УДК 005.7+ 004.6
JEL Classification A11, D80
DOI 10.33111/EE.2023.51.KlymenkoS

S. Klymenko
PhD in Economics, Associate Professor of the Department business economics and entrepreneurship KNEU them. V. Hetman

С. М. Клименко
к.е.н., доцент кафедри бізнес-економіки та підприємництва, Київський національний економічний університет імені Вадима Гетьмана

ORCID: 0000-0001-9418-7360

ПРОБЛЕМИ РИЗИК-МЕНЕДЖМЕНТУ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

АНОТАЦІЯ. Актуальність теми обумовлена дослідженням впливу процесів цифровізації економічних відносин на особливості організації системи ризик-менеджменту підприємства. Цифровізація супроводжується виникненням нових загальносистемних видів ризиків, детермінованних цифровою трансформацією бізнес-процесів. Визначено економічний зміст діджиталізації в умовах сьогодення та її вплив на побудову сучасних систем ризик-менеджменту підприємств. Проаналізовано вплив основних процесів розвитку цифрових технологій на відповідні структурно-функціональні складові систем ризик-менеджменту організацій. Встановлено основні види ризиків, пов'язані з цифровізацією: стратегічні, нормативно-правові, технологічні, кібернетичні, кадрові ризики, ризики втрати даних, конфіденційності, третіх осіб. Виявлено управлінські заходи з напрямів мінімізації цих ризиків. Розглянуто основні підходи до створення сучасної системи ризик-менеджменту в організаціях та обґрунтовано доцільність впровадження цифрових механізмів у структуру ризик-менеджменту для підвищення ефективності його роботи.
КЛЮЧОВІ СЛОВА. ризик-менеджмент; цифровізація; цифрова трансформація; кібербезпека.

PROBLEMS OF RISK MANAGEMENT IN THE ERA OF DIGITAL TRANSFORMATION

ANNOTATION: The relevance of the topic is determined by the study of the impact of the processes of digitalization of economic relations on the peculiarities of the organization of the enterprise's risk management system. It is known that digitalization is accompanied by the emergence of new system-wide types of risks determined by the digital transformation of business processes. Determined the economic meaning of digitization in today's conditions and its impact on the construction of modern enterprise risk management. The

influence of the main processes of development of digital technologies on the corresponding structural and functional components of the risk management systems of organizations is analyzed. The main types of risks associated with digitalization are identified: strategic, regulatory, technological, cyber, personnel risks, risks of data loss, confidentiality, and third party risks. Management measures for the minimization of these risks have been identified.
The main approaches to the creation of a modern risk management system in organizations are considered and the expediency of introducing digital mechanisms into the risk management structure to increase the efficiency of its work is substantiated. Modern risk management models of the company must extend internal control over the expected results in order to guarantee the achievement of the planned goals of the organization.
Current models of risk management do not sufficiently reflect the current dynamics of changes in the external environment and processes that occur in all subsystems of the company's management and fragmentarily reflect the information necessary for making adequate management decisions. The article substantiates the expediency of introducing digital mechanisms into the structure of risk management to increase the efficiency of its work.
Based on the fact that digitalization is an inevitable change that is already happening in all areas of business, the main critical fields of risks and threats are outlined: data security, transformation of business processes, reliability of digital systems and infrastructure.
KEY WORDS. risk management; digitalization; digital transformation; cyber security.

Вступ. Сучасні моделі управління ризиками компанії повинні розширювати внутрішній контроль над очікуваними результатами, щоб гарантувати досягнення запланованих цілей організації. Діючі моделі ризик-менеджменту недостатньо відображають сучасну динаміку змін зовнішнього середовища і процесів, які відбуваються у всіх підсистемах управління фірмою та фрагментарно відображають інформацію, яка необхідна для прийняття адекватних управлінських рішень. У статті обґрунтовується доцільність впровадження цифрових механізмів у структуру ризик-менеджменту для підвищення ефективності його роботи.

Дослідженню ризиків в організаціях присвячено переважну більшість зарубіжних наукових публікацій, серед яких класичними вважають праці Р. Баззела, И. А. Бланка, Р. Галлахера, Д. Кокса, Д. Купера, В. Лоуренса, П. Мура, Ф. Найта, Д. Рикардо, В. Роу, А. Смита, У.Снайдера та інших.

Проблемами впливу цифрової економіки на ризик-менеджмент організацій, роллю та особливостями діджиталізації опікувались такі вітчизняні дослідники, як Б. Андрушків, З. Варналій, В. Вірченко, О. Грибіненко, О. Данченко, Г. Жекало, О. Іванкевич,

С. Криниця, Л. Лазебник, І. Маркович, В. Мазур, М. Макарова, А. Наторіна, Л. Радкевич, В.Скіцько, Н. Чеснокова та інші. Але з кожним роком проблема кібербезпеки на всіх рівнях набуває дедалі більшої актуальності.

Постановка завдання. Цифрова революція, яка охопила світову економіку, вражає масштабом, темпами і географією. З кожним роком зростає інтенсивність впровадження нових технологій у виробництво й обслуговування людських потреб [3]. Проте зростання масштабів цифровізації всіх сфер життя веде до того, що громадяни і бізнес усього світу та, зокрема, України частіше потерпатимуть від зростання кіберзлочинності.

Найнебезпечнішими для економіки та громадян є кібератаки на критичну інфраструктуру України (енергозабезпечення, транспортне управління, банківський та телекомунікаційний сектори, медичне обслуговування, водопостачання тощо). Такі автори, як В. М. Гранатуров та І. А. Кораблінов у дослідженнях розкривають сутність поняття «інформаційні ризики», розглядають виникнення їх на різних ієрархічних рівнях: держави, загалом економіки, корпорацій, окремих підприємств і та ін., детально описують склад, види та умови виникнення ризиків, які утворюють загальне поняття «інформаційний ризик». Так, наприклад, незважаючи на те, що проблема ризиків, пов'язаних із використанням інформації та інформаційних технологій, є відносно новою у загальній теорії ризиків, деякі з них вже включено до переліку глобальних ризиків, які загрожують людству та з якими воно поки що не в змозі впоратися [8].

Актуальність цього дослідження пояснюється формуванням специфічних ризиків та загроз, що виникають у процесі цифровізації. Існує потреба в їх виявленні та ідентифікації, а також розробці заходів мінімізації або уникнення залежно від видових характеристик.

Попри різноманітність наукових праць та емпіричних досліджень, що базуються на ризикологічному підході, деякі аспекти ідентифікації ризиків, які супроводжують цифрову трансформацію, потребують уточнення, що визначає мету та завдання дослідження.

Результати. Сучасні підприємства в процесі управління ризиками вимушені проходити через суворі регуляторні вимоги. Однак у контексті діджиталізації синергія з управлінням ризиками часто недооцінюється. Це, безумовно, пов'язано з тим, що регуляторні вимоги до цифровізації не мають методичного підґрунтя, чітких обмеженнь та рекомендацій.

Розглянемо більш детально окремі ключові напрями і ризики, що супроводжують впровадження діджиталізації в основні бізнес-процеси організацій.

1. ***Цифровізація як Четверта промислова революція***. Цифровізація — невід'ємна риса сучасної реальності, що символізує Четверту промислову революцію. Цифровізація включає не лише цифрове відображення процесів, а й фундаментальну трансформацію всього корпоративного світу через впровадження нових технологій на основі Інтернету з далекосяжним впливом на суспільство в цілому [1]. Однак зміни повинні мати більш глибинний характер, ніж просто використання нових технологій: це зміна лідерства співробітників, ролей та обов'язків у суспільстві, бізнес-моделей, а також процесів і десятиліттями усталених рутинних процедур.

Формується «цифрове мислення», відбуваються інвестиції в цифрові технології, обладнання та інфраструктуру, а також у кваліфікований персонал, який досконало володіє цифровими навичками, сприяє успішним перетворенням, створює нові конкурентні переваги організацій [3].

Спираючись на дослідження фірми «Делойт», до 2025 р. найбільш конкурентоспроможні компанії повністю автоматизують усі рутинні та механічні господарські процеси, включаючи стратегічні завдання, а технології блокчейну, великих даних, програмних комплексів управління компаніями (ERP-системи) складуть основу автоматизації [1].

2. ***Стрес-тест для бізнес-моделей організацій***. Діджиталізація докорінно змінює всі існуючі бізнес-моделі. Найуспішнішою компанією з надання послуг з автомобільних перевезень у світі є Uber, і хоча вона не має жодного власного автомобіля, володіє великою кількістю IT-інфраструктури ринку таксі. Найбільшою медіакомпанією у світі є Facebook, яка не має власного контенту, проте виступає посередником між відповідними профілями користувачів. Найбільша компанія в світі на ринку оренди житла — Airbnb, також не володіє жодним об'єктом нерухомості. Що об'єднує усі згадані компанії? Вони зорієнтували свої бізнес-моделі на діджиталізацію і особливо — на розумне використання даних. Багато компаній, які працюють на ринку достатньо довгий час усе ще вважають, що існуюча дієва бізнес-модель може залишатися незмінною протягом тривалого часу і що діджиталізація обмежується лише наявністю в Інтернеті привабливої домашньої сторінки фірми. Втім досягнення певного рівня конкурентоспроможності на ринку потребує впровадження революційної цифрової трансформації всіх бізнес-процесів організацій. Прикладами креативних ідей цифровізації можуть слугувати залучення цифрових аборигенів після попереднього відповідного інструктажу, створення смарт-контрактів у блокчейні, які дозволять

скасувати послуги посередників, таких як нотаріуси, земельні кадастри або навіть банки тощо.

Поява нових повноваженнь у гравців на ринку може змінити правила гри. Що станеться, наприклад, якщо Amazon або Apple увійдуть у банківський сектор? Чи потрібен буде тоді клієнту домашній банк? Чи буде застосовна стара цитата Білла Гейтса, що «банківська справа необхідна, а банки — ні»? Що станеться, якщо Facebook впровадить власну цифрову валюту Libra або якщо Alibaba і Tencent / Whatsapp також вийдуть на європейський ринок? Такі сценарії є справжніми стрес-тестами. Ці та подібні заходи можуть кардинально змінити ринки, не просто незначним збільшенням рівня дефолтів або, можливо, гіршими умовами рефінансування, а появою фундаментальних ризиків, які змінять існуючі бізнес-моделі. Чим раніше компанія буде готова вводити нові креативні ідеї цифровізації, тим краще буде підготовка до успішного функціонування в умовах стрімких змін зовнішнього середовища.

3. ***Діджиталізація — це більш ніж просто технології.*** У разі впровадження цифровізації в бізнес важливо відшукати правильний баланс між технічними можливостями впровадженнь та економічним ефектом від них та необхідністю збереження та посилення клієнтоорієнтованості компанії. Важливо, щоб унікальні компетенції, які раніше приваблювали споживачів даної компанії, зберігалися або, в ідеалі, навіть посилювалися.

На сучасному ринку існує дві технології, які зараз активно набирають поширення, — це роботизована автоматизація процесів (RPA) і хмарні обчислення. Багато компаній вже впровадили ці технології або розглядають можливість зробити це. Розглянемо ризики впровадження цих систем.

Роботизована автоматизація процесів (RPA). Можливості впровадження RPA мають велику кількість конкурентних переваг. Програмні роботи допомагають автоматизувати повністю бізнес-процеси чи його окремі етапи. Існують різні ліцензійні моделі та форми виконання, наприклад, боти під наглядом або без нагляду, тобто в інтерактивному або у фоновому режимі, функціонування в текстовому або мультимедійному форматі тощо. Для того щоб вирішити, які процеси автоматизувати та який тип бота використовувати, потрібно заздалегідь з'ясувати деякі основні питання:

- Яка мета розгортання RPA? Економія коштів, прискорення часу виконання завдань чи навіть відкриття нових можливостей для бізнесу?
- Які процеси будуть підтримувати RPA? (Як правило, це прості та однорідні дії, подібні до макросу Excel, але також перехресні додатки.)

- У яких сферах не слід розміщувати RPA-додатки за жодних обставин або лише за умови підвищених заходів безпеки?

Переваги RPA не викликають сумнівів. Водночас виникає небезпека систематичних помилок. Бот не ставить запитань, якщо це здається йому нелогічним, а радше бездумно виконує свої інструкції. Звичайно, бот не припускається необережних помилок, а також значно швидший за людину, але це і є проблемою. Адже систематична помилка може швидко призвести до того, що десятки тисяч процесів чи записів даних доведеться виправляти, якщо в них закралася систематична помилка: будь то записи в бухгалтерії, документах клієнтів чи навіть записи у ERP-системі. З цієї причини нагальним вбачається постійний і ретельний процес перевірки та затвердження протоколів роботи. Оскільки ці додатки, створені кінцевим користувачем, як правило, без знань програмування, є індивідуальною обробкою даних (IDV).

Регульовані установи в банківському середовищі вже добре знайомі з цим, наприклад, у використанні таблиць Excel з макросами та без них. Однак переваги точної інвентаризації IDV дуже високі для компаній у всіх секторах: навіть експертна третя сторона може швидко зорієнтуватися, надається мінімум пояснень, а кінцевий користувач змушений відповідати мінімальному стандарту якості. Зважаючи на те що RPA є проміжною технологією і фактично функціонує лише як перехідне рішення, поки інтерфейси та/або функції не стануть можливими у ERP-системі, така документація вбачається дуже корисною. Тому що існують дві безперечні переваги RPA, які все ще значною мірою недооцінюються сьогодні. Перша — структуроване документування змін процесів для специфікацій у разі адаптації в ERP-системі. Завдяки RPA можна точно задокументувати навіть міжсистемні / міжмодульні процеси. Друга — тестування коригувань в ERP-системі. Автоматизовані процеси RPA можуть зробити тестування після змін в модулях ERP набагато ефективнішим, наприклад, шляхом автоматичного моделювання 10 тис. або 100 тис. тестових кейсів за допомогою процесів RPA.

За принципом Парето, 80 % тестів можна автоматизувати за допомогою RPA, а ще 20 % індивідуальних тестів можуть виконувати ключові користувачі. Це повинно підвищити якість змін програмного забезпечення і водночас збільшити ефективність.

Хмарні обчислення. У користувачів виникають побоювання щодо доцільності зберігання даних у «хмарі» та безпечного користування інформацією. Постійно постають запитання: Що станеться, якщо виникнуть проблеми? Чи є можливість відновити дані? Наскільки захищені дані і що станеться у випадку їх вито-

ку? Це все слушні побоювання, які мають бути оцінені в стратегічному рішенні компанії. Тут немає готового рецепту.

Насамперед усе залежить від власної стратегічної орієнтації компанії, розуміння важливості мати доступ до інформації цілодобово, особливо для критично важливих даних. Організації, які постачають фінансові послуги, мають відносно суворі регуляторні вимоги від органів банківського нагляду щодо того, яких умов необхідно дотримуватися під час використання хмарних обчислень. Вони охоплюють інформацію про спроможність постачальників послуг, змісту договору аутсорсингу, питання про контроль та можливості примусового виконання зобов'язань у разі незадовільного перебігу подій.

Виникають проблеми, пов'язані зі зростаючими вимогами у сфері штучного інтелекту (ШІ), великих даних і постійного збільшення навантаження на дані через Інтернет речей, що підвищують важливість доступності та обсягів серверних потужностей, якими треба вчасно опікуватися. Зокрема, великі технологічні компанії інвестують великі ресурси для подальшого розширення свого лідерства в галузі ШІ. Виникає питання правильного балансу між вкладеними ресурсами та отриманою віддачею від них, і основна проблема полягає в тому, наскільки цього вимагають клієнти, чи потрібно використовувати максимальний ШІ, чи споживач послуг готовий оплатити це розширення і та ін. Перед використанням хмарних сервісів у будь-якому разі слід провести процес адаптації з окремим аналізом ризиків, а потім вже маштабувати одержані результати. Лише у такий спосіб аспекти управління ризиками будуть належно враховані під час прийняття стратегічного рішення цифровізації бізнесу.

Використовуйте можливості та мінімізуйте ризики. Цифровізація дає безліч можливостей для бізнесу, а й збільшує ризики. Тому треба бути готовим до того, що багато інвестицій у діджиталізацію, наприклад, у розвиток штучного інтелекту, таких сфер, як віртуальна та доповнена реальність, Інтернет речей тощо, мають тривалий період окупності. Хоча такі стратегічні інвестиції, як правило, розраховані на довгострокову перспективу, це не повинно слугувати виправданням для зниженням прибутковості компаній. Це ще одна причина, чому в таких випадках бізнес-план із прогнозом прибутковості слід регулярно переглядати і оновлювати.

На додаток до жорстких фінансових фактів, також коригуються або, принаймні, піддаються ретельній перевірці в деяких сферах «м'які» чинники, особливо у сфері корпоративної культури.

Наведемо приклад впровадження гнучкого підходу у компанії Manager Magazin до роботи в ING як «найрадикальніший лабораторний експеримент у німецькому корпоративному світі». Раптом існуючі ієрархії руйнуються, а працюючі менеджери опиняються в офісі з відкритим плануванням. Або з'являються нові способи діловодства з незліченною кількістю англіцизмів. Значна небезпека при таких радикальних змінах буде у втрачанні цінних, досвідчених співробітників або неможливості їх вчасного навчання новим цифровим компетенціям. Обидва варіанти однаково небезпечні.

Крім того, незважаючи на застосування новітніх методів, таких як Scrum, Sprint, Agile і та ін., завжди потрібно знаходити правильний баланс організації бізнес-процесів. Навіть гнучке управління проєктами з елементами Scrum не може обійтися без базової проєктної документації — особливо в IT-середовищі. І хоча, якщо слідкувати принципу «ділитися — значить піклуватися», усе ж таки не вся інформація може бути опублікована на «GitHub». Навіть всередині компанії не вся інформація і не всім повинна бути доступна. Пошук правильного балансу та потенційних ризиків витоку зайвої інформації є центральним завданням керівництва компанії.

Основна ідея діджиталізації — це не технології. Найбільшим викликом у процесі діджиталізації не є робота з новими технологіями чи проблеми їх впровадження. У більшості випадків це можна дуже легко освоїти. Це радше зміна підходу та культури компанії. Отже, це не стільки зміна жорстких параметрів бізнес-процесів, а й кардинально нова корпоративна культура організацій. Тому діджиталізація необов'язково повинна відбуватися в першу чергу в IT-відділі, головним завданням менеджерів є впровадження її в ДНК компанії. Окрім корпоративної культури, це особливо стосується культури лідерства та інновацій. Управління ризиками — не просто відділ організації, а функція, яка відіграє провідну роль, особливо в рамках стратегічного управління. Тому що компанія може бути успішною лише тоді, коли беруться до уваги не тільки можливості та передбачувані потреби клієнтів, а й цілісний погляд на стратегічні цілі з урахуванням ризиків.

У цьому контексті функція управління ризиками відіграє активну роль у підвищенні стійкості компанії. В останні роки термін «стійкість» став широковживаним і використовується в оцінюванні інвестиційної привабливості компанії. Однак у контексті застосування можливостей діджиталізації це прагнення тепер може бути реалізовано на практиці в конкретних термінах, вже включивши його в розробку і подальший розвиток бізнес-моделі.

Можливості позитивного впливу цифровізації на підприємницькі рішення пропорційно рівню ризикованості цих рішень. Кожна відповідальна особа повинна усвідомити цю можливість, але також і величезну відповідальність. Адже «цифровий дарвінізм» ще більше підвищить підприємницькі ставки в майбутньому. Чим раніше інноваційні ідеї будуть масштабовані, тим більша ймовірність того, що компанія стане успішною в довгостроковій перспективі. Виходячи з того факту, що цифровізація — це неминуча зміна, яка вже відбувається в усіх сферах бізнесу, окреслимо основні критичні поля виникнення ризиків та загроз: безпека даних, трансформація бізнес-процесів, надійність цифрових систем та інфраструктури. Аналіз літературних джерел та практики впровадження дозволяє виділити види ризиків, які найчастіше зустрічаються в сучасних умовах, розглянути взаємозв'язок із загрозами та заходами упередження (табл. 1).

Таблиця 1

ВИДИ РИЗИКІВ ТА ЗАХОДИ ЗАПОБІГАННЯ У ЦИФРОВІЙ ЕКОСИСТЕМІ ОРГАНІЗАЦІЙ

Види ризиків	Загрози втрат	Заходи упередження ризиків
Технологія / технологічні	Зароза втрат через технологічні збої або застарілі технології	Масштабованість, сумісність та функціональна точність впроваджуваних технологій
Кіберпростір / кібернетичні	Несанкціонований доступ (експлуатація мережі) з подальшим використанням проникнення для зловмисних дій, наприклад, вимагання та перешкоджання нормальному перебігу бізнес-процесів	Зміцнення платформи мережевої архітектури, безпека додатків, запобігання вразливості та моніторинг безпеки
Стратегія / стратегічні	Загроза втрат зазвичай пов'язана з цілями та завданнями організації. Зовнішній ризик викликає зміну стратегічного спрямування її діяльності та впливає на взаємодію з клієнтами, цінність бренду, репутацію та конкурентні переваги на ринку	Розвиток системи моніторингу, досягнення відповідного рівня контролю в операційних процедурах

Закінчення табл. 1

Критерій	Переваги	Недоліки
Дані / ризики витоку даних	Загроза витоку або втрати даних	Забезпечення захисту даних у цифровій екосистемі на різних етапах життєвого циклу; захист даних під час класифікації, зберігання,обробки, шифрування даних тощо
Треті особи (споживачі, постачальники) / сторонні	Ризики, що виникають через неналежний контроль з боку постачальників, сторонні операційні середовища, їх кібервразливість	обмін даними, інтеграція технологій, залежності від операцій, стійкість до відмови постачальників і та ін.
Конфіденційність / ризики конфіденційності	Загрози, що виникають через неналежне поводження з особистими та конфіденційними персональними даними клієнтів, співробітників,тощо	Дотримання принципів конфіденційності: повідомлення, вибору, згоди, точності і та ін.
Нормативно-правове середовище / нормативні	Загроза втрат через впровадження будь-яких нових вимог або правил, які виходять за рамки існуючих в організації уможливіть ризик недотримання нормативних вимог щодо бізнес-операцій, зберігання даних та інших правил ведення бізнесу	Дотримання законодавчих вимог, які містять закони стособно технологій, міжнародне та галузеве законодавство та нормативні акти
Стійкість компаній / ризики втрати стійкості	Ризики збоїв в роботі або недосяжності послуг через занадто високі залежності від тісно пов’язаних технологій	Неперервність бізнес-процесів, аварійне відновлення ІТмереж, кіберстійкість та антикризове управління
Персонал / кадрові	Низька цифрова обізнанність співробітників, плинність персоналу	Розвиток людських ресурсів, навчання та підвищення цифрової грамотності; аутсорсинг персоналу

Висновки. Узагальнемо результати аналізу впливу діджизалізації на сучасну систему ризик-менеджменту та сформулюємо

основні положення, які є базовими з позицій інтерпретації сутності досліджуваного поняття.

Окреслимо три основні рівні побудови системи захисту від цифрових ризиків: тактичний, оперативний, стратегічний. На тактичному рівні фахівці рекомендують ідентифікувати уразливі системи та по можливості вчасно видаляти їх.

Крім того, до мінімізації цифрових ризиків приведуть дії з блокування мережі (домена та IP-адреси через існуючі проксі-сервери або елементи керування периметром).

Операційний підхід використовується для постійного моніторінгу ризиків цифровізації: реалізується стратегія безперервного моніторингу домену, зокрема. моніторинг ризику інцидентів, їх виявлення, вивчення та обліку.

Стратегічний підхід пов'язаний із необхідністю оновлення моделей ризиків і загроз. Засоби забезпечення належного рівня безпеки організації повинні постійно оновлювати моделі загроз з урахуванням критичних цифрових активів, і навіть пов'язаних з третіми сторонами та ланцюгами постачання. Рекомендується інтегрувати керування цифровими ризиками у загальні процеси існуючого ризик-менеджменту в організації.

Загальні напрями мінімізації цифрових ризиків на рівні організації, на наш погляд, тісно пов'язані з подальшим прогресом цифрових технологій — штучного інтелекту, Інтернетом речей та «розумних» мереж, блокчейном, інтегрованими системними центрами з обробки великих даних, з розвитком технологій десенсибілізації даних, оцінки та сертифікації відповідності вимогам безпеки, механізмів захисту шифрування та пов'язаних з ними методів технічного моніторингу для збирання та інтеграції масових даних тощо.

Література

1.Glaserhttps.C., Risikomanagement im Kontext Digitalisierung. *Ganzheitliche Digitalisierung.2021* https://www.risknet.de/themen/risknews/risikomanagement-im-kontext-digitalisierung/(дата звернення 20.10.2023).

2. Данченко О. Б., Ланських Є. В., Семко О. В. Інформаційні ризики цифрового формату, *Вісник ЧДТУ 2020*, № 3, С. 58–66.

3. Blanka C., Krumay B., Ruecke D. The interplay of digital transformation and employee competency: A design science approach. *Technological Forecasting and Social Change.* 2022. p. 121. doi: 10.1016/j.techfore.2022.121575.

4. Ведерніков М. Д., Волянська-Савчук Л. В., Чернушкіна О. О., Базалійська Н. П. Цифрова трансформація у сфері hr-процесів: напрями, проблеми та можливості. *Збірник наукових праць Черкаського держав-*

ного технологічного університету.Серія:Економічні науки. 2022. Вип. 66, С. 39–48. URL: https://doi.org/10.24025/2306-4420.66.2022.268584. (дата звернення 20.10.2023).

5. Дубина М., Козлянченко О. Концептуальні аспекти дослідження сутності діджиталізації та її ролі в розвитку сучасного суспільства. *Проблеми і перспективи економіки та управління.* Випуск № 3 (19), 2019. С. 21–32

6. Bencsik A., Hargitai D.M., Kulachinskaya A. Trust in and Risk of Technology in Organizational Digitalization. Risks. 2022. № 5. p. 90. doi: 10.3390/risks10050090

7. Економічна стратегія України 2030. *Український інститут майбутнього*. URL: https://strategy.uifuture.org/index.html

8. Гранатуров В. М., Кораблінова І. А. Інформаційний ризик підприємства: щодо вирішення проблеми qui pro quo у визначенні поняття. *Інноваційна економіка*. 2017. № 5-6 (69). С. 199–206.

References

1.Christian Glaserhttps. Risikomanagement im Kontext Digitalisierung. *GanzheitlicheDigitalisierungsinitiativen*.22.06.2021.https:www.risknet.de/themen/risknews/risikomanagement-im-kontext-digitalisierung(data zvernennya: 20.10.2023)

2. Danchenko O. B., Lanskikh E. V., Semko O. V, 2020; Informaciyni ryzyky cifrofogo formatu [Information risks of digital format] *ChDTU Bulletin 2020*, № 3, C. 58–66. [in Ukrainian]

3. Blanka C., Krumay B., Ruecke D. The interplay of digital transformation and employee competency: A design science approach. *Technological Forecasting and Social Change*. 2022. p. 121575. doi: 10.1016/j.techfore.2022.121575.

4.Vedernikov M. D., Volyanska-Savchuk L. V., Chernushkina O. O., Bazaliyska N.P. Cifrova transformaciya u sferi hr-procesiv: napryamky, problemy ta mojlyvosty [Digital transformation in the sphere of hr-processes: directly, problems and possibilities]. *Collection of scientific works of the Cherkasy State Technological University. Series: Economic Sciences. 2022. VIP. 66. p. 39–*48. URL: https://doi.org/10.24025/2306-4420.66.2022.268584(data zvernennya: 20.10.2023)[in Ukrainian]

5. Dubina M., Kozlyanchenko O. Konceptualni aspekty doslidjeniia sutnosti didjitalizaciyi ta roli v rozvytku suchasnogo suspilstva [Conceptual aspects of studying the essence of digitalization and its role in the development of daily marriage] *Problems and prospects of economics and management. Vipusk № 3 (19), 2019 p. 21–32*[in Ukrainian]

6. Bencsik A., Hargitai D. M., Kulachinskaya A. Trust in and Risk of Technology in Organizational Digitalization. Risks. 2022. № 5. p. 90. doi: 10.3390/risks10050090

7. Ukrainian Institute of the Future. (2022). Ekonomichna stratehiia Ukrainy 2030 [Economic Strategy of Ukraine 2030].URL: https://strategy.uifuture.org/index.html (data zvernennya: 20.10.2023)

8. Granaturov V. M., Korablinova I. A. Informacijny'j ryzyk pidpriemstva sho do vuryshennya problemy qui pro quo u vuznachenny ponyattya [Information risk of entrepreneurship: how the problem of qui pro quo has increased in the established concept], *Innovation Economics, № 5-6 (69), p. 199–206, 2017*. [in Ukrainian]

Стаття надійшла до редакції 30.09.2023.