МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В. Н. КАРАЗІНА

Економічний факультет
Кафедра міжнародної економіки та світового господарства

Реєстр №_____ «До захисту»

Нормоконтролер В.о. завідувача кафедри
к. е. н., доц. Шуба Т. П.

_____ _____

ЦИФРОВІ РИЗИКИ В МІЖНАРОДНОМУ БІЗНЕСІ

Кваліфікаційна робота бакалавра

Виконав:
студент 4-го курсу
першого (бакалаврського) рівня
вищої освіти
денної форми навчання
гр. ЕМ-42 Павло ТРОЯКОВ

Науковий керівник :
к. е. н., доцент Наталія ДУНА

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У XXI столітті міжнародний бізнес став невід'ємною частиною сучасної цивілізації та ключовим чинником світової економіки, відіграючи важливу роль у формуванні глобальних ринків, технологічного розвитку та взаємозалежності між країнами.Стрімкий розвиток технологій спричинив масштабну трансформацію в міжнародному бізнесі. Сучасний міжнародний бізнес все більше залежить від цифрових технологій, які забезпечують швидкий доступ до інформації, автоматизацію процесів та глобальну комунікацію. Однією з головних тенденцій сучасної економіки є цифровізація міжнародного бізнесу. Вона сприяє підвищенню ефективності, зміцненню конкурентоспроможності та розвитку інноваційного потенціалу компаній, забезпечуючи швидкий обмін даними, автоматизацію процесів і глобальну інтеграцію ринків.

Впровадження цифрових технологій у різних країнах відбувається по-різному, що зумовлено рівнем економічного розвитку, ступенем державної підтримки та доступністю сучасних технологій. Ці фактори впливають на темпи цифрової трансформації бізнесу, створюючи як нові можливості, так і специфічні виклики для компаній у глобальному середовищі.Цифровізація бізнес-процесів дозволяє значно оптимізувати використання як матеріальних, так і нематеріальних ресурсів. Сучасні IT-технології відкривають підприємствам нові можливості для успішного розвитку на міжнародних ринках.

Нині цифрові технології дають змогу суб'єктам господарювання автоматизувати як простіші, так і складніші процеси, усуваючи непотрібні проміжні етапи.

Це сприяє підвищенню гнучкості компаній, які можуть ефективніше розподіляти свої ресурси та скорочувати витрати. В умовах сучасного конкурентного середовища використання цифрових технологій перетворюється на необхідність, оскільки воно дозволяє значно заощаджувати час та знижувати

операційні витрати. Цифрова трансформація вже не просто концепція, а ключовий фактор стратегічного розвитку сучасного бізнесу. Вона формує конкурентні переваги компаній, удосконалює бізнес-процеси та створює нові можливості для зростання в умовах глобальної цифрової економіки.

Завдяки цифровізації вдосконалюються бізнес-процеси та організаційна культура, що дозволяє компаніям підвищувати ефективність, впроваджувати інновації та залишатися конкурентоспроможними. Проте необхідно й зазначити, що цифрова трансформація супроводжується і низкою викликів. Вона вимагає певних змін в організаційній культурі, навчання співробітників новим технологіям, гарантування конфіденційності даних, вирішення проблем соціальних нерівностей, врахування змін на ринку праці та управління кібербезпекою, що потребує значних ресурсів і уваги. Тобто під цифровою трансформацією мається на увазі не лише інтеграція технологій, але й кардинальна зміна підходів до ведення бізнесу та способів мислення. Впровадження цифрових технологій забезпечує компаніям підвищення ефективності, інноваційності та адаптивності, що є ключовими для конкурентного успіху в глобальному середовищі.Однак, щоб визначити конкретний вплив диджиталізації на міжнародний бізнес та оцінити його масштаб, необхідний ґрунтовний аналіз. Саме в цьому й полягає актуальність кваліфікаційної роботи.

Ступінь наукової вивченості.Теоретичні аспекти міжнародного бізнесу у контексті цифрової економіки висвітлено в роботах зарубіжних і вітчизняних науковців. Зокрема проблема цифровізації стала предметом вивчення у працях Е. Бріньолфссона та Е. Макафі[7; 63], К. Шваба [56], Т. Дейвенпорта [66] та ін. Згадані дослідники зробили істотний внесок у вивчення питань цифровізації бізнесу та створення стратегій для ефективної цифрової трансформації підприємств.

На роль цифровізації в економічному прогресізвертали увагу й українські науковці, зокрема Г. Карчева, Д. Огородня, В. Опенько [28]. Міжнародні стратегії економічного розвитку стали предметом досліджень таких науковців,

як В. Білоцерківець, О. Завгородня, В. Лебедєва [4]. Виклики та загрози, що виникають у міжнародному бізнесі В. Вергун, В. Карп[11].Аналіз наукових джерел показав, що розвиток міжнародного бізнесу в умовах цифровізації є важливою проблемою, що потребує вирішення. Оскільки цифровізаціянесе з собою значні ризики, які можуть вплинути на стабільність і ефективність підприємств, виникає необхідність розробки ефективних стратегій ризик-менеджменту, щоб мінімізувати потенційні негативні наслідки.

Мета дослідження полягає у визначенні основних цифрових ризиків, що виникають у міжнародному бізнесі, та оцінці їх впливу на бізнес.

Об'єктом дослідження виступають процеси розвитку міжнародного бізнесу в умовах цифровізації.

Предмет дослідження - цифрові ризики у міжнародному бізнесі та їхній вплив на діяльність підприємств.

Для досягнення поставленої мети у роботі було визначено та вирішено такі **завдання**:

- визначити природу та сутність цифрових ризиків;
- дослідити види цифрових ризиків;
- систематизувати методи та інструменти оцінки цифрових ризиків;
- розкрити ідентифікацію та оцінку цифрових ризиків в міжнародному бізнесі;
- проаналізувати вплив цифрових ризиків на розвиток міжнародного бізнесу;
- визначити сучасні стратегії управління цифровими ризиками в міжнародних компаніях.

Для досягнення мети роботи використано низку специфічних та загально-наукових **методів:**

- аналіз і синтез – використані для розкриття сутності цифрових ризиків та визначення їхніх характеристик у міжнародному бізнесі;

- порівняльний аналіз – застосовано для зіставлення впливу цифрових ризиків у різних країнах і регіонах;
- метод узагальнення та систематизації –використаний для класифікації та структурування основних видів цифрових ризиків;
- статистичний метод – використаний для обробки кількісних даних щодо проявів цифрових ризиків та їхніх наслідків;
- економіко-статистичні методи –застосовані для аналізу тенденцій і динаміки цифрових ризиків у контексті міжнародного бізнесу.

Апробація. Результати досліджень за тематикою кваліфікаційної роботи були оприлюднені в тезах «Цифрові ризики в міжнародному бізнесі: види та наслідки» на VIII Всеукраїнській науково-практичній конференції «Сучасні перетворення міжнародного бізнесу» (м. Харків, 22.04.2025).

Структура роботи. Робота складається зі вступу, двох основних розділів, висновків до кожного розділу, загальних висновків, списку використаних джерел та додатків. Кваліфікаційна робота містить 4 таблиць, 14 рисунків. Загальний обсяг роботи 68 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СУТНОСТІ ЦИФРОВИХ РИЗИКІВ

1.1. Природа та сутність цифрових ризиків

Одним з основних факторів економічного розвитку сучасного світу є міжнародний бізнес. Він є важливим інструментом глобалізації, оскільки дозволяє компаніям виходити на міжнародні ринки, оскільки міжнародний бізнес це встановлення і розвиток стійких, довгострокових виробничих, науково-технічних, фінансових та комерційних зв’язків між підприємствами різних країн.

З розвитком технологій та інтеграцією цифрових рішень, міжнародний бізнес стає ще більш динамічним і ефективним. Цей процес відображає перехід до цифрової економіки, яка базується на використанні цифрових технологій для покращення бізнес-процесів, зменшення витрат, забезпечення глобальної комунікації та оптимізації ланцюгів постачання. Цифрова економіка відіграє ключову роль у розвитку країн в умовах глобалізації та формування інформаційного суспільства. Вона є основою для створення нових можливостей у багатьох сферах, включаючи бізнес, освіту, охорону здоров’я та управління. Тому вбачаємо необхідність визначити дане поняття.

Під цифровою економікою (англ. Digital economy) в науковій літературі розуміють глобальну мережу економічних і соціальних подій, які здійснюються через такі платформи, як Інтернет, а також мобільні та сенсорні мережі. Це економічна модель, що базується на перевагах доступу до Інтернету, зокрема на підвищенні ефективності праці, зміцненні конкурентних позицій підприємств і зниженні виробничих витрат. В умовах цифрової економіки можливості задоволення людських потреб значно розширюються. Її ефективне функціонування ґрунтується на трьох ключових елементах: інфраструктурі (доступ до Інтернету, програмне забезпечення, телекомунікації), електронному

бізнесі (ведення підприємницької діяльності через цифрові мережі) та електронній комерції (розповсюдження товарів і послуг онлайн) [39, с. 22].

Термін «цифрова економіка» вперше з'явився у 1994 році з публікацією відомої книги канадського економіста та бізнес-консультанта Д. Тапскотта «Digital Economy» [72]. У 1995 році цей термін набув ширшого вжитку й вийшов за межі суто наукового середовища завдяки американському інформатику з Массачусетського університету Н. Негропонте. Він сформулював ідеологію цифрової економіки як «перехід від обробки атомів, що є складовою фізичних речовин, до обробки бітів, які становлять матерію програмних кодів»[69].

Цифрова економіка, її модельна складова, розглядається як віртуальне середовище, яке дедалі більше органічно доповнює фізичну реальність та інтегрується з нею. У цифровій економіці трансформація бізнес-процесів відбувається в режимі реального часу завдяки розвиненим інформаційним системам, які забезпечують швидкий обмін, обробку та аналіз даних. У такому середовищі головним активом стає зміст – інформація та вміння ефективно з нею працювати у всіх економічних процесах. Якість та цілісність даних набувають вирішального значення, що робить їх захист стратегічним пріоритетом.

Проте саме це створює підґрунтя для нових цифрових ризиків. Глобальним викликом цифрової економіки стає ризик пошкодження або втрати даних, що може мати катастрофічні наслідки як для окремих компаній, так і для цілих економічних систем. Такі загрози ускладнюються зростанням обсягів оброблюваної інформації та залежністю критичних інфраструктур від цифрових технологій.

Таким чином, природа цифрових ризиків полягає в постійному технологічному оновленні, що створює нестабільність і вразливість цифрових середовищ до нових форм загроз – від кібератак до технічних збоїв і людських помилок.

У традиційній економічній моделі основний акцент робиться на підвищенні ефективності виробничих і бізнес-процесів шляхом автоматизації, без кардинальної зміни їхньої структури. Натомість у цифровій економіці бізнес-процеси трансформуються в режимі реального часу завдяки розвиненим інформаційним системам.

Впровадження технологій цифрової економіки сприяє економічному розвитку та підвищенню ефективності роботи державних і суспільних інституцій. Водночас варто зазначити, що діджиталізація, окрім очевидних переваг та економічних дивідендів, у разі її безконтрольного впровадження та відсутності міжнародного консенсусу, здатна породжувати вагомі ризики та загрози. Зокрема, зростання питомої ваги цифрової компоненти у глобальній економіці та динамізація темпів зростання ВВП за рахунок цифрових технологій стали одними з ключових глобальних викликів сучасності. Прискорена діджиталізація супроводжується підвищенням вразливості до кіберзагроз, що підкреслює актуальність проблеми кібербезпеки.

При цьому слід звернути увагу на нерівномірність інформаційного висвітлення цифрових ризиків у різних країнах. Так, кібератаки в країнах із високим рівнем доходів зазвичай активно висвітлюються у засобах масової інформації, тоді як значна кількість атак у країнах з низькими та нижче середнього доходу залишається поза увагою. Це є особливо небезпечним, зважаючи на те, що саме ці країни демонструють найбільшу зацікавленість у забезпеченні ширшого доступу до фінансових послуг, що зумовлює стрімкий перехід до цифровізації фінансового сектору – зокрема, через впровадження мобільних платіжних систем.

Таким чином, цифрові ризики є невід’ємним супутником цифрової трансформації, охоплюючи як технічні, так і соціально-економічні аспекти, і мають різний рівень прояву залежно від економічного контексту країн.

Перш за все необхідно розуміти, що розуміють під «ризиком». У науковій літературі існує широкий спектр трактувань поняття «ризик». Проте, попри

різноманітність підходів, досі не вироблено єдиного універсального визначення цього терміна.

У сучасному контексті «ризик» означає будь-яку загрозу, пов'язану з непередбаченими витратами або зменшенням доходів, що не відповідають очікуванням компанії [27, с. 42].

Сам термін «ризик» має глибоке значення, що сформувалося на перетині різних культур і мов. У дослідженнях етимології цього поняття простежується паралель з ієрогліфічними знаками китайської та японської мов, підкреслюючи кореневу подібність між термінами ризик, нещастя та страхування. В українській мові слово «ризик» також відображає усвідомлення можливості небезпеки або втрати в умовах невизначеності [33, с. 171].

Сучасні теорії, зокрема неокласична теорія, визнають комплексний характер ризику, який включає як можливість отримання прибутку, так і особисте ставлення підприємця до ризику. Бізнес-ризики безпосередньо залежать від численних факторів, серед яких споживчі вподобання, попит, конкуренція та загальні економічні умови. У цьому контексті ефективне управління ризиками є важливим елементом для забезпечення успіху підприємства та стабільного розвитку в умовах змінного економічного середовища.

Можливо, в майбутньому з'явиться єдине універсальне визначення, але кіберризик, ймовірно, залишатиметься частиною більш широкого поняття цифрового ризику.

У процесі аналізу економічної літератури виокремлено кілька ключових підходів до тлумачення категорії «ризик»(див. рис. 1.1).

У рамках цифрової економіки доцільно використовувати термін «цифровий ризик». Зазвичай, коли йдеться про цифрові технології, вживається також термін «кіберризик».В професійних колах обидва ці поняття трактуються як синоніми, хоча на практиці вони позначають схожі, але не зовсім ідентичні явища.

Рис. 1.1 *–Ключові підходи до визначення сутності категорії «ризик»*

Джерело: [33, с. 175]

Кіберризик означає потенційні фінансові збитки та шкоду діловій репутації організації (підприємства), які виникають через дефекти або неполадки в її системі інформаційних технологій (IT-системі), викликані різноманітними факторами [13, с. 72].

Цифровий ризик полягає у процесах впровадження та використання цифрових технологій в діяльності компанії, зокрема в прийнятті рішень, що стосуються комп'ютеризації всіх етапів, застосування робототехніки та розширення аналітичних можливостей завдяки машинному навчанню і штучному інтелекту [66].

Цифровий ризик це не лише технологічна проблема, а й проблема самого бізнесу, що охоплює загальні проблеми бізнесу, тоді як кіберризик стосується лише інформаційних технологій (IT).

Цифровий ризик у контексті цифрової економіки є економічною категорією, яка відображає особливості сприйняття суб'єктами економічних відносин об'єктивної невизначеності та конфліктності, що виникають у процесах функціонування та управління компанією (організацією, підприємством тощо). Ці проблеми зумовлені можливими збоями в роботі цифрових технологій та інструментів, які застосовуються компанією. Об'єкт та суб'єкт цифрового ризику залишаються такими ж, як і для традиційного ризику, оскільки вони стосуються тих самих аспектів – підприємства, організації або окремих осіб, що зазнають впливу ризиків, пов'язаних з використанням цифрових технологій.

Основними джерелами цифрового ризику є самі цифрові технології, як поділяють на:

1) Пристрої та апаратне забезпечення. Апаратне забезпечення включає фізичні компоненти комп'ютерних систем, від серверів і робочих станцій до мережевих пристроїв. Збої або несправності в апаратному забезпеченні можуть призвести до значних фінансових втрат або тимчасових зупинок діяльності компанії.

2) Програмне забезпечення та інноваційні технології. Програмне забезпечення є критично важливою складовою цифрових технологій. Програмні системи, від операційних систем до специфічного бізнес-програмного забезпечення, можуть стати джерелом ризику, якщо вони мають вразливості або несправності, що можуть призвести до збою в роботі.

3) Мережі (локальні, глобальні, Інтернет). Мережі, включаючи локальні та глобальні, зокрема Інтернет, є важливим джерелом цифрового ризику. Порушення в роботі мереж або хакерські атаки можуть серйозно вплинути на безпеку даних і цілісність інформаційних систем.

4) Цифрові ризики може мати значний вплив на бізнес. Це можуть бути як фінансові втрати, так і негативні наслідки для репутації компанії. Наприклад, втрата даних або кібератака може не лише призвести до збитків, а й порушити довіру клієнтів до компанії. Важливо розуміти, що цифровий ризик –

це не лише технічна проблема, а й стратегічне питання для керівництва компанії, яке повинно бути готовим до таких загроз [13, с. 73].

Природа цифрових ризиків полягає в тому, що вони є наслідком стрімкого розвитку технологій та постійних змін у способах використання цифрових інструментів. Така динаміка створює ситуацію, коли темпи впровадження цифрових рішень значно випереджають здатність суспільства, бізнесу та держави адекватно реагувати на нові виклики. У результаті цифровізація, незважаючи на свою позитивну роль у модернізації економіки та підвищенні якості життя, несе низку потенційних ризиків. Серед найбільш значущих варто виокремити [53, с. 757]:

- несанкціонований доступ до інформації та інші загрози кібербезпеці, що підривають довіру до цифрових систем;
- масове безробіття, спричинене автоматизацією процесів і витісненням традиційних професій;
- цифрову нерівність – зростаючі соціальні та економічні розриви в рівні цифрової освіти та можливостях доступу до цифрових послуг між різними верствами населення, бізнесами, а також між окремими країнами.

Таким чином, цифрові ризики є багатовимірними й охоплюють як технологічну, так і соціально-економічну площини, що потребує системного та глобально узгодженого підходу до їхнього управління.

Цифровий ризик не може існувати без матеріальних елементів, оскільки він містить інформацію та є віртуальним за своєю природою. Це означає, що цифрові ризики виникають внаслідок обробки, зберігання та передачі даних у цифровому середовищі, при цьому вони можуть мати суттєві наслідки для фізичних і віртуальних систем, на яких базуються ці дані.

Транскордонний характер цифровізації та відкритість суб’єктів господарювання суттєво впливають на рівень економічної безпеки. Інтеграція у глобальні цифрові мережі забезпечує доступ до нових ринків і технологій, але водночас підвищує ризики кіберзагроз, витоку конфіденційної інформації та економічної нестабільності через зовнішні чинники. Вразливість національного

сегмента економіки до зовнішніх впливів потребує ефективних механізмів регулювання, розробки кіберстратегій та адаптації до швидких змін цифрового середовища.

Основними характеристиками цифрових ризиків є:

1) невизначеність та динамізм, що полягає в швидкій зміні цифрових технологій, і їхнє використання може створювати нові, часто непередбачувані ризики. Технології, які здаються безпечними на момент впровадження, можуть з часом стати вразливими до нових видів атак або збоїв.

2) технічні та системні складнощі. Це може бути пов’язано з помилками в програмному забезпеченні, проблемами з апаратним забезпеченням, а також із недоліками в розробці та інтеграції систем. Технічні збої можуть призвести до серйозних наслідків для організацій, таких як втрата даних, порушення операцій або зупинка виробничих процесів.

3) безпека та конфіденційність. У будь-якому бізнесі існують вразливі точки в інформаційних системах, якими можуть скористатися нападники для здійснення кібератак, таких як крадіжка або знищення важливих даних, порушення конфіденційності персональних даних, а також відмова в доступі до даних чи ресурсів (DDoS-атаки). Захист інформаційної безпеки є важливою складовою управління цифровими ризиками.

4) залежність від сторонніх постачальників. Сучасні компанії активно використовують зовнішні платформи, хмарні сервіси та інші інструменти сторонніх постачальників для зберігання даних або обробки інформації. Однак така залежність може створювати нові ризики. Порушення роботи сервісу чи збої у роботі постачальників можуть вплинути на функціонування бізнесу.

5) незавершеність та уразливість інновацій. Інноваційні технології, такі як штучний інтелект, блокчейн, робототехніка або великі дані (BigData), активно впроваджуються в бізнесі,але водночас залишаються недосконалими та потенційно вразливими до зовнішніх загроз. Незавершеність цих технологій пов’язана з їхньою швидкою еволюцією, тестуванням у реальних умовах і

постійними оновленнями, що можуть містити недоопрацьовані аспекти безпеки [17, с. 54].

У сучасних умовах цифровізаціїкіберризики залишаються однією з найбільш недооцінених загроз для бізнесу, державних структур та суспільства загалом. Нині вони здатні привести до значних наслідків для міжнародного бізнесу. Через транскордонний характер цифровізації, взаємопов'язаність ринків і залежність від інформаційних технологій, ризики, пов'язані з цифровізацією, можуть впливати не лише на окремі компанії, а й на цілі економічні системи.

Серед основних наслідків цифрових ризиків для міжнародного бізнесу можемо назвати:

1) припинення або уповільнення бізнес-процесів;
2) втрата конкурентної переваги;
3) збиток для бренду та втрата репутації;
4) судові розгляди та позови;
5) втрата клієнтів та прибутку;
6) додаткові витрати на усунення наслідків, штрафи і санкції регулюючих органів;
7) зниження вартості бізнесу [12, с. 113].

Цифрові ризики мають глобальний характер і можуть сильно вплинути на міжнародний бізнес. Компанії повинні інтегрувати ефективні стратегії кібербезпеки, зокрема для захисту своїх інформаційних технологій і бізнес-процесів, щоб мінімізувати наслідки цих ризиків і зберегти свою конкурентоспроможність на міжнародному ринку.

Протидія цифровим ризикам потребує узгоджених та скоординованих дій з боку організацій, що мають спільну зацікавленість у зменшенні загроз, пов'язаних із кібербезпекою та цифровим регулюванням. Спільна взаємодія дозволяє сформувати цілісну систему реагування на виклики цифрового середовища. Основні принципи управління ризиками окреслено в міжнародних стандартах, розроблених Міжнародною організацією зі стандартизації (ISO),

зокрема в стандартах, що регламентують підходи до загального управління ризиками, інформаційної безпеки та кіберзахисту.

Таким чином,цифрові ризики можуть бути спричинені як внутрішніми, так і зовнішніми факторами. Внутрішні фактори включають технічні збої, недосконаліть внутрішніх процесів або людські помилки. Зовнішні фактори – це атаки з боку хакерів, зміни в нормативно-правовому регулюванні або природні катастрофи, які можуть порушити роботу цифрових інфраструктур.

Отже, цифрові ризики є невід'ємною частиною сучасного міжнародного бізнесу, і їх усунення або мінімізація є необхідними для забезпечення безпеки та стабільності компаній. Кіберзагрози, проблеми з конфіденційністю, збої в технологіях і юридичні труднощі можуть призвести до значних фінансових і репутаційних втрат. Тому важливо, щоб компанії активно управляли цифровими ризиками, використовуючи сучасні інструменти та стратегії захисту для збереження конкурентоспроможності та досягнення успіху на міжнародному ринку.

1.2. Види цифрових ризиків

Цифрові ризики можуть бути класифіковані за різними ознаками, зокрема за їх джерелом, видом загрози та потенційними наслідками.

І. Віннікова та С. Марчук, спираючись на результати наукових і практичних досліджень, у контексті кіберризиків, здійснили класифікацію основних ризиків відповідно до визначених критеріїв[12, с. 112]:

1) втрата або крадіжка носіїв інформації та мобільних пристроїв;
2) несанкціонований доступ сторонніх осіб до конфіденційної інформації через вразливі хмарні сховища;
3) ненавмисне розголошення конфіденційної інформації співробітниками;
4) навмисні дії співробітників (інсайдерські загрози);
5) неконтрольоване копіювання даних працівниками.

На основі зазначених критеріїв розроблено узагальнену класифікацію кіберризиків, яка представлена на Рис. 1.2.

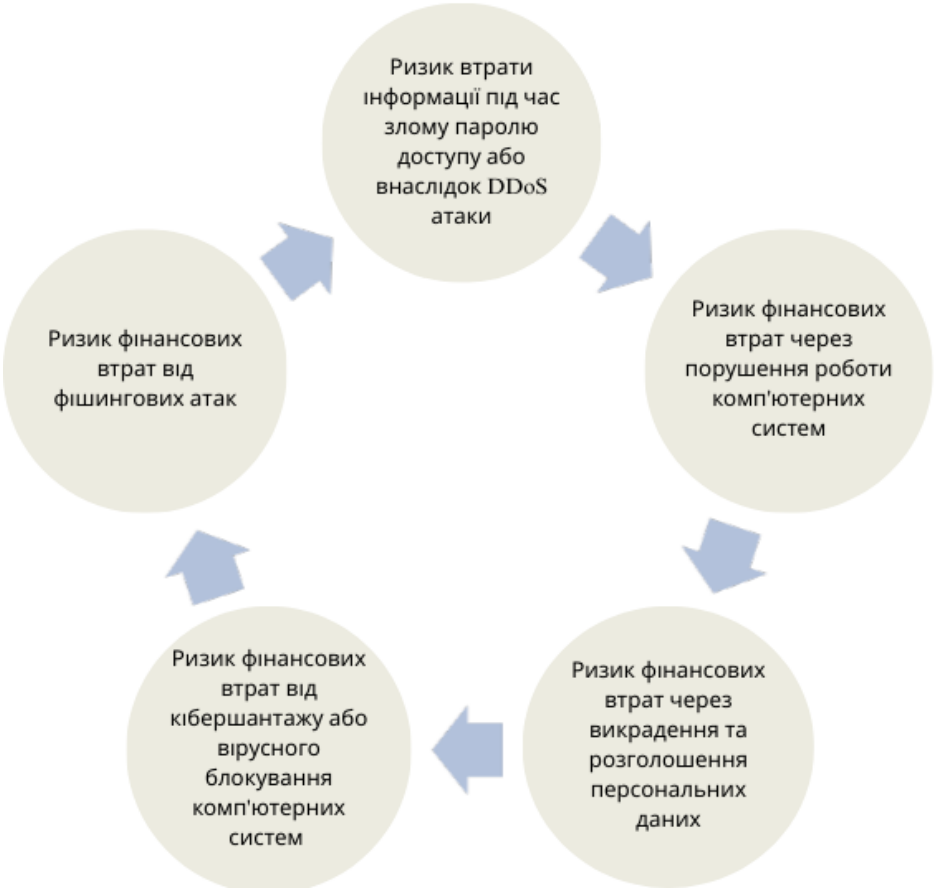

Рис. 1.2 *– Класифікація кіберризиків*

Джерело: [12, с.112].

Дослідження цифрової економіки значною мірою зосереджується на аналізі потенційних ризиків, що виникають у процесі впровадження цифрових технологій в міжнародному бізнесі. Зокрема, І. Шевчук, Б. Депутат, О. Тарасенко виділяють такі ризики:

1. Ризики, пов’язані із використанням Інтернету речей: вразливість пристроїв до кібератак, недостатній рівень безпеки підключених систем, можливість несанкціонованого доступу до даних.

2. Ризики використання технології блокчейн: потенційні вразливості в самій системі блокчейна та інфраструктурі, що базується на ній; неможливість виправлення помилково введеної або некоректної інформації через незмінність записів у мережі; ймовірність використання токенів для відмивання коштів та фінансування терористичної діяльності.

3. Ризики застосування штучного інтелекту, роботизації та автоматизації: зростання рівня безробіття та соціальної напруженості через скорочення робочих місць, посилення соціального відчуження, загроза тотального контролю за населенням, можливі витоки комерційної таємниці та інших конфіденційних даних.

4. Ризики, пов'язані з використанням імпортної мікроелектроніки: значна частка програмного забезпечення, зокрема системного програмного забезпечення операційних систем та систем управління базами даних, а також комп'ютерної техніки, що використовується в багатьох країнах, зокрема в Україні, є імпортованою. Це створює ризики наявності спеціальних чіпів для шпигунства або інших.

5. Ризики, пов'язані із застосуванням хмарних і розподілених обчислень: залежність від стабільності телекомунікаційної інфраструктури, розмиття відповідальності за інформаційну безпеку через її розподіл між користувачами, організацією-власником хмарної платформи та Інтернет-провайдером, а також зниження рівня контролю над збереженням даних.

6. Ризики, пов'язані зі стійкістю роботи Інтернету: можливість перебоїв у роботі цифрових сервісів через атаки на глобальну інфраструктуру, технічні збої або централізований контроль доступу до мережі.

7. Ризики впливу на суспільну свідомість: розвиток технологій великих даних, розширення цифрового простору та досягнення у сфері когнітивних і поведінкових наук сприяють створенню ефективних механізмів для прихованого збору інформації та маніпуляції масовою поведінкою.

8. Ризики, пов'язані зі зростанням складності бізнес-моделей і браком кваліфікованих кадрів: необхідність адаптації до швидких змін у цифровій економіці, дефіцит фахівців у сфері інформаційних технологій, що може сповільнювати інноваційний розвиток компаній[58].

Н. Гражевська та А. Чигиринський, аналізуючи світовий досвід цифрової трансформації національних економік, виділяють такі ризики та загрози, що безпосередньо стосуються міжнародного бізнесу:

1. Поляризація кадрів за рівнем цифрових навичок: це збільшує ризик невідповідності професійних і освітніх знань вимогам сучасного ринку праці, що створює проблеми для компаній при підборі кваліфікованого персоналу з необхідними цифровими вміннями.

2. Поглиблення соціальної нерівності: через зменшення можливостей для формування середнього класу, обмеження соціальних ліфтів та зниження мобільності населення, що негативно позначається на соціальній структурі. Особливо важливими є процеси, пов'язані з утворенням нестабільної праці та зростанням трудової міграції, що може призвести до втрати трудового потенціалу в країні.

3. Соціально-психологічні проблеми: зростання нерівності за рівнем цифрових компетенцій серед населення призводить до погіршення трудових навичок та функціональних можливостей. Це може вплинути на зміну мотиваційних орієнтирів, створюючи бар'єри для ефективної адаптації до нових умов праці[17,с. 45].

Згідно з іншими дослідженнями О.Шишкіної, до цифрових ризиків у бізнесі можна віднести наступні:

1. Адміністративні ризики, до яких відносять невідповідність існуючого законодавства потребам нового технологічного середовища, відсутність єдиних стандартів, обмеження на закупівлю іноземного обладнання та програмного забезпечення в умовах відсутності вітчизняних аналогів.

2. Фінансові ризики: необхідність значних інвестицій для впровадження цифрових технологій, що може призвести до фінансової нестабільності або надмірних витрат на розвиток цифрової інфраструктури.

3. Інформаційні ризики: відсутність достовірної та актуальної інформації, що знижує рівень довіри до цифрових технологій і обмежує ефективність їх впровадження та використання в бізнес-процесах.

4. Операційні ризики: низький рівень готовності підприємств до адаптації до цифрових технологій, що зменшує ефективність трансформаційних процесів, а також необхідність підвищення цифрової грамотності працівників.

5. Кадрові ризики: дефіцит висококваліфікованих спеціалістів, що ускладнює впровадження та підтримку нових технологій на підприємствах.

6. Управлінські ризики: відсутність мотивації керівництва до впровадження та інтеграції цифрових технологій в стратегічні процеси компанії, що може призвести до затримок або навіть відмови від цифрових трансформацій [60, с. 134].

Таким чином, аналіз цифрових ризиків в контексті міжнародного бізнесу потребує виокремлення ризиків, що виникають як на макрорівні, так і на рівні підприємств у глобальному середовищі. На рис. 1.3. представлена система цифрових ризиків у бізнесі.

МАКРОРІВЕНЬ	МІКРОРІВЕНЬ
соціальні екологічні інформаційні інституційні управлінські інфраструктурні кадрові	управлінські інфраструктурні кадрові економічні

Рис. 1.3 *– Цифрові ризики у бізнесі*

Джерело: складено автором на основі [18, с. 35]

Таким чином,на макрорівні виділяють низку ризиків. Серед соціальних ризиків виділяють зростання безробіття внаслідок автоматизації, дефіцит IT-спеціалістів та необхідність їхньої постійної перекваліфікації, а також поглиблення соціально-економічної нерівності через нерівномірний доступ до цифрових технологій. Інфраструктурні ризики проявляються у вигляді цифрового розриву, спричиненого нерозвиненістю цифрової інфраструктури. Екологічні ризики пов’язані з підвищеним споживанням енергії та зростанням викидів парникових газів [36, с. 245]. Інформаційні ризики зумовлені низьким рівнем інформаційної безпеки, що проявляється у хакерських атаках, кіберзлочинності та поширенні дезінформації. Інституційні ризики виникають

через відсутність чіткого понятійного апарату цифрової економіки, проблеми з визначенням правового статусу учасників цифрового ринку та недостатнє нормативне регулювання. Економічні ризики є наслідком глобалізації економічних процесів і посилення конкуренції в умовах цифрової трансформації.

На макрорівні цифровізація економіки породжує низку важливих ризиків, які можуть впливати на загальний розвиток держави та бізнес-середовище. Технологічні ризики включають залежність від глобальних цифрових платформ та рішень провідних IT-компаній, збої в роботі технологічних систем і використання застарілих технологій, що можуть гальмувати розвиток. Кадрові ризики полягають у зростанні плинності кадрів, а також у недостатній підготовленості робочої сили до вимог цифрової трансформації, що зумовлює потребу в перепідготовці та підвищенні кваліфікації. Управлінські ризики включають стратегічні помилки в процесі цифровізації, зокрема, невідповідність традиційних бізнес-моделей новим умовам цифрової економіки. Інформаційні ризики пов’язані з низькою ефективністю використання інформаційних технологій, затримками у поширенні даних або їх недостатньою достовірністю, що може вплинути на прийняття правильних рішень [68, с. 153]. Фінансові ризики полягають у зростанні витрат на впровадження нових цифрових рішень, що потребує великих капіталовкладень і може негативно позначитися на фінансовій стабільності.

Однією з можливих схем класифікації є поділ на чотири основні категорії: причини (методи), актори, мотивації та наслідки. Це дозволяє систематизувати цифрові загрози за різними аспектами їх прояву та впливу.

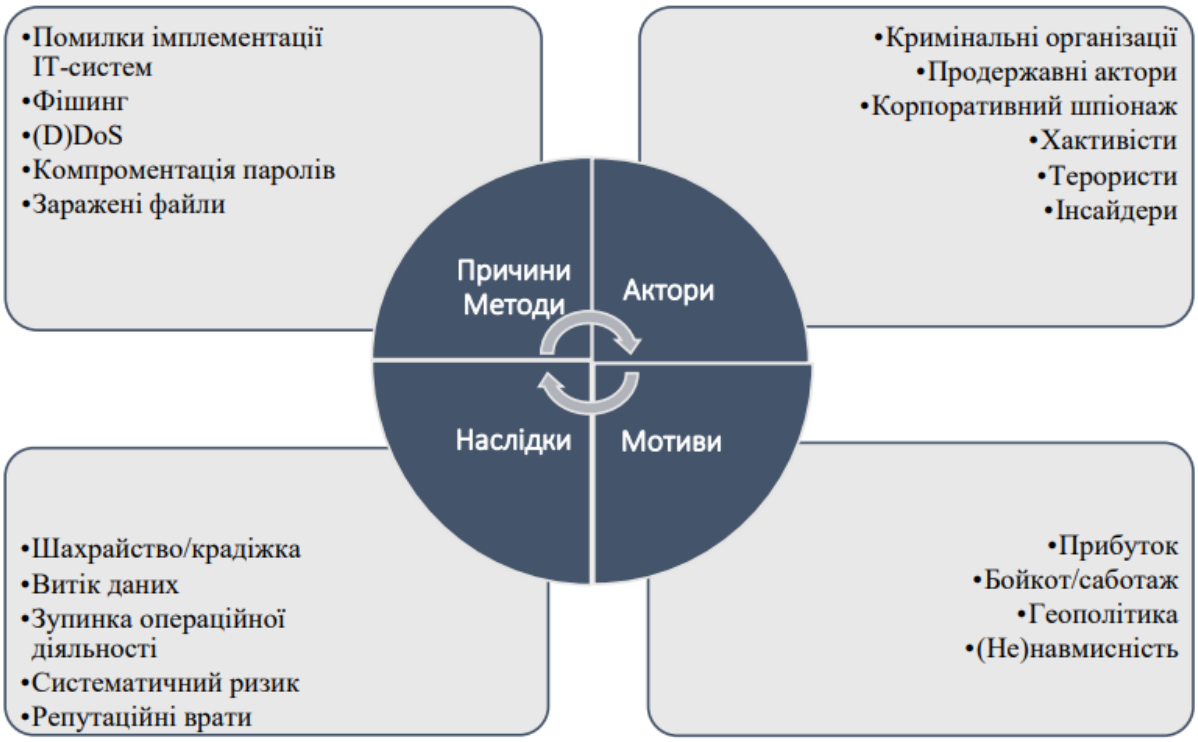

***Рис. 1.4**.–Сфери таксономічного поділу цифрових загроз*

Джерело: [33, с. 175].

Цей підхід до класифікації цифрових ризиків допомагає не лише зрозуміти їх структуру, а й визначити пріоритети для розробки стратегії захисту та управління ними.

Аналіз літературних та електронних джерел свідчить про різноманіття підходів до класифікації ризиків у сфері електронного бізнесу. Серед основних видів цифрових ризиків в бізнес-середовищі виділяють:

– Систематичні ризики – охоплюють загальні коливання ринку, які впливають на всі компанії в галузі. Прикладом є крах дотком-компаній у 2000–2001 роках, що продемонстрував важливість фінансової стійкості бізнес-моделей.
– Ризики мережевої безпеки – пов’язані з кіберзлочинністю, витоком персональних даних клієнтів, вірусами та хакерськими атаками. Вони потребують впровадження сучасних засобів кіберзахисту та відповідного правового забезпечення.

– Бізнес-ризики (ділові) – охоплюють проблеми, що виникають у процесі повсякденної діяльності підприємства: збої у ланцюгах постачання, управлінні запасами, витратами або персоналом. Особливо це актуально для електронного бізнесу, який залежить від ефективної логістики та зовнішніх партнерів [48].

Невід'ємною частиною міжнародного бізнесу через інтеграцію сучасних технологій у всі аспекти бізнес-процесів є ризики.У міжнародному бізнесі існує кілька видів цифрових ризиків, які можуть взаємодіяти між собою, що призводить до конфліктів. Зниження одного виду ризику може спричинити підвищення ступеня іншого. Тому важливим є розробка моделей та методів штучного інтелекту, які здатні адекватно моделювати ці взаємозв'язки та конфлікти, пов'язані з цифровими ризиками у міжнародному бізнесі. Це дозволяє обґрунтовано приймати раціональні рішення для ефективного управління ризиками, враховуючи їх взаємодію та динаміку в глобальному контексті.

Отже, існування різних видів цифрових ризиків зумовлене багатовимірністю цифрового середовища та постійною еволюцією технологій. Ці ризики можуть виникати як у технічній площині – у вигляді кіберзагроз, збоїв у роботі систем, втрати даних чи порушення доступу, так і в соціально-економічному вимірі – через цифрову нерівність, загрозу масового безробіття або неадекватне цифрове регулювання. Кожен з видів ризиків вимагає окремих підходів до ідентифікації, оцінювання та управління, що підкреслює важливість системного підходу до цифрової безпеки.

1.3. Методи та інструменти оцінки цифрових ризиків

Важливими елементами управління бізнесом є ідентифікація та оцінка ризиків, оскільки вони допомагають передбачити можливі загрози, уникнути раптових фінансових втрат і швидко адаптуватися до змін зовнішнього середовища.

Ключовим аспектом є вибір методу та інструментів управління ризиками. Важливо зазначити, що «метод» охоплює ширший зміст, ніж «інструмент», оскільки в рамках обраного методу можуть бути застосовані конкретні інструменти. Виділяють такі основні методи управління ризиками: усунення, запобігання та контроль, страхування та поглинання ризиків:

- скасування ризику – передбачає відмову від певної діяльності або її радикальну трансформацію, що призводить до повного усунення ризику;
- запобігання та контролювання ризику – полягає в ефективній організації проектної діяльності, коли учасники можуть впливати на чинники ризику та знижувати ймовірність несприятливих подій;
- контролювання ризику охоплює реалізацію заходів, спрямованих на мінімізацію збитків після настання небажаної події;
- страхування ризику включає зменшення збитків шляхом фінансової компенсації з страхових фондів. Поглинання ризику полягає в тому, що учасники діяльності самостійно несуть всі збитки, якщо ризик матеріалізується.

Для зменшення впливу ризику необхідно провести його аналіз, на основі якого здійснюється управління. Таким чином, процес управління ризиками починається з виявлення проблеми і завершується лише після отримання результату від вжитих заходів для її вирішення. Таким чином, потрібно поступово переходити від однієї вразливості до іншої або проводити аналіз ризиків паралельно (див. рис. 1.5) [27, с. 42].

Рис. 1.5 *– Етапи ризик-менеджменту*

Джерело: [27, с. 42].

Процес оцінки ризиків дозволяє власникам ризиків визначати основні загрози, встановлюючи пріоритети з урахуванням їхніх наслідків, ймовірності виникнення або інших заданих критеріїв. Відповідно до стандарту ISO/IEC 27005:2022, цей процес включає три основні етапи[13, с. 141]:

- Ідентифікація ризиків (riskidentification) – виявлення потенційних загроз, які можуть вплинути на діяльність організації, активів, вразливостей, наслідків.
- Аналіз ризиків (riskanalysis) – оцінка ймовірності та масштабів впливу кожного визначеного ризику.Цей процес спрямований на аналіз причин та потенційних джерел ризику, а також на оцінку ймовірності виникнення події, яка може призвести до негативних наслідків.
- Оцінка ризиків (riskevaluation) – порівняння отриманих результатів аналізу з прийнятними рівнями ризику для прийняття управлінських рішень. На цьому етапі визначається рівень ризиків, їхню значущість і пріоритетність, що дозволяє ефективно спрямувати подальші зусилля на їхнє управління та обробку.

Цей процес є основою для розробки стратегій з управління ризиками, що сприяють мінімізації негативних наслідків для організацій.Це дає можливість не лише мінімізувати негативні наслідки, а й забезпечити ефективне реагування на потенційні загрози, покращити безпеку та стійкість організації в умовах цифрової трансформації. Схему процесу оцінки ризиків представлено на рис. 1.6

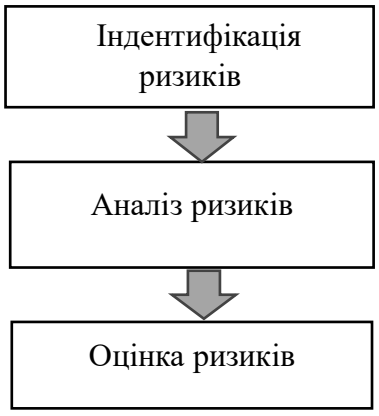

Рис. 1.6 *– Схема оцінки ризиків*

Джерело: [13, с. 42].

У цьому контексті ризик розглядається як можливі негативні наслідки. Лише в рідкісних випадках компанія, яка бере на себе ризик, може отримати значний прибуток. Для зниження впливу ризику необхідно провести його аналіз, на основі якого і реалізуються відповідні заходи.

Аналіз цифрових ризиків можна здійснювати наступнимчином[44, с. 177]:

1) Кількісна оцінка ризику–передбачає використання числових показників для вимірювання ризику.Для кількісної оцінки рівня ризику RRR, за умови, що всі фактори мають числове вираження, застосовується така формула:

$R=I\times E$

де:I – ймовірність настання небажаної події;

E – величина впливу (збитків, які може спричинити ризик).

Цей показник дозволяє оцінити фінансовий або інший вимірюваний вплив порушень безпеки, що допомагає організаціям визначати рівень загрози та необхідність запровадження заходів управління ризиками.

2)Якісна оцінка ризику – це метод аналізу, який використовує описові або категорійні значення для оцінки рівня ризику без застосування точних числових показників. Вона базується на експертних оцінках, класифікації та ранжуванні ризиків за певними критеріями.Якісна оцінка ризику визначає відносний рівень загроз, а не їхнє абсолютне значення, що спрощує аналіз і дає орієнтовну оцінку ризиків. Вона зазвичай достатня для виявлення найбільш значущих загроз, встановлення пріоритетів у витратах на безпеку та забезпечення керівництва впевненістю в тому, що ключові ризики враховані та пом’якшені. Такий підхід дозволяє ухвалювати ефективні управлінські рішення без складного математичного моделювання.

3) Комбінований підхід поєднує елементи обох методів, дозволяючи спочатку здійснити загальну якісну оцінку ризиків, а потім для найбільш критичних загроз застосувати кількісний аналіз. Це забезпечує баланс між швидкістю оцінки та точністю прогнозування.

Різні методи оцінки ризиків використовують різні інструменти, починаючи від простих опитувальників для фахівців організації до

спеціалізованого програмного забезпечення для автоматизованого розрахунку рівня ризиків. Оскільки застосування цих інструментів може передбачати додаткові витрати, важливо вибрати методологію, яка найбільше відповідає потребам організації. Оптимальним підходом є порівняння різних методів за об'єктивними критеріями для прийняття обґрунтованого рішення [70].

У роботах, що пов'язані з порівнянням методів оцінки ризиків, часто можна спостерігати неоднозначність у визначенні критеріїв, оскільки вони можуть змінюватися з часом, а також відсутність єдиного підходу щодо набору критеріїв порівняння. Аналіз джерел показав, що найбільш часто використовуваними ключовими критеріями при порівнянні методів оцінки кіберризиків є такі:

- ціна – витрати на застосування методу, сюди належать витрати на підтримку, програмне забезпечення чи інструменти, документацію та інші джерела, що пов'язані з використаним методом;
- відповідність міжнародним стандартам – відповідність методів міжнародним нормам та рекомендаціям, дотримання вимог стандартів з інформаційної безпеки, нормативних актів та інших методик, що забезпечує високий рівень впевненості в отриманих результатах методу;
- повнота – наскільки детально метод охоплює всі можливі ризики. Такий підхід гарантує консистентність і об'єктивність під час оцінки ризиків, забезпечуючи більш точні та надійні результати;
- валідність – оцінює, наскільки метод здатний точно і надійно виявляти та оцінювати ризики, а також чи використовує він об'єктивні й достовірні дані та підходи;
- відповідність цільовій організації – адаптованість методу до специфіки діяльності організації. Простішими методами можуть скористатися більш широкі кола користувачів, при цьому вони характеризуються більшою швидкістю впровадження;
- практичність – зручність і ефективність застосування методу на практиці;

– адаптивність – здатність методу адаптуватися до змін у зовнішньому та внутрішньому середовищі організації[39, с. 177].

Сьогодні існує безліч методів, що використовуються для оцінки та управління ризиками, особливо в умовах багатокритеріальності. До найпоширеніших належать такі:

1) AHP (Метод аналізу ієрархій) – дозволяє приймати рішення через побудову ієрархії критеріїв для порівняння альтернатив.
2) MULTIMOORA (Multi-Objective Optimization by Ratio Analysis)– комбінує кілька методів для визначення найбільш оптимального рішення.Він включає аналіз відношень, методи обчислення відносної переваги та оптимізацію з урахуванням різних критеріїв.
3) MAUT (Метод багатокритеріальної оцінки корисності)(Multi-Attribute Utility Theory) – застосовує функцію корисності для оцінки та вибору альтернатив.У цьому методі кожен критерій перетворюється на числову функцію корисності, що відображає перевагу або корисність певної альтернативи.
4) Метод зваженої суми – простий метод, де альтернативи оцінюються на основі зважених значень критеріїв.
5) TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) – метод, що вибирає найбільш ідеальну альтернативу на основі її подібності до ідеального рішення.
6) COPRAS(Complex Proportional Assessment) – метод, який порівнює альтернативи та оцінює їх за допомогою пропорційних показників.
7) PROMETHEE (Preference Ranking Organization METHod for Enrichment Evaluations)– метод, який допомагає визначити порядок альтернатив, враховуючи їх переваги по кожному з критеріїв.
8) ELECTRE (Elimination Et Choice Translating Reality)– сімейство методів для оцінки альтернатив на основі їх переваг і порівнянь.Вони дозволяють здійснити порівняння альтернатив через множину критеріїв і визначити їх відносну важливість[45, с. 172].

Ці методи допомагають аналізувати ризики в умовах невизначеності та багатокритеріальності, що особливо важливо у цифровій трансформації та управлінні бізнесом.

Цифрові ризики стали важливою складовою сучасного бізнесу, і їх оцінка є необхідною умовою для ефективного управління підприємством. З урахуванням постійного розвитку технологій та зростання кіберзагроз, правильна оцінка цифрових ризиків дозволяє організаціям вчасно виявити потенційні загрози і вжити необхідних заходів для їх нейтралізації. Різноманітність доступних інструментів, таких як фреймворки, моделі оцінки та спеціалізовані програмні рішення, дає можливість підприємствам вибирати найбільш підходящий підхід залежно від специфіки їх діяльності та ресурсів. Вибір відповідних методів оцінки ризиків дозволяє компаніям не лише зменшити можливі збитки, але й забезпечити більш стабільну та безпечну роботу в умовах цифрової трансформації.

Висновки до розділу 1

Таким чином, розглянуто теоретичні основи цифрових ризиків, що дозволяють краще зрозуміти природу і особливості їх виникнення та впливу на міжнародний бізнес.

Визначено, що цифрові ризики є складовою частиною сучасного бізнес-середовища та виникають у процесі використання інформаційних технологій та цифрових інструментів. Вони включають в себе потенційні загрози для безпеки даних, конфіденційності та цілісності інформації, а також можуть бути спричинені технічними несправностями, кібератаками чи людським фактором.

Розглянуто різноманітні види цифрових ризиків, які виникають у процесі цифрової трансформації міжнародного бізнесу. Ці ризики класифіковані за кількома критеріями, зокрема за джерелом, видом загрози та потенційними наслідками. Окреслено широкий спектр цифрових ризиків, що виникають через впровадження новітніх технологій у міжнародному бізнесі. Врахування цих

ризиків є ключовим для прийняття ефективних рішень щодо управління ними в умовах глобалізації та цифрової трансформації.

Оцінювання ризиків є ключовим елементом управлінської діяльності, особливо в умовах цифрової трансформації, коли технології та кіберзагрози мають зростаючий вплив на бізнес-середовище. У цьому розділі розглядаються основні підходи та інструменти, що застосовуються для аналізу цифрових ризиків. Детально описано головні етапи процесу: ідентифікація, аналіз та власне оцінювання ризиків. Зазначено, що ризики можуть оцінюватися за допомогою кількісного підходу – із використанням числових даних, або якісного – на основі експертних суджень. Найбільш ефективним є комбінований метод, який поєднує обидва підходи й дозволяє отримати більш повну та обґрунтовану картину ризиків.

Досліджено, інструменти оцінки ризиків варіюються від простих опитувальників до складних програмних рішень, що дає можливість організаціям вибирати найбільш відповідні методи. Вибір інструментів визначається їхньою відповідністю низці критеріїв, що розглядаються в останньому підрозділі.

Отже, розуміння сутності, видів та методів оцінки цифрових ризиків є основою для ефективного управління ними і забезпечення стабільності та безпеки бізнесу в умовах цифрової трансформації.

РОЗДІЛ 2
АНАЛІЗ ЦИФРОВИХ РИЗИКІВ У МІЖНАРОДНОМУ БІЗНЕСІ

2.1. Ідентифікація та оцінка цифрових ризиків в міжнародному бізнесі

В економічній діяльності невіддільним складником функціонування будь-якої бізнес-структури на міжнародному рівні є ризики, адже саме вони створюють фундамент для прийняття управлінських рішень у контексті мінливості та невизначеності внутрішнього та зовнішнього середовища. Загалом, поняття ризику традиційно пов’язують з можливістю втрат, що з’являються через розрив між фактичними та очікуваними результатами діяльності. Проте, в сучасній міжнародній економіці ризики набувають значно ширшого тлумачення, включаючи як загрози, так і потенційні можливості, які можна застосувати з метою підвищення ефективності міжнародного бізнесу.

Беручи до уваги глобалізацію та комп’ютеризацію сучасного світу, варто звернути увагу на зміни, які відбуваються в міжнародному бізнесі, зокрема – його перехід на цифровий рівень. Загалом, кожна міжнародна компанія веде свою діяльність в онлайн-форматі: проведення торгів, підпис договорів та домовленостей, співпраця з іншими компаніями все частіше відбувається за допомогою використання інформаційних технологій. В результаті цього, виникає категорія цифрового ризику у міжнародному бізнесі.

Варто зазначити, що джерелами цифрового ризику є саме цифрові технології, які розподіляють на наступні категорії:

- пристрої та апаратне забезпечення;
- інноваційні технології зберігання, генерування, передачі та обробки інформації;
- програмне забезпечення;
- мережі (глобальні, локальні, зокрема Інтернет);
- штучний інтелект.

Ідентифікація та оцінка цифрових ризиків у міжнародному бізнесі є досить складним процесом, який передбачає розуміння різних аспектів цифрових операцій, безпеки даних та дотримання регуляторних норм між різними юрисдикціями. Для організацій важливо мати всебічний підхід до визначення та оцінки потенційних цифрових ризиків (див. рис. 2.1.)

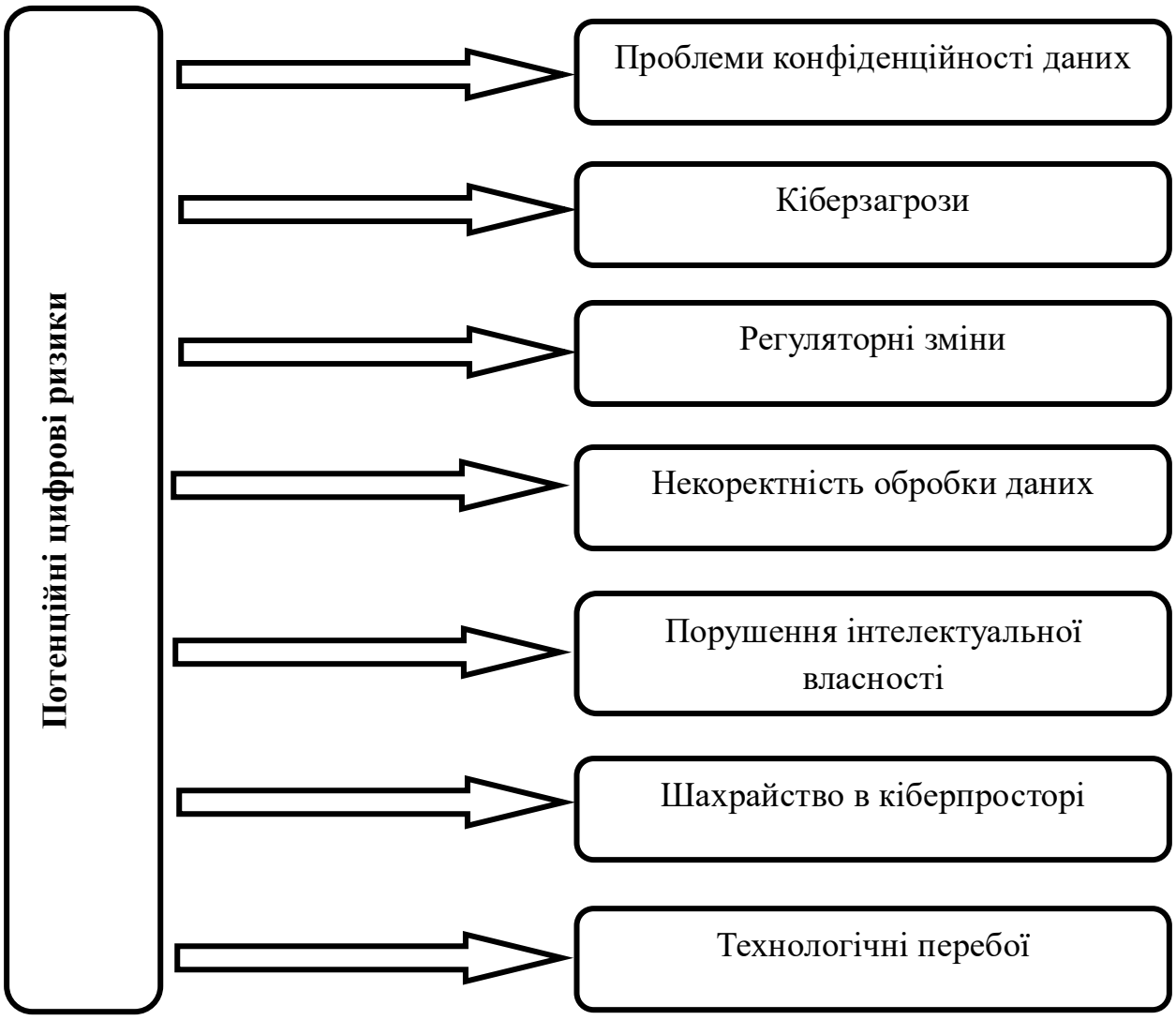

Рис. 2.1. *– Потенційні цифрові ризики у міжнародному бізнесі*

Джерело: [30, с. 72].

З метою ефективного управління цифровими ризиками в міжнародному бізнесі, компанії проводять ґрунтовні оцінки ризику, виконують регулярні аудити безпеки, контролюють утворювані загрози та посилюють підготовку працівників з найкращих практик кібербезпеки. На додаток, встановлення

надійної політики захисту даних, впровадження технологій шифрування та партнерства з надійними постачальниками кібербезпеки зменшує цифрові ризики та захищає конфіденційну ділову інформацію міжнародних компаній.

У цілому, проактивний підхід до визначення та оцінки цифрових ризиків є важливим для забезпечення безпеки та стійкості міжнародних бізнес-операцій у все більш взаємопов'язаній та оцифрованій глобальній економіці.

Провідні міжнародні компанії застосовують велику кількість різноманітних фреймворків, які спрямовані на проведення оцінки ризиків інформаційної безпеки та їх аналізу. Кожен з фреймворків відрізняється за певними критеріями, які є основними для різних підприємств. Беручи до уваги той факт, що існує декілька критеріїв і вони конфліктують між собою, переважна більшість міжнародних компаній використовує методи багатокритеріального аналізу, які дозволяють прогнозувати різні альтернативи за певними критеріями, що, в кінцевому результаті, повинне призвести до ефективного вибору оптимального методу оцінки ризиків.

Прикладом досить дієвого фреймворку є NIST Risk Management Framework, який не лише включає методики для оцінки ризиків, але й для організації управління ризиками інформаційної безпеки на різних рівнях, починаючи від стратегічного до конкретних застосувань на рівні окремих інформаційних систем. Цей підхід інтегрує безпеку, конфіденційність та управління ризиками у ланцюжок кіберпостачання, створюючи метод, який базується на оцінці ризиків при впровадженні кібербезпеки на ранніх етапах життєвого циклу системи.

Крім того, NIST RMF наголошує на ефективності, результативності та обмеженнях, які випливають з відповідних правових норм, директив, політик, стандартів і правил. Одночасно враховуючи ризики під час вибору та специфікації засобів управління.Основні цілі NIST Risk Management Frameworkподано на рис. 2.2.

Рис. 2.2*– Основні цілі NIST Risk Management Framework*

Джерело: [61, с. 11].

Компанії міжнародного рівня (Genesis, Dell Technologies,Carlsberg Group тощо) користуються методом багатокритеріального аналізу рішень (MCDA), який спрямований на визначення усіх можливих цифрових ризиків та визначення найкращої альтернативи, враховуючи не лише один, а кілька критеріїв. Це комплексний та багаторівневий процес, що містить ряд методів для формалізації та структурування прийняття рішень у послідовний та логічний спосіб. Важливим етапом в процесі аналізу є виокремлення критеріїв, за результатами яких надалі буде проводитись порівняння та оцінювання альтернатив та цифрових ризиків [44, с. 182].

Зазначимо, що процес оцінки ризиків у міжнародному бізнесі допомагає ідентифікації основних загроз для власників ризиків, встановлюючи пріоритети, які враховують їх наслідки та ймовірності, або інших визначених критеріїв. Відповідно до ISO/IEC 27005:2022 Risk management – Risk assessment techniques (Ризик-менеджмент – Техніки оцінювання ризиків), процес оцінки ризиків передбачає наступні етапи ідентифікації, аналізу та оцінки.

Розглянемо детальніше кожен з етапів:

- ідентифікація цифрових ризиків передбачає ідентифікацію активів, вразливостей, наслідків та загроз;
- аналіз цифрових ризиків має на меті розгляд можливих джерел та причин ризику, ймовірність, реалізації певної події, яка призведе до небажаних результатів;
- оцінка ризиків передбачає визначення рівня ризиків, їх пріоритетність та значущість для подальшої обробки(Детальну схему елементів оцінки ризиків подано у *Додатку А*).

Управління цифровими ризиками в інформаційній безпеці передбачає встановлення методів для проведення оцінки ризиків, аналізу цих ризиків, їх обробки, а також постійний перегляд та вдосконалення процесу дослідження цифрових ризиків.

Зазначимо, що процес оцінки ризиків у міжнародному бізнесі допомагає ідентифікації основних загроз для власників ризиків, встановлюючи пріоритети, які враховують їх наслідки та ймовірності, або інших визначених критеріїв.

Загалом, оцінка ризиків передбачає наступні етапи:

1. прогнозування ймовірності виникнення ризиків;
2. їх вплив на ведення бізнесу та розвиток компанії загалом;
3. прогнозування наслідків, до яких може призвести той чи інших цифровий ризик;
4. можливі дії, спрямовані на зниження чи уникнення загроз чи цифрових ризиків;
5. отримання якомога менших втрат від того чи іншого цифрового ризику;
6. розвиток та успішна діяльність компанії після подолання цифрових ризиків.

Підкреслимо, що ідентифікація ризиків є ключовим етапом управління цифровими бізнес-ризиками, який вимагає проведення ретельного аналізу з метою виявлення ситуацій та потенційних загроз, що можуть вплинути на

досягнення цілей міжнародної компанії. У міжнародному бізнесі цей процес базується на різних методах, таких як огляд процесів бізнесу, аналіз стейкхолдерів, використання досвіду, застосування технік та інструментів, сценарне планування, а також експертній оцінці.

Переважна більшість міжнародних компаній використовує комплексний підхід, який враховує можливість наявності різноманітних ризиків і включає участь різних стейкхолдерів, що дозволяє виконати повне охоплення та провести аналіз ризиків, які можуть виникнути в діяльності компанії. Шляхом проведення такого детального аналізу міжнародний бізнес може підготуватися до відповідного управління цифровими ризиками, зменшуючи їхні негативні наслідки та користуючись можливостями для покращення ефективності діяльності.

Аналіз цифрового ризику передбачає перевірку ймовірності та наслідки кожного ризику, що забезпечує змогу компанії обрати на чому зосередитися в першу чергу. Такі фактори, як втрачений час, ймовірні фінансові втрати для підприємства, складність впливу, відіграють важливу роль у точному аналізі кожного цифрового ризику.

Оцінка цифрових ризиків передбачає процес визначення можливості та впливу потенційних цифрових ризиків на досягнення загальних цілей міжнародного бізнесу, а також рівня їхньої важливості для організації. Процес оцінки ризиків виконується шляхом проведення оцінювання ризиків за допомогою різних інструментів і методів.

Основна відмінність полягає в тому, що якісний аналіз ризиків застосовує суб’єктивні показники, такі як:

- високий;
- середній;
- низький;
- життєво важливий;
- критично-важливий;
- еталонний рівень тощо.

Різні методи оцінки цифрових ризиків, застосовують різноманітні підходи. Провідні міжнародні компанії найчастіше користуються якісним, кількісним та комбінацією цих двох підходів (див. рис. 2.3.)

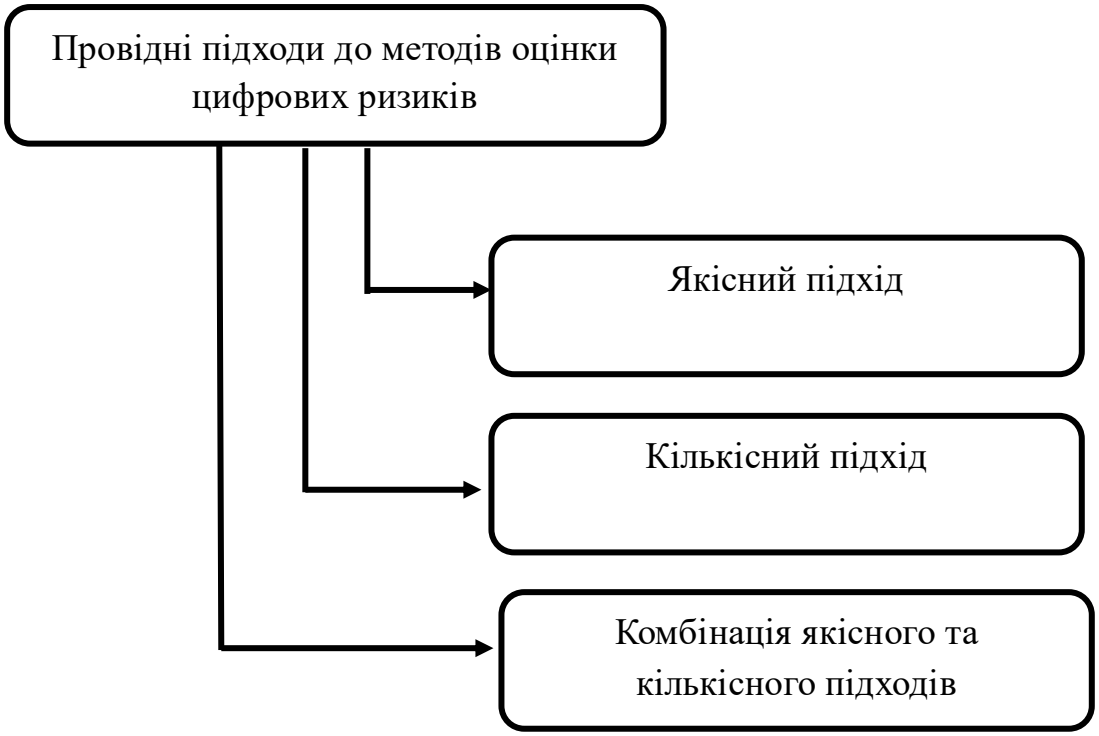

Рис. 2.3.*– Провідні підходи до методів оцінки цифрових ризиків у міжнародному бізнесі*

Джерело: [32, с. 177].

Основними інструментами якісного аналізу є наступні: SWOT-аналіз, метод «мозкового штурму», PESTLE-аналіз та експертні інтерв'ю. Перевагою якісного підходу є його відносна простота та універсальність, оскільки він не вимагає складних обчислень чи значних фінансових витрат. Однак обмеженням даного методу є суб'єктивність результатів, адже вони залежать від компетентності експертів.

Натомість кількісний метод забезпечує певні числові результати, які виражають ймовірність кожного ризику та його наслідки. Кількісний метод виражає результати за допомогою наступної формули 2.1:

$$Magnitudeofrisk = Likelihood \cdot Impact \quad (2.1)$$

де

Likelihood– це ймовірність настання ризику;

Impact– очікуваний вплив у грошовому еквіваленті [50, с. 177].

При наявності застосування правдивих даних, кількісний аналіз надає більш об’єктивну інформацію, ніж якісний аналіз ризиків.

В сучасних умовах хаотичних і швидких змін зовнішнього середовища ідентифікація ризиків діяльності міжнародного бізнесу, моніторинг рівня прояву цифрових ризиків, вчасне реагування на небезпеки є вкрай важливими аспектами ведення бізнесу. Цифрова міжнародна економіка дозволяє виявляти ризики через використання автоматизованих систем та програмних продуктів, зокрема MES і ERP систем, аналітичних програм SAS та когнітивних обчислень. Проте всі ці процеси мають відбуватися поетапно, заплановано, продумано та з використанням відповідних інструментів ідентифікації, оцінки та методів аналізу цифрових ризиків.

Сучасний міжнародний бізнес переважно використовує методи MCDA, які найкраще підходять для оцінювання альтернативи ризиків, враховуючи специфіку діяльності компаній чи організацій. Найпоширенішими серед методів сьогодні є наступні: AHP (Метод аналізу ієрархій); MAUT; MULTIMOORA; Метод зваженої суми; COPRAS; TOPSIS; PROMETHEE; методи ELECTRE (Elimination Et Choice Traduisant la Realite) тощо [49].

Беручи до уваги різні фактори та особливості оцінки ризиків, сучасні міжнародні компанії застосовують різні методи та їх інструментарій з метою проведення точного аналізу цифрових ризиків для бізнесу, починаючи зі звичайного опитувальника для спеціалістів підприємств та компаній, закінчуючи спеціальними програмними забезпеченнями для подальшого обрахування рівня ризиків. Вибір оптимальних методів міжнародними компаніями залежить від багатьох об’єктивних критеріїв. Як доводить світова

практика, ключовими критеріями, які найчастіше застосовують, порівнюючи методи оцінки цифрових ризиків є наступні (див. рис. 2.4)

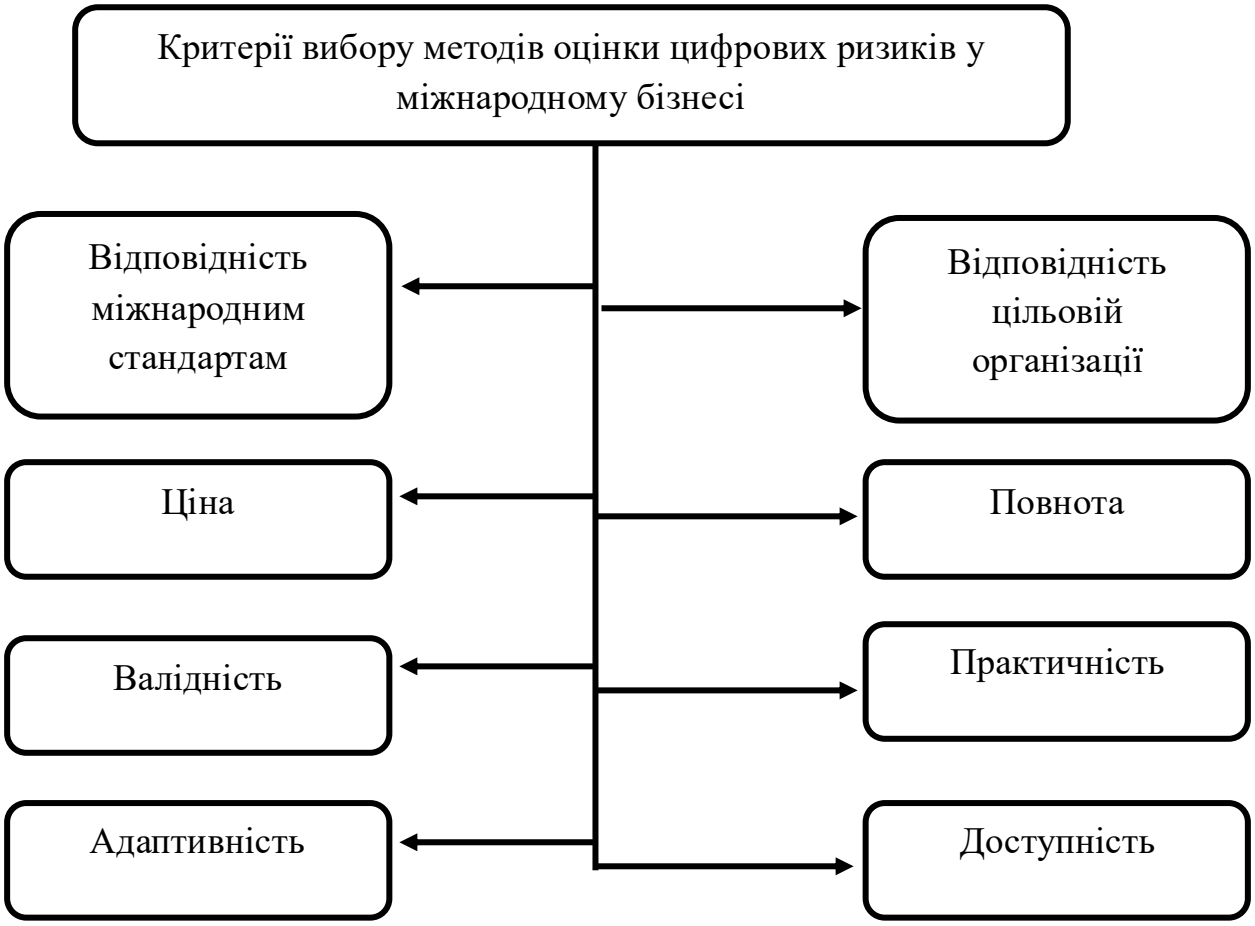

Рис. 2.4 *– Критерії вибору методів оцінки цифрових ризиків у міжнародному бізнесі*

Джерело:[50, с. 177].

AHP – це метод, що дозволяє оцінювати та порівнювати різні альтернативи, враховуючи різні критерії та їх вагомість. За допомогою AHP керівники можуть створити ієрархію цілей та критеріїв, порівняти їх та призначити їм ваги. Цей підхід дозволяє отримати комплексний рейтинг альтернатив і прийняти обґрунтоване рішення.

Метод MAUT (Мультиатрибутивна теорія корисності) є найбільш цілком виправданим у вирішенні завдань упорядкування альтернатив. Побудова

функції корисності проводиться незалежно від того, чи визначені конкретні альтернативи. Очевидно, що однакові діапазони значень критеріїв можливі для різних варіантів альтернатив[22, с. 51].

Метод SAW (Simple Additive Weighting Method) дозволяє здійснити просте адитивне зважування, що є найбільш простим методом вирішення багатокритеріальних завдань. Загальна оцінка кожної альтернативи обчислюється шляхом множення значення атрибуту кожної альтернативи на вагу, призначену цьому атрибуту. Альтернатива з найвищою оцінкою знаходиться відповіддю на завдання з прийняття рішення[8, с. 228].

Метод TOPSIS (Technique for order preference by Similarity to Ideal Solution) або метод ідеальної точки передбачає порівняння альтернатив через відстань значень атрибутів до найкращого та найгіршого рішення.

Методи ELECTRE (метод виключення та вибору, що віддзеркалює реальність) спрямовані на вибір кращого рішення з визначеного набору рішень, але й може застосовуватися для вирішення трьох типів проблем: ранжування, вибір та сортування.

Метод COPRAS (Complex Proportional Assessment) застосовує як мінімальні, так і максимальні критерії в розрахунку інтегрального показника оцінки, та не потребує перетворення перших на другі.

Група методів PROMETEE (Preference Ranking Organization Method for Enrichment Evaluation)відрізняється від інших методів своїм використанням функції переваги як основи методу. Таким чином, методи PROMETEE дозволяють оцінювати обрані критерії та їх важливість шляхом складного та глибокого підходу, використовуючи відбіркові функції, параметри та форми, які обираються експертами.Оскільки методи PROMETEE використовують значення функцій, які враховують рівень переваги однієї альтернативи над іншою, вони не вимагають перетворення мінімізуючих критеріїв на максимізуючі або негативних значень на позитивні під час нормалізації. Методи цієї групи легкі у застосуванні і не потребують припущень щодо пропорційності критеріїв.

Поглиблений аналіз міжнародного досвіду застосування методів оцінки цифрових ризиків дозволяє розглянути цифрову частку використання того чи іншого методу міжнародними компаніями різних спрямувань з метою детального вивчення цифрових ризиків у їхній діяльності (табл. 2.1.)

Таблиця 2.1 – Кількісна частка застосування методів оцінки цифрових ризиків у міжнародному бізнесі

№	Назва методу	Найвідоміші компанії-користувачі	Частота використання у межах 100%
1.	AHP (Метод аналізу ієрархії)	Syngenta, Ембер Ріал Естейт	54%
2.	MAUT	Greenbox, Liquid Robotics	43%
3.	MULTIMOORA	Patagonia, Boo-box	61%
4.	Метод зваженої суми	Red Bull Media House, James Corner Field Operations	30%
5.	COPRAS	Occupy Movement, SoundCloud	49%
6.	TOPSIS	Kiva Systems, Bug Agentes Biológicos	61%
7.	PROMETHEE	Genentech, Chobani	38%
8.	ELECTRE (Elimination Et Choice Traduisant la Realite)	Genesis, Facebook, SolarCity, PayPal, OpenSky, Knewton	73%

Джерело: розроблено автором[8, с. 228-230; 50, с. 177].

Як видно з табл. 2.5. методи ELECTRE є найчастіше використовуваними, адже вони мають просту логіку, забезпечують можливість порівняння альтернативи при сильній неоднорідності критеріїв та допускають непорівнянність між альтернативами.

Отже, з метою ефективного управління цифровими ризиками в міжнародному бізнесі, підприємства та компанії проводять ґрунтовні оцінки ризику, виконують регулярні аудити безпеки, контролюють виникаючі загрози та посилюють підготовку працівників з найкращих практик кібербезпеки. На додаток, встановлення надійної політики захисту даних, впровадження технологій шифрування та партнерства з надійними постачальниками кібербезпеки зменшує цифрові ризики та захищає конфіденційну ділову інформацію міжнародних компаній.

Процес оцінки ризиків передбачає наступні етапи: ідентифікація, аналіз та оцінка ризиків, які передбачають прогнозування ймовірності виникнення ризиків; дослідження їх впливу на ведення бізнесу та розвиток компанії загалом; прогнозування наслідків, до яких може призвести той чи інших цифровий ризик; можливі дії, спрямовані на зниження чи уникнення ризиків; отримання якомога менших втрат від того чи іншого ризику; розвиток та успішна діяльність компанії після подолання цифрових ризиків. Всі ці процеси відбуваються поетапно, заплановано, продумано та з використанням відповідних інструментів ідентифікації, оцінки та методів аналізу цифрових ризиків.

2.2. Вплив цифрових ризиків на розвиток міжнародного бізнесу

В останні роки спостерігається суттєве збільшення кількості кібератак на світові компанії. Провідною метою хакерів стають не лише великі міжнародні компанії, але й також середній та малий бізнес. Кіберзлочинці намагаються втрутитися в бізнес, знищити або послабити компанію-конкурента, викрасти інформацію та гроші. Згідно з даними Cybersecurity Venturesreport у 2024 році 49% американських компаній та 51% європейських компаній зазнали впливу цифрових ризиків, у результаті якихзазнали колосальних витрат. На додаток, розвиток інформаційно-технічної сфери доводить, що збільшення кількості кібератак буде зростати з кожним роком, відповідно, зростатиме й рівень складності кіберризиків.

Згідно зі звітом Барометра ризиків Allianz, який щорічно публікується Allianz Global Corporate & Specialty (AGCS) та ґрунтується на думці 1911 експертів із ризик-менеджменту з 80 країн світу, починаючи з 2022 року цифрові ризики входять у трійку найважливіших ризиків у міжнародному бізнесі. Для порівняння – у 2019 році цифрові ризики посідали 11 місце, а у 2020 році – 7 місце, у 2023 році –5, а вже в 2025 році – входять в трійку лідерів.

Крім того, найбільшими побоюваннями компаній у сфері кіберзагроз стали наступні:

1. витік даних (61%)
2. атаки на критичну інфраструктуру (57%)
3. зростання атак програм-вимагачів (49%)
4. перебої в цифрових ланцюжках поставок (29%)
5. підміна електронної пошти (18%) [1].

На основі наукових досліджень, цифрові ризики можна класифікувати за наступними ознаками (див. рис. 2.5.)

Рис. 2.5 *– Ознаки класифікації цифрових ризиків*

Джерело: [43, с. 111].

Як зазначають світові аналітики, порушення даних, хакерські атаки, перерви у виробництві в результаті кіберінцидентів доводять, що цифрові ризики є головними проблемами для бізнесу США та посідають друге місце за

значущістю серед бізнес-ризиків на Азійсько-тихоокеанському та Європейському континенті. Загалом, цифрові ризики посідають друге місце серед ризиків у міжнародному бізнесі та мають колосальний вплив на всі галузі міжнародної економічної діяльності, що призводить до досить негативних наслідків, зокрема втрати колосальних прибутків, одержання збитків і, навіть, до закриття цілих компаній та організацій.

Базуючись на ознаках класифікації цифрових ризиків у міжнародному бізнесі, виокремимо основні групи ризиків:

- ризик фінансових втрат від фішингових атак;
- ризик втрати інформації під час злому паролю доступу або внаслідок DDoS атаки;
- ризик фінансових втрат через порушення роботи комп'ютерних систем;
- ризик фінансових втрат через викрадення та розголошення персональних даних та інформації;
- ризик фінансових втрат від кібершантажу або вірусного блокування комп'ютерних систем [60, с. 133].

Аналітичні дослідження компанії Check Point показують, що у 2023 році кількість цифрових атак на бізнес зросла на 39% у порівнянні з попереднім роком[60, с. 133].Найбільш поширені типи атак – це програми-вимагачі, фішингові кампанії та атаки на постачальницькі ланцюги. Особливо небезпечними стали атаки на хмарні сервіси, адже велика кількість міжнародних компаній продовжують інтегрувати такі рішення у свою роботу.

Цифрові ризики, переважно, чинять негативний вплив на міжнародний бізнес, наприклад:

- викрадення корисної для хакера інформації;
- використання хакером персональної інформації підприємства чи організації з метою здійснення атаки на когось іншого;
- отримання хакером доступу до цілей більш високого профілю через послуги, товари або ролі в ланцюжку постачання;
- зниження продуктивності;

- втрата компанією прибутку;
- пошкодження інформаційної системи;
- неможливість одержання банківського кредиту;
- втрата репутації поміж клієнтів;
- втрата клієнтської аудиторії та прибутку [12, с. 111].

Розглянемо вплив цифрових ризиків на діяльність міжнародного бізнесу у табл. 2.2.

Таблиця 2.2 – Вплив цифрових ризиків на діяльність міжнародного бізнесу

Вплив	Наслідки
Припинення або уповільнення бізнес-процесів	Витік конфіденційної інформації через хакерські атаки або внутрішні помилки.В результаті кібератаки критично важливі бізнес-процеси можуть бути зупинені на тривалий час. Відділ підтримки стає перевантажений, а незадоволені клієнти вже готові припинити партнерство. Все це не лише ускладнює роботу компанії, але й впливає на її конкурентоспроможність.
Втрата конкурентної переваги	
Судові позови та судові розгляди	Витрати на усунення наслідків.Штрафи та санкції регулюючих органів, невідповідність вимогам щодо захисту персональних даних (наприклад GDPR або аналогічних законів у інших країнах) може призвести до значних штрафів та юридичних наслідків. Компанії можуть бути притягнуті до суду через витік особистих даних клієнтів.
Збиток для бренду	Викрадення коштів, шахрайство, зловмисне використання ресурсів. Атаки за допомогою програм-вимагачів можуть зупиняти роботу бізнесу на тривалий час, що в результаті призведе до значних фінансових втрат. На додаток, витрати на відновлення систем.Штрафи за порушення законів про захист даних і потенційні позови клієнтів можуть ще більше погіршити фінансовий стан компанії.
Втрата репутації	Якщо інформація про успішну атаку на компанію стає публічною - це може серйозно підірвати довіру клієнтів та партнерів. Бізнеси, які зазнали кібератаки стикаються з ризиком втрати клієнтської бази та погіршенням своїх позицій на ринку
Порушення роботи систем	Збої в IT-інфраструктурі, віруси або DDos-атаки.

Джерело:[60, с. 134].

Зазначимо, що кібершпигунство є інструментом одержання конкурентних переваг на міжнародному ринку. Як зазначають аналітики, досить часто фінансування кібершпигунства здійснюється урядами різних країн. Кібершпигунство полягає в здійсненні кібератак, зокрема фішингових кампаній, вчиненню витоків даних, зламу облікових записів адміністраторів і користувачів. На додаток, діяльність, пов'язана з кібершпигунством, зокрема крадіжкою конфіденційної інформації та інтелектуальної власності, також створює серйозні ризики для міжнародних компаній та їх діяльності. Такі інциденти не лише підривають стабільність і довіру до того чи іншого виду бізнесу, але й можуть завдати значних фінансових збитків. Загалом, вразливість цифрової інфраструктури різних міжнародних галузей створює ризики, що можуть призвести до збоїв у роботі систем, фінансових втрат і навіть до глобальних економічних криз.

Активне впровадження новітніх цифрових рішень сприяло не лише масштабуванню електронної торгівлі, але й значному ускладненню структури ризиків, з якими стикаються як споживачі, так і компанії. Цифрові загрози дедалі частіше проявляються у вигляді несанкціонованого доступу до конфіденційної інформації користувачів, її подальшого нецільового використання, викрадення, або навіть навмисного спотворення зловмисниками. Це може включати як фінансові махінації, так і маніпуляції з цифровими контрактами чи логістичними даними.

До основних цифрових ризиків, які загрожують учасникам міжнародної електронної торгівлі, належать кібератаки, фішинг, атаки програмами-вимагачами (ransomware), проникнення у внутрішні системи компаній через вразливості в програмному забезпеченні, компрометація електронної пошти, а також шахрайство, пов'язане з підробленими торговельними платформами. Всі ці фактори ставлять під загрозу безперервність торгівельних процесів, ділову репутацію та довіру споживачів до цифрового середовища.

Деталізовану візуалізацію цифрових ризиків представлено на рисунку 2.6.

Рис. 2.6 – *Загрози у вигляді несанкціонованого доступу до персональних даних клієнтів*

Джерело: [25, с. 299].

Отже, цифрові ризики мають колосальний вплив, переважно негативного характеру, на ведення бізнесу на міжнародному рівні. Загалом, вони здатні на припинення або уповільнення бізнес-процесів, що призводить до витоку конфіденційної інформації через хакерські атаки або внутрішні помилки та знижує конкурентоспроможність компанії; їх поява призводить до судових розглядів та позовів через витік особистих даних клієнтів; призводять до втрати репутації на міжнародному ринку, адже бізнеси, які зазнали кібератаки, стикаються з ризиком втрати клієнтської бази та погіршенням своїх позицій на ринку; стають причиною збитковості бренду, оскільки атаки за допомогою програм-вимагачів можуть зупиняти роботу бізнесу на тривалий час, що

призводить до значних фінансових втрат; стають причиною порушення роботи систем, а відповідно, й погіршення та призупинення роботи самої компанії.

2.3. Сучасні стратегії управління цифровими ризиками в міжнародних компаніях

Процес управління ризиками є провідним аспектом для функціонування та успішного розвитку міжнародних компаній, незалежно від галузі діяльності чи розміру організацій. В сучасних умовах глобальної цифровізації, коли світова економічна ситуація стає все більш непередбачуваною, а світові тренди та технології зазнають постійних змін, здатність бізнесу швидко ефективно мінімізувати потенційні цифрові загрози та адаптуватися до змін стає ключовим чинником успішного ведення міжнародного бізнесу.

У процесі розробки стратегії управління цифровими ризиками важливо розуміти, що ризики не можна повністю усунути, проте їх можна спрогнозувати, оцінити та знизити рівень небезпеки їх впливу та наслідків завдяки правильному підходу. Сучасне успішне управління цифровими ризиками передбачає реалізацію наступних кроків (див. рис. 2.7).

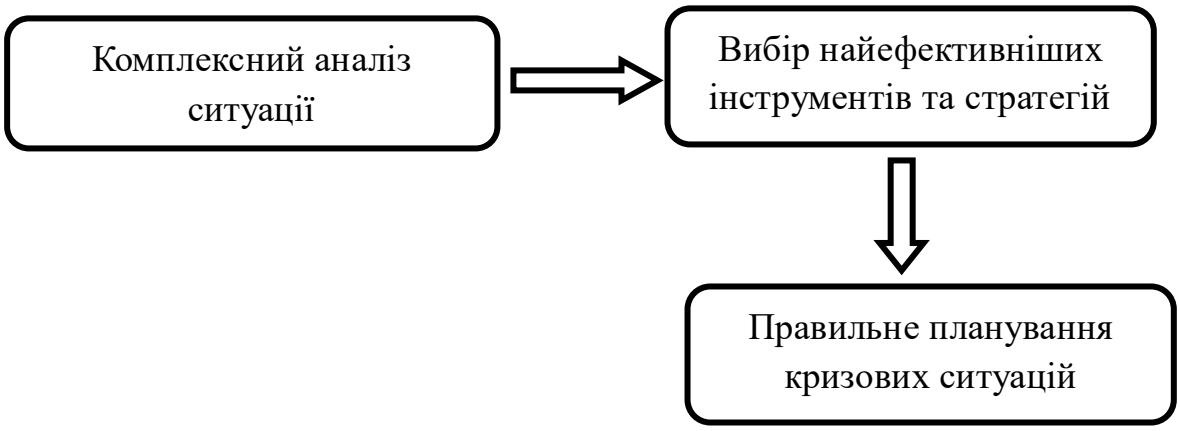

Рис. 2.7 *– Кроки успішного управління цифровими ризиками*

Джерело: [5, с. 350].

Розглянемо основні стратегії управління цифровими ризиками в міжнародному бізнесі. Варто зазначити, що управління ризиками – це не лише реакція на проблеми, а стратегічний підхід, який гарантує розвиток і стабільність бізнесу в умовах невизначеності. Результативне управління ризиками полягає не тільки в їхньому виявленні та аналізі, але й застосуванні різних стратегій та інструментів для мінімізації ймовірних цифрових загроз.

Першим етапом в управлінні цифровими ризиками є їх ідентифікація, яка полягає у виявленні потенційних цифрових ризиків, які можуть чинити значний вплив на діяльність міжнародної компанії. Загалом, ідентифікація включає декілька важливих етапів, які є взаємозалежними та виходять один з одного (див. рис. 2.8.)

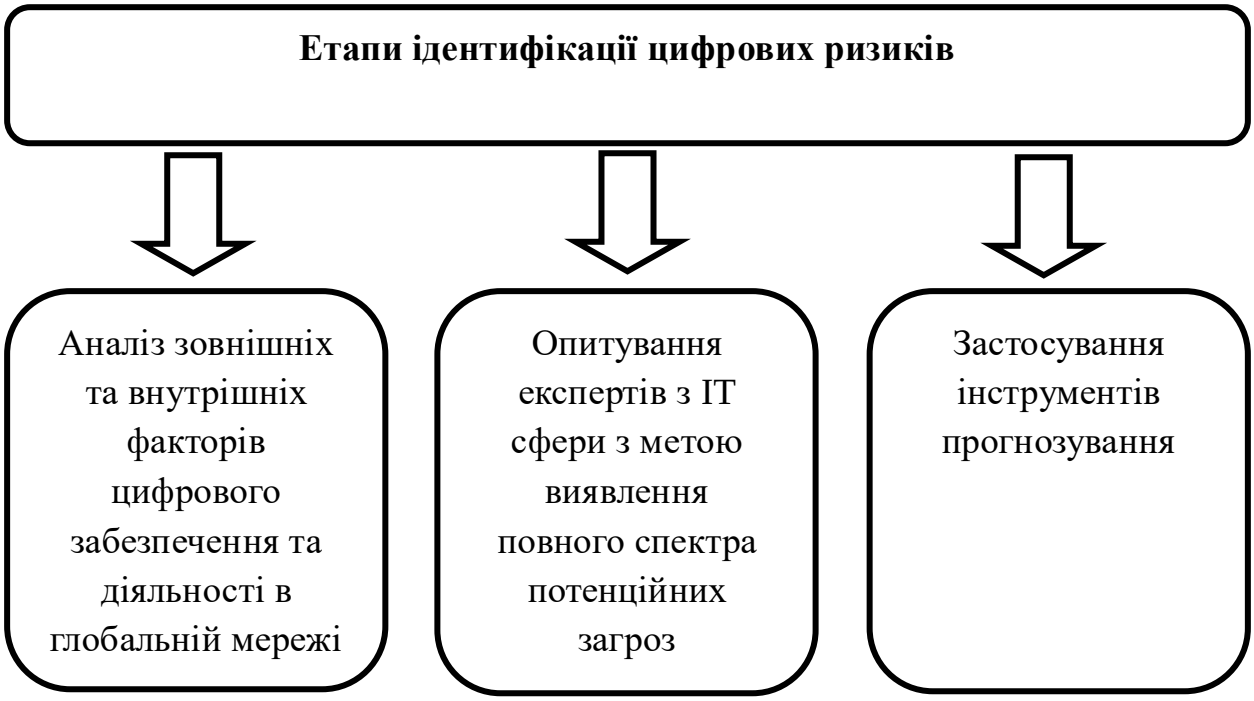

Рис. 2.8 *– Етапи ідентифікації цифрових ризиків*

Джерело: [50, с. 177].

Ідентифікація цифрових ризиків дозволяє створити базу для подальшої роботи з ними з метою розробки стратегій мінімізації.

Наступним кроком після ідентифікації є оцінка та аналіз впливу цифрових ризиків на бізнес-процеси, що допомагає зрозуміти, які саме аспекти

міжнародної діяльності організації можуть бути піддані впливу кіберризиків і в якій мірі це може загрожувати стабільності ведення бізнесу. Виокремимо ключові моменти оцінки бізнесу:

1. ідентифікація ключових бізнес-процесів. Наприклад, обробка замовлень або забезпечення доступності сайту;
2. оцінка ймовірності настання цифрового ризику;
3. визначення потенційного впливу цифрового ризику на діяльність компанії [44].

Застосування зазначеної інформації дозволяє зробити чіткі висновки про запровадження необхідних заходів для захисту від ймовірних цифрових ризиків.

Потужним інструментом для стратегічного управління та оцінки цифрових ризиків є SWOT-аналіз, який дозволяє систематизувати всю наявну інформацію про слабкі та сильні сторони бізнесу, а також зовнішні загрози та можливості. Ключові аспекти SWOT-аналізу подано в табл. 2.3

Таблиця 2.3 – Ключові аспекти SWOT-аналізу

Аспект	Зміст
Сильні сторони(Strengths)	Оцінка того, де бізнес має конкурентні переваги, що допомагає зосередитися на тих аспектах діяльності, які потребують найменше управління цифровими ризиками.
Слабкі сторони (Weaknesses)	Виявлення слабких місць, наприклад, у цифрових бізнес-процесах або організаційній структурі, дозволяє спрогнозувати потенційні цифрові ризики.
Можливості (Opportunities)	Оцінка зовнішніх можливостей для бізнесу допомагає виявити можливі вигоди, яких можна досягти, навіть з огляду на цифрові ризики.
Загрози (Threats)	Визначення цифрових загроз дозволяє підготувати стратегії для мінімізації їхнього впливу.

Джерело: [10, с. 296;34, с. 151].

Саме завдяки SWOT-аналізу компанії міжнародного бізнесу можуть побачити повну картину цифрових ризиків, які наявні в їхній діяльності, і прийняти обґрунтовані рішення щодо стратегій управління ними.

Важливу роль в управлінні цифровими ризиками відіграє процес мінімізації ризиків, який передбачає:

- страхування – найпоширеніша стратегія, спрямована на зменшення фінансових втрат. На додаток, страхування може допомогти захистити бізнес від непередбачуваних ситуацій. Найкращими видами страхування від цифрових ризиків є саме кіберстрахування (Cyber Insurance) та страхування від перерви в діяльності (Business Interruption Insurance). Кіберстрахування допомагає міжнародним компаніям захистити свої цифрові активи від зламу систем, кібернападів, витоку конфіденційної інформації або крадіжки даних. Страхування від перерви в діяльності допомагає компенсувати втрати доходів, одержані від кібератак; покрити операційні витрати та зберегти фінансову стабільність організації до повного відновлення її роботи. Наприклад, компанія Greenbox у 2022 році застрахувала власний бізнес від перерв у діяльності на випадок виникнення технічних неполадок. Через пів року на компанію відбулася хакерська атака, яка зламала систему обробки замовлень. В результаті, компанія Greenbox одержала компенсацію за втрачені доходи, що забезпечило стабільність у період, коли система була зламана;
- технічні рішення, які передбачаютьавтоматизацію процесів, провадження новітніх технологій, розробку систем моніторингу та захисту від кіберзагроз, що допомагають зменшити ризики, пов’язані з кібернападами або технологічними збоями;
- юридичні заходи, спрямовані на уникнення судових позовів та порушень законодавства, а також на забезпечення виконання контрактів. В роботі кожної компанії необхідно мати добре сформульовані юридичні угоди та постійно слідкувати за їх відповідністю змінам в сучасному законодавстві;

- організаційні заходи, які полягають у запровадженні змін в організаційній структурі бізнесу, перенавчанні співробітників або створенні резервних команд для виконання критичних функцій, що може значно знизити операційні ризики.

Сучасний міжнародний бізнес потребує швидкого реагування на зміни у внутрішніх процесах та зовнішньому середовищі. Для цього міжнародним компаніям необхідно мати не лише висококваліфіковану команду спеціалістів, але й досить потужні інструменти для автоматизації процесу управління цифровими ризиками. Сьогодні інструменти автоматизації гарантують швидку та ефективну ідентифікацію, оцінювання та реагування на потенційні цифрові загрози, зменшуючи вплив людського фактора та прискорюючи процес прийняття оптимальних рішень. З постійним розвитком сучасних технологій автоматизація стає дедалі важливішою для забезпечення злагодженого та оперативного управління цифровими ризиками в умовах високої конкуренції та мінливої економіки. Саме тому, сучасні стратегії управління цифровими ризиками передбачають використання основних інструментів для автоматизації управління ризиками, включаючи програмне забезпечення для аналізу та прогнозування ризиків, програмні платформи для моніторингу ризиків та інноваційні технології.

Досить важливим інструментом є програмне забезпечення для прогнозування та аналізу ризиків, наприклад:

- RiskWatch – інструмент для проведення моніторингу та оцінки цифрових та інших ризиків у різних сферах міжнародного бізнесу, зокрема в галузі управління якістю, кібербезпеки та охорони праці.
- SAS Risk Management – програма, призначена для управління та оцінки операційними, цифровими та фінансовими ризиками в діяльності компаній.
- Palantir – програмне забезпечення, призначене для аналізу цифрових ризиків, кібератак та обробки великих даних на основі моделей штучного інтелекту.

- NIST Cybersecurity Framework і ISO 27001 Framework – забезпечують ефективне управління цифровими загрозами та дотримання нормативних вимог[60, с. 132].

Досить популярними у міжнародному бізнесі є стратегії зменшення цифрових ризиків. Зокрема, це запровадження та використання технологій (наприклад, шифрування, брандмауери та виявлення вторгнень). Дані технології відіграють ключову роль у процесі виявленні, реагуванні та запобіганні цифрових загроз та кібератак. Як доводить світовий досвід провідних міжнародних компаній, запровадження правильних технологічних інструментів сприяє зменшенню ймовірності успішної кібератаки та обмежує шкоду бізнесу, спричинену цією атакою. Розглянемо ключові технології, які використовують міжнародні компанії у таблиці 2.4.

Таблиця 2.4 – Ключові технології зменшення цифрових ризиків

№	Назва	Функції
1.	Брандмауери	Діють як бар'єри між внутрішніми мережами та зовнішніми джерелами, виконуючи фільтрацію трафіку, щоб запобігти несанкціонованому доступу та атакам
2.	Системи виявлення вторгнень (IDS)	IDS відстежує трафік мережі на наявність підозрілих дій та повідомляє командам безпеки про можливі загрози в режимі реального часу.
3.	Шифрування	Процес шифрування конфіденційних даних гарантує, що навіть у разі перехоплення даних, можливість їх прочитання залишається не доступною для неавторизованих осіб. Це є досить важливим для захисту конфіденційної інформації під час зберігання та передачі.
4.	Захист кінцевої точки	Встановлення рішень безпеки та антивірусних рішень кінцевих точок на всіх пристроях гарантує, що будь-які загрози будуть виявлені та пом'якшені на рівні пристрою.
5.	Запобігання втраті даних (DLP)	Інструменти DLP обмежують та контролюють переміщення конфіденційних даних задля запобігання несанкціонованого доступу або витоку даних

Джерело: [50, с. 177].

Таким чином, аналітичні інструменти допомагають не лише оцінити поточні ризики, але й розробити оптимальні стратегії для мінімізації цих ризиків. Новітнє та високоякісне програмне забезпечення може допомогти обрати ефективні стратегії для зниження цифрових ризиків на основі одержаних даних та прогнозів.

Отже, сучасні стратегії управління цифровими ризиками передбачають використання великої кількості інструментів (програмного забезпечення, цифрових технологій тощо), які спрямовані на детальне вивчення, ідентифікацію, оцінювання, дослідження впливу та прогнозування наслідків впливу цифрових ризиків у міжнародному бізнесі, а також дослідженні подальшої роботи компаній. Основними стратегіями управління цифровими ризиками є наступні: стратегія зменшення (мінімізації) ризиків; стратегія юридичного захисту, стратегія страхування від ймовірності виникнення цифрових ризиків. Однак, найрезультативнішою стратегією управління цифровими ризиками є комплексне та продумане використання усіх сильних сторін кожної із зазначених стратегій.

Висновки до розділу 2

У другому розділі наукового дослідження було проаналізовано процес ідентифікації та оцінки цифрових ризиків в міжнародному бізнесі; досліджено вплив цифрових ризиків на розвиток міжнародного бізнесу та визначено сучасні стратегії управління цифровими ризиками в міжнародних компаніях.

Ідентифікація ризиків є ключовим етапом управління цифровими бізнес ризиками, який вимагає проведення ретельного аналізу з метою виявлення ситуацій та потенційних загроз, що можуть вплинути на досягнення цілей міжнародної компанії. У міжнародному бізнесі цей процес базується на різних методах, таких як огляд процесів бізнесу, аналіз стейкхолдерів, використання досвіду, застосування технік та інструментів, сценарне планування, а також експертній оцінці. Аналіз цифрового ризику передбачає перевірку ймовірності

та наслідки кожного ризику, що забезпечує змогу компанії обрати на чому зосередитися в першу чергу. Оцінка цифрових ризиків передбачає процес визначення можливості та впливу потенційних цифрових ризиків на досягнення загальних цілей міжнародного бізнесу, а також рівня їхньої важливості для організації. Процес оцінки ризиків виконується шляхом проведення оцінювання ризиків за допомогою різних інструментів і методів. Сучасні міжнародні компанії застосовують методи та їх інструментарій з метою проведення точного аналізу цифрових ризиків для бізнесу, починаючи зі звичайного опитувальника для спеціалістів підприємств та компаній, закінчуючи спеціальними програмними забезпеченнями для подальшого обрахування рівня ризиків.

Цифрові ризики мають колосальний вплив, переважно негативного характеру, на ведення бізнесу на міжнародному рівні. Загалом, вони здатні на припинення або уповільнення бізнес-процесів, що призводить до витоку конфіденційної інформації через хакерські атаки або внутрішні помилки та знижує конкурентоспроможність компанії; їх поява призводить до судових розглядів та позовів через витік особистих даних клієнтів; призводять до втрати репутації на міжнародному ринку, адже бізнеси, які зазнали кібератаки, стикаються з ризиком втрати клієнтської бази та погіршенням своїх позицій на ринку; стають причиною збитковості бренду, оскільки атаки за допомогою програм-вимагачів можуть зупиняти роботу бізнесу на тривалий час, що призводить до значних фінансових втрат; стають причиною порушення роботи систем, а відповідно, й погіршення та призупинення роботи самої компанії.

Сучасні стратегії управління цифровими ризиками у міжнародних компаніях передбачають застосування великої кількості інструментів, які спрямовані на детальне вивчення, ідентифікацію, оцінювання, дослідження впливу та прогнозування наслідків впливу цифрових ризиків у міжнародному бізнесі, а також дослідженні подальшої роботи компаній. Сьогодні ключовими стратегіями управління цифровими ризиками є стратегія зменшення (мінімізації) ризиків; стратегія юридичного захисту, стратегія страхування від ймовірності виникнення цифрових ризиків.

ВИСНОВКИ

Результати виконання кваліфікаційної роботи з проблеми цифрових ризиків у міжнародному бізнесідали підстави для таких висновків:

Цифрові ризики – економічна категорія, що відображає специфіку невизначеності та конфліктності в умовах цифрової економіки. Вони виникають через збої у роботі цифрових технологій та інструментів, що застосовуються в управлінні та функціонуванні компаній. Отже, сутність і природа цифрових ризиків полягають у наявності невизначеностей та загроз, що виникають у результаті використання цифрових технологій у міжнародному бізнесі. Ці потенційні збої впливати на ефективність функціонування компаній в умовах цифрової економіки.

Досліджено види цифрових технологій, що використовуються в сучасному бізнес-середовищі.Аналізуючи світовий досвід цифрової трансформації національних економік, виділяють різні ризики та загрози для міжнародного бізнесу, за різними критеріями. Це перш за все вразливість Інтернету речей до кібератак, проблеми з безпекою хмарних платформ, потенційні вразливості у технології блокчейн, ризики, пов’язані з використанням імпортної мікроелектроніки тощо. Існує багато різних класифікацій цифрових ризиків, однак вони мають спільну мету – систематизувати потенційні загрози та визначити методи їх оцінки та управління, що дозволяє ефективно мінімізувати негативний вплив на бізнес-процеси та безпеку компаній.

Критично важливим етапом у стратегічному управлінні міжнародним бізнесом є процес оцінки ризиків. Методи оцінки ризиків включають як кількісні, так і якісні підходи.Для кожного методу є реальні приклади застосування. Вибір оптимальних інструментів для оцінки ризиків безпосередньо залежить від низки критеріїв, які забезпечують ефективність і релевантність обраного методу в конкретному контексті. Це перш за все ціна,

адаптивність,відповідність міжнародним стандартам, які є ключовими для правильного вибору методу оцінки ризиків.

Ідентифікація ризиків є важливим етапом управління цифровими бізнес-ризиками. Даний процес вимагає докладного аналізу для визначення ситуацій та потенційних загроз, які можуть впливати на досягнення цілей міжнародної компанії. У міжнародному бізнесі цей процес ґрунтується на різних методах, таких як огляд бізнес-процесів, аналіз зацікавлених сторін, застосування досвіду, використання технік та інструментів, сценарне планування та експертна оцінка. Аналіз цифрового ризику включає перевірку ймовірності та наслідки кожного ризику, що дозволяє компанії вибрати пріоритети для управління. Оцінка цифрових ризиків передбачає процес визначення можливості та впливу потенційних цифрових ризиків на досягнення загальних цілей міжнародного бізнесу, а також рівня їхньої важливості для організації. Процес оцінки ризиків виконується шляхом проведення оцінювання ризиків за допомогою різних інструментів і методів. Беручи до уваги фактори та особливості оцінки ризиків, сучасні міжнародні компанії застосовують ряд методів та їх інструментарій з метою проведення точного аналізу цифрових ризиків для бізнесу, починаючи зі звичайного опитувальника для спеціалістів підприємств та компаній, закінчуючи спеціальними програмними забезпеченнями для подальшого обрахування рівня ризиків.

Цифрові ризики мають колосальний вплив, переважно негативного характеру, на ведення бізнесу на міжнародному рівні. Загалом, вони здатні на припинення або уповільнення бізнес-процесів, що призводить до витоку конфіденційної інформації через хакерські атаки або внутрішні помилки та знижує конкурентоспроможність компанії; їх поява призводить до судових розглядів та позовів через витік особистих даних клієнтів; призводять до втрати репутації на міжнародному ринку, адже бізнеси, які зазнали кібератаки, стикаються з ризиком втрати клієнтської бази та погіршенням своїх позицій на ринку; стають причиною збитковості бренду, оскільки атаки за допомогою програм-вимагачів можуть зупиняти роботу бізнесу на тривалий час, що

призводить до значних фінансових втрат; стають причиною порушення роботи систем, а відповідно, й погіршення та призупинення роботи самої компанії.

Сучасні стратегії управління цифровими ризиками у міжнародних компаніях охоплюють широке використання різноманітних інструментів, таких як програмне забезпечення та цифрові технології. Ці інструменти спрямовані на детальне вивчення, ідентифікацію, оцінку, аналіз впливу та прогнозування наслідків цифрових ризиків у міжнародному бізнесі, а також на подальше удосконалення діяльності компаній.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Огляд глобальних ризиків 2025 року / Аналітика / Адвокатське об'єднання AZONES. *Адвокатське об'єднання AZONES*. URL: https://azones.law/analytics/oglyad-globalnyh-ryzykiv-2025-roku/ (дата звернення: 06.04.2025).

2. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. *Вісник Дніпропетровського університету. Серія «Менеджмент інновацій».* Випуск 4. Дніпропетровськ. 2015. С. 9-18.

3. Артемчук М. Д. Цифровізація бізнес-процесів як фактор зниження ризиків у кризових умовах. *Здобутки економіки: перспективи та інновації*. 2025. №15. С. 1-22.

4. Білоцерківець В. В., Завгородня О. О., Лебедєва В. К. та ін. Міжнародна економіка. Підручник/ За ред. А. О. Задої, В. М. Тарасевича. Київ: Центр учбової літератури. 2012.386 с.

5. Бобось О. Л. Інноваційні стратегії управління ризиками для забезпечення захисту бізнесу. *Право та державне управління*. *Серія: економічні науки.*2023. № 4. Київ. С. 349-354.

6. Братюк В.П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9. С. 421–427.

7. Бріньолфссон Е., Макафі Е. Друга епоха машин [Текст]: робота, прогрес та процвітання в часи надзвичайних технологій: пер. з англ.Київ: К.FUND, 2016. 233 с.

8. Буряченко А. Є., Куць Н. В. Застосування методів багатокритеріального аналізу у стратегічному плануванні діяльності фінансових установ. *Збірник праць з економіки*. Випуск 3. Київ. 2017. С. 224-236.

9. Величко К.Ю., Цибульська Є.І., Овчаренко К.В. Трансформація бізнес-моделей суб'єктів економічних відносин в цифровій економіці. *Вчені записки ХГУ «НУА».* Том XXIX. 2022. С. 157–170.

10. Вергал К. Ю. Загрози та ризики цифрової трансформації економіки. *Вісник Хмельницького національного університету.* 2020. № 4. Том 3.С. 294-298.

11. Вергун В.А., Карп В.С. Виклики і загрози у сучасному міжнародному бізнесі. Видавництво: ВАДЕКС, 2019. С. 336–344.

12. Віннікова І.І., Марчук С.В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними.*Економіка та управління підприємствами.* 2018.Випуск 5 (16). С. 110-114.

13. Вітлінський В.В. Аналіз, оцінка й моделювання ризику: монографія. Київ: ДЕМІУР. 1996. 212 с.

14. Вітлінський В.В., Скіцько В.І. Ризик у цифровій економіці. *EconomicsLetters*. 2018. № 163. С. 6-9.

15. ВолосовичС., КлапківЛ. Детермінанти виникнення та реалізації кіберризиків. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 3. С. 101-115.

16. ГорбатюкМ. Вплив діджиталізації на темпи розвитку міжнародного бізнесу. *Розвиток підприємництва як фактор росту національної економіки*. 2022. №21. С. 30.

17. Гражевська Н. І., Чигиринський А.М. Цифрова трансформація економіки в умовах посилення глобальних ризиків і загроз. *Економіка та держава.* 2021. № 8. С. 53–57.

18. Грибіненко О. Діджиталізація економіки в новій парадигмі цифрової трансформації. *Міжнародні відносини. Серія «Економічні науки»*. 2018. № 16. С. 35-37.

19. Гусєва О.Ю., Легомінова С.В. Діджиталізація – як інструмент удосконалення бізнес-процесів, їх оптимізація. *Економіка. Менеджмент. Бізнес.* 2018. №1 (23). С. 33–39.

20. Дергачова В.В, Воржакова Ю.П., Хлебінська О.І. Організація бізнес-процесів в умовах цифровізації. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм.* 2021. № 14. С. 60–68.

21. Дергачова Г.М., Колешня Я.О. Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології. *Економічний вісник НТУУ «КПІ».* 2020. № 17. С. 280–290.

22. Дубас. А. С., Смирнов С. А. Прийняття рішень за неточними оцінками на основі MAUT. Математичні методи комп'ютерного моделювання та кібернетичної безпеки. Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених. № 3. Київ. 2018. С. 51-54.

23. Дюгованець О. М. Комплексний аналіз управління ризиками в галузі міжнародного бізнесу. *Науковий вісник Ужгородського національного університету.Серія: Міжнародні економічні відносини та світове господарство.* 2016. Вип. 6(1). С. 92-97.

24. Дюгованець О.М. Підвищення ефективності управління ризиками фірми в умовах нестабільності. Фірма в умовах глобальної нестабільності: виклики, можливості та ризики нової економіки: [кол. монографія]. Ужгород: АУТДОР-ШАРК, 2015. С. 193–310.

25. Дюк Р. І. Кіберризики в діяльності фінансових установ в умовах цифровізації. *Фінансові інструменти сталого розвитку держави в умовах системної економічної науки.* 2024.Випуск 12. Київ. С. 297-304.

26. Заяць Д. Ф., Кицюк І. В. Роль кібербезпеки в міжнародних економічних відносинах. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. Випуск 53. Львів. 2024. С. 11-19.

27. Зварич Р., Дудник Ю., Гомотюк В., Боднар С. Ризик-менеджмент цифрової трансформації в умовах пандемії. *Вісник Економіки*. 2022. Вип. 1. С. 38–53.

28. Карчева Г. Т., Огородня Д. В., Опенько В. А. Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. *Фінансовий простір*. 2017. № 3. С. 13-23.

29. Кифяк В. Інституційне забезпечення управління ризиками бізнесу в умовах цифровізації. *Проблеми інноваційно-інвестиційного розвитку*. 2022. № 28. С. 85-98.

30. Коломоєць Є. Цифрова трансформація бізнесу як основа підвищення його конкурентоспроможності.*Сталий розвиток економіки*. 2024. № 4 (51). С. 72-80.

31. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні і у світі. *Економіка. Фінанси. Менеджмент*. 2016. № 6. С.106–107.

32. Корват О. В. Управління ризиками в цифрових бізнес-екосистемах. *Збірник доповідей НДІ правового забезпечення інноваційного розвитку НАПрН України*. Харків. 2023. С. 176-179.

33. Коробка С.В.Особливості управління бізнес-ризиками малих підприємств в умовах війни. *Проблеми сучасних трансформацій. Серія економіка і управління*. 2023. № 7. С. 171-206.

34. КравченкоМ. О., СалабайВ. О. Роль цифрових трансформацій бізнес–процесів підприємств. *Економічний вісник НТУУ «КПІ»: збірник наукових праць.* 2023. № 26. С.143–158.

35. Ксьонжик І. В., Жовта Н., Павліна А.Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. *Економічні науки. Збірник статей*. Випуск 15. Тернопіль. 2021. С. 57-63.

36. Липов В., Ушенко Н. Вплив платформізації на розвиток ринку відновлювальної енергетики в україні: ризики та перспективи розвитку. *Modeling the development of the economicsystems*,2023. № 4. С. 244–251.

37. Лісова Р. М. Вплив діджиталізації на бізнес-моделі: етапи та інструменти цифрової трансформації. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство.* 2019. № 24 (2). С. 114-118.

38. Ляшенко В. І. Цифрова модернізація економіки України як можливість проривного розвитку: монографія; НАН України, Ін-т економіки пром-сті. Київ, 2018. 252 с.

39. МельничукГ., Марченко О. Окремі аспекти цифровізація бізнес-процесів підприємства в сучасних умовах. *Збірник наукових праць Державного податкового університету*. 2021.№. 1. С. 169–185.

40. Мосумова А. К., Селезньова Г. О., Гагарінов О. В. Цифровізація бізнесу: міжнародний досвід. *Український журнал прикладної економіки та техніки.* 2024. Том 9. № 2. С. 323–328.

41. НайдьоноваЛ. А. Цифрові ризики в умовах дистанційної освіти в часи пандемії: Наукова доповідь на методологічному семінарі НАПН України «Актуальні проблеми психологічної протидії негативним інформаційним впливам на особистість в умовах сучасних викликів» 8 квітня 2021 р. *Вісник Національної академії педагогічних наук України*. 2021. № 1(3). С. 1-4.

42. Панченко Є. Г. Цифровізація міжнародного бізнесу: еволюція, інструменти, ризики. *Економіка та підприємництво*: зб. наук. пр. М-во освіти і науки України, Київ. нац. екон. ун-т ім. Вадима Гетьмана; [редкол.: І. М. Рєпіна (голов. ред.) та ін.]. Київ: КНЕУ, 2023. Вип. 50. С. 219–232.

43. Піжук О. І. Цифрова трансформація економіки України: обмеження та можливості: монографія / Ун-т ДФС України. Ірпінь, 2020. 504 с.

44. Приказюк Н. В., Гуменюк Л. С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка*. № 4. 2020. DOI: 10.32702/2307-2105-2020.4.6 (дата звернення 06.04.2025).

45. Райхлінг П., Перерва П.Г. Оцінювання ризиків в цифровій економіці. *Цифрова трансформація та цифрова економіка в умовах воєнного стану:аспекти інтелектуальної власності:*зб. матеріалів 5-ї Всеукр. наук.-практ. конф. з проблем економіки інтелектуальної власності, 27 травня 2022 р. / Наук.-дослід. ін-т інтелектуальної власності НАПрН України. Київ: Інтерсервіс, 2022. С. 181-186.

46. СаврасІ. З., ФединецьН. І. Цифровізація та інноваційний розвиток підприємства: тенденції, проблеми та перспективи. *Вісник ЛТЕУ.* Економічні науки. 2023. Вип. 74. С. 108–114.

47. Семчук Ж., Іваш А., Хоростіль О., Вовк Ю., Хміль Ю., Підгірняк О. Роль цифрових технологій у трансформації бізнес-моделей сучасних підприємств. *Академічні візії.* 2024. Випуск 28. С. 1-8.

48. Тарасюк М. В. Інновації в глобальній цифровій сфері: оцінка трансформацій. *Актуальні проблеми міжнародних відносин*. 2017. Вип. 131. С. 94-110.

49. Тимохова Г.Б., Кудінова М.М. Особливості формування цифрових стратегій розвитку. *Економіко-правові аспекти господарювання: сучасний стан, ефективність та перспективи*: праці VII Міжнар. наук-практ. конф. (Одеса, 25–26 вересня). Одеса, 2022. С. 290–292.

50. Тостоган Є. Г., Гальчинський Л. Ю. Вибір інструментів оцінювання кіберризиків для організацій на основі багатокритеріального аналізу.XXII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених теоретичні і прикладні проблеми фізики, математики та інформатики. 2024. № 22. С. 176–178, URL: https://ela.kpi.ua/handle/123456789/69948 (дата звернення: 01.04.2025).

51. Цифрова економіка: Вплив інформаційно-комунікаційних технологій на людський капітал та формування компетентностей майбутнього: монографія / Л.Антонюк та ін.; за ред. АнтонюкЛ., ІльницькогоД., СевастюкА. Київ: КНЕУ, 2021. 337 с.

52. Хандій О.О., Шамілева Л.Л. Вплив цифрових трансформацій на економіку та сферу праці: соціально-економічні ризики та наслідки. *Економічний вісник Донбасу.* 2019. № 3 (57). С. 181-188.

53. Хаустова М.Г. Вигоди, ризики та проблеми цифровізації суспільства: загальнотеоретичний аспект.*Аналітичне-порівняльне правознавство*/ редкол.: Ю. М. Бисага (голов. ред.), В. В. Заборовський, Д. М. Бєлов, С. Б. Булеца та ін.; ДВНЗ «УжНУ». Ужгород, 2023. №5. С. 753-759.

54. ЧабанюкЄ. М., Андрощук І. О. Трансформація сучасних методів та інструментів управління сучасними підприємствами в контексті викликів цифровізації. *Центральноукраїнський науковий вісник. Економічні науки*. 2023. № 9 (42). С. 260-271.

55. Человань С. В. Методи та інструменти управління ризиками при здійсненні інноваційної діяльності. *Review of transport economics and management*. 2022. Випуск №3 (19). С. 189-192.

56. Шваб Л.І. Економіка підприємства: навч. посібник. Київ: Каравела, 2007. 584 с.

57. Шевченко Л. С. Цифрова трансформація бізнесу: сутність, конкурентні переваги і ризики. *Економіка та підприємництво*.2022. Випуск7. Тернопіль. С. 10-15.

58. Шевчук І.Б., Депутат Б.Я., Тарасенко О.Є. Цифровізація та її вплив на економіку України: переваги, виклики, загрози й ризики. *Причорноморські економічні студії.* 2019. Випуск 47-2. С. 173-177. URL: http://bses.in.ua/journals/2019/47_2_2019/34.pdf/ (дата звернення: 01.04.2025).

59. Шишкіна О. В. Механізм управління фінансовими ризиками промислових підприємств: теорія, методологія, практика: монографія Чернігів: ЧНТУ, 2020. 318 с.

60. Шишкіна О. В. Цифрові технології фінансових установ: ризики і перспективи використання. *Актуальні проблеми розвитку економіки регіону*. 2023. Т.2.№ 19. С. 130–143.

61. Alesta. URL: https://alesta.net.ua/blog/nist-cybersecurity-framework-efektivna-osnova-dlya-zahistu-vid-kiberzagroz(дата звернення 27.04.2025).

62. Brauers W.K.M., Zavadaskas E.K.Robustness of MULTIMOORA:a Method for Multi-Objective Optimization. *Informatica*. 2012. Vol. 23. № 1. 1–25, P. 10.

63. Brynjolfsson E., McAfee A. The second machine age: Work, progress, and prosperity in a time of brilliant technologies. 2014. URL: https://psycnet.apa.org/record/2014-07087-000(дата звернення: 11.02.2025).

64. Ganguly S., Harreis H., Margolis B., Rowshankish K. Digitalrisk: Transforming risk management for the 2020. February 2017. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/digital-risk-transforming-risk-management-for-the-2020s (дата звернення: 1.04.2025).

65. Grytsenko A., LypovV. PlatformCooperativism and itsApplication in RenewableEnergy. *Science and Innovation*, 2024. № 20(6), P. 3–17.URL:https://doi.org/10.15407/scine20.06.003

66. Davenport T. The Rise of Analytics 3.0: How to Compete in the Data Economy.2013. URL: https://analyticsconsultores.com.mx/wp-content/uploads/2019/02/The-Rise-of-Analytics-3.0.-How-to-Compete-in-the-Data-Economy-Thomas-H.-Davenport-IIA-2013.pdf (дата звернення: 11.02.2025).

67. Klaus Schwab. Fourth Industrial Revolution. 2016. URL: https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf (дата звернення: 1.04.2025).

68. Lypov, V. V. Industry 4.0 and the Formation of Chains (Networks) Creation of ValueBased on DigitalPlatforms. Visnykekonomichnoi nauky Ukrainy, 2024. № 2 (47), pp. 152-161. DOI: https://doi.org/10.37405/1729-7206.2024.2(47).152-161

69. Negroponte N. Being Digital. NY: Knopf. 1995. 256 p.

70. Nosova O., Lypov V. TransformingCompetitivenessbyIntroducingDigital Platforms. *Journal of World Economy: Transformations&Transitions, ERUDITUS*. 2021. vol. 1(3).

71. Oxford English Dictionary. URL: https://dictionary.cambridge.org/uk/dictionary/english/oxford#google_vignete(дата звернення: 01.04.2025).

72. Tapscott Don. Digital Economy. NewYork: McGraw-Hill. 1994. 368 p.

73. Tirole J. Overcoming adverse selection: How public intervention can restore market functioning. *American Economic Review*. 2012. № 102.P. 29–59.

74. World Economic Forum. The Global Risks Report. 2025.URL: https://www.weforum.org/meetings/world-economic-forum-annual-meeting-2025/ (дата звернення 06.04.2025).

ДОДАТКИ

Додаток А

Схема елементів оцінки ризиків