DOI: https://doi.org/10.32782/2524-0072/2025-75-92

УДК 366.56

СТРАТЕГІЧНІ ОРІЄНТИРИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ МАЛОГО ПІДПРИЄМНИЦТВА

STRATEGIC GUIDELINES FOR THE DEVELOPMENT OF THE INFORMATION SECURITY SYSTEM FOR BUSINESS ENTITIES

Топалов Володимир Миколайович
аспірант,
Луцький національний технічний університет
ORCID: https://orcid.org/0009-0006-1745-3171

Topalov Volodymyr
Lutsk National Technical University

Стаття присвячена питанням забезпечення інформаційної безпеки суб'єктів малого підприємництва. Обґрунтовано стратегічні орієнтири формування та розвитку системи забезпечення інформаційної безпеки суб'єктів малого підприємництва в умовах цифрової трансформації та зростаючих кіберзагроз. В дослідженні проаналізовано та систематизовано рівні стану інформаційної безпеки суб'єктів малого підприємництва, до кожного рівня запропоновано відповідні типи стратегій забезпечення інформаційної безпеки. Запропоновано структуровану модель формування стратегії, яка включає визначення місії та бачення, аналітичне оцінювання середовища, формування SMART-цілей, стратегічних ініціатив, ресурсне забезпечення, моніторинг ефективності та управління змінами. Розкрито основні напрями вдосконалення системи забезпечення інформаційної безпеки.

Ключові слова: суб'єкти підприємництва, інформаційна безпека, ризики, стійкість, стратегія.

The purpose of the article is to substantiate the strategic guidelines for the formation and development of the information security system of small business entities in the context of digital transformation and growing cyber threats. The relevance of the study is due to the increased vulnerability of small businesses to information risks due to limited resources, low staff awareness and the lack of systematic approaches to information security management. The need to develop an adaptive and economically sound strategy for protecting information assets for this segment of entrepreneurship is extremely relevant in the modern economic and digital context. In the process of the study, methods of systemic, structural-functional and comparative analysis, elements of SWOT and PESTEL analysis were used to assess the external and internal environment, as well as expert modeling to determine the levels of maturity of information security of enterprises and the corresponding strategic approaches to managing them. The methodological basis is supplemented by the logic of strategic management and the principles of risk-oriented thinking. The result of the study was the development of a level classification of the state of information security of small business entities and IS support strategies corresponding to each level. A structured model of strategy formation is proposed, which includes defining a mission and vision, analytical assessment of the environment, formation of SMART goals, strategic initiatives, resource provision, monitoring of effectiveness and change management. The article also reveals the main areas of improvement of the organizational and economic mechanism for IS support, taking into account the real capabilities of small businesses. The practical value of the article lies in the possibility of using the results to develop effective information security strategies at the level of small businesses, which will contribute to reducing information risks, increasing the level of trust from partners and clients, as well as integrating information security into the overall business strategy.

Keywords: business entities, information security, risks, sustainability, strategy.

Постановка проблеми. У сучасних умовах стрімкої цифровізації бізнес-процесів, посилення кіберзагроз та зростання значущості інформаційних ресурсів, питання забезпечення інформаційної безпеки (ІБ) набуває пріоритетного значення для суб'єктів підприємництва. Інформація перетворилася на один із основних стратегічних активів, який безпосередньо впливає на конкурентоспроможність, репутацію, фінансову стабільність і життєз-

датність бізнес-структур [12]. Незважаючи на наявність окремих методичних рекомендацій, сучасна наукова думка ще не сформувала комплексної моделі стратегічного управління інформаційною безпекою суб'єктів малого підприємництва з урахуванням національного та регіонального контексту [4]. Сьогодні актуальними залишаються питання розробки адаптивних стратегій, які б включали інституційні, технологічні та освітні компоненти, орієнтовані на мінімізацію ризиків за умов обмеженості ресурсів. Особливе значення набувають також публічно-приватні ініціативи, цифрова інклюзія та розбудова локальних екосистем безпеки, що дозволяють суб'єктам малого підприємництва об'єднуватися, отримувати доступ до знань, сервісів та інфраструктури інформаційного захисту. Необхідність наукового дослідження формування та реалізації стратегій інформаційної безпеки суб'єктів малого підприємництва зумовлена як викликами цифрового середовища, так і потребою в нових управлінських підходах, які забезпечать довготривалу стійкість, гнучкість і конкурентоспроможність малого бізнесу в цифрову епоху.

Аналіз останніх досліджень і публікацій. Значний внесок у формування базових положень та концепцій забезпечення інформаційної безпеки суб'єктів підприємництва зроблено як вітчизняними, так і зарубіжними дослідниками. У контексті економічного аналізу заслуговують на увагу праці Білько С. [1], де оцінено взаємозв'язки між економічною та інформаційною безпекою підприємств на основі аналізу стратегій бізнесу. У працях Дубницького В. та Науменка Н. [2] визначено методологічні засади забезпечення інформаційної безпеки регіонів. Праці Крауса К. [3] розкривають особливості цифрової трансформації кібербезпеки під час воєнного стану. Дослідження Ковальської Л. [4] розкривають економічний зміст інформаційної безпеки регіону.

Публікації, як Кузьомка В. [5] та Леоненко Н. і Поступної О. [6], визначають вплив цифровізації на інформаційну безпеку підприємств сучасних в умовах. Науменко Н. [7] у своїх дослідженнях систематизує напрями забезпечення інформаційної безпеки. Дослідження Шостак Л. та Помазуна О. [8], зосереджені на зв'язку між захистом даних та інноваційними бізнес-моделями. Яковенко Я. [9] аналізує стратегічні орієнтири цифрової трансформації суб'єктів підприємництва України. Таким чином, аналіз досліджень процесу забезпечення інформаційної безпеки суб'єктів господарювання, демонструє високу актуальність зазначеної проблематики, а також доцільність визначення стратегічних орієнтирів розвитку інформаційної безпеки суб'єктів підприємництва.

Виділення невирішених раніше частин загальної проблеми. Ефективне управління інформаційною безпекою потребує як технічних рішень так і методологічно обґрунтованих підходів до її дослідження. Зокрема, необхідно враховувати специфіку суб'єктів підприємництва за масштабами, галузевими особливостями, рівнем цифрової досконалості. Також актуальними залишаються питання розробки адаптивних стратегій, які б включали інституційні, технологічні та освітні компоненти, орієнтовані на мінімізацію ризиків за умов обмеженості ресурсів. Необхідність дослідження формування та реалізації стратегій інформаційної безпеки суб'єктів малого підприємництва зумовлена як викликами цифрового середовища, так і потребою в нових управлінських підходах, які забезпечать довготривалу стійкість, гнучкість і конкурентоспроможність малого бізнесу в цифрову епоху.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування стратегічних орієнтирів формування та розвитку системи забезпечення інформаційної безпеки суб'єктів малого підприємництва в умовах цифрової трансформації та зростаючих кіберзагроз.

Виклад основного матеріалу дослідження. У сучасних умовах трансформації цифрового середовища, розвиток малого підприємництва в Україні набуває особливого значення, зважаючи на його роль у забезпеченні економічної стійкості, створенні робочих місць та стимулюванні інновацій [2]. Проте поряд із потенціалом зростає і вразливість малого бізнесу до інформаційних загроз, що зумовлює необхідність вивчення економічних, соціальних та регуляторних факторів впливу та засад інформаційної безпеки [1]. Інформаційна безпека для суб'єктів малого підприємництва є стратегічною передумовою сталого розвитку.

Аналіз досліджуваної проблеми засвідчив, що у більшості випадків, суб'єкти малого підприємництва працюють на основі стандартного програмного забезпечення та не впроваджують формалізованих політик безпеки. Така ситуація створює ризики як для самих підприємств так і для їх споживачів і партнерів, що робить проблему інформаційної безпеки

системною. Тому, суб'єктам малого підприємництва, необхідно впроваджувати гнучкі, адаптивні та поетапні стратегії захисту, що враховують їх поточний стан захищеності. Відсутність системного підходу до інформаційної безпеки призводить до накопичення ризиків, втрат комерційної інформації та зниження конкурентоспроможності. У зв'язку з цим актуальним є поділ підприємств за рівнями інформаційної безпеки та відповідне стратегічне планування, що дозволяє раціонально розподілити ресурси, підвищити стійкість до кіберзагроз та забезпечити поступовий перехід до зрілих моделей управління бізнес процесами [5]. Суб'єктам малого підприємництва доцільно використовувати адаптовані стратегії інформаційної безпеки, виходячи з наявних рівнів їхньої захищеності. Систематизовані характеристики кожного рівня, рекомендовані стратегії та основні управлінські дії представлено в таблиці 1.

Аналіз процесу управління інформаційною безпекою суб'єктів малого підприємництва засвідчив важливість врахування специфіки ресурсного, організаційного та кадрового потенціалу досліджуваних суб'єктів господарювання [7]. Тому, вибір стратегії забезпечення інформаційної безпеки доцільно здійснювати на основі поточного рівня захищеності, адаптуючи підходи до реалій малого бізнесу. Так, суб'єкти малого підприємництва з низьким рівнем інформаційної безпеки характеризуються повною відсутністю системного підходу, низькою обізнаністю працівників, відсутністю навіть базових технічних засобів захисту (антивірусів, фаєрволів) та високими ризиками витоку або втрати даних [3]. У таких умовах пропонуємо застосовувати стратегію базового захисту, головна мета якої – якнайшвидше знизити критичні загрози. До основних дій належать: впровадження мінімально необхідного програмного забезпечення для захисту, організація резервного копіювання даних, а також підвищення обізнаності персоналу шляхом коротких тренінгів або інструктажів.

Суб'єкти підприємництва з середнім рівнем інформаційної безпеки характеризуються фрагментарним впровадженням відповідних заходів, де зазвичай, деякі засоби вже працюють але загальна політика безпеки не систематизована, а ризики залишаються значними. Для цього рівня підходить стратегія формування системи ІБ, яка передбачає проведення внутрішнього або зовнішнього аудиту наявної ситуації, створення політики інформаційної безпеки підприємства, мінімізацію виявлених вразливостей та підвищення технічної грамотності співробітників.

Достатній рівень інформаційної безпеки суб'єктів підприємництва свідчить про те що, підприємство вже має формалізовану політику безпеки, здійснює оновлення програмного забезпечення та резервне копіювання,

Таблиця 1

Стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва залежно від поточного рівня інформаційної безпеки

Поточний рівень інформаційної безпеки	Характеристика стану інформаційної безпеки	Рекомендована стратегія	Рекомендовані дії
Низький	Відсутність системного підходу до ІБ, низька обізнаність персоналу, високі ризики	Стратегія базового захисту	Встановлення базового антивірусу, навчання працівників, регулярні резервні копії
Середній	Наявні окремі заходи захисту, політики ІБ фрагментарні, недостатній технічний контроль	Стратегія формування системи ІБ	Розробка політики безпеки, аудит поточних засобів, мінімізація вразливостей
Достатній	Формалізовані політики безпеки, регулярне оновлення ПЗ, частковий моніторинг	Стратегія оптимізації і контролю	Впровадження систем моніторингу, періодичне тестування захищеності, розмежування прав доступу
Високий	Повноцінна система управління ІБ, аудит, інтеграція ІБ у бізнес-процеси	Стратегія інтеграції та розвитку	Автоматизація процедур безпеки, зовнішній аудит, інвестиції у кіберстійкість

Джерело: сформовано на основі [3; 6; 7; 8, 9]

контролює доступ до ресурсів, однак рівень автоматизації або моніторингу ще не є високим [6]. У цьому випадку доцільно впроваджувати стратегію оптимізації і контролю, яка орієнтована на регулярний аналіз ефективності наявних рішень, застосування систем моніторингу активності (наприклад, логування подій), а також сегментацію доступу до важливих даних за принципом мінімального привілею.

Високий рівень інформаційної безпеки суб'єктів підприємництва передбачає наявність сформованої системи ІБ, її відповідність національним або міжнародним стандартам (зокрема ISO/IEC 27001), регулярний аудит та інтеграцію процесів безпеки у загальну бізнес-стратегію. У таких умовах найбільш ефективною буде стратегія інтеграції та розвитку, що фокусується на вдосконаленні поточних рішень, автоматизації процесів, впровадженні кіберстійких підходів, а також залученні зовнішніх експертів або участі в галузевих ініціативах з кіберзахисту. Таким чином, поетапне просування від базового захисту до стратегічного управління інформаційною безпекою є реалістичним шляхом для підприємств. Такий підхід забезпечує відповідність регуляторним вимогам та підвищення конкурентоспроможності за рахунок захисту інформаційних активів. Крім того, стратегічне управління інформаційною безпекою суб'єктів підприємництва потребує системного і комплексного підходу, який поєднує місію, бачення, аналіз зовнішнього та внутрішнього середовища, формування цілей, визначення стратегічних ініціатив, впровадження, контроль та інноваційний розвиток.

Система побудови стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва представлена на рис. 1.

У запропонованій моделі визначено логічну послідовність етапів формування стратегії, яка базується на сучасних концепціях стратегічного менеджменту, цифрової трансформації та ризик-орієнтованого мислення, що загалом являє собою інклюзивне інституційне забезпечення досліджуваних процесів. Першим етапом є визначення місії та бачення розвитку системи забезпечення інформаційної безпеки, що дозволяє окрес-

Рис. 1. Система побудови стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва

Джерело: сформовано за результатами дослідження

лити довгострокові орієнтири підприємства у сфері інформаційної безпеки. Місія відображає основне призначення системи – збереження конфіденційності, цілісності та доступності інформаційних активів, а бачення формує уявлення про бажаний стан системи ІБ у перспективі.

Другим етапом є аналіз середовища функціонування системи ІБ, що здійснюється з використанням таких інструментів, як SWOT-аналіз (визначення сильних і слабких сторін, можливостей та загроз) та PESTEL-аналіз (оцінка політичних, економічних, соціальних, технологічних, екологічних і правових факторів) [2]. Такий підхід дозволяє адаптувати стратегію до реального контексту функціонування суб'єктів малого підприємництва, виявити бар'єри та драйвери цифрової безпеки.

На основі аналітичної оцінки формуються цілі та завдання системи ІБ, які мають бути конкретними, вимірюваними, досяжними, релевантними та обмеженими в часі (SMART) [10; 11]. Цілі охоплюють як превентивні заходи (запобігання інцидентам), так і реактивні (оперативне реагування та відновлення), а також стратегічні – інтеграцію ІБ у загальну систему управління підприємством.

Стратегічні напрями та ініціативи визначають вектори дій для досягнення поставлених цілей. Сюди належать розробка політик безпеки, впровадження навчальних програм, вибір технологічних рішень, побудова партнерських мереж тощо. Важливо, що стратегічні напрями мають бути узгоджені з конкурентною стратегією підприємства, адже інформаційна безпека все частіше розглядається як фактор конкурентоспроможності.

Особливу увагу доцільно приділити інноваціям у сфері ІБ, які передбачають впровадження новітніх технологій (AI, Big Data, Zero Trust), адаптацію до змін у цифровому середовищі, розвиток інституційних форм підтримки (наприклад, ІБ-кластерів). Зазначене пропонуємо доповнити цифровізацією виробничих і сервісних процесів, що вимагає відповідних механізмів захисту цифрових платформ, даних споживачів і транзакцій.

У практичному аспекті реалізації стратегії значущим є компонент управління ресурсами, включаючи кадрові, фінансові та технічні ресурси, необхідні для функціонування системи інформаційної безпеки, що також передбачає впровадження механізмів контролю результативності, зокрема регулярні аудити та оцінку ефективності прийнятих рішень.

Завершальним етапом стратегічного циклу є управління ризиками та змінами, що дозволяє підтримувати гнучкість системи інформаційної безпеки, швидко адаптуватися до нових загроз і переглядати політики безпеки відповідно до змін у внутрішньому або зовнішньому середовищі. Цей етап забезпечує життєздатність стратегії та її динамічну відповідність викликам цифрової епохи.

Таким чином, запропонована система побудови стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва є логічно цілісною, адаптованою до сучасних умов ведення бізнесу та орієнтованою на результат. Її впровадження сприятиме підвищенню рівня захищеності МП та формуванню довіри з боку споживачів, партнерів і держави. Розроблена модель ґрунтується на комплексному підході, що поєднує стратегічне бачення, аналітичну оцінку середовища, формування цілей, визначення пріоритетних ініціатив, ресурсне забезпечення, інноваційність та ефективні механізми реалізації. Така структура дозволяє суб'єктам малого підприємництва протистояти сучасним інформаційним загрозам та інтегрувати інформаційну безпеку в загальну бізнес-стратегію як фактор конкурентної переваги досліджуваних підприємств.

Висновки. Запропоновано підхід до формування стратегії інформаційної безпеки суб'єктів малого підприємництва, який базується на принципах системності, адаптивності та економічної доцільності. Поетапна логіка впровадження, від базового захисту до інтегрованої системи стратегічного управління, враховує реалії українського бізнес-середовища, зокрема обмеженість фінансових та трудових ресурсів, недостатній рівень цифрової грамотності, а також потребу в поступовому нарощуванні організаційної спроможності. Такий підхід, дозволяє мінімізувати ризики втрати або загрозу втрати важливої інформації, забезпечити правову відповідність, підвищити ефективність внутрішніх процесів і сформувати довіру серед партнерів, споживачів та державних інституцій.

Подальший розвиток системи забезпечення інформаційної безпеки, доцільно орієнтувати на застосування інституційного потенціалу (кластеризація, партнерства, асоціації малого бізнесу), а також підвищення цифрової культури керівників та персоналу підприємств. Доцільно також розробляти

державні та регіональні програми підтримки малих підприємств у сфері кіберзахисту, зокрема через надання грантів, податкових пільг або доступу до спеціалізованих сервісів ІБ. Результати проведеного дослідження можуть бути покладені в основу нормативно-правового вдосконалення політик цифрової безпеки малого підприємництва в Україні, а також використані у практичній діяльності консультантів, аудиторів та самих підприємців для стратегічного планування і модернізації систем захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Білько С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. *Науковий вісник Полісся.* 2022. 1 (24), С. 58–77.

2. Дубницький В.І., Науменко Н.Ю. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. *Вісник економічної науки України.* 2019. №1. URL: http://dspace.nbuv.gov.ua/handle/123456789/151638 (дата звернення: 07.05.2025).

3. Краус К.М., Краус Н.М., Штепа О.В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26–37.

4. Ковальська Л., Топалов В., Топалов Р. Інформаційна безпека регіону: підходи до розгляду та економічна сутність. *Економічний форум*. 2023. № 13 (2), С. 18–24.

5. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. *Інноваційне підприємництво: стан та перспективи розвитку*: збірник матеріалів VI Всеукраїнської науково-практичної конференції (м. Київ, 29-30.03.2021). Київ: КНЕУ. 2021. С. 26–28.

6. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України. Серія: Державне управління.* 2022. №2 (17). URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883 (дата звернення: 25.05.2025).

7. Науменко Н.Ю. Аналіз економічних наукових напрямків у сфері інформаційної безпеки. *Електронне наукове фахове видання з економічних наук "Modern Economics".* 2019. №16. С. 115–120. URL: http://dspace.mnau.edu.ua/jspui/bitstream/123456789/6290/1/naumenko.pdf (дата звернення: 25.05.2025).

8. Шостак Л., Помазун О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека.* 2024. № 5 (14), С. 160–165.

9. Яковенко Я.Ю., Білик М.Ю., Олійник Є.В. Цифрова трансформація бізнес-структур: стратегічні орієнтири в епоху інновацій та технологічних змін. *Економічний простір.* 2024. № 190. С. 355–360.

10. State of Digital Transformation 2025. TEKsystems. 2025. https://www.teksystems.com/en/insights/state-of-digital-transformation-2025 (дата звернення: 25.05.2025).

11. Global Cybersecurity Outlook 2025. World Economic Forum. 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата звернення: 20.05.2025).

12. C-suite disconnect on cybersecurity threatens business value and resilience. Ernst & Young. 2025. https://www.ey.com/en_us/newsroom/2025/04/c-suite-disconnect-on-cybersecurity-threatens-business-value-and-resilience-ey-study-finds (дата звернення: 4.05.2025).

REFERENCES:

1. Bilko S. (2022). Informatsiina ta ekonomichna bezpeka: otsiniuvannia rivnia ta vzaiemozviazku [Information and economic security: assessment of level and interconnection]. *Naukovyi visnyk Polissia*, 1 (24), pp. 58–77. (in Ukrainian).

2. Dubnytskyi V.I., Naumenko N.Yu. (2019). Metodolohichne zabezpechennia formuvannia informatsiinoi bezpeky v sferi ekonomichnoi bezpeky rehionu [Methodological support for the formation of information security in the field of regional economic security]. *Visnyk ekonomichnoi nauky Ukrainy*, (1). Retrieved from http://dspace.nbuv.gov.ua/handle/123456789/151638 (accessed: May 7, 2025). (in Ukrainian).

3. Kraus K.M., Kraus N.M., Shtepa O.V. (2022). Tsyfrova transformatsiia kiberbezpeky na mikroriavni v umovakh voiennoho stanu [Digital transformation of cybersecurity at the micro level under martial law]. *Innovation and Sustainability*, (3), pp. 26–37. (in Ukrainian).

4. Kovalska L., Topalov V., Topalov R. (2023). Informatsiina bezpeka rehionu: pidkhody do rozghliadu ta ekonomichna sutnist [Regional information security: approaches and economic essence]. *Ekonomichnyi forum*, 13 (2), pp. 18–24. (in Ukrainian).

5. Kuziomko V. (2021). Informatsiina bezpeka biznesu v umovakh tsyfrovykh transformatsii ekonomiky [Information security of business in conditions of digital transformation of the economy]. In *Innovatsiine pidpryiemnytstvo: stan ta perspektyvy rozvytku* (pp. 26–28). Kyiv: KNEU. (in Ukrainian).

6. Leonenko N.A., Postupna O.V. (2022). Informatsiina bezpeka Ukrainy: mekhanizmy, suchasni vyklyky ta zahrozy v umovakh informatsiinoho hlobalizmu [Information security of Ukraine: mechanisms, current challenges and threats in the context of information globalism]. *Visnyk Natsionalnoho universytetu tsivilnoho zakhystu Ukrainy*. *Seriia: Derzhavne upravlinnia,* (2) 17. Retrieved from http://repositsc.nuczu.edu.ua/handle/123456789/16883 (accessed: May 25, 2025). (in Ukrainian).

7. Naumenko N.Yu. (2019). Analiz ekonomichnykh naukovykh napriamkiv u sferi informatsiinoi bezpeky [Analysis of economic scientific approaches in the field of information security]. *Modern Economics*, (16), pp. 115–120. Retrieved from http://dspace.mnau.edu.ua/jspui/bitstream/123456789/6290/1/naumenko.pdf (accessed: May 25, 2025). (in Ukrainian).

8. Shostak L., Pomazun O. (2024). Informatsiina bezpeka v konteksti innovatsiinoho rozvytku biznes-modeli vitchyznianykh pidpryiemstv v umovakh tsyfrovoi ekonomiky [Information security in the context of innovative development of domestic business models under digital economy]. T*syfrova ekonomika ta ekonomichna bezpeka*, 5 (14), pp. 160–165. (in Ukrainian).

9. Yakovenko Ya.Yu., Bilyk M.Yu., Oliinyk Ye.V. (2024). Tsyfrova transformatsiia biznes-struktur: stratehichni oriientyry v epokhu innovatsii ta tekhnolohichnykh zmin [Digital transformation of business structures: strategic guidelines in the age of innovation and technological change]. *Ekonomichnyi prostir*, (190), pp. 355–360. (in Ukrainian).

10. TEKsystems. (2025). *State of Digital Transformation 2025*. Retrieved from https://www.teksystems.com/en/insights/state-of-digital-transformation-2025 (accessed: May 25, 2025).

11. World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. Retrieved from https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (accessed: May 20, 2025).

12. Ernst Young. (2025). C-suite disconnect on cybersecurity threatens business value and resilience. Retrieved from https://www.ey.com/en_us/newsroom/2025/04/c-suite-disconnect-on-cybersecurity-threatens-business-value-and-resilience-ey-study-finds (accessed: May 4, 2025).