

ЦИФРОВІ РИЗИКИ В УПРАВЛІННІ РОЗВИТКОМ ПІДПРИЄМСТВА

Плесюк Олексій Степанович

здобувач освіти ступеня доктора філософії,
Черкаський національний університет імені Богдана Хмельницького
ORCID: 0000-0002-9480-9198
plesiu.oleksii422@vu.cdu.edu.ua

Доведено, що кількість цифрових ризиків, інтенсивність їх впливу та ймовірність їх прояву у межах фінансово-господарської діяльності підприємств постійно зростає: природа цифрових ризиків багатогранна, а вплив – системний і масштабний, і тому вони становлять загрозу для функціонування компаній і реалізації стратегічних цілей їх розвитку. Надано аргументи на користь гіпотези, що ефективне управління цифровими ризиками є критично важливим елементом стратегічного планування і функціонального менеджменту. Встановлено, що управління цифровими ризиками є ефективним інструментом для підтримання високого рівня довіри клієнтів, партнерів та інших стейкхолдерів до діяльності компанії, а також є важливим для формування корпоративної віри персоналу у перспективи розвитку підприємства. Узагальнено рейтингові позиції країн за показниками кібербезпеки та цифрового розвитку (у розрізі лідерів та аутсайдерів, станом на початок 2025 року). Конкретизовано перелік основних видів цифрових ризиків, до якого увійшли: фішинг, програми-вимагачі, DDoS-атаки, шкідливе програмне забезпечення, кібервзаємозалежність, геополітичні ризики, дїпфейки, кіберзлочинність. Зроблено припущення, що рівень цифрової грамотності персоналу підприємств суттєво впливає на здатність запобігати цифровим ризикам і мінімізувати їх наслідки для корпоративних ресурсів, ділової репутації. Виявлено, що поєднання технічних рішень, кадрових заходів, правового захисту та стратегічного управління створює основу для зниження цифрових ризиків під час реалізації стратегії розвитку підприємства. Встановлено, що як реакція на активне поширення цифрових ризиків у науці управління та на практиці сформувався окремий функціональний напрям менеджменту організацій – управління цифровими ризиками (digital risk management), метою якого є своєчасна ідентифікація, оцінювання та розробка заходів щодо зниження рівня цифрових ризиків та мінімізації їх кількості. Для професійного виконання завдань цифрового ризик-менеджменту підприємством доцільно об'єднувати зусилля внутрішніх фахівців з безпеки орієнтованого управління і зовнішніх професіоналів з ризик-менеджменту у цифровій сфері, таких як працівники сервісних ІТ-компаній.

Ключові слова: цифровий ризик, цифровізація, цифрова трансформація, управління розвитком підприємства, управління ризиками, управління цифровими ризиками, економічна безпека.

DOI: <https://doi.org/10.32782/bsnau.2025.3.10>

Постановка проблеми у загальному вигляді.

Розвиток підприємства – це тривалий процес, результат якого очікується у майбутньому, а отже, важко піддається точному передбаченню та прогнозуванню. Фактори зовнішнього та внутрішнього середовища, які можуть з'явитися раптово, вимагають від управлінців гнучкості та здатності до адаптації. Цифровізація – це масштабний тренд трансформації підходів до ведення бізнесу, і він охоплює усі види та форми підприємницької діяльності, змінює класичні практики господарювання та формує інноваційні ризики, з якими працівники підприємств часто не вміють або не готові ефективно працювати, демонструючи лише пасивні реакції на їх прояви. З плином часу, цифрові ризики набувають різних форм і проявів, виникають у різних сферах економічного життя підприємства, мають різні та часто непередбачувані наслідки – кадрові, фінансові, інформаційні, репутаційні, матеріальні, тощо. Окрема проблемна траєкторія наукових пошуків – це інструменти управління ризиками. Також увагу дослідників має привернути «подвійна» природа цифрового ризику, який, з одного боку, може призвести до збитків або недоотримання бажаного ефекту, а з іншого навпаки – стати джерелом неочікуваного позитивного результату.

Аналіз останніх досліджень і публікацій.

Цифрові ризики часто виступають об'єктом досліджень у публікаціях, які присвячені питанням безпеки орієнтованого управління підприємствами, формуванню комплексних систем економічної безпеки та підвищенню ефективності функціонування її інформаційної складової [1]. Різні вектори та контексти дослідження цифрових ризиків українськими вченими засвідчують актуальність цього питання, а також різноманітність проявів і можливих наслідків цифрових ризиків для функціонування соціально-економічних систем на мікро та макrorівнях. Наприклад, Гудзь О. Є. вивчає нові інструменти та методи управління ризиками в цифровій економіці, фокусуючи увагу на розвитку ринку страхування та діяльності його учасників [2], Леонов С. В., Семко О. В. розглядають можливості використання інформаційних технологій для управління інформаційними ризиками у проєктах цифрової трансформації бізнесу [3], Новікова О. Ф., Панькова О. В., Шастун А. Д. відстежують проблематику цифрового розвитку під час реалізації заходів щодо подолання ризиків і небезпек в умовах пандемії COVID-19 [4], Поврозник П. П. характеризує особливості інноваційного розвитку підприємництва в Україні під впливом глобальних безпекових викликів

і ризиків цифровізації [5], Прокоф'єва О. В., Беспалова Ю. Ю. фокусують увагу на кібер-ризиках і підходах до управління ними у контексті поширення явищ глобалізації [6], Разумова Г. В., Курносова О. І. зосереджуються на аспекті управління ризиками інвестиційної діяльності в умовах цифрової трансформації [7], Сазонова С. В. цілеспрямовано займається вирішенням завдання ідентифікації ризиків стратегічного управління телекомунікаційними підприємствами на теренах цифрової економіки [8], Степанов В. Ю. узагальнено вивчає питання цифровізації та ризиків цифрової безпеки [9], Хандій О. О., Кобцева Д. А. конкретизують можливості та ризики цифровізації для суб'єктів ринку праці [10], а Швидка О. П., Дзюбенко Л. М. уточнюють перспективи та ризики для підприємств малого бізнесу у процесі обрання їх очільниками інноваційних бізнес-моделей функціонування та розвитку в умовах цифрової трансформації [11].

Невирішені частини загальної проблеми, які досліджуються у статті. Сфокусованість досліджень сучасних вчених на окремих аспектах існування або впливу цифрових ризиків на процеси діяльності підприємств звужують об'єкт наукових пошуків. У цій статті буде здійснено спробу комплексно підійти до питання існування та прояву впливу цифрових ризиків в управлінні розвитком підприємства.

Формулювання цілей статті. Метою дослідження є конкретизація та узагальнення цифрових ризиків, які є найбільш відчутними в управлінні розвитком підприємства, та які можуть справити найбільший деструктивний вплив на економічні показники його діяльності.

Методи дослідження. Для конкретизації видів і впливу цифрових ризиків на процес управління розвитком підприємства було використано такі методи наукового дослідження, як контент-аналіз фахової економічної літератури, який дозволив з'ясувати можливості своєчасної ідентифікації ризиків за допомогою використання методичних і аналітичних прийомів і практик; метод синтезу та узагальнення – для розроблення пропозицій щодо протидії цифровим ризикам; метод систематизації та графічний метод – для підготовки та демонстрації числового матеріалу у межах проведення наукових пошуків.

Результати дослідження. Увага менеджменту підприємницьких структур в усьому світі привернута до вирішення проблеми існування та мінімізації цифрових ризиків такими методами, які б не знижували темпи розвитку бізнесу та не ставали на заваді науковому прогресу. Перрі Дж. зазначає, що впродовж 2024 року спостерігалось постійне зростання масштабів і інтенсивності прояву цифрових ризиків географічно – у кожному регіоні, та функціонально – у кожній сфері. Починаючи з ризиків, які походять від публічного управління та геополітики до ризиків, які виникають від фінансової та ідеологічної мотивації, загрози для компаній лише посилюються із поширенням дедалі досконаліших цифрових технологій, і ситуація у 2025 році загостриться для усіх організацій, і особливо для тих, які не готові до безпекоорієнтованого розвитку у період тотальної цифровізації бізнесу [12].

Цифрові ризики чинять суттєвий вплив на управління розвитком підприємства, оскільки їх є джерелами виникнення великої кількості загроз пов'язаних із цифровою трансформацією бізнесу. Вплив цифрових ризиків можна на розвиток підприємства можна узагальнити та систематизувати за об'єктами їх впливу. Так, значна частина цифрових ризиків пов'язана з кібербезпекою ресурсів суб'єкта господарювання. Це викликало появу такого терміну, як кібер-ризик. Гудзь О.Є. пропонує дефініцію: кібер-ризик – це ризик, що генерується використанням: телекомунікаційного обладнання, програмного забезпечення, локальних і Інтернет-мереж, розрахунково-платіжних систем, систем інтернет-торгівлі, промислових систем менеджменту, а також це ризик, що пов'язаний з накопиченням, зберіганням, передачею і використанням персональних даних [2, с. 5]. Такі негативні явища, як зловмисні хакерські атаки, витоки цифрових даних, несанкціонований доступ до корпоративних інформаційних систем і мереж з корисливою метою провокують ризики втрати результатів інтелектуальної власності, нематеріальних ресурсів, призводять до перевитрат фінансових активів та викликають падіння рівня довіри клієнтів до компанії. Такі обставини суттєво ускладнюють реалізацію стратегії розвитку підприємства та досягнення його цілей щодо нарощення економічного потенціалу та збереження інтелектуального капіталу.

Проблема кіберзлочинності та кібербезпеки, як ризиків цифрової трансформації країни, є актуальною в Україні, оскільки в умовах війни кіберзлочинців активно залучають до зламу урядових серверів, дезінформування населення, використання при цьому фейкових профілів у соцмережах, тощо. Поширенням на сьогодні є кібершахрайство. Після повномасштабного вторгнення росії кількість кіберзлочинів різко зросла [5, с. 119]. Ефективним інструментом для пом'якшення наслідків кібератак Прокоф'єва О. В., Беспалова Ю. Ю. вважають страхування кіберризиків, оскільки воно забезпечує фінансовий захист організацій, покриваючи витрати, пов'язані з кіберінцидентами [6]. Однак, така практика не надто поширена в Україні.

Сазонова С. В. у своєму дослідженні згадує у якості інформаційного інструменту Національний індекс кібербезпеки (National Cyber Security Index, NCSI) – глобальний індекс, який вимірює готовність країн запобігати кіберзагрозам і керувати кіберінцидентами (рис. 1).

NCSI також є базою даних із загальнодоступними доказовими матеріалами та інструментом для створення потенціалу національної кібербезпеки [8, с. 10]. Центром науки та міжнародних відносин Роберта та Рене Бельфера у якості статистичного інструменту для аналізу стану кібербезпеки держави було розроблено Національний індекс сил кібербезпеки (National Cyber Power Index, NCPI).

Кадровий ресурс підприємства відіграє вагомe значення у поширенні цифрових ризиків. Персонал, що має високий рівень цифрової грамотності, може ефективно зменшувати ймовірність реалізації цифрових ризиків на практиці, попереджувати їх виникнення, управляти ними та їх наслідками без залучення зовнішньої допомоги від

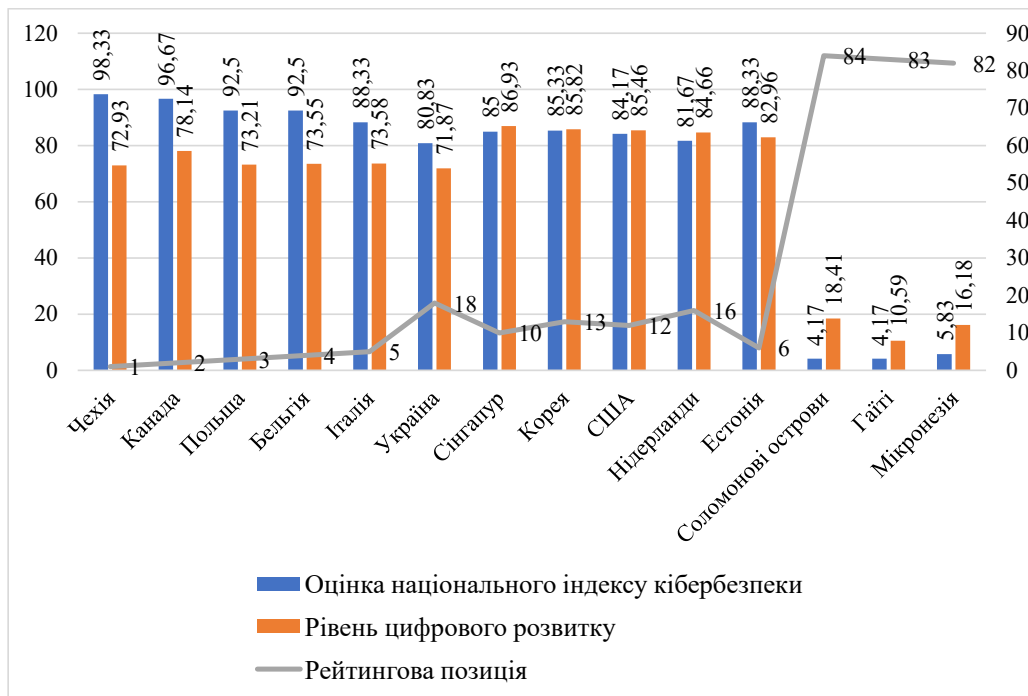


Рис. 1. Рейтингові позиції країн за показниками кібербезпеки та цифрового розвитку (лідери та аутсайди, станом на початок 2025 року)

Джерело: узагальнено автором за даними [13]

спеціалізованих фірм. Водночас, невміння працівників забезпечити дані, необхідні для коректної роботи, використання ними робочих гаджетів для особистих цілей, спілкування з робочих питань незахищеними комунікаційними каналами провокує виникнення додаткових загроз для компанії, її корпоративних ресурсів, стейкхолдерів, чиї інтереси можуть постраждати від «цифрової недбалості» та необачності працівників. Отже, рівень цифрової грамотності персоналу, опір змінам, пов'язаних із цифровізацією, з боку працівників, тощо, можуть суттєво загальмувати запровадження цифрових ініціатив та мінімізувати можливості управлінського впливу на стратегічний розвиток підприємства.

Операційні цифрові ризики, які супроводжують бізнес-процеси суб'єкта господарювання, виникають внаслідок впровадження сучасних цифрових технологій для автоматизації та пришвидшення операцій, які виконуються у межах щоденної фінансово-господарської діяльності підприємства. Запровадження комплексних цифрових екосистем у бізнесі може супроводжуватися затримками та збоями роботі обладнання, втратою даних, помилками під час аналітичного опрацювання відомостей або оцінювання ризиків, неправильним налаштуванням роботи цифрових інформаційних систем, в результаті чого можуть бути поставлені некоректні цілі для розвитку підприємства або унеможливлені їх досягнення.

У правовому полі функціонування бізнесу цифрові ризики тісно пов'язані з юридичними та регуляторними загрозами. Недотримання вимог цифрового законодавства, наприклад, щодо збирання, збереження та захисту персональних даних, отримання дозволів на їх поширення з комерційною метою, тощо, може призве-

сти до фінансових, матеріальних, репутаційних втрат, наприклад, до штрафів, обмежень ділової активності підприємства, що суттєво загальмує процеси його розвитку та створить імідж недобросовісного бізнесу на ринку. Водночас, нехтування можливостями цифровізації, надмірні стриманість і розважливість менеджменту підприємства щодо запровадження цифрових технологій, нездатність суб'єкта господарювання адаптуватися до темпів поширення цифрових змін призведуть до втрати конкурентних позицій на ринку, що неодмінно означатиме суттєву загрозу для успішної реалізації стратегії розвитку у перспективі.

Таким чином, цифрові ризики суттєво впливають на успішність реалізації класичних функцій менеджменту, таких як планування, організація, контроль процесу розвитку підприємства. Ефективна робота з цифровими ризиками, тобто ефективне управління ними вимагає від керівництва компанії адаптації їх стратегії до цифрових трансформацій та вжиття управлінських заходів щодо посилення систем захисту даних та підвищення рівня цифрової грамотності персоналу, зокрема, через мотиваційні та освітні інструменти.

Степанов В.Ю. відзначає: «Цифровізація потребує нового підходу до стратегічного планування – розробки цифрової стратегії. Окрім бачення ролі, яку підприємства планують грати на цифрових ринках майбутнього, цифрова стратегія включає конкретні заходи та проекти цифрової трансформації, це план дій щодо реалізації цифрової трансформації для підприємства. Вона включає розвиток цифрових бізнес-процесів, цифрового маркетингу, цифрових продажів, а також розробку цифрових бізнес-моделей. Зокрема, в розробці цифрової стратегії беруть участь усі відділи підприємства» [9, с.57]. Не

остання роль у цьому процесі має відводитись і спеціалістам з управління ризиками.

Фахівці української асоціації ризик-менеджерів назвали ризики, пов'язані з інформаційною безпекою, другим номером у ТОП-10 операційних ризиків підприємств за результатами 2024 року. Причиною цього була цифровізація, оскільки кібератаки та злами інформаційних систем компаній стали можливими завдяки активному використанню мережі Інтернет у бізнес-цілях [14].

До переліку найпоширеніших цифрових ризиків для функціонування та розвитку сучасних підприємств можна внести: фішинг, спрямований на отримання закритої інформації та подальше її злочинне використання, програми-вимагачі, які призначені для блокування доступу до даних підприємства до моменту отримання фінансової вигоди за його розблокування, DDoS-атаки, що перезавантажують сервери та сайти і унеможливають, таким чином, здійснення поточних операцій компанії, зловмисне програмне забезпечення, націлене на шпигування за діяльністю суб'єкта господарювання та його персоналом з метою подальшого використання отриманої інформації з особистою вигодою [14]. Більш масштабними та глобальними з позиції впливу на економіку в цілому можна вважати ризик кібервзаємозалежності, геополітичні кіберризики, гібридну війну, дії організованої кіберзлочинності, ризики використання криптовалют, кібернетичний активізм, дезінформацію, генеративний штучний інтелект і дипфейки, шахрайські дії з боку третіх сторін та ризик для цілісності компаній, посилення правил і контролю за цифровою інформацією (NIS2 та DORA – вимоги до локалізації даних і нагляду за критично важливими даними) [12].

Поширення цифрових ризиків набуло такого масштабу, що у відповідь на виклики, які вони за собою несуть, виник окремий напрям менеджменту – управління цифровими ризиками (Digital Risk Management). Управління цифровими ризиками – це процес, який реалізується через механізми ідентифікації, оцінювання та «пом'якшення» впливу ризиків, пов'язаних із цифровими технологіями, великими даними та онлайн-діяльністю підприємства. Паралельно існує та використовується і інший термін – управління ризиками цифрової безпеки – як процес, за допомогою якого особи, які приймають рішення, враховують у плануванні та здійсненні своєї діяльності фактори, які можуть вплинути на досягнення їхніх цілей [9, с.59].

Управління цифровими ризиками є ефективним інструментом для підтримання високого рівня довіри клієнтів, партнерів та інших стейкхолдерів до діяльності компанії, а також є важливим для формування корпоративної віри персоналу у перспективи розвитку підприємства. Його самостійними функціональними напрямками, що потребують власних суб'єктів реалізації – менеджерів, та виділених ресурсів, мають бути: захист конфіденційної інформації від втрати та несанкціонованого доступу; дотримання відповідності цифрового підприємництва регулятивним вимогам і нормам законодавства та забезпечення цілісності й доступності цифрових активів для використання їх з метою

досягнення поточних і стратегічних цілей розвитку підприємства.

Основними інструментами управління цифровими ризиками на рівні менеджменту суб'єкта господарювання є програмне забезпечення та послуги цифрового ризик-менеджменту, які надаються зовнішніми організаціями, наприклад, сервісними ІТ-компаніями. Послуги з управління цифровими ризиками призначені для виявлення, аналізу, мінімізації та моніторингу цифрових ризиків, з якими стикаються компанії під час здійснення цифрових операцій. Цифрові ризики можуть виникати при використанні хмарних і локальних сховищ даних, супроводжують діяльність як малих і середніх, так і великих підприємств. Цифрові ризики, які виникають у таких галузях, як банківська справа, фінансові послуги та страхування, інформаційні технології та телекомунікації, охорона здоров'я, роздрібна торгівля, виробництво та інші галузі, охоплюють і інші, суміжні сфери, примножуються та інтенсифікуються для підприємств, які є активними користувачами цифрових послуг із різних сегментів.

Висновки. Дослідження проблемних аспектів питання існування та прояву негативних наслідків цифрових ризиків у процесі управління розвитком сучасних підприємств дало змогу зробити наступні висновки та припущення.

1. Сучасний стан цифровізації в Україні та її впливу на підприємницьку діяльність та розвиток суб'єктів господарювання характеризується поширенням цифрових ризиків. У 2024–2025-у роках зафіксовано зростання кількості і частоти прояву та збільшення негативних наслідків цифрових ризиків у різних локаціях і сферах економічного життя. Джерелами їх походження переважно є державне регулювання, публічне управління та адміністрування бізнесу, геополітична ситуація, поведінка персоналу та дії конкурентів. Відсутність комплексних систем ризик-менеджменту та управління економічною безпекою погіршує ситуацію, адже цифрові ризики деструктивно впливають на розвиток підприємства, унеможливаючи досягнення його стратегічних цілей.

2. Серед основних та найбільш поширених видів цифрових ризиків (паралельно вживаються терміни кібер-ризик і ризик кібернетичної безпеки) належать: кіберзлочинність, викрадення та псування даних, хакерські атаки, втрата інтелектуального капіталу, помилки у налаштуванні цифрових екосистем підприємств, недотримання вимог законодавства щодо збереження та несумлінного використання персональних даних, фішингові атаки, дипфейки, шкідливе програмне забезпечення.

3. Як реакція на активне поширення цифрових ризиків у науці управління та на практиці сформувався окремий функціональний напрям менеджменту організацій – управління цифровими ризиками (digital risk management). Його метою є своєчасна ідентифікація, оцінювання та розробка заходів щодо зниження рівня цифрових ризиків та мінімізації їх кількості. Для професійного виконання завдань цифрового ризик-менеджменту підприємствам доцільно об'єднувати зусилля внутрішніх фахівців з безпекою орієнтованого управління

і зовнішніх професіоналів з ризик-менеджменту у цифровій сфері, таких як працівники сервісних ІТ-компаній.

4. Існування цифрових ризиків має знайти відображення у розробці цифрової стратегії розвитку бізнесу. Вона повинна містити стратегічні орієнтири щодо цифровізації бізнес-процесів підприємства, зокрема, таких операцій, як маркетинг, продажі, логістика, фінансові розрахунки, інформаційний обмін та діловодство, мати

комплексний характер та охоплювати усі відділи суб'єкта господарювання, активно інтегруючи їх до цифрової екосистеми компанії.

Перспективи подальших досліджень полягають у розробці основ стратегії цифрового розвитку для сучасного підприємства із врахуванням обмеженості ресурсів українського бізнесу у воєнний час і ризиків цифровізації господарських та управлінських процесів.

Список використаної літератури:

1. Cherevko O., Nazarenko S., Zachosova N., Nosan N. Financial and economic security system strategic management as an independent direction of management. *The 8th International Conference on Monitoring, Modeling & Management of Emergent Economy (M3E2 2019)*. 2019. M3E22019. DOI: <https://doi.org/10.1051/shsconf/20196503001> (дата звернення: 07.05.2025).
2. Гудзь О. Є. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес*. 2019. № 3. С. 4–12.
3. Леонов С. В., Семко О. В. Інформаційна технологія управління інформаційними ризиками для проєктів цифрової трансформації бізнесу. *Управління розвитком складних систем*. 2023. Вип. 56. С. 64–69.
4. Новікова О. Ф., Панькова О. В., Шастун А. Д. Цифровий розвиток в процесах подолання ризиків та небезпек в умовах пандемії COVID-19. *Бізнес-навігатор*. 2020. Вип. 5. С. 93–97.
5. Поврозник П. П. Особливості інноваційного розвитку підприємництва в Україні в контексті глобальних безпечових викликів та ризиків цифровізації. *Міжнародний науковий журнал "Інтернаука". Серія: Економічні науки*. 2023. № 8. С. 113–123.
6. Прокоф'єва О. В., Беспалова Ю. Ю. Кібер-ризик та управління ними в умовах глобалізації та цифрової трансформації. *Ефективна економіка*. 2024. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2024_5_89 (дата звернення: 07.05.2025).
7. Разумова Г. В., Курносорова О. І. Управління ризиками інвестиційної діяльності в умовах цифрової трансформації. *Бізнес Інформ*. 2024. № 3. С. 96–101.
8. Сазонова С. В. Ідентифікація ризиків стратегічного управління телекомунікаційними підприємствами в умовах цифрової економіки. *Причорноморські економічні студії*. 2021. Вип. 72 (2). С. 7–12.
9. Степанов В. Ю. Цифровізація та ризики цифрової безпеки. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2024. Вип. 1. С. 55–61.
10. Хандій О. О., Кобцева Д. А. Можливості та ризики цифровізації для суб'єктів ринку праці. *Вісник економічної науки України*. 2023. № 1. С. 70–76.
11. Швидка О. П., Дзюбенко Л. М. Інноваційні бізнес-моделі в умовах цифрової трансформації: перспективи та ризики для малого бізнесу. *Фінанси України*. 2024. № 11. С. 118–128.
12. Parry J. The top 10 digital risks for organisations in 2025. URL: https://www.controlrisks.com/our-thinking/insights/the-top-10-digital-risks-for-organisations-in-2025?utm_referrer=https://www.google.ru (дата звернення: 07.05.2025).
13. National Cyber Security Index. URL: <https://ncsi.ega.ee/country/ua/> (дата звернення: 07.05.2025).
14. Бабич С. Ризики, пов'язані з інформаційною безпекою, – №2 серед ТОП-10 операційних ризиків 2024 року. URL: <https://ukrarm.org/riziki-pov-yazani-z-informacijnoju-bezpekoju-2-sered-top-10-operacijnih-rizikiv-2024-roku/> (дата звернення: 07.05.2025).

References:

1. Cherevko O., Nazarenko S., Zachosova N., Nosan N. (2019). Financial and economic security system strategic management as an independent direction of management. *The 8th International Conference on Monitoring, Modeling & Management of Emergent Economy (M3E2 2019)*. M3E22019. DOI: <https://doi.org/10.1051/shsconf/20196503001> (accessed on May 7, 2025).
2. Hudz O. Ye. (2019). Rozvytok strakhuvannia: novi instrumenty ta metody upravlinnia ryzykamy v tsyfrovii ekonomitsi [Development of insurance: new tools and methods of risk management in the digital economy]. *Ekonimika. Menedzhment. Biznes – Economics. Management. Business*, no. 3, pp. 4–12.
3. Leonov S. V., Semko O. V. (2023). Informatsiina tekhnolohiia upravlinnia informatsiinymy ryzykamy dlia proiektiv tsyfrovoy transformatsii biznesu [Information technology for managing information risks in business digital transformation projects]. *Upravlinnia rozvytkom skladnykh system – Management of Complex Systems Development*, iss. 56, pp. 64–69.
4. Novikova O. F., Pankova O. V., Shastun A. D. (2020). Tsyfrovyy rozvytok v protsesakh podolannia ryzykiv ta nebezpek v umovakh pandemii COVID-19 [Digital development in the process of overcoming risks and threats in the context of the COVID-19 pandemic]. *Biznes-navigator – Business Navigator*, iss. 5, pp. 93–97.
5. Povroznyk P. P. (2023). Osoblyvosti innovatsiinoho rozvytku pidpriemnytstva v Ukraini v konteksti hlobalnykh bezpekovykh vyklykiv ta ryzykiv tsyfrovizatsii [Peculiarities of innovative entrepreneurship development in Ukraine in the context of global security challenges and digitalization risks]. *Mizhnarodnyi naukovyi zhurnal "Internauka". Seriya: Ekonomichni nauky – International Scientific Journal "Internauka". Series: Economic Sciences*, no. 8, pp. 113–123.
6. Prokofieva O. V., Bespalova Yu. Yu. (2024). Kiber-ryzyky ta upravlinnia nymy v umovakh hlobalizatsii ta tsyfrovoy transformatsii [Cyber risks and their management under globalization and digital transformation]. *Efektivna ekonomika – Effective Economy*, no. 5. Available at: http://nbuv.gov.ua/UJRN/efek_2024_5_89 (accessed on May 7, 2025).

7. Razumova H. V., Kurnosova O. I. (2024). Upravlinnia ryzykamy investytsiinoi diialnosti v umovakh tsyfrovoy transformatsii [Risk management of investment activities in the context of digital transformation]. *Biznes Inform – Business Inform*, no. 3, pp. 96–101.
8. Sazonova S. V. (2021). Identyfikatsiia ryzykiv stratehichnoho upravlinnia telekomunikatsiinykh pidpriemstvamy v umovakh tsyfrovoy ekonomiky [Identification of strategic management risks in telecommunications enterprises under digital economy conditions]. *Prychornomorski ekonomichni studii – Black Sea Economic Studies*, iss. 72 (2), pp. 7–12.
9. Stepanov V. Yu. (2024). Tsyfrovizatsiia ta ryzyky tsyfrovoy bezpeky [Digitalization and digital security risks]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriya: Derzhavne upravlinnia – Bulletin of the National University of Civil Defense of Ukraine. Series: Public Administration*, iss. 1, pp. 55–61.4.
10. Khandii O. O., Kobtseva D. A. (2023). Mozhlyvosti ta ryzyky tsyfrovizatsii dlia subiektiv rynku pratsi [Opportunities and risks of digitalization for labor market entities]. *Visnyk ekonomichnoi nauky Ukrainy – Bulletin of Economic Science of Ukraine*, no. 1, pp. 70–76.
11. Shvydka O. P., Dziubenko L. M. (2024). Innovatsiini biznes-modeli v umovakh tsyfrovoy transformatsii: perspektyvy ta ryzyky dlia maloho biznesu [Innovative business models in the context of digital transformation: prospects, risks for small business]. *Finansy Ukrainy – Finance of Ukraine*, no. 11, pp. 118–128.
12. Parry J. (2025). The top 10 digital risks for organisations in 2025. Available at: https://www.controlrisks.com/our-thinking/insights/the-top-10-digital-risks-for-organisations-in-2025?utm_referrer=https://www.google.ru (accessed on May 7, 2025).
13. National Cyber Security Index. Available at: <https://ncsi.ega.ee/country/ua/> (accessed on May 7, 2025).
14. Babich S. (2025). Ryzyky, pov'yazani z informatsiynoyu bezpekoyu, – №2 sered TOP-10 operatsiynykh ryzykiv 2024 roku. [Risks related to information security – No. 2 among the TOP-10 operational risks of 2024]. Available at: <https://ukrarm.org/riziki-pov-yazani-z-informacijnoju-bezpekoju-2-sered-top-10-operacijnih-rizikiv-2024-roku/> (accessed on May 7, 2025).

Oleksii Plesiuk, Ph.D. Degree Applicant, Bohdan Khmelnytsky National University of Cherkasy

DIGITAL RISKS IN BUSINESS DEVELOPMENT MANAGEMENT

It is proven that the number of digital risks, the intensity of their impact and the probability of their manifestation within the financial and economic activities of enterprises are constantly growing: the nature of digital risks is multifaceted, and the impact is systemic and large-scale, and therefore they pose a threat to the functioning of companies and the implementation of their strategic development goals. Arguments are provided in favor of the hypothesis that effective digital risk management is a critically important element of strategic planning and functional management. It is established that digital risk management is an effective tool for maintaining a high level of trust of customers, partners and other stakeholders in the company's activities, and is also important for forming corporate faith of personnel in the prospects for the development of the enterprise. The ranking positions of countries in terms of cybersecurity and digital development indicators (in terms of leaders and outsiders, as of the beginning of 2025) are summarized. The list of main types of digital risks is specified, which includes: phishing, ransomware, DDoS attacks, malware, cyber interdependence, geopolitical risks, deep fakes, cybercrime. It is assumed that the level of digital literacy of enterprise personnel significantly affects the ability to prevent digital risks and minimize their consequences for corporate resources and business reputation. It is found that the combination of technical solutions, personnel measures, legal protection and strategic management creates the basis for reducing digital risks during the implementation of the enterprise's development strategy. It is established that as a reaction to the active spread of digital risks in management science and in practice, a separate functional direction of organizational management has been formed – digital risk management, the purpose of which is the timely identification, assessment and development of measures to reduce the level of digital risks and minimize their number. For a company to professionally perform digital risk management tasks, it is advisable to combine the efforts of internal security-oriented management specialists and external digital risk management professionals, such as employees of IT service companies.

Keywords: digital risk, digitalization, digital transformation, enterprise development management, risk management, digital risk management, economic security.

Дата надходження до редакції: 01.07.2025 р.