



Розвиток продуктивних сил і регіональна економіка

УДК: 330.342.146:004(477)

DOI <https://doi.org/10.5281/zenodo.15333050>

**Вплив цифровізації на стратегії забезпечення економічної безпеки
бізнесу в Україні**

Фаїзов Анатолій Вікторович,

кандидат економічних наук, доцент, завідуючий кафедрою економіко-
правових дисциплін, Національна академія внутрішніх справ, Навчально-
науковий інститут права та психології, м. Київ, Україна,
<https://orcid.org/0000-0002-5090-5145>

Мацюра Світлана Іванівна,

кандидат економічних наук, доцент, кафедра економіки та цифрового
бізнесу, Державний університет економіки і технологій, м. Кривий Ріг,
Україна, <https://orcid.org/0000-0002-3243-7683>

Мікуліна Марина Олександрівна,

кандидат економічних наук, доцент, інженерно-технологічний факультет,
Сумський національний аграрний університет, Агроінжиніринг,
м. Суми, Україна, <https://orcid.org/0000-0002-6918-5192>

Прийнято: 18.04.2025 | Опубліковано: 30.04.2025

***Анотація.** Цифровізація економіки України є важливим чинником, що
впливає на всі аспекти господарської діяльності. Вона не лише змінює способ*



ведення бізнесу, але й вимагає перегляду стратегій гарантування економічної безпеки підприємств, адже впровадження інновацій не тільки відкриває нові можливості, а також створює додаткові ризики, зокрема в контексті кіберзагроз та захисту даних. **Метою** статті є аналіз впливу цифровізації на економічну безпеку підприємств України в умовах інтенсивної трансформації бізнес-процесів. Досліджено основні чинники, що супроводжують цифрову трансформацію, зокрема зростання кіберзлочинності, порушення конфіденційності даних, внутрішні загрози та пошкодження інфраструктури. Проаналізовано можливості впровадження ефективних стратегій управління ризиками з метою мінімізації загроз, а також розроблено комплексні заходи кібербезпеки для підприємств. **Методи дослідження** охоплювали аналіз статистичних даних, оцінку індексів цифрової трансформації на регіональному рівні та вивчення ризиків, що виникають унаслідок упровадження цифрових технологій. Здійснено порівняльну оцінку рівня цифровізації регіонів України за індексом цифрової трансформації з подальшим аналізом вразливостей, зокрема впливу кіберзлочинності, порушення конфіденційності та внутрішніх загроз у бізнес-середовищі. **Результати дослідження** свідчать про високий рівень ризиків, пов'язаних з кіберзагрозами, що можуть заподіяти значні фінансові та репутаційні втрати для підприємств. Зокрема виявлено, що найвищі індекси цифрової трансформації мають регіони з розвинутою інфраструктурою та активною підтримкою цифровізації, тоді як низькі показники вказують на необхідність покращення підтримки цифрових інновацій у менш розвинених областях. Оцінка ризиків показала, що кіберзлочинність та порушення конфіденційності мають найбільший вплив на бізнес, що вимагає від підприємств упровадження комплексних заходів захисту та постійного оновлення стратегій безпеки. **Висновки** дослідження доводять необхідність



інтеграції систем управління інформаційною безпекою в загальну стратегію підприємств, а також в заходи підвищення рівня цифрової грамотності працівників. Для мінімізації загроз підприємствам слід упроваджувати ефективні заходи кібербезпеки, навчання персоналу, використання шифрування даних та інвестування в сучасні технології захисту.

Ключові слова: цифрові технології, фінансова стабільність, кібербезпека, керування інформацією, захист інформаційних систем, показник цифрової трансформації, підприємницькі ризики, інноваційні технології, захист даних.

The impact of digitalization on strategies for ensuring economic security of business in Ukraine

Anatolii Faizov,

Candidate of Economic Sciences, Associate Professor, Head of the Department of Economic and Legal Disciplines, National Academy of Internal Affairs, Educational and Scientific Institute of Law and Psychology, Kyiv, Ukraine,
<https://orcid.org/0000-0002-5090-5145>

Svitlana Matsiura,

PhD in Economics, Assistant Professor, Department of Economics and Digital Business, State University of Economics and Technologies, Kryvyi Rih, Ukraine,
<https://orcid.org/0000-0002-3243-7683>



Maryna Mikulina,

Candidate of Economic Sciences, Associate Professor of the Department of
Agricultural Engineering, Faculty of Engineering and Technology, Sumy National
Agrarian University, Agroengineering, Sumy, Ukraine,
<https://orcid.org/0000-0002-6918-5192>

Abstract. *The digitalization of Ukraine's economy is a crucial factor influencing all aspects of economic activity. It not only transforms the way businesses operate but also necessitates a revision of strategies for ensuring economic security, as the transition to new digital technologies and the implementation of innovations create both new opportunities and additional risks—particularly in the context of cyber threats and data protection. **The aim of this article is to analyze the impact of digitalization on the economic security of Ukrainian enterprises amid the intensive transformation of business processes. The study anticipates the examination of key factors accompanying digital transformation, including the rise of cybercrime, data privacy breaches, internal threats, and infrastructure damage. The task is to analyze the potential for implementing effective risk management strategies aimed at minimizing threats, as well as to develop comprehensive cybersecurity measures for enterprises. The research methods included the analysis of statistical data, the assessment of digital transformation indices at the regional level, and the examination of risks arising from the adoption of digital technologies. The article provides a comparative assessment of the level of digitalization across Ukrainian regions based on the digital transformation index, followed by a risk analysis addressing the impact of cybercrime, data breaches, and internal threats on the business environment. A comparison of the digitalization levels in various regions of Ukraine was conducted using the digital transformation index, enabling the evaluation of regional readiness***



*for adapting to new technologies. Risk assessment in the context of digital transformation is based on the analysis of how cybercrime, data confidentiality breaches, and internal disruptions affect business operations. **The research findings** indicate a high level of risks associated with cyber threats, which can lead to significant financial and reputational losses for businesses. It was found that the highest digital transformation indices are observed in regions with well-developed infrastructure and active digitalization support, while low indicators point to the need for enhanced support of digital innovation in less developed areas. Risk assessment revealed that cybercrime and data breaches have the greatest impact on business, requiring enterprises to implement comprehensive protection measures and continuously update their security strategies. **The conclusions of the study** emphasize the need to integrate information security management systems into the overall enterprise strategy and to increase the level of digital literacy among employees. To minimize threats, enterprises should implement effective cybersecurity measures, provide personnel training, use data encryption, and invest in modern protection technologies.*

Keywords: *digital technologies, financial stability, cybersecurity threats, information management, information systems protection, digital transformation index, business risks, innovative technologies, data protection.*

Постановка проблеми. У сучасних умовах цифрової трансформації глобального економічного простору питання гарантування економічної безпеки бізнесу набуває нових форм і змісту. Стрімкий розвиток цифрових технологій, з одного боку, надає широкі можливості для підвищення ефективності господарської діяльності, але з іншого – створює нові виклики, пов'язані з кіберзагрозами, витоком даних, цифровим шахрайством та залежністю від інформаційної інфраструктури. В Україні, яка активно



інтегрується у світовий цифровий простір, проблема гарантування економічної безпеки бізнесу в умовах цифровізації є особливо актуальною з огляду на нестабільне економічне становище, військові дії, високий рівень інформаційних ризиків та необхідність адаптації до нових цифрових реалій. У цьому контексті постає наукове завдання комплексного осмислення впливу цифровізації на формування стратегій економічної безпеки, що дозволить виявити нові інструменти захисту, удосконалити практики до ризик-менеджменту та підвищити адаптивність українського бізнесу до викликів цифрової економіки. Дослідження цієї проблеми має не лише теоретичне, а й вагоме практичне значення, адже його результати можуть бути покладені в основу державної політики цифрової трансформації, розвитку нормативно-правової бази у сфері економічної безпеки та впровадження цифрових стратегій управління ризиками на рівні окремих підприємств.

Аналіз останніх досліджень і публікацій. Дослідники С. Датта, Б. Ланвен, Л. Р. Леон, С. Вунш-Вінсент [1] у звіті Global Innovation Index (2022) аналізують перспективи інноваційно орієнтованого зростання в умовах глобальних викликів, підкреслюючи важливість інноваційної екосистеми для стабільного розвитку. Автор Т. А. Коцко [2] розглядає екологізацію економіки як механізм переходу до сталого розвитку, акцентуючи на незавершеності трансформаційних процесів в Україні. Науковці К. А. Зіненко, Т. О. Кобелева [3] детально аналізують компоненти формування економічної безпеки, як-от фінансовий, інформаційний, технічний та кадровий. Важливим аспектом є вивчення впливу інтеграції цих компонентів для забезпечення стабільного функціонування підприємства. Акцентовано на необхідності стратегічної практики в управлінні економічною безпекою та запропоновано шляхи удосконалення управлінських практик. Дослідниця В. Кудлай [4] вивчає глобальні тенденції екологічного розвитку в умовах цифровізації, зокрема



взаємозв'язок між екологічними стратегіями та цифровими трансформаціями. Вчені С. Т. Пілецька, Т. Ю. Коритько, Є. В. Ткаченко [5] зосереджуються на використанні комплексних показників для визначення рівня безпеки підприємства в різних аспектах: фінансовому, ресурсному, управлінському. Модель передбачає моніторинг показників ризику та вразливості, що дозволяє підприємствам здійснювати своєчасне коригування своїх стратегій для мінімізації можливих загроз. Група авторів Ю. Г. Неустроев, Т. І. Єгорова-Гудкова, В. В. Острянюк [6] аналізують вплив цифровізації на економічну безпеку держави, розглядаючи ризики та переваги цифрової трансформації. Науковиця І. В. Томашук [7] досліджує вплив глобалізаційних процесів на сучасні економіки, висвітлюючи адаптаційні механізми країн із перехідною економікою. Дослідники І. Томашук, В. Балдинюк [8] визначають екоінновації як основу сталого розвитку, підкреслюючи їхню роль у зміцненні економіки в умовах глобальних викликів. Група вчених І. Томашук, В. Балдинюк, Л. Болтовська [9] акцентують на використанні зеленої економіки як основного чинника забезпечення сталого розвитку, пропонуючи комплексну практику до впровадження екологічних інструментів. Дослідники В. Фіщук, В. Матюшко, Є. Чернів, О. Юрчак, Я. Лаврик, А. Амелін [10] розглядають концепцію цифрової економіки як засадничу для майбутнього національного розвитку. Автори В. Гросул, Р. Буріменко, П. Смірнова, О. Тімченко, Г. Баламут, О. Рачкован [11] аналізують особливості цифрової трансформації економіки в контексті диверсифікаційних процесів, наголошуючи на складності адаптації до нових умов. Науковці О. Шумило, В. Бабенко, Л. Любохинець, І. Воловельська, О. Арєф'єва [12] розробляють методику оцінки економічної безпеки підприємства, акцентуючи на стратегічному управлінні ризиками. Дослідники С. Т. Пілецька, Т. Ю. Коритько, Н. М. Кравчук [13] вивчають механізми гарантування економічної безпеки підприємств, пропонуючи



ефективні практики. Економічний потенціал підприємств у системі управління їхньою безпекою розглядається у роботі С. Т. Пілецької, Т. Ю. Коритько, В. М. Лукаржевської-Мялик [14]. Автор М. Ю. Демченко [15] аналізує використання офшорних юрисдикцій міжнародними компаніями в контексті змін глобального оподаткування, акцентуючи на стратегічних аспектах структурування бізнесу.

Виділення невирішених раніше частин загальної проблеми. Попри зростання уваги до економічної безпеки бізнесу в умовах цифровізації, низка важливих аспектів залишається недостатньо дослідженою. Зокрема актуальним є питання адаптації бізнесу до цифрових ризиків в умовах нестабільної економіки України, де цифрова трансформація супроводжується правовими та інституційними перешкодами. Водночас недостатньо висвітлено механізми інтеграції цифрових інструментів у систему управління ризиками, особливо для малого та середнього бізнесу. Потребує подальшого аналізу взаємодія держави й бізнесу задля створення ефективної системи запобігання цифровим загрозам. Наукова новизна дослідження полягає в поглибленому аналізі цих проблем та розробці інноваційних стратегій економічної безпеки в цифровому середовищі.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження впливу цифровізації на стратегії гарантування економічної безпеки бізнесу в Україні. Завданнями дослідження є:

1. Проаналізувати основні тенденції цифровізації та їхній вплив на економічну безпеку, зокрема на ризики кіберзагроз і захисту інформації.
2. Розробити дієві стратегії мінімізації цифрових загроз з акцентом на малий та середній бізнес, на заходи, що реалізуються на рівні державної політики.



3. Удосконалити рекомендації щодо адаптації стратегії економічної безпеки до впровадження цифрових технологій, що допоможе створити ефективнішу систему захисту в цифровому середовищі.

Виклад основного матеріалу дослідження. Цифровізація економіки України істотно трансформує не лише бізнес-процеси, а й практики гарантування економічної безпеки підприємств. Вона відкриває нові можливості, водночас посилюючи ризики, пов'язані з кіберзагрозами, захистом даних і управлінням інформацією. Зростання кількості цифрових атак на бізнес актуалізує розробки адаптованих стратегій безпеки, що враховують технологічні виклики, економічні реалії України, а також загрози, зумовлені ворожою агресією Російської Федерації. Автоматизація, впровадження електронних сервісів та використання великих даних підвищують ефективність, проте супроводжуються ризиками, що можуть призвести до втрат і підриву довіри клієнтів [1, с. 4].

Однією з основних проблем є захист персональних даних та комерційної інформації. З впровадженням цифрових технологій, як-от хмарні сервіси, з'являються нові шляхи, через які зловмисники можуть отримати доступ до важливої інформації. Порушення кібербезпеки часто має серйозні наслідки, зокрема фінансові збитки через крадіжки або втрати даних, а також можливість отримання конкурентами доступу до корпоративної таємниці. Різноманітність та складність кіберзагроз вимагають від бізнесу постійного оновлення засобів захисту інформації, а також інвестицій у технології кібербезпеки.

У цьому контексті цифрові загрози можна поділити на такі основні групи: зовнішні загрози, що йдуть від кіберзлочинців, й внутрішні загрози, пов'язані з людським чинником – несанкціонованим доступом або необережністю працівників. Зовнішні загрози можуть містити атаки на



корпоративні мережі, викрадення даних, використання шкідливого програмного забезпечення для проникнення в системи компаній. Внутрішні загрози можуть бути результатом недостатнього контролю за доступом до інформації або порушення політики безпеки. З цієї причини важливо гарантувати не лише технічний захист, але й правові та організаційні заходи щодо безпеки даних.

Управління даними є ще одним важливим компонентом цифрової безпеки бізнесу. Підприємства повинні ретельно розробляти політику збереження та обробки персональної чи корпоративної інформації, що потребує високих стандартів конфіденційності та захисту. Порушення цих вимог може призвести до серйозних юридичних наслідків, а також до втрати довіри клієнтів, що є критичним для довгострокового успіху бізнесу [2, с. 66].

Поширення цифрових технологій висуває нові вимоги до бізнесу. Проблеми, пов'язані з управлінням цифровими ризиками, потребують постійного удосконалення та адаптації бізнес-процесів. Підприємства повинні активно працювати над підвищенням рівня цифрової грамотності своїх працівників, що дозволить ефективно реагувати на нові виклики. Також важливим є впровадження комплексних систем управління безпекою, що забезпечують цілісну стратегію захисту підприємства від різноманітних кіберзагроз [3, с. 10]. У таблиці 1 представлено дані щодо індексу цифрової трансформації різних регіонів України у 2024 році.

Таблиця 1

Індекс цифрової трансформації України, 2024 р.

Назва області	Значення індексу	Назва області	Значення індексу
Загалом для України	0,632	Черкаська	0,672
Дніпропетровська	0,908	Хмельницька	0,620
Львівська	0,891	Житомирська	0,560



Полтавська	0,833	Чернігівська	0,553
Волинська	0,831	Чернівецька	0,546
Тернопільська	0,827	Кіровоградська	0,531
Харківська	0,787	Миколаївська	0,441
Одеська	0,785	Луганська	0,404
Вінницька	0,777	Донецька	0,359
Закарпатська	0,732	Херсонська	0,316
Рівненська	0,727	Запорізька	0,289
Івано-Франківська	0,685	Сумська	0,178
Київська	0,684	Автономна Республіка Крим	Дані відсутні

Джерело: [16]

Як видно з наведених даних, загальний рівень цифрової трансформації по Україні становить 0,632, що свідчить про помірний прогрес у цьому напрямку. Найвищі значення індексу спостерігаються в Дніпропетровській (0,908) та Львівській (0,891) областях, що вказує на активне впровадження цифрових технологій в цих регіонах. Полтавська (0,833) та Волинська (0,831) області також демонструють високі показники, що може свідчити про наявність інфраструктури та підтримку цифровізації на регіональному рівні.

Однак низькі значення індексу у таких областях, як-от Сумська (0,178), Херсонська (0,316) і Запорізька (0,289), свідчать про недостатній рівень цифрових інновацій та впровадження новітніх технологій. У першу чергу це пов'язано з військовими діями на території України.

У результаті тривалої окупації Автономної Республіки Крим відсутні дані щодо її цифрової трансформації. Загалом для досягнення однакового рівня цифровізації всієї України необхідно зосередити зусилля на підтримці слабших регіонів, упровадженні ефективних стратегій цифровізації та покращенні інфраструктури на місцевому рівні. В таблиці 2 представлено оцінку ризиків цифрової трансформації бізнесу в Україні.



Таблиця 2

Оцінка ризиків цифрової трансформації бізнесу в Україні

Тип загрози	Оцінка впливу на бізнес	Частота виникнення	Можливі наслідки
Кіберзлочинність	Висока	Середня	Фінансові втрати, крадіжка даних
Порушення конфіденційності	Висока	Висока	Втрата довіри клієнтів, юридичні наслідки
Внутрішні порушення	Середня	Низька	Втрата даних
Пошкодження інфраструктури	Висока	Низька	Зупинка бізнесу, фінансові втрати

Джерело: власна розробка авторів

Впровадження надійних заходів кібербезпеки є основою захисту підприємств від постійно зростаючих цифрових загроз. Застосування міжмережевих екранів, антивірусного ПЗ та систем виявлення вторгнень забезпечує багаторівневий захист і допомагає ефективно запобігати кібератакам, які залишаються одними з найпоширеніших ризиків у сучасній економіці [4, с. 11].

Не менш важливим елементом є навчання персоналу, оскільки людський чинник часто є слабкою ланкою, особливо при фішингових атаках та інших маніпуляціях соціальної інженерії. Підготовка співробітників до виявлення загроз і правильного реагування на них значно знижує ймовірність успішного злому [5, с. 58]. Ця практика має помірну ефективність, проте істотно зменшує вразливість на рівні користувачів.

Сучасне шифрування даних є потужним інструментом захисту конфіденційної інформації. Завдяки шифруванню навіть у разі перехоплення даних сторонні особи не зможуть отримати доступ до вмісту [6, с. 206]. Така практика є особливо ефективною для підприємств, що працюють з персональними або фінансовими даними, і дозволяє уникнути витоків, що є актуальним як в Україні, так і за її межами [7, с. 155].



Регулярні аудити систем безпеки та тестування на вразливості дають змогу виявляти потенційні слабкі місця ще до того, як ними скористаються зловмисники [8, с. 55]. Ця проактивна практика має середній рівень ефективності, однак є невіддільною частиною комплексної стратегії захисту, особливо в умовах стрімких змін цифрових загроз.

Стратегічне співробітництво з міжнародними кібербезпековими організаціями сприяє виявленню новітніх загроз та впровадженню передових практик на підприємствах. Така співпраця є високоефективною, оскільки компанії отримують доступ до найновіших інструментів захисту та глобальної мережі підтримки. Це особливо важливо для бізнесу в Україні, де цифрове середовище все ще знаходиться на етапі розвитку, і міжнародна співпраця може значно покращити ефективність місцевих ініціатив [9, с. 197].

В українських реаліях цифрова трансформація не лише відкриває нові можливості для бізнесу, а й загострює вразливість до кіберзагроз. Злочини у цифровому середовищі набувають нових форм, завдаючи шкоди не лише фінансам, а й діловій репутації компаній. Витік даних та неналежний рівень інформаційної безпеки матимуть як правові наслідки, так і втрату довіри клієнтів. Водночас внутрішні нерегулярні загрози мають потенціал серйозно впливати на стабільність бізнес-процесів. Усе це формує необхідність переосмислення підходів до захисту в цифрову епоху. Окремим чинником є пошкодження інфраструктури, що може призвести до зупинки роботи підприємства та спричинити значні фінансові втрати [10].

Для зменшення таких ризиків важливо впроваджувати комплексні практики цифрової безпеки. У таблиці 3 узагальнено основні напрямки захисту й методи оцінки загроз, актуальних для цифрового середовища України.



Таблиця 3

Стратегії зниження ризиків цифрових загроз: міжнародні практики та специфіка українського ринку

Стратегія	Опис стратегії	Міжнародні практики	Специфіка українського ринку
Впровадження комплексних заходів кібербезпеки	Використання міжмережевих екранів, антивірусних програм, систем виявлення вторгнень	США, ЄС – державні програми захисту інфраструктури та корпоративних даних (наприклад, GDPR в ЄС)	Низький рівень упровадження таких заходів у малому та середньому бізнесі
Захист конфіденційних даних	Шифрування даних, двофакторна автентифікація та криптографічні методи захисту	Великі корпорації США та Європи активно використовують ці методи для захисту клієнтських даних та інформації	Шифрування часто не застосовується на всіх рівнях, особливо в малому бізнесі
Навчання та підвищення кваліфікації персоналу	Підготовка співробітників до виявлення кіберзагроз і фішингових атак	Японія, Німеччина – регулярне навчання співробітників, тренінги на основі реальних сценаріїв атак	Часте недотримання цього аспекту, особливо в малих та середніх компаніях
Інвестування в технології захисту	Використання інноваційних рішень: штучний інтелект для аналізу загроз, блокчейн для захисту транзакцій	США, Великобританія – застосування ІТ-рішень для автоматизації виявлення та запобігання загроз у реальному часі	Низький рівень інвестицій в сучасні технології, особливо серед малих компаній
Аудити та тестування на вразливості	Регулярні перевірки та тестування систем на виявлення вразливих місць і слабких місць у безпеці	Канада, Сінгапур – державні ініціативи для гарантування високого рівня безпеки через проведення аудитів	Нечасте проведення тестувань, відсутність державної підтримки
Співпраця з міжнародними організаціями	Співпраця з провідними міжнародними кібербезпековими організаціями для обміну досвідом і технологіями	ЄС, ООН – спільні ініціативи щодо глобального підвищення кібербезпеки в бізнесі через обмін знаннями та досвідом	Співпраця з міжнародними організаціями не є загальноприйнятою, особливо серед малого бізнесу

Джерело: власна розробка авторів



Отже, комплексні практики гарантування кібербезпеки на усіх рівнях бізнесу є ефективними інструментами для захисту даних у цифровому середовищі [11, с. 156]. Високий рівень інвестицій у технології захисту, регулярні аудити та тісна співпраця з міжнародними організаціями є важливими чинниками для зниження вразливості [12]. Для українського бізнесу це означає необхідність запровадження програм навчання, розвитку інфраструктури кібербезпеки та активнішої співпраці з міжнародними партнерами.

Для стратегії економічної безпеки малого та середнього бізнесу в Україні адаптація цифрових технологій є важливою умовою для гарантування стійкості підприємств, особливо в умовах сучасних викликів цифровізації та швидких змін на ринку [13, с. 66]. Вчасне впровадження ефективних цифрових рішень на рівні малих та середніх підприємств дозволяє не тільки зменшити ризики, пов'язані з кіберзагрозами та фінансовими втратами, але й посилити конкурентоспроможність та інноваційний потенціал бізнесу [14, с. 2]. Їхнє застосування дає змогу автоматизувати багато процесів, що своєю чергою дозволяє знижувати витрати на адміністрування, підвищувати точність фінансової звітності, а також забезпечувати більш прозоре управління ризиками. Зокрема автоматизація обліку та звітності значно зменшує ймовірність людських помилок і дозволяє підприємствам швидше реагувати на зміни у бізнес-середовищі [15, с. 309].

В Україні у малому та середньому бізнесі цифрова трансформація має свої особливості, що потребують не лише дослідження загальної практики, а й урахування обмежених ресурсів, браку фахівців, наявності вищого рівня вразливості до кіберзагроз. Важливо не просто інтегрувати цифрові технології, але максимізувати їхню ефективність за мінімальних витрат. Основну увагу слід зосередити на практичних, доступних рішеннях, що легко масштабуються



та не потребують значних інвестицій. Також для малих і середніх підприємств критично важливо підвищувати цифрову грамотність персоналу, спрощувати бізнес-процеси за допомогою цифрових інструментів і водночас забезпечувати базовий, але надійний рівень кіберзахисту. Державна підтримка в цьому процесі відіграє роль каталізатора, дозволяючи підприємствам уникнути пастки цифрової нерівності та зосередитися на сталому розвитку навіть за умов високих ризиків.

Сьогодні цифровізація стає важливим інструментом підвищення економічної стабільності малого та середнього бізнесу в Україні, що дозволяє не тільки мінімізувати ризики, але й покращити операційну ефективність підприємства. Запропоновано основні рекомендації щодо забезпечення надійного захисту і розвитку малого та середнього бізнесу в умовах диджиталізації:

1. Забезпечити шифрування даних, багаторівневу автентифікацію та антивірусний захист для зниження кіберризиків.
2. Інтегрувати програмне забезпечення для автоматичного обліку, управління замовленнями та запасами для покращення ефективності.
3. Організувати тренінги з цифрових технологій та кібербезпеки для підвищення кваліфікації співробітників.
4. Запровадити новітні технології, зокрема штучний інтелект і блокчейн, для підвищення конкурентоспроможності.
5. Використовувати державні програми, гранти та пільгові кредити для фінансування цифрових проєктів.

У процесі цифровізації особливо важливою для малого і середнього бізнесу є роль державної підтримки. Надання грантів, пільгових кредитів та створення платформ для обміну досвідом знижує перешкоди для входу малих та середніх підприємств у цифрову економіку та надає можливість отримання



необхідного фінансування для трансформації. Таким чином, ці заходи є основними напрямками, що дозволяють підвищити економічну безпеку бізнесу та сприяють його сталому розвитку в нових економічних умовах.

Висновки. Основними напрямками зниження ризиків та підвищення конкурентоспроможності підприємств є кібербезпека, автоматизація бізнес-процесів, підвищення кваліфікації персоналу та інвестування в інноваційні технології. Державна підтримка відіграє важливу роль у подоланні перешкод для цифровізації малого та середнього бізнесу, основними проблемами яких є низький рівень інвестицій та відсутність комплексних заходів кібербезпеки. Перспективи подальших досліджень спрямовані на вивчення ефективних технологічних рішень для малого та середнього бізнесу, а також механізмів державної підтримки та впливу інновацій на економічну безпеку. Крім того, необхідно розширювати інтеграцію міжнародного досвіду у національні стратегії розвитку цифрових технологій на всіх рівнях.

Список використаних джерел

1. Dutta S., Lanvin B., León L.R., Wunsch-Vincent S. Global Innovation Index 2022. What is the future of innovation-driven growth? URL: <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf>. (дата звернення: 08.02.2025).
2. Коцко Т.А. Екологізація економіки як інструмент переходу до сталого розвитку в умовах незавершеності трансформаційних процесів. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Економіка і управління*. 2020. Т. 31, № 3. С. 63–70. DOI: <https://doi.org/10.32838/2523-4803/70-3-11>.
3. Зіненко К.А., Т. О. Кобелева. Економічна безпека підприємства: методологічна сутність та складові формування. *Вісник Національного*



технічного університету «Харківський політехнічний інститут». Сер.: *Економічні науки*. 2022. № 4. – С. 9–16.

4. Кудлай В. Глобальні тренди екологічного розвитку світової економіки в умовах цифровізації. *Галицький економічний вісник*. 2023. № 5 (84). С. 7–14. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2023.05.

5. Пілецька С.Т., Коритько Т.Ю., Ткаченко Є.В. Модель інтегральної оцінки економічної безпеки підприємства. *Економічний вісник Донбасу*. 2021. № 3 (65). С. 56–65.

6. Неустроев Ю.Г., Єгорова-Гудкова Т.І., Острянюк В.В. Аналіз впливу цифровізації економіки на систему економічної безпеки держави. *Вчені записки Університету «КРОК»*. 2020. № 4 (60). С. 202–209. DOI: <https://doi.org/10.31732/2663-2209-2020-60-202-209>.

7. Томашук І.В. Вплив глобалізаційних процесів на сучасні економічні системи. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2022. № 1(59). С. 153–165. DOI: <https://doi.org/10.37128/2524-0447-2022-1-153-165>.

8. Tomashuk I., Baldynyuk V. Eco-innovation as a basis for sustainable development. *Three Seas Economic Journal*. 2023. Vol. 4, № 1. P. 71–87. DOI: <https://doi.org/10.30525/2661-5150/2023-1-9>.

9. Tomashuk I., Baldynyuk V., Boltovska L. Green economy as a factor for ensuring sustainable development. *Baltic Journal of Economic Studies*. 2023. Vol. 9, № 3. P. 194–206. DOI: <https://doi.org/10.30525/2256-0742/2023-9-3-194-206>.

10. Фіщук В., Матюшко В., Чернів Є., Юрчак О., Лаврик Я., Амелін А. Україна 2030Е – країна з розвинутою цифровою економікою. URL: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html> (дата звернення: 08.02.2025)



11. Hrosul V., Buhrimenko R., Smirnova P., Timchenko O., Balamut H., Rachkovan O. Specifics of economical digital transformation in the context of the diversification processes impact. *Journal of Interdisciplinary Research*. 2022. Vol. 12, № 2. P. 154–159. URL: https://www.magnanimitas.cz/ADALTA/120231/papers/A_27.pdf (дата звернення: 08.02.2025).

12. Shumilo O., Babenko V., Liubokhynets L., Volovelska I., Arefieva O. Method of Enterprise Economic Security Evaluation. *Studies of Applied Economics*. 2021. Vol. 39, № 7. URL: <http://ojs.ual.es/ojs/index.php/eea/article/view/4998> (дата звернення: 08.02.2025)

13. Пілецька С. Т., Коритько Т. Ю., Кравчук Н. М. Механізм забезпечення економічної безпеки підприємства. *Вісник економічної науки України*. 2022. № 1 (42). С. 64–68. DOI: [https://doi.org/10.37405/1729-7206.2022.1\(42\).64-69](https://doi.org/10.37405/1729-7206.2022.1(42).64-69).

14. Пілецька С. Т., Коритько Т. Ю., Лукаржевська-Мялик В. М. Економічний потенціал розвитку підприємства в системі управління його безпекою. *Економіка та суспільство*. 2022. № 44. <https://doi.org/10.32782/2524-0072/2022-44-34>.

15. Демченко М. Ю. Структурування міжнародних компаній через офшорні юрисдикції в контексті зміни глобальних правил оподаткування. *Європейські перспективи*. 2025. № 1. С. 301–311. DOI: <https://doi.org/10.71404/ep.2025.1.43>.

16. Державна служба статистики. Офіційний сайт. URL: <https://www.ukrstat.gov.ua/> (дата звернення: 08.02.2025).