КЛАСИФІКАЦІЯ РИЗИКІВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПІДПРИЄМСТВ У КОНТЕКСТІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

CLASSIFICATION OF RISKS OF DIGITAL TRANSFORMATION OF ENTERPRISES IN THE CONTEXT OF ECONOMIC SECURITY

УДК 658.5:005.334:330.131.7
DOI: https://doi.org/10.32782/dees.18-31

Фісуненко П.А.
д.е.н., доцент,
професор кафедри девелопменту нерухомості,
фінансів, обліку та маркетингу,
Навчально-науковий інститут
«Придніпровська державна академія будівництва та архітектури»
Українського державного університету науки і технологій
Булєєв Ю.С.
аспірант,
Навчально-науковий інститут
«Придніпровська державна академія будівництва та архітектури»
Українського державного університету науки і технологій

Fisunenko Pavlo
Educational and Research Institute
"Prydniprovska State Academy
of Civil Engineering and Architecture",
Ukrainian State University of Science
and Technology
Bulieiev Yurii
Educational and Research Institute
"Prydniprovska State Academy
of Civil Engineering and Architecture",
Ukrainian State University of Science
and Technology

У публікації досліджено спектр ризиків, що виникають у процесі цифрової трансформації підприємств та можуть порушувати їхню стійкість, стабільність і функціональну цілісність. Визначено ключові загрози, які негативно впливають на фінансову, інформаційну, технічну, управлінську та кадрову складові діяльності суб'єктів господарювання. Здійснено критичний огляд сучасних наукових підходів, проведено узагальнення практичних кейсів. Результатом дослідження є авторська класифікація ризиків за джерелами формування, рівнями прояву та об'єктами впливу. Особливу увагу приділено ідентифікації ризиків, що прямо чи опосередковано загрожують стратегічним і тактичним параметрам безпеки суб'єктів господарювання в умовах цифровізації. Запропоновано концептуальний підхід до їх систематизації як інструменту посилення антикризової та адаптивної спроможності підприємства.
Ключові слова: *цифрова трансформація, економічна безпека підприємства, систематизація ризиків, цифрові загрози, стратегічна стійкість підприємства, ризик-орієнтоване управління, адаптивність бізнесу.*

The active integration of digital technologies into enterprise operations creates not only new opportunities but also a broad spectrum of threats and challenges. Ensuring the long-term viability and sustainability of enterprises in the context of digital transformation requires a clear understanding of the risks it entails. These risks are often hybrid in nature, combining technological, financial, informational, organizational, legal, and reputational components. The interaction of these factors can undermine enterprise functionality and disrupt critical infrastructure and decision-making processes. The complexity of the issue lies in the pervasive character of digital transformation, which influences all levels of business activity - from operational routines to strategic planning. As a result, the identification and assessment of risks become significantly more difficult. This requires new managerial approaches. In practice, many enterprises struggle to diagnose and anticipate the effects of digital innovations on their financial and economic stability, especially in the absence of a structured typology of digital threats and risk factors. Moreover, digital transition frequently unfolds asymmetrically across departments and systems, leading to latent and cumulative vulnerabilities that are hard to detect without a comprehensive analytical framework. This study aims to systematize the full spectrum of risks arising from digital transformation and proposes a conceptual classification that reflects their multidimensional character. Particular attention is given to risks that threaten adaptability, strategic resilience, and operational continuity. By highlighting the relationship between digital transformation risks and enterprise vulnerability, the article seeks to contribute to the development of a theoretical and methodological basis for risk-informed management in the digital economy. Such a foundation is essential not only for academic research but also for practical applications in enterprise governance, strategic planning, and crisis prevention.
Key words: *digital transformation, enterprise economic security, risk systematization, digital threats, enterprise strategic sustainability, risk-based management, business adaptability.*

Постановка проблеми. Цифрова трансформація (ЦТ) стає одним з головних чинників розвитку сучасної економіки та умовою конкурентоспроможності країн і бізнесів у довгостроковій перспективі, відкриваючи нові можливості для зростання, підвищення ефективності та інновацій, проте водночас вона супроводжується цілою низкою ризиків і загроз. переважна частина цифрових трансформаційних ініціатив не досягає очікуваних результатів саме через недооцінку ризиків, які виникають у процесі впровадження цифрових рішень Таким чином, актуальним є ґрунтовне наукове дослідження природи цих ризиків, їх систематизації та методів управління ними. У контексті даного дослідження особливу увагу слід приділяти впливу ЦТ саме на економічну безпеку підприємства, тобто спроможність суб'єкта господарювання підтримувати стійке функціонування, фінансову стабільність, захищеність критичних ресурсів та конкурентоспроможність у цифрово зміненому середовищі. Цифрова трансформація, хоча й несе стратегічні можливості, водночас формує низку ризиків, які потенційно загрожують ключовим складовим економічної безпеки: фінансовій, інформаційній, техніко-технологічній, кадровій, інституційно-правовій тощо.

Аналіз останніх досліджень і публікацій. Проблематика ЦТ в економічній науці останніх років займає важливе місце з огляду на її стратегічний вплив на діяльність підприємств, ринків і національних економік. Зокрема, за оцінками A. Brosnan, G.O'Brien, E. Manning, A. Whelan, від 64% до 90% проєктів цифрової трансформації завершуються невдачею або не досягають поставлених цілей [1, с. 2]. Велика увага серед науковців приділяється технологічним, організаційним та соціальним ризикам цифрової трансформації. У роботах Н.І. Гражевської, А.М. Чигиринського [2], а також В.О. Корнівської [3] досліджено структурну взаємодію фінансових ризиків і ризиків клієнтоорієнтованих сервісів у цифровому середовищі. У роботі І.О. Ревак та Р.Т. Греня [4, с. 62] вказано на

системний характер ЦТ, який охоплює як технологічні інновації, так і управлінські, соціальні та інституційні процеси. Автори підкреслюють важливість формування цілісного уявлення про ризики цифрової трансформації на макро- і мікрорівнях. Р. Зварич, Ю. Дудник, В Гомотюк, С. Боднар розробляють практичні моделі ризик-менеджменту цифрових трансформаційних проектів [5, с. 48]. Пропонується поетапний підхід до виявлення та управління ризиками з урахуванням галузевої специфіки.

Щодо взаємозв'язку ЦТ та економічної безпеки підприємств, варто зазначити, що безпосередній акцент на цій дихотомії робиться рідко. Поняття ЕБП найчастіше фігурує у зв'язку з фінансовою стабільністю, інформаційною захищеністю, технікотехнологічною надійністю та кадровою стійкістю. Так, у роботі К.Ю. Вергал [6, с. 296] розглядаються загрози цифрової економіки для безпеки функціонування підприємств в умовах невизначеності.

Разом із тим, існує відчутна наукова прогалина у системному узагальненні ризиків цифрової трансформації саме в контексті ЕБП. Більшість існуючих досліджень зосереджені на технологічних, організаційних або фінансових аспектах, залишаючи поза увагою інтегральне бачення того, як сукупність ризиків загрожує ключовим складовим економічної безпеки: інформаційній, фінансовій, кадровій, управлінській та іншим. Отже, дане дослідження спрямоване на заповнення цього аналітичного вакууму шляхом побудови типології ризиків ЦТ з чіткою прив'язкою до системи економічної безпеки підприємства.

Постановка завдання. Метою статті є ідентифікація та дослідження ризиків, з якими стикаються підприємства в процесі цифрової трансформації та розроблення їхньої типології на основі узагальнення досвіду вітчизняних і зарубіжних досліджень науковців. Для досягнення мети використано методи аналізу і синтезу наукової літератури, порівняння різних класифікацій ризиків, а також елементи авторського підходу до систематизації ризиків ЦТ. Зроблено акцент на міждисциплінарному характері цієї проблематики, розглядаючи ризики як на рівні окремих організацій (мікрорівень), так і на рівні економіки та суспільства в цілому (макрорівень). Результатом дослідження є узагальнена класифікація ризиків цифрової трансформації, що охоплює технологічні, організаційні, економічні, соціальні, політико-правові та інші їх види, а також визначення напрямів мінімізації їхнього впливу на рівень економічної безпеки підприємств (ЕБП). Дослідження спирається на наукові праці українських учених та провідні світові публікації, забезпечуючи комплексний погляд на поставлену проблему.

Виклад основного матеріалу дослідження. Поняття «*цифрова трансформація*» відображає глибинні зміни в бізнес-моделях, процесах і продуктах під впливом масового впровадження сучасних цифрових технологій [4, с. 61]. На відміну від простого впровадження окремих інформаційних технологій (цифровізації бізнес-процесів) ЦТ передбачає стратегічне переосмислення діяльності підприємства як економічної системи в цілому, що веде до якісно нових результатів і цінності. Серед передумов стрімкого її поширення дослідники відзначають розвиток глобальної інтернет-інфраструктури, вибухове зростання кількості інтернет-користувачів, бурхливий розвиток електронної комерції та ІТ-галузі, а також удосконалення систем електронного урядування. Ці фактори створили сприятливе середовище для масового впровадження цифрових рішень у різних сферах. Основні напрямки ЦТ можна розглядати з точок зору технологій, а також сфер застосування. До основних технологічних напрямків, що сьогодні визначають цифрову трансформацію та формують потенційні ризики, належать:

• *Інтернет речей (Internet of Things, IoT)* – підключення пристроїв до мережі, що забезпечує збір і обмін даними в реальному часі. Ця технологія трансформує виробництво, логістику, розумні міста тощо, але створює й нові ризики, зокрема уразливість пристроїв до несанкціонованого втручання та кібератак [7, с. 174].

• *Штучний інтелект і автоматизація* у форматах впровадження алгоритмів машинного навчання, робототехніки, автоматизованих рішень у бізнес-процеси, що підвищує продуктивність і точність і відкриває можливості для персоналізації послуг. Водночас виникають ризики витоку конфіденційних даних, тотального контролю за поведінкою користувачів, а головне – соціальні ризики, пов'язані зі скороченням робочих місць та зростанням безробіття через автоматизацію.

• *Хмарні обчислення та розподілені сервіси* – перенесення ІТ-інфраструктури та даних у хмарні середовища дозволяє компаніям швидко масштабувати бізнес, знижувати витрати на ІТ та прискорювати впровадження інновацій. Але залежність від надійності інтернет-з'єднання та сторонніх провайдерів, розмитість відповідальності за безпеку даних створюють суттєві ризики для безперервності бізнесу.

• *Блокчейн та розподілені реєстри* – технології, що забезпечують децентралізоване зберігання й перевірку даних. Вони докорінно змінюють фінансовий сектор (криптовалюти, смарт-контракти), логістику, управління ланцюгами постачань, проте несуть ризики, пов'язані з незворотністю запису (неможливістю виправити помилково введені дані), потенційними вразливостями безпеки інфраструктури та можливим використанням токенів у протиправних цілях [6, с. 296].

• *Великі дані та аналітика (Big Data)* надають бізнесу інструменти для прийняття рішень,

підвищення ефективності маркетингу, прогнозування поведінки споживачів, але масове використання великих даних породжує ризики порушення приватності, маніпулювання суспільною свідомістю та виникнення «цифрового диктату», коли технології можуть використовуватись для прихованого впливу на поведінку великих груп людей.

До інших важливих напрямків цифрової трансформації належать впровадження технологій доповненої та віртуальної реальності (AR/VR) в освіті, торгівлі, розвагах; розвиток фінтеху (цифрові фінансові сервіси, мобільні платежі, p2p-кредитування); електронне урядування та смарт-сіті у державному секторі; цифрова медицина (телемедицина, електронні медичні записи) тощо. Кожен із цих напрямків має свою специфіку реалізації та супутні ризики, але всі вони підпорядковані спільній логіці – використанню цифрових технологій для радикального покращення процесів та сервісів.

Для системного аналізу ЦТ доцільно структурувати її за ключовими напрямами впровадження. Кожен з них охоплює певні бізнес-функції, технологічні інструменти та приклади реального застосування, які в сукупності формують трансформаційний профіль підприємства. Узагальнену типологію таких напрямів наведено у таблиці 1.

Таким чином, ЦТ є багатовимірним явищем, що охоплює технологічні інновації, організаційні зміни та соціально-економічні зрушення. Її успіх залежить від здатності керівників і суспільства збалансувати потенційні вигоди та ризики.

Впровадження цифрових технологій приносить численні *переваги на різних рівнях*. На макроекономічному рівні це прискорення економічного зростання, підвищення продуктивності праці, створення нових ринків і підвищення якості життя населення. Для бізнесу ЦТ означає оптимізацію операційних процесів, зниження витрат (наприклад, за рахунок автоматизації та скорочення транзакційних витрат), доступ до ширших ринків через електронну комерцію, швидше впровадження інноваційних продуктів [4, с. 61]. Споживачі також отримують вигоди: дешевший і зручніший доступ до послуг, персоналізовані продукти, нові можливості навчання, комунікації та розваг. Однак, разом з можливостями виникають і виклики, які часто набувають форми ризиків та загроз. Цифрова трансформація носить характер «необхідного потрясіння» для існуючих структур, тому супроводжується опором змінам, невизначеністю результатів та потенційними втратами. Наприклад, автоматизація процесів може призвести до звільнення працівників і соціальної напруженості; перехід на нові технологічні платформи – до зривів у безперервності бізнесу через технічні збої або кібератаки; оцифрування даних – до витоків конфіденційної інформації та проблем приватності. Без належного управління ці ризики можуть звести нанівець очікувані вигоди від цифрових ініціатив. До основних причин невдач ЦТ дослідники відносять недоліки в урахуванні людського фактора, організаційної культури, стратегії та процесів, а не лише технічні проблеми [1, с. 6]. Зокрема, недостатня підтримка керівництва та непродумана стратегія, опір працівників змінам, нестача цифрових компетенцій, неузгоджені бізнес-процеси і застарілі IT-системи стають джерелами ризиків провалу навіть при інвестиціях у більш сучасні технології.

Класифікація ризиків цифрової трансформації. Ризики цифрової трансформації мають багато проявів і торкаються різних аспектів діяльності. У науковій літературі пропонуються різні підходи до їх систематизації. Так, К.Ю. Вергал [6, с. 294, 297] розділяє ризики на макрорівневі (що впливають на економіку та суспільство в цілому) та мікрорівневі (що виникають на рівні окремої організації). До макрорівневих відносять соціальні, екологічні, економічні, технологічні, інформаційні,

Таблиця 1

Напрями цифрової трансформації та приклади

Напрям трансформації	Приклади	Технології / інструменти
Операційна (виробництво)	Смарт-заводи, автоматизовані лінії	IoT, SCADA, MES
Фінансова	E-фінанси, CRM у фінансах	FinTech, AI-аналітика
Клієнтський досвід	Персоналізація, омніканальність	Big Data, ML, Chatbots
Управлінська	Електронні документи, KPI-системи	ERP, DMS, BPM
HR і навчання	E-навчання, платформи розвитку	LMS, EdTech
IT-інфраструктура	Хмари, віртуалізація, DevOps	Cloud, Kubernetes, CI/CD
Інноваційна	Нові продукти, швидкі MVP	Agile, Design Thinking
Державна / публічна	E-сервіси, Smart City	GovTech, Blockchain
Медична	Телемедицина, ЕМЗ	eHealth, IoMT
Безпекова	Аналітика інцидентів, кіберзахист	SIEM, SOAR

Джерело: складено авторами

інституційні, тоді як на мікрорівні виділяють кадрові, управлінські, інформаційні та технологічні ризики підприємства. Інший підхід від J. O'Brien, M. Singh, A. Whelan, E. Manning – виділення ключових напрямів ризиків за сферами впливу: ризики, пов'язані зі стейкхолдерами (людьми), культурою, організацією та стратегією, процесами і технологіями трансформації [1, с. 4]. У межах цього дослідження для повноти охоплення запропоновано інтегрований підхід, що поєднує обидві перспективи. Зокрема, ризики класифіковано за їхньою природою на кілька основних груп з урахуванням як внутрішньоорганізаційних, так і зовнішніх чинників. Представлена типологія дозволяє окрім структурування ризиків ЦТ ще й оцінити, яким складовим ЕБП вони потенційно загрожують (табл. 2).

Наведена типологія надає змогу окреслити основні вектори ризиків, з якими стикаються підприємства в процесі ЦТ. Далі кожна з категорій розглянута окремо, з деталізацією конкретних загроз, їхніх джерел, наслідків і прикладів реалізації на практиці.

Технологічні ризики безпосередньо впливають на інформаційну та техніко-технологічну складові ЕБП, оскільки стосуються захищеності IT-інфраструктури, безперервності технологічних процесів і контролю над критичними даними. Вони охоплюють проблеми і загрози, пов'язані безпосередньо з цифровими технологіями, платформами та IT-інфраструктурою, які впроваджуються під час трансформації:

1. Ризики надійності та безпеки IT-систем. Переходячи до цифрових бізнес-процесів організації стають вкрай залежними від безперебійної роботи інформаційних систем, мереж та серверів. Будь-який збій, відмова або кібератака можуть зупинити операційну діяльність підприємства. Проблеми сумісності нових цифрових рішень із наявними legacy-системами створюють ризики на етапі впровадження. За оцінками експертів Oracle, інтеграція нових технологій з традиційними системами є одним із найскладніших викликів, що може призвести до виникнення ізольованих «силосів» даних та порушення цілісності процесів [8]. Такі технічні бар'єри можуть сповільнити або зірвати трансформаційні проєкти.

2. Кіберризики та інформаційна безпека. З ростом цифровізації підвищується вразливість до кіберзагроз. Хмарні сервіси, IoT-пристрої, мобільні додатки генерують величезні обсяги даних, які циркулюють між численними учасниками, що підвищує ризик несанкціонованого доступу, хакерських атак і витоків інформації [6, с. 297]. Низький рівень кібербезпеки та захищеності даних визначається як один із основних інформаційних ризиків цифрової економіки. Особливо важливим є захист персональних даних клієнтів у фінансових, медичних та інших сферах, тому що будь-який масштабний витік підриває довіру та веде до правових наслідків. Крім того, технології штучного інтелекту відкривають новий формат ризиків – можливість використання алгоритмів для зловмисних цілей (наприклад, deepfake, автоматизовані кібератаки тощо).

3. Залежність від сторонніх платформ і постачальників. У сучасній цифровій екосистемі багато компаній покладаються на глобальні цифрові платформи, програмні рішення та хмарні інфраструктури, які надаються обмеженим колом провідних IT-корпорацій. Така залежність несе технологічні ризики макрорівня: монополізація ринку технологій, загроза технологічного суверенітету країни (особливо актуально для України) та вразливість до санкцій або політики постачальників. Також ризикованим є використання імпортного обладнання та мікроелектроніки. Велика частка програмного забезпечення та комп'ютерної техніки імпортована, і не виключено наявність у них прихованих «бекдорів» або шпигунських чипів [6, с. 296], що створює загрозу як для окремих компаній, так і для національної безпеки.

4. Відставання технологій та інфраструктури. Швидкий прогрес цифрових рішень означає, що наявні технології можуть швидко застарівати. Компанії, що не встигають оновлювати IT-архітектуру, наражаються на ризик технологічного відставання, що знижує їхню ефективність

Таблиця 2

Типологія ризиків цифрової трансформації

Категорія	Сутність	Приклади
Технологічні	Збої, уразливості, кіберзагрози	Відмова систем, кібератаки
Організаційні	Опір змінам, неузгодженість процесів	Конфлікти, бюрократія
Кадрові	Недостатність IT-компетенцій	Відставання персоналу
Економічні	Збитковість, непрогнозованість ROI	Перевищення бюджету
Соціальні	Вплив на зайнятість і рівень життя	Цифрова нерівність
Правові	Невизначеність законів, інституційні бар'єри	Відсутність стандартів
Екологічні	Витрати енергії, електронні відходи	Майнінг, скорочення циклів використання електроніки

Джерело: складено авторами

і конкурентність [6, с. 297]. На рівні країни нерозвиненість цифрової інфраструктури (наприклад, недостатнє покриття швидкісним інтернетом у регіонах) призводить до виникнення «цифрового розриву» та обмежує ефекти цифрової трансформації, стаючи інфраструктурним ризиком макрорівня.

Таким чином, технологічні ризики є багатогранними і включають як суто інженерні проблеми надійності та захищеності систем, так і стратегічні виклики технологічної залежності та інфраструктурної відсталості. Управління ними ризиками потребує сучасної системи кібербезпеки, резервного копіювання, диверсифікації постачальників технологій і планів безперервності бізнесу.

Організаційні та кадрові ризики загрожують управлінській, кадровій і стратегічній складовим економічної безпеки. Організаційні ризики стосуються внутрішнього середовища підприємства, яке здійснює ЦТ: структури, процесів управління, корпоративної культури, кадрів. Цей блок ризиків часто є визначальним в успішності чи провалі трансформацій, оскільки навіть найкращі технології не дадуть ефекту без адаптації організації до нових умов [1, с. 6]. Основними проявами цих ризиків є:

1. Опір змінам і корпоративна культура. ЦТ підприємства за своєю суттю є процесом змін, іноді радикальних. Співробітники можуть сприймати це вороже через страх втратити роботу (у зв'язку з автоматизацією), небажання виходити із зони комфорту чи недовіру до нових технологій. Негативна або інертна корпоративна культура, що не заохочує інновації, творчість і навчання, зводять нанівець усі зусилля трансформації, а відсутність лідерства та чіткої комунікації з боку топ-менеджменту тільки посилює ці ризики. Дослідження підкреслюють, що успіх цифрових ініціатив значною мірою визначається людським фактором – залученістю персоналу, їх готовністю опановувати нові інструменти і процеси [8]. Якщо ж працівники не розуміють цілей трансформації і не мотивовані до участі, проєкт ризикує зазнати невдачі навіть попри наявність ресурсів.

2. Брак цифрових компетенцій і «кадровий голод». Швидкий розвиток технологій породжує підвищений попит на фахівців із відповідними знаннями: аналітиків даних, ШІ-розробників, кібербезпеківців тощо. Ринок праці часто не встигає задовольнити цей попит, що призводить до дефіциту висококваліфікованих спеціалістів [6, с. 296]. Компанії стикаються з ситуацією, коли впроваджені нові системи не використовуються на повну через нестачу навичок у персоналу. Наявні співробітники потребують перекваліфікації та постійного навчання, а це час і витрати. Якщо підприємство не інвестує в програму розвитку цифрових навичок, то наражається на ризик невикористання потенціалу технологій. На макрорівні ж ця проблема проявляється у вигляді поляризації кадрів, коли суспільство поділяється на тих, хто володіє сучасними цифровими компетенціями, і тих, хто відстає, що підвищує нерівність і структурне безробіття.

3. Недоліки управління проєктами та стратегічні помилки. ЦТ підприємств часто реалізується у форматі масштабних проєктів або програм. Неефективний проєктний менеджмент породжує ряд ризиків: від перевищення бюджету і строків до впровадження невідповідних бізнесу рішень. Частою помилкою є «технології заради технологій», коли організація впроваджує «модні інновації» без достатньої прив'язки до бізнес-стратегії та потреб клієнтів. У результаті інвестиції здійснюються в рішення, які не дають очікуваного ефекту, або розбалансовують наявні процеси (у гіршому випадку). Наприклад, впровадження складної CRM-системи без розуміння, як вона покращить роботу з клієнтами, може лише ускладнити працю персоналу і викликати невдоволення. Стратегічні прорахунки включають також невірну оцінку масштабів змін, бо трансформація зачіпає одразу багато аспектів і точка завершення у неї менш чітка, ніж у традиційних IT-проєктів [9, с. 6]. Тому відсутність гнучкої поетапної стратегії з проміжними цілями є серйозним ризиком.

4. Застарілі бізнес-моделі та процеси. Існуючі моделі управління, оргструктура і процеси можуть не відповідати новим цифровим реаліям. Якщо компанія не перегляне свої бізнес-процеси, а просто «накладе» на них нові технології, то не отримає значного покращення, а негнучкі і забюрократизовані процеси гальмуватимуть реалізацію цифрових рішень. Цей ризик непристосованих процесів вимагає реінжинірингу процесів під цифрову логіку. Крім того, нові цифрові моделі (наприклад, використання agile-методологій, крос-функціональних команд, відкритих інновацій) можуть конфліктувати зі старою ієрархічною структурою. Небажання керівництва змінювати усталені підходи («ми завжди так працювали») є істотним ризиком діджиталізації підприємств [6, с. 297].

Для пом'якшення організаційно-кадрові ризиків рекомендуємо приділяти увагу управлінню змінами: комунікувати зі співробітниками стосовно цілей та користі ЦТ, залучаючи їх до процесу та інвестуючи в навчання і мотивування персоналу до опанування нових інструментів. Важливу роль відіграє підтримка з боку вищого керівництва; успішні компанії демонструють, що проєкти ЦТ очолюються топ-менеджерами, які активно беруть участь у їх реалізації і своїм прикладом задають тон змінам. Розробка чіткої дорожньої карти трансформації, узгодженої зі стратегією розвитку бізнесу, та гнучке управління проектами (з можливістю коригування планів) також знижують ці ризики.

Економічні ризики напряму підривають фінансову складову ЕБП, оскільки пов'язані з перевитратами, невизначеністю окупності інвестицій, втратою ринкових позицій та посиленням конкуренції в умовах цифрової економіки. Вони стосуються впливу цифрових змін на економічні показники, ринкове середовище та фінанси підприємств і держави:

1. Висока вартість та невизначеність окупності інвестицій. ЦТ потребує значних фінансових вкладень у придбання технологій, модернізацію ІТ-інфраструктури, навчання персоналу, залучення консультантів тощо. Для багатьох підприємств (особливо малого і середнього бізнесу) це становить фінансовий ризик, коли інвестиції можуть перевищувати запланований бюджет [8] або не привести до очікуваного зростання доходів. Крім того невизначеність ринку і швидкість технологічних змін ускладнюють оцінку ROI (окупності інвестицій) і є ризик, що вкладені кошти не повернуться у вигляді підвищених прибутків, якщо, наприклад, клієнти не приймуть новий цифровий продукт або конкуренти швидко запропонують щось краще.

2. Посилення конкуренції і загрози бізнесу. Цифрова епоха відзначається ефектом «переможець отримує все» на багатьох ринках. Цифрові бізнес-моделі (наприклад, платформи на кшталт Uber, Airbnb) швидко захоплюють значну частку ринку, витісняючи традиційних гравців. Для існуючих компаній це створює ризик втрати конкурентних позицій, якщо вони зволікають із трансформацією. Згідно з дослідженнями К.Ю. Вергал, глобалізація, зумовлена цифровими технологіями, призводить до посилення конкуренції у всіх сферах економіки [6, с. 297]. ЦТ може також розмивати межі галузей: ІТ-компанії виходять у фінансовий сектор (фінтех), телекомунікаційні – в медіа, тощо, створюючи нові ризики для бізнесів, які раніше працювали у стабільних сегментах. Хто не адаптується, ризикують стати неконкурентоспроможними або взагалі збанкрутувати. З іншого боку, цифрові монополії (найбільші гравці, що захопили ринок) можуть диктувати свої умови, що є ризиком для здорової конкуренції та споживачів.

3. Зміна структури ринку праці і макроекономічні ефекти. Цифровізація спричиняє зсув у попиті на робочу силу: зростає потреба в ІТ-фахівцях і водночас автоматизація знижує потребу в деяких традиційних професіях. Звільнені внаслідок автоматизації працівники не завжди можуть одразу знайти себе у новій цифровій економіці, що посилює соціально-економічну нерівність [6, с. 296]. Також існують ризик «відтоку мізків», коли висококваліфіковані ІТ-спеціалісти мігрують у країни з кращими умовами, якщо на батьківщині немає достатніх можливостей. Це все накладається на економічні ризики макрорівня з уповільненням зростання через структурне безробіття, недовикористанням трудового потенціалу та необхідністю витрат на соціальну допомогу та перекваліфікацію.

4. Адміністративні та регуляторні бар'єри (частково стосуються і правових ризиків, але мають економічний вимір). Невідповідність чинного законодавства потребам цифрової економіки, бюрократичні перепони у впровадженні нових технологій можуть стримувати бізнес-ініціативи. Наприклад, регулювання фінансового сектора може не встигати за розвитком криптовалют чи краудфандингу, що створює правову невизначеність і ризики як для компаній, так і для інвесторів. Аналогічно, відсутність єдиних стандартів у галузі (наприклад, стандартів обміну даними) може гальмувати інновації та збільшувати витрати підприємств, які змушені працювати в умовах невизначеності.

Для мінімізації економічних ризиків компаніям рекомендується ретельно прораховувати бізнес-кейси цифрових ініціатив, поетапно інвестуючи у проєкти з найбільшим очікуваним ефектом та створювати «фінансові подушки» для покриття можливих перевитрат. Важливо також відстежувати зміни в конкурентному середовищі, співпрацювати зі стартапами і стежити за глобальними трендами, щоб вчасно реагувати на виклики. На макрорівні держава має відігравати проактивну роль, сприяючи розвитку цифрових компетенцій населення (освіта, перекваліфікація), підтримуючи підприємництво у високотехнологічних сферах та оновлюючи регуляторну базу відповідно до потреб цифрової економіки.

Соціальні та особистісні ризики впливають переважно на кадрову та інституційну безпеку підприємства, оскільки визначають стабільність трудового колективу, ризик втрати людського потенціалу та рівень соціальної напруги. Ними відображається негативний вплив цифрової трансформації на суспільство, громади та окремі соціальні групи. Вони тісно пов'язані з економічними та організаційними, але їхній вимір – більш широкі соціальні наслідки. Основні моменти:

1. Зростання безробіття і соціальна нерівність. Автоматизація та впровадження ШІ можуть витіснити частину працівників. Якщо суспільство не зможе оперативно інтегрувати цих людей у нові сфери (через навчання, створення нових робочих місць), можливе формування стійкого шару безробітних, що посилює тягар на систему соціального захисту. В той же час, висококваліфіковані працівники, що володіють цифровими навичками, будуть користуватися підвищеним попитом і отримувати більші доходи. Сукупно це веде до поляризації суспільства за рівнем доходів і доступом до благ. Деякі дослідники вже говорять про тенденції звуження середнього класу та нестабільної

зайнятості значної частини населення у зв'язку з цифровими змінами [6, с. 296], що становить соціальну загрозу, оскільки може викликати зростання невдоволення і протестних настроїв.

2. Цифрова нерівність. Попри глобальне поширення інтернету досі існує цифровий розрив між тими, хто має доступ до сучасних технологій і вміє ними користуватися, та тими, хто ні. Це може мати географічний вимір (місто-село, країни з різним рівнем розвитку інфраструктури) або демографічний (молодь – літні люди). ЦТ суспільства ризикує посилити відсталість тих груп, які не змогли своєчасно приєднатися до «цифрового світу». Наприклад, впровадження електронних державних послуг може ускладнити життя пенсіонеру, який не користується комп'ютером, а нерівномірна інформатизація регіонів призводить до відставання цілих громад від загального прогресу. Це соціальний ризик, який потрібно враховувати при плануванні цифрових ініціатив, інвестуючи в цифрову інклюзію (навчальні програми, розширення доступу).

3. Зміни в характері праці та соціально-психологічні ефекти. Цифровізація змінює те, як люди працюють і взаємодіють. Поширення дистанційної роботи з одного боку надає гнучкість, а з іншого – веде до ризиків соціальної ізоляції працівників, розмивання меж між роботою і особистим життям і хронічного стресу. Постійне навчання та необхідність слідкувати за стрімкими змінами можуть викликати «цифрову тривожність» – страх не встигнути адаптуватися. Особистісні ризики включають також технострес (від роботи з новими технологіями) та вигорання через інформаційне перенавантаження. У людей, які постійно переключаються між цифровими каналами, з'являються проблеми з концентрацією уваги та зниженням глибини обробки інформації, що впливає на когнітивні здібності особистості. Окремо стоїть питання приватності та захисту персональних даних, бо в цифрову епоху межа між приватним і публічним розмивається. Люди добровільно чи несвідомо надають купу особистої інформації різним онлайн-сервісам, що може використовуватися третіми сторонами.

4. Вплив на суспільну свідомість і етику. Сюди можна віднести феномен «цифрових інформаційних бульбашок» та поширення дезінформації. Алгоритми соцмереж схильні підлаштовувати контент під уподобання користувачів, що замикає людей в певних інформаційних полях та поляризуючи суспільство за поглядами та створюючи помилкове відчуття реальності. Масові інформаційні впливи та фейки теж є частиною ризиків цифрової трансформації суспільства. Не менш важливим є етичний аспект: впровадження ШІ ставить питання етики (наприклад, прийняття рішення алгоритмами замість людей, використання біометричних даних для стеження тощо). Невирішеність цих питань може підривати суспільну довіру до цифрових інновацій.

Для адресації соціальних ризиків потрібні спільні зусилля держави, бізнесу і громади. Держава має розробляти політику цифрової рівності – забезпечувати доступний інтернет у найвіддаленіших куточках, навчати населення цифровій грамотності (через освітні програми, бібліотеки, центри тощо). Бізнес-структури, впроваджуючи нові технології, мають враховувати соціальний вплив (наприклад, програми перепідготовки для звільнюваних працівників, дотримання етичних норм роботи з даними). На рівні організацій доцільно впроваджувати практики управління змінами, що враховують психологічний стан працівників, підтримку балансу робота-життя, заходи з командоутворення при віддаленій роботі. Таким чином, пом'якшення соціально-особистісних ризиків полягає в тому, щоб ставити людину в центр ЦТ, зберігаючи її добробут і права.

Правові ризики створюють загрози інституційно-правовій та інформаційній безпеці підприємства, оскільки пов'язані з нестабільним нормативним середовищем, дефіцитом правових гарантій та потенційними зовнішніми обмеженнями цифрової діяльності. Вони стосуються зовнішнього середовища, в якому здійснюється цифрова трансформація, а саме – дій держави, законодавства, нормативного регулювання, а також можливих політико-суспільних загроз. До цієї категорії належать:

1. Невідповідність законодавства цифровим реаліям. Цифрова економіка розвивається швидше, ніж законодавче поле. У багатьох випадках відсутні необхідні закони та підзаконні акти з регулювання нових видів діяльності від електронної комерції та електронного документообігу до питань обігу криптовалют тощо. Така правова невизначеність створює ризики як для бізнесу (незрозумілі «правила гри», можливі штрафи чи заборони постфактум), так і для споживачів (незахищеність прав у цифровій сфері).

2. Недостатнє регулювання нових ринків та монополізація. Дерегуляція та підтримка інновацій – це добре, але повна відсутність контролю на нових цифрових ринках може призводити до зловживань. Наприклад, ринок великих цифрових платформ (Google, Facebook, Amazon) у світі практично не регулювався на початкових етапах, що дозволило їм вирости до монополій, впливаючи на економіку і політику. Зараз багато держав намагаються виробити підходи до їх регулювання, але це складно зробити постфактум. Для України актуальним є питання регулювання ринку цифрових фінансових послуг (FinTech), який з одного боку відкриває доступ до кредитів сегментам, не охопленим банками, з іншого – породжує ризики

зростання боргового навантаження населення та монополізації певними онлайн-платформами [3, с. 156]. Таким чином, виклик для держави – знайти баланс між стимулюванням інновацій та запобіганням негативним наслідкам через запізніле регулювання.

Для зменшення цих ризиків необхідна своєчасна модернізація законодавства. Українські науковці наголошують на потребі адаптації нормативної бази до умов нового технологічного укладу, розробки державної стратегії розвитку цифрової економіки. Також слід переймати кращі світові практики, зокрема, імплементувати GDPR-подібне законодавство про захист даних, впроваджувати стандарти кібербезпеки (ISO, NIST) на рівні державних установ і критичної інфраструктури. Резюмуючи, держава має одночасно стимулювати цифрові інновації та створювати «правила гри», що мінімізують пов'язані з ними ризики.

Хоча *екологічні ризики* менш очевидні у контексті економічної безпеки, однак вони можуть впливати на репутаційну, ресурсну та стратегічну складові, особливо для компаній, чия діяльність залежить від енерговитрат, логістики чи взаємодії з громадськістю в питаннях сталого розвитку. Вони не завжди виокремлюються в контексті ЦТ, проте сучасні дослідження звертають увагу і на цю складову [6, с. 297]. Цифрові технології самі по собі можуть мати суттєвий вплив на довкілля, опосередковано створюючи ризики сталого розвитку. Основними аспектами серед цього є:

1. Збільшення споживання енергії. Центри обробки даних (ЦОД), що забезпечують роботу хмарних сервісів, великі мережі серверів для майнінгу криптовалют і мільярди підключених пристроїв потребують електроенергії. ІТ-сектор стає одним з найбільших споживачів електроенергії у світі і якщо значна частка цієї енергії виробляється з викопного палива, це призводить до зростання викидів парникових газів. Цифровізація економіки породжує додаткове навантаження на екологію саме через енергоспоживання. Таким чином, є ризик, що без впровадження «зелених» ІТ-рішень ЦТ вступатиме в конфлікт з цілями сталого розвитку, сприяючи негативним змінам клімату.

2. Електронні відходи. Масове використання електронних пристроїв скорочує їх життєвий цикл (через швидке моральне старіння), призводячи до утворення значних обсягів електронних відходів (комп'ютери, гаджети, сенсори тощо). Неналагоджена система утилізації та переробки електроніки створює екологічні ризики отруєння довкілля токсичними компонентами.

3. Вплив на споживчі патерни. Цифровізація сервісів може призводити до збільшення пакування, транспортних перевезень, що теж має екологічний слід. Хоча ці ефекти не є прямим результатом цифрових технологій, вони опосередковані зміною моделі споживання і логістики, що супроводжують цифрову економіку.

Для врахування екологічних ризиків потрібен підхід Green IT – перехід ЦОД на відновлювані джерела енергії, оптимізація алгоритмів з точки зору енергоспоживання (зокрема, у сфері блокчейн активно шукають менш енергоємні протоколи). Державна політика має стимулювати переробку електронних відходів, встановлювати нормативи енергоефективності для цифрової інфраструктури.

Управління ризиками цифрової трансформації. З огляду на вищенаведену типологію стає зрозуміло, що ризики ЦТ комплексні і взаємопов'язані, тому управління ними (ризик-менеджмент) вимагає системного підходу. На основі аналізу наукових досліджень та практичних кейсів можна окреслити ряд основних принципів і заходів управління такими ризиками:

1. Ідентифікація та оцінка ризиків на початковому етапі. Ще на стадії планування цифрової ініціативи варто провести всебічний аналіз потенційних ризиків (технологічних, фінансових, соціальних тощо). Побудова матриці ризиків цифрової трансформації з оцінкою ймовірності та впливу ризик-факторів є ефективним інструментом для пріоритезації управлінських дій [10, с. 14]. Особливо важливо відстежувати «ризики з низькою контрольованістю» (опір змінам, культурні бар'єри тощо) та закладати завчасно стратегії їх пом'якшення.

2. Розробка стратегії ризик-менеджменту. Виявлені ризики потребують плану реагування: уникнення, зменшення, передача або прийняття ризику. Для ЦТ підприємств доцільно сформувати систему ризик-менеджменту з визначенням відповідальних осіб, етапів моніторингу ризиків та протоколів дій при настанні негативних подій. Р. Зварич, Ю. Дудник, В. Гомотюк, С. Боднар [5, с. 49] пропонують поетапну модель ризик-менеджменту цифрової трансформації, яка включає: 1) підготовчий етап (формування команди, методології), 2) ідентифікацію ризиків, 3) кількісну і якісну оцінку, 4) розробку заходів реагування, 5) моніторинг та коригування. В умовах динамічних змін така стратегія має бути гнучкою і переглядатися по мірі реалізації проекту.

3. Технічні заходи безпеки. Для мінімізації технологічних та кіберризиків потрібне впровадження сучасних засобів інформаційної безпеки: систем кіберзахисту, моніторингу мережевої активності, резервного копіювання даних, планів аварійного відновлення. Важливо також проводити стрес-тестування нових цифрових систем перед повноцінним запуском, щоб виявити слабкі місця. Компанії мають дотримуватися принципів SecDevOps, інтегруючи безпеку на всіх етапах

розробки та експлуатації цифрових продуктів. Крім технічного аспекту варто приділити увагу і контролю постачальників (вимоги до їх безпеки, резервні варіанти на випадок збою їх сервісів).

4. Людський фактор та зміни. Управління організаційними ризиками полягає у роботі з людьми. Необхідно реалізувати програми навчання співробітників новим навичкам, проводити роз'яснювальні кампанії щодо цілей ЦТ, залучати «агентів змін» – авторитетних працівників, які підтримують інновації, для поширення позитивного ставлення. Винагородження ініціативності та інноваційної активності персоналу також знижує культурний опір. Окремо стоїть питання лідерства, коли керівники мають демонструвати послідовність у реалізації цифрової стратегії та власним прикладом заохочувати підлеглих долати труднощі. Компанії, які успішно трансформувалися, відзначають важливу роль директора з цифрових технологій (Chief Digital Officer, CDO), що сконцентрована на управлінні всіма аспектами цифрових змін, включно з ризиками.

5. Моніторинг та адаптація. ЦТ – процес тривалий, тому моніторинг ризиків має здійснюватися на постійній основі. Ризик-профіль може змінюватися: спочатку домінантні ризики можуть успішно мінімізуватися, натомість з'являються нові (наприклад, технології впроваджено і технічні ризики знизились, але збільшились ризики експлуатації та підтримки). Необхідно регулярно переглядати матрицю ризиків, включати їх обговорення у порядок денний управлінських нарад. Адаптивне управління означає, що за появи нових загроз оперативно впроваджуються контрзаходи (наприклад, якщо в ході проєкту виявлено, що користувачі масово не приймають нову систему, слід додатково інвестувати в UX-дослідження чи навчання, навіть якщо це не було спочатку заплановано).

Оскільки ризики ЦТ в різних напрямах проявляються нерівномірно, доцільно зіставити трансформаційні сфери із характерними для них групами ризиків. Така співвіднесеність дозволяє виявити найбільш ризиконесучі напрями, які потребують особливої уваги в системі управління ризиками. Узагальнені результати наведено в таблиці 3.

Сучасний підхід до ризик-менеджменту ЦТ полягає у превентивності та проактивності: не чекати, коли ризик реалізується, а передбачати і діяти на випередження. Це стає можливим завдяки накопиченню бази знань про минулі проєкти (власні та сторонні кейси), використанню інструментів моделювання сценаріїв та розвитку внутрішньої культури, де ризики відкрито обговорюються. Повністю уникнути усіх ризиків неможливо і певна частка невизначеності завжди лишається, але грамотне управління дозволяє знизити ймовірність найгірших сценаріїв і підготувати план дій на випадок їх настання, що зрештою підвищує стійкість організації в умовах цифрової турбулентності.

Висновки. Цифрова трансформація виступає двояким явищем для економіки і суспільства: з одного боку, вона є двигуном прогресу, що забезпечує нові можливості росту, з іншого – породжує комплекс ризиків, які можуть гальмувати або навіть нівелювати очікувані вигоди. Проведене дослідження дозволило здійснити ґрунтовний аналіз ризиків ЦТ підприємств та запропонувати їх інтегровану класифікацію. Визначено шість основних груп ризиків: технологічні, організаційні (кадрові), економічні (фінансові), соціальні (включно з особистісними), правові (інституційні) та екологічні. Кожна з цих груп включає низку конкретних ризик-факторів від кіберзагроз, технічних збоїв, нестачі ІТ-спеціалістів і опору змінам до законодавчих прогалин, соціальної нерівності та зростання викидів CO_2.

ЦТ формує багатовимірне ризикове середовище, яке вимагає від підприємств не лише технологічної адаптації, а й усвідомленої побудови системи забезпечення економічної безпеки. Виявлені ризики зачіпають ключові її складові: фінансову, інформаційну, організаційну, кадрову, що вказує на необхідність інтеграції ризик-менеджменту цифрової трансформації у загальну стратегію ЕБП.

Наукова новизна полягає в тому, що ризики ЦТ розглянуті комплексно, на перетині мікро- та макропідходів. Запропонована типологія враховує як внутрішні проблеми підприємств (невідповідність структури, брак навичок, культурні бар'єри), так і зовнішні виклики (ринкові, регуляторні,

Таблиця 3

Матриця «напрям трансформації → типові ризики»

Напрям трансформації	Технол.	Організ.	Екон.	Кадр.	Соц.	Прав.	Екол.
Виробництво	✓	✓	✓	✓			✓
Фінанси	✓	✓	✓	✓		✓	
Управління	✓	✓	✓	✓		✓	
HR / навчання		✓	✓	✓	✓		
ІТ-інфраструктура	✓		✓			✓	✓
Держ. сектор	✓	✓	✓		✓	✓	✓

Джерело: складено авторами

суспільні), пов'язані з цифровізацією. Багато в чому ці ризики взаємопідсилюють один одного, тому ефективне управління ними має базуватися на системному, холістичному підході.

Практична цінність отриманих результатів полягає у можливості їх використання при плануванні і реалізації програм цифрової трансформації як на рівні окремих компаній, так і при формуванні державної політики цифрового розвитку. Усвідомлення потенційних загроз на ранніх етапах дозволить розробити засоби нейтралізації ризиків та підвищити ймовірність успіху цифрових ініціатив.

Надалі доцільно поглибити дослідження шляхом розробки методичних підходів до кількісної оцінки впливу окремих ризиків та моделювання сценаріїв ЦТ з урахуванням невизначеностей. В умовах швидкоплинності технологічних змін також потрібен моніторинг новітніх ризиків (впровадження квантових технологій, Web3, метавсесвіту тощо).

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Brosnan A. Towards an Understanding of Digital Transformation Risk: A Systematic Literature Review / A. Brosnan, J. O'Brien, E. Manning [та ін.] // Proceedings of the Thirty-first European Conference on Information Systems (ECIS 2023), Kristiansand, Norway, May 2023. 15 p. URL: https://www.researchgate.net/profile/Andrew-Brosnan-3/publication/369301763_Unpacking_Digital_Transformation_Risk_A_Systematic_Review_On_Why_Digital_Transformations_Often_Fail_To_Deliver_Value/links/6413e9ee66f8522c38aeb8ec/Unpacking-Digital-Transformation-Risk-A-Systematic-Review-On-Why-Digital-Transformations-Often-Fail-To-Deliver-Value.pdf

2. Гражевська Н. І., Чигиринський А. М. Цифрова трансформація економіки в умовах посилення глобальних ризиків і загроз. *Економіка та держава*. 2021. № 8. С. 53–57. DOI: https://doi.org/10.32702/2306-6806.2021.8.53

3. Корнівська В. О. Цифрові трансформації: ризики клієнтоорієнтованих фінансів. *Проблеми економіки*. 2022. № 3 (53). С. 156–163. DOI: https://doi.org/10.32983/2222-0712-2022-3-156-163

4. Revak I. O., Gren R. T. Digital Transformation: Background, Trends, Risks, and Threats. *Соціально-правові студії.* 2022. Т. 5, № 2. P. 61–67. DOI: https://doi.org/10.32518/2617-4162-2022-5-2-61-67

5. Зварич Р., Дудник Ю., Гомотюк В., Боднар С. Ризик-менеджмент цифрової трансформації в умовах пандемії. *Вісник економіки*. 2022. Вип. 1. С. 38–53. DOI: https://doi.org/10.35774/visnyk2022.01.038

6. Вергал К. Ю. Загрози та ризики цифрової трансформації економіки. *Вісник Хмельницького національного університету. Економічні науки.* 2020. № 4(3). С. 294–299. DOI: https://doi.org/10.31891/2307-5740-2020-284-4(3)-53

7. 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. Вип. 47(2). С. 173–177. DOI: https://doi.org/10.32843/bses.47-66

8. Tsidulko J. Digital Transformation Decoded / J. Tsidulko // Oracle. – Sept. 19. 2024. URL: https://www.oracle.com/cloud/digital-transformation/

9. Brosnan A., McCarthy S., Carroll N. Exploring the Nature of Risk in Digital Transformation: A Problematisation Perspective of Low-Code/No-Code Platform Risk / Proceedings of the Thirty-Second European Conference on Information Systems (ECIS 2024), Paphos, Cyprus, June 2024. 14 p. URL: https://www.researchgate.net/profile/Noel-Carroll-5/publication/381461807_Exploring_the_Nature_of_Risk_in_Digital_Transformation_A_Problematisation_Perspective_of_Low-Code_No-Code_Platform_Risk/links/666ebddaa54c5f0b94664d21/Exploring-the-Nature-of-Risk-in-Digital-Transformation-A-Problematisation-Perspective-of-Low-Code-No-Code-Platform-Risk.pdf

10. Brosnan A., Manning E., Whelan A. [etc.]. The Digital Transformation Risk Matrix: A Tool for Assessing the Impact/Control Nature of Digital Transformation Risk / Proceedings of the International Conference on Information Systems (ICIS 2024), Bangkok, Thailand, December 2024. URL: https://www.researchgate.net/profile/Andrew-Brosnan-3/publication/384500478_The_Digital_Transformation_Risk_Matrix_A_Tool_for_Assessing_the_ImpactControl_Nature_of_Digital_Transformation_Risk/links/66fbebbbf599e0392fb179cd/The-Digital-Transformation-Risk-Matrix-A-Tool-for-Assessing-the-Impact-Control-Nature-of-Digital-Transformation-Risk.pdf

REFERENCES:

1. Brosnan A., O'Brien J., Manning E., et al. (2023) *Towards an understanding of digital transformation risk: A systematic literature review. Proceedings of the Thirty-first European Conference on Information Systems (ECIS 2023), Kristiansand, Norway*, May 2023, 15 p. Available at: https://www.researchgate.net/profile/Andrew-Brosnan-3/publication/369301763_Unpacking_Digital_Transformation_Risk_A_Systematic_Review_On_Why_Digital_Transformations_Often_Fail_To_Deliver_Value/links/6413e9ee66f8522c38aeb8ec/Unpacking-Digital-Transformation-Risk-A-Systematic-Review-On-Why-Digital-Transformations-Often-Fail-To-Deliver-Value.pdf

2. Grazhevska N. I., Chyhyrynskyi A. M. (2021) Tsyfrova transformatsiia ekonomiky v umovakh posylennia hlobal'nykh ryzykiv i zahroz [Digital transformation of the economy in the context of growing global risks and threats]. *Ekonomika ta derzhava*, no. 8, pp. 53–57. DOI: https://doi.org/10.32702/2306-6806.2021.8.53

3. Kornivska V. O. (2022) Tsyfrovi transformatsii: ryzyky kliientooriientovanykh finansiv [Digital transformations: risks of client-oriented finance]. *Problemy ekonomiky*, no. 3(53), pp. 156–163. DOI: https://doi.org/10.32983/2222-0712-2022-3-156-163

4. Revak I. O., Gren R. T. (2022) Digital transformation: background, trends, risks, and threats. *Sotsial'no-pravovi studii – Social-Legal Studios*, vol. 5(2), pp. 61–67. DOI: https://doi.org/10.32518/2617-4162-2022-5-2-61-67

5. Zvarych R., Dudnyk Yu., Homotiuk V., Bodnar S. (2022) Ryzyk-menedzhment tsyfrovoi transformatsii v umovakh pandemii [Risk management of digital transformation in the conditions of the pandemic].

Visnyk ekonomiky, issue 1, pp. 38–53. DOI: https://doi.org/10.35774/visnyk2022.01.038

6. Verhal K. Yu. (2020) Zahrozy ta ryzyky tsyfrovoi transformatsii ekonomiky [Threats and risks of digital transformation of the economy]. *Visnyk Khmelnytskoho natsional'noho universytetu. Ekonomichni nauky*, no. 4(3), pp. 294–299. DOI: https://doi.org/10.31891/2307-5740-2020-284-4(3)-53

7. Shevchuk I. B., Deputat B. Ya., Tarasenko O. Ye. (2019) Tsyfrovyzatsiia ta yii vplyv na ekonomiku Ukrainy: perevahy, vyklyky, zahrozy y ryzyky [Digitalization and its impact on the economy of Ukraine: advantages, challenges, threats and risks]. *Prychornomorski ekonomichni studii*, issue 47(2), pp. 173–177. DOI: https://doi.org/10.32843/bses.47-66

8. Tsidulko J. (2024, September 19) *Digital transformation decoded. Oracle.* Available at: https://www.oracle.com/cloud/digital-transformation/

9. Brosnan A., McCarthy S., Carroll N. (2024, June) *Exploring the nature of risk in digital transformation: A problematisation perspective of low-code/no-code platform risk. Proceedings of the Thirty-Second European Conference on Information Systems (ECIS 2024), Paphos, Cyprus,* 14 p. Available at: https://www.researchgate.net/profile/Noel-Carroll-5/publication/381461807_Exploring_the_Nature_of_Risk_in_Digital_Transformation_A_Problematisation_Perspective_of_Low-Code_No-Code_Platform_Risk/links/666ebddaa54c5f0b94664d21/Exploring-the-Nature-of-Risk-in-Digital-Transformation-A-Problematisation-Perspective-of-Low-Code-No-Code-Platform-Risk.pdf

10. Brosnan A., Manning E., Whelan A., et al. (2024, December) *The digital transformation risk matrix: A tool for assessing the impact/control nature of digital transformation risk. Proceedings of the International Conference on Information Systems (ICIS 2024), Bangkok, Thailand.* Available at: https://www.researchgate.net/profile/Andrew-Brosnan-3/publication/384500478_The_Digital_Transformation_Risk_Matrix_A_Tool_for_Assessing_the_ImpactControl_Nature_of_Digital_Transformation_Risk/links/66fbebbbf599e0392fb179cd/The-Digital-Transformation-Risk-Matrix-A-Tool-for-Assessing-the-Impact-Control-Nature-of-Digital-Transformation-Risk.pdf