DOI: https://doi.org/10.32782/2308-1988/2026-59-155
УДК 004.056:005.52:658

Обрамич Орест Сергійович
аспірант,
Національний університет «Львівська політехніка»
ORCID: https://orcid.org/0009-0006-2280-5549

Orest Obramych
Lviv Polytechnic National University

ЕКСПРЕС-ДІАГНОСТИКА СТАНУ ЦИФРОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

EXPRESS DIAGNOSTICS OF THE STATE OF DIGITAL SECURITY OF AN ENTERPRISE

Анотація. У статті досліджено теоретичні та прикладні аспекти експрес-діагностики стану цифрової безпеки підприємства в умовах цифрової трансформації. Цифрову безпеку розглянуто як інтегровану систему інформаційної та кібербезпеки, що забезпечує захист ресурсів і стійкість інфраструктури. Визначено зростання цифрових ризиків і обмеженість традиційних методів оцінювання. Доведено ефективність експрес-діагностики як інструменту оперативного виявлення критичних зон і підтримки управлінських рішень. Запропоновано ризик-орієнтований підхід із селективним відбором індикаторів, визначенням їх вагомості та розрахунком інтегрального індексу цифрової безпеки. Обґрунтовано доцільність зонування результатів діагностики. Практичне значення полягає у підвищенні ефективності управління ризиками та прийняття обґрунтованих рішень.

Ключові слова: цифрова безпека підприємства, інформаційна безпека, кібербезпека, експрес-діагностика, цифрові ризики, інтегральний індекс, цифрова трансформація, управління безпекою.

Summary. The article examines theoretical and applied aspects of express diagnostics of enterprise digital security in the context of digital transformation of the economy. Digital security is substantiated as an integrated system combining information security and cybersecurity, ensuring both the protection of information resources and the resilience of digital infrastructure. It is determined that modern business environments are characterized by an increasing level of digital risks, growing complexity of information systems, and the need for rapid response to threats, which limits the effectiveness of traditional research methods such as analysis, evaluation, and comprehensive diagnostics. The study proves that express diagnostics is an effective tool for rapid assessment of the state of enterprise digital security, enabling the identification of critical risk areas within a short time frame and providing an informational basis for managerial decision-making. The essence of express diagnostics is defined as a type of managerial diagnostics based on a limited but representative set of indicators. Its key advantages include operational efficiency, cost-effectiveness, adaptability, and practical orientation. The scientific novelty of the research lies in the proposed risk-oriented adaptive methodological approach to express diagnostics of enterprise digital security. This approach involves the selective choice of indicators depending on their criticality, the determination of weighting coefficients considering industry-specific features and the level of digital maturity, and the calculation of an integral digital security index. The feasibility of result zoning is substantiated in order to enhance the effectiveness of managerial decision-making. The practical significance of the obtained results lies in their applicability for improving digital risk management, timely threat identification, and substantiating the need for in-depth diagnostics. Prospects for further research include the development of a comprehensive system of indicators for express diagnostics and the adaptation of the methodology to different sectors of the economy.

Keywords: enterprise digital security, information security, cybersecurity, express diagnostics, digital risks, integral index, digital transformation, security management.

Постановка проблеми. Цифровізація бізнес-процесів, стрімке впровадження інформаційно-комунікаційних технологій та інтеграція підприємств у глобальні цифрові екосистеми суттєво трансформують підходи до забезпечення їхньої безпеки. У сучасних умовах цифрова безпека підприємства доцільно розглядати як синергетичну єдність інформаційної та кібербезпеки, що охоплює захист даних, інформаційних систем, цифрових інфраструктур і каналів комунікації від внутрішніх і зовнішніх загроз. Водночас динамічність цифрового середовища, зростання кількості кіберінцидентів, а також ускладнення архітектури інформаційних систем актуалізують проблему

своєчасного виявлення вразливостей і оцінювання рівня захищеності підприємств.

Традиційні підходи до дослідження стану безпеки, зокрема комплексна діагностика, аудит, глибоке оцінювання або аналітичне дослідження, характеризуються значною тривалістю, ресурсоємністю та потребою у високоспеціалізованих експертних знаннях. За умов обмеженості часу управлінських рішень та необхідності оперативного реагування на загрози такі підходи не завжди є ефективними, особливо для підприємств, що функціонують у висококонкурентному та турбулентному середовищі. Це зумовлює об'єктивну потребу у застосуванні більш гнучких, швидких та адаптивних інструментів оцінювання стану цифрової безпеки.

У цьому контексті особливої актуальності набуває експрес-діагностика як інструмент оперативного визначення поточного рівня цифрової безпеки підприємства, що дозволяє у стислі терміни ідентифікувати критичні зони ризику, сформувати первинну інформаційну базу для прийняття управлінських рішень та визначити доцільність проведення поглиблених досліджень. Проте, незважаючи на значний науковий доробок у сфері інформаційної та кібербезпеки, питання методичного забезпечення експрес-діагностики залишаються недостатньо розробленими. Зокрема, відсутня уніфікована система показників, не сформовано чітких вимог до процедури її проведення, а також не визначено місце експрес-діагностики у загальній системі управління цифровою безпекою підприємства.

Таким чином, існує науково-практична проблема, що полягає у необхідності обґрунтування сутності експрес-діагностики стану цифрової безпеки підприємства, визначення її переваг у порівнянні з традиційними методами дослідження, а також розроблення методичного підходу до її проведення. Вирішення зазначеної проблеми сприятиме підвищенню ефективності управління цифровими ризиками та забезпеченню стійкості підприємств в умовах цифрової трансформації економіки.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення цифрової безпеки підприємств та інструментів її оцінювання формується на перетині досліджень цифрової трансформації, економічної безпеки та діагностичних підходів до управління діяльністю суб'єктів господарювання. Зокрема, у праці О. Правдивця [1] обґрунтовано науково-практичний інструментарій оцінювання рівня цифрової трансформації та інноваційного розвитку системи економічної безпеки підприємств ІТ-сфери, що дозволяє ідентифікувати взаємозв'язок між цифровізацією та рівнем захищеності бізнесу. Автор акцентує увагу на комплексному підході до оцінювання, який поєднує технологічні та управлінські аспекти.

Подальший розвиток підходів до оцінювання цифрового розвитку бізнес-організацій представлено у дослідженні Л. Лігоненко та К. Зеленько [2], де розкрито сутність цифрової зрілості та систематизовано інструменти її вимірювання. Запропоновані підходи дозволяють оцінити готовність підприємства до цифрових змін, однак потребують значних ресурсів і часу, що обмежує їх застосування в умовах оперативного управління.

У роботі M. Chepeliuk [3] досліджено бар'єри та драйвери цифрової трансформації бізнес-структур в Україні, що дає підстави стверджувати про зростання значущості цифрових ризиків у діяльності підприємств. У свою чергу, G. Cainelli, A. D'Amato та M. Mazzanti [4] доводять, що впровадження інновацій, зокрема цифрових, супроводжується необхідністю підвищення ефективності використання ресурсів і управління ризиками, що опосередковано стосується і питань цифрової безпеки.

Вагомий внесок у розвиток діагностичного інструментарію здійснено у працях, присвячених експрес-діагностиці. Так, О. Мельник [5] розробила методичні положення щодо експрес-діагностики загрози банкрутства підприємства, підкреслюючи її значення як інструменту швидкого реагування. Аналогічні підходи розглядаються у роботі В. Петрякова [6], де здійснено порівняння експрес- та фундаментальної діагностики в антикризовому управлінні, що дозволяє визначити переваги оперативності та адаптивності першої. Дослідження А. Сотник [7] підтверджує можливість застосування експрес-діагностики для оцінювання ефективності комерційної діяльності підприємств, акцентуючи на її практичній доцільності.

Теоретичні засади економічної діагностики узагальнено у праці Т. Загорної [8], де визначено її сутність, види та місце в системі управління підприємством. Доповненням до цього є дослідження З. Литвин [9], в якому обґрунтовано доцільність діагностики бізнес-процесів як інструменту підвищення ефективності функціонування підприємств у сучасних умовах.

Окремий напрям досліджень пов'язаний з оцінюванням цифрової зрілості підприємств. Зокрема, Т. Тардаскіна [10] пропонує методичні підходи до оцінки цифрової зрілості підприємств сфери електронних комунікацій, що дозволяє враховувати галузеву специфіку. Водночас у роботі Т. Передерій [11] підкреслюється роль стратегії цифрової безпеки як ключового елементу цифрової трансформації економіки. Результати дослідження Н. Аванесової, О. Мордовцева та Т. Колодяжної [12] спрямовані на формування механізму комплексного забезпечення цифрової безпеки промислових підприємств, що передбачає інтеграцію організаційних, технічних та економічних інструментів.

У працях В. Міщенка [13] розглядаються стратегічні аспекти управління цифровою трансформацією економіки, що визначають загальний контекст функціонування підприємств у цифровому середовищі. Дослідження Т. Полозової та співавторів [14] зосереджені на механізмах мінімізації ризиків економічної безпеки в умовах цифровізації, що безпосередньо пов'язано з необхідністю оцінювання цифрових загроз. Водночас В. Ящук [15] аналізує роль кібербезпеки у системі інформаційної безпеки, підкреслюючи її стратегічне значення.

Незважаючи на значний науковий доробок, слід зазначити, що існуючі дослідження здебільшого орієнтовані на комплексні або фундаментальні підходи до оцінювання цифрової безпеки та цифрової зрілості підприємств. Водночас питання формування методичного забезпечення експрес-діагностики стану цифрової безпеки, визначення її сутності, принципів та інструментарію залишаються недостатньо розробленими. Це обумовлює необхідність подальших наукових досліджень у даному напрямі.

Метою статті є теоретичне обґрунтування сутності експрес-діагностики стану цифрової безпеки підприємства як інструменту оперативного управління цифровими ризиками в умовах цифрової трансформації. Досягнення поставленої мети передбачає визначення переваг експрес-діагностики порівняно з традиційними методами дослідження, обґрунтування вимог до її здійснення та розроблення методичного підходу до її проведення.

Виклад основного матеріалу дослідження. У сучасних умовах цифрової трансформації економіки поняття цифрової безпеки підприємства набуває системного характеру та розглядається як інтегрована сукупність інформаційної та кібербезпеки [11; 15]. Такий підхід дозволяє охопити як захист інформаційних ресурсів (даних, знань, інформаційних потоків), так і забезпечення стійкості цифрової інфраструктури (мереж, програмного забезпечення, апаратних засобів) до зовнішніх і внутрішніх загроз. Відтак цифрова безпека підприємства виступає не лише технічною, а й управлінською категорією, що безпосередньо впливає на безперервність бізнес-процесів, конкурентоспроможність і економічну стійкість суб'єкта господарювання. В умовах зростання складності цифрових екосистем та поширення кіберризиків виникає об'єктивна потреба у впровадженні ефективних інструментів оцінювання її стану.

Традиційні підходи до дослідження цифрової безпеки, зокрема аналізування, оцінювання та фундаментальна діагностика, мають значну наукову та практичну цінність, проте характеризуються високою трудомісткістю, тривалістю реалізації та необхідністю залучення значних ресурсів [8; 9]. Аналізування передбачає детальне дослідження окремих складових системи безпеки, оцінювання – встановлення кількісних або якісних параметрів її стану, тоді як фундаментальна діагностика орієнтована на комплексне виявлення причинно-наслідкових зв'язків і глибинних проблем. Утім, зазначені підходи не завжди відповідають потребам оперативного управління, коли необхідне швидке отримання узагальненої інформації для прийняття рішень.

У цьому контексті доцільним є застосування експрес-діагностики, яку слід розглядати як специфічний різновид управлінської діагностики, спрямований на оперативне визначення поточного стану цифрової безпеки підприємства на основі обмеженого, але репрезентативного набору показників [5; 6; 7]. Сутність експрес-діагностики полягає у швидкому виявленні критичних відхилень і потенційних загроз без проведення глибокого аналітичного дослідження, що забезпечує її високу адаптивність до динамічних умов функціонування підприємства. На відміну від аналізування та оцінювання, експрес-діагностика не передбачає деталізованого розкриття всіх аспектів системи безпеки, а зосереджується на ключових індикаторах, які відображають її загальний рівень і проблемні зони.

Порівняльний аналіз дозволяє виокремити низку переваг експрес-діагностики [6]. По-перше, це оперативність отримання результатів, що забезпечує можливість швидкого реагування на загрози. По-друге, відносно низька ресурсоємність, що робить її доступною для широкого кола підприємств, у тому числі малих і середніх. По-третє, гнучкість та адаптивність до змін зовнішнього середовища, що дозволяє модифікувати інструментарій залежно від специфіки діяльності підприємства. По-четверте, орієнтація на підтримку управлінських рішень, оскільки результати експрес-діагностики можуть використовуватися як основа для подальшого поглибленого дослідження або розроблення заходів підвищення рівня цифрової безпеки.

Разом з тим ефективність експрес-діагностики значною мірою залежить від дотримання певних вимог до її здійснення. До ключових із них слід віднести оперативність проведення, що передбачає мінімізацію часових витрат; репрезентативність, яка забезпечується відбором найбільш інформативних показників; валідність результатів, що визначає їхню достовірність та обґрунтованість; економічність, яка полягає у мінімізації витрат на проведення діагностики; а також адаптивність, що дозволяє враховувати галузеві та організаційні особливості підприємства. Важливим є також забезпечення узгодженості експрес-діагностики із загальною системою управління цифровою безпекою, що дозволяє інтегрувати її результати у процес прийняття управлінських рішень.

З огляду на зазначене, доцільним є формування методичного підходу до проведення експрес-діагностики стану цифрової безпеки підприємства. З огляду на обмеження традиційних підходів, у дослідженні запропоновано удосконалений методичний підхід до проведення експрес-діагностики стану цифрової безпеки підприємства, що ґрунтується на принципах ризик-орієнтованості, адаптивності та інтегрального оцінювання. На відміну від існуючих підходів, запропонована методика передбачає не лише фіксацію поточного стану, а й врахування критичності цифрових загроз та їхнього впливу на функціонування підприємства.

Перший етап передбачає ідентифікацію об'єкта діагностики та структуризацію складових цифрової безпеки на інформаційну та кібербезпеку.

На другому етапі здійснюється ризик-орієнтований відбір індикаторів, які групуються за рівнем їхньої значущості (критичні, значущі, допоміжні), що дозволяє зосередити увагу на найбільш вразливих елементах цифрового середовища підприємства.

Третій етап включає визначення вагових коефіцієнтів індикаторів з урахуванням галузевої специфіки, рівня цифрової зрілості підприємства та характеру актуальних загроз [2; 10]. Такий підхід забезпечує адаптивність експрес-діагностики та підвищує достовірність отриманих результатів.

На четвертому етапі здійснюється розрахунок інтегрального індексу цифрової безпеки підприємства, який формується на основі агрегування часткових оцінок із урахуванням їх вагомості.

Заключний етап передбачає інтерпретацію результатів шляхом віднесення підприємства до відповідної зони цифрової безпеки (безпечної, контрольованої або критичної), що створює основу для прийняття управлінських рішень щодо необхідності поглибленої діагностики або впровадження заходів з мінімізації ризиків.

Таким чином, експрес-діагностика стану цифрової безпеки підприємства виступає ефективним інструментом оперативного оцінювання, який поєднує наукову обґрунтованість і практичну доцільність. Її застосування дозволяє забезпечити своєчасне виявлення загроз, підвищити якість управлінських рішень та сприяти зміцненню економічної безпеки підприємства в умовах цифрової трансформації. Водночас подальшого розвитку потребує формування системи показників експрес-діагностики, що забезпечить підвищення точності та універсальності її застосування.

Висновки. У результаті проведеного дослідження обґрунтовано, що цифрова безпека підприємства доцільно розглядати як інтегровану систему, яка поєднує інформаційну та кібербезпеку і забезпечує стійкість функціонування бізнес-процесів в умовах цифрової трансформації. Доведено, що зростання динамічності зовнішнього середовища, ускладнення цифрових інфраструктур та підвищення рівня кіберзагроз зумовлюють необхідність застосування оперативних інструментів оцінювання стану цифрової безпеки.

Встановлено, що традиційні методи дослідження, зокрема аналізування, оцінювання та фундаментальна діагностика, хоча й забезпечують глибоке вивчення проблематики, проте не відповідають вимогам оперативності та гнучкості управління. У цьому контексті експрес-діагностика визначена як ефективний інструмент швидкого виявлення критичних відхилень у системі цифрової безпеки підприємства, що дозволяє сформувати інформаційну основу для прийняття управлінських рішень.

У роботі розкрито сутність експрес-діагностики як різновиду управлінської діагностики, що базується на використанні обмеженої, але репрезентативної системи індикаторів, а також визначено її ключові переваги, серед яких оперативність, економічність, адаптивність і практична орієнтованість. Обґрунтовано основні вимоги до її проведення, зокрема забезпечення валідності результатів, репрезентативності показників та узгодженості із системою управління підприємством.

Запропоновано ризик-орієнтований адаптивний методичний підхід до експрес-діагностики стану цифрової безпеки підприємства, що базується на селективному відборі індикаторів, їх ваговій диференціації та інтегральному оцінюванні з урахуванням критичності загроз. Практичне значення отриманих результатів полягає у підвищенні оперативності та обґрунтованості управлінських рішень у сфері цифрової безпеки, а також своєчасній ідентифікації ризиків.

Перспективи подальших досліджень полягають у розробленні науково обґрунтованої системи показників експрес-діагностики стану цифрової безпеки підприємства, а також у вдосконаленні інструментарію її практичного застосування з урахуванням галузевої специфіки та рівня цифрової зрілості суб'єктів господарювання.

Список використаних джерел:

1. Правдивець О. Науково-практичний інструментарій оцінювання рівня цифрової трансформації, інноваційного розвитку системи економічної безпеки підприємств сфери інформаційних технологій. Вчені записки Університету «КРОК». 2023. № 3 (71). С. 92–102.

2. Лігоненко Л., Зеленько К. Оцінювання цифрової зрілості бізнес-організації: сутність та інструментарій оцінювання. Review of Transport Economics and Management. 2025. № 14 (30). С. 159–169.

3. Chepeliuk M. Digital transformation of business structures in Ukraine: the barriers and drivers. Бізнес Інформ. 2021. № 8. С. 48–53.

4. Cainelli G., D'Amato A., Mazzanti M. Resource efficient eco-innovations for a circular economy: evidence from EU firms. Research Policy. 2020. Vol. 49, No. 1. Article 103827. DOI: https://doi.org/10.1016/j.respol.2019.103827

5. Мельник О. Г. Методичні положення з експрес-діагностики загрози банкрутства підприємства. Фінанси України. 2010. № 6. С. 108–116.

6. Петряков В. Експрес-діагностика та фундаментальна діагностика в антикризовому управлінні. Економіка та суспільство. 2025. № 77. URL: https://economyandsociety.in.ua

7. Сотник А. А. Експрес-діагностика ефективності комерційної діяльності торговельних підприємств. Економічний простір. 2021. № 176. С. 89–94.

8. Загорна Т. О. Економічна діагностика : навч. посіб. Київ : Центр навчальної літератури, 2007. 400 с.

9. Литвин З. Б. Доцільність діагностики бізнес-процесів в сучасних умовах господарювання. Причорноморські економічні студії. 2017. Вип. 22. С. 205–208.

10. Тардаскіна Т. М. Методичні підходи до оцінки цифрової зрілості підприємства сфери електронних комунікацій. Актуальні питання економічних наук. 2025. № 10.

11. Передерій Т. С. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. Вісник економічної науки України. 2019. № 2 (37). С. 201–204. DOI: https://doi.org/10.37405/17297206.2019.2(37).201-204

12. Аванесова Н., Мордовцев О., Колодяжна Т. Формування механізму комплексного забезпечення цифрової безпеки промислового підприємства України. Вісник Національного технічного університету «ХПІ» (економічні науки). 2020. № 3. С. 9–14.

13. Міщенко В. І. Стратегічне управління процесами цифрової трансформації економіки. Економіка України. 2022. № 1. С. 67–81.

14. Полозова Т. В., Ткаченко А. Г., Осадчук І. О., Осадчук М. О. Механізми мінімізації ризиків економічної безпеки в процесі цифрової трансформації підприємств. Sustainable economic development: innovative approaches and strategic perspectives: collective monograph. 2025. P. 248–261. DOI: https://doi.org/10.30837/EK.2024.021

15. Ящук В. І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави. Theoretical and Applied Cybersecurity. Матеріали всеукраїнської науково-практичної конференції (TACS-2024). – Київ: Інжиніринг. 190 с. С. 119–122.

References:

1. Pravdyvets O. (2023) Naukovo-praktychnyi instrumentarii otsiniuvannia rivnia tsyfrovoi transformatsii, innovatsiinoho rozvytku systemy ekonomichnoi bezpeky pidpryiemstv sfery informatsiinykh tekhnolohii [Scientific and practical tools for assessing the level of digital transformation and innovative development of the economic security system of IT enterprises]. Vcheni zapysky Universytetu "KROK", vol. 3 (71), pp. 92–102. (in Ukrainian)

2. Lihonenko L., Zelenko K. (2025) Otsiniuvannia tsyfrovoi zrilosti biznes-orhanizatsii: sutnist ta instrumentarii otsiniuvannia [Assessment of digital maturity of a business organization: essence and evaluation tools]. Review of Transport Economics and Management, vol. 14 (30), pp. 159–169. (in Ukrainian)

3. Chepeliuk M. (2021) Digital transformation of business structures in Ukraine: the barriers and drivers. Biznes Inform, no. 8, pp. 48–53.

4. Cainelli G., D'Amato A., Mazzanti M. (2020) Resource efficient eco-innovations for a circular economy: evidence from EU firms. Research Policy, vol. 49, no. 1, article 103827. DOI: https://doi.org/10.1016/j.respol.2019.103827

5. Melnyk O. H. (2010) Metodychni polozhennia z ekspres-diahnostyky zahrozy bankrutstva pidpryiemstva [Methodological provisions for express diagnostics of enterprise bankruptcy threat]. Finansy Ukrainy, no. 6, pp. 108–116. (in Ukrainian)

6. Petriakov V. (2025) Ekspres-diahnostyka ta fundamentalna diahnostyka v antykryzovomu upravlinni [Express diagnostics and fundamental diagnostics in crisis management]. Ekonomika ta suspilstvo, no. 77. Available at: https://economyandsociety.in.ua (in Ukrainian)

7. Sotnyk A. A. (2021) Ekspres-diahnostyka efektyvnosti komertsiinoi diialnosti torhovelnykh pidpryiemstv [Express diagnostics of efficiency of commercial activity of trade enterprises]. Ekonomichnyi prostir, no. 176, pp. 89–94. (in Ukrainian)

8. Zahorna T. O. (2007) Ekonomichna diahnostyka [Economic diagnostics]. Kyiv: Tsentr navchalnoi literatury. (in Ukrainian)

9. Lytvyn Z. B. (2017) Dotsilnist diahnostyky biznes-protsesiv v suchasnykh umovakh hospodariuvannia [The expediency of business process diagnostics in modern economic conditions]. Prychornomorski ekonomichni studii, vol. 22, pp. 205–208. (in Ukrainian)

10. Tardaskina T. M. (2025) Metodychni pidkhody do otsinky tsyfrovoi zrilosti pidpryiemstva sfery elektronnykh komunikatsii [Methodological approaches to assessing digital maturity of enterprises in the field of electronic communications]. Aktualni pytannia ekonomichnykh nauk, no. 10. (in Ukrainian)

11. Perederii T. S. (2019) Stratehiia tsyfrovoi bezpeky pidpryiemstva yak draiver tsyfrovoi transformatsii ekonomiky Ukrainy [Digital security strategy of an enterprise as a driver of digital transformation of Ukraine's economy]. Visnyk ekonomichnoi nauky Ukrainy, vol. 2 (37), pp. 201–204. DOI: https://doi.org/10.37405/17297206.2019.2(37).201-204 (in Ukrainian)

12. Avanesova N., Mordovtsev O., Kolodiazhna T. (2020) Formuvannia mekhanizmu kompleksnoho zabezpechennia tsyfrovoi bezpeky promyslovoho pidpryiemstva Ukrainy [Formation of a mechanism for comprehensive provision of digital security of an industrial enterprise of Ukraine]. Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI" (ekonomichni nauky), no. 3, pp. 9–14. (in Ukrainian)

13. Mishchenko V. I. (2022) Stratehichne upravlinnia protsesamy tsyfrovoi transformatsii ekonomiky [Strategic management of digital transformation processes in the economy]. Ekonomika Ukrainy, no. 1, pp. 67–81. (in Ukrainian)

14. Polozova T. V., Tkachenko A. H., Osadchuk I. O., Osadchuk M. O. (2025) Mekhanizmy minimizatsii ryzykiv ekonomichnoi bezpeky v protsesi tsyfrovoi transformatsii pidpryiemstv [Mechanisms for minimizing risks of economic security in the process of digital transformation of enterprises]. Sustainable economic development: innovative approaches and strategic perspectives: collective monograph, pp. 248–261. DOI: https://doi.org/10.30837/EK.2024.021 (in Ukrainian)

15. Yashchuk V. I. (2024) Rol ta mistse stratehii kiberbezpeky Ukrainy u zabezpechenni informatsiinoi bezpeky derzhavy [The role and place of Ukraine's cybersecurity strategy in ensuring state information security]. Theoretical and Applied Cybersecurity: Proceedings of the All-Ukrainian Scientific and Practical Conference (TACS-2024). Kyiv: Inzhynirynh, pp. 119–122. (in Ukrainian)

Дата надходження статті: 22.04.2026
Дата прийняття статті: 13.05.2026
Дата публікації статті: 28.05.2026