УДК 338.14
JEL: L86; M21
DOI: https://doi.org/10.32983/2222-4459-2023-7-83-91

ВПЛИВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ НА ФОРМУВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

©2023 БІЛИЧЕНКО М. М., КАСЬЯНОВА Н. В.

УДК 338.14
JEL: L86; M21

Біличенко М. М., Касьянова Н. В. Вплив цифрової трансформації на формування системи економічної безпеки підприємства

Мета статті полягає в дослідженні особливостей формування системи економічної безпеки підприємства з урахуванням ризиків, які виникають в умовах цифрової трансформації. При аналізі, систематизації й узагальненні наукових праць багатьох вітчизняних та іноземних учених було детально розглянуто особливості цифрової трансформації підприємства та її вплив на складові загальної системи економічної безпеки підприємства. У результаті дослідження було виділено й узагальнено основні проблеми та ризики, з якими стикаються більшість підприємств, що знаходяться у процесі цифрової трансформації, зокрема виділено такі групи: технологічні, операційні, управлінські, фінансові та ризики конфіденційності. Визначено негативний вплив нових ризиків, які пов'язані із цифровою трансформацією, на фінансову, технологічну, інформаційну, кадрову та інтелектуальну підсистеми загальної системи економічної безпеки підприємства. Обґрунтовано, що ефекти від реалізації нових ризиків можуть мати деструктивний характер щодо діяльності всього суб'єкта господарювання та призвести до істотних фінансових, економічних та організаційних втрат підприємства. Запропоновано поетапне управління ризиками в системі економічної безпеки підприємств, що перебувають в процесі цифрової трансформації, а саме: ідентифікація та діагностика нових ризиків; оптимізація ризику; моніторинг стану економічної безпеки підприємства. З метою забезпечення нормального функціонування та мінімізації дії негативних факторів та ризиків цифрової трансформації сформовано такі пропозиції: впровадження та використання комплексної автоматизованої системи управління та раціоналізації бізнес-процесів; використання хмарних обчислень і рішень SaaS; розробка необхідних матеріалів для навчання персоналу; використання нових інформаційно-комунікативних та аналітичних технологій; забезпечення інвестицій у розвиток цифрових навичок; укладання угод з технологічними партнерами; розвиток культури інновацій та адаптивності. Перспективами подальших досліджень у даному напрямі є визначення та кількісна оцінка впливу цифрової трансформації на систему економічної безпеки підприємства, а також розробка підходів до управління новою системою економічної безпеки на основі використання новітніх технологій штучного інтелекту та цифровізації бізнес-процесів.
Ключові слова: *цифрова трансформація, економічна безпека, підприємство, ризик, управління ризиками.*
Рис.: *4.* ***Бібл.:*** *27.*

Біличенко Максим Миколайович *– аспірант, Національний авіаційний університет (просп. Любомира Гузара, 1, Київ, 03058, Україна)*
E-mail: *mbilich9@gmail.com*
ORCID: *https://orcid.org/0000-0003-4657-1039*
Researcher ID: *https://www.webofscience.com/wos/author/record/HDM-2240-2022*
Касьянова Наталія Віталіївна *– доктор економічних наук, професор, завідувачка кафедри бізнес-аналітики і цифрової економіки, Національний авіаційний університет (просп. Любомира Гузара, 1, Київ, 03058, Україна)*
E-mail: *nat_kas@ukr.net*
ORCID: *https://orcid.org/0000-0001-7729-2011*
Researcher ID: *https://www.webofscience.com/wos/author/record/S-5635-2018*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=55990612200*

UDC 338.14
JEL: L86; M21

Bilychenko M. M., Kasianova N. V. The Impact of Digital Transformation on the Formation of the Enterprise's Economic Security System

The article is aimed at studying the features of formation of the system of economic security of enterprise, taking into account the risks that arise under conditions of digital transformation. When analyzing, systematizing and generalizing scientific works of many domestic and foreign scholars, the features of the digital transformation of the enterprise and its impact on the components of the overall system of economic security of the enterprise were considered in detail. As result of the study, the main problems and risks faced by the majority of enterprises in the process of digital transformation were identified and summarized, in particular, the following groups were allocated: technological, operational, managerial, financial and risks to privacy. The negative impact of the novel risks associated with digital transformation on the financial, technological, informational, personnel, and intellectual subsystems of the general system of economic security of enterprise is determined. It is substantiated that the effects of materialization of new risks can be destructive in relation to the activities of the entire economic entity and lead to significant financial, economic and organizational losses of enterprise. The step-by-step risk management in the system of economic security of enterprises undergoing digital transformation has been proposed, which includes: identification and diagnosis of further risks; risk optimization; monitoring of the state of economic security of the enterprise. In order to ensure the normal functioning and also to minimize the effect of negative factors and risks of digital transformation, the following proposals are formed: introduction and use of an integrated automated system of management and rationalization of business processes; use of cloud computing and SaaS solutions; development of necessary materials for staff training; use of new information-communicative and analytical technologies; ensuring investment in the development of digital skills; concluding agreements with technology partners; development of a culture of innovation and adaptability. Prospects for further research in this direction are the definition and quantitative assessment of the impact of digital transformation on the system of economic security of enterprise, as well as the development of approaches to managing a new system of economic security based on the use of the latest technologies of artificial intelligence and digitalization of business processes.
Keywords: *digital transformation, economic security, enterprise, risk, risk management.*
Fig.: *4.* ***Bibl.:*** *27.*

Bilychenko Maksym M. *– Postgraduate Student, National Aviation University (1 Liubomyra Husara Ave., Kyiv, 03058, Ukraine)*
E-mail: *mbilich9@gmail.com*
ORCID: *https://orcid.org/0000-0003-4657-1039*
Researcher ID: *https://www.webofscience.com/wos/author/record/HDM-2240-2022*
Kasianova Nataliia V. *– D. Sc. (Economics), Professor, Head of the Department of Business Analytics and Digital Economy, National Aviation University (1 Liubomyra Husara Ave., Kyiv, 03058, Ukraine)*
E-mail: *nat_kas@ukr.net*
ORCID: *https://orcid.org/0000-0001-7729-2011*
Researcher ID: *https://www.webofscience.com/wos/author/record/S-5635-2018*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=55990612200*

Цифрові технології вже увійшли в переважну більшість сфер нашого життя, зокрема в: освіту, навчання, засоби масової інформації, робоче середовище, повсякденне життя, спорт, сприяння здоров'ю та розваги. Майбутнє цифрове суспільство створить досить складну, але повністю трансформовану екосистему як технологій, так і людей, які матимуть нове, інше спільне життя та співіснування.

Цифрова трансформація є дуже дорогим і довготривалим процесом для будь-яких підприємств, особливо для малого та середнього бізнесу. З цього випливає те, що компанії повинні чітко визначити свої цифрові стратегії, тобто ті сфери цифрової трансформації, які є для них пріоритетними. На основі цих пріоритетів підприємства змушені сприймати зміни та впроваджувати нові інноваційні рішення, пов'язані з цифровою трансформацією, як програмні так і методологічні. Ці рішення можуть мати багато позитивних наслідків, але водночас будуть представляти для них нові, раніше не відомі загрози та ризики, на які потрібно звертати увагу та які треба буде враховувати для забезпечення загальної економічної безпеки підприємства та кожної з її підсистеми.

Значний внесок у дослідження процесу провадження цифрової трансформації на підприємствах і наслідків диджиталізації зробили такі вітчизняні та закордонні вчені, як С. Берман (*S. J. Berman*) [1], Б. Гебремескел, Г. Джонатан, С. Ялей (*B. Gebremeskel, G. Jonathan, S. Yalew*) [2], А. Болтон, Л. Гузен, Е. Кріцінгер (*A. Bolton, L. Goosen, E. Kritzinger*) [3], С. Шкарлет, І. Садчикова [4], Г. Чміль [5], В. Вовк зі співавторами [6]. Проте питання впливу цифрової трансформації на систему економічної безпеки через призму аналізу ризиків в проаналізованих роботах не було достатньо вивчене і потребує більш ґрунтовного дослідження.

Метою статті є дослідження особливостей формування системи економічної безпеки підприємства з урахуванням ризиків, які виникають в умовах цифрової трансформації.

У науковій літературі існує багато різних визначень поняття цифрової трансформації підприємства. Так, у роботі С. Бермана [1] цифрова трансформація розглядається як серія загально-організаційних змін в управлінні та інформаційних технологіях (ІТ) у відповідь на нові зміни в зовнішньому середовищі. З іншого боку, Г. Віал (*G. Vial*) [7] у своєму дослідженні виділяє цифрову трансформацію як процес, у якому цифрові технології створюють збурення, викликаючи стратегічну реакцію організацій, які прагнуть змінити свої шляхи створення цінності, одночасно керуючи структурними змінами та організаційними бар'єрами, які впливають на позитивні та негативні результати цього процесу. За словами І. Гьокальпа та В. Мартінеса (*E. Gökalp, V. Martinez*) [8], цифрову трансформацію можна визначити як революційне технологічне досягнення, яке приносить нові бізнес-моделі та операційні моделі в усі сектори.

Загалом, огляд наявної літератури вказує на те, що організації отримують вигоду, коли інтегрують нові цифрові технології в існуючі бізнес-процеси та ІТ-інфраструктуру відповідно до загальних організаційних цілей. Емпіричні дослідження також доводять, що успішна цифрова трансформація допомагає організаціям поліпшити комунікацію між постачальниками, підприємством і партнерами для створення додаткової вартості [9].

Водночас поряд з інноваційними можливостями, які можуть бути реалізовані завдяки впровадженню процесів цифрової трансформації на підприємствах, виникає велика кількість нових ризиків та загроз, які з'являються під час цього процесу. Дослідження, проведене корпорацією Майкрософт, показує, що 62% малих і середніх підприємств по всьому світу називають проблеми кібербезпеки ключовим викликом на шляху цифрової трансформації [10]. Зокрема, страх перед витоком даних і кіберзагрозами перешкоджає бажанню повністю впроваджувати в діяльність підприємства цифрові технології.

Доцільно виділити ключові проблеми та ризики, з якими стикаються більшість підприємств, які знаходяться або планують впроваджувати цифрову трансформацію в себе на підприємстві.

1. *Технологічні ризики* – потенційні втрати через збій технології. Згідно зі звітом Всесвітнього економічного форуму [11] саме кібератаки та кіберзлочинність належать до топ-10 найбільших ризиків, які загрожують людству як у найближчій, так і в довгостроковій перспективі. Поряд зі зростанням кіберзлочинності спроби порушити роботу критично важ-

ливих технологічних ресурсів і послуг стануть більш поширеними, з можливими атаками проти сільського господарства та водопостачання, фінансових систем, транспорту, енергетики, побутової, космічної та підводної комунікаційної інфраструктури.

До цього блоку також можна віднести найбільш поширені кіберризики, пов'язані з несанкціонованим доступом до цифрового середовища підприємства, забезпечення конфіденційності та цілісності технологічних систем. Більше того, згідно з опитуванням, проведеним компанією PwC у 2022 р., більше 4 тисяч генеральних директорів вважають кіберризики найбільшою загрозою для розвитку та безпеки власних підприємств [12].

2. *Ризики конфіденційності* виникають через неналежне поводження з персональними та конфіденційними даними клієнта або працівника, що може вплинути на конфіденційність особи [13]. Також до цього блоку можна додати ризики витоку даних, тобто ризики щодо неналежного забезпечення захисту даних у цифровій екосистемі на різних етапах життєвого циклу даних.

Так, згідно з дослідженням IBM [14] витрати, пов'язані з витоком даних, у 2022 р. становили в середньому $4,35 млн, що є рекордним показником за останні 17 років. Як показано на *рис. 1*, середня вартість витоку даних у світі в середньому зростає на 4% на рік. Більш того, 52% опитаних компаній у всьому світі виявляли порушення конфіденційності власних даних, причому з них 35% зазнавали витоку інформації або даних за останній рік [15]. Отже, більше половини підприємств у всьому світі мають проблеми з правильним зберіганням, обробкою та використанням конфіденційної інформації, а значить, ризик конфіденційності становить суттєву загрозу для них. Так, витік даних компанії Okta у 2022 р. зменшив її ринкову капіталізацію приблизно на $6 млрд протягом тижня, коли відповідний інцидент був оприлюднений [16].

3. *Фінансові ризики* – витрати на впровадження цифрових технологій та засобів контролю економічної безпеки можуть стати фінансовим тягарем для компанії. Більше того, початкові бюджети на цифрову трансформацію часто не враховують багато факторів (наприклад, навчання своїх співробітників, коригування робочих процесів, підготовку посібників і оновлення своєї політики), що може призвести до затримки впроваджень. Згідно з дослідженням [17] 70% цифрових перетворень перевищують початкові бюджети, а 7% у підсумку обходяться вдвічі дорожче початкового прогнозу.

Згідно з опитуванням компанії McKinsey, ті організації, які протягом останніх двох років здійснили масштабні зміни в напрямку цифрової трансформації, отримали набагато менше прибутку, ніж спочатку очікували [18]. Відповідно до даних на *рис. 2* у середньому компанії змогли отримати лише 31% від додаткового прибутку, який очікували внаслідок технологічних змін. Ці дані підтверджуються іншим дослідженням [19], яке показало, що лише 30% цифрових трансформацій досягли або перевищили цільове значення та привели до стійких змін у діяльності організацій, тоді як інші ініціативи створили певну цінність, але не привели до суттєвих позитивних змін.

4. *Операційні ризики* – ускладнення процесів взаємодії всередині та за межами організації та зниження загальної продуктивності. Цифрова трансформація має на меті зробити взаємодію між співробітниками, організаціями та іншими зацікавленими сторонами плавною та ефективною, проте для зменшення ризику порушення інформаційної безпеки багато організацій створюють певні засоби контролю, додаткові правила та процедури, обмежують можливість доступу до інформації різним групам робітни-

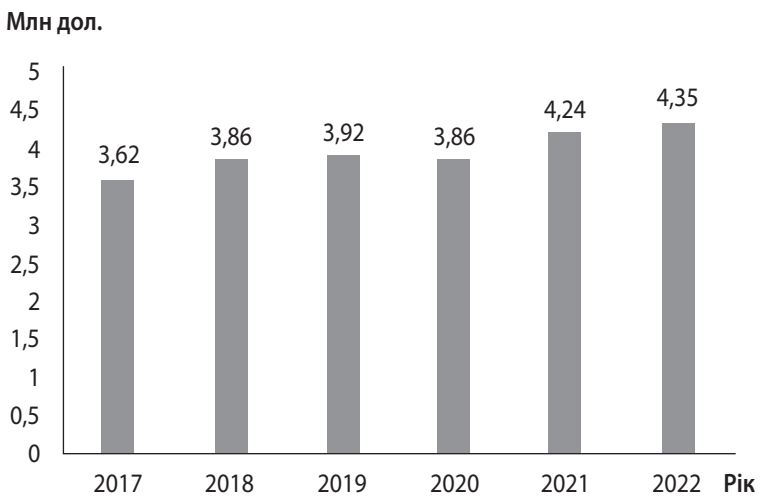

Рис. 1. Динаміка середньої вартості одного витоку даних у світі ($ млн)

Джерело: сформовано авторами на основі [14].

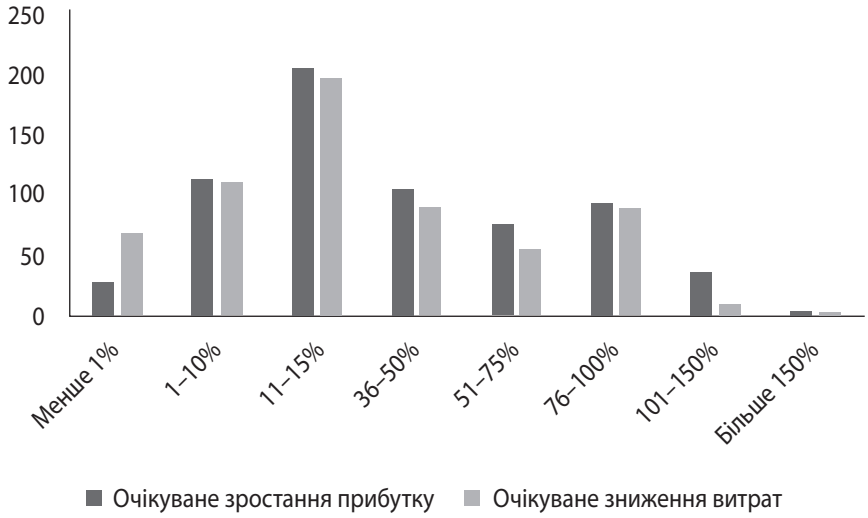

Рис. 2. Частка реалізованого фінансового прибутку та частка зниження витрат від цифрової трансформації (кількість респондентів, од.)

Джерело: сформовано авторами на основі [18].

ків. Виявлено, що лише 16% респондентів вважають, що цифрова трансформація їхніх організацій підвищила продуктивність [20]. Тоді як заходи інформаційної безпеки потенційно можуть знижувати продуктивність робітників і можливості співпраці з іншими компаніями [2].

5. *Управлінські ризики* пов'язані з необхідністю комплексного управління економічною безпекою в умовах цифрової трансформації. Цей ризик включає відсутність ресурсів для контролю та впровадження цифрової трансформації на підприємствах, зокрема експертів з економічної та інформаційної безпеки та менеджерів з цифрової трансформації. Згідно з дослідженням [21] значною перешкодою для цифрової трансформації на малих і середніх підприємствах є дефіцит людських ресурсів з необхідними знаннями та здатністю відповідати критеріям процесу цифрової трансформації.

За результатами Всесвітнього економічного форуму «Робота майбутнього» [22] саме нестача кваліфікованих спеціалістів на ринку праці є найбільшою перешкодою та проблемою, з якою компанії стикаються перед упровадженням нових технологічних змін (*рис. 3*).

Таким чином, сучасна система економічної безпеки підприємства має бути адаптована до появи перелічених нових ризиків, які виникають внаслідок проведення цифрової трансформації.

У загальному розумінні, економічна безпека підприємства – це певний стан розвитку підприємства, за якого забезпечується стабільність фінансового та економічного розвитку та ефективний контроль усіх ризиків та негативних факторів, які можуть діяти на підприємстві [23]. Більш повне визначення дає О. Марченко через призму багатоаспектного підходу, за якого економічна безпека розглядається як стан захищеності підприємства від можливо негативного впливу загроз з боку внутрішнього та зовнішнього середовища, що характеризується певними результатами діяльності та підлягає управлінню з боку системи менеджменту [24]. Метою системи економічної безпеки підприємства є захист підприємства від внутрішніх і зовнішніх загроз та ризиків для досягнення найбільш можливого рівня ефективності.

Отже, економічна безпека підприємства – це складна багатогранна система, в якій можна виділити окремі підсистеми, що в сукупності забезпечують досягнення стратегічних і тактичних цілей, а саме: фінансову, політико-правову, кадрову, техніко-технологічну, інформаційну та екологічну складові.

Розглянемо вплив вищезазначених ризиків на ключові підсистеми економічної безпеки підприємства внаслідок реалізації та проведення цифрової трансформації.

Фінансова підсистема, що характеризує досягнення суб'єктом підприємництва раціонального використання ресурсів, в умовах цифрової трансформації вимагає створення відповідних інформаційних систем, розробки програмного забезпечення та належних засобів захисту інформації. Підприємствам необхідно враховувати, прогнозувати та забезпечувати необхідні фінансові витрати для навчання співробітників, коригування робочих процесів, підготовки посібників і оновлення своєї політики. Управління фінансовими ризиками як інструмент створення економічної безпеки є актуальною вимогою сучасності для забезпечення фінансової стійкості компанії в умовах цифрової трансформації.

Технологічна підсистема. Використання нових цифрових технологій, таких як технології штучного

Рис. 3. Перешкоди для впровадження нових технологій

Джерело: сформовано авторами за [22].

інтелекту, технології роботи з великими даними, здобутків роботехніки, використання хмарних технологій та Інтернету речей приводить то суттєвого поліпшення ефективності бізнес-процесів суб'єктів господарювання. Водночас потребують вдосконалення застарілі технологій, які використовуються підприємством; необхідно забезпечити своєчасне оновлення програмного забезпечення та реалізацію наукових досягнень відповідно до завдань цифрової трансформації. Ці ризики також можуть бути взаємопов'язані з фінансовими, оскільки первинні витрати на інновації зазвичай мають суттєвий вплив на фінансове становище підприємств, особливо малих і середніх, а невизначений попит на інноваційну продукцію ускладнює можливість точного прогнозування прибутку від упровадження цифрових технологій.

Інформаційна підсистема спрямована на забезпечення цифрової та інформаційної безпеки та є одним із пріоритетних напрямів діяльності підприємства щодо ефективного захисту від зовнішніх кібератак на внутрішні інформаційно-комунікативні системи та забезпечення максимального рівня конфіденційності даних. В умовах цифровізації з'являються нові можливості в частині виявлення, вимірювання, реєстрації, накопичення, узагальнення та передачі інформації відповідно до інформаційних потреб системи управління. Водночас, широке використання інформаційно-комунікаційних технологій призводить до якісно та кількісно нового рівня інформаційних загроз для підприємства, зокрема несанкціонованого доступу до комерційної таємниці та іншої звітності, витоку конфіденційної інформації. Забезпечення інформаційної безпеки підприємства є одним із найбільших викликів, який цифрова трансформація ставить перед менеджментом підприємства.

Інтелектуальна та кадрова складові економічної безпеки підприємства реалізуються шляхом ефективного управління персоналом підприємства. Наслідки цифрової трансформації включають в себе більшу еміграцію національного інтелектуального капіталу, дефіцит підготовлених професіоналів із цифровими навичками та збільшення дисбалансів на ринку праці [25]. Нагальні зміни необхідних навичок і компетенцій призводять до розриву між професійними профілями, доступними на ринку праці, і тими, що потрібні компаніям [26]. Цифрова трансформація збільшує складність і абстрактність завдань, що вирішуються робітниками підприємства. Крім того, ризики втрати конфіденційної інформації чи витоку даних потребують постійного контролю за правилами поводження працівників з даними та надання різного рівня доступу до інформації, що, своєю чергою, потребує вдосконалення відповідних навичок праці та поліпшення існуючих процедур і протоколів роботи з даними та програмним забезпеченням компанії. З огляду на це, слід констатувати наявність низки кадрових ризиків у діяльності підприємств та існування необхідності забезпечення їх кадрової безпеки.

Для забезпечення нормального функціонування та мінімізації дії негативних факторів та ризиків доцільно виділити такі ініціативи в системі економічної безпеки, які можуть бути реалізовані підприємствами, що перебувають у процесі цифрової трансформації:

- *впровадження та використання комплексної автоматизованої системи управління та раціоналізації бізнес-процесів підприємства* для забезпечення їх інформаційної інтеграції,

наприклад систем технологічної підготовки виробництва – CAM, управління проєктними даними – PDM, управління взаємостосунками з клієнтами – CRM тощо [27];

- *використання хмарних обчислень і рішень SaaS:* хмарні технології, включно з рішеннями «Програмне забезпечення як послуга», пропонують гнучкість, масштабованість і економічну ефективність. Використовуючи хмарні платформи, компанії, а особливо малий і середній бізнес, можуть отримати доступ до розширених функціональних можливостей без необхідності значних початкових інвестицій в апаратне забезпечення чи інфраструктуру. Хмарні обчислення також забезпечують перевагу автоматичних оновлень і посилених заходів безпеки, що полегшує деякі проблеми, пов'язані з обслуговуванням і кібербезпекою;
- *розробка необхідних управлінських і методичних матеріалів* для навчання персоналу щодо використання нових інформаційно-комунікативних та аналітичних технологій;
- *вдосконалення організаційної структури управління підприємством* з метою підвищення якості та швидкості взаємодії персоналу; заміна організаційних структур ієрархічного типу на адаптивні; створення позиції менеджерів з цифрової трансформації та їх належну підготовку;
- *інвестиції в розвиток цифрових навичок працівників підприємства:* розробка та впровадження навчальних програм, ініціатив з підвищення кваліфікації або навіть партнерства із зовнішніми організаціями чи консультантами для подолання розриву в навичках;
- *укладання угод з технологічними партнерами:* співпраця з технологічними партнерами, такими як постачальники програмного забезпечення, консультанти або системні інтегратори, може надати підприємствам досвід і рекомендації, необхідні для успішної цифрової трансформації. Ці партнери можуть допомогти у виборі правильних технологій, впровадженні рішень і подоланні технічних проблем, дозволяючи компаніям використовувати зовнішні знання та ресурси. Також це дозволить зменшити початкові інвестиції та мінімізувати можливі ризики витоку даних через некоректний і неправильний вибір програмного забезпечення;
- *розвиток культури інновацій та адаптивності: створення культури, яка заохочує інновації, експерименти та адаптацію*, має важливе значення для успішної цифрової трансформації. Компанії повинні сприяти навчанню, заохочувати співпрацю та надавати працівникам можливість вносити ідеї та приймати зміни. Культура інновацій дозволить підприємствам постійно досліджувати нові технології й адаптуватися до мінливих ринкових умов.

Зазначені ініціативи в системі економічної безпеки доцільно покласти в основу формування стратегії економічної безпеки підприємства. Загальну модель формування системи економічної безпеки підприємства під час цифрової трансформації наведено на *рис. 4*.

Підбиваючи підсумки, слід зазначити, що підприємства повинні почати з розробки чітко визначеної стратегії цифрової трансформації, яка відповідає їхнім бізнес-цілям і враховує нові види ризиків. Ця стратегія має окреслити бажані результати, визначити ключові сфери впровадження цифрових технологій та повинна стати основною для визначення нових можливостей і загроз, які цифрова трансформація буде мати стосовно загальної системи економічної безпеки підприємства.

ВИСНОВКИ

Таким чином, в умовах цифрової трансформації підприємства повинні адаптувати свою загальну систему економічної безпеки до нових ризиків, які можуть виникнути внаслідок упровадження цифрових інновацій. У зв'язку з цим доцільно виокремити такі етапи управління ризиками в системі економічної безпеки підприємств, що перебувають в процесі цифрової трансформації:

- ідентифікація та діагностика нових ризиків, пов'язаних з цифровою трансформацією, включно з характеристикою, значущістю та контрольними показниками, які використовуватимуться для визначення цього ризику.
- мінімізація ризику: впровадження ініціатив, які відповідають стратегічним цілям цифрової трансформації підприємства.
- моніторинг стану економічної безпеки підприємства: розрахунок основних показників кожної підсистеми загальної системи економічної безпеки, визначення загального рівня економічної безпеки, якісний і кількісний аналіз роботи з визначеними ризиками, аналіз і перевірка виконання планів.

Отже, забезпечення економічної безпеки в умовах цифровізації має базуватися на цифровій безпеці – тобто на формуванні якісно нових факторів, що сприяють участі підприємств в єдиній інформаційній, кадровій, технологічній, фінансовій системах для забезпечення економічної безпеки підприємств та зниження зовнішніх і внутрішніх ризиків. ■

БІБЛІОГРАФІЯ

1. Berman S. J. Digital transformation: opportunities to create new business models. *Strategy & Leadership*. 2012. Vol. 40. Iss. 2. P. 16–24. DOI: https://doi.org/10.1108/10878571211209314

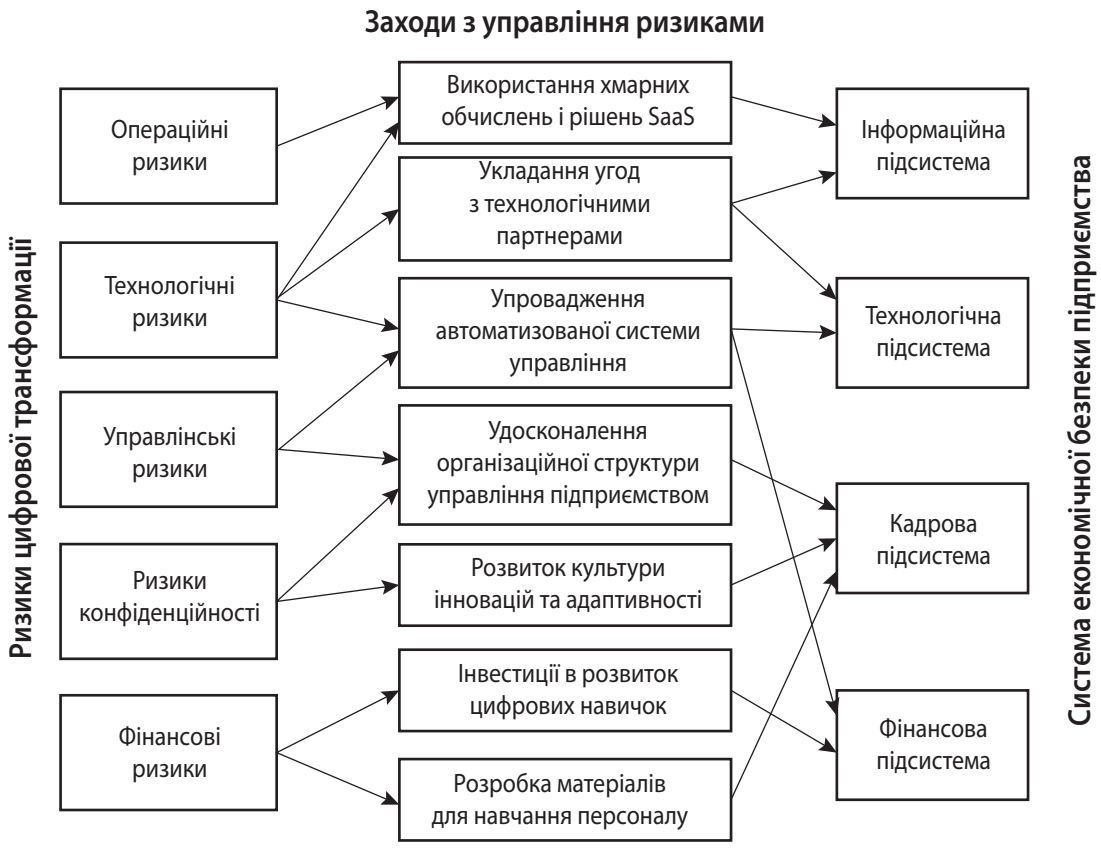

Рис. 4. Загальна схема управління економічною безпекою підприємства в умовах цифрової трансформації

Джерело: авторська розробка.

2. Gebremeskel B., Jonathan G., Yalew S. Information Security Challenges During Digital Transformation. *Procedia Computer Science*. 2023. Vol. 219. P. 44–51. DOI: https://doi.org/10.1016/j.procs.2023.01.262
3. Bolton A., Goosen L., Kritzinger E. Security aspects of an empirical study into the impact of digital transformation via unified communication and collaboration technologies on the productivity and innovation of a global automotive enterprise. *Information and Cyber Security*. 2020. P. 99–113 DOI: https://doi.org/10.1007/978-3-030-43276-8_8.
4. Шкарлет С., Садчикова І. Трансформація системи фінансово-економічної безпеки підприємства в умовах цифрової економіки. *Проблеми і перспективи економіки і управління*. 2019. № 3. С. 264–276. DOI: https://doi.org/10.25140/2411-5215-2019-3(19)-264-276
5. Чміль Г. Л. Цифровізація діяльності суб'єктів споживчого ринку: можливості та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм»*. 2021. Вип. 13. С. 124–134. DOI: https://doi.org/10.26565/2310-9513-2021-13-13
6. Vovk V. et al. Financial monitoring in the bank as a market instrument in the conditions of innovative development and digitalization of economy: management and legal aspects of the risk-based approach. *International Journal of Industrial Engineering & Production Research*. 2020. Vol. 31. Iss. 4. P. 559–570. DOI: https://doi.org/10.22068/ijiepr.31.4.559
7. Vial G. Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*. 2019. Vol. 28. Iss. 2. P. 118–144. DOI: https://doi.org/10.1016/j.jsis.2019.01.003
8. Gökalp E., Martinez V. Digital transformation capability maturity model enabling the assessment of industrial manufacturers. *Computers in Industry*. 2021. Vol. 132. Art. 103532. DOI: https://doi.org/10.1016/j.compind.2021.103522
9. Matt Ch., Hess Th., Benlian A. Digital Transformation Strategies. *Business & Information Systems Engineering*. 2015. Vol. 57. P. 339–343. DOI: https://doi.org/10.1007/s12599-015-0401-5
10. Yvanovich R. Navigating Challenges: the Worrying State of Digital Transformation for SMEs. URL: https://blog.trginternational.com/digital-transformation-sme-small-medium-sized-enterprises
11. The Global Risks Report 2023. 18th Edition / World Economic Forum. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
12. PwC's 25th Annual Global CEO Survey: Reimagining the outcomes that matte. URL: https://www.pwc.com/gx/en/ceo-survey/2022/main/content/downloads/25th_CEO_Survey.pdf
13. Managing Risk in Digital Transformation / Deloitte. October 2018. URL: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf
14. Cost of a Data Breach. Report 2022. URL: https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf

15. 2023 Thales Data Threat Report: Global Edition. URL: https://cpl.thalesgroup.com/data-threat-report
16. Huang K., Wang X., Wei W., Madnick S. The Devastating Business Impacts of a Cyber Breach. URL: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach#:~:text=Managing%20Cyber%20Risk&text=On%20average%2C%20companies%20experiencing%20a,and%20cost%20to%20secure%20financing
17. Babbar A., Janardhanan R., Paternoster R., Soller H. Why most digital banking transformations fail – and how to flip the odds. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/why-most-digital-banking-transformations-fail-and-how-to-flip-the-odds
18. LaBerge L., Smaje K., Zemmel R. Three new mandates for capturing a digital transformation's full value. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-new-mandates-for-capturing-a-digital-transformations-full-value
19. Forth P., Reichert T., De Laubier R., Chakraborty S. Flipping the Odds of Digital Transformation Success. URL: https://www.bcg.com/publications/2020/increasing-odds-of-success-in-digital-transformation
20. De la Boutetière H., Montagner A., Reich A. Unlocking success in digital transformations. URL: https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/unlocking-success-in-digital-transformations
21. Nguyen T. H., Newby M., Macaulay M. J. Information Technology Adoption in Small Business: Confirmation of a Proposed Framework. *Journal of Small Business Management*. 2015. Vol. 53. Iss. 1. P. 207–227. DOI: https://doi.org/10.1111/jsbm.12058
22. The Future of Job Report 2020 / World Economic Forum. URL: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf
23. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посіб. Київ : Атіка, 2005. 432 с
24. Марченко О. С. Економічна безпека підприємства : навч. посіб. Харків : Право, 2022. 246 с.
25. Irtyshcheva I., Trushliakova A., Sirenko I. Strategic Human Capital Management in the Context of Digitalization. *Baltic Journal of Economic Studies*. 2020. Vol. 6. No. 5. P. 178–183. DOI: https://doi.org/10.30525/2256-0742/2020-6-5-178-183
26. Goulart V., Liboni L., Cezarino L. Balancing skills in the digital transformation era: The future of jobs and the role of higher education. *Industry and Higher Education*. 2022. Vol. 36. Iss. 2. P. 118–127. DOI: https://doi.org/10.1177/09504222211029796
27. Сосновська О. О. Система економічної безпеки підприємств зв'язку : монографія. Київ : ЦУЛ, 2019. 440 с.

REFERENCES

"2023 Thales Data Threat Report: Global Edition". https://cpl.thalesgroup.com/data-threat-report

Babbar, A. et al. "Why most digital banking transformations fail – and how to flip the odds". https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/why-most-digital-banking-transformations-fail-and-how-to-flip-the-odds

Berman, S. J. "Digital transformation: opportunities to create new business models". *Strategy & Leadership*, vol. 40, no. 2 (2012): 16-24. DOI: https://doi.org/10.1108/10878571211209314

Bolton, A., Goosen, L., and Kritzinger, E. "Security aspects of an empirical study into the impact of digital transformation via unified communication and collaboration technologies on the productivity and innovation of a global automotive enterprise". *Information and Cyber Security* (2020): 99-113. DOI: https://doi.org/10.1007/978-3-030-43276-8_8

"Cost of a Data Breach. Report 2022". https://www.key-4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf

Chmil, H. L. "Tsyfrovizatsiia diialnosti subiektiv spozhyvchoho rynku: mozhlyvosti ta zahrozy" [Digitalization of Consumer Market Entities Activity: Opportunities and Threats]. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia «Mizhnarodni vidnosyny. Ekonomika. Krainoznavstvo. Turyzm»*, no. 13 (2021): 124-134. DOI: https://doi.org/10.26565/2310-9513-2021-13-13

De la Boutetiere, H., Montagner, A., and Reich, A. "Unlocking success in digital transformations". https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/unlocking-success-in-digital-transformations

Forth, P. et al. "Flipping the Odds of Digital Transformation Success". https://www.bcg.com/publications/2020/increasing-odds-of-success-in-digital-transformation

Gebremeskel, B., Jonathan, G., and Yalew, S. "Information Security Challenges During Digital Transformation". *Procedia Computer Science*, vol. 219 (2023): 44-51. DOI: https://doi.org/10.1016/j.procs.2023.01.262

Gokalp, E., and Martinez, V. "Digital transformation capability maturity model enabling the assessment of industrial manufacturers". *Computers in Industry,* art. 103532, vol. 132 (2021). DOI: https://doi.org/10.1016/j.compind.2021.103522

Goulart, V., Liboni, L., and Cezarino, L. "Balancing skills in the digital transformation era: The future of jobs and the role of higher education". *Industry and Higher Education*, vol. 36, no. 2 (2022): 118-127. DOI: https://doi.org/10.1177/09504222211029796

Huang, K. et al. "The Devastating Business Impacts of a Cyber Breach". https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach#:~:text=Managing%20Cyber%20Risk&text=On%20average%2C%20companies%20experiencing%20a,and%20cost%20to%20secure%20financing

Irtyshcheva, I., Trushliakova, A., and Sirenko, I. "Strategic Human Capital Management in the Context of Digitalization". *Baltic Journal of Economic Studies*, vol. 6, no. 5 (2020): 178-183. DOI: https://doi.org/10.30525/2256-0742/2020-6-5-178-183

Kamlyk, M. I. *Ekonomichna bezpeka pidpryiemnytskoi diialnosti. Ekonomiko-pravovyi aspekt* [Economic Security of Business Activity. Economic and Legal Aspect]. Kyiv: Atika, 2005.

LaBerge, L., Smaje, K., and Zemmel, R. "Three new mandates for capturing a digital transformation's full value".

https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-new-mandates-for-capturing-a-digital-transformations-full-value
Matt, Ch., Hess, Th., and Benlian, A. "Digital Transformation Strategies". *Business & Information Systems Engineering*, vol. 57 (2015): 339-343. DOI: https://doi.org/10.1007/s12599-015-0401-5
Marchenko, O. S. *Ekonomichna bezpeka pidpryiemstva* [Economic Security of the Enterprise]. Kharkiv: Pravo, 2022.
"Managing Risk in Digital Transformation". *Deloitte*. October 2018. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf
Nguyen, T. H., Newby, M., and Macaulay, M. J. "Information Technology Adoption in Small Business: Confirmation of a Proposed Framework". *Journal of Small Business Management*, vol. 53, no. 1 (2015): 207-227. DOI: https://doi.org/10.1111/jsbm.12058
"PwC's 25th Annual Global CEO Survey: Reimagining the outcomes that matte". https://www.pwc.com/gx/en/ceo-survey/2022/main/content/downloads/25th_CEO_Survey.pdf
Shkarlet, C., and Sadchykova, I. "Transformatsiia systemy finansovo-ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovoi ekonomiky" [Transformation of Enterprise Financial and Economic Security System in Digital Economics]. *Problemy i perspektyvy ekonomiky i upravlinnia*, no. 3 (2019): 264-276. DOI: https://doi.org/10.25140/2411-5215-2019-3(19)-264-276
Sosnovska, O. O. *Systema ekonomichnoi bezpeky pidpryiemstv zviazku* [System of Economic Security of Communication Enterprises]. Kyiv: TsUL, 2019.
"The Future of Job Report 2020". *World Economic Forum*. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf
"The Global Risks Report 2023. 18th Edition". *World Economic Forum*. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
Vial, G. "Understanding digital transformation: A review and a research agenda". *The Journal of Strategic Information Systems*, vol. 28, no. 2 (2019): 118-144. DOI: https://doi.org/10.1016/j.jsis.2019.01.003
Vovk, V. et al. "Financial monitoring in the bank as a market instrument in the conditions of innovative development and digitalization of economy: management and legal aspects of the risk-based approach". *International Journal of Industrial Engineering & Production Research*, vol. 31, no. 4 (2020): 559-570. DOI: https://doi.org/10.22068/ijiepr.31.4.559
Yvanovich, R. "Navigating Challenges: the Worrying State of Digital Transformation for SMEs". https://blog.trginternational.com/digital-transformation-sme-small-medium-sized-enterprises

УДК 005.95/.96
JEL: J24; L10; L86; O15
DOI: https://doi.org/10.32983/2222-4459-2023-7-91-99

ЦИФРОВІ КОМПЕТЕНТНОСТІ ЛЮДСЬКОГО КАПІТАЛУ В РЕАЛІЗАЦІЇ ЦИФРОВИХ СТРАТЕГІЙ ПІДПРИЄМСТВ МАШИНОБУДУВАННЯ

©2023 **МЕЛЬНИЧУК В. Е.**

УДК 005.95/.96
JEL: J24; L10; L86; O15

Мельничук В. Е. Цифрові компетентності людського капіталу в реалізації цифрових стратегій підприємств машинобудування

Метою дослідження є виявлення впливу цифрових компетентностей людського капіталу на формування стратегій цифровізації підприємства. У статті запропоновано розподіл цифрових компетентностей на базові, функціональні, операційні компетентності та компетентності власника. Виокремлено стратегії цифровізації підприємств, які поділяються на стратегію цифровізації бізнес-процесів, стратегію цифровізації продуктів, стратегію цифровізації підприємства та стратегію цифрового аутсорсингу. У ході дослідження було побудовано (застосувавши методологію аналізу пріоритетів) ієрархію мети, критеріїв та альтернатив формування цифрових компетентностей. Сформовано залежності цифрових компетентностей людського капіталу машинобудівних підприємств з виокремленими стратегіями цифровізації. Проведено попарне порівняння критеріїв за принципом оцінювання відносної важливості одного із критеріїв стосовно іншого за шкалою, запропонованою Т. Саамі. У статті визначено показник випадкової узгодженості. На основі наведеної методики розраховано відповідні показники із застосуванням попарного порівняння, яке дозволило виявити роль кожного із критеріїв (цифрових компетентностей) у реалізації субкритеріїв (стратегій цифровізації). У статті зазначено, що наявність у власника цифрових компетентностей визначає глибину проникнення цифрових технологій у процеси виробничої та економічної діяльності. Відмічено, що результативність упровадження цифрових технологій корелює з розвитком цифрових компетентностей власника, який може виступати генератором майбутніх цифрових змін на підприємстві. Здійснено структурування пріоритетів цифрових компетентностей для кожної із стратегій для виявлення ролі кожної із групи цифрових компетентностей у реалізації стратегій цифровізації підприємств машинобудування. Визначено глобальні пріоритети стратегічних альтернатив у розвитку цифрових компетентностей працівників підприємства машинобудування. У статті ідентифіковано вимоги до видів цифрових компетентностей для кожної із стратегій та здійснено їх групування за вимогами до їх обсягу.

Ключові слова: *людський капітал, цифрові компетентності, цифрові стратегії, машинобудівні підприємства, цифровізація.*
Рис.: *3.* ***Табл.:*** *7.* ***Формул:*** *4.* ***Бібл.:*** *10.*

Мельничук Вікторія Едуардівна *– аспірантка, асистентка кафедра економічної кібернетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» (просп. Берестейський, 37, Київ, 03056, Україна)*
E-mail: *vickikitoria@gmail.com*
ORCID: *https://orcid.org/0000-0001-8246-4076*
Researcher ID: *https://www.webofscience.com/wos/author/record/AGR-8905-2022*