Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2025. № 7.

DOI: http://doi.org/10.32702/2307-2105.2025.7.71

УДК 330.658.012

В. О. Задоя,

к. е. н., доцент, доцент кафедри економіки та менеджменту,

Український державний університет науки і технологій

ORCID ID: https://orcid.org/0000-0001-9408-4978

ІНСТИТУЦІЙНІ ТА УПРАВЛІНСЬКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ БІЗНЕСУ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

V. Zadoia,

PhD of Economics, Associate Professor,

Associate Professor of the Department of Economics and Management,

Ukrainian State University of Science and Technology

INSTITUTIONAL AND MANAGERIAL ASPECTS OF ENSURING ECONOMIC SECURITY OF BUSINESS IN THE DIGITAL ECONOMY

Актуальність обумовлена глибинною цифровою трансформацією бізнес-середовища, що одночасно розширює можливості та загострює загрози економічній безпеці підприємств. Метою статті є методичне обґрунтування інтегральної моделі узгодження цифрової стратегії зі системою економічної безпеки. Наукова новизна полягає у виокремленні п'яти взаємопов'язаних управлінських контурів - стратегічного,

організаційного, технологічного, правового та фінансового і розробленні алгоритму їхньої синхронізації на різних фазах життєвого циклу підприємства. Методологічну основу становлять інституційний аналіз, сценарне моделювання та проєктно-процесний підхід. Практична значущість проявляється у запропонованому наборі індикаторів, процедурах аудиту й механізмах прийняття рішень, які допомагають підприємствам оцінювати вразливість, адаптувати ресурси та підвищувати стійкість у воєнних і поствоєнних умовах. Результати дослідження формують базу аналізу стійкості та можуть бути використані під час розроблення програм підтримки бізнесу.

The relevance of this study stems from the accelerating digitalisation of economic processes and the heightened security challenges faced by Ukrainian enterprises during wartime and subsequent reconstruction efforts. This research provides a theoretical and methodological rationale for aligning corporate digital transformation with integrated systems of economic security, ensuring resilience and competitiveness in a volatile environment. The proposed conceptual framework, termed the "Digital–Security Alignment" model, integrates strategic, organisational, technological, legal, and financial governance loops, emphasising their coordinated action throughout the firm's life cycle.

Methodologically, the study employs institutional analysis, scenario planning, project–process management, and a critical review of regulatory guidance to develop a robust framework. Central focus is placed on big-data-driven risk detection, adaptive cyber-resilience, and balanced scorecards for secure value creation. The novelty of this work lies in bridging the fragmented discourse between digital strategy and security governance, offering a coherent set of principles, decision rules, and implementation pathways applicable to organisations of varying scale and complexity.

The study elucidates how digital initiatives can either amplify or mitigate

classical and emergent threats, depending on their design and execution. It proposes criteria for selecting organisational designs, resource configurations, and partnership mechanisms under conditions of uncertainty. These criteria enable enterprises to navigate the complexities of digital transformation while safeguarding critical operations.

The practical significance of the findings manifests in actionable audit procedures, indicator matrices, and managerial guidelines. These tools assist enterprises in identifying vulnerabilities, rationalising investments, and ensuring the continuity of critical functions while pursuing data-driven growth. The study's outcomes provide a flexible platform for designing sectoral support programmes and inform policy instruments aimed at enhancing the competitiveness and resilience of the Ukrainian economy within the single market.

By addressing the interplay between digitalisation and security, this research contributes to both academic discourse and practical implementation, offering a roadmap for enterprises to thrive in a rapidly evolving economic landscape while maintaining robust security measures.

Ключові слова: *Економічна безпека, цифрова трансформація, інституційні аспекти, управління ризиками, конкурентоспроможність бізнесу, підприємницька діяльність.*

Keywords: *Economic security, digital transformation, institutional aspects, risk management, business competitiveness, entrepreneurship.*

Постановка «проблеми». Сучасна цифрова трансформація кардинально змінює основи ведення бізнесу, особливо у сфері малого, середнього та інноваційного підприємництва. Відбувається своєрідна «цифрова революція», що охоплює всі сфери суспільного життя, зокрема і підприємницьку діяльність. Це призводить до зміни конкурентного

середовища та кон’юнктури ринків, що становить пряму загрозу економічній безпеці підприємств, особливо традиційних галузей економіки.

Іншими словами, нові цифрові технології стимулюють зростання ефективності бізнес-процесів, але водночас генерують нові ризики і загрози - від кібератак до порушення бізнес-операцій.

Забезпечення економічної безпеки підприємства набуває нового змісту, потрібно захищати не лише матеріальні активи, а й дані, інформаційні системи, безперервність діяльності. Особливо актуальним це стало у контексті воєнної агресії проти України 2022 року, коли постала воєнна економіка, а цифрові рішення стали інструментом виживання бізнесу.

Під час війни цифрові технології допомагають підтримувати комунікації, управління, фінансові операції попри фізичні руйнування, тобто слугують основою антикризового управління і бізнес-стійкості. Одночасно війна породжує і нові загрози - кібератаки на підприємства та інфраструктуру, перебої енергопостачання та зв’язку, що вимагає підвищеної уваги до кіберзахисту та ризик-менеджменту. Таким чином, проблема синергії між процесами цифровізації бізнесу та управління економічною безпекою підприємницьких структур є надзвичайно актуальною як з наукової, так і з практичної точок зору.

Зв’язок з важливими завданнями полягає в тому, що цифровізація бізнесу сьогодні - пріоритет державної політики і є умовою повоєнного відновлення економіки. Для України, що переживає повномасштабну війну, цифрові трансформації стали критично важливим інструментом підтримання економічної активності та забезпечення життєдіяльності суспільства.

З одного боку, уряд впроваджує цифрові сервіси (наприклад, платформа «Дія») для забезпечення адміністративних послуг та прозорості управлінських рішень. З іншого боку, бізнес змушений швидко освоювати онлайн-торгівлю, віддалену роботу, хмарні технології, щоб пристосуватися до умов війни і зберегти безперервність діяльності.

Це породжує нові наукові та практичні завдання: як узгодити цифрові інновації з системами економічної безпеки підприємств; які механізми управління ризиками ефективні в цифрову еру; як забезпечити модель прозорості управлінських рішень на основі цифрових даних; якою має бути роль держави та публічно-приватного партнерства в цій сфері тощо. Необхідність вирішення цих питань визначає актуальність дослідження.

Аналіз останніх досліджень і публікацій. Питання взаємодії цифрової трансформації бізнесу та економічної безпеки підприємств активно обговорюється в науковій літературі останніх років.

Вітчизняні та зарубіжні дослідники відзначають, що цифровізація вимагає перегляду підходів до забезпечення економічної безпеки. Так, Дергалюк Б. В. обґрунтовує, що цифрова трансформація підсилює роль нематеріальних факторів (знань, інформації) і ставить нові виклики перед системою безпеки підприємства. Зокрема, інформаційна складова економічної безпеки виходить на перший план, автор пропонує виокремити поняття «цифрова безпека підприємства», під яким розуміється захист економічних та інформаційних інтересів підприємства за допомогою сучасних технологій [1].

Аналогічно, колективне дослідження Самойленко Ю. та ін. зазначає, що пріоритетним компонентом економічної безпеки в умовах цифрової економіки стає цифровий (інформаційний) актив, і що необхідно модернізувати систему безпеки з урахуванням нових ризиків цифровізації. Автори запропонували замість традиційної «інформаційної складової» вживати термін «цифрова безпека підприємства», а також пропонують інституційний механізм оцінювання рівня цифрової безпеки підприємств (методика коефіцієнтів) [2].

Окремі роботи фокусуються на ризиках і загрозах, що супроводжують цифрові трансформації. Muravskyi S. та ін. у своєму дослідженні дійшли висновку, що впровадження цифрових технологій, з одного боку, підвищує операційну ефективність бізнесу, а з іншого - підвищує вразливість до

кібератак, фінансових ризиків та регуляторних викликів. Вони підкреслюють, що підприємствам необхідно стратегічно узгоджувати цифрові ініціативи з цілями організації та системою ризик-менеджменту, аби забезпечити довгострокову стійкість [3].

Тобто в літературі формується ідея так званого *alignment* - вирівнювання чи гармонізації цифрової стратегії зі стратегією економічної безпеки. Це один із недостатньо досліджених аспектів, на який вказують багато авторів.

Ще один важливий напрям - дослідження впливу цифровізації на стійкість економіки в умовах кризи та війни. Kolodiziev O. та співавт. проаналізували роль цифрової трансформації у підтримці інклюзивної економіки України під час війни. Вони виявили, що регіони з вищим рівнем цифровізації краще переносять соціально-економічні потрясіння: наприклад, у найцифровізованіших областях рівень безробіття в середньому на 12% нижчий, ніж у відсталих [4].

Дослідження також зафіксувало прискорення цифровізації у воєнний період: за 2021-2023 рр. використання мобільного додатку «Дія» зросло на 42%, інтернет-проникнення населення піднялось з 62% (2019) до 78% (2023), експорт ІТ-послуг зріс на 20% у 2022 р., а кількість технологічних стартапів подвоїлась від 2019 до 2023 р. [4].

Ці факти підтверджують, що війна, попри руйнування, стала драйвером цифрових змін. Водночас автори акцентують, що цифрові рішення слід спрямувати на забезпечення бізнес-стійкості і соціальної згуртованості, і пропонують стратегічні рамки адаптації регіонів, де цифровізація поєднується з інклюзивністю.

Міжнародні організації також приділяють увагу цифровій трансформації бізнесу в Україні в контексті економічної безпеки. Звіт OECD (2024) [5] підкреслює, що цифрові технології здатні підвищити продуктивність фірм і їхню стійкість у часи кризи (війни). Уряд України від початку повномасштабного вторгнення значно прискорив цифровізацію

публічних послуг та підтримку МСП у цифровому розвитку. Водночас, за даними OECD, українські МСП ще не повністю використовують потенціал цифровізації: заважають воєнні ризики, брак обізнаності, дефіцит цифрових навичок, галузева специфіка та фінансові обмеження.

За опитуваннями, 64% українських малих і середніх бізнесів на початку війни призупиняли або закривали діяльність, і хоч 84% з них відновили роботу протягом півроку, постійні атаки на критичну інфраструктуру, відключення електрики та перебої зв'язку гальмують відновлення економічної активності [5].

В цих умовах ІКТ-сектор України продемонстрував високу стійкість і навіть зростання, частково компенсуючи спад традиційних галузей [4-5].

Таким чином, у наукових джерелах закладено підґрунтя для подальших досліджень - вивчені окремі аспекти цифрової економіки та безпеки (кібербезпека, ризик-менеджмент, безперервність бізнесу), але не вирішеними залишаються питання комплексного узгодження цифрових трансформацій з управлінням економічною безпекою підприємництва, особливо в умовах України, що переживає війну та готується до повоєнного відновлення.

Недостатньо дослідженою є і практична сторона впровадження моделей цифрово-безпекового узгодження на рівні малих і середніх підприємств.

Метою даної статті є теоретичне узагальнення та методичне обґрунтування процесу узгодження цифрової трансформації бізнес-процесів із системою економічної безпеки підприємства шляхом розроблення інтегральної концептуальної моделі і формування на її основі інструментарію практичної реалізації, спрямованого на мінімізацію ризиків, підвищення стійкості суб'єктів господарювання в умовах воєнних й поствоєнних викликів.

Виклад основного матеріалу дослідження. Цифровізація впливає практично на всі функціональні елементи бізнесу - виробництво, операційну

діяльність, маркетинг, фінанси, управління персоналом. Однією з базових змін є перехід від традиційних бізнес-моделей до цифрових.

Компанії впроваджують електронну комерцію, цифровий маркетинг, дистанційну взаємодію з клієнтами, автоматизовані системи управління тощо. Наприклад, впровадження CRM-систем і аналітики великих даних дозволяє приймати управлінські рішення на основі реальних даних в режимі реального часу, що підвищує прозорість управлінських рішень і їх обґрунтованість.

Цифрові платформи об’єднують учасників ринку в нові екосистеми управління - наприклад, маркетплейси зводять разом виробників, продавців, логістичних операторів та споживачів, утворюючи цілі екосистеми з власними правилами гри.

Вагомий вплив цифровізації відчувається у сфері операцій та безперервності бізнес-процесів. Хмарні технології дають бізнесу гнучкість та масштабованість, підприємства можуть швидко збільшувати чи зменшувати потужності, зберігати резервні копії даних, забезпечувати віддалений доступ до систем. Це прямо підсилює економічну безпеку, адже дозволяє працювати без простоїв у разі форс-мажорів (наприклад, фізичного знищення офісу або перебоїв в електропостачанні) - дані та сервіси залишаються доступними через хмару.

Як відзначають експерти, гнучкість хмарних рішень і наявність резервних копій нині є передумовами безперервності діяльності підприємства під час кризових ситуацій. До прикладу, перехід частини державних інформаційних ресурсів на хмарні платформи прямо передбачений Планом відновлення України: планується до 2025 р. перенести 30% державних інформаційних ресурсів у хмару в рамках зміцнення кіберстійкості [6].

Цифрові технології також змінюють підходи до управління і прийняття рішень на підприємствах. Сучасні системи бізнес-аналітики, штучний

інтелект для підтримки рішень, датчики IoT дають можливість керівникам отримувати цілісну картину діяльності підприємства майже у реальному часі.

Це підвищує прозорість, але й висуває нові вимоги до компетенцій менеджменту - необхідно вміти інтерпретувати великі масиви даних, будувати сценарне моделювання розвитку подій.

Наприклад, методи сценарного аналізу та тестування стійкості дедалі ширше застосовуються в управлінні ризиками, менеджери моделюють можливі кризові ситуації (наприклад, масована кібератака, відмова IT-інфраструктури, раптові зміни регуляції) та заздалегідь розробляють плани реагування. Таким чином, цифровізація стимулює впровадження проактивного, прогностичного стилю управління економічною безпекою, коли підприємство не лише захищається від наявних загроз, а й прогнозує майбутні ризики і готує варіанти дій.

Для малих і середніх підприємств цифрова трансформація відкриває нові можливості росту і водночас створює особливі виклики. МСП отримують доступ до глобальних ринків через онлайн-платформи, можуть оптимізувати витрати завдяки хмарним сервісам «за запитом», впроваджувати електронний документообіг для економії часу тощо.

В Україні одним із драйверів цифрового розвитку підприємництва стала національна платформа *Дія.Бізнес* - екосистема підтримки МСП, що включає онлайн-портал з безкоштовними консультаціями, освітніми програмами, каталогами сервісів і навіть інструментами для цифрового розвитку бізнесу.

Прочинаючи з 2020 року, портал Дія.Бізнес залучив понад 13 млн відвідувачів. відкрив 14 офлайн центрів підтримки по країні [7]. У 2024 р. портал було оновлено з впровадженням персоналізованих кабінетів для підприємців, рекомендацій подій та маркетплейсу фінансових можливостей (гранти, програми підтримки) [7].

Ці кроки показують, як держава у партнерстві з міжнародними донорами та бізнесом (публічно-приватне партнерство) створює цифрову інфраструктуру для розвитку підприємництва.

В контексті економічної безпеки варто відзначити появу на порталі Дія.Бізнес спеціального розділу «Digital», з інструментами кібергігієни: там доступні послуги кібердіагностики для бізнесу, тести на цифрову грамотність персоналу, каталоги ІТ-рішень для захисту даних. Фактично формується своєрідна платформа цифрової безпеки для підприємців, інтегрована в загальнодержавну цифрову екосистему.

Попри ці позитивні тенденції, більшість МСП усе ще стикаються з численними проблемами у цифровізації. Однією з головних є дефіцит знань та навичок: не всі підприємці володіють цифровою грамотністю, достатньою для впровадження сучасних ІТ-рішень.

За даними Міністерства цифрової трансформації України, лише близько 60% дорослого населення мають базовий чи вище базового рівень цифрових навичок, проте ця частка швидко зростає завдяки масовим освітнім програмам (рис. 1) [5].

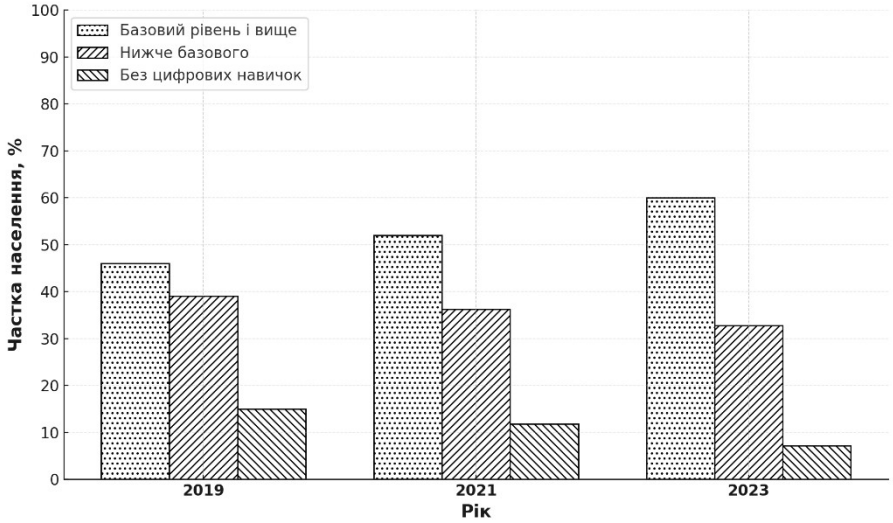

Рис. 1. Рівень цифрової грамотності серед дорослого населення України в динаміці протягом 2019-2023 років

Джерело: сформовано автором на основі [5].

Інша проблема - брак фінансових ресурсів на цифрову модернізацію. Для малого бізнесу інвестиції в кібербезпеку чи спеціалізоване ПЗ можуть бути надто дорогими, особливо в умовах воєнної економіки, коли обороти впали. До того ж, сам ризик кібератак розглядається багатьма підприємцями як абстрактний, поки вони самі не постраждали. На жаль, статистика свідчить про зворотнє: кібератаки все частіше націлені саме на МСП, адже великі корпорації поступово зміцнюють свої кіберзахисні периметри. Таким чином, утворюється «прогалина захисту» для малих підприємств. За оцінками експертів, у 2023 році малий бізнес став жертвою понад 40% усіх кіберінцидентів, але лише меншість МСП мають сформовану систему кібербезпеки (відповідний відділ, плани реагування на інциденти тощо).

Окремо слід розглянути вплив воєнних ризиків. Прямі фізичні загрози (знищення виробничих потужностей, логістичні проблеми) для бізнесу частково компенсуються за рахунок переходу на цифрові канали.

Підприємства, які змогли оперативно перейти на віддалений формат роботи, впровадити онлайн-продажі або перенести дані в хмару, продемонстрували вищі шанси на виживання під час активних бойових дій. За даними опитувань, наведеними в [5], близько 84% українських компаній, що призупиняли діяльність на початку вторгнення, відновили роботу в цифровому форматі чи частково цифровізувавши процеси протягом перших 6 місяців війни. Це свідчить, що цифровізація стала важливим чинником антикризового управління.

Але війна принесла і нові типи кіберзагроз, зросла кількість деструктивних кібератак (віруси-вайпери, DDoS атаки на сайти українських компаній), посилилась роль державних суб’єктів у кіберпросторі (російські хакерські групи атакують український бізнес і держоргани). З метою протидії новим викликам цифрової епохи в Україні розгортається інституційна інфраструктура кіберзахисту, функціонують галузеві центри кібербезпеки, а також урядова команда реагування на комп’ютерні надзвичайні події CERT-UA, що координується Держспецзв’язком.

Ці структури виконують роль оперативної ланки національної системи економічної безпеки. Їх діяльність доповнює традиційні механізми управління ризиками на рівні суб'єктів господарювання, забезпечуючи проактивну взаємодію між державним і приватним секторами у сфері захисту цифрових активів.

Досягнення стійкого розвитку підприємство має забезпечити перекриття (синергію) між своїми цифровими ініціативами та системою управління безпекою. Іншими словами, цифрова трансформація повинна йти пліч-о-пліч з належним управлінням ризиками, кіберзахистом, фінансовою стійкістю - лише тоді підприємство отримає конкурентні переваги без втрати стійкості. Схематично ця концепція представлена на рисунку 2.

Узгодження цифрового розвитку і економічної безпеки передбачає кілька важливих елементів. По-перше, це стратегічне планування з урахуванням ризиків: при розробці цифрової стратегії (впровадженні нових IT-систем, виході на онлайн-ринок тощо) керівництво підприємства повинно одночасно оцінювати ризики і закладати заходи безпеки. Наприклад, перехід на електронний документообіг має супроводжуватися впровадженням засобів криптографічного захисту, систем резервного копіювання та навчанням персоналу кібергігієні.

Рис. 2. Модель узгодження цифрової стратегії та стратегії економічної безпеки підприємства.

Джерело: розроблено автором

По-друге, це організаційна єдність: ІТ-відділ, служба безпеки і бізнес-підрозділи мають працювати не ізольовано, а як єдиний механізм управління. Практика показує, що розрізненість цих функцій призводить до вразливостей - скажімо, впровадження нового застосунку маркетингу без участі фахівців з безпеки може створити «дірку» для кібератаки. Тому сучасні компанії все частіше запроваджують посади директора з цифрової трансформації чи керівника служби інформаційної безпеки, на рівні топ-менеджменту. Саме вони відповідають за координацію технологічного розвитку з заходами захисту, що дозволяє забезпечити єдність стратегій цифровізації та безпеки.

По-третє, інституційний механізм підтримки цифрової безпеки має включати як внутрішні політики, так і зовнішні ресурси. Внутрішньо підприємство розробляє нормативи (політики інформаційної безпеки, плани реагування на інциденти, програми навчання персоналу). Зовнішньо - співпрацює з галузевими центрами кіберзахисту, страхує кіберризики, вступає до асоціацій для обміну інформацією про загрози.

Роль держави та регуляторів тут полягає у створенні сприятливого середовища: законодавство в сфері кібербезпеки, стимули для бізнесу інвестувати в захист (наприклад, гранти або податкові пільги на впровадження засобів кібербезпеки), розвиток освітніх ініціатив.

Публічно-приватне партнерство може виражатися і у спільних проектах: наприклад, державні органи можуть надавати МСП безкоштовні сканування на вразливості або платформи для обміну інформацією про кіберзагрози.

По-четверте, важливим елементом є моніторинг та сценарне планування. Модель узгодження цифрової стратегії та стратегії економічної безпеки підприємства передбача неперервний моніторинг цифрового середовища організації, що охоплює аналіз журналів подій, мережевого трафіку, поведінкових аномалій у фінансових операціях, спроб несанкціонованого доступу. Для цього впроваджуються сучасні аналітичні

інструменти, зокрема системи управління інформаційною безпекою (SIEM),тсистеми виявлення та попередження вторгнень, а також модулі поведінкової аналітики. Такий підхід дозволяє своєчасно виявляти потенційні загрози, адаптувати захисні заходи до змін у цифровому ландшафті та зменшувати ризики порушення стійкості бізнес-процесів.

Зібрані дані не лише дозволяють швидко реагувати на інциденти, а й живлять моделі прогнозування. Підприємство має моделювати різні сценарії розвитку подій: від оптимістичних (ріст онлайн-продажів, масштабування) до кризових (витік даних, кібератака з шифруванням даних, раптовий від'їзд ключових IT-фахівців за кордон). Для кожного сценарію напрацьовуються управлінські рішення, що мінімізують втрати і забезпечуютьи стійкість.

Узагальнення основних емпіричних показників впливу цифрової трансформації на бізнес-стійкість представимо в таблиці 1. Ці дані вказують, як на позитивні ефекти цифровізації, так і нові виклики.

Як бачимо, цифровізація в Україні набирає обертів: інтернет-інфраструктура покращилась, залученість громадян до цифрових сервісів зросла, IT-сектор показує зростання навіть під час війни, стартап-екосистема розвивається. Це створює фундамент для повоєнного відновлення та модернізації економіки на нових засадах.

Таблиця 1. Показники цифрової трансформації економіки України та її впливу на бізнес-діяльність в період 2019-2023 рр.

Показник (Україна)	Базове значення (рік)	Останнє значення (рік)
Інтернет-проникнення серед населення	62% (2019)	78% (2023)
Кількість користувачів застосунку «Дія»	13,7 млн (2021)	19,5 млн (2023)
Експорт IT-послуг (обсяг)	$5.0 млрд (2021)	$6.0 млрд (2022)
Число технічних стартапів (індекс)	100 (2019)	200 (2023)
Частка дорослих з цифровими навичками (базовий рівень і вище)	53% (2021)	60% (2023)
Частка МСП, що впроваджують цифрові технології (орієнтовна оцінка)	30% (2020)	50% (2023)

Джерело: скадено автором [4-6]

Разом з тим, ці процеси вимагають підкріплення належними заходами безпеки - адже зростання цифрової активності робить країну і бізнес більш залежними від кіберстабільності. Тому серед цілей Плану відновлення України до 2025 року зазначено - забезпечити сенсорами 100% об'єктів критичної інформаційної інфраструктури та перевести значну частину державних сервісів у електронний вигляд [6].

Уряд чітко усвідомлює, що цифрова трансформація і безпека повинні йти поруч. Як зазначив віце-прем'єр Михайло Федоров, «в умовах повномасштабної війни підприємці відіграють критично важливу роль - ми повинні створити всі умови для їх успіху», маючи на увазі передусім цифрові можливості та захищені умови роботи [7].

Висновки. Цифрові трансформації суттєво впливають на основи бізнесу, змінюючи традиційні моделі ведення підприємницької діяльності, джерела створення вартості та конкурентні переваги. Для українських підприємницьких структур цифровізація стала не лише фактором розвитку, але й елементом антикризового управління, особливо в умовах війни.

Дослідження показало, що впровадження цифрових технологій тісно пов'язане з новими викликами у сфері економічної безпеки підприємства. Підприємства всіх галузей стикаються з кіберзагрозами, інформаційними ризиками та необхідністю забезпечувати безперервність бізнес-процесів. Успішність цифрової трансформації таким чином значною мірою залежить від спроможності бізнесу інтегрувати заходи безпеки у всі етапи цього процесу.

В роботі проаналізовано останні публікації та досвід України, на підставі чого запропоновано концептуальну модель узгодження цифрової стратегії розвитку підприємства із стратегією та механізмами управління його економічною безпекою. Основна ідея моделі полягає в тому, що цифрові ініціативи повинні плануватися та реалізовуватися в тісній зв'язці з оцінкою ризиків і впровадженням захисних заходів, тобто цифрова трансформація та безпека мають розглядатися не окремо, а як єдиний процес.

Такий підхід дозволить підприємствам отримувати максимальний ефект від нових технологій (підвищення продуктивності, вихід на нові ринки, оптимізація витрат) без втрати контролю над ризиками (кіберінциденти, фінансові втрати, простої).

Практична значущість отриманих результатів полягає у тому, що вони можуть бути використані при розробці напрямків цифрової трансформації на рівні підприємств, галузей і держави. Наприклад, запропоновану модель може бути покладено в основу програм підтримки МСП а частині розробки типових рекомендацій або аудитів для малого бізнесу щодо безпечної цифровізації (наприклад, чек-листи з кібербезпеки при переході на віддалену роботу, при впровадженні e-commerce тощо). Також положення з управління цифровими ризиками можливо застосувати в процесі формування освітніх програм для підприємців.

В подадьших дослідженнях доцільно провести емпіричну перевірку ефективності моделі виконавши вибіркове опитування українських МСП і стартапів, оцінити рівень цифровізації, наявний досвід кіберзахисту, частоту інцидентів тощо, аби виявити залежність між рівнем узгодженості цифрової і безпекової стратегій та фактичними показниками стійкості (наприклад, фінансовими втратами від інцидентів, тривалістю простоїв).

Також доцільно дослідити галузеві особливості - як сектор транспорту чи фінтех реагують на цифрові виклики, які специфічні загрози мають місце і як коригувати модель під ці особливості.

Загалом, забезпечення економічної безпеки підприємництва в умовах цифрової економіки та постконфліктного відновлення країни є багатовимірним завданням, яке потребує подальших наукових розвідок на стику технологій, менеджменту та безпеки.

Література

1. Дергалюк Б. В. Вплив цифрової трансформації на забезпечення економічної безпеки підприємств. *Економічний вісник НТУУ «КПІ»:* зб. наук. пр. 2023. - №26. - С. 65-68.

2. Samoilenko Yu., Britchenko I., Levchenko Ya. Economic Security of the Enterprise within the Conditions of Digital Transformation. *Economic Affairs.* 2022. - Vol. 67, No. 4. - P. 619-629.

3. Muravskyi S., Tolpezhnikov R. Цифрова трансформація та її вплив на економічну безпеку підприємства. *Вісник Маріупольського держ. ун-ту. Серія Економіка*. 2024. - Т. 14, №28. - С. 62-70.

4. Kolodiziev O., Shcherbak V., Kostyshyna T. та ін. Digital transformation as a tool for creating an inclusive economy in Ukraine during wartime. *Problems and Perspectives in Management.* 2024. - Vol. 22(3). - P. 440-454.

5. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine*. Paris: OECD Publishing,* 2024. - 135 p.

6. Bandura R., Staguhn J. *Digital Will Drive Ukraine's Modernization*. URL: https://csis.org/analysis/digital-will-drive-ukraines-modernization (Дата звернення 21.06.25).

7. Оновлений портал Дія.Бізнес - потужний інструмент для розвитку підприємництва. URL: https://brdo.com.ua/news/onovlenyj-portal-diya-biznes-potuzhnyj-instrument-dlya-rozvytku-pidpryyemnytstva/ (Дата звернення 20.06.25).

References

1. Derhaliuk, B.V. (2023), "The impact of digital transformation on ensuring the economic security of enterprises", Ekonomichnyj visnyk NTUU «KPI», vol. 26, pp. 65-68.

2. Samoilenko, Yu. Britchenko, I. and Levchenko, Ya. (2022), “Economic Security of the Enterprise within the Conditions of Digital Transformation”, Economic Affairs, vol. 67, No. 4, pp. 619-629.

3. Muravskyi, S. and Tolpezhnikov, R. (2024), “Digital transformation and its impact on the economic security of the enterprise”, Visnyk Mariupol's'koho derzh. un-tu. Seriia Ekonomika, vol. 14, no. 28, pp. 62-70.

4. Kolodiziev, O. Shcherbak, V. and Kostyshyna, T. (2024), “Digital transformation as a tool for creating an inclusive economy in Ukraine during wartime”, Problems and Perspectives in Management, vol. 22(3), pp. 440-454.

5. OECD (2024), Enhancing Resilience by Boosting Digital Business Transformation in Ukraine, OECD Publishing, Paris.

6. Bandura, R. and Staguhn, J. (2023), “Digital Will Drive Ukraine's Modernization”, available at: https://csis.org/analysis/digital-will-drive-ukraines-modernization (Accessed 21.06.25).

7. BRDO (2024), “Updated Diia.Business portal: a powerful tool for entrepreneurship development”, available at: https://brdo.com.ua/news/onovlenyj-portal-diya-biznes-potuzhnyj-instrument-dlya-rozvytku-pidpryyemnytstva/ (Accessed 20.06.25).

Стаття надійшла до редакції 15.07.2025 р.