскільки Китай для значної кількості західних компаній залишається стратегічно важливим ринком і одним із провідних торговельних партнерів. Отже, геополітичні конфлікти спричиняють посилення ринкової нестабільності та

змінюють конфігурацію міжнародного бізнес-середовища, що проявляється у таких напрямах (рис. 1.2).

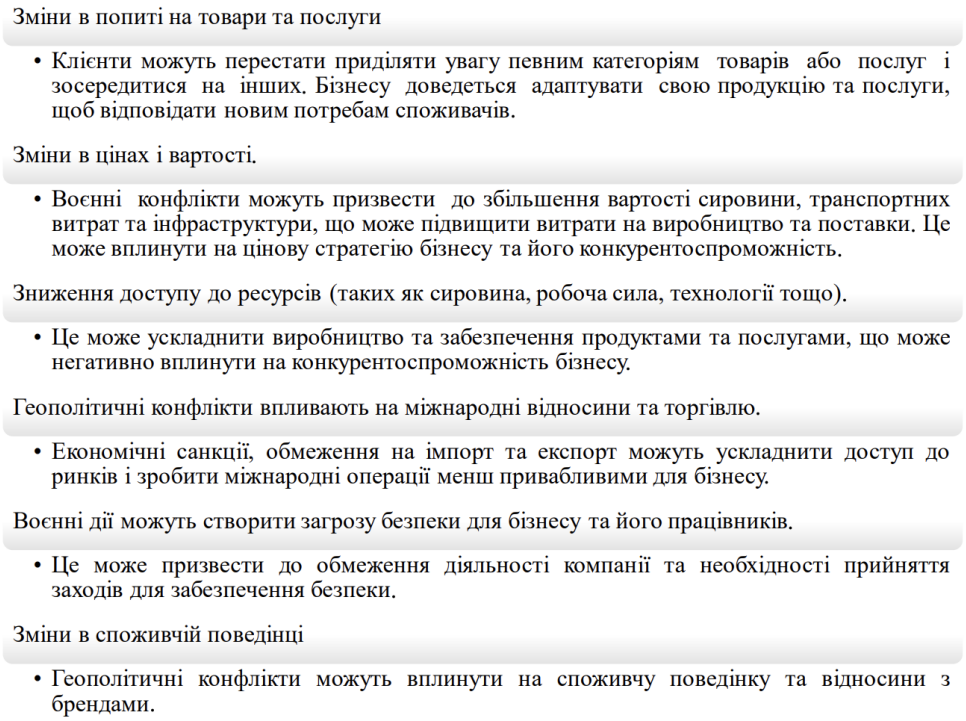

Рис. 1.2. Аспекти нестабільності міжнародного бізнес-середовища

Примітка. Джерело: складено автором з використанням [16]

Відповідь західних країн на агресивний зовнішньополітичний курс Росії створила значущий прецедент використання фінансових санкцій, як засобу стримування та протидії силовим геополітичним діям. Унаслідок цього банківські установи й інші суб’єкти фінансового сектору фактично перетворилися на важливих виконавців зовнішньополітичних рішень держав. Для підприємницького середовища така ситуація зумовлює потребу в постійному моніторингу змін регуляторних режимів і глибокому розумінні того, як ці зміни впливають на господарські процеси.

Озброєнні конфлікти по всьому світу завжди породжують для великих корпоративних підприємств та інвесторів ряд ускладнень. Це завжди виклик міжнародному бізнесу, порушення логістики, економічні та фінансові ризикі і втрати. В таких умовах компаніям треба не тільки адаптуватися до світових метаморфоз, а й розробити нові стратегії планування і результативності, щоб вистояти цей мінливий період.

Такі великі держави, як США та Китай протягом довгого часу не можуть прийти до спільного рішення, їх контрольоване охолодження відносин в будь-який момент може перерости у фазу загострення, що в свою чергу запустить ланцюгову реакцію по всій світовій системі. Тому підприємства прагнуть до превентивних дій, для зниження ризиків ще задовго до можливого зіткнення, наприклад, обмеження співпраці із постачальниками китайської держави і перегляд інших альтернативних шляхів. Ці трансформації можуть спричинити перебудову, скорочення або регіональне переорієнтування ланцюгів постачання, а також зміну напрямів руху інвестиційних потоків. У перспективі очікується їх суттєве переформатування, що водночас відкриватиме нові можливості для окремих регіонів. Зокрема, Японія та Південна Корея, які мають географічну близькість до Китаю й володіють потужним технологічним потенціалом, можуть отримати додаткові інвестиційні надходження внаслідок перенесення частини виробничої та інвестиційної активності [17].

Підтримуємо підхід, відповідно до якого у центрі сучасних геополітичних трансформацій перебувають чотири провідні сектори економіки (рис. 1.3).

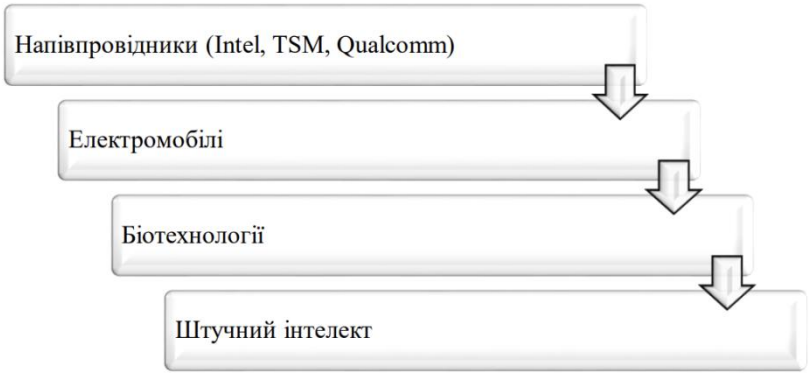

Рис. 1.3. Сектори в епіцентрі поточного геополітичного руху

Примітка. Джерело: складено автором з використанням [18]

Загострення геополітичної ситуації знижує прагнення інвесторів брати на себе невиправдані ризики, навіть короткі економчні коливання мають значно потужніший вплив, ніж позитивні зрушення. Найбільш відчутно такі наслідки проявляються саме на ринках, що розвиваються, тоді як розвинені економіки реагують на них відносно стриманіше. Серед розвинених ринків європейські майданчики, як правило, виявляються чутливішими до геополітичних потрясінь, ніж

ринок США. Підвищення нафтових цін, спричинене можливими перебоями у пропозиції, може впливати на споживчу поведінку в США, однак, попри поширені очікування, найбільш імовірно воно позначатиметься не стільки на дорогих товарах дискреційного попиту, скільки на секторі базового споживання, зокрема на супермаркетах, дискаунтерах і товарах особистого користування [19].

Саме цим можна частково пояснити відносно нижчу питому вагу базових споживчих товарів у відповідному портфельному підході порівняно з більшою часткою товарів дискреційного споживання. Разом із тим компанії енергетичного сектору здатні отримувати додаткові переваги від зростання вартості нафти, а вищий рівень енергетичної самозабезпеченості США може певною мірою пом'якшувати наслідки глобальних шоків пропозиції.

Фінансові вливання в розробку передових технологій набуває все більших труднощів через високу варість, обмежені ресурси і необхідності доволі суттєвого проміжку часу очікування бажаної рентабельності. Сповільнений розвиток даної сфери призводить до того, що увійти до числа обраних учасників технологічного прориву вже не вдастся, а разом з тим і використати іноваційні підходи для підвищення результативності діяльності не буде можливим.

Розвиток технологічної сфери вже не раз довів своє ефективність докорінно змінювати роботу у важливих галузях онорони здоров'я та виробництва. Стрімкий розвиток штучного інтелекту посилює загрозу кібератак, в той час як немає чіткої межі для визначення відповідальності між державними органами, комерійними підприємствами та звичайними користувачами, що ставить це питання на одне із перших місць для скорішого вирішення проблеми.

Зростання складності та винахідливості кібернападів, а також ускладнення управління кіберризиками свідчать про те, що бізнес і надалі змушений буде реагувати на масштабні виклики у сфері цифрової безпеки. Водночас підприємства не завжди мають змогу своєчасно встановити джерело потенційного саботажу або визначити, від кого саме може походити така загроза.

Для реалістичного визначення рівня кіберзахищеності організації особливого значення набувають глибоке моделювання ризиків та їх кількісна оцінка. Такі

інструменти дають управлінцям можливість з’ясувати, які саме механізми контролю у сфері кібербезпеки найбільше сприяють зниженню ризиків, а отже, дозволяють спрямовувати ресурси на напрями з найвищою практичною віддачею. Разом із тим наведені чинники можна трактувати як наслідок недосконалості управлінських рішень, що ухвалюються різними органами державної влади. На жаль, діяльність державних інституцій і надалі залишається суперечливою: вона часто орієнтується на досягнення окремих цілей, однак недостатньо враховує необхідність практичного пристосування запроваджуваних заходів до реальних умов, у яких перебуває Україна. У результаті поряд із частковим вирішенням окремих макроекономічних проблем відбувається подальше загострення соціально-економічних труднощів.

1.3. Методи забезпечення економічної та кібербезпеки міжнародного бізнесу

Численні міжнародні організації та аналітичні структури наголошують на зростанні ймовірності кібератак проти сучасних підприємств, оскільки їх дедалі глибша інтеграція у глобальні цифрові мережі водночас підвищує рівень технологічної взаємозалежності та вразливості. Показовими в цьому контексті є дані, наведені у звіті Cisco: у 86% організацій було зафіксовано принаймні одну спробу переходу працівників на фішинговий сайт; 70% організацій мали користувачів, які стикалися зі шкідливою рекламою у браузері; у 48% компаній виявлено активність зловмисного програмного забезпечення, спрямованого на викрадення інформації [21].

У звіті Europol [21] окрему увагу приділено формуванню та розширенню кіберзлочинної економіки, що охоплює діяльність організованих злочинних груп, особливості їхньої внутрішньої структури, механізми залучення спеціалістів, способи підготовки й реалізації кібератак, а також отримання матеріальної вигоди від протиправної діяльності. Крім того, у документі аналізуються трансформації, яких зазнав європейський ринок після початку російсько-української війни. Базовим ресурсом такої нелегальної економічної моделі виступають викрадені дані, що здобуваються за допомогою різних видів кібернападів і надалі реалізуються на

тіньових ринках. Збільшення кількості інцидентів у сфері інформаційної безпеки в умовах цифровізації економіки зумовлене широким упровадженням, ускладненням і поширенням цифрових технологій. Значна частина загроз для інформаційної, а отже, і для економічної безпеки підприємств, виникає саме через цифрові інструменти, які вони використовують. Вразливості як ключові джерела ризику можуть бути присутніми в різних елементах цифрової екосистеми: вебсайтах, мобільних застосунках, офіційних онлайн-ресурсах підприємств, підключених мережевих пристроях, корпоративних серверах та інших технологічних компонентах.

Підприємства Європейського Союзу застосовують різноманітні підходи до забезпечення кіберзахисту та зниження ризиків, пов'язаних із цифровими загрозами. За інформацією Статистичної служби Eurostat [22], до найпоширеніших інструментів захисту даних і протидії кібератакам належать автентифікація із застосуванням складних паролів, резервне копіювання важливої інформації з використанням хмарних технологій, а також мережевий контроль доступу, що узагальнено в таблиці 1.3.

Таблиця 1.3

Основні інструменти захисту даних, що застосовуються підприємствами ЄС

Показник	2019	2022
Частка підприємств ЄС, які використовують щонайменше один засіб IT-безпеки	85%	92%
Використання складних паролів для автентифікації	76%	82%
Застосування резервного копіювання даних (зокрема хмарних сервісів)	75%	78%
Використання систем контролю доступу до мережі	64%	65%
Використання VPN для захищеного з'єднання	42%	49%
Ведення журналів подій після інцидентів безпеки	45%	45%
Моніторинг та виявлення підозрілої активності	41%	–
Шифрування даних, документів та електронної пошти	38%	36%
Проведення тестування IT-безпеки	35%	35%

Оцінювання ІТ-ризиків	33%	32%
Використання щонайменше двох факторів автентифікації	31%	–
Використання біометричних методів ідентифікації	9,6%	13%

Примітка. Джерело: складено автором з використанням [22]

Отже, європейські компанії дедалі активніше залучають цифрові рішення для запобігання кіберзагрозам і мінімізації їхнього впливу на господарську діяльність. Водночас значна частина підприємств формує спеціалізовані внутрішні політики, регламенти та протоколи, спрямовані на захист даних і належну організацію системи кібербезпеки. Узагальнення теоретичних напрацювань [23-26] дало змогу виокремити сім основних інструментів забезпечення економічної безпеки підприємства в умовах цифрової трансформації, що систематизовано на рис. 1.4.

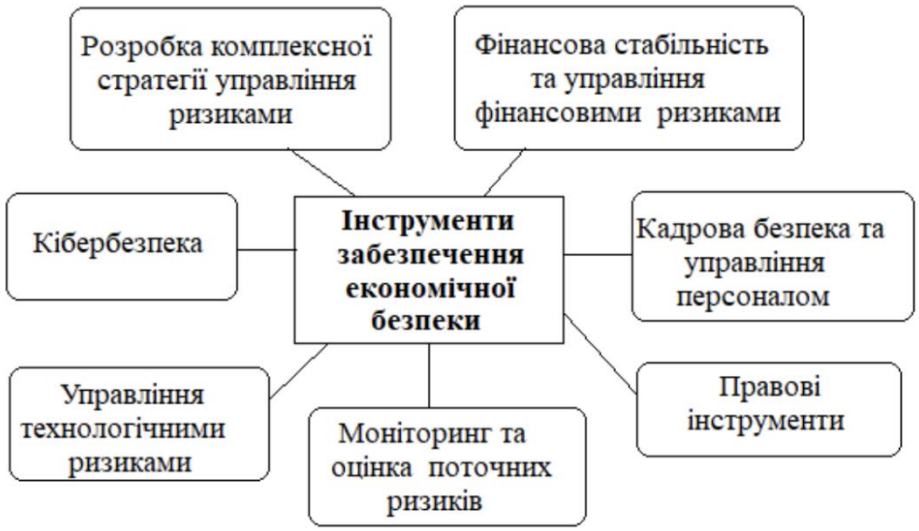

Рис. 1.4. Методи (інструменти) забезпечення економічної безпеки підприємства під час упровадження цифрових інновацій

Примітка. Джерело: складено автором з використанням [23-26]

Розробка стратегії ризик-менеджменту підприємств має включати визначення і оцінку всіх ймовірних ризиків, впровадження засобів їх послаблення та відшкодування можливих витрат, постійне спостереження щодо змін у характері загроз. Створення резервних планів допоможе підготуватися до нестандартних,

надзвичайних кризових ситуацій, з можливістю оперативного реагування та швидкого відновлення діяльності.

Використання систем кіберзахисту, такі як шифрування даних та інформації, багатоступінчаста автентифікація, безперервне оновлення програм і системи антивірусів можуть забезпечити стабільне функціонування інформаційної сфери підприємств.

Основі інструменти зниження ризиків в системі екномічної безпеки - це рішення і стратегії, які допомагають обмежити негативний фактор впливу загроз із внутрішнього та зовнішнього середовищ.Розмежування активів між різними галузями і географічними напрямами, зменшить високу вирогідність фінансових втрат на багальох ринкових сегментах.

Людський ресурс та кадровий захист важливі в управлінні бізнес-процесами. Програми підвищення кваліфікації, розвиток та утримання фахових спеціалістів, за допомогою систем мотивації та винагород, суттєво зменшить ризики втрати робочої сили.

Постійна перевірка і оцінка можливих ризиків мають охоплювати аналітичний сегмент, прогнозування і інструменти превентивного впливу для ранньої стадії виявлення загрози. Хмарні технології дають можливість опрацьовувати великий обсяг даних і інформації, спрогнозувати небезпеку та тенденції, які негативно позначаються на рівні фінансової безпеки підприємств.

Підприємства різних галузей у світовій практиці дедалі активніше використовують цифрові інструменти для мінімізації ризиків і підтримання належного рівня економічної безпеки, що узагальнено в табл. 1.4.

Подані приклади демонструють, як великі корпорації впроваджують цифрові стратегії з урахуванням можливих загроз, передусім у напрямах кіберзахисту та охорони даних.

Їхній досвід свідчить про можливість поєднання інноваційного розвитку із забезпеченням бізнес-стійкості, що дає змогу ефективніше пристосовуватися до змін цифрового середовища.

Вивчення таких практик може слугувати для інших компаній практичним орієнтиром під час визначення пріоритетів цифрового інвестування, спрямованого на збереження фінансової та операційної стабільності.

Таблиця 1.4

Приклади застосування цифрових інструментів для забезпечення економічної безпеки компаніями

Компанія, галузь	Цифрові інструменти	Програма оцінки ризиків та її результати
Siemens (електроніка)	Стратегія «Vision 2020+», IoT-платформа MindSphere, Mendix (платформа для розробки застосунків), цифрові сервіси	Запроваджено багаторівневу систему захисту, здійснюється постійний моніторинг кіберзагроз у режимі реального часу, реалізуються програми підвищення обізнаності персоналу щодо кібербезпеки. Це забезпечило стабільність операційної діяльності та зниження впливу цифрових ризиків, а також підвищення ефективності виробництва завдяки автоматизації й аналітиці.
General Electric (електротехніка, машинобудування)	Концепція «Industrial Internet», орієнтована на інтеграцію IoT для оптимізації виробництва та зменшення витрат	Сформовано надійну систему кіберзахисту, що включає виявлення аномалій, багатофакторну автентифікацію, шифрування інформації та регулярні перевірки безпеки виробничих процесів.
Netflix (медіа)	Використання Big Data для персоналізації контенту та прогнозування поведінки користувачів	Застосовується шифрування даних і системи моніторингу для оперативного виявлення кіберзагроз. Також впроваджено політики тестування безпеки та відновлення даних у разі збоїв або атак.
Walmart (ритейл)	Аналітика даних і штучний інтелект для прогнозування попиту, управління запасами та оптимізації логістики	Компанія забезпечує захист персональних даних клієнтів шляхом використання шифрування та багатофакторної автентифікації при обробці інформації.
Toyota (автомобілебудування)	Впровадження IoT у виробництво та автомобільні технології, створення «розумних» транспортних засобів, використання даних для оптимізації процесів	Для захисту інформації застосовуються криптографічні методи, що забезпечують безпеку збережених і переданих даних.
Bank of America (фінансовий сектор)	Онлайн-банкінг і мобільні фінансові сервіси	Використовуються технології штучного інтелекту для управління ризиками та кредитування, а також аналітика великих

		даних для підтримки управлінських рішень.
PayPal (онлайн-платежі)	Цифрові платіжні платформи, мобільні сервіси	Застосовуються алгоритми машинного навчання та штучного інтелекту для виявлення шахрайства, а також шифрування даних для захисту транзакцій.

Примітка. Джерело: складено автором з використанням [27-30]

Таким чином, цифрові технології мають глибокий і багатогранний вплив на різні аспекти економічної безпеки. Для мінімізації ризиків та оптимізації переваг необхідно забезпечити баланс між технологічними інноваціями та захистом ключових компонентів економічної безпеки.

Висновки до розділу 1

Дослідження показало, що економічна безпека підприємства має не лише складну, а й багатоступінчату природу у поєднанні із кількома різними аспектами. Згідно проведеного аналізу можна сказати, що економічна безпека - це стан захищеності від реальних та можливих загроз, швидка адаптація при непередбачуваних обставинах та підвищення конкурентно спроможності з урахуванням зовнішніх факторів та змін, таких як воєнний стан, світові фінансові кризи, цифрові метаморфози в економічній сфері.

Визначено, що методологічне підґрунтя дослідження економічної безпеки формується на основі міждисциплінарного бачення, яке інтегрує базові положення економічної теорії, управлінської науки та суміжних галузей знань.

За сучасних умов для підприємств дедалі важливішим стає не лише усвідомлення сутності геополітичних ризиків, а й формування дієвих механізмів реагування на виклики, пов’язані із зовнішньополітичними процесами.

Якщо раніше локальні прояви нестабільності переважно сприймалися як чинники можливих порушень у ланцюгах постачання, то нині глобальні конкуренти значно активніше використовують санкційні режими, фінансові обмеження та торговельні ембарго. Такі інструменти виконують не тільки функцію регулювання

міжнародної торгівлі, що ґрунтується на визначених правилах, а й дедалі частіше застосовуються як засоби реалізації зовнішньополітичних цілей. Унаслідок цього бізнес стає більш залежним від подій, які відбуваються на значній географічній відстані, а також від урядових рішень, ухвалених у відповідь на ці події.

Приклади застосування цифрових інструментів для забезпечення економічної безпеки компаніями демонструють, як великі корпорації впроваджують цифрові стратегії з урахуванням можливих загроз, передусім у напрямах кіберзахисту та охорони даних. Їхній досвід свідчить про можливість поєднання інноваційного розвитку із забезпеченням бізнес-стійкості, що дає змогу ефективніше пристосовуватися до змін цифрового середовища.

Вивчення таких практик може слугувати для інших компаній практичним орієнтиром під час визначення пріоритетів цифрового інвестування, спрямованого на збереження фінансової та операційної стабільності.

Цифрові технології мають глибокий і багатогранний вплив на різні аспекти економічної безпеки. Для мінімізації ризиків та оптимізації переваг необхідно забезпечити баланс між технологічними інноваціями та захистом ключових компонентів економічної безпеки.

РОЗДІЛ 2

АНАЛІЗ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ МІЖНАРОДНОГО БІЗНЕСУ В УМОВАХ КІБЕРЗАГРОЗ ТА ГЕОПОЛІТИЧНОЇ НЕСТАБІЛЬНОСТІ

2.1. Тенденції розвитку загроз та механізми протидії економічній та кіберзлочинності у світовому господарстві

Швидкий розвиток інформаційних технологій, такі як хмарні сервіси, платформи блокчейну та інтернет суттєво розширюють цифрову комунікацію, тим самим наражають на небезпеку як корпоративні, так і персональні мережеві середовища. З урахуванням цих умов виникають нові типи кіберзагроз. Кібератаки мають такі форми противоправних дій, як:

- ✓ привласнення персональних даних;
- ✓ різні форми шахрайств інформації;
- ✓ незаконне втручання у роботу критичної інфраструктури;
- ✓ програми з ціллю вимагання та фішингові кампанії.

Згідно із даними онлайн-платформи Statista, у 2022 р. глобальні збитки, спричинені кіберзлочинністю сягають 7,1 трлн дол. США, в той час як у 2019 р. це було 1,2 трлн дол. США. Крім того, за інформацією Chainalysis, упродовж 2021–2022 рр. помітно зросла інтенсивність атак на криптовалютні біржі та протоколи, зокрема з боку північнокорейського хакерського угруповання Lazarus, яке пов’язують із державними структурами [31].

Результати досліджень, проведених фахівцями антивірусної компанії McAfee разом із Центром стратегічних та міжнародних досліджень, показують, що середньорічні глобальні втрати від хакерських атак становлять близько 600 млрд дол. США [4]. Головна проблема таких атак - це втрата персональної інформації про клієнтів та даних працівників. Викрадення даних або ж розкриття конфіденційної інформації дуже підриває репетацію компанії, знижує рівень довіри, і відповідно

має наслідки в стабільних прибутках та втраті фінансів. У пандемію COVID-19 - ця проблема набула дуже гострого характеру, більшість змушені були перейти на дистанційну форму роботи, що виявило численні прогалини у захисті IT-середовищ, і збільшило потенційну загрозу безпосередньо хмарних сервісів, зберігання цифрових даних та інших мережевих ресурсів. У 2022 р. міжнародна мережа професійних послуг PwC (PricewaterhouseCoopers) провела дослідження та підтвердила значний ріст кіберзлочинності у глобальному просторі. Велика частина користувачів, які зазнали впливу кібератак було зафіксовано в Індії, що склало 68%, у США - 49%. Ці дані свідчать про те, що кіберзлочини мають масштабну площину атак і становлять загрозу будь-якому користувачу у будь-якій країні проживання та перебування. З урахуванням цієї проблеми дуже актуальним стає набуття цифрової грамотності для захисту користувачів, нові шляхи захисту та удосконалення інструментів безпеки та розробки правил, які прямовані на запобігання всіх видів атак (рис. 2.1).

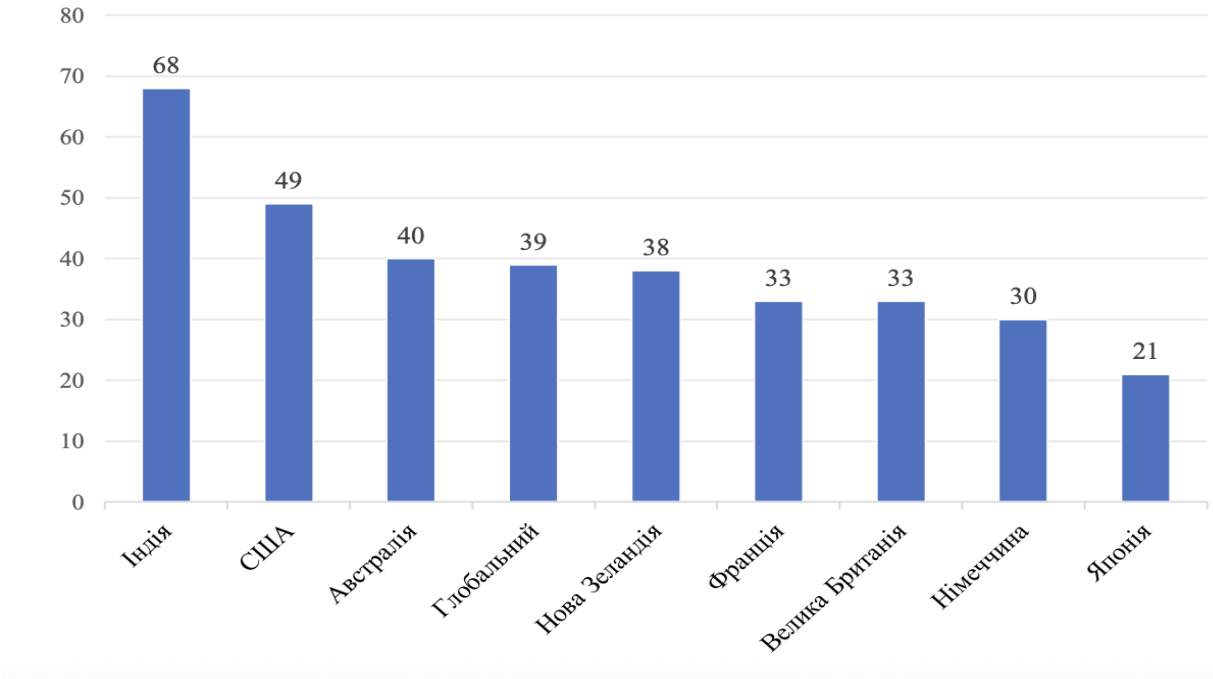

Рис. 2.1. Частка користувачів мережі «Інтернет» в окремих країнах, які коли-небудь стикалися з кіберзлочинами у 2022 р., %

Примітка. Джерело: складено автором з використанням [32]

У 2022 році фішингові атаки склали половину зафіксованих кіберзлочинів - 53,2%, які підтверджують факт найпоширенішого виду цифрового шахрайства. Такі дані свідчити можуть лише про одне, а саме, простота організації таких атак та її висока результативність. Фішинг із ціллю викрадення паролів та реквізитів банківських даних користувача може бути реалізований через комунікацію у соціальних мережах, введення в оману через будь-які форми впливу у електронних повідомленнях, перехід на фейковий вебресурс тощо. У запобіганні таких проблем допоможе двухфакторна або трехфакторна автентифікація і підвищенна обережність самого користувача мережею.

Варто звернути увагу, на те що інвестиційне шахрайство з урахуванням меншої частини залучених осіб - 5,4%, може мати більші наслідки, а саме шляхи маніпуляції інвесторами щодо невірних даних про акції, боргові зобов'язання та інші відомості про фінансові інструменти, може завдати не тільки шкоди окремим учасникам фінансових ринків, а й світовій економічній системі. Крім фінансових збитків, такі злочини підривають довіру до фінансових установ і механізмів економічного простору. Головні правила протидій цього виду шахрайств:

1) Посилання моніторингу підозрілих дій і швидкого виявлення шахрайських схем;
2) Вдосконалення систем боротьби із кібератаками та загрозами;
3) Підвищення рівня цифрової грамотності населення.

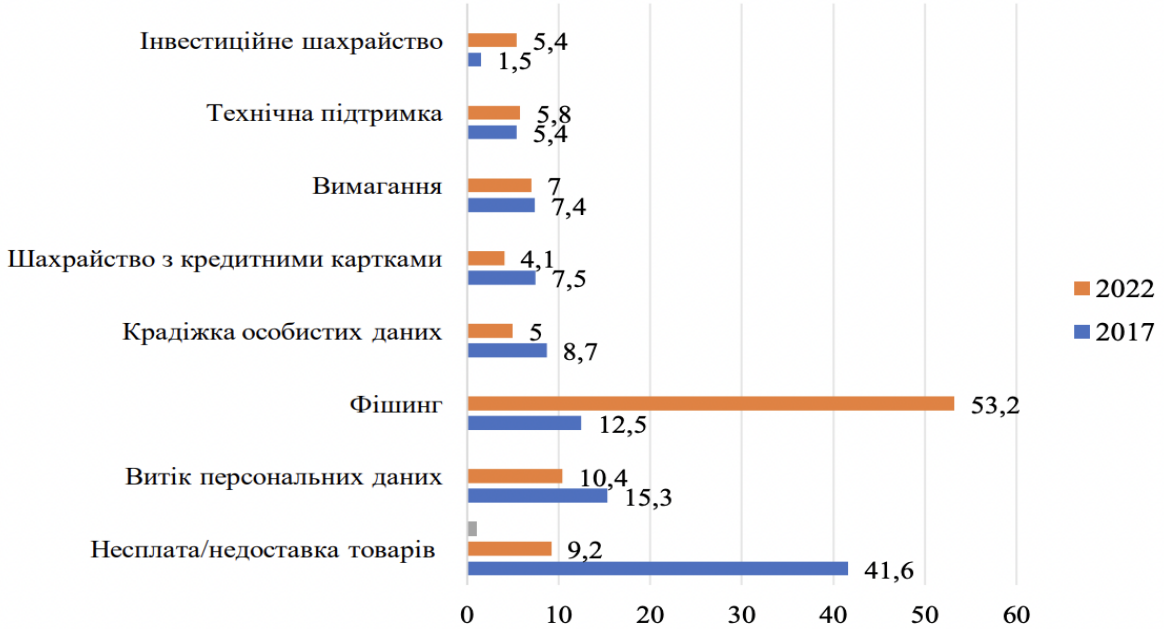

Рис. 2.2 Найпопулярніші кіберзлочини в мережі «Інтернет» у світі, 2017–2022 рр., %

Примітка. Джерело: складено автором з використанням [33-35]

Кіберзлочинність щороку ускладнюється, набуває нових форм і швидко пристосовується до технологічних змін. Динаміку кібератак за 2016–2023 рр. у розрізі їх основних видів подано на рис. 2.3.

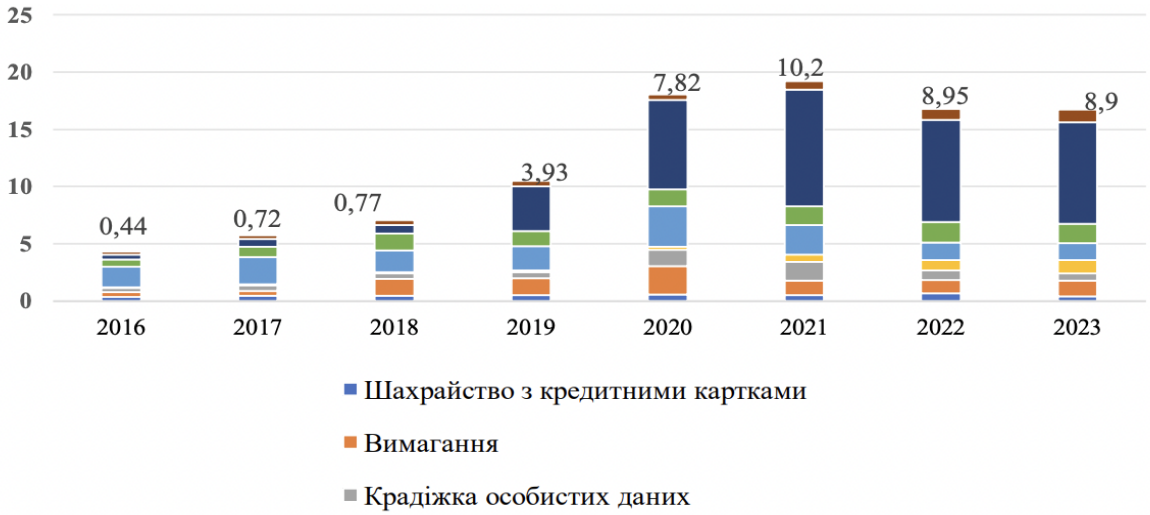

Рис. 2.3. Динаміка кібератак у світі в розрізі їх видів, 2016–2023 рр., млн од.

Примітка. Джерело: складено автором з використанням [36;37]

В період з 2016 по 2023 роки виявлено чітку тенденцію активного поширення фішингових атак у світі, в 2024 році зафіксовано більше 1 млн фішингових вебсайтів.

Друге місце серед видів кіберзлочинів займають атаки спрямовані на викрадення персональних даних, в 2022 році їх кількість досягла 1,66 млн випадків. Третє місце займають інциденти недоставки або несплати товарів - більше 1,5 млн.

Фішинг зазвичай здійснюється шляхом повідомлень, які отримує користувач через електронну пошту або в соціальних мережах. В даних повідомленнях завжди є пряме посилання на відповідні вебресурси, де жертва залишає свої конфіденційні дані для використання цієї інформації в подальшому шахраями задля отримання

доступу до аккаунту користувача. Крім того, посилання, розміщені у фальшивих повідомленнях, часто використовуються як канал проникнення шкідливого програмного забезпечення в інформаційні системи користувачів. За результатами дослідження PwC, проведеного у 2022 р. серед респондентів окремих країн, які коли-небудь зазнавали крадіжки персональних даних, найвищі показники було зафіксовано в Індії: зловмисники викрали дані понад 27,2 млн дорослих осіб (рис. 2.4).

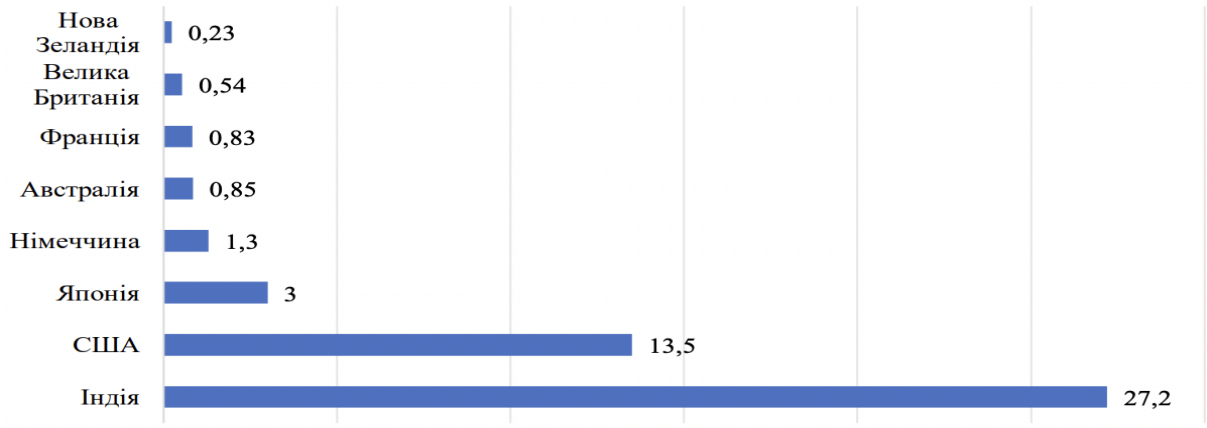

Рис. 2.4. Кількість дорослих, які стали жертвами крадіжки персональних даних у 2022 р., млн осіб

Примітка. Джерело: складено автором з використанням [38]

За обсягом втрат персональної інформації наступне місце посідають Сполучені Штати Америки, де кількість осіб, що постраждали внаслідок таких інцидентів, становить орієнтовно 13,5 млн. Третьою у цьому переліку є Японія, де було виявлено понад 3 млн випадків незаконного заволодіння особистими даними [32].

У 2023 році особливо поширена була схема шахрайства пов’язана із платіжними операціями. Більша частина правопорушень була спрямована саме з метою заволодіння доступів до банківських рахунків та електронних гаманців. Найпоширеніші випадки введення в оману жертви були через соціальні мережі, де шахраї за допомогою різних технік маніпуляції спонукали користувача для розкриття та підтвердження фінансової операції. Разом з тим і зросла інтенсивність

шахрайств в компаніях, робота яких є безпосередньою обробкою великих обсягів фінансових транзакцій.

Такі противоправні дії становлять загрозу як для компаній та підприємств, так і для споживачів, що часто призводить до фінансових збитків та небезпеку для зберігання конфіденційної інформації. Боротьба із платіжним шахрайством в 2023 році була направлена на оновлення шляхів посилення кіберзахисту, впровадження технологій штучного інтелекту на виявлення аномальних фінансових транзакцій та вдосконалення засобів шифрування даних.

Динаміку та масштаби шахрайських дій, пов'язаних із платежами у 2023 р., відображено на рис. 2.5.

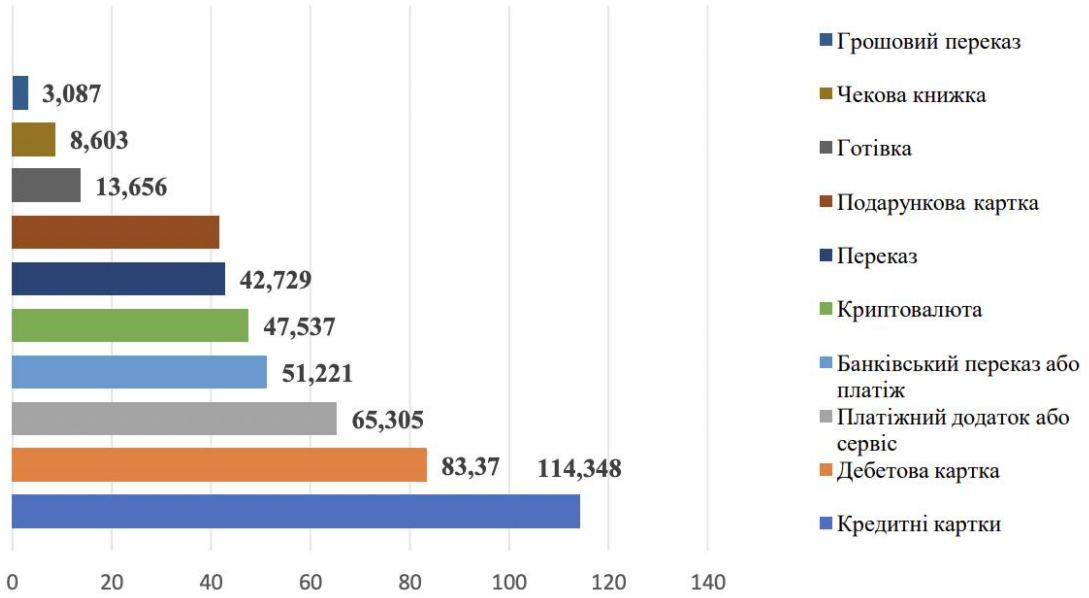

Рис.2. 5. Динаміка кількості випадків шахрайства, пов'язана з платежами у 2023 р., тис. од.

Примітка. Джерело: складено автором з використанням [39]

Основними передумовами зростання масштабів платіжного шахрайства є активне використання соціальної інженерії, поширення фішингових атак, а також експлуатація вразливостей, наявних у цифрових платіжних інфраструктурах. Додатковим чинником стала інтенсифікація онлайн-транзакцій у період пандемії COVID-19, що створило сприятливі умови для активізації шахрайських схем. У 2023 р. найбільшу кількість повідомлень було зафіксовано щодо шахрайства з

кредитними картками – близько 114 348 тис. випадків. Другу позицію займали звернення, пов'язані з шахрайськими операціями з дебетовими картками, тоді як третє місце посідали інциденти, що стосувалися платіжних застосунків.

Динаміку атак із використанням шкідливого програмного забезпечення у світі за 2015-2023 рр. відображено на рис. 2.6.

У 2023 р. світова кількість атак із застосуванням шкідливого програмного забезпечення збільшилася на 10 % порівняно з попереднім роком і досягла 6,06 млрд випадків.

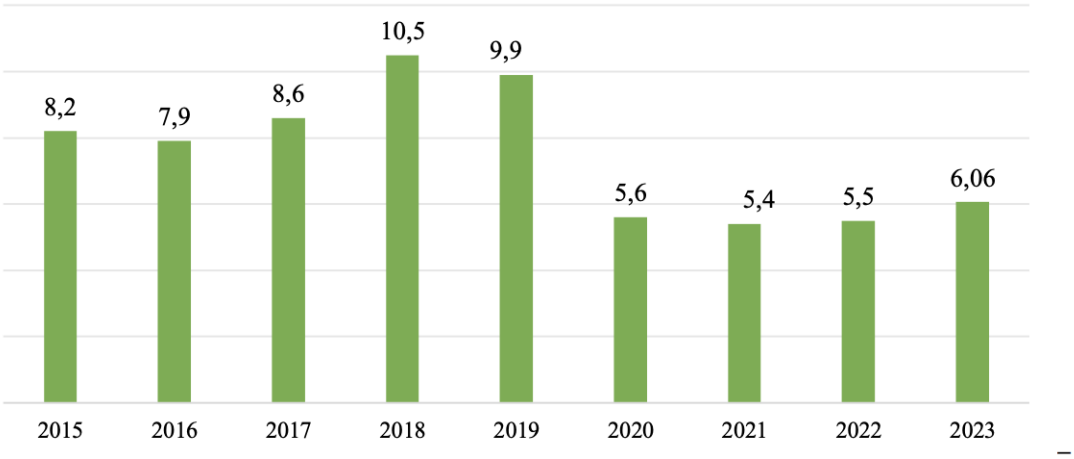

Рис. 2.6. Динаміка атак із використанням зловмисного програмного забезпечення у світі, 2015-2023 рр., тис. од.

Примітка. Джерело: складено автором з використанням [34]

Найвищий рівень такої активності було зафіксовано у 2018 р., коли загальна кількість атак у глобальному масштабі становила 10,5 млрд. У 2023 р. найбільш уразливою виявилася сфера освіти, на яку в середньому припадало 2046 атак щотижня, що є дещо нижчим показником порівняно з 2314 атаками на тиждень у попередньому році. Друге місце за рівнем ураження посіли урядові та військові структури, після яких найбільших атак зазнавали заклади охорони здоров'я. Загалом у 2022 р. освітній сектор зіткнувся з понад п'ятьма мільйонами атак із використанням зловмисного програмного забезпечення [33-35; 37].

За результатами дослідження SonicWall Capture Labs [40], у першому півріччі 2024 р. кількість атак, спрямованих на пристрої Інтернету речей (IoT) із

використанням шкідливого програмного забезпечення, зросла на 107 %. Пристрої, що ставали об’єктами таких кібератак, у середньому перебували під загрозою протягом 52,8 години. На рис. 2.7 відображено галузі світової промисловості, які в період з листопада 2022 р. до жовтня 2023 р. найчастіше зазнавали атак із застосуванням зловмисного програмного забезпечення.

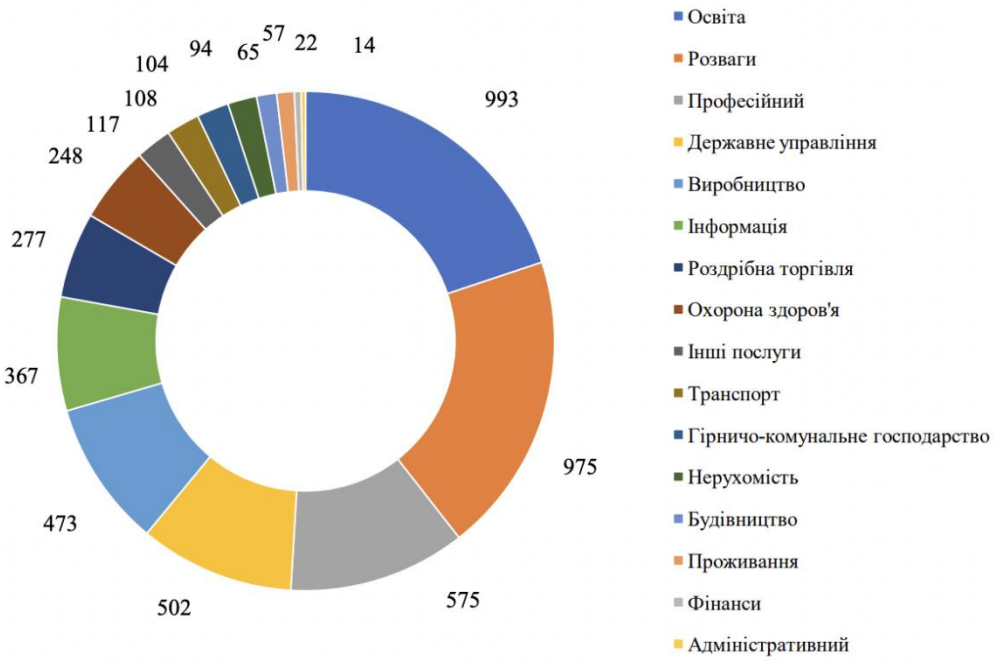

Рис. 2.7. Сектори промисловості у світі, які найбільше зазнавали атак зловмисного програмного забезпечення, листопад 2022 р.-жовтень 2023 р., тис. од.

Примітка. Джерело: складено автором з використанням [39]

У 2023 р. організації в різних країнах світу зареєстрували понад 317,59 млн спроб атак із застосуванням програм-вимагачів (рис. 2.8). Цей показник є нижчим за рівень попереднього року на 175,74 млн спроб. Зазвичай такі атаки спрямовуються проти організацій, які володіють великими масивами даних або виконують критично важливі функції. У разі успішного нападу такі установи нерідко надають перевагу виплаті викупу за відновлення доступу до викраденої чи заблокованої інформації, а не негайному публічному повідомленню про інцидент. Додатковим чинником замовчування атак програм-вимагачів є репутаційна шкода, оскільки втрата даних може негативно вплинути на довіру до компанії та її позиції на ринку.

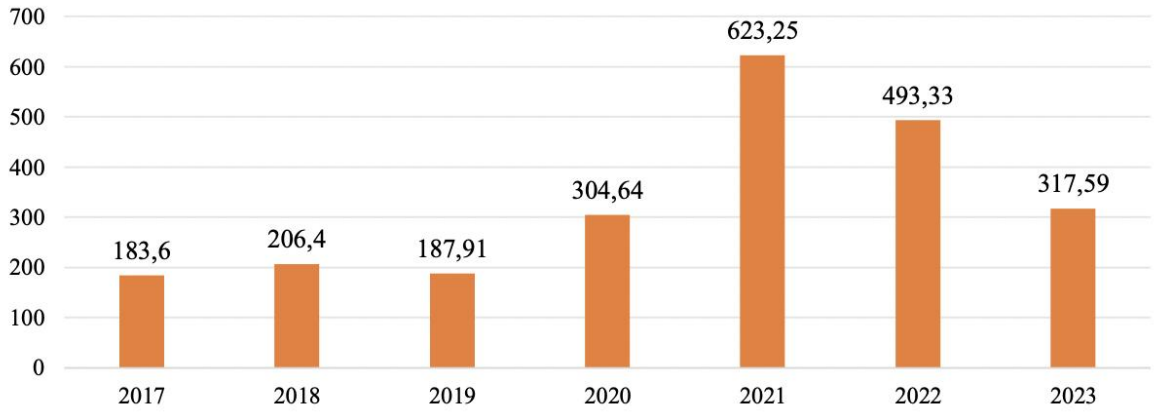

Рис. 2.8. Динаміка спроб атаки програм-вимагачів у світі, 2017–2023 рр., тис. од.

Примітка. Джерело: складено автором з використанням [41]

Станом на 2023 р. атаки із застосуванням програм-вимагачів торкнулися понад 72,7 % компаній у світі. Порівняно з результатами досліджень за попередні п’ять років цей показник демонструє помітне зростання і є найвищим серед зафіксованих значень. Загалом із 2018 р. щороку більше половини опитаних повідомляли, що їхні організації зазнавали впливу програм-вимагачів. Розподіл кібератак за основними галузями світової економіки у 2023 р. представлено на рис. 2.9.

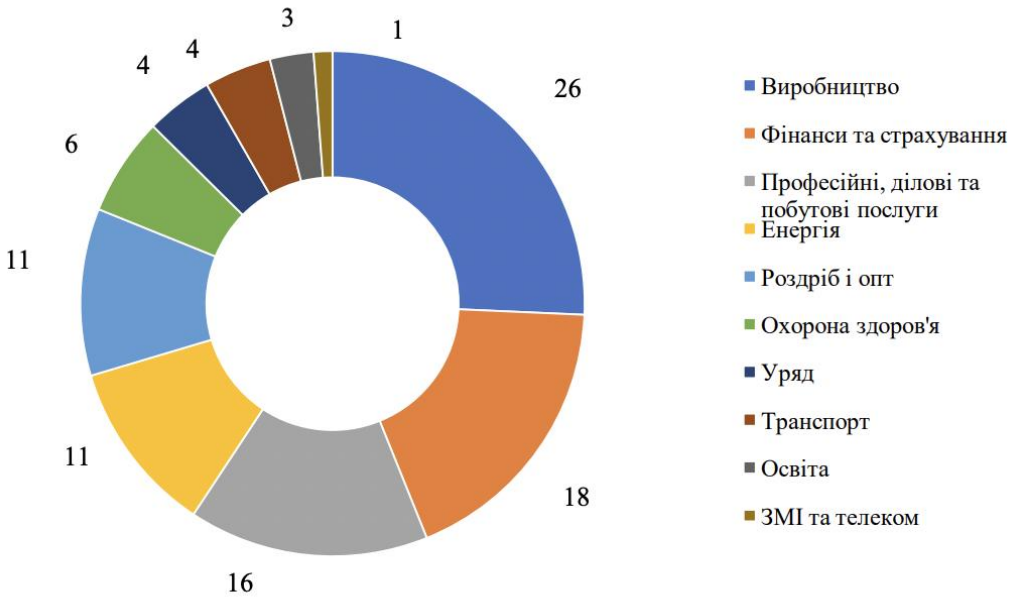

Рис. 2.9 Розподіл кібератак у світових галузях в 2023 р., %

Примітка. Джерело: складено автором з використанням [42-44]

У 2023 р. найбільша питома вага зафіксованих кібератак у розрізі світових галузей припадала на виробничий сектор. Упродовж аналізованого року підприємства цієї сфери зазнали майже чверті від загальної кількості кіберінцидентів. Другу позицію займали фінансові та страхові установи, на які припало близько 18 % атак. Третє місце посіли професійні, ділові та споживчі послуги, де було зареєстровано 15,4 % від загальної кількості кібератак.

У Канаді понад 95 % організацій перебували в зоні високого ризику кібератак. У Сінгапурі більшість опитаних представників рад директорів, а саме понад 89 %, вважали, що їхні компанії можуть зіткнутися з такими загрозами протягом наступного року. Японські підприємства посіли третю позицію за рівнем занепокоєння щодо ймовірності нових кіберзлочинів: відповідні ризики відзначили близько 84 % респондентів. Середню вартість збитків, спричинених витоком даних у світовому масштабі, подано на рис. 2.10.

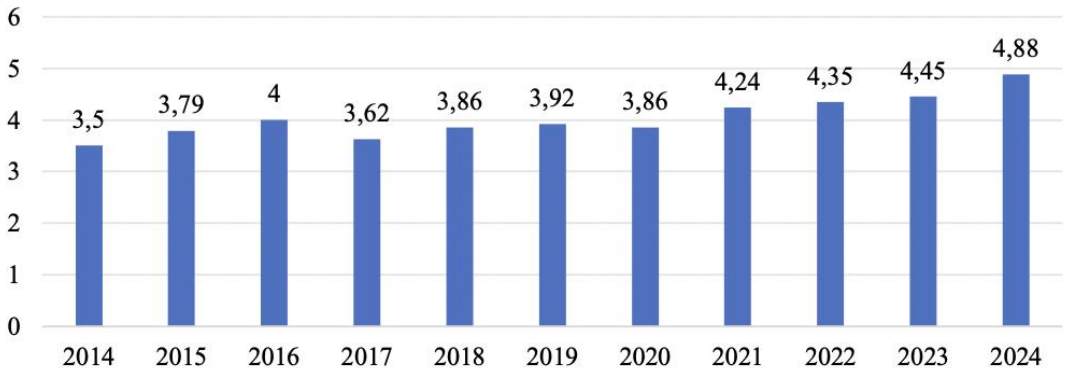

Рис. 2.10. Середня вартість збитків від витоку даних у світі, з 2018 р. по лютий 2024 рр., млрд дол. США

Примітка. Джерело: складено автором з використанням [44]

Середня вартість збитків, спричинених витоком даних, щороку демонструє тенденцію до зростання. Якщо у 2023 р. обсяг таких втрат оцінювався приблизно у 4,45 млрд дол. США, то вже станом на кінець лютого 2024 р. цей показник зріс до 4,88 млрд дол. США. Витоки інформації мають особливо тяжкі фінансові наслідки,

оскільки їхній вплив поширюється не лише на окремих користувачів, а й на організації, бізнес-структури та державні установи загалом.

У 2023 р. серед найтиповіших наслідків втрати конфіденційних даних для організацій у світовому масштабі найбільшу частку становило скорочення доходів – понад 56,6 % у загальній структурі. Другою за поширеністю проблемою було погіршення ділової репутації компаній, що становило 38,9 %, а третє місце посіло послаблення конкурентних позицій із часткою 35,8 %. Станом на жовтень 2023 р. Сполучені Штати Америки займали провідне місце за кількістю джерел фінансування кібератак (рис. 2.11), забезпечуючи понад 33,7 % від їх загального світового обсягу. Така ситуація значною мірою пояснюється концентрацією великої кількості серверної інфраструктури для інтернет-користувачів саме на території США. Другу позицію посідала росія з часткою 7,94 %, тоді як третє місце фактично розподіляли між собою Франція та Нідерланди, показники яких становили відповідно 7,26 % і 7,15 %.

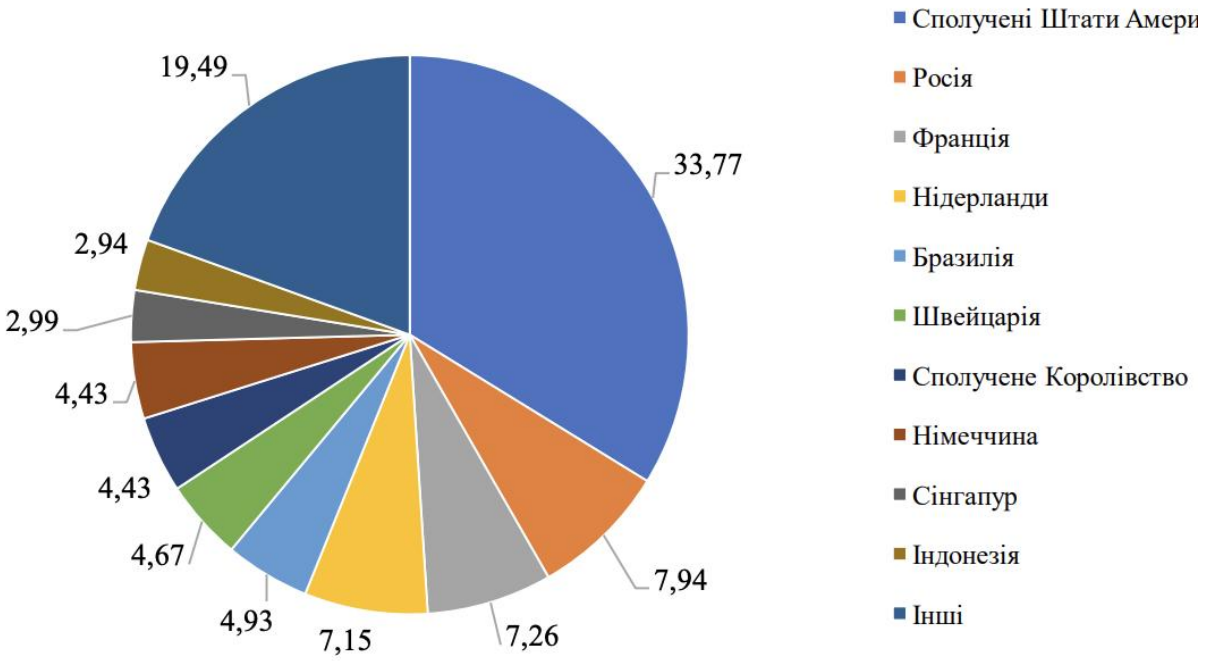

Рис. 2.11. Розподіл джерел кібератак у світі з листопада 2022 р. по жовтень 2023р. за країнами

Примітка. Джерело: складено автором з використанням [44]

Можна зробити висновок після проведеного аналізу тенденцій кіберзлочинів у світі, що рівень атак кожного року тільки зростає, механізми своєчасно виявити та попередити кіберзлочині менш єфективні, ніж системи вдосконалення цифрових загроз у шахраїв. Фішинг - це домінуюча ланка кіберзлочинців, яка характеризується зростаючою дінамікою для подальшого поширення. Тільки у 2023 році обсяг загроз використання небезпечного програмного забезпечення для атак на користувачів досягнула понад 6 млрд, що може свідчити про масштабну та глобальну проблему у цій сфері. Світові економічні збитки, які наносяться шахраями перевищили у 2023 році 7 трлн дол. США, а згідно прогнозу вже в 2029 році може сягнути до 15 трлн дол. США.

Для організацій найбільш типовими наслідками втрати конфіденційної інформації є зменшення доходів, частка якого становить 56,6 %, погіршення ділової репутації – 38,9 %, а також послаблення конкурентних позицій - 35,8 %. Найвищу вразливість до кіберзагроз зберігають освітній сектор, державні установи, сфера розваг і фінансові організації, оскільки саме в цих напрямах фіксується значна кількість інцидентів, пов’язаних із використанням шкідливого програмного забезпечення.

Країни, з яких визначено найбільшу загрозу атак очолює США, далі йде Росія, потім Нідерланди і Франція. Боротьба з противоправними діями шахраїв має бути не окремо в кожній державі, а згуртованною світовою спільнотою для найвищої результативності знешкодження кіберзагроз. Саме обмежений обмін інформацією щодо вчинення атак між державами і недостаній аналіз ситуацій, підвищують ймовірність повторних та значно вдосконалених в майбутньому кіберризиків, яким буде важче протистояти. Хакерські атаки варто стримувати тісною координацією між компаніями, організаціями і всіма органами держави, оперативним сповіщенням щодо актуальної загрози.

2.2. Оцінка впливу кіберінцидентів та воєнних дій на функціонування суб’єктів міжнародної економічної діяльності в Україні

За даними аналітичного звіту Державної служби спеціального зв'язку та захисту інформації України, підготовленого у співавторстві з ICE Task Force під назвою «War and Cyber: Three Years of Struggle and Lessons for Global Security», у 2024 році в Україні було зареєстровано 4 315 кіберінцидентів. Такий показник перевищує рівень 2023 року, коли було зафіксовано 2 543 випадки, на 69,7 %, а порівняно з довоєнним 2021 роком, у якому налічувалося 1 350 інцидентів, є більшим у 3,2 раза [45].

В 2024 році кількість кібератак в більшості прийшлася на публічний сектор - 58%. На оборонний сектор припало більше 18% атак. Також, під загрозами опинилися і енергетична, комерційна та телекомунікаційна сфери, в загальному обсяг таких злочинів становили 6%, 3% і 2%.

Структуру зареєстрованих кіберінцидентів за цільовими секторами упродовж 2021–2024 років відображено на рис. 2.12.

MOST TARGETED SECTORS, 2021-2024							
2021		2022		2023		2024	
1350		2194		2543		4315	
Public Sector and Local Governments	20%	Public Sector and Local Governments	26%	Public Sector and Local Governments	25%	Public Sector and Local Governments	58%
Security and Defense Sector	16%	Security and Defense Sector	14%	Security and Defense Sector	7%	Security and Defense Sector	18%
Commercial sector	6%	Commercial sector	6%	Commercial sector	5%	Energy sector	6%
Financial sector	6%	Financial sector	5%	Energy sector	4%	Commercial sector	3%
Energy sector	3%	Energy sector	5%	Telecom sector	4%	Telecom sector	2%

Рис 2.12. Структура зареєстрованих кіберінцидентів за цільовими секторами в Україні за період 2021-2024 роки

Примітка. Джерело: складено автором з використанням [45]

На основі аналізу динаміки кіберзагроз з 2021 по 2024 рік найвразливішими та найпривабливішими для шахраїв є сфери публічного сектору і органи місцевого самоуправління. Галузь оборони займає друге місце, що може свідчити про те що дії держави-агресора орієнтовані на підрив системи державного врядування та

суттєвого ослаблення оборонного потенціалу країни. З урахуванням таких подій дуже важливе подальше дослідження кіберстійкості, так як це ключовий момент у безперервному функціонуванні держави за умов воєнного стану. Кіберстійкість у цьому контексті доцільно трактувати як інтегровану спроможність держави протидіяти кібератакам, пристосовуватися до їхніх наслідків і зберігати стабільність критично важливих процесів. Її зміцнення передбачає системне оцінювання національних можливостей, зокрема шляхом визначення рівня технологічної озброєності, яка формує основу для результативного реагування, адаптації та відновлення після кіберінцидентів. Крім того, технологічна конкурентоспроможність виступає важливою умовою посилення позицій країни у глобальній економічній системі [46].

National Cyber Security Index (NCSI) являє собою міжнародний індекс, за допомогою якого оцінюється готовність держав запобігати кіберзагрозам і реагувати на кіберінциденти. Його значення не обмежується лише вимірюванням поточного стану кібербезпеки, адже він також формує відкриту інформаційну основу, яку країни можуть використовувати для розширення власних можливостей у сфері кіберзахисту [47].

Індекс NCSI забезпечує кількісне відображення здатності держав попереджати цифрові загрози та реагувати на інциденти в кіберпросторі. Ключовим показником у його структурі є NCSI Score, який демонструє рівень кіберстійкості країни у відсотковому співвідношенні до максимально можливої сукупності індикаторів, де найвища оцінка становить 100 %. Окрім цього, до уваги береться рівень цифрового розвитку держави — Digital Development Level (DDL). Важливе аналітичне значення має співвідношення між показниками кіберзахищеності та цифрового розвитку: якщо різниця між ними є позитивною, це свідчить про те, що система кібербезпеки відповідає темпам цифрової трансформації або навіть випереджає їх. Відповідно до даних National Cybersecurity Index (NCSI), станом на 29.11.2023 Україна займала 15 місце серед 58 оцінених країн із загальним показником 80,84. Разом із тим результати за окремими компонентами індексу засвідчують нерівномірність розвитку ключових напрямів національної кібербезпеки [48].

Протягом 2020-2024 років Україна досягла прогресу в таких ключових компонентах кібербезпеки, як:

- ✓ Зростання та розширення набору технічних методів, які протидіють кіберзагрозам
- ✓ Розвиток потенціалу міжнародної співпраці та підготовка фахівців сфери кібербезпеки.
- ✓ Оптимізація правового сегменту направлена на вдосконалення законодавчого впорядкування у галізу кібербезпеки.

З моменту повномасштабного вторгнення Росії в 2022 році Україна кожного дня стикається із інтенсивними кіберзагрозами, які спрямовані проти оргранів державного управління, сфери СМІ, енергетичної інфраструктури та важливих напрямів соціального забезпечення. Інфомаційна війнашляхом поширення дезінформації також ведеться паралельно із атаками на кіберпростір та постійними обстрілами, для активного поширення фейкової інформації використовуються кіберінструменти для ураження всіх можливиз систем операційного напряму. У 2024 році Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка функціонує при Держспецзв'язку, опрацювала 4315 кіберінцидентів [49].

Схеми шахрайств реалізовані через відомі месенджери, такі як Viber та Telegram широко застосовуються зловмисниками під прикриттям волонтерської діяльності, зборів фінансової підтримки ЗСУ та допомоги жертвам обстрілів. Також, поширення набуло і використання підробних мабільних додатків військового направлення, наприклад, програми сповіщення повітряних тривог, за допомогою яких ворог встановлював шпигунські програми та інструменти збору персональної інформації та даних.

В умовах війни особливу цінність для противника становлять дані про плани сил оборони України, інформація підприємств оборонно-промислового комплексу, державних органів та організацій, що забезпечують підтримку військових. Для досягнення таких цілей кіберзловмисники найчастіше використовують масове розповсюдження шкідливого програмного забезпечення і фішингових повідомлень, тому саме ці типи атак, імовірно, залишатимуться найбільш поширеними. Усе це

зумовлює потребу в реалізації системного комплексу заходів, спрямованих на зміцнення кібербезпеки. Водночас в Україні вже можна спостерігати певні позитивні зміни у цьому напрямі.

Зокрема, у 2009 році було створено Департамент кіберполіції Національної поліції України, який функціонує як міжрегіональний територіальний орган Національної поліції та відповідно до законодавства забезпечує реалізацію державної політики у сфері протидії кіберзлочинності. Його діяльність охоплює організацію й проведення оперативно-розшукових заходів, а також спеціалізується на запобіганні, виявленні, припиненні та розкритті кримінальних правопорушень, підготовка, вчинення або приховування яких пов'язані з використанням електронно-обчислювальних машин, телекомунікаційних, комп'ютерних, інтернет-мереж і систем. У 2016 році при РНБО було утворено Національний координаційний центр кібербезпеки. Серед його основних завдань — аналіз стану кібербезпеки, оцінювання результатів огляду національної системи кібербезпеки, визначення готовності суб'єктів забезпечення кібербезпеки до виконання завдань із протидії цифровим загрозам, контроль за дотриманням законодавчих вимог щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, захист якої передбачений законом, а також об'єктів критичної інформаційної інфраструктури. Крім того, Центр здійснює аналіз відомостей про кіберінциденти, що стосуються державних інформаційних ресурсів в інформаційно-телекомунікаційних системах [50].

Найуразливіший зараз є малий та середній бізнес. Сучасні кібератаки дедалі частіше будуються на використанні складних тактик, які дають змогу обходити традиційні механізми виявлення шкідливого програмного забезпечення та діяти всередині комплексних цифрових середовищ цільових організацій. Такі атаки можуть бути спрямовані на викрадення інформації, встановлення програм-вимагачів, шифрування даних або створення масштабних перебоїв у роботі підприємств. Проведене дослідження показало, що серед галузей, представники яких розглядають можливість сплати викупу, переважають будівельний сектор — 74 %, технологічна сфера — 51 % та енергетика — 43 % [51].

2.3. Аналіз стану економічної безпеки та інструментів кіберзахисту суб'єктів міжнародного бізнесу на території України

Економічний захист комерційної діяльності має комплекс факторів:

- ✓ Стійка світова економічна система.
- ✓ Стабільність валютних ринків та руху інвестицій.
- ✓ Баланс міжнародної торгівлі та надійсніть логістичних шляхів.
- ✓ Відсутність фінансових, продовольчих криз та збоїв енергетичних сфер.
- ✓ Взаємодія провідних центрів світової економіки.

Окремий блок впливів формують глобальні виклики, до яких належать кліматичні зміни, пандемічні загрози, міграційні процеси та збройні конфлікти. Забезпечення економічної безпеки на світовому рівні значною мірою здійснюється через функціонування міжнародних організацій, зокрема ООН, МВФ, Світового банку, СОТ, а також регіональних політичних і економічних інтеграційних об'єднань. Водночас між усіма рівнями економічної безпеки існує тісна взаємозалежність: стійкість окремого суб'єкта господарювання позначається на безпеці галузі, стабільність галузевого середовища впливає на економічну стійкість держави, а національна економіка є складовою частиною глобальної господарської системи. Саме тому дослідження мікрорівня, тобто економічної безпеки підприємства, має важливе значення для побудови ефективної, збалансованої та стійкої економічної системи на вищих рівнях.

Для підприємств, що здійснюють діяльність із орієнтацією на міжнародні ринки, особливої значущості набувають зони перетину зазначених рівнів економічної безпеки. До таких зон можна віднести зовнішньополітичні рішення держав, дію міжнародних санкційних режимів, регуляторні обмеження, зміну структури глобального попиту, а також трансформацію логістичних маршрутів і транспортних коридорів. З огляду на це міжнародну економічну безпеку підприємства доцільно розглядати як сукупність взаємопов'язаних підсистем або компонентів, що утворюють цілісну структуру та відображені на рис. 2.13.

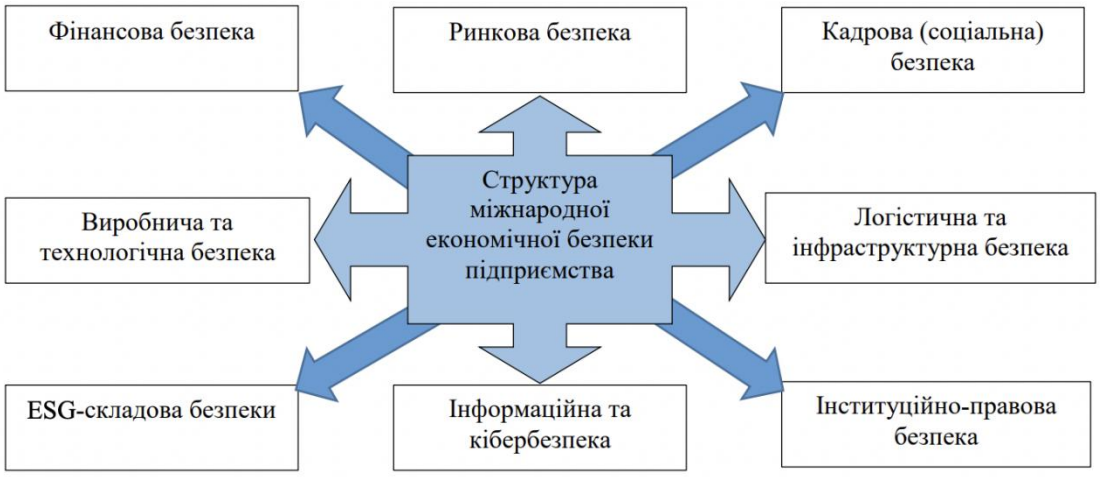

Рис. 2.13. Структура міжнародної економічної безпеки підприємства

Примітка.Джерело: складено автором на основі [50-51]

Отже, міжнародну економічну безпеку підприємства варто трактувати як узагальнену характеристику його здатності зберігати стабільність функціонування, конкурентні позиції та безперервність розвитку в умовах глобалізаційних процесів, загострення міжнародної конкуренції, валютних коливань, геоекономічної нестабільності й транснаціональних викликів. Вона відображає рівень захищеності основних ресурсів, управлінського потенціалу та стратегічних можливостей компанії в межах міжнародного бізнес-середовища.

Зміст міжнародної економічної безпеки підприємства розкривається через взаємоузгоджене поєднання низки функціональних компонентів, серед яких фінансова, виробничо-технологічна, інноваційна, зовнішньоекономічна, інвестиційна, кадрова, інформаційна, логістична та правова безпека. У своїй сукупності ці елементи формують цілісний механізм, орієнтований на запобігання, послаблення та нейтралізацію загроз як зовнішнього, так і внутрішнього походження. Її структура має системно-ієрархічну природу, оскільки включає підсистеми відстеження ризиків, інструменти превентивного реагування, механізми стратегічного управління та адаптаційні можливості підприємства щодо змін кон’юнктури світових ринків, оновлення регуляторних вимог і трансформації глобальних ланцюгів постачання.

Перехід підприємства до міжнародного формату діяльності істотно збільшує кількість потенційних ризиків, оскільки його функціонування починає залежати від складного багаторівневого середовища, у якому одночасно діють політичні, правові, соціокультурні, валютно-фінансові, логістичні та екологічні чинники. З урахуванням цього доцільно виділити основні групи ризиків, що визначають рівень міжнародної економічної безпеки підприємств.

Геополітичні та воєнно-політичні ризики є одними з найнебезпечніших у системі міжнародної економічної безпеки підприємств, оскільки їм властиві високий ступінь непередбачуваності, широкий масштаб впливу та здатність породжувати ланцюгові наслідки у світових виробничих, логістичних і фінансових системах.

Підприємства, що працюють на зовнішніх ринках та мають об'єднанні шляхи постачання із міжнародними партнерами найбільш схильні до втрати конкурентоспроможності, порушення інформаційної стійкості, збільшення витрат, що несе за собою зменшення прибутків (табл. 2.1).

Таблиця 2.1

Геополітичні та воєнно-політичні ризики у системі міжнародної економічної безпеки підприємств

Категорія ризиків	**Характеристика ризику**	**Ймовірні наслідки для підприємств**	**Приклади прояву**
1	2	3	4
Геополітичні ризики	Міжнародні конфлікти, економічні санкції, торговельні суперечки між державами, зміни політичної влади	Втрата доступу до зовнішніх ринків, ускладнення експортно-імпортних операцій, припинення співпраці з партнерами	Введення санкцій щодо держав або окремих секторів економіки, скасування міжнародних угод
	Політична нестабільність у державах-партнерах	Порушення логістичних процесів, збільшення транспортних витрат, ризик фінансових втрат через неплатежі	Девальвація національної валюти, обмеження роботи портів і пунктів пропуску
	Посилення державного контролю над міжнародною торгівлею та рухом капіталу	Ускладнення інвестиційної діяльності, обмеження доступу до фінансових ресурсів і технологій	Заборона експорту технологічної продукції, обмеження міжнародних банківських операцій

Продовження табл. 2.1

1	2	3	4
Воєнно-політичні ризики	Воєнні конфлікти, агресія та бойові дії	Пошкодження виробничих потужностей, зупинка діяльності підприємства, евакуація персоналу	Руйнування інфраструктурних об’єктів, мобілізація працівників
	Блокування транспортних маршрутів і логістичних каналів	Затримки постачання, підвищення собівартості перевезень, дефіцит ресурсів	Закриття морських портів, повітряного простору або ключових транспортних шляхів
	Підвищення рівня небезпеки для персоналу та матеріальних ресурсів	Необхідність додаткових витрат на безпеку, страхування та релокацію бізнесу	Зростання страхових платежів, переміщення виробничих потужностей у безпечні регіони
	Кібератаки та інформаційний вплив у період воєнних дій	Втрата або витік даних, порушення роботи цифрових систем підприємства	Атаки на банківські системи, логістичні платформи та корпоративні мережі
	Нестабільність валютного ринку в умовах кризових ситуацій	Фінансові збитки, збільшення витрат на імпорт продукції та сировини	Різкі коливання валютних курсів під час воєнних або політичних криз

Примітка.Джерело: складено автором на основі [51]

Ризики пов’язані із політичною та військовою сферами несуть в собі широкий спект проблем, через безпосередній вплив збройного зіткненн, в першу чергу під удором опиняються виробнича, логістична на транспортна ланки підприємства. Ріст страхових гарантій, часткова або повна зупинка виробничої діяльності, мобілізаційні міри, нестача робочої сили, збільшення кібератак, дестабілізація фінансової сфери в сукупності унеможливлюють функціонування будь-якого виробництва, підприємство напряму залежить тільки від зовніхніх ринків, поставок та дій міжнародних партнерів. В такій ситуації, тільки системне впорядкування ризиків дає можливість не лише підвищити об’єктивність їх оцінювання, а й сформувати дієву модель реагування, що поєднує превентивні, адаптаційні та компенсаційні інструменти.

Висновки до розділу 2

Можна зробити висновок після проведеного комплексного аналізу тенденцій кіберзлочинів у світі, що рівень атак кожного року тільки зростає, механізми своєчасно виявити та попередити кіберзлочині менш єфективні, ніж системи вдосконалення цифрових загроз у шахраїв.

Світова економіка несе глобальні витрати від хакерських атак, викраденні або розкриття персональної інформації про клієнтів та даних працівників, що підриває репутацію компанії, знижує рівень довіри, і відповідно має наслідки в стабільних прибутках.

Фішинг - це домінуюча ланка кіберзлочинців, яка характеризується зростаючою дінамікою для подальшого поширення. Найвищу вразливість до кіберзагроз зберігають освітній сектор, державні установи, сфера розваг і фінансові організації, оскільки саме в цих напрямах фіксується значна кількість інцидентів, пов’язаних із використанням шкідливого програмного забезпечення.

Найуразливіший зараз також є малий та середній бізнес. Сучасні кібератаки дедалі частіше будуються на використанні складних тактик, які дають змогу обходити традиційні механізми виявлення шкідливого програмного забезпечення та діяти всередині комплексних цифрових середовищ цільових організацій. Такі атаки можуть бути спрямовані на викрадення інформації, встановлення програм-вимагачів, шифрування даних або створення масштабних перебоїв у роботі підприємств.

Ризики пов’язані із політичною та військовою сферами несуть в собі широкий спект проблем, через безпосередній вплив збройного зіткненн, в першу чергу під ударом опиняються виробнича, логістична на транспортна ланки підприємства.

Ріст страхових гарантій, часткова або повна зупинка виробничої діяльності, мобілізаційні міри, нестача робочої сили, збільшення кібератак, дестабілізація фінансової сфери в сукупності унеможливлюють функціонування будь-якого виробництва, підприємство напряму залежить тільки від зовнішніх ринків, поставок та дій міжнародних партнерів.

Геополітичні та воєнно-політичні ризики є одними з найнебезпечніших у системі міжнародної економічної безпеки підприємств, оскільки їм властиві високий ступінь непередбачуваності, широкий масштаб впливу та здатність породжувати ланцюгові наслідки у світових виробничих, логістичних і фінансових системах.

Кіберзлочини мають масштабну площину атак і становлять загрозу будь-якому користувачу у будь-якій країні проживання та перебування. З урахуванням цієї проблеми дуже актуальним стає набуття цифрової грамотності для захисту користувачів, нові шляхи захисту та удосконалення інструментів безпеки та розробки правил, які спрямовані на запобігання всіх видів атак.

РОЗДІЛ 3

СТРАТЕГІЧНІ НАПРЯМИ ЗМІЦНЕННЯ ЕКОНОМІЧНОЇ ТА КІБЕРБЕЗПЕКИ МІЖНАРОДНОГО БІЗНЕСУ В УМОВАХ КІБЕРЗАГРОЗ ТА ГЕОПОЛІТИЧНОЇ НЕСТАБІЛЬНОСТІ

3.1. Міжнародний досвід компаній щодо підвищення рівня управління економічною безпекою та його прийнятність для українських реалій

Порівняння наукових і практичних підходів до розуміння категорії «економічна безпека» в Україні та окремих країнах Європейського Союзу дає підстави визначати її переважно як елемент системи національної безпеки, спрямований на запобігання, послаблення й нейтралізацію загроз внутрішнього та зовнішнього походження. Її кінцева функція полягає у створенні умов для належного рівня життя населення через скоординовану взаємодію державних інституцій і суб'єктів приватного сектору. У цьому зв'язку важливим є аналіз моделей та механізмів забезпечення національної економічної безпеки, які сформувалися в різних державах світу. Серед них можна виокремити японську модель, що значною мірою зорієнтована на підтримання внутрішньої соціальної стабільності; американську, яка охоплює як внутрішній, так і зовнішній виміри безпеки та нерідко використовується іншими країнами як орієнтир; китайську, що відображає особливості безпекових підходів держав із соціалістичною моделлю суспільного розвитку; а також моделі країн, які порівняно недавно здобули незалежність або перебувають на етапі інтенсивної переорієнтації власного політико-економічного курсу. У межах Європейського Союзу економічна безпека розглядається у тісному зв'язку з позицією ЄС у глобальній економічній системі. Саме тому для зміцнення конкурентних переваг в умовах глобалізації європейська інтеграція визначається як один із провідних інструментів досягнення стратегічних цілей Союзу.

Стратегічний орієнтир Європейського Союзу полягає у зміцненні економічної безпеки об'єднання та поступовому створенні повністю інтегрованого

європейського простору, у межах якого рівень життя в державах-учасницях має поступово наближатися. При формуванні системи економічної безпеки необхідно враховувати національні особливості окремих країн, оскільки держави використовують різні правові інструменти, міжнародні угоди та законодавчі механізми для регулювання цієї сфери. Кожна країна вибудовує власну модель управління економічною безпекою відповідно до політичних, економічних та інституційних умов свого розвитку. У частині держав відсутня спеціалізована законодавча база, безпосередньо присвячена забезпеченню економічної безпеки; до них належать, зокрема, Німеччина, Франція, Італія, Велика Британія, Чехія, Болгарія, Угорщина, Польща, Латвія, Словаччина, Литва та Естонія. Водночас в інших країнах, серед яких Іспанія, Румунія та Білорусь, правове забезпечення економічної безпеки займає особливо важливе місце в системі державного управління. Слід підкреслити, що національні контрольні механізми у цій сфері здебільшого орієнтовані на зменшення вразливості економіки перед зовнішніми негативними впливами, формування належного нормативно-правового підґрунтя, створення сприятливих умов для розвитку конкуренції, забезпечення результативного валютного контролю, підтримання стабільності національної грошової одиниці, розвиток підприємницького середовища та захист вітчизняного виробника. Провідні країни світу застосовують комплекс практичних заходів для зниження ризиків у ключових сферах суспільного розвитку, а їхня результативність значною мірою залежить від чіткого визначення стратегічних пріоритетів державної політики. Для ефективного використання міжнародного досвіду державного управління у сфері національної економічної безпеки в Україні необхідно враховувати напрацювання провідних держав, визначати основні загрози та формувати реалістичні напрями їх подолання.

Як зазначає Роберт А. Невсон (Newson, Robert A. (2022)), серед основних загроз економічній безпеці держав у міжнародному вимірі можна виокремити ізоляцію у світовому економічному просторі, яка здатна призвести до дискримінаційних умов у торгівлі та втрати суверенітету в окремих напрямах економічної політики; недостатню конкурентоспроможність національної

економіки, спричинену високим рівнем зношеності основних фондів і зниженням інноваційної активності; дефіцит зовнішньоторговельного балансу та неефективну структуру імпорту, що посилює залежність від зовнішніх постачань; відсутність дієвих механізмів залучення іноземного капіталу, яка може сприяти зростанню зовнішньої заборгованості; слабку ефективність експортного й валютного контролю, що створює передумови для відтоку капіталу; а також недостатній розвиток інфраструктури, необхідної для забезпечення зовнішньоекономічної діяльності [52].

Відтак міжнародну економічну інтеграцію доцільно інтерпретувати як поступовий процес зближення національних господарських систем і економіко-правових механізмів різних держав, що супроводжується поглибленням економічних зв'язків, узгодженням міждержавної політики та структурною перебудовою економік на підставі міжнародно-правових домовленостей. Як правило, інтеграція передбачає утворення нового відносно самостійного міждержавного об'єднання, учасники якого набувають певних економічних і міжнародно-правових переваг. Найчастіше інтеграційні процеси розгортаються у регіональному форматі, поступово переходячи від суто економічної взаємодії до політичного зближення. Зокрема, у європейсько-правовій доктрині виокремлюють три ключові підстави на користь інтеграції: вона знижує ймовірність воєнних зіткнень; усунення національних бар'єрів у торгівлі сприяє економічному зростанню; а за умов вільної торгівлі саме політичне об'єднання може виступати гарантією збереження демократичного устрою [53].

За змістовим критерієм інтеграційні процеси можуть набувати різних функціональних форм, серед яких виокремлюють загальні союзи, прикладом яких є Benelux Union, а також спеціалізовані функціональні або галузеві об'єднання, зокрема European Atomic Energy Community, EAEC (Euratom). Залежно від характеру взаємодії із зовнішнім середовищем інтеграційні утворення можуть бути закритими, тобто автаркічними, напівзакритими, відкритими лише для держав певного регіону, або відкритими для ширшої міжнародної співпраці. За критерієм кількісного охоплення учасників розрізняють союзи з обмеженим складом сторін, наприклад Союзну державу росії та білорусії, і масштабніші об'єднання, до яких

належить EU. Інтеграційні структури також можуть класифікуватися за рівнем економічного розвитку держав-учасниць: до першої групи належать союзи розвинених країн, зокрема EU і NAFTA; до другої - об'єднання держав, що розвиваються, наприклад ASEAN; до третьої - союзи країн із перехідною економікою, серед яких СНД [54].

Подібна класифікація сприяє глибшому розумінню розстановки соціально-політичних сил у міжнародному середовищі та дає змогу прогнозувати міжнародно-правову позицію окремих груп держав щодо актуальних проблем сучасних міжнародних економічних відносин. Водночас така типологія є певною мірою умовною, оскільки подальший технологічний прогрес може вивести на провідні позиції ті країни, які нині не належать до центру глобальної економічної уваги. Попри це, у найбільш узагальненому вигляді можна окреслити основні напрями розвитку економічної безпеки в інтеграційному контексті. До них належить формування зони вільної торгівлі, у межах якої усуваються внутрішні регіональні обмеження для переміщення товарів і послуг; створення митного союзу, що передбачає застосування узгоджених зовнішніх тарифів для захисту економічних інтересів держав-учасниць; становлення єдиного ринку, де ліквідовуються внутрішні бар'єри для використання факторів виробництва; утворення валютного союзу, який ґрунтується на узгодженні грошової, податкової та валютної політики; а також формування економічного союзу, у межах якого діють наднаціональні органи економічної координації, єдина грошова система, спільний центральний банк, уніфіковане податкове регулювання та погоджена економічна стратегія.

Формування системи міжнародної економічної безпеки супроводжується появою низки важливих економічних процесів. Серед них особливе значення мають зростання відкритості міждержавних кордонів для руху фінансових потоків, інтенсифікація переміщення товарів, послуг, технологій і робочої сили, а також поширення режимів найбільшого сприяння й національного режиму у відповідних сферах співпраці. У країнах із ринковою економікою поступово відбувається зближення рівнів цін на товари, показників прибутковості підприємств і оплати праці, а також збільшується кількість і масштаб корпоративних злиттів як у межах

окремих держав, так і на міжнародному рівні. Паралельно простежується часткова універсалізація ринкових відносин, що виявляється в утвердженні спільних економічних принципів, звичаїв і правових норм у системі забезпечення міжнародної економічної безпеки. У результаті посилюється взаємозалежність і взаємопов'язаність національних ринків. Разом із тим глобалізаційні процеси мають і суперечливі наслідки. Насамперед орієнтація капіталістичної системи на максимізацію прибутку зумовлює нерівномірність розвитку між економічно розвиненими державами та країнами, що розвиваються, сприяє концентрації економічної сили в руках обмеженого кола суб'єктів, посиленню експлуатації найманої праці капіталом, поглибленню соціальної диференціації, зростанню добробуту заможних груп і збідненню вразливих верств населення, що в підсумку може створювати передумови для виникнення глобальних економічних криз.

Поглиблення глобалізаційних процесів породжує додаткові ризики для державного суверенітету та економічної самостійності країн, оскільки звужує можливості самостійного маневрування в межах економічної політики, підвищує мобільність капіталу, посилює вплив транснаціональних корпорацій і прискорює поширення цифрових комунікацій, зокрема Інтернету. І. Бузан акцентує увагу на суперечливих наслідках таких трансформацій, серед яких тиск транснаціональних корпорацій на національні економіки, недостатнє врахування соціального виміру розвитку, обмеження сфери дії національного права, послаблення законодавчих інститутів і звуження реального змісту державного суверенітету [53].

До найбільш актуальних глобальних економічних викликів сучасного періоду належать технологічні зрушення, що змінюють саму структуру економіки; перехід до інноваційно орієнтованої моделі розвитку; збереження технологічного відставання окремих країн; гіперконкуренція, яка поєднує елементи економічного протистояння та маніпулятивних впливів; а також геоекономічні конфлікти, пов'язані з боротьбою за доступ до стратегічних ресурсів [56].

Однією з визначальних проблем сучасного етапу є те, що наявні глобальні, регіональні й національні механізми забезпечення міжнародної економічної безпеки не повною мірою відповідають реальним суспільним потребам. Значною мірою це

зумовлено відставанням правового регулювання від темпів розвитку економічних відносин. За таких умов виникає потреба у формуванні нових підходів і положень, спрямованих на приведення чинних систем у відповідність до сучасних умов розвитку, насамперед через удосконалення правового захисту глобальних економічних інтересів і підвищення його практичної результативності. Відповідно, актуальним стає створення належних правових передумов для забезпечення економічної безпеки на міжнародному рівні, що передбачає розроблення концептуального й методологічного підґрунтя для своєчасного та ефективного реагування на нові загрози.

Провідні держави світу використовують превентивну модель економічної безпеки на підприємствах, суть полягає у ранньому виявлені ризиків та прогнозування потенційних ситуацій і можливих атак. Такі інструменти застосовуються в транснаціональних корпораціях США, Німеччини, Японії, Великої Британії, Південної Кореї.

Компанії в США створюють інтергровані системи risk management. Корпорації Microsoft, IBM, Amazon та Tesla безперервно відстежують фінансові, технологічні, інформаційні та ринкові ризики. Головна роль відведена кібербезпеці, так як інформаційний ресурс в наш час відноситься до найцінніших активів підприємств. Активне застосування штучного інтелекту, аналітики та автоматизації виявлення підозрілої активності та потенційних атак. Корпоративна безпека передбачає постійний контроль і персональну відповідальність робітників щодо можливого росповсюдження комерційної таємниці.

Підприємства Євросоюзу, такі як німецькі промислові корпорації Siemens, Bosch і Volkswagen, активно впровадили механізми економічної безпеки до загальної системи стратегічного менеджменту. Ключовими ланками є внутрішній аудит, комплаєнс-контроль, управління ланцюгами постачання та забезпечення захисту виробничої інфраструктури.

Європейські компанії надають великого значення цифровій безпеці. Цифрові платформи та використання хмарних технологій дають сприятливе підґрунття для залучення інвестицій у стовренні багаторівневих систем кіберзахисту. Сучасні

методи шифрування, багатофакторна автентифікація та інші методи контролю дають змогу суттєво знизити ризики зовнішнього проникнення у корпоративні системи даних. Також, європейські компанії широко впровадили ESG-підходи, у межах яких безпека бізнесу розглядається крізь призму екологічних, соціальних і управлінських чинників.

Японська модель економічної безпеки має найвищий рівень дисципліни та корпоративної відповідальності з орієнтацією на довгострокове планування. Японські компанії розробили підхід з урахуванням якого система безпеки об'єднує всі процеси підприємства. Їх кадрова політика направлена на професійний розвиток працівників і колективну відповідальність. В корпораціях Toyota, Sony та Mitsubishi запроваджена копцепція безперервної адаптації системи безпеки до зовнішніх змін.

У міжнародній практиці широко застосовуються stress-testing, SWOT-аналіз, сценарне моделювання та системи прогнозування ризиків, що дозволяє підприємствам завчасно підготуватися до можливих кризових ситуацій і знизити їхній негативний вплив на фінансовий стан компанії (табл. 3.1).

Таблиця 3.1

Міжнародний досвід компаній щодо підвищення рівня управління економічною безпекою міжнародного бізнесу та його корисність для України

Назва країни	**Набутий досвід в сфері економічної безпеки**	**Чим досвід провідних світових держав корисний для України?**
1	2	3
Компанії США	Впровадження системи "ризик менеджмент", безперервна перевірка всіх фінансових, ринкових ризиків, та загроз пов'язаних із інформацією і технологіями, використання штучного інтелекту, як інструменту аналітики вияслення небезпеки, розробка оновлених видів систем кіберзахисту даних	Покращення стану систему кібербезпек для своєчасного виявлення загроз, забезпечення безперервного функціонування підприємств в умоває воєнного стану, зниження втрат від кібератак
Німецькі провідні компанії	Впровадження економічної безпеки у стратегічне планування, нові розробки систем аудиту компанії, оновлення менеджменту ланок, які відповідають за постачання і захист виробництва, комплаєнс-контроль	Допомога в усуненні ризиків внутрішнього менедженту, підвищення довіри для інвестування та підтримці міжнародного партнерства
Компанії країн Євросоюзу	Введеня багатоступінчатих систем кібербезпеки, сучасні підходи в сфері шифрування даних, багатофакторна автентифікація, запровадження ESG-підходи для корпоративного менеджменту	Впровадження европейських стандартів інвестування та забезпечення діяльності відповідного рівня європейського ринку

Продовження табл. 3.1

1	2	3
Японські компанії	Планування із багаторічною орієнтацією, колективна відповідальність, корпоративну відповідальність, постійне оновлення системи Kaizen та обов'язкова участь співробітників в системі ризик менеджементу	Допомога в адаптації бізнесу до криз в економічній сфері, формування основ корпоративної та колективної відповідальності організаційних структур
Високотехнологічні корпорації Південної Кореї	Розширення виробництва та шляхів постачань введення інновацій в технологічні сфери, створення резервних шляхів сбуту та альтернативних постачальників	Допомога у збереженні стабільності українських підприємств при порушенні логістичних шляхів і зовнішніх потрясінь при кризових світових спадах в економіці

Примітка.Джерело: складено автором на основі [53-56]

Український бізнес існує в середовищі постійного стресу, який пов'язаний із обстрілами об'єктів підприємства, руйнуваннями, логістичними обмеженнями, дефіцитом ресурсу та відсутностю фінансової стабільності, частково спричиненою втратою кваліфікованих кадрів. Саме через ці фактори досвід міжнародних технік економічної безпеки може стати корисним для українських компаній та установ.

Важливим напрямом є створення альтернативних шляхів логістики, резервування ресурсів, пошук різних постачальників. Важливий фактор - це впровадження системи контролю, системи прозорого корпоративного управління, усунуння внутрішніх небезпек, що підвищить зацікавленість інвесторів та світових партнерів. Важливу роль також відіграє формування культури економічної безпеки серед працівників, оскільки людський фактор залишається одним із ключових джерел ризиків для підприємств в Україні.

3.2. Удосконалення державної політики України щодо зміцнення економічної безпеки підприємництва в умовах геополітичних ризиків та кіберзагроз

Економічна безпека України за умов наростання глобальних викликів вимагає розроблення узгодженої та системної стратегії реагування, орієнтованої на

зміцнення державної стійкості, підвищення результативності інституцій, обмеження впливу зовнішніх ризиків і формування адаптивної моделі економічного розвитку. Особливої ваги набувають ті напрями, які дають змогу одночасно зменшувати внутрішні вразливості та посилювати здатність національної економіки протистояти як зовнішнім, так і внутрішнім шокам. Україна нині функціонує в умовах багаторівневого тиску, що поєднує воєнні загрози з масштабними економічними, технологічними та інституційними змінами. Саме тому стратегічне зміцнення економічної безпеки має охоплювати комплекс дій у структурній, фінансовій, технологічній та інституційній площинах. В умовах постійних екзистенційних загроз, зумовлених військовою агресією РФ, а також накопичених внутрішніх дисбалансів, традиційні підходи до забезпечення економічної безпеки України вже не відповідають актуальному рівню ризиків. Як показав аналіз, проведений у попередніх розділах, інтегральний показник економічної безпеки перебуває в зоні критичного ризику, що відповідає помаранчевому рівню, а отже, потребує не точкового реагування на окремі загрози, а переходу до стратегічного конструювання нової архітектури безпеки. Стратегія посилення економічної безпеки України повинна ґрунтуватися на принципах людиноцентричності, економічної свободи та інституційної спроможності. Її головним завданням має стати трансформація національної економіки від моделі виживання до моделі стійкого розвитку за умов збереження воєнних ризиків [57].

З огляду на результати проведеного аналізу ключових загроз, серед яких особливе місце посідають інституційна слабкість, високе боргове навантаження та демографічна криза, доцільно запропонувати схему стратегічних пріоритетів забезпечення економічної безпеки, подану на рис. 3.1.

Рис.3.1. Архітектура стратегічних пріоритетів економічної безпеки України

Примітка.Джерело: складено автором на основі [57-59]

Україна має відмовитися від ситуативного подолання криз і переходу добільш гнучкої стратегічної моделі економічної безпеки. Орієнтир потрібно тримати на збереженні поточної стабільності, забезпеченні якісного, тривалого та стійкого економічного зростання, така практична реалізація можлива лише за умови трансормації трьох взаємопов'язаних рівнів: інституційної основи, ресурсного забезпечення та секторальної модернізації.

Головним базовим рівнем має бути інституційний фундамент, саме цей рівень визначає якість державного управління, раціональність розподілу ресурсів, прозорість економічних процесів і ступінь інвестиційної привабливості країни. За умов слабкості або ненадійності інституцій будь-які інші заходи можуть втрачати результативність або не забезпечувати очікуваного практичного ефекту. Проведений аналіз підтверджує, що однією з найбільш небезпечних внутрішніх загроз для України залишається низька ефективність державних інститутів [58].

Ключовими завдання зміцнення економічної безпеки підприємства є:

а) Спрощення дозвільних процедур;

b) Зменшення адміністративного тиску на бізнес і скорочення кількості контролюючих органів;
c) Підвищення рівня економічної свободи для посилення конкурентоспроможність;
d) Розширення електронних сервісів, по типу платформи «Дія»;
e) Цифровізація митних та податкових функці задля сприяння підвищення прозорості;
f) Зменшення ролі людського фактора, обмеження корупційних ризиків і раціоналізації державних видатків.

Однією з найгостріших довгострокових загроз для економічної безпеки залишається відтік кваліфікованої робочої сили як за межі країни, так і всередині неї. У зв'язку з цим необхідним є розроблення комплексної державної програми, спрямованої на стимулювання повернення громадян, передусім жінок і висококваліфікованих спеціалістів. Така програма має включати створення безпечних умов праці, забезпечення доступного житла та системну підтримку сімей, що потребує тісної взаємодії з міжнародними організаціями [59].

Важлива умова економічної безпеки та подальшого зростання є вирішення проблеми державного боргу, яка наразі є критичною. Необхідно розробити стратегії, які включатимуть в себе такі складові, як реструктуризація та часткове списання боргу. Водночас атаки на централізовану енергосистему продемонстрували її надзвичайну вразливість, тому стратегічний акцент має бути зміщений у бік децентралізації генерації. Йдеться про розвиток малих і середніх модульних реакторів, сонячної та вітрової енергетики на рівні громад. Такий підхід не лише підвищує енергетичну безпеку, а й зміцнює здатність економіки витримувати воєнні загрози. Стратегічним завданням є поступовий відхід від радянської моделі надмірно централізованої енергетики та стимулювання розподіленої генерації на основі відновлюваних джерел енергії, газопоршневих установок і малих модульних реакторів. Це дасть змогу зменшити ризик повних блекаутів у разі атак на критичну інфраструктуру [60].

Структурна перебудова української економічної системи - це третій рівень. Запровадження виробництва власного військово-промислового комплексу та

напряму Military-Tech буде і складовою національного захисту, а також потужним фактором економічного розвитку. Інвестиції направлені на дослідження та розробку цього напряму забезпечить нові робочі місця, оптимізацію економічних та фінансових сфер, що зробить привабливим для тестування інноваційних технологій на території України.

Зважаючи на те, що обсяг державного боргу наближається до позначки 100 % ВВП, стратегічна логіка економічної політики має передбачати переорієнтацію з подальшого нарощування боргових зобов'язань на стимулювання такого економічного зростання, темпи якого перевищуватимуть швидкість збільшення боргового навантаження.

Європейська інтеграція може розглядатися як одна з ключових стратегічних рамок зміцнення економічної безпеки України. Поступове наближення до Європейського Союзу формує для держави чітку систему орієнтирів у сфері економічної політики, інституційного оновлення та впровадження сучасних безпекових стандартів. У цьому контексті пріоритетного значення набувають гармонізація регуляторного середовища з acquis ЄС, поетапне включення до внутрішнього ринку Європейського Союзу, участь у програмі відбудови «Ukraine Facility», розширення співпраці в енергетичній сфері, цифровій економіці та безпеці [60], а також долучення до європейських механізмів раннього виявлення кризових процесів.

Євроінтеграційний вектор сприяє посиленню інституційної стійкості держави, зниженню політичних та економічних ризиків і розширенню доступу до фінансових, технологічних та управлінських ресурсів. Успішна реалізація запропонованої трирівневої стратегії може забезпечити Україні не лише відновлення втраченого економічного потенціалу, а й створення якісно нової економічної системи, здатної витримувати майбутні глобальні та геополітичні потрясіння. Визначальною умовою досягнення стратегічної мети, пов'язаної з економічною потужністю та безпекою, є узгоджене поєднання інституційних реформ, мобілізації людського й фінансового капіталу та структурного оновлення ключових секторів. Отже, стратегічні напрями забезпечення економічної безпеки України мають комплексну природу й

охоплюють підтримання макроекономічної стабільності, розвиток інституційної спроможності, зміцнення енергетичної та інфраструктурної стійкості, модернізацію економічної структури, посилення людського капіталу й поглиблення міжнародної інтеграції. Реалізація цих напрямів формує основу для довгострокової стійкості національної економіки, її здатності адаптуватися до глобальних ризиків і забезпечувати сталий розвиток навіть в умовах високої невизначеності.

Управління ризиками має кілька взаємопов'язаних етапів - від постійного відстеження загроз до коригування державної політики. Головним етапом виступає моніторинг загроз, що передбачає безперервне збирання, систематизацію, оброблення та аналіз інформації про наявні й потенційні ризики. Такий моніторинг повинен охоплювати як зовнішні чинники, серед яких динаміка світових цін на енергоресурси та продовольство, зміни у геополітичних альянсах, обсяги зовнішнього фінансування й загострення конфліктів, так і внутрішні вразливості, зокрема стан критичної інфраструктури, рівень фіскальної стійкості та масштаби відтоку капіталу. Основним інструментом цього етапу має бути система раннього попередження (Early Warning System), що ґрунтується на використанні інтегральних та індивідуальних індикаторів економічної безпеки [61].

Зважаючи на те, що обсяг державного боргу наближається до позначки 100 % ВВП, стратегічна логіка економічної політики має передбачати переорієнтацію з подальшого нарощування боргових зобов'язань на стимулювання такого економічного зростання, темпи якого перевищуватимуть швидкість збільшення боргового навантаження.

Європейська інтеграція може розглядатися як одна з ключових стратегічних рамок зміцнення економічної безпеки України. Поступове наближення до Європейського Союзу формує для держави чітку систему орієнтирів у сфері економічної політики, інституційного оновлення та впровадження сучасних безпекових стандартів. У цьому контексті пріоритетного значення набувають гармонізація регуляторного середовища з acquis ЄС, поетапне включення до внутрішнього ринку Європейського Союзу, участь у програмі відбудови «Ukraine Facility», розширення співпраці в енергетичній сфері, цифровій економіці та безпеці

[60], а також долучення до європейських механізмів раннього виявлення кризових процесів.

Євроінтеграційний вектор сприяє посиленню інституційної стійкості держави, зниженню політичних та економічних ризиків і розширенню доступу до фінансових, технологічних та управлінських ресурсів. Успішна реалізація запропонованої трирівневої стратегії може забезпечити Україні не лише відновлення втраченого економічного потенціалу, а й створення якісно нової економічної системи, здатної витримувати майбутні глобальні та геополітичні потрясіння. Визначальною умовою досягнення стратегічної мети, пов'язаної з економічною потужністю та безпекою, є узгоджене поєднання інституційних реформ, мобілізації людського й фінансового капіталу та структурного оновлення ключових секторів. Отже, стратегічні напрями забезпечення економічної безпеки України мають комплексну природу й охоплюють підтримання макроекономічної стабільності, розвиток інституційної спроможності, зміцнення енергетичної та інфраструктурної стійкості, модернізацію економічної структури, посилення людського капіталу й поглиблення міжнародної інтеграції. Реалізація цих напрямів формує основу для довгострокової стійкості національної економіки, її здатності адаптуватися до глобальних ризиків і забезпечувати сталий розвиток навіть в умовах високої невизначеності.

Для практичного впровадження визначених стратегічних орієнтирів необхідним є застосування конкретного набору інструментів, здатних послаблювати вплив глобальних ризиків, зокрема геополітичних конфліктів, кліматичних змін, технологічних зрушень, а також внутрішніх загроз. Управління ризиками має послідовну логіку й охоплює кілька взаємопов'язаних етапів - від постійного відстеження загроз до коригування державної політики. Моніторинг повинен охоплювати як зовнішні чинники, серед яких динаміка світових цін на енергоресурси та продовольство, зміни у геополітичних альянсах, обсяги зовнішнього фінансування й загострення конфліктів, так і внутрішні вразливості, зокрема стан критичної інфраструктури, рівень фіскальної стійкості та масштаби відтоку капіталу. Основним інструментом цього етапу має бути система раннього

попередження (Early Warning System), що ґрунтується на використанні інтегральних та індивідуальних індикаторів економічної безпеки [61].

Наступний етап - це оцінка впливу, яка з урахуванням зібраних даних може визначити потенційний або вже проявлений вплив виявленної загрози на основні складові фінансової, виробничої та соціальної сфер. Застосувавши сценарний аналіз та стрес-тестування можна визначити майбутні втирати, наприклад, припинення зовнішнього фінансування або суттєвої втрати енергетичних потужностей, що дає можливість не тільки ранжування ризиків за рівнем їх важливості, а й встановити пріоритети управлінського реагування (табл. 3.2).

Таблиця 3.2

Основні інструменти підвищення економічної стійкості підприємств та зниження рівня ризиків

Категорія ризику	Інструменти забезпечення стійкості	Принцип реалізації
Порушення глобальних логістичних ланцюгів	Nearshoring та Friendshoring	Розміщення виробничих потужностей у географічно близьких або партнерських країнах, а також інтеграція підприємств у європейські транспортно-логістичні системи
Недостатній рівень інвестицій	Розвиток індустріальних парків та спеціальних економічних зон	Надання податкових і митних стимулів для бізнесу, зокрема пільгового режиму імпорту обладнання та тимчасового звільнення від окремих податків
Енергетичні ризики та дефіцит ресурсів	Механізми «Net Billing» і підтримка альтернативної енергетики	Створення умов для розвитку власної генерації електроенергії та можливості продажу надлишків енергії до загальної мережі
Тіньова економіка та корупційні ризики	Цифрові державні сервіси та електронне адміністрування	Автоматизація адміністративних процесів, підвищення прозорості фінансових операцій та скорочення прямого контакту бізнесу з державними органами
Міграція трудових ресурсів та дефіцит кадрів	Грантові та державні програми підтримки підприємництва	Фінансова підтримка створення малого та середнього бізнесу за умови розвитку зайнятості та створення нових робочих місць

Примітка.Джерело: складено автором на основі [61-63]

Перший аналітичний блок орієнтований на розгляд інструментів зниження вразливості глобальних ланцюгів постачання, загострення якої стало наслідком

пандемії COVID-19, геоекономічної фрагментації та повномасштабної агресії Росії проти України. Перенесення виробництва і частково бізнесу у інші країни та стратерічне партнерство є найбільш надійними складовими цієї концепції. Для України використання таких підходів відкриває можливості для глибшого залучення до ключових транспортних коридорів, розміщення виробництв у сферах машинобудування, електроніки та легкої промисловості, зменшення логістичних витрат європейського бізнесу, створення значної кількості нових робочих місць і формування стійких транскордонних виробничих кластерів. Стратегічне значення цього напряму полягає в тому, що він може одночасно посилити участь України у світовій торгівлі та зменшити її залежність від нестабільних азійських ринків.

Другим блоком є подолання дефіциту капіталу. Промислові парки, що діють на засадах спеціальних податкових режимів, створюють для інвесторів середовище зі зниженими бар'єрами входу. Серед ключових стимулів можна виокремити звільнення від сплати податку на прибуток упродовж перших 5-10 років, застосування нульового мита на імпорт обладнання, державне співфінансування інженерної інфраструктури та спеціальні умови для високотехнологічних виробництв. Міжнародна практика свідчить, що подібні механізми стали одним із чинників економічного прориву Польщі, Чехії, Словаччини та Туреччини. Для України розвиток індустріальних парків має принципове значення не лише як інструмент післявоєнного відновлення, а й як спосіб локалізації європейських виробництв на українській території.

Ризики, пов'язані із корупцією та тінізацією підприємств суттєво зменшують залучення інвестицій. Гарні результати Україна демонструє в розвитку цифровізації, яка обмежує безпосередній контакт громадянина чи бізнесу з особою посадовцем. Такі застосунки як «Дія», e-Excise, електронні митні та податкові сервіси, сприяють автоматизації податкового адміністрування, зниженню корупційних ризиків через усунення зайвих посередницьких ланок, інтеграції баз даних, підвищенню прозорості операцій, скороченню масштабів тіньового сектору та зміцненню довіри бізнесу до державних інституцій. Україна вже належить до

визнаних світових лідерів у сфері електронного урядування, що підтверджується міжнародними оцінками, зокрема UN Digital Governance Index.

Також, програма «єРобота» є дієвим інструментом для підтримки бізнесу в умовах війни. Надання фінансової допомоги для відкриття власної справи, яка створює нові робочі місця та підтримка виробництва і аграрного бізнесу формує сприятливі умови для повернення українців із-за кордону (табл. 3.3).

Таблиця 3.3

Напрями удосконалення державної політики України щодо зміцнення економічної безпеки підприємництва в умовах геополітичних ризиків та кіберзагроз

Напрями вдосконалення політики України	**Введення яких змін потребує для зміцнення економічної безпеки підприємств країни**
1	2
Інвестування, програми грантів та покращення функцій держаного адміністрування	Зменшення корупційних ризиків, зниження тиску для підприємств з боку держави, прозора система регуляторної політики, залучення не тільки зовнішнього, а й внутрішнього інвестування, оптимізація виробничих процесів підприємств, залучення малого та середнього бізнесу до фінансових джерел, тим самим стимулюючи створення нових комерційних структур та робочих місць
Зниження державних обмежень для підприємств	Спрощення стандартів державних органів щодо дотримання вимог, які прискорять відкриття і стабільний розвиток нових підприємств, підвищення конкурентоспроможності
Автоматизація адміністративних послуг, інтенсивне зростання сфери електронного керування	Усунення людського фактору та переведення більшої частини завдань в цифрову форму, що покращить взаємодію комерційних структур із адміністративною ланкою
Посилення заходів в сфері кіберзахисту всіх держаних стратегічно важливих установ та життєво важливих об’єктів	Гарантії безперервної виробничої діяльності, безпека електронних сервісів, що значно зменшить ризики пов’язані із кібератаками
Введення системи виявлення фінансових ризиків на ранній стадії - Early Warning System	Вчасне виявлення криз, аналітика можливих загроз для прогнозування, попередження та підвищення реагування в умовах можливих фінансових ризиків
Підвищення кількості технологічних парків, індустріальних зон	Необхідність у створенні робочих місць, розробка нових напрямів залучення інвестиції, розвиток більших можливостей для виробництва
Акцент на курсі повернення працездатного насення та його підтримка	Вирішення проблем дифіциту кадрів, забезпечення підприємств кваліфікованим персоналом, підвищення результативності
Пошуки шляхів перерозроділу енергетики	Розробка напрямів стійкості підприємств в кризових умовах, децентралізація джерел енергетики, перехід на власну генерацію
Об’єднання українського виробництва та логістичних шляхів із державами євросоюзу	Пошук нових напрямків сбуту, розробка методів експортних можливостей підприємств, зниження ризиків пов’язаних із логістикою

Продовження табл. 3.3

1	2
Активний розвиток високотехнологічних сфер, введення штучного інтелекту в сфери цифрового та технічного напрямів	Оптимізацій старих та створення нових високотехнологічних виробництв, пошук шляхів підвищення технологічної спроможності для незалежності та повної автономії
Оптимізація механізму зменшення державного боргу та економічної стійкості	Розробка способів усунення ризиків пов'язаних із макроекономічною ситуацією, забезпечення стабільної роботи фінансової сфери для інтенсивного розвитку бізнесу

Примітка. Джерело: складено автором на основі [60-64]

Україна має прийняти участь у тестуванні новітніх технологій, зумовлених стрімким розвитком штучного інтелекту, держава буде виконувати не тільки роль регулятора, а ще й замовника та партнера. Така участь здатна підвищити інтегральний індекс економічної безпеки з нинішнього помаранчевого рівня до зони стійкого розвитку, перетворивши глобальні ризики на ресурс глибокої модернізації України.

3.3. Стратегічні шляхи та ефективні інструменти посилення економічної безпеки українських компаній як суб'єктів міжнародного бізнесу у воєнний час та в період повоєнного відновлення країни

Повномасштабне вторгнення для бізнесу створило комплекс викликів:

1) Порушення логістики.
2) Втрата виробничих потужностей.
3) Зниження інвестиційної привабливості.
4) Різке погіршення фінансового стану підприємств.
5) Дефіцит кадрів.
6) Збільшення кіберзагроз.
7) Економічна внутрішня криза.

Українські підприємства були змушені в умовах стресу пристосовуватися до нових реалій, переглядати стратегії подальшої діяльності з урахуванням майбутнього повоєнного відновлення держави. У зв'язку з цим стратегічні напрями

зміцнення економічної безпеки мають формуватися, як комплексна система заходів, яка має охоплювати одночасно фінансову, виробничу, кадрову, інформаційну, інноваційну, інвестиційну, зовнішньоекономічну сфери.

Диверсифікація зовнішньоекономічної діяльності має значну провідну роль. До війни більша частина компаній та виробництв були зосереджені в дуже вузькому колі шляхів збуту і постачальників. Після повномасштабного вторгнення така залежність прийнята критичний стан, саме тому розширюючи географію бізнесу виробничі процеси варто перенести на нові зарубіжні площини, адаптувати продукцію до стандартів кількох держав, а також створювати альтернативні канали постачання сировини, матеріалів і комплектуючих. Необхідність об'єднання виробництва українських та європейських компаній суттєво зменшить фінансові ризики.

Для більшого зміцнення економічної безпеки є потреба в залученні програм грантів, кредитів міжнародних фінансових організацій, інвестиційних фондів та програм підтримки бізнесу, які реалізуються Європейським Союзом, Світовим банком, ЄБРР та іншими міжнародними інституціями.

Війна показала, що підприємства, які активно використовують цифрові технології, мають вищу здатність до адаптації та краще витримують кризові впливи. Застосування хмарних сервісів, автоматизації бізнес-процесів, цифрових платформ управління ресурсами, електронного документообігу та інструментів дистанційної роботи дає змогу підтримувати безперервність діяльності підприємств навіть за умов фізичних загроз, руйнування інфраструктури або обмеженого доступу до офісних і виробничих приміщень.

Кібербезпека потребує пильної уваги, тому що після лютого 2022 року обсяг кібератак на бізнес в Україні, банківські і державні установи та критичну інфраструктуру суттєво збільшився. За таких умов підприємства зобов'язані впроваджувати інноваційні системи кіберзахисту, інструменти резервного копіювання і зберігання інформації та даних, технології моніторингу загроз та способи підвищення цифрової грамотності персоналу.

Кадрова стабільність та розвиток людського капіталу стратегічно важливий напрям економічної безпеки. Війна є причиною значних демографічних втрат, трудова міграція загострила труднощі нехватки кваліфікованих спеціалістів. З урахуванням цих обставин підприємства мають переглянути підходи управління персоналом і забезпечити працівників додатковими системами мотивації, розвитку професійних якостей за рахунок компанії, психологічна та, при необхідності, матеріальна підтримка.

У період повоєнного відновлення одним із визначальних чинників економічної безпеки стане інноваційний розвиток українських компаній. Світовий досвід підтверджує, що держави, які успішно проходили етап післявоєнної відбудови, робили акцент на модернізації виробництва, технологічному оновленні та розвитку інноваційного сектору. Для українського бізнесу це означає потребу в переході від сировинно орієнтованої моделі експорту до виробництва продукції з високою доданою вартістю, розвитку технологічних стартапів, цифрових платформ, екологічних технологій і сучасних виробничих рішень.

Важливу роль у забезпеченні економічної безпеки відіграє державна політика підтримки підприємництва. За сучасних умов ефективна взаємодія держави та приватного сектору є необхідною умовою стабілізації економічної системи. До основних інструментів державної підтримки можна віднести податкові стимули, державні гарантії для інвесторів, програми кредитування бізнесу, страхування воєнних ризиків, розвиток індустріальних парків, підтримку експорту та стимулювання локалізації виробництва.

До результативних засобів зміцнення економічної безпеки українських компаній у період війни та на етапі повоєнного відновлення доцільно віднести сукупність управлінських, фінансових, організаційних, цифрових, кадрових і зовнішньоекономічних інструментів. Їхня практична цінність полягає не лише у здатності забезпечувати реагування на вже наявні загрози, а й у можливості завчасно формувати внутрішню стійкість підприємства до потенційних кризових ситуацій.

Одним із основних інструментів виступає система ризик-менеджменту, яка охоплює систематичне виявлення, оцінювання, пріоритизацію та відстеження ризиків, здатних впливати на діяльність компанії. Для українських підприємств особливо значущими є ризики воєнного, логістичного, валютного, фінансового, інвестиційного, кадрового, кібернетичного та репутаційного характеру. На практиці така система може реалізовуватися через розроблення карти ризиків підприємства, визначення критично важливих бізнес-процесів, підготовку сценаріїв дій у кризових умовах і закріплення відповідальних осіб за окремими напрямами безпеки.

Важливе місце посідає антикризове фінансове планування, сутність якого полягає у створенні фінансових резервів, контролі руху грошових потоків, оптимізації витрат, коригуванні платіжного календаря та підтриманні належного рівня ліквідності. У воєнних умовах підприємство має формувати кілька варіантів бюджету, зокрема оптимістичний, базовий і кризовий. Такий підхід дає змогу оперативно змінювати фінансову політику у відповідь на валютні коливання, скорочення попиту, затримки платежів або підвищення витрат на логістику й енергозабезпечення.

Окремого значення набуває диверсифікація джерел фінансування. Компаніям недоцільно покладатися виключно на власний прибуток або один банківський кредит, оскільки така залежність підвищує фінансову вразливість. Доцільним є використання грантових програм, міжнародних інструментів підтримки бізнесу, кредитів міжнародних фінансових організацій, державних компенсаційних програм, інвестиційних фондів, експортного фінансування та механізмів державно-приватного партнерства. У повоєнний період саме доступ до різних джерел капіталу стане однією з важливих передумов швидкого відновлення виробництва та активного виходу підприємств на зовнішні ринки.

Страхування ризиків в умовах конфлікту є важливим елементом майнових, вантажних, експортних, воєнних та політичних небезпек Для міжнародних партнерів та інвесторів велике значення мають не тільки виробничий потенціал підприємств, а також і рівень захисту операцій, активів та договірних зобов’язань.

Страхування забезпечує зменшення фінансових збитків, збою поставок та невиконань умов контракту.

Компанія повинна усунути залежність від одного постачальника та одного логістичного напряму, важливою є диверсифікація постачальників і ринків збуту. Акцент необхідно робити саме на рамкових домовленностях із декількома партнерами, налагодити продажі в кілька різних держав та модернізувати продукцію направлену на кілька ринків.

Перебої транспортування, підвищення цін перевізників, обмежені морські шляхи та ризики ужкодження вантажу - це все реалії українських компаній в рокі війни. Забезпечення цифрового моніторингу поставки вантажу, своєчасне планування маршрутів та резервні запаси критично важливих ресурсів допоможуть дотримуватися дедлайнів міжнародних домовленостей та виконання контрактів, які будуть сприяти безперервному процесу виробництва.

До ключових цифрових інструментів належать ERP-, CRM- та SCM-системи, які забезпечують централізоване управління ресурсами, клієнтськими відносинами, запасами, постачанням і фінансовими потоками. Їх використання дозволяє підприємству оперативно отримувати актуальну інформацію про стан бізнес-процесів, контролювати витрати, прогнозувати потребу в матеріалах, управляти замовленнями та швидко реагувати на зміну попиту. Для міжнародного бізнесу такі системи мають особливу цінність, оскільки забезпечують координацію діяльності між різними країнами, складами, партнерами та клієнтами.

Окремим практичним засобом виступає цифровий моніторинг економічної безпеки, який ґрунтується на застосуванні аналітичних панелей, BI-систем, фінансових показників, автоматизованої звітності та механізмів раннього попередження. За допомогою таких інструментів підприємство може відстежувати динаміку дебіторської заборгованості, зміну собівартості продукції, валютні коливання, затримки у постачанні, зниження обсягів продажу або перевищення запланованих бюджетних витрат. У разі виходу певного індикатора за встановлені допустимі межі система повинна автоматично інформувати керівництво про можливе виникнення загрози.

Кіберзахист дуже важливий напрям, до інструментів якого належать:

- ✧ Резервне копіювання даних та інформації;
- ✧ Багатоступінчаста автентифікація;
- ✧ Шифрування;
- ✧ Системи антивірусного захисту;
- ✧ Забезпечення захищенності корпоративної електронної пошти;
- ✧ Безперервне оновлення програмного забезпечення;
- ✧ Контроль та відстежування доступів до внутріншіх конфіденційних систем;
- ✧ Навчання робітників цифрової грамотності.

Будь-який витік інформації або злам корпоративних систем може спричинити фінансові збитки та погіршення ділової репутації.

Підприємствам необхідно ввести формат Business Continuity Planning - це порядок дій в кризових та стресових ситуаціях, такі як припинення електропостачання, руйнування складських приміщень, перешкоди для логістики, кібрзагрози, ймовірність евакуацій працівників, неможливість доступу до офісного приміщення. Цей порядок визначає план дій та алгоритм комунікації, за допомогою резервних каналів зв'язку, осіб які мають організувати процес, альтернативні місця та час відновлення виробничого процесу.

Не менш важливим фактором є енергетична незалежність підприємств, з урахуванням частих атак, бізнес просто зобов'язаний мати резерв електропостачання такі, як:

1. Генератори.
2. Акумуляторні системи.
3. Сонячні панелі.
4. Договори з альтернативними постачальниками енергії.
5. Плани раціонального використання ресурсів.

Стабільність енергозабезпечення напряму впливає на виконання замовлень і збереження клієнтських контрактів.

Корпоративна безпека має відіграє роль у функціонуванні підприємств, саме формування кадрового резерву, система гнучкого графіку роботи, можливість

працювати диистанційно, прозора ситема мотивації разом із програмами підвищення кваліфікації та психологічної підтримки дають суттєві переваги в утриманні фахівців та запобіганні плинності кадрів.

В час активних воєнних дій бізнес має враховувати ризики, які пов'язані із міграцією працівників, емоційне вигорання персоналу, оперативна заміна важливих спеціалістів.

Для зміцнення міжнародної конкурентоспроможності вагомим інструментом є сертифікація продукції та впровадження міжнародних стандартів. Йдеться про стандарти якості, безпечності продукції, екологічного менеджменту, інформаційної безпеки й корпоративного управління. Наявність міжнародних сертифікатів спрощує вихід на зовнішні ринки, підвищує рівень довіри з боку партнерів і зменшує бар'єри для експорту (табл. 3.4).

Таблиця 3.4

Стратегічні заходи та ефективні інструменти посилення економічної безпеки українських компаній як суб'єктів міжнародного бізнесу у воєнний час та в період повоєнного відновлення країни

Стратегічні заходи та ефективні інструменти	**Результати впровадження стратегічних заходів**
1	2
Диверсифікація зовнішніх шляхів збуту, постачальників та марштрутів логістики	Зменшення залежності від певних ринків до 50%, більш результативна експорта діяльність, зниження ризиків фінансових втрат у випадку закриття одного із напряму сбуту, зменшення імовірності зупитки виробничого процесу до 60%, стабільність постачань та виконання договорів
Об'єднання виробництва із компаніями Євросоюзу	Ріст експорту, можливість доступу на ринку ЄС, скорочення витрат на логістику до 20%
Планування ризиків і резервні фонди	Підвищить рівень ліквідності підприємств, зменшить ймовірність несплатоспроможності до 35%, збільшить фінансову стійкість в умовах криз
Пошуки нових джерел фінансової підтримки (кредити, інвестиції, гранти)	Збільшення доступу до нових моделей фінансування до 50%, можливість швидкого відновлення бізнесу
Оновлення систем кібербезпеки	Суттєве зменшення можливих кібератак до 80%, мінімальна ймовірність витоку даних та втрати важливої інформації, що може завдати фінансових збитків
Підготовка кадрів з питань економічної безпеки, резерв кадрового потенціалу	Скорочення випадків людського фактору до 60%, збільшення продуктивності праці до 20%, усунення можливого дефіциту важливих спеціалістів і плинності кадрів
Мультмодальна логістика, складскі приміщення	Усунення логістичних перешкодо 40%, більший рівень надійності постачань та виконання контрактів

Продовження табл. 3.4

1	2
Сертифікована продукція згідно стандартів ISO та ESG, інноваційна дяльність у виробніцтві продукції із більшою вартістю	Ріст прибутку підприємств до 40%, вихід на нові зовнішні ринки, підвищення конкурентоспроможності, збільшення експорту
Перехід до енергетичної незалежності	Зменшення ризику часткового або повного відключення від електрики з урахуванням використання генераторів, акумуляторів та систем ВДЕ до 80%, стабільність виробничої діяльності
Дистанційна робота та гнучкий графік	Безперервна робота персоналу в умовах війни, зменшення операційних витрат до 15%
Комплаєнс, міжнародний стандарт коропоративного менеджменту	Суттєве зниження штрафних санкцій та судових процесів, підвищений рівень довіри інвесторів і міжнародних партнерів
Страхування від всіх можливих ризиків	Зменшення ймовірних фінансових втрат до 70% на майнові, експортні, воєнні чи політичні ризики, підвищення привабливість для вливання інвестицій
Впровадження системи due diligence	Усунення до 50% ризикованих угод із контрагентами пов'язаних із юридичними, фінансовими та репутаційними небезпеками
Планування безперервного бізнес процесу	Менший час на відновлення виробничої діяльності пов'язаним із кризами та стресовими ситуаціями на 60%, підвищення стійкості підприємства
Системи ризик-менеджменту	Суттєве зниження втрат на 40%, швидкість реагування в кризових ситуаціях, підвищення якості організаційних рішень
Перехід до цифрової автоматизації бізнес-процесу	Ріст продуктивності до 30%, зниження на операційні витрати до 25%, більш раціональне управління ресурсами
Цифровий моніторинг в сфері економічного захисту	Зменшення часу для виявлення небезпек в три рази, можливість більш точно спрогнозувати ризики та фінансові результати

Примітка. Джерело: розроблено автором на основі [59-64]

Забезпечення економічної безпеки українських компаній у воєнний час і в період повоєнної відбудови потребує реалізації цілісної системи стратегічних заходів, спрямованих на підвищення стійкості підприємств до внутрішніх і зовнішніх загроз. Основними напрямами її посилення є диверсифікація зовнішньоекономічної діяльності, підтримання фінансової стабільності, цифрова трансформація бізнесу, розвиток кібербезпеки, зміцнення кадрового потенціалу, інноваційне оновлення виробництва та ефективна державна підтримка підприємництва. Упровадження зазначених заходів сприятиме не тільки збереженню конкурентоспроможності українських підприємств у складних умовах

війни, а й формуванню основ для їх успішного функціонування в післявоєнній економіці та глобальному бізнес-середовищі.

Висновки до розділу 3

Український бізнес існує в середовищі постійного стресу, який пов'язаний із обстрілами об'єктів підприємства, руйнуваннями, логістичними обмеженнями, дефіцитом ресурсу та відсутностю фінансової стабільності, частково спричиненою втратою кваліфікованих кадрів. Саме через ці фактори досвід міжнародних технік економічної безпеки може стати корисним для українських компаній та установ.
Важливим напрямом є створення альтернативних шляхів логістики, резервування ресурсів, пошук різних постачальників. Важливий фактор - це впровадження системи контролю, системи прозорого корпоративного управління, усунення внутрішніх небезпек, що підвищить зацікавленість інвесторів та світових партнерів.
Економічна безпека України за умов наростання глобальних викликів вимагає розроблення узгодженої та системної стратегії реагування, орієнтованої на зміцнення державної стійкості, підвищення результативності інституцій, обмеження впливу зовнішніх ризиків і формування адаптивної моделі економічного розвитку. Особливої ваги набувають ті напрями, які дають змогу одночасно зменшувати внутрішні вразливості та посилювати здатність національної економіки протистояти як зовнішнім, так і внутрішнім шокам. Україна нині функціонує в умовах багаторівневого тиску, що поєднує воєнні загрози з масштабними економічними, технологічними та інституційними змінами. Саме тому стратегічне зміцнення економічної безпеки має охоплювати комплекс дій у структурній, фінансовій, технологічній та інституційній площинах.

Інструменти зміцнення економічної безпеки українських компаній повинні мати не декларативний, а реально впроваджений характер у системі управління підприємством. Найбільш результативним є поєднання фінансових, цифрових, організаційних, логістичних, кадрових, правових та інноваційних засобів. Саме така комплексність дає бізнесу змогу не лише підтримувати стабільність у період війни, а

й створювати передумови для активного розвитку в умовах повоєнного відновлення України.

Забезпечення економічного захисту українських компаній у воєнний час і в період повоєнної відбудови потребує реалізації цілісної системи стратегічних заходів, спрямованих на підвищення стійкості підприємств до внутрішніх і зовнішніх загроз. Основними напрямами її посилення є диверсифікація зовнішньоекономічної діяльності, підтримання фінансової стабільності, цифрова трансформація бізнесу, розвиток кібербезпеки, зміцнення кадрового потенціалу, інноваційне оновлення виробництва та ефективна державна підтримка підприємництва. Упровадження зазначених заходів сприятиме не тільки збереженню конкурентоспроможності українських підприємств у складних умовах війни, а й формуванню основ для їх успішного функціонування в післявоєнній економіці та глобальному бізнес-середовищі.

ВИСНОВКИ

Економічна безпека підприємства має не лише складну, а й багатоступінчату природу у поєднанні із кількома різними аспектами. Згідно проведеного аналізу можна сказати, що економічна безпека - це стан захищеності від реальних та можливих загроз, швидка адаптація при непередбачуваних обставинах та підвищення конкурентно спроможності з урахуванням зовнішніх факторів та змін, таких як воєнний стан, світові фінансові кризи, цифрові метаморфози в економічній сфері. Визначено, що методологічне підґрунтя дослідження економічної безпеки формується на основі міждисциплінарного бачення, яке інтегрує базові положення економічної теорії, управлінської науки та суміжних галузей знань.

За сучасних умов для підприємств дедалі важливішим стає не лише усвідомлення сутності геополітичних ризиків, а й формування дієвих механізмів реагування на виклики, пов’язані із зовнішньополітичними процесами. Якщо раніше локальні прояви нестабільності переважно сприймалися як чинники можливих порушень у ланцюгах постачання, то нині глобальні конкуренти значно активніше використовують санкційні режими, фінансові обмеження та торговельні ембарго. Такі інструменти виконують не тільки функцію регулювання міжнародної торгівлі, що ґрунтується на визначених правилах, а й дедалі частіше застосовуються як засоби реалізації зовнішньополітичних цілей. Унаслідок цього бізнес стає більш залежним від подій, які відбуваються на значній географічній відстані, а також від урядових рішень, ухвалених у відповідь на ці події.

Приклади застосування цифрових інструментів для забезпечення економічної безпеки компаніями демонструють, як великі корпорації впроваджують цифрові стратегії з урахуванням можливих загроз, передусім у напрямах кіберзахисту та охорони даних. Їхній досвід свідчить про можливість поєднання інноваційного розвитку із забезпеченням бізнес-стійкості, що дає змогу ефективніше пристосовуватися до змін цифрового середовища. Вивчення таких практик може слугувати для інших компаній практичним орієнтиром під час визначення пріоритетів цифрового інвестування, спрямованого на збереження фінансової та

операційної стабільності. Можна сказати, що цифрові технології мають глибокий і багатогранний вплив на різні аспекти економічної безпеки. Для мінімізації ризиків та оптимізації переваг необхідно забезпечити баланс між технологічними інноваціями та захистом ключових компонентів економічної безпеки.

Можна зробити висновок після проведеного комплексного аналізу тенденцій кіберзлочинів у світі, що рівень атак кожного року тільки зростає, механізми своєчасно виявити та попередити кіберзлочині менш єфективні, ніж системи вдосконалення цифрових загроз у шахраїв. Світова економіка несе глобальні витрати від хакерських атак, викраденні або розкриття персональної інформації про клієнтів та даних працівників, що підриває репутацію компанії, знижує рівень довіри, і відповідно має наслідки в стабільних прибутках.

Фішинг - це домінуюча ланка кіберзлочинців, яка характеризується зростаючою дінамікою для подальшого поширення. Найвищу вразливість до кіберзагроз зберігають освітній сектор, державні установи, сфера розваг і фінансові організації, оскільки саме в цих напрямах фіксується значна кількість інцидентів, пов’язаних із використанням шкідливого програмного забезпечення.

Найуразливіший зараз також є малий та середній бізнес. Сучасні кібератаки дедалі частіше будуються на використанні складних тактик, які дають змогу обходити традиційні механізми виявлення шкідливого програмного забезпечення та діяти всередині комплексних цифрових середовищ цільових організацій. Такі атаки можуть бути спрямовані на викрадення інформації, встановлення програм-вимагачів, шифрування даних або створення масштабних перебоїв у роботі підприємств.

Ризики пов’язані із політичною та військовою сферами несуть в собі широкий спект проблем, через безпосередній вплив збройного зіткненн, в першу чергу під ударом опиняються виробнича, логістична на транспортна ланки підприємства. Ріст страхових гарантій, часткова або повна зупинка виробничої діяльності, мобілізаційні міри, нестача робочої сили, збільшення кібератак, дестабілізація фінансової сфери в сукупності унеможливлюють функціонування будь-якого

виробництва, підприємство напряму залежить тільки від зовнішніх ринків, поставок та дій міжнародних партнерів.

Геополітичні та воєнно-політичні ризики є одними з найнебезпечніших у системі міжнародної економічної безпеки підприємств, оскільки їм властиві високий ступінь непередбачуваності, широкий масштаб впливу та здатність породжувати ланцюгові наслідки у світових виробничих, логістичних і фінансових системах.

Кіберзлочини мають масштабну площину атак і становлять загрозу будь-якому користувачу у будь-якій країні проживання та перебування. З урахуванням цієї проблеми дуже актуальним стає набуття цифрової грамотності для захисту користувачів, нові шляхи захисту та удосконалення інструментів безпеки та розробки правил, які спрямовані на запобігання всіх видів атак. Після проведеного комплексного аналізу тенденцій кіберзлочинів у світі, що рівень атак кожного року тільки зростає, механізми своєчасно виявити та попередити кіберзлочині менш єфективні, ніж системи вдосконалення цифрових загроз у шахраїв. Світова економіка несе глобальні витрати від хакерських атак, викраденні або розкриття персональної інформації про клієнтів та даних працівників, що підриває репутацію компанії, знижує рівень довіри, і відповідно має наслідки в стабільних прибутках.

Фішинг - це домінуюча ланка кіберзлочинців, яка характеризується зростаючою дінамікою для подальшого поширення. Найвищу вразливість до кіберзагроз зберігають освітній сектор, державні установи, сфера розваг і фінансові організації, оскільки саме в цих напрямах фіксується значна кількість інцидентів, пов’язаних із використанням шкідливого програмного забезпечення.

Найуразливіший зараз також є малий та середній бізнес. Сучасні кібератаки дедалі частіше будуються на використанні складних тактик, які дають змогу обходити традиційні механізми виявлення шкідливого програмного забезпечення та діяти всередині комплексних цифрових середовищ цільових організацій. Такі атаки можуть бути спрямовані на викрадення інформації, встановлення програм-вимагачів, шифрування даних або створення масштабних перебоїв у роботі підприємств.

Ризики пов’язані із політичною та військовою сферами несуть в собі широкий спект проблем, через безпосередній вплив збройного зіткненн, в першу чергу під ударом опиняються виробнича, логістична на транспортна ланки підприємства. Ріст страхових гарантій, часткова або повна зупинка виробничої діяльності, мобілізаційні міри, нестача робочої сили, збільшення кібератак, дестабілізація фінансової сфери в сукупності унеможливлюють функціонування будь-якого виробництва, підприємство напряму залежить тільки від зовнішніх ринків, поставок та дій міжнародних партнерів.

Геополітичні та воєнно-політичні ризики є одними з найнебезпечніших у системі міжнародної економічної безпеки підприємств, оскільки їм властиві високий ступінь непередбачуваності, широкий масштаб впливу та здатність породжувати ланцюгові наслідки у світових виробничих, логістичних і фінансових системах.

Кіберзлочини мають масштабну площину атак і становлять загрозу будь-якому користувачу у будь-якій країні проживання та перебування. З урахуванням цієї проблеми дуже актуальним стає набуття цифрової грамотності для захисту користувачів, нові шляхи захисту та удосконалення інструментів безпеки та розробки правил, які спрямовані на запобігання всіх видів атак. Інструменти зміцнення економічної безпеки українських компаній повинні мати не декларативний, а реальний характер впроваджений у систему управління підприємством. Найбільш результативним є поєднання фінансових, цифрових, організаційних, логістичних, кадрових, правових та інноваційних засобів. Саме така комплексність дає бізнесу змогу не лише підтримувати стабільність у період війни, а й створювати передумови для активного розвитку в умовах повоєнного відновлення України.

Гарантування економічної безпеки українських компаній у воєнний час і в період повоєнної відбудови потребує реалізації цілісної системи стратегічних заходів, спрямованих на підвищення стійкості підприємств до внутрішніх і зовнішніх загроз. Основними напрямами її посилення є диверсифікація зовнішньоекономічної діяльності, підтримання фінансової стабільності, цифрова трансформація бізнесу, розвиток кібербезпеки, зміцнення кадрового потенціалу,

інноваційне оновлення виробництва та ефективна державна підтримка підприємництва. Упровадження зазначених заходів сприятиме не тільки збереженню конкурентоспроможності українських підприємств у складних умовах війни, а й формуванню основ для їх успішного функціонування в післявоєнній економіці та глобальному бізнес-середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства: монографія; 2-ге вид., переробл. Київ : НІСД, 2015. 348 с. URL: https://niss.gov.ua/sites/default/ files/2015-10/lyashenko_1_druk-43fc7.pdf

2. Чернишов О. Особливості застосування концепції адаптивного управління при забезпеченні економічної безпеки підприємств. Економіка та суспільство, 2023. №48. https://doi.org/10.32782/2524-0072/2023-48-13

3. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства: монографія; 2-ге вид., переробл. Київ : НІСД, 2015. 348 с. URL: https://niss.gov.ua/sites/default/ files/2015-10/lyashenko_1_druk-43fc7.pdf

4. Кравченко О., Гаврилюк О., Челомбітько О., Бойко С. Управління економічною безпекою підприємств в умовах цифрової економіки. Адаптивне управління: теорія і практика. Серія Економіка, 2024. №19(38). DOI: https://doi.org/10.33296/2707-0654-19(38)-12

5. Данілова Е. І. Концепція системного підходу до управління економічною безпекою підприємства : монографія. Вінниця : Європейська наукова платформа, 2020. 342 с. URL: https://publishing.logos-science.com/index.php/books/article/view/danilova.kontseptsiia-2020/7

6. Шуст Наталія. Проблема впливу геополітичного концепту на імплементацію демократії. Наукові перспективи (Naukovì perspektivi), 2022, 5 (23). С.159-167.

7. Рогач О. Міжнародні інвестиції: Теорія та практика бізнесу транснаціональних корпорацій: Підручник. К.: Либідь, 2005. С. 589-591.

8. Yu Miaozhi, Wang Na. The Influence of Geopolitical Risk on International Direct Investment and Its Countermeasures. Sustainability, 2023, 15.3: 2522. [Електронний ресурс]. Режим доступу: https://doi.org/10.3390/su15032522

9. Оніщенко І. Г. Геополітичні ризики у новій політичній конфігурації світу. Держава і право. Серія: Політичні науки, 2018, 81. С. 193-203.

10. Паршин Ю. І., Паршина М. Ю. Аналіз соціально-економічного розвитку країн в умовах геополітичної напруженості. Східна Європа: економіка, бізнес та управління. 2020. № 25. С. 61-68.

11. Sharma Prashant, Kumar Surender. Zero-COVID policy and stock market sectoral performance in China. Innovations, 2023, 20.2. P. 116-126.

12. Антонюк В. П., Миценко І. М. Війна в Україні як глобальний цивілізаційний конфлікт: причини та наслідки для економіки та людського розвитку. Економіка і організація управління. 2023. С. 4-17.

13. Редзюк В., Редзюк Н. Сучасні проблеми інформаційної безпеки України та напрями їх вирішення. Публічне управління: концепції, парадигма, розвиток, удосконалення, 2023, 3. С. 59-65.

14. Глобальний трекер конфліктів. [Електронний ресурс]. Режим доступу: https://www.cfr.org/global-conflict-tracker

15. Пащенко О. Сучасні тренди розвитку міжнародного інвестування. Організаційно-економічні аспекти розвитку підприємницьких структур в Україні та світі: моногр. за заг. ред. д-ра екон. наук, проф. Т. Гринько. Дніпро : Видавець Біла К. О., 2022. С. 278-308.

16. Краєвська А. Тенденції та чинники управління конкурентоспроможністю бізнесу в сучасних умовах. Modeling the development of the economic systems, 2023, 2. С. 173-178.

17. Ariyani Anisa, Dwi Firmansyah. Determining factors of foreign direct investment in Emerging Market Asia: A panel data analysis (2005-2020). Optimum: Jurnal Ekonomi dan Pembangunan, 2023, 13.2. P. 195-206.

18. Kirkham Ksenia, Toplišek Alen. The Impact of Western Sanctions on Global Supply Chains and the Green Transition: The Case of EV Battery Manufacturing in South

Korea and the EU. In: The Routledge Handbook of the Political Economy of Sanctions. Routledge. P. 234-248.

19. Дергачова В. В., Голюк В. Я. Тренди та моделі розвитку світової економіки. Конспект лекцій. 2022. 151 с.

20. Cisco Comp. Digital Vortex: how digital disruptions is redefining industries. June 2015. URL: http://surl.li/eqrtod.

21. Europol Internet organized crime threat assessment (IOCTA) 2023. Publications Office of the European Union, Luxembourg. URL: http://surl.li/qhsutt.

22. Eurostat Security policy: measures, risks and staff awareness by size class of enterprise URL: http://surl.li/hgqfwu.

23. Гринкевич С., Когут М., Станкевич М. Еволюція теоретичних концепцій економічної безпеки підприємства. Економіка та суспільство. 2023. № 50. https://doi.org/10.32782/2524-0072/2023-50-70 261

24. Кравченко М., Немировський Ф. Теоретичні підходи до визначення поняття «економічна безпека підприємства». Наукові інновації та передові технології. 2024. № 11(39). С. 932-943.

25. Адаменко Т. М. Система економічної безпеки підприємства: підхід до формування. Економіка Менеджмент Підприємництво. 2013. № 25(II). С. 265- 273. URL: http://eme.ucoz.ua/publ/zbirniki/25_ii_2013/adamenko_t_m_/39-1-0-333

26. Міщенко В. І. Механізми регулювання процесів цифровізації для забезпечення національно укоріненої стійкості економічного розвитку. Економічний простір. 2024. № 189. С. 283-290.

27. Schwertner K. Digital transformation of business. Trakia Journal of Sciences, 2017. Vol. 15. Suppl. 1. pp. 388-393.

28. Siemens. Vision 2020+: Shaping the future Siemens. Press Conference. Munich, 2 August, 2018. URL: http://surl.li/vwiqua

29. Digital Adoption Top 5 digital transformation risks. 31.05.2024. URL: https://www.digital-adoption.com/digital-transformation-risks/

30. McKinsey&Company. Digital risk: transforming risk management for the 2020s. URL: http://surl.li/jkwfpa.

31. Statista, «Cyber incidents targeting governments global by attack vector 2023», [Online], available at: https://www.statista.com/statistics/1428581/government-worldwide-targeted-cyber-incidents-by-attack-vector/

32. «Vsesvitnii ohliad ekonomichnykh zlochyniv», [Online], available at: https://www.pwc.com/ua/uk/Україна

33. eSentire, «Cybercrime to Cost the World $9.5 Trillion USD Annually In 2024», [Online], available at: https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in 2024?utm_medium=email& utm_source=pardot&utm_campaign=autoresponder

34. Council of the EU, «Cybersecurity package: Council adopts new laws to strengthen cybersecurity capacities in the EU», [Online], available at: https://www.consilium.europa.eu/en/press/press-releases/2024/12/02/cybersecuritypackage-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/

35. European Commission, «Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres», [Online], available at: https://digitalstrategy.ec.europa.eu/en/news/cybersecurity-eu-launches-first-phase-deployment-european-infrastructure-cross-bordersecurity

36. Baranov, O.A. (2014), «Pro tlumachennia ta vyznachenni poniattia «kiberbezpeka»», Pravova informatyka, No. 2 (42), pp. 54–62.

37. ITU DataHub, «The worldâs richest source of ICT statistics and regulatory information», [Online], available at: https://datahub.itu.int/dashboards/idi/?y=2024&e=UKR

38. Belskii, Yu. (2014), «Shchodo vyznachennia poniattia kiberzlochynu», Yurydychnyyi visnyk, Vol. 2014/6, pp. 414–418.

39. ITU Publication, «Global Cybersecurity Index 2024», [Online], available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

40. European Commission, «LAB – FAB – APP», [Online], available at: https://data.europa.eu/doi/10.2777/477357

41. StatPlanet, «EC-OECD STIP Compass», [Online], available at: https://stip.oecd.org/stats/SBStatTrends.html?i=TOP10_X&v= 3&t=2006,2020&s=UKR

42. European Commission, «The Digital Markets Act», [Online], available at: https://digital-marketsact.ec.europa.eu/index_en

43. European Commission, «The Digital Services Act», [Online], available at: https://commission.europa.eu/strategyand-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

44. European Commission, «The EU Cyber Solidarity Act», [Online], available at: https://digitalstrategy.ec.europa.eu/en/policies/cyber-solidarity

45. State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force. War and Cyber: Three Years of Struggle and Lessons for Global Security. Analytical report. Kyiv, 2025. 21 p. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=69131.

46. Покришка Д. С. Технологічна конкурентоспроможність національної економіки як чинник економічної безпеки України: дис. … канд. екон. наук : 21.04.01. Київ, 2021. 303 с. URL: https://niss.gov.ua/sites/default/files/2021-04/pokryshka_dissertation.pdf

47. NCSI :: Methodology. Index. URL: https://ncsi.ega.ee/methodology/.

48. Mynenko S., Kochnieva V., Babych Y. ОЦІНКА РІВНЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ. Європейський науковий журнал Економічних та

Фінансових інновацій. 2024. Т. 2, № 14. С. 487–500. URL: https://doi.org/10.32750/2024-0243

49. Державна служба спеціального зв’язку та захисту інформації України. Офіційний сайт. URL: https://cip.gov.ua/ua/news/

50. Рада національної безпеки і оборони України. Офіційний сайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/3303.html

51. Sinha A. Safeguarding India's Digital Frontier: Unveiling Ransomware Challenges and Cybersecurity Strategies. Microsoft. URL: https://www.msn.com/en-in/money/news/safeguarding-indias-digital-frontier-unveilingransomware-challenges-and-cybersecurity-strategies

52. Newson, Robert A. Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There? URL: https://smallwarsjournal.com/blog/counter-unconventional-warfare-isthe-way-of-the-future-how-can-we-get-there

53. Security Strategy for Society. URL: https://turvallisuuskomitea.-fi/en/security-strategyfor-society

54. Coats D. R. Worldwide Threat Assessment of the US Intelligence Community. Washington, DC, USA. 2017.

55. Buzan People, States and Fear. People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era, Ed. Cartier, Chişinău, Central Bank of Latvia annual report of 2013 URL: http://www.lb.lt/lithuanian_economic_review_may_2014

56. Костицький В.В. Інформаційна війна проти України – виклик світовому порядку. URL: http://oksamyt.org/2015/02/02/0202201511

57. Стратегія економічної безпеки України на період до 2025 року : Указ президента України від 11.08.2024 № 347/2021. URL: https://ips.ligazakon.net/ document/MUS35837

58. D. Beder, Y. Tsal-Tsalko, Formation of economic indicators of national security in the context of business digitalization and economic changes, Society and Security 1 (2024) 3–13. doi:10.26642/ sas-2024-1(2)-3-13.

59. Polozova T., Stepanenko S., Murzabulatova O., Ponomarov S. Specific of the creation and functioning of the financial and economic security system of business entities. Український журнал прикладної економіки та техніки. 2023. Том. 8. № 3. С. 70-77

60. IMF. World Economic Outlook Database. Washington, D.C.: International Monetary Fund, 2024. European Commission. Ukraine: Economic Review 2024. Brussels: EC, 2024.

61. Yuan, Guanghui, Fei Xie, and Huiling Tan. 2022. Construction of Economic Security Early Warning System Based on Cloud Computing and Data Mining. Computational Intelligence and Neuroscience 22: 2080840.

62. Blanchard, O. (2020). Public debt and low interest rates. IMF Economic Review, 68(1), 1-17. https://doi.org/10.1057/s41308-019-00108-0

63. Ліщинський, І., & Лизун, М. (2020). Концептуальні візії регіональної та глобальної безпеки. Вісник Економіки, (2), 148-161.

64. World Bank - база даних World Development Indicators (WDI): https://data.worldbank.org

ЗГОДА здобувачки освіти Державного університету економіки і технологій про перевірку кваліфікаційної роботи на прояви академічного плагіату та розміщення в Репозитарії ДУЕТ

Я, **Гребенюк Анастасія Дмитрівна**, підтримую політику Державного університету економіки і технологій з академічної доброчесності і відкритого доступу. Стверджую, що кваліфікаційна бакалаврська робота «**Економічна безпека міжнародного бізнесу в умовах кіберзагроз та геополітичної нестабільності»** виконана самостійно та не містить академічного плагіату. Я не надавала і не одержувала недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають покликання на відповідне джерело.

Із чинним Положенням про запобігання та виявлення академічного плагіату в роботах здобувачів вищої освіти Державного університету економіки і технологій ознайомлена. Чітко усвідомлюю, що в разі виявлення у кваліфікаційній роботі порушення норм академічної доброчесності робота не допускається до захисту або оцінюється незадовільно.

Також я поінформована, що відповідно до пункту 5.8 «Положення про Репозитарій (електронну базу даних) Державного університету економіки і технологій» згадана робота буде розміщена в Електронному архіві Університету (Репозитарії ДУЕТ) та ознайомлена з умовами такого розміщення.

08.06.2026 **А. ГРЕБЕНЮК**