

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА
ТА ПРИРОДОКОРИСТУВАННЯ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА
ТА ПРИРОДОКОРИСТУВАННЯ

Кваліфікаційна наукова праця на правах рукопису

РОЗДОПЧЕНЮК ВАСИЛЬ МИКОЛАЙОВИЧ

УДК 005.334:658.1:004

ДИСЕРТАЦІЯ
ОЦІНКА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ
ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ

Спеціальність 051 – Економіка

Галузь знань 05 – Соціальні та поведінкові науки

Подается на здобуття наукового ступеня доктора філософії в галузі

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.



В. М. Роздопченко

Науковий керівник:

ОСАДЧА Ольга Олексіївна

доктор економічних наук, професор

Рівне – 2026

АНОТАЦІЯ

Роздопченюк В. М. Оцінка економічної безпеки підприємства в умовах цифрової трансформації економіки України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 051 «Економіка». – Національний університет водного господарства та природокористування Міністерства освіти і науки України, Рівне, 2026.

Роботу виконано в Національному університеті водного господарства та природокористування Міністерства освіти і науки України, у якому і відбудеться захист.

У дисертації здійснено теоретичне обґрунтування та розроблено методичні підходи і практичні рекомендації щодо оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки.

У першому розділі «Теоретичні та методичні аспекти оцінювання економічної безпеки підприємства в контексті цифрових змін в економіці України» досліджено еволюцію наукових підходів до трактування економічної безпеки підприємства та обґрунтовано перехід від захисно-стабілізаційної до стратегічно-розвиткової парадигми її розуміння. Визначено, що економічна безпека підприємства формується як результат взаємодії фінансових, організаційних, інформаційних і технологічних чинників, а цифровізація змінює природу ризиків, критерії стійкості та параметри управлінських рішень.

Систематизовано ризики економічної безпеки підприємства з урахуванням цифровізації, що дозволило виокремити зовнішні, зокрема політичні, воєнні, соціально-економічні й глобальні, та внутрішні, зокрема правові, організаційні, структурні й індивідуальні ризики. Розкрито взаємозв'язок між ризиками та параметрами стійкості підприємства. Сформовано типологію стійкості, що охоплює економічну, технічну, цифрову,

енергоефективну й інноваційну складові та дозволяє інтерпретувати економічну безпеку як здатність підприємства забезпечувати стабільність і розвиток у змінному середовищі.

Визначено, що поєднання показників ефективності та ризику забезпечує оцінювання результативності діяльності з урахуванням ризиків і формує основу ризик-орієнтованого управління. Систематизовано міжнародні підходи до ризик-орієнтованого управління, зокрема ISO 31000, COSO ERM, NIST CSF, та сформовано засади інтеграції ризик-орієнтованої моделі управління у систему стратегічного планування підприємства. Запропоновано концептуальну модель економічної безпеки підприємства в умовах цифрової трансформації, у якій відображено взаємозв'язок між цифровими ризиками, параметрами стійкості, управлінськими рішеннями та показниками ефективності і ризику.

Удосконалено методичні підходи до формування системи цифрового моніторингу, що передбачає інтеграцію принципів оцінювання, системи показників результативності та ризику з цифровими технологіями аналітичної обробки даних. Визначено, що оцінювання економічної безпеки в умовах цифрової трансформації має здійснюватися з урахуванням взаємозв'язку результативності діяльності підприємства та рівня ризиків його функціонування. Розкрито принципи оцінювання економічної безпеки та уточнено логіку формування системи показників.

Встановлено, що традиційний індикаторний підхід потребує доповнення показниками, які відображають ризикогенність і адаптивність діяльності підприємства. Визначено роль цифрових технологій у системі оцінювання та моніторингу економічної безпеки. Обґрунтовано, що використання цифрових платформ і аналітичних систем забезпечує оперативне виявлення відхилень та підвищує обґрунтованість управлінських рішень.

Розкрито вплив цифрової трансформації на бізнес-процеси та архітектуру управління підприємством. Визначено, що цифровізація змінює організацію діяльності, посилює роль цифрових платформ і підвищує

залежність від інформаційних технологій, що зумовлює трансформацію підходів до забезпечення економічної безпеки. Систематизовано технологічні ризики цифрової трансформації, зокрема кіберризики, регуляторні обмеження та ризики платформної залежності, і визначено потребу у формуванні адекватних механізмів управлінського реагування. Сформовано підхід до інтеграції ключових показників ефективності та ключових індикаторів ризику у систему моніторингу економічної безпеки підприємства.

У другому розділі *«Дослідження економічної безпеки підприємств в умовах цифровізації: ризики та управління»* узагальнено існуючі підходи до оцінювання економічної безпеки підприємств, що дозволило розвинути функціонально-ресурсний підхід до її діагностики. Такий підхід передбачає структурування складових економічної безпеки за ключовими напрямками функціонування та відповідними ресурсними елементами, забезпечує взаємозв'язок між її складовими й дозволяє перейти від ізольованого аналізу окремих показників до комплексної оцінки їх взаємодії. Виокремлено складові економічної безпеки підприємства та сформовано систему індикаторів для їх діагностики, що дає змогу відобразити поточний стан функціонування підприємства й потенційні відхилення у його розвитку. Визначено, що запропонована система індикаторів забезпечує узгоджене оцінювання результативності діяльності та рівня ризиків, підвищуючи аналітичну обґрунтованість діагностичних висновків. Застосовано кейс-аналіз як інструмент апробації функціонально-ресурсного підходу, що підтвердило його практичну доцільність і дозволило виявити вплив окремих складових та показників на загальний рівень економічної безпеки.

Визначено, що цифровізація виступає системоутворюючим чинником трансформації економічної безпеки підприємств, оскільки змінює характер бізнес-процесів, структуру створення вартості та умови функціонування, одночасно генеруючи нові види загроз. Обґрунтовано, що ризики в цифровому середовищі формуються як результат взаємодії технологічних, регуляторних і платформних чинників. Набули подальшого розвитку положення щодо

систематизації цифрових ризиків економічної безпеки підприємств шляхом їх структуризації на взаємопов'язані групи, що охоплюють кіберризики, регуляторні ризики та ризики залежності від цифрових платформ. Розкрито механізми впливу цифрових ризиків на бізнес-процеси підприємства, що проявляються у зростанні вразливості інформаційних систем, ускладненні регуляторного середовища та посиленні залежності від цифрової інфраструктури. Встановлено кореляцію цифрових ризиків із ключовими показниками ефективності та ключовими індикаторами ризику підприємства, що забезпечує узгодження результативності з рівнем ризиків, підвищує чутливість моніторингу до критичних відхилень і формує основу для управлінських рішень.

Дослідження міжнародних практик цифрового ризик-менеджменту дозволило встановити, що їх ефективність ґрунтується на інтеграції управління ризиками у стратегічне та фінансове управління підприємством і використанні стандартизованих рамок моніторингу цифрової стійкості. Визначено, що міжнародні підходи поєднують технічні й економічні інструменти, орієнтуючись на зниження економічних втрат і підвищення стійкості підприємств. Набули подальшого розвитку науково-прикладні засади адаптації міжнародних практик цифрового ризик-менеджменту до умов національної економіки, що передбачає їх систематизацію за напрямками застосування, урахування інституційних і технологічних обмежень та інтеграцію інструментів міжнародних стандартів у систему управління економічною безпекою підприємств. Встановлено доцільність використання індикаторів цифрової стійкості, витрат на безпеку, часу відновлення та рівня зрілості систем управління ризиками. Обґрунтовано, що адаптація міжнародних практик має враховувати інституційні обмеження, рівень гармонізації законодавства та кадрове забезпечення, а їх інтеграція формує основу ризик-орієнтованого управління економічною безпекою, підвищує адаптивність підприємств і узгоджує національні підходи з європейськими вимогами.

У третьому розділі «Методика інтегрального оцінювання, діагностики та прогнозування економічної безпеки підприємств в умовах цифрової трансформації економіки України» удосконалено методику інтегрального оцінювання економічної безпеки підприємств, що передбачає формування системи показників із визначенням їх економічного змісту, розрахункових залежностей і джерел інформаційного забезпечення. Встановлено, що за відсутності у фінансовій звітності прямих кількісних індикаторів цифрової трансформації оцінювання доцільно здійснювати на основі взаємопов'язаних показників, які опосередковано відображають вплив цифрових змін на фінансовий стан, інвестиційну активність і здатність підприємства до розвитку. Сформовано порядок побудови інтегрального індексу на основі нормалізації показників методом мін–макс, їх зважування за ентропійним методом та агрегування, що забезпечує зіставність показників, зменшує суб'єктивність визначення ваг і підвищує об'єктивність інтегральної оцінки. Обґрунтовано використання інтерпретаційної шкали інтегрального індексу в межах $[0;1]$, що дозволяє класифікувати рівні економічної безпеки та формує основу для аналітичної діагностики, міжгалузевого порівняння і прогнозування.

Обґрунтовано можливість використання інтегрального підходу для аналітичної діагностики економічної безпеки підприємств, що забезпечує перехід від оцінювання окремих показників до комплексного вимірювання її рівня у динаміці та за видами економічної діяльності. Зіставність результатів досягнуто шляхом уніфікації фінансових даних, їх нормалізації та приведення до єдиної аналітичної бази, що дозволило здійснити міжчасове та міжпідприємницьке порівняння за 2020–2024 рр. На основі розрахунку інтегрального індексу для сформованої вибірки підприємств, зокрема ПАТ «НЕК «Укренерго», ТОВ «ГПК «Нафтогаз України», АТ «Українська залізниця», АТ «Укрпошта», INTERPIPE HOLDINGS PLC, проведено порівняльну аналітичну діагностику, що дозволило виявити диференціацію рівнів економічної безпеки та відмінності у структурі її формування. Отримані

результати засвідчують нерівномірність адаптації підприємств до умов цифрової трансформації, що проявляється у варіативності значень інтегрального показника та зміні його динаміки. Застосування інтегрального підходу в поєднанні з аналізом функціональних складових дозволило ідентифікувати внутрішні чинники формування економічної безпеки, здійснити порівняльне ранжування підприємств і сформувати аналітичну основу для економетричного моделювання та прогнозування.

Використання панельного економетричного моделювання дозволило оцінити взаємозв'язок між інтегральним рівнем економічної безпеки підприємств і системою визначальних факторів з урахуванням часової динаміки та індивідуальних особливостей підприємств. Побудовано панельну економетричну модель залежності інтегрального показника від сукупності факторів та обґрунтовано вибір її специфікації на основі статистичних критеріїв. Оцінювання параметрів моделі забезпечило кількісну ідентифікацію впливу ключових факторів і їх значущості у формуванні динаміки інтегрального показника. На основі моделі здійснено прогнозування інтегрального рівня економічної безпеки та оцінено можливі траєкторії його зміни. Сценарний аналіз у межах базового, оптимістичного та песимістичного сценаріїв дозволив визначити діапазон коливань показника й формалізувати вплив змін середовища. Поєднання економетричного моделювання та сценарного підходу підвищує обґрунтованість прогнозних оцінок і формує основу для прийняття управлінських рішень щодо зміцнення економічної безпеки підприємств.

Ключові слова: економічна безпека; цифрова трансформація; цифрові ризики; бізнес-процеси; система показників; інтегральний індекс; аналітична діагностика; ризик-орієнтоване управління; фінансова звітність.

SUMMARY

Rozdopcheniuk V. M. Assessment of Enterprise Economic Security under the Conditions of Digital Transformation of the Economy of Ukraine. – Qualifying scientific work as a manuscript.

Thesis for the degree of Doctor of Philosophy in specialty 051 «Economics».
– National University of Water and Environmental Engineering of the Ministry of Education and Science of Ukraine, Rivne, 2026.

The research was conducted at the National University of Water and Environmental Engineering of the Ministry of Education and Science of Ukraine, where the defense will also take place.

The dissertation provides a theoretical substantiation and develops methodological approaches and practical recommendations for assessing enterprise economic security under the conditions of the digital transformation of the economy.

In the first chapter, “Theoretical and Methodological Aspects of Assessing Enterprise Economic Security in the Context of Digital Changes in Ukraine’s Economy”, the evolution of scientific approaches to the interpretation of enterprise economic security is examined, and the transition from a protective and stabilizing paradigm to a strategic and development-oriented paradigm of its understanding is substantiated. It is determined that enterprise economic security is formed as a result of the interaction of financial, organizational, informational, and technological factors, while digitalization changes the nature of risks, the criteria of resilience, and the parameters of managerial decision-making.

The risks of enterprise economic security are systematized with due regard to digitalization, which made it possible to distinguish external risks, including political, military, socio-economic, and global risks, as well as internal risks, including legal, organizational, structural, and individual risks. The relationship between risks and the parameters of enterprise resilience is revealed. A typology of resilience is developed, covering economic, technical, digital, energy-efficiency, and innovation components, which allows enterprise economic security to be interpreted

as the ability of an enterprise to ensure stability and development in a changing environment.

It is determined that the combination of performance and risk indicators enables the assessment of business performance with due regard to risks and forms the basis for risk-oriented management. International approaches to risk-oriented management are systematized, in particular ISO 31000, COSO ERM, and NIST CSF, and the foundations for integrating a risk-oriented management model into the enterprise strategic planning system are formulated. A conceptual model of enterprise economic security under the conditions of digital transformation is proposed, reflecting the relationship between digital risks, resilience parameters, managerial decisions, and performance and risk indicators.

Methodological approaches to the formation of a digital monitoring system are improved, which involves the integration of assessment principles, a system of performance and risk indicators, and digital technologies for analytical data processing. It is determined that the assessment of economic security under the conditions of digital transformation should be carried out with regard to the relationship between enterprise performance and the level of risks associated with its functioning. The principles of assessing economic security are disclosed, and the logic of forming a system of indicators is clarified.

It is established that the traditional indicator-based approach needs to be supplemented with indicators that reflect the risk-generating nature and adaptability of enterprise activity. The role of digital technologies in the system of assessment and monitoring of economic security is determined. It is substantiated that the use of digital platforms and analytical systems ensures the prompt detection of deviations and increases the validity of managerial decisions.

The impact of digital transformation on business processes and the architectonics of enterprise management is revealed. It is determined that digitalization changes the organization of activity, strengthens the role of digital platforms, and increases dependence on information technologies, which necessitates the transformation of approaches to ensuring economic security.

Technological risks of digital transformation are systematized, in particular cyber risks, regulatory constraints, and risks of platform dependence, and the need to form adequate mechanisms of managerial response is determined. An approach to integrating key performance indicators and key risk indicators into the enterprise economic security monitoring system is developed.

In the second chapter, “Research on Enterprise Economic Security under the Conditions of Digitalization: Risks and Management”, existing approaches to assessing enterprise economic security are generalized, which made it possible to develop a functional-resource approach to its diagnostics. This approach provides for the structuring of economic security components according to key areas of functioning and relevant resource elements, ensures the interconnection between its components, and makes it possible to move from an isolated analysis of individual indicators to a comprehensive assessment of their interaction. The components of enterprise economic security are identified, and a system of indicators for their diagnostics is formed, which makes it possible to reflect both the current state of enterprise functioning and potential deviations in its development. It is determined that the proposed system of indicators ensures a coordinated assessment of business performance and the level of risks, thereby increasing the analytical validity of diagnostic conclusions. Case analysis is applied as a tool for testing the functional-resource approach, which confirmed its practical feasibility and made it possible to identify the influence of individual components and indicators on the overall level of economic security.

It is determined that digitalization acts as a system-forming factor in the transformation of enterprise economic security, since it changes the nature of business processes, the structure of value creation, and the conditions of functioning, while simultaneously generating new types of threats. It is substantiated that risks in the digital environment are formed as a result of the interaction of technological, regulatory, and platform-related factors. The provisions on the systematization of digital risks to enterprise economic security are further developed through their structuring into interrelated groups, covering cyber risks, regulatory risks, and risks

of dependence on digital platforms. The mechanisms of the impact of digital risks on enterprise business processes are revealed, manifested in the growing vulnerability of information systems, the increasing complexity of the regulatory environment, and the strengthening of dependence on digital infrastructure. The correlation between digital risks and key performance indicators and key risk indicators of the enterprise is established, which ensures the alignment of performance with the level of risks, increases the sensitivity of monitoring to critical deviations, and forms a basis for managerial decisions.

The study of international practices of digital risk management made it possible to establish that their effectiveness is based on the integration of risk management into the strategic and financial management of an enterprise and on the use of standardized frameworks for monitoring digital resilience. It is determined that international approaches combine technical and economic instruments, focusing on reducing economic losses and increasing enterprise resilience. The scientific and applied foundations for adapting international practices of digital risk management to the conditions of the national economy are further developed, which involves their systematization by areas of application, taking into account institutional and technological constraints, and integrating instruments of international standards into the system of enterprise economic security management. The expediency of using indicators of digital resilience, security costs, recovery time, and the maturity level of risk management systems is established. It is substantiated that the adaptation of international practices should take into account institutional constraints, the level of legislative harmonization, and human resource capacity, while their integration forms the basis of risk-oriented economic security management, increases enterprise adaptability, and aligns national approaches with European requirements.

In the third chapter, “Methodology of Integral Assessment, Diagnostics, and Forecasting of Enterprise Economic Security under the Conditions of Digital Transformation of Ukraine’s Economy”, the methodology of integral assessment of enterprise economic security is improved, which provides for the formation of a system of indicators with the definition of their economic content, calculation

dependencies, and sources of information support. It is established that, in the absence of direct quantitative indicators of digital transformation in financial statements, the assessment should be carried out on the basis of interrelated indicators that indirectly reflect the impact of digital changes on the financial condition, investment activity, and development capacity of an enterprise. The procedure for constructing an integral index based on the min–max normalization of indicators, their weighting by the entropy method, and subsequent aggregation is developed, which ensures the comparability of indicators, reduces subjectivity in determining weights, and increases the objectivity of the integral assessment. The use of an interpretative scale of the integral index within the interval $[0;1]$ is substantiated, which makes it possible to classify levels of economic security and forms the basis for analytical diagnostics, intersectoral comparison, and forecasting.

The possibility of using the integral approach for analytical diagnostics of enterprise economic security is substantiated, which ensures the transition from the assessment of individual indicators to the comprehensive measurement of its level over time and by types of economic activity. The comparability of results is achieved through the unification of financial data, their normalization, and their transformation into a single analytical base, which made it possible to conduct intertemporal and inter-enterprise comparisons for 2020–2024. Based on the calculation of the integral index for the selected sample of enterprises, in particular PJSC “NEC Ukrenergo”, LLC “GPK Naftogaz of Ukraine”, JSC “Ukrainian Railways”, JSC “Ukrposhta”, and INTERPIPE HOLDINGS PLC, a comparative analytical diagnosis was carried out, which made it possible to identify differentiation in the levels of economic security and differences in the structure of its formation. The obtained results indicate the uneven adaptation of enterprises to the conditions of digital transformation, which is manifested in the variability of the integral indicator values and changes in its dynamics. The application of the integral approach in combination with the analysis of functional components made it possible to identify internal factors in the formation of economic security, rank

enterprises comparatively, and form an analytical basis for econometric modeling and forecasting.

The use of panel econometric modeling made it possible to assess the relationship between the integral level of enterprise economic security and a system of determining factors, taking into account temporal dynamics and the individual characteristics of enterprises. A panel econometric model of the dependence of the integral indicator on a set of factors is constructed, and the choice of its specification is substantiated on the basis of statistical criteria. The estimation of model parameters ensured the quantitative identification of the influence of key factors and their significance in shaping the dynamics of the integral indicator. On the basis of the model, the integral level of economic security was forecast, and possible trajectories of its change were assessed. Scenario analysis within the basic, optimistic, and pessimistic scenarios made it possible to determine the range of fluctuations of the indicator and to formalize the impact of environmental changes. The combination of econometric modeling and the scenario approach increases the validity of forecast estimates and forms the basis for making managerial decisions aimed at strengthening the economic security of enterprises.

Keywords: economic security; digital transformation; digital risks; business processes; system of indicators; integral index; analytical diagnostics; risk-oriented management; financial statements.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті в періодичних наукових виданнях, проіндексованих у базі даних «Scopus»:

1. Osadcha O., Levytska S., Zinkevych O., Rozdopcheniuk V. and Didukh R. Formation of a resilient economy through the integration of digital risk management and “green” modernization of enterprises. *5th International Conference on Environmental Sustainability in Natural Resources Management (ISCES 2025). IOP Conf. Ser.: Earth Environ. Sci.* Volume 1576, 012002. DOI 10.1088/1755-1315/1576/1/012002 (особистий внесок здобувача – систематизовано ризики економічної безпеки підприємств з урахуванням цифрових та екологічних чинників, обґрунтовано інтеграцію індикаторів KPI/KRI у контексті «twin transition» та визначено підхід до оцінювання цифрово-екологічної стійкості підприємств; 0,8 / 0,16 ум. д.а.)

Статті у наукових фахових виданнях України:

1. Осадча О. О., Роздопченко В. М. Оцінювання показників інноваційної діяльності підприємства та їх використання в системі управління економічною безпекою. *Вісник Національного університету водного господарства та природокористування. Сер. «Економічні науки»*, 2023. Випуск 2. С. 152-160. URL: <https://visnyk.nuwm.edu.ua/index.php/econ/article/view/1380> (особистий внесок здобувача – систематизовано та узагальнено показники інноваційної діяльності підприємства, обґрунтовано критерії їх відбору та визначено їх роль у формуванні інформаційної бази управління економічною безпекою; 0,6 / 0,3 ум. д.а.).

2. Осадча О. О., Роздопченко В. М. Ризики економічної безпеки підприємства в умовах цифровізації. *Вісник Національного університету*

водного господарства та природо-користування. Сер. «Економічні науки», 2024. Вип. 3(107). С. 116-126. URL: <https://visnyk.nuwm.edu.ua/index.php/econ/article/view/1555> (особистий внесок здобувача – систематизовано та класифіковано ризики економічної безпеки підприємства в умовах цифровізації, обґрунтовано їх ранжування та визначено підхід до групування за типами стійкості підприємства; 0,7 / 0,35 ум. д.а.).

3. Осадча О. О., Роздопченко В. М. Цифровізація бізнес-процесів підприємства як інструмент економічної безпеки. *Вісник Національного університету водного господарства та природокористування. Сер. «Економічні науки»*, 2025. Вип. 1(109). С. 136-148. URL: <https://visnyk.nuwm.edu.ua/index.php/econ/article/view/1625> (особистий внесок здобувача – обґрунтовано роль цифровізації бізнес-процесів підприємства як інструменту забезпечення економічної безпеки, систематизовано напрями цифрової трансформації та розроблено організаційну модель цифровізації бізнес-процесів; 0,8 / 0,4 ум. д.а.).

4. Роздопченко В. М. Синергія ключових індикаторів ефективності та ризику у забезпеченні стійкості підприємств до цифрових викликів. *Міжнародний науковий журнал «Грааль науки»*. № 55 (серпень, 2025). С. 186–192. URL: <https://archive.journal-grail.science/index.php/2710-3056/article/view/2907> (0,4 ум. д.а.).

5. Роздопченко В. М. Методичні підходи до оцінювання економічної безпеки підприємств у цифровій економіці. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*, 2025. Випуск №: 2 (72). С. 77–87. URL: <http://efm.vsau.org/en/particles/methodological-approaches-to-the-assessment-of-enterprises-economic-security-in-the-digital-economy> (0,8 ум. д.а.).

6. Осадча О. О., Роздопченко В. М. Інтегральне оцінювання економічної безпеки підприємств в умовах цифрової трансформації економіки. *Грааль науки : міжнародний науковий журнал*. 2026. № 64 (березень). С. 260–267. DOI 10.36074/grail-of-science.20.03.2026.027 (особистий внесок здобувача

– обґрунтовано методичний підхід до інтегрального оцінювання економічної безпеки підприємств, сформовано систему показників та визначено процедуру їх нормалізації і агрегування в умовах цифрової трансформації; 0,5 / 0,25 ум. д.а.).

Праці апробаційного характеру:

1. Роздопченюк В. М. Аналіз показників інноваційної діяльності підприємства. *Проблеми та перспективи розвитку сучасної науки : збірник тез доповідей Міжнародної науково-практичної конференції молодих науковців, аспірантів і здобувачів вищої освіти*, м. Рівне, 11–12 травня 2023 року. Рівне : НУВГП, 2023. С. 373–376 (0,2 ум. д.а.).

2. Осадча О. О., Роздопченюк В. М. Система управління ризиками як інструмент економічної безпеки підприємства в умовах цифровізації. *Комплексний підхід до модернізації науки: методи, моделі та мультидисциплінарність: матеріали III Міжнародної наукової конференції*, м. Житомир, 18 серпня 2023 р. / Міжнародний центр наукових досліджень. Вінниця: Європейська наукова платформа, 2023. С. 50–52 (особистий внесок здобувача – систематизовано ризики діяльності підприємства в умовах цифровізації, обґрунтовано роль ризик-менеджменту у забезпеченні економічної безпеки та розроблено алгоритм і структурну модель системи управління ризиками підприємства; 0,2 / 0,1 ум. д.а.).

3. Роздопченюк В. М. Фактори економічної безпеки підприємства. *Modernization of science and its influence on global processes: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference*, September 20, 2024. Bern, Swiss Confederation: International Center of Scientific Research. DOI 10.36074/scientia-20.09.2024. С. 52–54 (0,15 ум. д.а.).

4. Осадча О.О., Роздопченюк В. М. Забезпечення економічної безпеки через цифрову трансформацію підприємства. *Наукові тренди*

постіндустріального суспільства: збірник наукових праць з матеріалами IX Міжнародної наукової конференції, м. Тернопіль, 21 березня, 2025 р. / Міжнародний центр наукових досліджень. Вінниця: ТОВ «УКРЛОГОС Груп, 2025. С. 71–74 (особистий внесок здобувача – обґрунтовано роль цифрової трансформації у забезпеченні економічної безпеки підприємства, систематизовано напрями цифровізації бізнес-процесів та визначено їх вплив на підвищення стійкості та ефективності діяльності підприємства; 0,3 / 0,15 ум. д.а.).

5. Роздопченюк В. М. Цифрова трансформація бізнес-процесів як детермінанта економічної безпеки підприємства в умовах цифровізації економіки України. *Актуальні проблеми теорії і практики менеджменту в контексті євроінтеграції: Збірник матеріалів XIV Міжнародної науково-практичної конференції, 22 травня 2025 р. Рівне : НУВГП, 2025. С. 707–709 (0,15 ум. д.а.).*

6. Роздопченюк В. М. Інтеграція цифрових платформ у систему управління підприємством як чинник зміцнення його економічної безпеки. *Інтелектуальний ресурс сьогодення: наукові задачі, розвиток та запитання: збірник наукових праць з матеріалами V Міжнародної наукової конференції, м. Чернівці, 29 серпня, 2025 р. / Міжнародний центр наукових досліджень. — Вінниця: ТОВ «УКРЛОГОС Груп, 2025. С. 28–30 (0,25 ум. д.а.).*

7. Роздопченюк В. М., Хахльов О. В. Цифрові ризики та стійкість підприємства як складові економічної безпеки України. Детермінанти соціально-економічного відновлення держави, регіонів та суб'єктів господарювання: збірник тез доповідей III Міжнародної науково-практичної конференції, присвяченої 50-річчю Навчально-наукового інституту економіки та менеджменту, м. Рівне, 14 листопада 2025 року. Рівне : НУВГП, 2025. С. 215–218 (особистий внесок здобувача – систематизовано цифрові ризики підприємства у розрізі складових його стійкості, визначено ключові показники ефективності та обґрунтовано взаємозв'язок між ризиками і параметрами економічної безпеки; 0,3 / 0,15 ум. д.а.).

8. Роздопченюк В. М. Економічні наслідки цифровізації: трансформація ризиків і показників ефективності підприємства. *Сучасні виклики сталого розвитку бізнесу: тези виступів VI Міжнар. наук.-практ. конф.* Житомир: Житомирська політехніка, 2025. С. 205–206 (0,15 ум. д.а.).

9. Осадча О., Роздопченюк В. Формування системи показників оцінювання економічної безпеки підприємства в умовах цифрової трансформації. *New paradigms of interdisciplinary research: theories, ideas and developments : proceedings of the 19th International scientific and practical conference*, Prague, Czech Republic, May 12–15, 2026. Prague : International Science Group, 2026. С. 101–104 (особистий внесок здобувача – обґрунтовано систему показників оцінювання економічної безпеки підприємства на основі фінансових індикаторів; визначено їх роль у подальшому розрахунку інтегрального індексу економічної безпеки підприємства; 0,4 / 0,2 ум. д.а.).

ЗМІСТ

ВСТУП.....	21
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ АСПЕКТИ ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВИХ ЗМІН В ЕКОНОМІЦІ УКРАЇНИ	30
1.1. Теоретичні засади економічної безпеки підприємства в умовах цифрової трансформації	30
1.2. Система індикаторів та цифровий моніторинг економічної безпеки підприємства.....	61
1.3. Трансформація системи економічної безпеки підприємства під впливом цифровізації.....	81
Висновки до розділу 1.....	99
РОЗДІЛ 2. ДОСЛІДЖЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ: РИЗИКИ ТА УПРАВЛІННЯ	102
2.1. Аналіз середовища формування економічної безпеки підприємств на основі комплексної системи показників	102
2.2. Цифрові фактори та ризики економічної безпеки підприємств.....	124
2.3. Міжнародні практики цифрового ризик-менеджменту та їх адаптація в національній економіці	142
Висновки до розділу 2.....	174
РОЗДІЛ 3. МЕТОДИКА ІНТЕГРАЛЬНОГО ОЦІНЮВАННЯ, ДІАГНОСТИКИ ТА ПРОГНОЗУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ	179
3.1. Методика формування інтегрального індексу економічної безпеки підприємств	179
3.2. Аналітична діагностика та порівняльна оцінка економічної безпеки підприємств на основі інтегрального підходу	193

3.3. Економетричне моделювання, прогнозування та сценарний аналіз інтегрального рівня економічної безпеки підприємств.....	220
Висновки до розділу 3.....	245
ВИСНОВКИ	249
ДОДАТКИ.....	280

ВСТУП

Актуальність теми дослідження. Сучасний етап розвитку економіки України характеризується глибокими структурними змінами, зумовленими цифровізацією господарських процесів, посиленням глобальної конкуренції, нестабільністю зовнішнього середовища та воєнними викликами. За таких умов особливої ваги набуває проблема забезпечення економічної безпеки підприємства як необхідної передумови його стабільного функціонування, збереження конкурентних позицій, фінансової стійкості та здатності до адаптації в умовах зростаючої невизначеності. Саме на рівні підприємства концентрується практичний вплив більшості сучасних економічних, технологічних та інституційних трансформацій, що обумовлює потребу в оновленні наукових підходів до оцінювання економічної безпеки.

Цифрова трансформація економіки, що супроводжується впровадженням інформаційно-комунікаційних технологій, автоматизацією бізнес-процесів, розвитком цифрових платформ та систем управління на основі даних, з одного боку, відкриває нові можливості для підвищення ефективності діяльності підприємств, а з іншого - формує нові джерела ризику. Йдеться про зростання кіберзагроз, посилення залежності від цифрової інфраструктури, ускладнення захисту інформаційних ресурсів, підвищення вимог до цифрових компетентностей персоналу та зростання вразливості управлінських систем до технологічних збоїв. За даними урядової команди реагування на комп'ютерні надзвичайні події, у 2024 році в Україні було опрацьовано 4315 кіберінцидентів, що на 69,8 % більше, ніж у 2023 році [30], а це підтверджує істотне посилення цифрових загроз для функціонування суб'єктів господарювання.

За цих обставин традиційні підходи до трактування економічної безпеки підприємства як переважно стану захищеності ресурсів і результатів діяльності вже не повною мірою відповідають сучасним умовам господарювання. Цифровізація змінює не лише інструменти ведення бізнесу, а

й саму природу ризиків, критерії стійкості та параметри управлінських рішень. Це зумовлює необхідність переосмислення теоретико-методологічних засад оцінювання економічної безпеки підприємства, розроблення адекватного аналітичного інструментарію та формування підходів, які дають змогу врахувати взаємодію фінансових, організаційних, інформаційних і технологічних чинників у межах єдиної системи оцінювання.

Значний внесок у дослідження проблематики економічної безпеки, формування її категорійного апарату, а також розроблення теоретичних і методичних підходів до її оцінювання здійснили такі вітчизняні та зарубіжні вчені, як: Д. Грицишен, Н. Савіна, Н. Ковшун, О. Дем'янчук, В. Андрійчук, К. Лопатка, О. Павелко, Ю. Шаранова, О. Солодовнік, В. Калинюк, Т. Цвігун, А. Ковальчук, К. Жадько, Д. Самойленко, О. Паршина, Ю. Паршин, Ю. Савченко, а також зарубіжні дослідники, зокрема Р. Каплан, Д. Нортон, М. Кросіньяні, М. Маккіавеллі, А. Сілва, Г. Латтанціо.

Окремі аспекти ризик-орієнтованого управління, цифровізації бізнес-процесів та її впливу на економічну безпеку підприємств висвітлені у працях О. Воскобоевої, О. Ромащенко, А. Макаренка, С. Пілецької, Т. Коритько, Є. Ткаченка, Т. Ткаченко, А. Гречко, О. Чумаченко, О. Нескородько та інших учених, які обґрунтовують необхідність інтеграції сучасних інструментів управління ризиками, показників ефективності та аналітичних моделей у систему забезпечення стійкого функціонування підприємств.

Аналіз наукових праць свідчить, що проблематика економічної безпеки підприємства є достатньо розробленою у вітчизняній і зарубіжній науковій літературі. Водночас більшість досліджень зосереджена на традиційних підходах до її оцінювання, що сформувалися в умовах індустріальної економіки, тоді як специфіка функціонування підприємств у цифровому середовищі залишається недостатньо врахованою. Недостатньо опрацьованими є питання комплексного оцінювання економічної безпеки підприємства з урахуванням цифрових чинників, інтеграції показників

ефективності та ризику, а також використання економетричних методів для моделювання та прогнозування її рівня.

Отже, необхідність поглиблення теоретичних положень, удосконалення методичних підходів та розроблення прикладного інструментарію оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки України зумовлює актуальність теми дисертаційного дослідження, визначає його наукову новизну та практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано відповідно до плану науково-дослідних робіт Національного університету водного господарства та природокористування.

Результати дослідження пов'язані з виконанням науково-дослідної теми «Розвиток потенціалу регіону: економічні чинники та ресурсні передумови» (номер державної реєстрації 0121U111063, 2021–2025 рр.), у межах якої досліджено роль економічної безпеки підприємств у формуванні економічного потенціалу в умовах цифровізації.

У межах теми «Актуальні проблеми обліково-аналітичного забезпечення управління в умовах цифрової трансформації» (номер державної реєстрації 0121U113751, 2021–2024 рр.) обґрунтовано теоретичні та прикладні аспекти оцінювання економічної безпеки підприємств, зокрема формування системи показників та інформаційно-аналітичного забезпечення.

Результати дослідження також узгоджуються з темою «Бухгалтерський облік, оподаткування, аналіз та аудит в умовах воєнного стану та повоєнного відновлення України» (номер державної реєстрації 0124U004773, 2024–2027 рр.), у межах якої проаналізовано вплив воєнних чинників на економічну безпеку підприємств та обґрунтовано необхідність удосконалення підходів до її оцінювання в умовах підвищених ризиків.

Мета і завдання дослідження. Мета дослідження полягає у теоретичному обґрунтуванні та розробленні методичних підходів і практичних рекомендацій щодо оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки України.

Для досягнення мети дослідження поставлено такі завдання:

- запропонувати концептуальну модель економічної безпеки підприємства в умовах цифрової трансформації економіки;
- удосконалити методичні підходи до оцінювання та цифрового моніторингу економічної безпеки підприємства;
- розвинути функціонально-ресурсний підхід до діагностики економічної безпеки підприємств;
- систематизувати цифрові ризики економічної безпеки підприємств;
- дослідити міжнародні практики цифрового ризик-менеджменту та визначити можливості їх адаптації в національній економіці;
- удосконалити методику інтегрального оцінювання економічної безпеки підприємств;
- поглибити аналітичну діагностику та порівняльну оцінку економічної безпеки підприємств на основі інтегрального підходу;
- розвинути методичні засади прогнозування та сценарного аналізу інтегрального рівня економічної безпеки підприємств на основі економетричного моделювання.

Об’єктом дослідження є процес забезпечення економічної безпеки підприємства в умовах цифрової трансформації економіки України.

Предметом дослідження є сукупність теоретичних, методичних і прикладних положень оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки України.

Методи дослідження. У дисертаційній роботі використано сукупність загальнонаукових і спеціальних методів дослідження, що забезпечило розв’язання поставлених завдань та досягнення мети дослідження. Діалектичний і гносеологічний методи застосовано для поглиблення теоретичних засад економічної безпеки підприємства та уточнення її змісту в умовах цифрової трансформації економіки (підр. 1.1). Історичний метод використано для дослідження еволюції підходів до трактування поняття економічної безпеки (підр. 1.1). Методи аналізу, синтезу, індукції, дедукції,

порівняння та узагальнення застосовано при дослідженні методичних підходів до оцінювання економічної безпеки підприємства та узагальненні наукових підходів до її забезпечення (підр. 1.2, 2.3). Системний підхід використано для дослідження впливу цифрової трансформації на бізнес-процеси та систему економічної безпеки підприємства, а також обґрунтування взаємозв'язку її складових (підр. 1.3, 3.1). Методи групування, класифікації, порівняльного та коефіцієнтного аналізу застосовано для систематизації ризиків економічної безпеки підприємства та діагностики її рівня (підр. 2.1, 2.2). Методи економіко-статистичного аналізу, нормалізації, інтегрального оцінювання та графічного подання даних використано для оцінювання рівня економічної безпеки підприємств і проведення міжгалузевого порівняння (підр. 3.2). Економетричні методи, зокрема панельне моделювання, застосовано для оцінювання впливу факторів на інтегральний рівень економічної безпеки підприємств та його прогнозування (підр. 3.3).

Інформаційною базою дослідження є законодавчі та нормативно-правові акти України, офіційні матеріали органів державної влади і регулювання, зокрема Державної служби статистики України, Національного банку України, Ради національної безпеки і оборони України, а також нормативні документи і аналітичні матеріали Європейського Союзу та міжнародних організацій, зокрема Організації економічного співробітництва та розвитку, Світового банку, Міжнародного валютного фонду, Програми розвитку Організації Об'єднаних Націй. Інформаційну основу дослідження становлять також річна звітність підприємств, аналітичні огляди, міжнародні рейтинги та індекси, наукові праці вітчизняних і зарубіжних учених, матеріали науково-практичних конференцій, фахові публікації, інтернет-ресурси та власні розробки автора.

Наукова новизна одержаних результатів полягає у поглибленні теоретичних положень, удосконаленні методичних засад та розробленні науково-практичних рекомендацій щодо оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки. Найбільш

суттєвими теоретичними та прикладними результатами, що визначають наукову новизну дисертаційної роботи та відображають особистий внесок автора, є такі:

удосконалено:

- концептуальну модель економічної безпеки підприємства в умовах цифрової трансформації, яка розкриває її зміст як динамічної, багаторівневої та адаптивної системи стратегічного управління та інтегрує захисну й розвиткову функції, цифрові ризики, параметри стійкості, показники ефективності й індикатори ризику, що формує науково-методичне підґрунтя для комплексного оцінювання економічної безпеки і підвищення обґрунтованості управлінських рішень;

- методичні підходи до формування системи цифрового моніторингу економічної безпеки підприємства, які ґрунтуються на поєднанні принципів оцінювання, показників результативності та ризику а також цифрових технологій моніторингу, характеризуються врахуванням впливу цифрової трансформації на бізнес-процеси, технологічні ризики та механізми управлінського реагування, що забезпечує підвищення адаптивності системи управління економічною безпекою;

- методику інтегрального оцінювання економічної безпеки підприємств, яка доповнює існуючі підходи шляхом побудови інтегрального індексу на основі нормалізації та агрегування показників з урахуванням цифрової трансформації, що забезпечує комплексність оцінювання і формує аналітичну основу для визначення пріоритетів управлінського реагування;

набули подальшого розвитку:

- функціонально-ресурсний підхід до діагностики економічної безпеки підприємств, що забезпечує комплексність діагностики, підвищує обґрунтованість висновків і створює основу для виявлення ризиків і резервів забезпечення економічної безпеки;

- положення щодо систематизації цифрових ризиків економічної безпеки підприємств шляхом виділення взаємопов'язаних груп ризиків, визначення

механізмів їх впливу на бізнес-процеси та встановлення їх кореляції з ключовими показниками ефективності й ключовими індикаторами ризику, що дозволяє комплексно відобразити сучасну структуру загроз, інтегрувати цифрові чинники у систему моніторингу економічної безпеки та підвищити обґрунтованість управлінських рішень;

– науково-прикладні засади адаптації міжнародних практик цифрового ризик-менеджменту до умов національної економіки, які враховують інституційні та технологічні обмеження цифровізації, а також орієнтацію на інтеграцію інструментів міжнародних стандартів у систему управління економічною безпекою підприємств, що забезпечує підвищення ефективності ризик-орієнтованого управління і адаптивність підприємств до умов цифрової трансформації;

– положення щодо аналітичної діагностики та порівняльної оцінки економічної безпеки підприємств на основі інтегрального підходу, що передбачають поєднання динамічного та міжсекторального аналізу інтегрального індексу, оцінку його варіативності та структурної диференціації між підприємствами, що дозволяє виявляти стійкі тенденції, ідентифікувати відхилення у рівнях економічної безпеки та підвищує аналітичну обґрунтованість управлінських висновків;

– методичні засади прогнозування та сценарного аналізу інтегрального рівня економічної безпеки підприємств на основі економетричного моделювання, що передбачають використання панельної регресійної моделі для оцінювання взаємозв'язку між інтегральним індексом та системою факторів, а також варіювання їх значень у межах базового, оптимістичного та песимістичного сценаріїв, що дозволяє формалізувати вплив змін зовнішнього і внутрішнього середовища на рівень економічної безпеки та підвищує обґрунтованість прогнозних оцінок і управлінських рішень.

Практичне значення одержаних результатів полягає у розробленні науково-методичних положень, аналітичного інструментарію та практичних рекомендацій, що забезпечують підвищення обґрунтованості оцінювання

економічної безпеки підприємств в умовах цифрової трансформації економіки, а також можуть бути використані для прийняття управлінських рішень щодо підвищення їх стійкості та ефективності функціонування.

Окремі результати дисертаційного дослідження пройшли апробацію та впроваджені у практичну діяльність, що підтверджується відповідними довідками, наведеними у додатку Р.

Результати дослідження, представлені у дисертації, використано в практичній діяльності ТОВ «Наш Простір» (довідка № 11/26 від 22.04.2026 р.), Департаменту економічного розвитку і торгівлі Рівненської обласної державної адміністрації (довідка № 389/0/26 від 07.05.2026 р.), ТОВ «Українські деревинні пелети» (довідка № 19 від 11.05.2026 р.). Результати дослідження використовуються в навчальному процесі Національного університету водного господарства та природокористування результатів при викладанні навчальних дисциплін «Роль бухгалтера в бізнес-середовищі» та «Податкове планування» (довідка № 011-04 від 16.03.2026 р.).

Особистий внесок здобувача. Дисертаційна робота є самостійно виконаним науковим дослідженням, результати якого, включно з висновками та положеннями наукової новизни, що виносяться на захист, отримані автором особисто. Використання наукових здобутків, ідей та текстів інших дослідників супроводжується відповідними посиланнями на джерела. Із наукових праць, опублікованих у співавторстві, у дисертації використано лише ті матеріали, що є результатом особистого внеску автора, зокрема щодо дослідження питань оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки.

Апробація результатів дисертації. Основні ідеї та положення дисертаційної роботи обговорювалися та були представлені на 9 міжнародних науково-практичних конференціях: «Проблеми та перспективи розвитку сучасної науки» (м. Рівне, 2023 р.), «Комплексний підхід до модернізації науки: методи, моделі та мультидисциплінарність» (м. Житомир, 2023 р.), «Modernization of science and its influence on global processes» (м. Берн,

Швейцарська Конфедерація, 2024 р.), «Наукові тренди постіндустріального суспільства» (м. Тернопіль, 2025 р.), «Актуальні проблеми теорії і практики менеджменту в контексті євроінтеграції» (м. Рівне, 2025 р.), «Інтелектуальний ресурс сьогодення: наукові задачі, розвиток та запитання» (м. Чернівці, 2025 р.), «Детермінанти соціально-економічного відновлення держави, регіонів та суб'єктів господарювання» (м. Рівне, 2025 р.), «Сучасні виклики сталого розвитку бізнесу» (м. Житомир, 2025 р.), «New paradigms of interdisciplinary research: theories, ideas and developments» (м. Прага, Чехія, 2026 р.).

Публікації. За результатами дисертаційної роботи опубліковано 16 наукових праць загальним обсягом 6,70 друк. арк., з яких особисто автору належить 4,16 друк. арк., у тому числі: 1 стаття у науковому виданні, проіндексованому в наукометричній базі даних Scopus; 6 статей у наукових фахових виданнях України; 9 публікацій апробаційного характеру.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Обсяг основного тексту дисертаційної роботи становить 8,9 авторських аркушів. Дисертація містить 23 таблиці, 18 рисунків та 13 додатків, які викладені на 25 сторінках. Список використаних джерел налічує 182 найменування, оформлених на 25 сторінках.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ АСПЕКТИ ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВИХ ЗМІН В ЕКОНОМІЦІ УКРАЇНИ

1.1. Теоретичні засади економічної безпеки підприємства в умовах цифрової трансформації

Термін «економічна безпека» має тривалу історію розвитку. Ще в 1930-х роках він використовувався у соціально-економічному контексті. Зокрема, в програмах «Нового курсу» президента США Ф. Рузвельта економічна безпека ототожнювалась із захищеністю громадян від бідності, гарантіями зайнятості, соціального забезпечення та правом на гідне існування [1]. Отже, первинно дане поняття стосувалося індивідуального рівня – так званої економічної безпеки особи.

Протягом XX століття відбулося розширення цього поняття на рівень держав та міжнародних організацій. У трактуванні «безпеки» середини XX століття пріоритет надавався військово-політичним загрозам, тоді як економічні виклики трактувались другорядно. Лише наприкінці «холодної війни», особливо після розпаду СРСР, економічна складова національної безпеки посіла чільне місце у політичному та науковому дискурсах [2].

З початку 1990-х років термін «економічна безпека» активно використовується для характеристики здатності національної економіки протистояти внутрішнім і зовнішнім загрозам, забезпечувати самодостатній розвиток і стабільність. Одним із перших визначень у постсоціалістичних країнах запропонував В. В. Рубанов, який трактував економічну безпеку як здатність національної економіки забезпечити добробут нації та стабільність внутрішнього ринку незалежно від дії зовнішніх чинників [4]. Подібну інтерпретацію сформулював В. І. Паньков, визначаючи економічну безпеку як стан економіки, що характеризується стійкістю та імунітетом до внутрішніх і

зовнішніх впливів [3]. Ці підходи репрезентують захисно-стабілізаційну парадигму, за якою економічна безпека постає як здатність системи зберігати функціонування в умовах загроз.

Поглиблення теоретико-методологічного змісту категорії «економічна безпека» в українській науковій думці засвідчує еволюцію від традиційного захисного трактування до стратегічно-розвиткової парадигми. Так, В. Г. Андрійчук акцентує увагу на багатовимірності економічної безпеки, яка охоплює не лише стійкість до зовнішніх шоків, а й здатність економіки до самовідтворення, збалансованого зростання та ефективного функціонування в умовах структурних трансформацій [5]. Учений пропонує підходити до економічної безпеки як до системної категорії, що інтегрує індикатори фінансової, виробничої, ресурсної, соціальної, екологічної безпеки та інституційної спроможності держави. Особливий акцент робиться на визначенні превентивних інструментів захисту, які мають ґрунтуватися на системному моніторингу та багаторівневому аналізі вразливостей.

Додатково, у публікації К. А. Лопатки та Ю. Г. Шаранової пропонується інституційний підхід до розуміння економічної безпеки, що підкреслює важливість ефективного функціонування правових, адміністративних та регуляторних механізмів забезпечення стійкості національної економіки [6]. Автори акцентують увагу на важливості дієвих механізмів державного управління, зокрема моніторингу загроз, індикативного аналізу та адаптивності політик. Особливої актуальності, за спостереженням дослідників, набуває потреба в забезпеченні прозорості інституцій та довіри до економічної політики держави, оскільки саме ці чинники визначають здатність країни до мобілізації ресурсів у кризових умовах.

Узагальнюючи підходи сучасних українських дослідників, слід зазначити, що поняття економічної безпеки поступово трансформується в напрямі синтезу захисної, регуляторної та розвитку-орієнтованої функцій. Економічна безпека більше не обмежується виключно запобіганням загрозам, а розглядається як стратегічний потенціал держави щодо збереження

економічного суверенітету, підвищення стійкості до глобальних шоків і реалізації національних інтересів у довгостроковій перспективі [7].

У західному дискурсі термін «економічна безпека» у цей період також починає фігурувати у стратегічному плануванні, поступово перетворюючись із суто економічного поняття на багатовимірну категорію, інтегровану в систему національної та міжнародної безпеки.

У США акценти економічної безпеки були зосереджені на зміцненні конкурентоспроможності, розвитку національної промисловості, диверсифікації ланцюгів постачання, зниженні критичної залежності від іноземних технологій та сировини, досягненні енергетичної незалежності, стабільності фінансової системи, а також захисті критичної інфраструктури в умовах транснаціональних загроз. У Стратегії національної безпеки США 2022 року окрему увагу приділено зміцненню економічної стійкості як одного з головних інструментів протидії авторитарним державам, економічному шантажу та загрозам національним інтересам. Документ також підкреслює необхідність інвестування в інновації, «зелені» технології, цифрову інфраструктуру та людський капітал як засобів довгострокового забезпечення економічної безпеки країни [8]. У рамках національної безпекової стратегії економічні інтереси дедалі більше визнаються ключовими компонентами геополітичної сили держави, а не лише внутрішньоекономічними пріоритетами.

У документах міжнародних організацій, передусім Програми розвитку Організації Об'єднаних Націй (ПРООН), домінує гуманітарно-орієнтований підхід, відповідно до якого економічна безпека визначається як захищеність людини від хронічної бідності, структурного безробіття, нестачі доходів, нерівного доступу до основних благ і ресурсів, що забезпечують мінімальний рівень гідного існування [9]. Такий підхід започаткував концепцію «людської безпеки», яка трансформувала фокус безпекової політики від держави до індивіда, вимагаючи міждисциплінарного підходу та залучення інструментів сталого розвитку.

Таким чином, історичний розвиток концепції економічної безпеки засвідчує її поступову еволюцію від локальної (індивідуальної) до макроекономічної та глобальної категорії, з акцентом на інтеграцію до стратегій сталого розвитку, забезпечення соціальної стабільності, зміцнення економічного суверенітету та інституційної спроможності держав адаптуватися до динамічних глобальних трансформацій.

У цьому контексті важливим є порівняння стратегічних підходів до економічної безпеки. Так, у Європейському Союзі (ЄС) дедалі більше значення надається економічній відкритості, цифровому суверенітету, кліматичній нейтральності та зниженню залежності від третіх країн у критично важливих сферах. Відповідно до концепції «Європа, що захищає» (A Europe that protects), питання економічної безпеки розглядаються як частина загальної стратегії стратегічної автономії ЄС, у межах якої пріоритет надається зміцненню внутрішнього ринку, розвитку інновацій, технологічного потенціалу та зменшенню вразливості до зовнішніх шоків. Особлива увага приділяється також «зеленій» трансформації, цифровій інфраструктурі, захисту даних і критично важливим технологіям, зокрема виробництву мікроелектроніки (мікročіпів), розвитку штучного інтелекту (ШІ) та мобільного зв'язку п'ятого покоління (5G), що відображено в стратегіях Digital Compass 2030, Industrial Strategy 2021 та концепції Open Strategic Autonomy [10].

На відміну від США, де пріоритетом є збереження геоекономічного домінування, захист ланцюгів постачання та протидія авторитарним режимам, європейський підхід акцентує на досягненні балансу між відкритістю і захистом, на соціальній та екологічній стійкості як основі економічної безпеки. Європейська економічна безпека має чіткий інституційний контекст, у якому провідну роль відіграють Європейська комісія, Рада ЄС, Європейський центральний банк та інші наднаціональні органи, що забезпечує узгодженість між країнами-членами та інтегрованість підходів.

В Україні концепція економічної безпеки також зазнає трансформації під впливом глобальних трендів, цифровізації, воєнної агресії з боку російської федерації, посилення кіберзагроз і потреби адаптації до стандартів ЄС. У Стратегії економічної безпеки України на період до 2025 року наголошено на необхідності створення інтегрованої системи забезпечення економічної безпеки, що охоплює фінансову, енергетичну, інформаційну, інституційну, інноваційну та ресурсну компоненти. Основними напрямками визначено: розвиток цифрової економіки, зміцнення кібербезпеки, енергетичну незалежність, підтримку внутрішнього виробника, а також посилення стійкості до зовнішніх шоків. Це свідчить про формування нової парадигми економічної безпеки в Україні – гнучкої, проактивної та інтегрованої з міжнародними практиками [11].

Проблематика економічної безпеки в українській науці активізувалася від початку 1990-х років як відповідь на виклики становлення державної незалежності та ринкової трансформації. На ранньому етапі зміст поняття вибудовувався навколо макрорівневих орієнтирів – економічного суверенітету, стійкості інститутів і здатності до довгострокового розвитку, що відображено в фундаментальних наукових працях, присвячених економічній безпеці держави [12]. У подальшому – із формуванням нормативно-політичної рамки (зокрема Стратегії економічної безпеки України до 2025 р.) – ці інваріантні ознаки були конкретизовані через перелік функціональних складових (макроекономічну, фінансову, інвестиційно-інноваційну, зовнішньоекономічну тощо) й індикативні орієнтири моніторингу [13]. На цьому тлі в академічному дискурсі поступово утвердився багатовимірний характер дефініції, що поєднує захищеність інтересів і спроможність до розвитку як дві взаємодоповнювальні сторони однієї категорії.

Наведена у Додатку Б таблиця створена з метою систематизації та порівняння наукових підходів до трактування поняття «економічна безпека» в сучасній і класичній вітчизняній та зарубіжній літературі. До переліку включено дефініції, що охоплюють два рівні аналізу: макрорівень –

економічна безпека держави як здатність економіки забезпечувати суверенний розвиток, стійкість інститутів і захист національних інтересів; *мікрорівень* – економічна безпека підприємства як стан захищеності ресурсів, процесів та результатів діяльності від внутрішніх і зовнішніх загроз.

З позицій методологічних засад можливим є виокремлення кількох базових теоретичних підходів до трактування економічної безпеки.

1. *Ресурсно-функціональний*: безпека інтерпретується як стан ефективного використання ресурсів та наявних ринкових можливостей задля довгострокової життєздатності економічної системи попри дію загроз. У класичних працях це чітко окреслено для рівня підприємства (як окремої економічної системи): економічна безпека постає як такий стан ресурсів і управлінських можливостей, який забезпечує стабільне функціонування та розвиток і мінімізує вплив внутрішніх і зовнішніх ризиків. Хоча дане трактування подано для мікрорівня, зміст підходу узгоджується з макрорівневою логікою забезпечення потенціалу стійкого зростання.

2. *Захисно-системний (комплексний)*: у центрі уваги – захищеність життєво важливих інтересів і стійкість системи до шоків. Для держави економічна безпека визначається як спроможність гарантувати суверенний розвиток, інституційну стабільність, обороноздатність, а також захист національних інтересів від багатофакторних загроз. Така рамка дозволяє операціоналізувати поняття через систему складових і загроз, що корелює з державними стратегічними документами.

3. *Стратегічно-цільовий*: наголос робиться на досягненні стратегічних цілей розвитку (економічне зростання, інноваційність, технологічна автономність, соціальна стійкість). У прикладному вимірі цей підхід відтворено в аналітичних і методичних працях останніх років (зокрема в статтях, присвячених оновленню індикаторного інструментарію та сценарному оцінюванню безпеки), де безпека трактується як здатність системи передбачати, нейтралізувати та менеджеризувати загрози, забезпечуючи виконання стратегічних пріоритетів [14; 15].

4. *Ринково-інституційний / ризик-орієнтований*: трактування поняття «економічна безпека» зосереджується на гармонізації економічних інтересів у конкурентному середовищі та на управлінні ризиками як домінуючій парадигмі. Для рівня підприємства це проявляється у фокусі на методах і підходах до оцінювання (ризик-/індикаторно-орієнтовані моделі, сценарний аналіз), що трансформують економічну безпеку з «стану» в динамічний процес постійної адаптації. На макрорівні ризик-орієнтація матеріалізується у винесенні в політику питань стійкості ланцюгів постачання, технологічної залежності та системної вразливості до зовнішніх шоків.

Особливе місце у вітчизняній традиції посідає перетин макро- та мікрорівневих трактувань. По-перше, для держави економічна безпека системно пов'язується з економічним суверенітетом і інституційною спроможністю забезпечувати відтворення та розвиток (у т.ч. в умовах екзогенних шоків), що підтверджується як академічними узагальненнями, так і офіційною стратегією [16; 17; 18]. По-друге, для підприємств – із керованістю ресурсно-процесних і фінансових ризиків, підтриманням конкурентоспроможності та інноваційної динаміки, що відображено в сучасних публікаціях із систематизацією підходів і методик оцінювання. Такий «вертикальний» зв'язок пояснює, чому у працях, присвячених підприємствам, дедалі частіше фіксуються структурні й технологічні детермінанти безпеки (цифрові компетентності, інтеграція даних, кіберзагрози) як похідні від ширших трендів макрорівневої безпеки [14; 16].

Зміна парадигми, спричинена цифровою трансформацією, суттєво вплинула на зміст поняття в обох вимірах. На макрорівні зростає важливість технологічної автономності, стійкості критичної інфраструктури і ланцюгів постачання, що інтегровано у положення Стратегії економічної безпеки України [11]. На мікрорівні цифрова трансформація зумовлює перехід до процесно- та даноорієнтованих моделей управління економічною безпекою, у межах яких оцінювання будується на комплексному застосуванні індикаторного, ризик-орієнтованого та сценарного підходів. Така інтеграція

дає змогу не лише більш повно відобразити динамічний і багатовимірний характер технологічних і ринкових змін, але й підвищити адаптивність системи управління до виникнення нових загроз. Зазначений підхід дозволяє своєчасно ідентифікувати критичні вразливості, обґрунтовувати пріоритети ресурсного забезпечення заходів безпеки та формувати ефективні стратегії розвитку, що є ключовою умовою забезпечення стійкості суб'єкта господарювання в умовах цифровізації економіки. Можемо стверджувати, що синтез цих підходів у сучасній українській літературі дозволяє розглядати *економічну безпеку як динамічний, адаптивний процес, що поєднує захист від загроз зі спроможністю до інноваційного розвитку і досягнення стратегічних цілей у середовищі підвищеної невизначеності.*

Діяльність підприємства у сфері економічної безпеки в умовах цифровізації спрямована на протистояння тим зовнішнім і внутрішнім викликам, які можуть негативно вплинути на його фінансові результати.

1. *Зовнішні ризики* можуть бути представлені такими групами: політичні, соціально-економічні та загрози національній безпеці.

Політичні ризики зумовлені, насамперед, так званими «перегонами у сфері цифрових технологій» – суперництвом країн у досягненнях науково-технологічного прогресу, що визначає їх роль у світовій економіці. Таке суперництво породжує «цифрову нерівність»: найбільш інноваційно розвинені країни займають передові позиції на світовому ринку, а країни з уповільненим інноваційним розвитком набувають статусу наздоганяючих, менш конкурентоспроможних, що безпосередньо відображається як на національній економіці таких країн в цілому, так і на окремих галузях та підприємствах. Політичні ризики також спричиняють соціально-економічні проблеми, такі як соціальна нерівність громадян, залежність від експортної політики країн-лідерів світової економіки.

У сферах національної та воєнної безпеки треба передбачати можливість нанесення цифровізацією суттєвих втрат без фізичного військового втручання.

Розвиток цифрових та інформаційних технологій створює такі загрози воєнній безпеці:

- виявлення інформації військового характеру;
- здійснення психологічного впливу на супротивника;
- знищення інформаційних баз супротивника;
- впровадження вірусних програм в інформаційні бази противника.

Інформаційна війна охоплює широкий спектр об'єктів впливу і не має фізичної форми, тому при такому протистоянні виникає більше можливостей впливу на супротивника, ніж при збройних способах.

Також необхідно відзначити вплив нових технологій на оборонний комплекс. Інноваційні розробки призводять до появи нових видів зброї масового ураження. Технології 3D-друку докорінно змінюють концепцію виробничого циклу і дають можливість виготовлення певної продукції без налагодження великомасштабного виробництва. Такі технології можуть дозволити виготовляти зброю та призвести до зростання рівня злочинності у кілька разів, суттєво підриваючи національну безпеку та безпеку суспільства.

2. *Внутрішні ризики* пропонується розділити на такі підгрупи: правові, структурні, суб'єктів господарювання (організаційні) та особистості.

Загрози правового характеру це, насамперед, відсутність сформованої нормативно-правової бази, що регулює відносини, що виникають між суб'єктами цифрового середовища.

По-перше, виникає проблема ідентифікації самих суб'єктів, у віртуальному середовищі вони можуть бути знеособлені, виступаючи від імені віртуальної особистості.

По-друге, цифровізація впливає на розуміння об'єкта правовідносин: їх основним об'єктом стає інформація. Питання володіння та доступу до інформації стають ключовими як у приватному, так і у публічному праві. З'являються нові об'єкти права: електронні гроші, нові інструменти створення матеріальних цінностей, віртуальні об'єкти. За таких умов виникає

необхідність у адаптації чинних норм права, а в деяких випадках і розробка абсолютно нових.

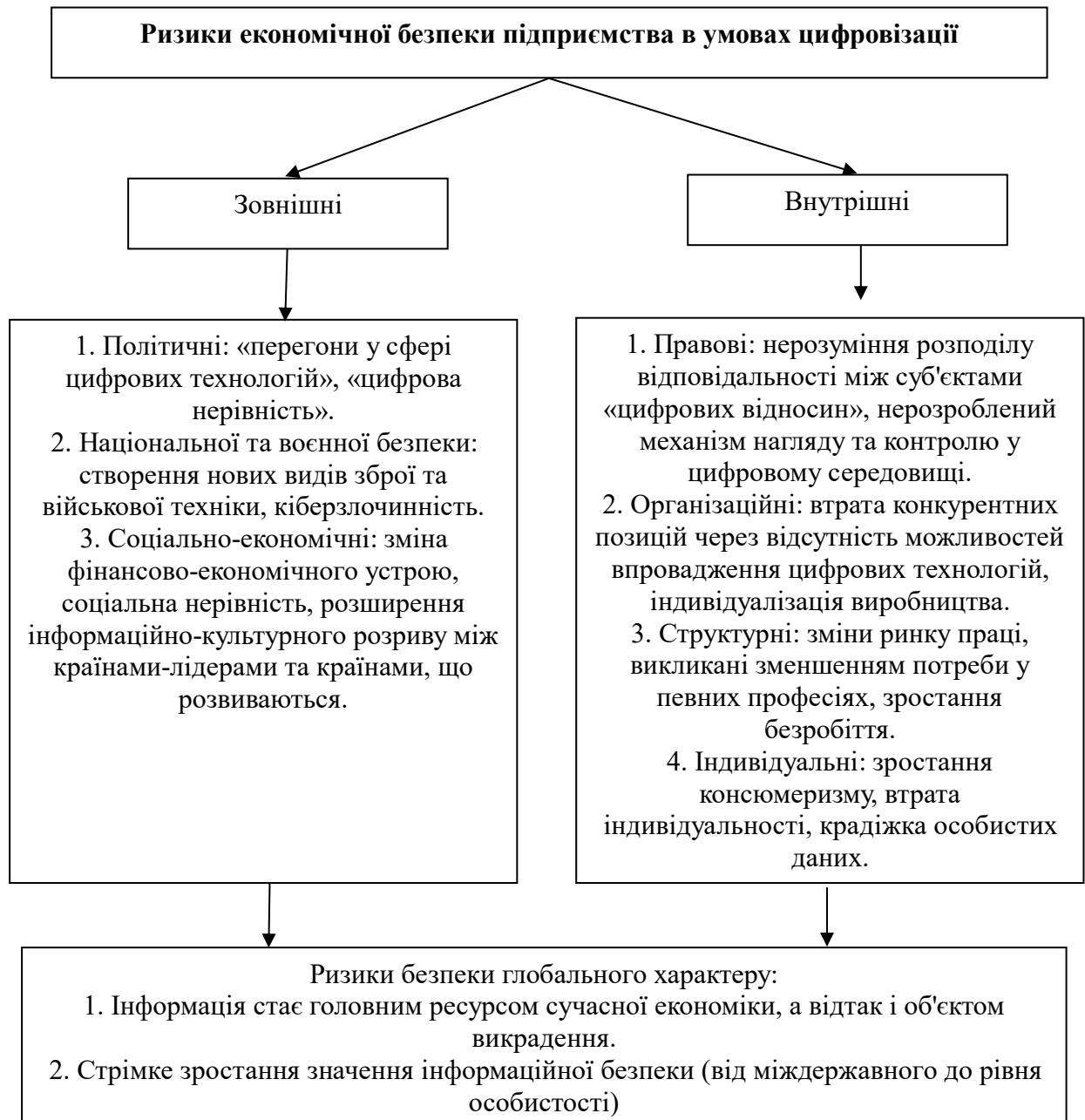


Рис. 1.1. Класифікація ризиків економічної безпеки підприємства в умовах цифровізації

Джерело: узагальнено автором на основі [17; 18; 19].

На державному рівні спостерігається масштабне впровадження цифрових технологій у систему державного управління: багатофункціональні центри, міжвідомча взаємодія, цифрові платформи (наприклад, Дія).

Основним ризиком цієї категорії залишається кіберзлочинність, однак можемо виділити ще низку загроз: залежність від мережі Інтернет – будь-який збій повністю паралізує роботу цифрових систем різних рівнях; зниження державного контролю.

Загрози структурного характеру представлені потенційною можливістю скорочення робочих місць та подальшим зростанням рівня безробіття. Цифровізація може призвести до незатребуваності та зникнення деяких професій, з одного боку, та дефіциту компетентних фахівців, з іншого.

Сьогодні на ринку праці існує гостра нестача кадрів: багато претендентів не мають не тільки високого рівня підготовки, але й не володіють цифровими компетенціями. Також спостерігаються тенденції до збільшення частки віддаленої зайнятості. Для сучасних компаній кадрові ризики особливо важливі, оскільки виважена управлінська політика та компетентний кадровий склад багато в чому визначають ефективність та стійкість суб'єкта господарювання.

У зв'язку із втратою робочих місць, страхом перед новими технологіями та консервативними звичками виникає низка індивідуальних ризиків на рівні особистості, які можуть знайти свій розвиток у трьох напрямках:

- пов'язані з розвитком віртуального середовища: втрата індивідуальності та орієнтації у реальному світі;
- стимулюючі споживання: масовий консюмеризм, пов'язаний з розвитком Інтернет-торгівлі та технологіями маркетингу;
- конфіденційність приватного життя: крадіжка особистих даних та дії щодо їх захисту є істотним наслідком розвитку мережі Інтернет та соціальних мереж.

Для сучасного підприємства ризики тісно пов'язані із втратою конкурентних позицій на ринку, нестачею коштів та неготовністю впровадження цифрових технологій, інформаційною безпекою. У межах нашого дослідження ризики суб'єкта господарювання розглянуті за ознакою типів стійкості.

У сучасній теорії управління існує кілька десятків класифікацій ризиків за різними ознаками: за суб'єктами, за сферами впливу, причинами виникнення, за ступенем шкоди, за рівнем передбачуваності та інші. Оскільки науковцями не розроблено єдиного підходу до класифікації ризиків, які можуть виникнути в умовах цифровізації, у роботі запропоновано ранжування ризиків у контексті збереження стабільного фінансового стану підприємства.

Класичний підхід дослідження ризиків економічної безпеки не передбачає вивчення питань, пов'язаних із цифровізацією, що не зовсім правильно, адже сучасні реалії ведення бізнесу потребують окремого виділення ризиків, пов'язаних з нею. Облік цифрових ризиків здатний змінювати набір функцій суб'єкта господарювання і навіть архітектуру ринку.

У таблиці 1.1 розглянуто можливі ризики, що виникають в умовах цифровізації та можуть істотно вплинути на значення ключових показників ефективності та на стійке становище сучасного підприємства в умовах цифровізації.

Таблиця 1.1

Класифікація ризиків стійкості підприємства як елемента економічної безпеки в умовах цифровізації

Тип стійкості	Ключовий показник ефективності	Ризики, які можуть вплинути на ефективність підприємства в умовах цифровізації
1	2	3
Економічна стійкість	Виручка від реалізації продукції (товарів, робіт, послуг). Зниження питомих операційних витрат.	1. Потреба у значних фінансових вкладеннях на нове обладнання та програмне забезпечення (до витрат на впровадження цифрових технологій доцільно відносити витрати на всі технології, системи та програмно-апаратні комплекси, задіяні у зчитуванні/обробці та передачі даних). 2. Невизначеність очікуваного економічного ефекту (терміни окупності різних цифрових технологій становлять від 5 до 10 років).

Продовження табл. 1.1

1	2	3
Технічна стійкість	Виконання виробничого плану. Завантаження нововведених потужностей.	1. Невідповідність існуючого рівня технічного оснащення вимогам та стандартам цифровізації. 2. Відсутність каналів зв'язку та зон обслуговування у віддалених регіонах. 3. Зростання ймовірності відмови основного обладнання через збільшення кількості автоматизованих ланок. 4. Нестабільні природні та погодні умови в період ремонтних робіт.
Цифрова стійкість	Виручка від надання додаткових послуг. Підвищення продуктивності праці.	1. Ризик зростання безробіття. 2. Невідповідність кваліфікації персоналу потребам цифрових інструментів, що впроваджуються, недостатнє знання сучасних ІТ-технологій. 3. Відсутність мотивації працівників до освоєння нових компетенцій, пов'язаних із цифровізацією виробництва.
Стійкість енергоефективності	Рівень втрат. Коефіцієнт корисного використання енергії.	1. Навмисне виведення з ладу приладів обліку, що перебувають у громадському доступі, призведе до неврахованого споживання електроенергії. 2. Загрози інформаційній безпеці.
Інноваційна стійкість	Ефективність інноваційної діяльності. Виконання графіка введення нових об'єктів в експлуатацію.	1. Пристрої та програмне забезпечення різних виробників – існує ризик поганої інтеграції один з одним. 2. Відсутність систем передачі та аналізу даних. 3. Нестабільні природні та погодні умови.

Джерело: авторська розробка.

Застосування ризик-орієнтованого підходу дозволить підвищити ефективність діяльності підприємства, зберегти стійке становище, мінімізувати помилки під час прийняття управлінських рішень.

Необхідно також відзначити такий аспект, як складність державного контролю за правильністю нарахування податків та формуванням бази оподаткування в умовах цифровізації бізнесу, адже більша частина потоків переходить у цифровий простір і не потрапляє у поле зору податкових органів.

Найважливішим ефектом, з погляду координації бізнес-процесів, є інтеграція всіх управлінських процесів в один. Також слід зазначити, що ефект

цифровізації матиме місце тоді, коли використання відбуватиметься на макрорівні, масово. Будь-яка інституційна зміна спричинить не лише перегляд характеру процесу, а й трансформацію відносин між усіма задіяними в ньому учасниками.

Запропонована класифікація ризиків (рис. 1.1) та типів стійкості економічної безпеки підприємства (табл. 1.1) створює системну основу для визначення потенційних загроз і вразливостей. Однак для перетворення цього знання на дієву систему управління необхідне застосування сучасних концепцій *ризик-орієнтованого управління безпекою* (РОУБ). Саме ризик-орієнтований підхід дозволяє інтегрувати процеси ідентифікації ризиків, їх кількісної та якісної оцінки, розробки стратегій реагування та постійного моніторингу у єдину адаптивну систему [20; 21; 22]. Він формує перехід від виключно захисної парадигми до стратегічно-розвиткової, де превенція загроз поєднується із забезпеченням досягнення довгострокових цілей у середовищі високої невизначеності [23].

Ризик-орієнтоване управління безпекою підприємства ґрунтується на циклічній логіці, яка передбачає послідовне здійснення низки взаємопов'язаних етапів. Передусім відбувається ідентифікація ризиків, що включає системне виявлення внутрішніх і зовнішніх чинників, здатних вплинути на досягнення стратегічних та операційних цілей суб'єкта господарювання. Далі здійснюється аналіз і оцінювання ризиків, під час якого визначається ймовірність настання потенційних подій і масштаби їх можливого впливу на фінансово-економічні показники, безпеку виробничих процесів та репутацію підприємства. На основі результатів аналізу формується перелік варіантів реагування на ризики, що охоплюють заходи з уникнення, зниження, передавання або прийняття ризику з урахуванням встановленого рівня допустимості. Наступним кроком є розробка та впровадження заходів реагування, які мають на меті запобігти реалізації загроз або мінімізувати їх негативні наслідки. Завершальним етапом циклу виступають моніторинг і перегляд підходів до управління ризиками, що забезпечують своєчасне

оновлення ризик-профілю підприємства у зв'язку зі зміною зовнішнього і внутрішнього середовища його функціонування [24; 25].

Відповідно до ДСТУ ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови» (ISO 31000:2018, IDT) управління ризиками має інтегруватися в усі процеси підприємства, охоплюючи стратегічний і тактичний рівні управління. Норматив передбачає, що ризик-орієнтований підхід має бути адаптивним, гнучким і пропорційним масштабам діяльності організації [21]. Комплементарним документом ІЕС/ISO 31010:2019 «Risk assessment techniques», який містить систематизований перелік методик якісного і кількісного аналізу ризиків: аналіз сценаріїв, аналіз дерева відмов, аналіз дерева подій, метод Монте-Карло, аналіз чутливості тощо [22]. Використання зазначених методів дозволяє адаптувати систему управління безпекою до специфіки діяльності підприємства та зовнішнього середовища.

У процесі реалізації зазначеної логіки ключового значення набувають такі поняття, як ризик-апетит (допустимий рівень ризику, який підприємство готове прийняти заради досягнення визначених цілей) і толерантність до ризику (гранично допустимі відхилення від заданих параметрів). Важливими інструментами є також ключові показники ризиків (Key Risk Indicators – KRI), що дають змогу кількісно виміряти імовірність або наслідки ризикових подій, та ключові показники ефективності (Key Performance Indicators – KPI), які фіксують результативність реалізації стратегії підприємства. Для поглибленого розуміння взаємозв'язків між ризиками та їх детермінантами активно застосовуються сценарний аналіз (метод прогнозування можливих варіантів розвитку подій із врахуванням невизначеності), карти ризиків (heat-map), що візуалізують рівні ймовірності та величини впливу ризиків, а також діаграми «метелик» (bow-tie), які дозволяють систематизувати причини виникнення ризикової події та можливі наслідки її реалізації. Додатковим елементом є стрес-тестування, що імітує екстремальні сценарії для перевірки стійкості бізнес-процесів і систем безпеки. Відповідно до Моделі трьох ліній (The IIA's Three Lines Model), розробленої Інститутом внутрішніх аудиторів

(Institute of Internal Auditors, ІА), практика стрес-тестування є невід’ємною складовою системи внутрішнього контролю та управління ризиками і має реалізовуватися у тісній взаємодії між першою лінією (операційний менеджмент), другою лінією (функції ризик-менеджменту та комплаєнсу) та третьою лінією (внутрішній аудит), яка надає незалежні запевнення щодо достатності й ефективності таких перевірок [26].

В Україні ризик-орієнтований підхід поступово впроваджується не лише у корпоративному секторі, але й у державному управлінні. Так, Національний банк України у 2022 році затвердив ризик-орієнтовану методологію нагляду за банківськими установами, яка ґрунтується на принципах ДСТУ ISO 31000:2018 і визначає пріоритети регуляторних дій залежно від рівня ризику в кожній установі [21]. У сфері енергетики НЕК «Укренерго» у 2023 році впровадила систему оцінювання операційних і кіберризиків з використанням KRI та карт ризиків, що дало змогу оптимізувати процеси планування заходів із кіберзахисту критичної інфраструктури [28]. У галузі промислового виробництва компанії з високим рівнем автоматизації використовують метод Монте-Карло і сценарний аналіз для прогнозування ризиків збоїв у виробничих процесах і порушень ланцюгів постачання [29].

Ризик-орієнтоване управління безпекою передбачає тісну інтеграцію процесів управління ризиками у систему корпоративного управління та стратегічного планування підприємства. Такий підхід дозволяє не лише зменшувати ймовірність настання критично небезпечних подій, а й підвищувати гнучкість і здатність організації використовувати нові можливості у середовищі постійних змін. Інтеграція РОУБ у стратегічні механізми управління створює умови для узгодження допустимого рівня ризику із довгостроковими цілями підприємства, формування прозорих процедур прийняття управлінських рішень, а також посилення корпоративної культури, орієнтованої на усвідомлене ставлення до ризиків і ефективне управління ними.

Сучасні концепції ризик-орієнтованого управління безпекою реалізуються через низку міжнародних стандартів і методологічних підходів, які визначають принципи, етапи та інструменти управління ризиками в організаціях різного профілю діяльності. Найбільш поширеними з них є ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови», який формує універсальну методологічну основу ідентифікації та оцінювання ризиків [21]; COSO ERM (Enterprise Risk Management), що акцентує на інтеграції управління ризиками у корпоративне управління та стратегічне планування [23]; а також NIST Cybersecurity Framework (CSF) 2.0, розроблений Національним інститутом стандартів і технологій США для підвищення кіберстійкості та управління інформаційними ризиками в умовах цифровізації [31].

Кожен із зазначених підходів відрізняється рівнем деталізації, сферою застосування, специфікою процедур і вимогами до документування процесів управління ризиками. Наприклад, ISO 31000 характеризується універсальністю і може бути застосований у будь-якій галузі, тоді як COSO ERM має чітко виражену орієнтацію на узгодження з корпоративними цілями та фінансовими показниками ефективності (KPI). NIST CSF є вузькоспеціалізованим підходом, орієнтованим на кіберризики та цифрову інфраструктуру, що особливо актуально в умовах діджиталізації та посилення кіберзагроз.

Для систематизації ключових характеристик зазначених стандартів і методологій у дослідженні сформовано таблицю 1.2. Метою її побудови є можливість здійснити ґрунтовний аналіз сильних сторін і обмежень кожного підходу, а також виявити сфери їх найбільш ефективного застосування у контексті забезпечення економічної безпеки підприємств. Такий підхід дозволяє дослідити взаємодоповнюваність зазначених систем і визначити, які з їхніх положень доцільно імплементувати в українську практику управління ризиками.

Таблиця 1.2

Порівняльна характеристика міжнародних стандартів ризик-орієнтованого управління економічною безпекою підприємства

Стандарт/ методологія	Призначення	Ключові принципи	Основні етапи процесу	Сильні сторони в умовах цифровізації	Обмеження / виклики впровадження
1	2	3	4	5	6
ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови» (ДСТУ ISO 31000:2018, IDT)	Міжнародний стандарт, що встановлює універсальні принципи, структуру та процеси управління ризиками для організацій будь-якого типу та масштабу діяльності. Його метою є створення єдиної інтегрованої системи, яка дозволяє своєчасно ідентифікувати ризики, оцінювати їх вплив на досягнення стратегічних цілей та розробляти ефективні заходи реагування.	Інтегрованість у всі рівні управління, структурованість та системність підходу, гнучкість і адаптивність до особливостей конкретної організації, а також постійне вдосконалення процесів ризик-менеджменту на основі аналізу результатів і зовнішніх змін.	Визначення внутрішнього та зовнішнього середовища діяльності підприємства і його стратегічних цілей → ідентифікація потенційних ризиків → їх якісна та кількісна оцінка → вибір і застосування заходів реагування (уникнення, зниження, передавання або прийняття ризику) → моніторинг, звітність та регулярний перегляд ефективності процесу.	Стандарт характеризується високою гнучкістю, уніфікованою термінологією та можливістю застосування в будь-якій галузі, що робить його придатним для інтеграції в цифрові системи управління, автоматизовані платформи моніторингу ризиків та корпоративні інформаційні середовища.	Надмірна загальність положень стандарту потребує розроблення додаткових внутрішніх методик і процедур, адаптованих до специфіки діяльності конкретної компанії. Вимагає наявності зрілої культури управління ризиками та ресурсів для побудови деталізованих регламентів.

Продовження табл. 1.2

1	2	3	4	5	6
COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Управління ризиками підприємства, інтегроване зі стратегією і діяльністю)	Методологічна система, спрямована на інтеграцію управління ризиками у систему корпоративного управління та стратегічного планування підприємства. COSO ERM передбачає тісний взаємозв'язок процесів ризик-менеджменту зі встановленням стратегічних цілей та прийняттям управлінських рішень на всіх рівнях підприємства, забезпечуючи при цьому визначення та підтримання прийнятного рівня ризик-апетиту, який узгоджується з довгостроковими пріоритетами розвитку підприємства.	Орієнтація на досягнення стратегічних і операційних цілей підприємства через узгодження ризик-апетиту з довгостроковими пріоритетами розвитку. Формування контрольного середовища з чітким розподілом ролей і відповідальності за управління ризиками на всіх рівнях. Особлива увага приділяється корпоративній культурі, яка підтримує усвідомлене ставлення до ризиків, підзвітність і прозорі процедури прийняття рішень.	Встановлення стратегічних і операційних цілей підприємства → ідентифікація ризиків, що можуть вплинути на їх досягнення → оцінювання рівня ризиків (якісне та кількісне) → розроблення та впровадження заходів реагування → моніторинг, контроль та звітність для забезпечення прозорості та підзвітності процесу.	COSO ERM забезпечує чітке узгодження ризик-менеджменту з фінансовими цілями та ключовими показниками ефективності (KPI), що дозволяє інтегрувати управління ризиками у цифрові платформи корпоративного планування і звітності.	Впровадження COSO ERM потребує наявності розвиненої культури управління ризиками в межах підприємства, значного обсягу документування процесів і ресурсного забезпечення для належної підтримки всіх етапів методології.

Продовження табл. 1.2

1	2	3	4	5	6
NIST Cybersecurity Framework (CSF) 2.0 – Рамкова модель кібербезпеки Національного інституту стандартів і технологій США (NIST)	Нормативно-методичний підхід для побудови та вдосконалення системи управління інформаційними та кіберризиками на рівні підприємства. CSF 2.0 орієнтований на підвищення кіберстійкості (здатності витримувати, виявляти, стримувати та відновлюватися після кіберінцидентів) у приватному й державному секторах, з можливістю масштабування для підприємств різного розміру та галузевої належності.	Ризик-орієнтованість і результативність; технологічна нейтральність; узгодженість зі стратегічними цілями підприємства; модульність та масштабованість; безперервне поліпшення; сильна компонентна управління, що охоплює політики, ролі, відповідальність, вимоги до постачальників і взаємодію з екосистемою.	Identify (Ідентифікуй) → Protect (Захищай) → Detect (Виявляй) → Respond (Реагуй) → Recover (Відновлюй) – інтегровані з керівними результатами CSF 2.0 (цільові стани та практики), профілями (поточний та цільовий профілі підприємства) і рівнями впровадження, які відображають зрілість системи управління кіберризиками.	Висока деталізація саме для цифрових та кіберризиків; сумісність із іншими стандартами (наприклад, ISO/IEC 27001) і корпоративними циклами планування; підтримка роботи з KRI/KPI (через вимоги до моніторингу інцидентів, часу виявлення/відновлення, показників доступності/цілісності/конфіденційності); застосовність до ланцюгів постачання та керування ризиками сторонніх постачальників; наявність практичних довідників і профілів для різних секторів.	Зосередженість передусім на кібербезпеці (поза цією сферою потрібне доповнення іншими стандартами управління ризиками); потреба в кваліфікованих кадрових і технологічних ресурсах для належного моніторингу та автоматизації; необхідність адаптації контрольних заходів під специфіку ІТ-ландшафту підприємства та його регуляторного середовища.

Джерело: узагальнено автором на основі [21; 23; 31].

Аналіз міжнародних стандартів і методологічних систем управління ризиками засвідчує, що найбільш універсальним є міжнародний стандарт ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови» (International Organization for Standardization), оскільки він визначає базові принципи, загальну структуру та процеси управління ризиками для підприємств будь-якого типу та масштабу діяльності. Натомість методологія COSO ERM (Enterprise Risk Management – Управління ризиками підприємства), розроблена Комітетом спонсорських організацій Комісії Тредвея (Committee of Sponsoring Organizations of the Treadway Commission, COSO), забезпечує інтеграцію процесів ризик-менеджменту із системою корпоративного управління та досягненням фінансово-економічних цілей підприємства. Ця методологія особливо акцентує на визначенні ризик-апетиту, узгодженого з довгостроковими пріоритетами розвитку, формуванні ефективного контрольованого середовища та корпоративної культури підзвітності. У свою чергу, рамкова модель кібербезпеки NIST CSF (Cybersecurity Framework, розроблена Національним інститутом стандартів і технологій США – National Institute of Standards and Technology, NIST) характеризується високою деталізацією механізмів управління цифровими ризиками, що виникають унаслідок функціонування інформаційно-комунікаційних технологій. Вона визначає комплекс функцій – ідентифікація, захист, виявлення, реагування та відновлення – які є ключовими для забезпечення кіберстійкості підприємства.

У сучасних умовах цифрової трансформації економіки ризик-орієнтоване управління безпекою потребує глибокої інтеграції технологічних інструментів, що забезпечують безперервний моніторинг та аналіз ризиків. До таких інструментів належать методи управління ризиками на основі даних (data-driven risk management), панелі-дашборди для візуалізації та відстеження ключових показників ризиків (Key Risk Indicators – KRI), автоматизовані системи журналювання інцидентів і керування вразливостями. Особливу увагу приділяють ризикам кібербезпеки, пов'язаним із несанкціонованим доступом до інформаційних ресурсів, ризикам даних

(порушення цілісності, доступності чи конфіденційності інформації), а також ризикам залежності від критичних постачальників і технологічних платформ.

У контексті цифрової трансформації важливо враховувати ризики, що виникають унаслідок використання алгоритмічних рішень на базі технологій штучного інтелекту (Artificial Intelligence – AI) та машинного навчання (Machine Learning – ML). Такі ризики можуть призвести до значних негативних наслідків через можливі помилки під час навчання моделей, упередженість у даних або відсутність можливості пояснити результати роботи алгоритмів.

Одним із найефективніших інструментів реалізації ризик-орієнтованого управління безпекою підприємства є побудова матриці відповідності типів стійкості економічної безпеки підприємства, класифікованих ризиків та ключових індикаторів ризику (Key Risk Indicators – KRI). Така матриця дозволяє забезпечити системний зв'язок між виявленими ризиками, стратегічними цілями підприємства, допустимими межами ризик-апетиту і комплексом управлінських заходів, спрямованих на підтримання належного рівня економічної безпеки (табл. 1.3).

Таблиця 1.3

Аналітична матриця взаємозв'язку показників стійкості підприємства, ризиків та ключових індикаторів ризику

Тип стійкості	Ключові ризики	Показники моніторингу ризиків (ключові індикатори ризику, KRI)	Допустимий поріг (толерантність)	Міри реагування
1	2	3	4	5
Економічна	Недостатній рівень ліквідності підприємства, що обмежує його здатність виконувати короткострокові фінансові зобов'язання; значні коливання валютних курсів, які можуть призводити до зростання витрат і зниження прибутковості діяльності.	1. Коефіцієнт поточної ліквідності (відношення оборотних активів до короткострокових зобов'язань), який відображає здатність підприємства виконувати зобов'язання у найближчому періоді; 2. Частка валютних витрат у загальних витратах підприємства як показник залежності від валютних коливань.	Коефіцієнт поточної ліквідності $\geq 1,2$ (що свідчить про належний рівень платоспроможності); Частка валютних витрат у загальних витратах $\leq$ встановленого порогу (визначається політикою ризик-менеджменту підприємства).	Залучення резервних кредитних ліній для підвищення фінансової гнучкості; хеджування валютних ризиків за допомогою фінансових інструментів (форвардні та ф'ючерсні контракти, опціони); диверсифікація джерел постачання та використання валютної виручки для природного хеджування ризиків.
Технічна	Збої у функціонуванні виробничих потужностей підприємства, що можуть призвести до простоїв у виробничому циклі; надмірна зношеність або відсутність резервного обладнання, яка збільшує ризик тривалих зупинок виробництва.	1. Середній час відновлення після збоїв (Mean Time to Repair — MTTR) як показник оперативності усунення технічних проблем; 2. Коефіцієнт відмов обладнання (кількість відмов на одиницю часу), що характеризує надійність виробничих потужностей.	MTTR ≤ 4 години; Коефіцієнт відмов обладнання не перевищує визначеного внутрішнього стандарту (залежно від специфіки виробництва).	Резервування обладнання для забезпечення безперервності виробництва; впровадження програм превентивного та предиктивного технічного обслуговування; модернізація критично важливих елементів виробничої інфраструктури.

Продовження табл. 1.3

1	2	3	4	5
Цифрова	Кіберінциденти (несанкціонований доступ до інформаційних ресурсів, атаки з метою виведення з ладу систем), витік або втрата конфіденційних даних, що можуть негативно вплинути на безперервність бізнес-процесів і репутацію підприємства.	1. Кількість зареєстрованих кіберінцидентів протягом кварталу; 2. Відсоток критично важливих оновлень безпеки (патчів), встановлених у встановлені строки.	Кількість кіберінцидентів ≤ 2 на квартал; Відсоток своєчасно встановлених критичних патчів ≥ 95 %.	Впровадження систем управління інформаційною безпекою та подіями (SIEM – Security Information and Event Management), які забезпечують збір, аналіз і кореляцію подій із різних джерел інформаційної безпеки. Створення центрів операцій інформаційної безпеки (SOC – Security Operations Center) для безперервного моніторингу ІТ-інфраструктури підприємства, швидкого виявлення й усунення інцидентів безпеки. Проведення регулярного тестування на проникнення для виявлення вразливостей та підвищення обізнаності персоналу щодо кіберзагроз.

Продовження табл. 1.3

1	2	3	4	5
Енергоефективна	Зростання витрат на енергоносії, що безпосередньо впливає на собівартість продукції; низька ефективність використання енергоресурсів у виробничих процесах, яка знижує конкурентоспроможність підприємства.	1. Енергоємність продукції (обсяг спожитої енергії на одиницю продукції), що характеризує ефективність енергоспоживання; 2. Частка витрат на енергоносії у загальній собівартості продукції як показник залежності від цінкових коливань на енергоринку.	Допустимий поріг енергоємності продукції встановлюється підприємством залежно від галузі та технологічних особливостей. Наприклад, для підприємств із низьким рівнем енергоємності орієнтовне значення може становити $\leq 0,8 \text{ кВт} \cdot \text{год}$ на одиницю продукції; Частка витрат на енергоносії не перевищує встановленого внутрішнього нормативу.	Інвестування в енергоефективні технології та обладнання, модернізація виробничих процесів; впровадження систем енергоменеджменту відповідно до стандарту ISO 50001 «Системи енергетичного менеджменту». Вимоги та настанови щодо використання», які дозволяють забезпечити систематичне планування, моніторинг і підвищення ефективності енергоспоживання на підприємстві.
Інноваційна	Втрата конкурентних позицій через низьку інноваційну активність підприємства, використання застарілих технологій і продуктів, що не відповідають вимогам ринку	1. Частка витрат на дослідження та розробки у загальній виручці підприємства; 2. Кількість нових продуктів чи технологій, введених на ринок протягом року.	Витрати на дослідження та розробки $\geq 5 \%$ від виручки підприємства; Виведення щонайменше одного нового продукту або технології щорічно	Розвиток партнерств із науковими установами та стартапами, участь у державних і міжнародних програмах підтримки інноваційної діяльності; створення внутрішніх інноваційних інкубаторів.

Джерело: узагальнено автором на основі [20; 21; 22; 26; 31; 32; 33; 35].

Побудова матриці відповідності типів стійкості, ризиків і ключових індикаторів ризику (KRI) дозволяє систематизувати ризики відповідно до стратегічних і операційних цілей підприємства та створити прозору систему пріоритизації заходів реагування. Це підвищує ефективність прийняття управлінських рішень та оптимізує використання ресурсів. Матриця також слугує основою для визначення рівня ризик-апетиту підприємства, дозволяє відстежувати динаміку KRI та пов'язувати їх із показниками ефективності діяльності (Key Performance Indicators – KPI), що забезпечує збалансоване управління ризиками у довгостроковій перспективі.

Відстеження динаміки KRI здійснюється через формалізований моніторинг і порівняння фактичних значень із визначеними порогоми толерантності. Для цього застосовуються методи трендового аналізу, сценарного моделювання та автоматизовані інформаційно-аналітичні системи (дашборди), що дозволяють у режимі реального часу фіксувати відхилення показників і сигналізувати про зростання ризику. Інтеграція KRI із KPI реалізується шляхом побудови причинно-наслідкових зв'язків, які відображають вплив зміни KRI на досягнення ключових фінансових та нефінансових цілей підприємства. Наприклад, зростання KRI «середній час простою обладнання» прямо корелює зі зниженням KPI «обсяг виробництва» та «прибутковість», що дозволяє керівництву своєчасно вживати коригувальних заходів. Такий підхід формує систему раннього попередження відхилень у досягненні стратегічних показників, підвищує обґрунтованість управлінських рішень і забезпечує узгодження управління ризиками із загальною стратегією розвитку підприємства.

З метою наочного відображення ролей і зон відповідальності учасників ризик-орієнтованого управління безпекою (РОУБ) підприємства доцільно представити його організаційну структуру у форматі логічної моделі (рис. 1.2). Використання концепції «трьох ліній захисту» (The IIA's Three Lines Model), розробленої Інститутом внутрішніх аудиторів [26], дозволяє систематизувати відносини між керівним органом, менеджментом, функціями

ризик-менеджменту і внутрішнього аудиту, підкресливши принципи підзвітності, незалежності й узгодженості дій.

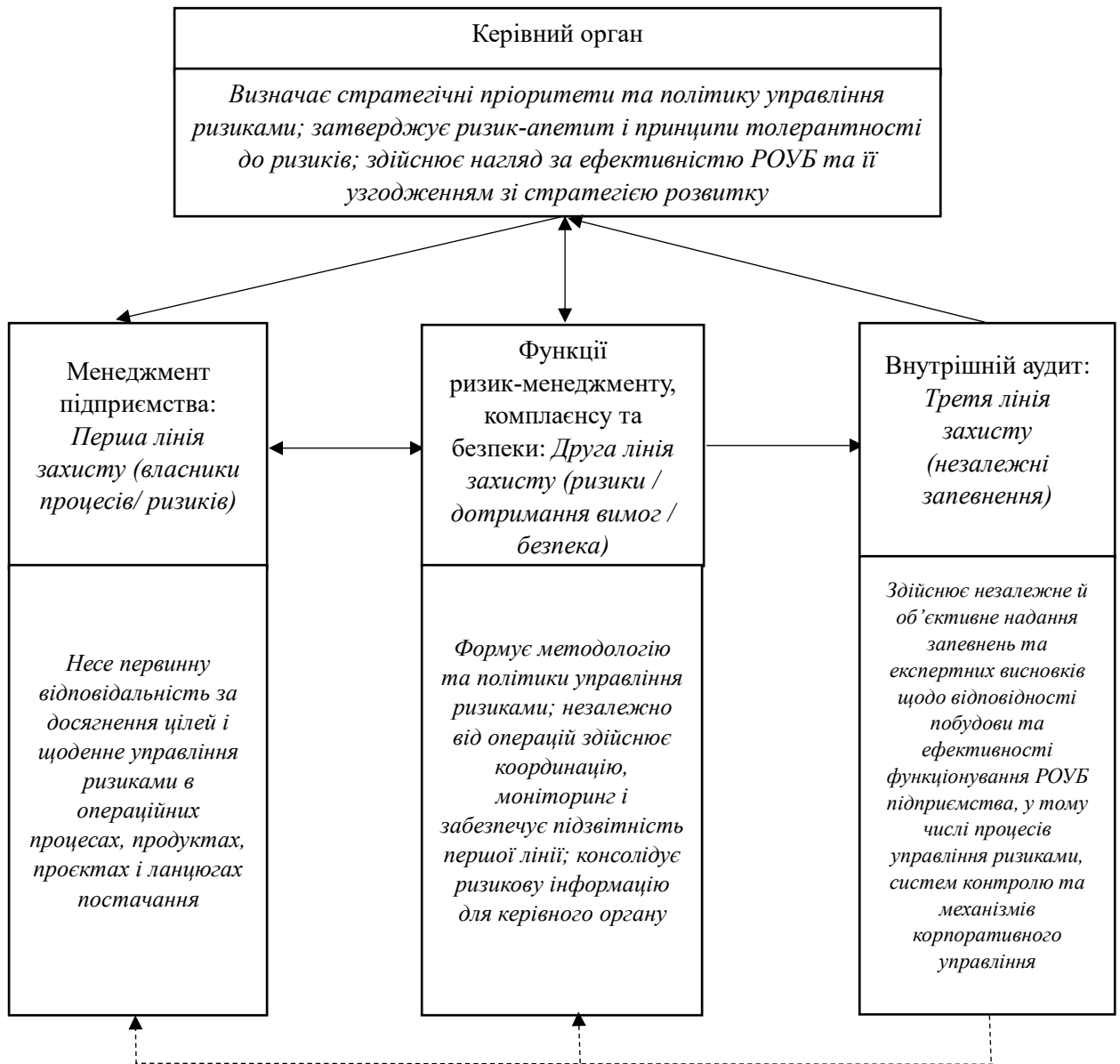


Рис. 1.2. Організаційна структура ризик-орієнтованої системи управління безпекою підприємства на основі логічної моделі трьох ліній захисту

Джерело: узагальнено автором на основі [21; 26].

Поданий вище рисунок відображає розподіл повноважень, інформаційних потоків та механізмів контролю між чотирма ключовими елементами ризик-орієнтованого управління безпекою підприємства: керівним

органом (наглядовою радою або комітетом з ризиків), менеджментом підприємства (першою лінією захисту), функціями ризик-менеджменту, комплаєнсу та безпеки (другою лінією захисту) і внутрішнім аудитом (третьою лінією захисту). Така модель створює основу для чіткого визначення ролей, мінімізації конфліктів інтересів і побудови ефективної системи запевнень у сфері економічної безпеки підприємства.

Процесна складова ризик-орієнтованого управління безпекою підприємства охоплює повний цикл управління ризиками, який забезпечує системність і безперервність цього процесу. Згідно з міжнародними стандартами та методичними рекомендаціями, до ключових етапів цього циклу належать: ідентифікація ризиків, їх кількісна та якісна оцінка, розроблення і впровадження заходів реагування, безперервний моніторинг ризикового середовища та регулярний перегляд відповідних процесів і процедур [21; 34]. Зазначений підхід дозволяє інтегрувати управління ризиками у стратегічне й операційне планування, забезпечуючи узгодженість цілей безпеки з загальними бізнес-цілями підприємства.

Не менш важливим елементом РОУБ є впровадження документованих процедур та планів, які визначають дії персоналу в умовах виникнення критичних інцидентів або кризових ситуацій. До таких документів належать:

1. плани реагування на інциденти, які описують алгоритм дій у разі виявлення або реалізації ризикової події з метою мінімізації її негативних наслідків;
2. плани безперервності діяльності, розроблені відповідно до вимог ДСТУ EN ISO 22301:2021, які визначають заходи, необхідні для збереження критично важливих бізнес-процесів у випадку серйозних збоїв або зовнішніх впливів [24];
3. плани відновлення після катастроф, що деталізують порядок відновлення функціонування інформаційних систем, виробничих потужностей та інших ключових ресурсів підприємства після надзвичайних подій.

Переконані, що ключовою передумовою ефективності РОУБ є формування корпоративної культури ризику, яка охоплює усвідомлене ставлення працівників до ризиків, розуміння ними ролі кожного в управлінні ризиками, дотримання затверджених політик і підзвітність на всіх рівнях організаційної ієрархії. Розвиток такої культури потребує реалізації комплексних заходів, серед яких особливе значення мають систематичне навчання персоналу, регулярні тренінги з управління ризиками та моделювання кризових ситуацій (стрес-тестування), які дозволяють відпрацювати алгоритми реагування у контрольованих умовах.

У сучасних умовах цифровізації одним із пріоритетів РОУБ є інтеграція його процесів в автоматизовані інформаційні системи управління підприємством, що забезпечує безперервний моніторинг ключових індикаторів ризику (KRI) та ключових показників ефективності діяльності (KPI). Такі інтегровані системи дозволяють оперативно ідентифікувати відхилення від установлених порогів толерантності та своєчасно коригувати заходи реагування залежно від змін зовнішнього й внутрішнього середовища.

Узагальнення результатів аналітичної матриці взаємозв'язку показників стійкості, ризиків та ключових індикаторів ризику (KRI) дозволяє перейти від їх ізольованого розгляду до формування цілісного підходу до управління економічною безпекою підприємства. Зокрема, встановлений взаємозв'язок між параметрами ефективності діяльності та рівнем ризиків обґрунтовує доцільність застосування ризик-орієнтованого підходу як базового принципу побудови сучасної системи економічної безпеки.

У цьому контексті економічна безпека підприємства перестає розглядатися як статичний стан захищеності та набуває ознак динамічної системи управління, що передбачає безперервну ідентифікацію, оцінювання, моніторинг і мінімізацію ризиків із одночасною орієнтацією на досягнення стратегічних цілей розвитку. Інтеграція ризик-орієнтованого підходу у систему стратегічного планування забезпечує узгодження цілей, ресурсів і управлінських рішень в умовах цифрової трансформації економіки.

Таким чином, результати проведеного теоретико-методологічного узагальнення, систематизації ризиків, обґрунтування типології стійкості та розвитку інструментарію ризик-орієнтованого управління створюють підґрунтя для формування концептуального бачення економічної безпеки підприємства як інтегрованої, багаторівневої та адаптивної системи. Візуалізація зазначеного підходу представлена у вигляді концептуальної моделі економічної безпеки підприємства в умовах цифровізації (рис. 1.3).

Таким чином, запропонована концептуальна модель відображає трансформацію підходу до розуміння економічної безпеки підприємства від статичного трактування як стану захищеності до інтегрованої, динамічної та адаптивної системи управління. На відміну від традиційних підходів, у моделі акцентовано взаємозв'язок між ризиками, параметрами стійкості та показниками ефективності діяльності, що забезпечує можливість комплексного оцінювання рівня економічної безпеки з урахуванням впливу внутрішніх і зовнішніх чинників, зокрема цифрових ризиків. Інтеграція ризик-орієнтованого підходу у систему стратегічного управління підприємством дозволяє забезпечити узгодженість управлінських рішень, ресурсного забезпечення та цільових орієнтирів розвитку. Це, у свою чергу, формує підґрунтя для підвищення стійкості підприємства, його здатності до адаптації в умовах цифрової трансформації та досягнення довгострокових стратегічних цілей.

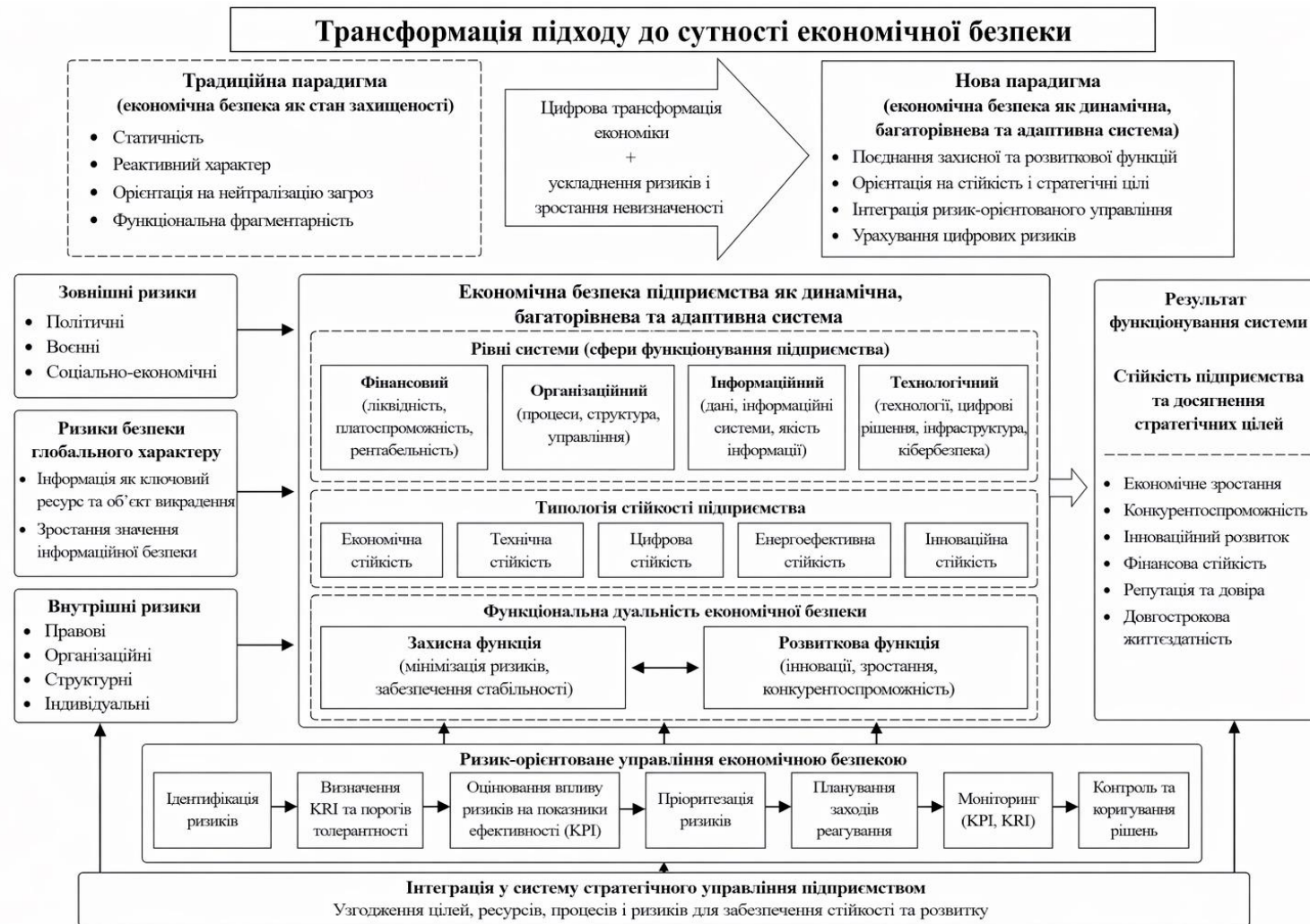


Рис. 1.3. Концептуальна модель економічної безпеки підприємства в умовах цифрової трансформації

Джерело: авторська розробка.

1.2. Система індикаторів та цифровий моніторинг економічної безпеки підприємства

Оцінювання економічної безпеки підприємства у сучасних умовах функціонує як ключова управлінська функція, що забезпечує стійкість суб'єкта господарювання до екзогенних і ендогенних ризиків, а також здатність до самозбереження та розвитку в умовах невизначеності. Цей процес охоплює системну діагностику потенційних загроз і вразливостей підприємства, моніторинг поточного стану за ключовими сферами безпеки (фінансовою, інформаційною, виробничою тощо), виявлення латентних ризиків і формування обґрунтованих управлінських рішень. У стратегічному контексті оцінювання економічної безпеки підприємства виконує функцію інформаційної підтримки прийняття рішень щодо пріоритетів розвитку, інвестицій, розподілу ресурсів та управління ризиками.

Цілісна система оцінювання економічної безпеки є інтегрованим компонентом стратегічного управління. Вона забезпечує зворотний зв'язок між встановленими стратегічними цілями підприємства, допустимим рівнем ризику, впливом регуляторних і ринкових чинників, а також результатами реалізованих заходів безпеки. Методичне осмислення цього процесу передбачає врахування трьох взаємопов'язаних рівнів:

- 1). концептуального – розуміння безпеки як багатовимірного стану;
- 2). інструментального – формування системи індикаторів і моделей оцінювання;
- 3). операційного – інтеграція процесів аналізу, моніторингу та реагування у щоденну діяльність підприємства.

Оцінювання економічної безпеки підприємства ґрунтується на сукупності принципів, які забезпечують цілісність, наукову обґрунтованість та адаптивність аналітичного підходу. У таблиці 1.4 представлено узагальнення ключових принципів, що мають бути враховані під час розроблення методики

оцінювання рівня економічної безпеки підприємства в умовах цифрової трансформації та зростання ризикогенності бізнес-середовища.

Таблиця 1.4

Ключові принципи оцінювання економічної безпеки підприємства

Принцип 1	Сутність принципу 2	Джерела 3
Комплексність	Комплексність означає необхідність охоплення всіх функціональних складових економічної безпеки підприємства: фінансової, виробничо-операційної, кадрової, інформаційної, інноваційної, ринкової. Важливим є також урахування взаємозалежностей між зазначеними складовими, що дозволяє ідентифікувати мультиплікативні ризики та посилення їхнього впливу внаслідок каскадних ефектів.	OECD-JRC, ДСТУ ISO 31000:2018
Системність	Системність передбачає інтеграцію процесу оцінювання економічної безпеки в загальну систему управління підприємством. Це означає логічне поєднання оцінки з функціями стратегічного планування, ризик-менеджменту, контролінгу та внутрішнього аудиту, що забезпечує послідовність і зворотний зв'язок між виявленими ризиками, управлінськими рішеннями та результатами їх реалізації.	COSO ERM, NIST CSF 2.0
Динамічність	Динамічність означає здатність методики до адаптації в умовах часової мінливості та нестабільності зовнішнього середовища. Методика має враховувати сезонні коливання, циклічність ринків, появу нових загроз і необхідність оперативного реагування на зміни, використовуючи інструменти моніторингу в реальному часі та сценарного аналізу.	OECD-JRC, COSO ERM
Адаптивність до цифрових викликів	Адаптивність до цифрових викликів полягає у спроможності методики враховувати зростаючу роль інформаційних технологій у структурі підприємства. Йдеться про інтеграцію цифрових ризиків, таких як порушення функціонування інформаційних систем, витоки даних, атаки на інфраструктуру, до контексту економічної безпеки та про необхідність оновлення індикаторів відповідно до рівня цифровізації.	NIST CSF 2.0, ДСТУ ISO/IEC 27001:2023

Джерело: узагальнено автором на основі [20; 21; 23; 25; 35;31].

Комплексність є базовим методичним принципом, що передбачає охоплення усіх функціональних підсистем підприємства у межах оцінювання економічної безпеки. Зокрема, до сфери уваги мають бути включені фінансова, виробничо-операційна, інформаційна, кадрова, інноваційна та ринкова складові. Такий підхід дозволяє здійснювати повну діагностику системи підприємства з позиції його стійкості до зовнішніх і внутрішніх загроз.

Особливої значущості цей принцип набуває в умовах динамічного бізнес-середовища, коли між окремими функціональними зонами безпеки виникають складні взаємозв'язки, здатні провокувати мультиплікативні ефекти. Ігнорування навіть одного зі складників безпеки здатне знизити загальний рівень захищеності підприємства, що обґрунтовує необхідність інтегративного підходу до побудови системи індикаторів та їх оцінювання.

Системність означає включення оцінювання економічної безпеки до загальної управлінської архітектури підприємства. Така інтеграція передбачає узгодженість з функціями стратегічного планування, бюджетування, ризик-менеджменту, внутрішнього контролю, аудиту та антикризового управління. Оцінка не повинна бути автономним процесом, а має забезпечувати постійний зворотний зв'язок між аналізом ризиків та прийняттям управлінських рішень.

Реалізація принципу системності дозволяє побудувати цілісну модель корпоративної безпеки, в якій кожен її елемент є функціонально взаємопов'язаним з іншими, а процес оцінювання виконує функцію інформаційного забезпечення управління ризиками. Такий підхід відповідає вимогам концепцій COSO ERM (Концептуальна модель інтегрованого управління ризиками, розроблена Комітетом організацій-спонсорів Комісії Тредвея) [23] та сучасних моделей корпоративного ризик-менеджменту.

Динамічність як методичний принцип передбачає врахування мінливості факторів зовнішнього та внутрішнього середовища. Економічна безпека не є сталою категорією – вона змінюється під впливом сезонності, технологічних зрушень, змін у поведінці споживачів, законодавчих новацій, а також

політичної або фінансової нестабільності. Тому система оцінювання повинна мати гнучкість до постійного оновлення параметрів та сценаріїв оцінки.

Дотримання принципу динамічності обумовлює потребу у впровадженні аналітичних інструментів, що забезпечують аналіз у реальному часі, передбачення сценаріїв та їх періодичний перегляд. У цьому контексті особливого значення набувають цифрові інструменти моніторингу, автоматизовані індикаторні панелі та адаптивні моделі прийняття рішень.

Адаптивність до цифрових викликів означає здатність методики оцінювання економічної безпеки трансформуватись відповідно до зростаючого значення інформаційних технологій у функціонуванні підприємства. Зокрема, йдеться про врахування нових типів загроз – кіберінцидентів, збоїв у роботі критичних цифрових платформ, порушення конфіденційності та цілісності даних, що безпосередньо впливають на стабільність бізнес-процесів.

Цей принцип передбачає не лише включення цифрових ризиків до структури оцінки, але й використання сучасних ІТ-рішень для збору, обробки й візуалізації даних про безпекову ситуацію. Інтеграція адаптивних індикаторів, цифрових слідів ризиків і автоматизованих систем попередження дозволяє оперативно реагувати на загрози нового покоління та підтримувати належний рівень інформаційної і техногенної безпеки підприємства.

Зазначені принципи слугують основою для розробки ефективної методики оцінювання, здатної не лише відображати поточний стан безпеки, але й прогнозувати ймовірність реалізації ризиків за різними сценаріями розвитку. Можемо зробити висновок, що методичні основи оцінювання економічної безпеки підприємства мають поєднувати класичні принципи системного аналізу з новітніми технологіями моніторингу, візуалізації й адаптації. Лише така інтегративна модель дозволить адекватно реагувати на виклики динамічного, цифрово-орієнтованого бізнес-середовища та забезпечити стійкий розвиток підприємства у довгостроковій перспективі.

Оцінювання економічної безпеки підприємства передбачає застосування комплексу кількісних та якісних інструментів, що забезпечують системний підхід до виявлення загроз, оцінки ризиків та обґрунтування управлінських рішень в умовах динамічного й часто турбулентного середовища. Використання відповідного інструментарію дає змогу забезпечити не лише ретроспективний аналіз стану безпеки, а й побудову прогностичних моделей з урахуванням змін у фінансовому, виробничому та зовнішньому середовищі.

До традиційних кількісних методів належать фінансово-економічні коефіцієнти, що охоплюють показники ліквідності, рентабельності, платоспроможності, фінансової автономії та ділової активності. Ці індикатори дозволяють оцінити ступінь фінансової стійкості, ефективності ресурсного використання та здатності підприємства функціонувати у кризових умовах. Наприклад, у роботі Чумаченко О. і Нескородька О. обґрунтовано використання симуляційного підходу до оцінювання ризиків на основі методу Монте-Карло, що є імітаційною процедурою багаторазового моделювання з урахуванням випадкових параметрів [36].

Метод Монте-Карло дає змогу моделювати поведінку системи у відповідь на зміни зовнішніх і внутрішніх чинників, оцінюючи ймовірності розвитку негативних сценаріїв. Це особливо важливо для прийняття рішень у ситуаціях із високою невизначеністю. За даними дослідження, методика ефективно застосовується в процесі обґрунтування інвестиційних рішень, оцінки надійності фінансових потоків та формування ризик-профілю підприємства [36].

Особливу увагу заслуговує модель імітаційного моделювання ризиків інвестиційних проєктів, розроблена Латишевою О. В. та Тетеренко Т. С., яка дозволяє оцінити вплив ключових змінних на результати проєкту (зокрема, чистий дисконтований дохід, строк окупності, індекс прибутковості), використовуючи систему багаторазових симуляцій. Дослідники підкреслюють, що в умовах нестабільного ринкового середовища саме імітаційне моделювання здатне виявити критичні комбінації факторів, які

можуть спричинити втрату безпечного рівня функціонування підприємства [37]. Таким чином, цей метод доцільно інтегрувати у систему стратегічного управління безпекою підприємства, особливо на етапі інвестиційного планування.

Крім того, вагоме значення мають інтегральні індекси, які дозволяють об'єднати множину часткових показників у єдиний узагальнений критерій безпеки. Формування композитного індексу можливе через нормування значень, використання вагових коефіцієнтів, визначених експертним або статистичним шляхом, а також застосування методів таксономії.

У ситуаціях, коли кількісні дані є недостатніми або неоднозначними, важливу роль відіграють якісні методи аналізу. Серед них слід виокремити SWOT-аналіз – метод стратегічного аналізу, що ідентифікує сильні та слабкі сторони підприємства, а також можливості й загрози у зовнішньому середовищі. Аналіз PESTEL (політичні, економічні, соціальні, технологічні, екологічні та правові чинники) дозволяє оцінити макроекономічне середовище і виявити зовнішні детермінанти ризиків [38].

Як засвідчує дослідження Богданюка І. В. та Мандича С. М., якісний аналіз PESTEL може бути інтегрований із інструментами управління ризиками (наприклад, FMEA – аналіз способів і наслідків відмов), що дозволяє ідентифікувати критичні точки впливу в умовах цифрових трансформацій та кіберзагроз [39]. Автори підкреслюють актуальність цих підходів у процесі адаптації управлінських рішень до нових умов, зокрема змін у політичному та правовому полі, інфляційних тенденцій, нестабільності попиту тощо.

Сучасні виклики цифрової трансформації зумовлюють необхідність інтеграції автоматизованих інструментів збору, обробки та візуалізації інформації в контекст управління економічною безпекою підприємства. Впровадження корпоративних систем управління бізнес-процесами – зокрема Enterprise Resource Planning (ERP, системи планування ресурсів підприємства) та Business Intelligence (BI, інструменти бізнес-аналітики) – забезпечує можливість збору і аналізу великих обсягів даних у режимі реального часу. Це

дозволяє формувати індикатори раннього попередження, автоматично виявляти операційні відхилення, зменшувати вплив людського фактора та оперативно реагувати на критичні сигнали.

Згідно із дослідженням Лігоненко Л. О., системи ERP та BI-платформи спроможні трансформувати управлінську архітектуру підприємства. Вони забезпечують прозорість бізнес-процесів, автоматизацію збору ключових показників (KPI, Key Performance Indicators), візуалізацію інформації у вигляді інтерактивних панелей (дашбордів) та реалізацію механізмів адаптивного реагування на ризики. Автор підкреслює, що цифрова культура підприємства, розвиток управлінських компетенцій і підтримка державних інституцій є критично важливими для успішного впровадження таких платформ [40].

Поєднання якісного аналізу з технологіями штучного інтелекту та машинного навчання сприяє підвищенню чутливості систем безпеки до слабких сигналів. Наприклад, методи машинного навчання – як класифікаційні, так і аномалійно-орієнтовані – допомагають автоматично ідентифікувати нетипову поведінку систем або процесів, котра може бути попередником кризової ситуації. Особливо актуальними такі методи стають для операційних центрів безпеки (Security Operations Centers), де постійний моніторинг подій вимагає аналізу величезних обсягів логів, поведінкових патернів та мережевих сигналів [39].

Поєднання експертних оцінок (аналіз сильних і слабких сторін, можливостей і загроз, а також політичного, економічного, соціального, технологічного, екологічного та правового середовища) із алгоритмами машинного навчання значно підвищує точність ідентифікації слабких сигналів загроз і оптимізує стратегії управління економічною безпекою. Машинне навчання дозволяє класифікувати події за рівнем ризику та прогнозувати потенційну ескалацію інцидентів на основі історичних даних.

Крім того, актуальним є підхід до побудови аналітичних систем управління економічною безпекою у цифровому середовищі – як, наприклад, описано у роботі Іванової Н. С., де запропоновано комплексну архітектуру

системи, що включає методичне, інформаційне, технічне та кадрове забезпечення. Важливою функцією таких систем є інтеграція ERP/BI-рішень із модулями ризик-менеджменту, аналізу сценаріїв, моніторингу кіберзагроз та автоматизованого реагування [41].

З огляду на вищевикладене, методичний інструментарій оцінювання економічної безпеки підприємства в умовах цифрової трансформації має містити:

- ✓ автоматизований збір даних із ERP-, BI-, GRC- (Governance, Risk and Compliance) та CRM- (Customer Relationship Management) систем;
- ✓ алгоритми машинного навчання для виявлення аномалій і прогнозування ризиків;
- ✓ інтерактивну візуалізацію через інтерактивні панелі для оперативного реагування;
- ✓ блоки аналізу сценаріїв та моделей попередження збоїв на основі аналізу критичних точок (FMEA – Failure Mode and Effects Analysis) у рамках цифрового ризик-менеджменту.

Формування системи індикаторів економічної безпеки підприємства в умовах цифрової трансформації є критичним елементом аналітичного забезпечення стратегічного управління. Індикатори виступають операційним інструментом діагностики, що дозволяє оперативно реагувати на зміну внутрішнього і зовнішнього середовища, своєчасно виявляти деструктивні тренди та адаптувати систему управління до нових викликів. Особливого значення набуває розробка гнучкої індикативної моделі, що охоплює не лише традиційні сфери (фінансова, виробнича, кадрова), а й новітні – зокрема інформаційну безпеку, рівень цифрової інтегрованості, стійкість до кіберзагроз і репутаційні ризики в цифровому середовищі [42].

Методичне підґрунтя формування системи індикаторів оцінювання економічної безпеки підприємства передбачає опору на низку ключових принципів, що забезпечують її наукову обґрунтованість, практичну придатність і стійкість до змін зовнішнього середовища. Передусім, це

принцип *релевантності* (відповідність індикаторів дійсним загрозам і викликам, характерним для конкретного підприємства), принцип *достатності* (вичерпне охоплення ключових сфер економічної безпеки без надмірної деталізації), *відтворюваності* (можливість періодичного вимірювання індикаторів з однаковими методами і засобами) та *цифрової доступності* (наявність автоматизованих джерел для збирання і обробки даних). Зокрема, мова йде про інтеграцію даних з таких систем, як ERP (Enterprise Resource Planning – планування ресурсів підприємства), CRM (Customer Relationship Management – управління відносинами з клієнтами), HRM (Human Resource Management – управління людськими ресурсами), BI (Business Intelligence – бізнес-аналітика).

Сукупність зазначених принципів формує методичну основу побудови адаптивної індикативної системи, здатної гнучко реагувати на цифрові виклики та динаміку ринкового середовища. Така система не лише дає змогу здійснювати оперативне оцінювання рівня економічної безпеки, а й виступає аналітичною платформою для ідентифікації ризиків, формування управлінських сценаріїв та прогнозування кризових ситуацій. Успішна реалізація зазначеного підходу передбачає одночасне дотримання стандартів уніфікації структури індикаторів і забезпечення їх адаптивності до галузевих та технологічних особливостей діяльності підприємства.

На практиці широко застосовується структуризація індикаторів за функціональними складниками економічної безпеки, зокрема фінансовим, кадровим, інноваційним, виробничим, інформаційним, екологічним тощо. Наприклад, для інформаційної безпеки можуть застосовуватись такі індикатори, як кількість зафіксованих кіберінцидентів, середній час реагування на загрозу, частка застарілих систем у загальній ІТ-архітектурі, а також наявність сертифікованих політик безпеки відповідно до стандартів ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги» [25]. У статті Цяпи С. М. справедливо акцентується увага на зростанні

уразливості до зовнішніх впливів у контексті цифрової інтеграції, зокрема у мережеских автономних системах, що актуалізує потребу у відповідних показниках стійкості [43].

Особливу увагу при побудові інтегральної системи оцінювання економічної безпеки підприємства слід приділяти методам агрегування часткових індикаторів у єдиний узагальнений показник. Така агрегація дозволяє не лише зменшити складність аналітичної оцінки, але й підвищити наочність моніторингу та полегшити процес ухвалення управлінських рішень. Серед найбільш поширених методів, що застосовуються в наукових і практичних підходах, варто виділити метод зваженого середнього, який передбачає множення нормованих значень індикаторів на задані вагові коефіцієнти; метод таксономії, заснований на визначенні відстані до умовного еталонного об'єкта за допомогою евклідової метрики; аналіз головних компонент (Principal Component Analysis – PCA), який дозволяє зменшити розмірність індикаторного простору, виділяючи найбільш інформативні фактори; а також методи нормування за еталонними значеннями, що передбачають порівняння фактичних показників із гранично допустимими або цільовими орієнтирами.

Значний науковий внесок у вдосконалення індикативного інструментарію здійснено у дослідженні Андріїв Н. М., де обґрунтовано доцільність використання комбінованого підходу до інтегрального оцінювання, що поєднує класичні індексні методики з алгоритмами інтелектуального аналізу даних (data mining – інтелектуальний пошук закономірностей у великих масивах інформації). Зокрема, авторка підкреслює, що використання кластерного аналізу, логістичної регресії та нейронних мереж дозволяє виявляти латентні (приховані) фактори ризику, які не піддаються традиційному кількісному аналізу, а також формувати адаптивні сценарії прогнозування рівня безпеки залежно від змін зовнішнього та внутрішнього середовища підприємства. Такий підхід сприяє підвищенню чутливості оцінювальної моделі до «слабких сигналів» – ранніх ознак

потенційних загроз, що є надзвичайно важливим у високодинамічному цифровому контексті функціонування бізнесу.

Крім того, у межах запропонованого комбінованого підходу авторкою було акцентовано на важливості врахування якісних чинників, зокрема рівня організаційної культури управління ризиками, цифрової грамотності персоналу та інституційної зрілості системи корпоративного контролю. Таке поєднання кількісних і якісних параметрів дозволяє створити комплексну модель оцінювання, придатну до застосування як у щоденному управлінні безпекою, так і в стратегічному плануванні [42].

Додаткову цінність у процесі оцінювання економічної безпеки підприємства становить візуалізація індикаторів за допомогою сучасних цифрових платформ бізнес-аналітики, таких як Power BI, Tableau та Qlik Sense. Використання цих інструментів дозволяє формувати інтерактивні панелі моніторингу, в яких дані оновлюються в режимі реального часу, а ключові індикатори можуть бути представлені в динаміці, із заданими пороговими значеннями та логікою автоматичного генерування попереджувальних сигналів. Такий підхід забезпечує не лише більш глибоке аналітичне опрацювання інформації, а й оперативність реагування на потенційні загрози, що особливо важливо в умовах високої турбулентності бізнес-середовища.

Згідно з результатами дослідження Кузьменко О. В., Сергєєвої О. Р. та Орлової В. М., впровадження інформаційних систем управління дозволяє досягти вагомих ефектів за рахунок централізованого збирання та обробки інформації, автоматизації звітності, підвищення прозорості операцій та зменшення людського чинника в ухваленні рішень. Автори підкреслюють, що використання цифрових аналітичних систем забезпечує адаптивність підприємств до змін зовнішнього середовища, підвищує якість стратегічного та оперативного планування, сприяє зростанню рівня обґрунтованості управлінських дій та знижує ризики суб'єктивних помилок [44].

Отже, інтеграція візуалізаційних інструментів у загальну архітектуру управління економічною безпекою дозволяє не лише структурувати великий

обсяг даних, а й сформувати єдину цифрову аналітичну екосистему, орієнтовану на проактивне виявлення загроз, забезпечення контролю ключових параметрів безпеки та їхню своєчасну корекцію.

Для комплексного оцінювання рівня економічної безпеки доцільно використовувати систему індикаторів, структуровану за ключовими функціональними складниками. У таблиці 1.5 подано деталізовану структуру таких індикаторів з урахуванням цифрових джерел збору даних.

Таблиця 1.5

Структура індикаторів економічної безпеки підприємства за функціональними складниками

Функціональний складник економічної безпеки	Ключові індикатори оцінювання	Джерела отримання інформації
1	2	3
Фінансова безпека	Коефіцієнти абсолютної, швидкої та поточної ліквідності; показники фінансової стійкості; рентабельність активів та капіталу; рівень платоспроможності; коефіцієнт фінансового важеля	Фінансова звітність підприємства; модулі фінансового обліку ERP-систем; аудиторські висновки
Виробнича безпека	Продуктивність праці; коефіцієнт технічної готовності основних фондів; частка бракованої продукції; рівень використання виробничих потужностей	Виробничі журнали; системи диспетчерського управління (SCADA); MES-системи (системи диспетчеризації виробництва); звіти технічного нагляду
Інформаційна безпека	Кількість кіберінцидентів; частота оновлення антивірусного та серверного ПЗ; ступінь відповідності стандартам ДСТУ ISO/IEC 27001:2023. «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги»; показник внутрішніх витоків інформації	Системи інформаційної безпеки (SIEM); журнали аудиту безпеки; звіти служб IT і кіберзахисту
Кадрова безпека	Коефіцієнт плинності персоналу; індекс внутрішньої мотивації; рівень професійної підготовки; відсоток персоналу, залученого до безперервного навчання	Звіти HRM-систем; результати внутрішніх опитувань; статистика з підвищення кваліфікації персоналу

Продовження табл. 1.5

1	2	3
Інноваційна безпека	Частка витрат на дослідження й розробки у структурі загальних витрат; кількість упроваджених інновацій; індекс патентної активності; темп оновлення продукції	CRM-системи; звіти інноваційних підрозділів; національні реєстри патентів; управлінський облік
Екологічна безпека	Рівень викидів шкідливих речовин; обсяг утилізованих відходів; частка впроваджених екотехнологій; відповідність сертифікації ДСТУ ISO 14001:2015 «Системи екологічного управління. Вимоги і керівництво до застосування»	Екологічна звітність; дані з датчиків моніторингу довкілля; звіти контролюючих органів
Соціальна безпека	Середній рівень заробітної плати; коефіцієнт задоволеності працівників умовами праці; частка соціальних витрат у загальній структурі витрат; показник внутрішньої комунікації	Анкетування персоналу; внутрішня соціальна звітність; звіти кадрової служби; колективні договори
Кібербезпека (цифрова стійкість)	Рівень проникнення загроз через мережеві протоколи; частота резервного копіювання даних; середній час простою інформаційних систем; частка інвестування в кіберзахист	Аналітика з SIEM-систем; звіти IT-департаменту; моніторинг кіберінцидентів

Джерело: авторська розробка.

Цифрова трансформація радикально змінює концептуальні та інструментальні засади оцінювання економічної безпеки підприємства. Запровадження цифрових рішень сприяє переходу від реактивної до проактивної моделі безпеки, в якій аналіз, діагностика, прогнозування та реагування на ризики здійснюються автоматизовано, з мінімізацією людського чинника. Цифрові технології забезпечують безперервний моніторинг внутрішніх і зовнішніх загроз, підвищуючи обґрунтованість управлінських рішень і швидкість реагування на критичні події.

Ключовими технологіями, які докорінно трансформують методику оцінювання економічної безпеки підприємства в умовах цифрової економіки, є великі дані (Big Data), штучний інтелект (Artificial Intelligence), машинне навчання, Інтернет речей (Internet of Things), технології обробки

неструктурованих даних, а також хмарні обчислення. Саме ці інструменти дозволяють здійснювати не лише постфактум-аналіз, а й проактивну діагностику ризиків із врахуванням динамічних змін у внутрішньому й зовнішньому середовищі функціонування підприємства.

Наприклад, методи аналізу великих даних дають змогу формувати прогностичні моделі на основі мільйонів спостережень, зібраних у реальному часі з телеметричних систем, цифрових слідів користувачів, журналів подій інформаційно-комунікаційних систем підприємства, поведінкових патернів персоналу, а також відкритих джерел. Це забезпечує глибину розуміння латентних загроз, таких як внутрішні порушення, аномалії поведінки працівників, невидимі у класичних облікових системах сигнали небезпеки. Технології обробки неструктурованих даних (зокрема текстових повідомлень, відео, аудіо) доповнюють кількісні індикатори якісними оцінками ризиків і посилюють аналітичну гнучкість систем.

Інтеграція рішень Інтернету речей дозволяє здійснювати постійний автоматизований моніторинг технічного стану обладнання, обробляючи сигнали з датчиків у режимі реального часу. Це критично важливо для забезпечення виробничої, енергетичної та технологічної безпеки, оскільки дає змогу виявляти ознаки потенційних відмов або аварій ще до їх фактичного настання та формувати відповідні запобіжні дії [40].

Важливу роль у побудові цифрової моделі безпеки відіграють інтегровані інформаційні платформи: системи планування ресурсів підприємства (Enterprise Resource Planning – ERP), платформи бізнес-аналітики (Business Intelligence – BI), інструменти управління ризиками, відповідністю та корпоративним управлінням (Governance, Risk and Compliance – GRC), а також рішення з управління інформаційною безпекою та подіями (Security Information and Event Management – SIEM). Усі ці системи виконують функцію об'єднання розрізнених джерел даних (фінансових, кадрових, виробничих, маркетингових, цифрових) в єдиний аналітичний простір, де забезпечується цілісний аналіз ситуацій і моделювання сценаріїв.

Особливої уваги заслуговує застосування систем бізнес-аналітики (Business Intelligence-систем), які дозволяють створювати інтерактивні панелі моніторингу, здійснювати візуалізацію ключових показників безпеки, відслідковувати динаміку змін, а також забезпечують зручну інтерфейсну взаємодію для менеджменту. Застосування таких систем дозволяє значно зменшити часові лаги між появою загрози і прийняттям відповідного управлінського рішення. У дослідженні Кузьменко О. В., Сергєєвої О. Р. та Орлової В. М. обґрунтовано, що впровадження інформаційних систем в управлінську практику торговельних підприємств знижує інерційність управлінських рішень, дозволяє оперативно адаптуватися до змін ринкових умов, а також оптимізувати ресурсне навантаження, підвищуючи загальну операційну ефективність суб'єктів господарювання в умовах високої ринкової турбулентності [44].

Цифрові панелі управління (dashboards) слугують інструментом інтеграції, візуалізації та оперативного моніторингу ключових індикаторів економічної безпеки підприємства. Вони надають можливість здійснювати централізоване спостереження за широким спектром показників, пов'язаних із фінансовою стійкістю, операційною стабільністю, інформаційною захищеністю, соціальною відповідальністю та екологічною безпекою. У межах таких панелей користувачі можуть встановлювати критичні порогові значення, налаштовувати автоматизовані механізми попереджень про відхилення від нормативних параметрів, а також проводити порівняльний аналіз у динаміці.

Використання сучасних платформ аналітики, таких як Power BI, Tableau, Qlik Sense, дає змогу реалізовувати глибоку багаторівневу візуалізацію, включаючи побудову кореляційних матриць, сценарних моделей, карт ризиків та теплових карт. Зокрема, функціонал таких систем підтримує виведення даних у режимі реального часу, фільтрацію за параметрами безпеки, а також формування інтерактивних моделей цільового профілю безпеки (тобто сукупності нормативних значень індикаторів, що відповідають стратегічним орієнтирам підприємства).

Крім того, інтеграція цифрових панелей з нормативно-методичними фреймворками, як-от рамкова модель кібербезпеки NIST CSF версії 2.0 (National Institute of Standards and Technology Cybersecurity Framework) [31], забезпечує уніфікацію підходів до управління ризиками, відповідність міжнародним стандартам і посилення контролю на всіх рівнях управління. У цьому контексті цифровізація постає не лише як виклик або зовнішній тренд, а як базисна складова трансформації управлінських технологій у сфері безпеки. Вона дозволяє здійснювати синтез класичних методів оцінювання з інструментами прогнозної та дескриптивної аналітики, що, у свою чергу, підвищує здатність підприємства до своєчасного виявлення латентних загроз і формування адаптивної стратегії реагування.

У сучасних умовах цифрової трансформації підприємства потребують впровадження інтегрованих систем моніторингу, здатних забезпечити виявлення, аналіз та реагування на ризики в реальному часі. Застосування цифрових платформ моніторингу економічної безпеки дозволяє централізувати контроль за ключовими індикаторами, мінімізувати вплив людського фактора та забезпечити проактивне управління загрозами. На рис. 1.4 представлено функціональну структуру такої системи, що відображає основні етапи цифрової обробки інформації та взаємозв'язки між модулями.

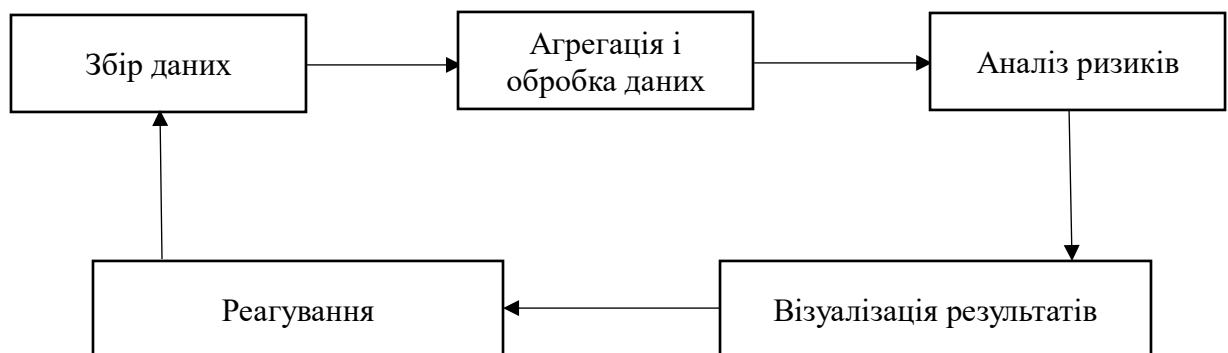


Рис. 1.4. Функціональна структура цифрової системи моніторингу економічної безпеки підприємства

Джерело: авторська розробка.

Система цифрового моніторингу економічної безпеки підприємства становить собою багаторівневу архітектуру, що забезпечує комплексне спостереження, аналіз та реагування на потенційні загрози у ключових сферах функціонування суб'єкта господарювання. Її функціональні компоненти логічно впорядковані за етапами обробки інформації – від первинного збору даних до реалізації керованого зворотного зв'язку.

Збирання даних (data collection) охоплює інтеграцію внутрішніх та зовнішніх джерел інформації. На цьому етапі використовуються як корпоративні інформаційні системи (системи планування ресурсів підприємства – ERP, системи управління виробництвом – MES, системи обліку та кадрів), так і сенсорна інфраструктура (датчики, телеметрія тощо), що забезпечують потокове надходження оперативних показників з фінансової, виробничої, кадрової, інформаційної, екологічної та інших сфер діяльності підприємства.

Агрегація, фільтрація та нормалізація даних відбувається в межах аналітичного модуля. Дані, отримані з різнотипних джерел, підлягають уніфікації, масштабуванню до єдиних інтервалів (зокрема за допомогою методів нормування або стандартизації), а також порівнянню з наперед встановленими нормативними чи пороговими значеннями. Це забезпечує можливість коректного міжпоказникового зіставлення та подальшого математичного агрегування у рамках комплексних індикаторів економічної безпеки.

Аналіз ризиків і прогнозування загроз реалізуються через використання сучасних аналітичних технологій, зокрема методів штучного інтелекту, машинного навчання, імітаційного моделювання (зокрема метод Монте-Карло), а також логіки систем виявлення аномалій. У структурі відповідного модуля функціонують підсистеми обробки інцидентів, побудови сценаріїв розвитку подій, а також формування ранніх попереджень на основі виявлених закономірностей.

Візуалізація результатів моніторингу здійснюється через інтерактивні панелі управління (інтерфейси типу dashboard), що дають змогу приймати оперативні управлінські рішення на основі об'єктивної аналітичної інформації. Важливо, що панелі налаштовуються відповідно до ієрархії користувачів – від оперативного персоналу до стратегічного менеджменту – з урахуванням специфіки їхніх інформаційних потреб.

Модуль реагування та підтримки рішень є завершальною ланкою системи, який забезпечує не лише фіксацію інцидентів, а й формування рекомендованих дій, автоматизоване оповіщення відповідальних осіб, а також – за потреби – ініціювання зворотного впливу на контрольовані підсистеми. Завдяки цьому забезпечується не лише інформування, а й безпосередня участь цифрової системи у процедурі управління безпекою підприємства.

Узагальнено, така цифрова система моніторингу виступає не просто інструментом обліку та контролю, а адаптивним середовищем для виявлення, аналізу та нейтралізації ризиків у реальному часі. Її впровадження сприяє трансформації системи управління економічною безпекою підприємства з реактивної на проактивну, що є критично важливим в умовах зростання швидкості змін у зовнішньому середовищі.

Інструментарій цифрового моніторингу охоплює широкий спектр програмно-аналітичних платформ, які інтегрують функції збору, обробки, аналізу та візуалізації інформації з різних сфер діяльності підприємства.

У таблиці 1.6 представлено основні класи цифрових технологій, які застосовуються в практиці побудови систем управління економічною безпекою. Для кожної технології наведено її функціональне призначення та приклади інструментів, що засвідчили свою ефективність у корпоративному середовищі.

Таблиця 1.6

**Цифрові технології моніторингу економічної безпеки підприємства:
функціональне призначення та приклади застосування**

Цифрова технологія	Функціональне призначення	Приклад інструментів
1	2	3
Big Data (великі дані)	Обробка великих обсягів структурованих і неструктурованих даних для виявлення закономірностей, трендів і потенційних ризиків.	Apache Hadoop, Apache Spark, Cloudera
Штучний інтелект	Застосування алгоритмів машинного навчання для аналізу даних, прогнозування загроз і автоматизації рішень.	IBM Watson, Azure Machine Learning, TensorFlow
Інтернет речей (Internet of Things)	Мережа пристроїв і сенсорів, які забезпечують збір оперативної інформації з фізичного середовища у реальному часі.	Siemens MindSphere, PTC ThingWorx, Bosch IoT Suite
ERP-системи (Enterprise Resource Planning)	Інтеграція всіх функціональних підрозділів підприємства в єдину систему для забезпечення прозорості процесів та ефективного управління ресурсами.	SAP ERP, Oracle NetSuite, Microsoft Dynamics 365
BI-системи (Business Intelligence)	Системи, що надають можливість аналітичного моніторингу та візуалізації ключових показників для підтримки прийняття рішень.	Power BI, Tableau, Qlik Sense

Джерело: узагальнено автором на основі [45–50].

Варто підкреслити, що інтеграція цифрових технологій у процеси моніторингу економічної безпеки підприємства є не просто інструментальним оновленням операційної діяльності, а суттєвим етапом стратегічного управління ризиками в умовах цифрової трансформації. Сучасні цифрові платформи – BI-системи, ERP-платформи, SIEM-рішення та інструменти візуалізації даних – формують нову парадигму прийняття рішень, засновану на даноцентричності, прозорості й адаптивності.

BI-системи (Business Intelligence), такі як Power BI, Tableau, Qlik Sense, забезпечують глибокий аналітичний моніторинг, виявлення тенденцій та візуалізацію ключових показників ефективності (KPI), що є ключовими у системі економічної безпеки. Платформа Power BI дозволяє об'єднувати дані з ERP-систем, CRM-систем, електронних таблиць, баз даних та інших джерел,

створюючи інтерактивні дашборди для оперативного аналізу та прийняття рішень [45; 46].

ERP-системи, зокрема SAP ERP, Microsoft Dynamics 365, Oracle NetSuite, інтегрують функціональні підрозділи підприємства в єдину цифрову екосистему. ERP-системи з модулями управління ризиками (наприклад, SAP GRC) дозволяють цілодобово контролювати фінансову стабільність, відповідність нормативним вимогам й кібербезпеку, що є фундаментом стійкого функціонування у динамічному середовищі.

Системи класу SIEM (Security Information and Event Management) забезпечують централізований збір, нормалізацію, кореляцію та аналіз подій із різних джерел IT-інфраструктури. Відомі продукти – IBM QRadar, Splunk Enterprise Security, Microsoft Sentinel – застосовують поведінковий аналіз, алгоритми машинного навчання та автоматизовані сценарії реагування, що дає змогу виявляти складні загрози, виявляти аномалії в реальному часі та активізувати захисні заходи [47; 49].

Зокрема, IBM QRadar SIEM дозволяє централізовано відображати події, виявляти загрози в реальному часі, оптимізувати відповідність вимогам і знизити операційні витрати завдяки автоматизації процесів. Splunk Enterprise Security надає широку екосистему інтеграцій, гнучкість архітектури та високу якість виявлення інцидентів, знижуючи кількість помилкових спрацьовувань і підвищуючи оперативність реакції. Microsoft Sentinel, як хмарне SIEM-рішення, інтегрується з Azure-екосистемою, використовує AI та ML-моделі для аналізу даних, що дозволяє зберегти існуючу інфраструктуру та поступово реалізовувати перехід до хмарного безпеки операційного центру [48].

Таким чином, інтеграція BI, ERP та SIEM-рішень формує багаторівневу підтримку системи контролю економічної безпеки: від аналітики й візуалізації даних, через прозоре управління ресурсами і ризиками, до виявлення й реакції на кіберзагрози. Це створює основу для ефективного ризик-орієнтованого

управління в цифрову епоху – з акцентом на гнучкість, адаптивність і проактивність у прийнятті рішень.

1.3. Трансформація системи економічної безпеки підприємства під впливом цифровізації

Цифрова трансформація управлінських процесів підприємства є фундаментальним чинником забезпечення його економічної безпеки в умовах динамічного розвитку цифрової економіки.

Рисунок 1.5 ілюструє концептуальну модель впливу ключових цифрових платформ (ERP, CRM, SCM, BI) на трансформацію архітектури управління підприємством в умовах цифрової економіки.



Рис. 1.5. Вплив цифрових платформ на архітектуру управління підприємством

Джерело: авторська розробка.

У межах цифрової трансформації управління підприємством особливого значення набуває інтеграція цифрових платформ, що змінюють логіку функціонування бізнес-процесів та підвищують рівень економічної безпеки. До таких платформ належать ERP-, CRM-, SCM-системи та інструменти бізнес-аналітики (BI), кожна з яких виконує специфічну функцію в загальній управлінській архітектурі підприємства.

Зокрема, ERP-системи забезпечують централізовану інтеграцію ключових функціональних блоків підприємства, охоплюючи фінансове управління, виробниче планування, логістику та управління персоналом. Їх впровадження сприяє уніфікації потоків даних, підвищенню прозорості процесів і переходу до ухвалення рішень на основі оперативної аналітики в реальному часі. Як показано на рисунку 1.4, ERP-рішення безпосередньо впливають на структуру прийняття управлінських рішень, забезпечуючи підвищення їх обґрунтованості та зниження ймовірності ризиків, пов'язаних із інформаційною асиметрією.

CRM-системи (Customer Relationship Management) виступають інструментом побудови клієнтоцентричних моделей управління, спрямованих на персоналізацію взаємодії, підвищення рівня лояльності та зростання життєвого циклу клієнта. Інформація, згенерована на основі поведінкових патернів споживачів, дозволяє оптимізувати маркетингові бюджети, удосконалювати стратегії залучення та утримання, а також оперативно реагувати на зміни у споживчих очікуваннях. У цьому контексті CRM-системи впливають на ефективність розподілу ресурсів, зокрема шляхом сценарного моделювання потреб та формування індивідуальних пропозицій на основі прогнозів попиту.

SCM-системи (Supply Chain Management) забезпечують цифрову координацію ланцюгів постачання, від постачальників сировини до кінцевого споживача. Вони сприяють автоматизації управління запасами, логістикою, відстеженню руху товарів у режимі реального часу та підвищенню гнучкості у

відповідь на зовнішні збурення. Як відображено на рисунку 1.4, SCM-рішення трансформують систему контролю шляхом впровадження механізмів прогнозного управління, цифрових індикаторів ефективності (KPI) та проактивного виявлення вузьких місць у ланцюгах поставок.

BI-платформи (Business Intelligence), зокрема Power BI, Qlik або Tableau, виконують аналітичну функцію, інтегруючи велику кількість розрізнених даних у структуровані інформаційні панелі. Вони дозволяють здійснювати глибокий аналіз операційної діяльності, прогнозувати ризики та виявляти приховані закономірності. У контексті економічної безпеки такі інструменти формують основу підзвітності, забезпечуючи прозорість процесів прийняття рішень, формування цифрового ланцюга аудиторських слідів, що унеможливорює приховані маніпуляції з даними та посилює довіру до системи управління.

Таким чином, цифрові платформи не лише забезпечують автоматизацію функціональних процесів, а й радикально змінюють архітектуру управління підприємством. Вони сприяють переходу до даноцентричної моделі, в якій рішення формуються на основі комплексного аналізу, цифрових рекомендаційних систем та інтелектуальної обробки інформації. Така трансформація, як візуалізовано на рисунку 1.4, є необхідною умовою формування адаптивної та стійкої системи управління, здатної ефективно реагувати на загрози економічної безпеки у цифровому середовищі.

Цифровізація бізнес-середовища, що є наслідком стрімкого розвитку інформаційно-комунікаційних технологій, слугує потужним каталізатором інноваційного оновлення підприємств, відкриваючи нові можливості для підвищення ефективності, гнучкості та конкурентоспроможності. Водночас цей процес супроводжується формуванням принципово нових типів ризиків, які істотно трансформують конфігурацію загроз економічній безпеці. Системне проникнення цифрових технологій у всі сфери функціонування підприємства зумовлює зростання його вразливості до зовнішніх і внутрішніх дестабілізуючих факторів. Найбільш критичними з них постають:

кіберзагрози, пов'язані з несанкціонованим доступом до інформаційних ресурсів та порушенням цілісності даних; технологічна залежність від зовнішніх цифрових платформ і постачальників програмного забезпечення; втрати або викрадення критичних даних, зокрема персональних, комерційних і фінансових; потенційні збої або відмова цифрової інфраструктури, які можуть паралізувати операційну діяльність підприємства; а також стратегічні ризики, пов'язані з підривом традиційної бізнес-моделі через появу цифрових конкурентів, які здатні швидко адаптуватися до змін ринку завдяки використанню передових цифрових інструментів.

Ці виклики формують нову площину загроз, у якій класичні методи забезпечення економічної безпеки стають недостатніми. У результаті зростає потреба в переосмисленні концептуального апарату ризик-менеджменту, розробці адаптивних моделей захисту цифрових активів і впровадженні комплексних систем кіберстійкості, що передбачають не лише технічні, але й організаційно-управлінські заходи реагування. З огляду на зазначене, цифрова трансформація потребує не лише модернізації інфраструктури, а й побудови нової парадигми безпеки, що інтегрує технологічні, нормативно-правові та поведінкові аспекти захисту в єдиний стратегічний контур економічної безпеки підприємства.

Рисунок 1.6 демонструє типологію технологічних ризиків, зумовлених цифровою трансформацією бізнес-середовища, а також відповідні превентивні й адаптивні заходи реагування, спрямовані на зниження їх деструктивного впливу на економічну безпеку підприємства. Запропонована структуризація дозволяє зіставити природу ризиків із релевантними управлінськими інструментами, які можуть бути інтегровані в систему стратегічного ризик-менеджменту.

Категорія ризику	Зміст ризику	Пріоритетні заходи реагування
<i>Кіберзагрози</i>	Включають зловмисні дії у кіберпросторі, спрямовані на порушення конфіденційності, цілісності або доступності даних (наприклад, фішинг, атаки типу DDoS, шкідливе ПЗ, експлуатація уразливостей ланцюгів постачання, використання ШІ для обману систем безпеки).	Побудова багаторівневої архітектури безпеки із впровадженням SIEM/EDR-систем, організація регулярних тренінгів з кібергігієни для персоналу, використання багатофакторної автентифікації, постійний моніторинг інцидентів.
<i>Залежність від цифрових платформ</i>	Означає критичну залежність бізнес-процесів від інфраструктури сторонніх провайдерів (хмарні обчислення, SaaS-рішення), що у разі їх відмови або змін політики створює ризики операційного характеру.	Формування стратегії багатохмарного розгортання (multi-cloud), запровадження незалежних резервних інфраструктур, аудит договорів SLA щодо безпеки й доступності, впровадження механізмів швидкого відновлення (disaster recovery).
<i>Технологічна вразливість</i>	Виникає внаслідок використання застарілих або ненадійних технологічних рішень, незахищених IoT/edge-пристроїв, або відсутності принципу «безпечний за замовчуванням» при проєктуванні IT-систем.	Проведення регулярного технічного аудиту інфраструктури, оновлення апаратного та програмного забезпечення, впровадження підходу secure-by-design у всіх етапах життєвого циклу IT-продуктів, сегментація мережі.
<i>Втрати та витоки даних</i>	Мають місце при неконтрольованому розширенні масивів даних, низькому рівні структуризації сховищ, відсутності політик збереження й обмеження доступу, що підвищує ймовірність витоку і санкцій.	Розробка політик інформаційної гігієни, каталогізація та класифікація даних, впровадження шифрування і систем контролю доступу, використання DLP-рішень, резервне копіювання та аудит відповідності стандартам (GDPR, 23. ДСТУ ISO/IEC 27001:2023).
<i>Підриб бізнес-моделі</i>	Зумовлюється агресивною конкуренцією з боку цифрових нішевих гравців, здатних швидко адаптуватися до ринку завдяки гнучким інноваційним моделям. Це спричиняє втрату клієнтської бази та зниження рентабельності традиційного бізнесу.	Запровадження адаптивних стратегій розвитку, моніторинг технологічних трендів, створення власних R&D-центрів, інвестування в діджитал-платформи й продуктові інновації, реінжиніринг ключових процесів відповідно до принципів цифрової економіки.
<i>Зростання витрат на захист</i>	Відображає зростання обсягу інвестицій, необхідних для підтримки базової кіберстійкості підприємства: від закупівлі захисних технологій до підготовки персоналу.	Побудова економічно збалансованої системи кіберзахисту з орієнтацією на ROI, оптимізація бюджету безпеки, впровадження автоматизованих систем, використання страхування кіберризиків, розвиток внутрішньої експертизи з безпеки.

Рис. 1.6. Технологічні ризики цифрової трансформації та заходи реагування

Джерело: узагальнено автором на основі [51–58].

До першочергових викликів цифрової трансформації, що безпосередньо впливають на економічну безпеку підприємства, належать кіберзагрози, які охоплюють широкий спектр шкідливих інцидентів – від соціально-інженерних атак, фішингових кампаній, деструктивного програмного забезпечення до високоточних DDoS-атак і цілеспрямованого використання уразливостей у цифрових ланцюгах постачання. Згідно з сучасними дослідженнями, у міру розгортання складних інфраструктур і розширення цифрових поверхонь підприємства, відбувається зростання кількості багатовекторних загроз, що комбінують автоматизовані вторгнення із використанням технологій штучного інтелекту, зокрема *deepfake*-ідентифікації та моделювання поведінки користувача [51; 53].

Для суб'єктів господарювання, особливо тих, чия діяльність значною мірою залежить від цифрових активів, кіберзагрози трансформуються з технічного питання у критичний чинник економічного ризику, що впливає на витрати, доходи та репутаційний капітал підприємства.

Наслідками успішних атак можуть стати як прямі фінансові втрати (через блокування бізнес-процесів, викрадення коштів, витрати на відновлення), так і непрямі – у вигляді санкцій за порушення нормативів захисту даних, зокрема Загального регламенту про захист даних Європейського Союзу (General Data Protection Regulation – GDPR), втрати клієнтів, розірвання контрактів або підризу інвестиційної привабливості.

У зв'язку з цим підвищується роль проактивних моделей управління кіберризиками, які базуються на системній інтеграції інформаційно-аналітичних рішень у загальну архітектуру управління. До таких інструментів належать системи типу SIEM (Security Information and Event Management) та EDR (Endpoint Detection and Response), що забезпечують централізований збір, кореляцію та аналіз подій безпеки, а також моделювання сценаріїв атак на основі поведінкових алгоритмів. Наприклад, Splunk Enterprise Security надає можливості виявлення аномалій у режимі реального

часу, тоді як Microsoft Sentinel інтегрує функціонал на базі хмарної інфраструктури з використанням потужностей машинного навчання [49].

Крім технологічних рішень, ефективне управління кіберризиками вимагає впровадження організаційних та економічних заходів, зокрема формування культури кібергігієни серед персоналу, регулярного тестування систем на проникнення (penetration testing), обов'язкового застосування багатофакторної автентифікації, а також створення спеціалізованих підрозділів з моніторингу інцидентів (SOC – Security Operations Center). З економічної точки зору, доцільним є використання інструментів оцінки окупності інвестицій у кіберзахист (Cybersecurity ROI) для прийняття зважених рішень щодо алокації ресурсів, а також розвиток внутрішньої аналітики для оцінювання ризик-орієнтованих витрат як частини загальної моделі стійкого розвитку підприємства [53; 54].

Кіберзагрози в умовах цифрової трансформації не лише змінюють конфігурацію технологічної архітектури підприємства, але й створюють нову парадигму економічного ризик-менеджменту, де пріоритет надається превентивним, інтелектуально-орієнтованим та ресурсно оптимізованим стратегіям забезпечення економічної безпеки.

Залежність від цифрових платформ виступає одним із критичних системних ризиків у контексті цифрової трансформації підприємств, що безпосередньо впливає на рівень їх економічної безпеки. Йдеться насамперед про делегування ключових бізнес-функцій зовнішнім провайдерам цифрових послуг, насамперед хмарних технологій (cloud computing), платформ управління даними (data platforms), інструментів взаємодії з клієнтами (PaaS/SaaS) тощо. Така інституціональна модель, що ґрунтується на аутсорсингу цифрової інфраструктури, значно знижує трансакційні витрати та прискорює інноваційні цикли. Водночас вона формує новий клас ризиків – залежність від цифрового монополізму, втрату контролю над критичними активами та підвищену чутливість до рішень зовнішніх операторів [51].

Особливо загрозливим такий ризик стає у випадку перегляду умов угод про рівень обслуговування (SLA, Service Level Agreement), припинення діяльності постачальника, перебоїв у наданні послуг або кібератак на стороні провайдера. Як зазначають автори дослідження [52], навіть короткострокове порушення доступу до хмарної IT-інфраструктури може призвести до каскадного ефекту – зупинки операційної діяльності, втрати клієнтів, розриву логістичних зв'язків і, як наслідок, – прямих фінансових збитків та зниження індексу ділової репутації.

З економічної точки зору, залежність від обмеженої кількості цифрових платформ створює ефект «цифрового замикання», за якого підприємство втрачає гнучкість у виборі альтернатив і змушене адаптувати внутрішні бізнес-процеси до вимог постачальника. Така ситуація ускладнює трансформаційне планування, посилює структурні бар'єри для масштабування та формує приховані витрати у довгостроковому періоді [53].

У цьому контексті забезпечення економічної безпеки підприємства вимагає розроблення диверсифікованої архітектури цифрової взаємодії, яка передбачає:

- впровадження стратегій багатохмарного середовища (multi-cloud policy) для зниження монозалежності;
- резервування інфраструктури на критичних етапах цифрових ланцюгів;
- контроль за юрисдикційними ризиками передачі даних (особливо для регульованих галузей);
- проведення незалежного аудиту умов SLA-договорів, включаючи сценарне моделювання вартості відновлення у випадку форс-мажору [52].

Крім того, доцільним є оцінювання економічного ефекту переходу на відкриті цифрові екосистеми та впровадження концепції «цифрового суверенітету підприємства» як нової парадигми управління ризиками цифрової залежності у довгостроковій перспективі.

Технологічна вразливість у системі цифрового управління підприємством розглядається як один із ключових структурних ризиків, що підриває економічну безпеку господарюючого суб'єкта. Вона виникає переважно внаслідок експлуатації застарілих технологічних рішень (legacy systems), недостатнього рівня захисту пристроїв Інтернету речей (IoT), edge-компонентів, а також систем, які були розроблені без урахування принципів «безпеки за замовчуванням» (security by design) [56].

Нехтування архітектурною кіберстійкістю під час розгортання ІТ-інфраструктури зумовлює збільшення площі потенційного вторгнення – так званої «цифрової зони вразливості», яка може бути використана як точка входу зломисників до основних корпоративних систем. Як засвідчують результати аналітичного огляду [56], саме слабо захищені периферійні пристрої часто стають інструментом для проведення гібридних атак, що поєднують елементи маніпуляції даними, саботажу та промислового шпіонажу.

Із точки зору фінансової захищеності діяльності підприємства, неконтрольована технологічна вразливість призводить до накопичення латентних витрат, які виявляються лише в момент реалізації загрози. До таких витрат належать:

- витрати на відновлення діяльності;
- втрати від зупинки операцій;
- зростання витрат на страхування кіберризиків;
- зниження ринкової вартості підприємства внаслідок репутаційного шоку.

Для мінімізації цього класу ризиків актуальним стає впровадження систематичного аудиту ІТ-інфраструктури, який включає як технічне сканування вразливостей, так і оцінку відповідності архітектури принципам безпечного проєктування (secure-by-design та privacy-by-design). Також важливою є регулярна модернізація цифрової екосистеми підприємства – не лише як технічна процедура, а як стратегічний інвестиційний процес, що

забезпечує довгострокову конкурентоспроможність і економічну стійкість [56].

Таким чином, технологічна вразливість у цифрову епоху не є лише технічною категорією: вона трансформується у мультивекторний економічний ризик, що вимагає інтегрованого реагування з боку менеджменту, ІТ-департаменту та функціонального контролю.

Втрати та витoki даних становлять один із найбільш поширених і економічно витратних ризиків цифрової трансформації підприємства. Зокрема, у сучасній практиці все більшого поширення набуває феномен «інформаційного розброду» (data sprawl), який характеризується як безконтрольне зростання обсягів створюваних, передаваних і збережених даних без належної структуризації, централізованого управління та контролю доступу [57]. У контексті економічної безпеки це явище є надзвичайно ризикованим, оскільки воно ускладнює оперативний моніторинг потоків інформації, підвищує ймовірність несанкціонованого доступу та унеможлиблює забезпечення належного рівня конфіденційності, цілісності й доступності інформаційних ресурсів.

Відповідно до сучасних досліджень, витoki даних призводять не лише до прямих фінансових втрат, пов'язаних з відшкодуванням збитків та штрафними санкціями, а й до тривалих репутаційних наслідків, які впливають на капіталізацію суб'єкта господарювання, доступ до фінансування та партнерські відносини. В умовах запровадження посиленних регуляторних режимів, зокрема Загального регламенту про захист даних (GDPR, General Data Protection Regulation) в ЄС, витoki персональних даних можуть мати суттєвий юридичний резонанс, що тягне за собою багатомільйонні штрафи, обмеження у роботі на європейському ринку та судові позови з боку зацікавлених осіб.

З позиції забезпечення економічної безпеки підприємства, втрати даних – це втрати нематеріального активу, який є фундаментом цифрової вартості фірми. Саме наявність структурованих, захищених і контрольованих даних

забезпечує ефективність аналітики, точність прийняття рішень, функціонування ланцюгів постачання та взаємодію з клієнтами. Відтак, захист інформаційних активів має бути інтегрований у стратегічне управління ризиками підприємства як окрема функціональна складова.

До ефективних інструментів мінімізації ризиків витоку даних належать:

- впровадження систем запобігання витокам даних (DLP – Data Loss Prevention), що дозволяють виявляти, блокувати й реєструвати несанкціоновані спроби переміщення конфіденційної інформації;
- використання технологій шифрування на всіх етапах життєвого циклу даних – під час збереження, передачі та обробки;
- класифікація даних за рівнем критичності із визначенням політик доступу відповідно до ризик-профілю;
- впровадження міжнародних стандартів інформаційної безпеки, зокрема ISO/IEC 27001 (в Україні – це ДСТУ ISO/IEC 27001:2023. «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги»), які передбачають розробку політик захисту інформації, проведення аудитів, інцидент-менеджмент та неперервне вдосконалення системи захисту [49].

Отже, управління ризиками втрати та витоку даних є не лише елементом технологічної політики, а важливою складовою загальної економічної стратегії підприємства, що визначає стійкість організації до цифрових загроз у довгостроковій перспективі.

Підрид бізнес-моделі в умовах цифрової трансформації є критичним вектором стратегічного ризику для підприємств, що функціонують на основі традиційних, маломобільних або слабо інноваційних підходів до створення цінності. Цей тип ризику виявляється у вигляді розмивання ролі традиційних посередників, посилення цінової конкуренції та втрати актуальності продуктового портфеля під впливом цифрових гравців, що функціонують на основі масштабованих платформних архітектур та орієнтованих на клієнта бізнес-моделей [51].

Сутність загрози полягає не стільки у безпосередньому зниженні доходів, скільки у втраті конкурентоспроможності через структурну інерційність підприємства, його неспроможність адаптуватися до змін у поведінці споживачів, технологічних трендів і очікувань щодо сервісу. Прикладом можуть слугувати традиційні роздрібні компанії, які зазнали витіснення з ринку через експансію онлайн-ритейлерів із персоналізованими пропозиціями, мінімальними операційними витратами та інноваційною логістикою [58].

З економічної точки зору, підривна інновація (disruptive innovation) створює для підприємства «вікно ризику», в межах якого ринкове середовище змінюється швидше, ніж адаптується організаційна структура. Внаслідок цього виникає розрив між наявними компетенціями та новими вимогами ринку, що у довгостроковій перспективі призводить до зниження доданої вартості, звуження маржі прибутку та, зрештою, втрати економічної безпеки.

Для протидії такому класу ризиків підприємству доцільно впроваджувати випереджувальну стратегію цифрової трансформації, зорієнтовану на швидке реагування на зміни в цифровому середовищі та адаптацію бізнес-моделі до нових умов, що включає:

- оцифрування продуктів і сервісів із фокусом на створення цифрової цінності;
- інтеграцію функцій досліджень і розробок, спрямованих на швидку генерацію та виведення інновацій на ринок;
- впровадження моделі відкритих інновацій (open innovation), що дозволяє залучати зовнішні ідеї, партнерства та технології для розширення горизонту інноваційної активності [59];
- переосмислення бізнес-моделі підприємства за логікою цифрової економіки – перехід до платформених архітектур, сервісного мислення, гнучкого управління портфелем цінностей для клієнта.

Таким чином, у контексті забезпечення економічної безпеки, підриві бізнес-моделі не є лише технологічним викликом – це системне стратегічне

питання, яке вимагає перегляду парадигми розвитку, оновлення управлінських рішень і формування внутрішньої інноваційної спроможності.

Зростання витрат на кіберзахист у цифрову епоху перетворюється на системну тенденцію, яка безпосередньо впливає на структуру витрат підприємства та його фінансову стійкість. На відміну від традиційних витрат на IT-інфраструктуру, витрати на забезпечення інформаційної безпеки мають подвійний характер: вони включають як прямі витрати на придбання та обслуговування спеціалізованого програмного забезпечення (антивіруси, SIEM-системи, рішення типу EDR/SOAR), так і непрямі витрати, пов'язані з підготовкою персоналу, зовнішніми аудитами безпеки, сертифікацією відповідності міжнародним стандартам (зокрема ISO/IEC 27001) та витратами на відновлення після інцидентів [49; 91].

Економічна доцільність інвестицій у кібербезпеку набуває ключового значення в контексті стратегічного управління ресурсами підприємства, особливо в умовах обмеженого бюджету та зростаючого тиску на рентабельність. Визначальним інструментом для обґрунтування таких інвестицій слугує показник рентабельності інвестицій у систему кібербезпеки (Cyber ROI, Return on Investment in Cybersecurity), який забезпечує кількісну оцінку ефективності вкладень у безпекову інфраструктуру. Цей індикатор дозволяє порівняти очікувані або фактичні збитки від кіберінцидентів, яких вдалося уникнути завдяки впровадженню захисних заходів, з понесеними витратами на відповідні технології, персонал та процедури [51].

У теоретико-економічному аспекті Cyber ROI є прикладом індикатора запобіжного інвестування, що відображає не стільки безпосередній приріст доходу, скільки уникнення потенційних втрат і стабілізацію основних виробничо-господарських процесів. Його застосування сприяє інтеграції кіберризиків до системи корпоративного фінансового планування, що дозволяє більш обґрунтовано формувати бюджети IT-напрямів, обирати між альтернативними технологічними рішеннями та визначати критичні точки у системі управління безпекою.

Окрім класичних інструментів оцінювання, сучасна практика кіберзахисту дедалі активніше впроваджує інноваційні моделі автоматизації процесів управління безпекою, що ґрунтуються на концепції координації, автоматизації та реагування на інциденти інформаційної безпеки (SOAR, Security Orchestration, Automation and Response). Такі системи дозволяють не лише скоротити витрати на ручну обробку інцидентів, а й підвищити швидкість та якість реагування завдяки алгоритмізації повторюваних дій, використанню машинного навчання для класифікації загроз та автоматизованому запуску сценаріїв реагування [49; 54]. З економічної точки зору, впровадження SOAR-платформ сприяє оптимізації операційних витрат, зменшенню потреби у великому штаті фахівців з безпеки, а також підвищенню масштабованості безпекових процесів у міру зростання цифрової складності підприємства.

Більш того, автоматизація безпекових процесів забезпечує узгодженість внутрішньої регламентації з зовнішніми вимогами, включаючи стандарти ISO/IEC 27001, NIST CSF та вимоги регуляторів у сфері захисту даних, що знижує ризики юридичної відповідальності та забезпечує стійкість до аудиторських перевірок. У довгостроковому вимірі це не лише мінімізує витрати, а й посилює позиції підприємства на ринку, формуючи конкурентну перевагу у вигляді довіри з боку клієнтів і партнерів, які дедалі більше цінують надійність інформаційної інфраструктури.

З макроекономічної точки зору, високі витрати на кіберзахист вимагають балансу між рівнем цифрової зрілості підприємства та обсягом ризиків, на які воно наражається. У цьому контексті страхування кіберризиків стає важливим елементом стратегії управління ризиками. Страхові механізми дозволяють частково перекладати фінансові наслідки атак на спеціалізовані страхові компанії, але водночас вимагають проходження ретельної оцінки цифрової гігієни підприємства, що стимулює додаткові інвестиції в безпекову інфраструктуру [55].

Таким чином, фінансування кіберзахисту слід розглядати не як ізольовану витратну статтю, а як елемент інвестиційного портфеля підприємства, що сприяє збереженню його довгострокової конкурентоспроможності, захисту інтелектуального капіталу та формуванню довіри з боку партнерів і клієнтів.

У сучасних умовах цифрової трансформації економіки підприємства змушені функціонувати в середовищі підвищеної невизначеності, що зумовлює необхідність постійного моніторингу як ефективності їхньої діяльності, так і рівня ризиків, які впливають на здатність досягати стратегічних і операційних цілей. Відтак актуалізується інтеграція двох класів індикаторів: ключових показників ефективності (Key Performance Indicators, KPI) та ключових показників ризику (Key Risk Indicators, KRI), у систему управління економічною безпекою підприємства. Водночас ефективність застосування таких індикаторів значною мірою визначається специфікою галузі, технологічною структурою бізнес-процесів і рівнем цифрової зрілості організації.

Формування узагальненої типології KPI та KRI у галузевому розрізі дає змогу систематизувати підходи до моніторингу ризиків та ефективності, враховуючи характерні для окремих секторів економіки загрози, регуляторні вимоги та бізнес-логіку операційної діяльності. Це, у свою чергу, дозволяє підвищити релевантність індикаторного інструментарію та забезпечити його адаптацію до практичних потреб підприємства у межах ризик-орієнтованого підходу. Особливої ваги набуває також поєднання методики обчислення KPI з чітким тлумаченням змісту KRI – як інструментів ранньої діагностики небажаних тенденцій, що можуть негативно позначитися на економічній стійкості суб'єкта господарювання.

У зв'язку з цим у таблиці 1.7 подано систематизовану типологію KPI та KRI з методиками розрахунку ключових індикаторів ефективності. Такий підхід дозволяє поєднати стратегічну орієнтацію системи управління ризиками з вимогами операційної адаптивності та дає можливість

формалізувати порогові значення допустимого рівня ризику і толерантності у рамках сучасного ризик-менеджменту підприємства.

Таблиця 1.7

Типологія ключових індикаторів ефективності (KPI) та ключових індикаторів ризику (KRI) за основними сферами функціонування підприємств

Сфера економічної діяльності	KPI – ключові індикатори ефективності	KRI – ключові індикатори ризику
1	2	3
Виробництво	• Собівартість одиниці продукції = Собівартість реалізованої продукції / Обсяг виробництва. • Рівень браку = (Обсяг дефектної продукції / Загальний обсяг виробництва) $\times 100\%$. • Рівень інноваційності = (Обсяг інноваційної продукції / Загальний обсяг реалізації) $\times 100\%$.	• FR (Failure Rate – частота відмов): кількість збоїв за одиницю часу. • MTTR (Mean Time to Repair – середній час ремонту): час відновлення обладнання. • Втрати ресурсів: частка втрат сировини чи енергії у загальних витратах.
Фінансовий сектор	• ROA (Return on Assets, рентабельність активів) = Чистий прибуток / Середньорічна вартість активів $\times 100\%$. • Cost-to-Income Ratio (індекс витратомісткості доходу) = Операційні витрати / Операційний дохід $\times 100\%$. • Дохідність портфеля = Чистий прибуток від портфеля / Середньорічна вартість активів портфеля $\times 100\%$.	• NPL (Non-Performing Loans): частка проблемних кредитів у портфелі. • Кількість інцидентів шахрайства: підозрілі операції. • Кількість кіберінцидентів: несанкціонований доступ до систем.
Роздрібна торгівля	• Середній чек = Загальний обсяг продажів / Кількість чеків. • Оборотноість запасів = Собівартість реалізованої продукції / Середньорічна вартість запасів. • Рівень утримання клієнтів (Customer Retention Rate, CRR) = ((Кількість клієнтів на кінець періоду – Нові клієнти за період) / Кількість клієнтів на початок періоду) $\times 100\%$.	• Відсоток повернень: частка поверненого товару. • Disruption Rate: збої у доставці чи поставках. • Loss Rate: втрати через крадіжки або псування товару.

Продовження табл. 1.7

1	2	3
Інформаційні технології та телекомунікації	• Середній дохід на одного користувача (ARPU, Average Revenue per User) = Загальний операційний дохід / Середня кількість активних користувачів за період. • Коефіцієнт залученості користувачів (DAU/MAU, Daily Active Users / Monthly Active Users) = Число щоденних активних користувачів / Число щомісячних активних користувачів $\times 100\%$. • Рівень доступності сервісу (Uptime) = Час без збоїв / Повний час функціонування $\times 100\%$.	• Кількість DDoS-атак: атаки на стабільність систем. • SLA (Service Level Agreement) Breach Rate: невиконані зобов'язання перед клієнтами. • MTTD (Mean Time to Detect): середній час виявлення інциденту.
Енергетика	• Коефіцієнт корисної дії (ККД) = Обсяг корисно використаної енергії / Загальні енергетичні витрати $\times 100\%$. • Частка електроенергії з відновлюваних джерел = Обсяг виробленої енергії з відновлюваних джерел / Загальне виробництво електроенергії $\times 100\%$. • Енергоємність виробництва = Сукупне енергоспоживання / Обсяг виробленої продукції (у вартісному або натуральному вимірі).	• Energy Loss Rate: втрати енергії в мережах. • SCADA (Supervisory Control and Data Acquisition) Incidents: зареєстровані випадки порушень, збоїв або атак на інфраструктуру автоматизованого управління технологічними процесами. • Кількість аварій: відмови у генерації чи постачанні.

Джерело: узагальнено автором на основі [21; 29; 31; 60; 61].

Зазначимо, що вибір і налаштування конкретних KRI і KPI мають здійснюватися з урахуванням стратегічних цілей підприємства, сфер економічної діяльності та цифрової зрілості організації. Ключова мета – це виявлення порогових значень, при перевищенні яких ініціюється реакція в межах системи управління ризиками.

Наведена типологізація ключових індикаторів ефективності (KPI) та ризику (KRI) у галузевому розрізі дозволяє комплексно оцінювати взаємозв'язок між результативністю функціонування підприємства та чинниками ризику, які можуть порушити його економічну стійкість. Поєднання кількісно вимірюваних KPI із галузево релевантними KRI формує підґрунтя для створення збалансованої системи моніторингу, яка є гнучкою до змін зовнішнього середовища та внутрішніх трансформацій бізнес-моделі.

Встановлення чітких методик розрахунку KPI забезпечує об'єктивність оцінювання ефективності, тоді як KRI функціонують як інструменти раннього попередження про можливу реалізацію загроз.

З огляду на галузеву специфіку, окреслені індикатори можуть бути використані як для внутрішньої аналітики підприємства, так і для побудови галузевих еталонів ризик-менеджменту. Зокрема, для підприємств, що функціонують в умовах цифровізації, особливої ваги набувають індикатори, пов'язані з кібербезпекою, технологічною надійністю, ефективністю використання енергетичних і людських ресурсів. Такий підхід забезпечує не лише своєчасну ідентифікацію відхилень, а й створення основи для сценарного прогнозування ризиків і оперативного ухвалення управлінських рішень у межах системи економічної безпеки підприємства.

У контексті розвитку ризик-орієнтованих моделей управління економічною безпекою підприємства особливого значення набуває системна візуалізація взаємозв'язків між ключовими індикаторами ризику та індикаторами ефективності. Формалізація таких зв'язків у вигляді блок-схеми дозволяє не лише окреслити логіку їх взаємодії, але й відобразити структурну послідовність інформаційних потоків, які забезпечують дієву підтримку управлінських рішень у динамічному середовищі.

Представлена у Додатку В модель структурована за принципом причинно-наслідкової залежності, де KRI виступають не лише інструментами моніторингу загроз, а й джерелами випереджувальних сигналів про потенційні відхилення від цільових показників діяльності. Вони інтегруються в процеси аналізу KPI, посилюючи здатність підприємства до ранньої діагностики кризових тенденцій і своєчасної реакції на зміни внутрішнього та зовнішнього середовища.

Блок-схема також ілюструє механізм управлінського циклу, у межах якого KRI і KPI взаємодіють із функціональними модулями системи управління: оцінкою ризиків, оперативним плануванням, аудитом безпеки, сценарним аналізом і контролем відповідності. Така структурна побудова

дозволяє забезпечити гнучкість управління, узгодження тактичних дій із довгостроковими цілями підприємства та створення адаптивного контуру економічної безпеки на основі цілісного інформаційно-аналітичного забезпечення.

Висновки до розділу 1

Результати дослідження теоретико-методологічних основ оцінювання економічної безпеки підприємства в умовах цифрової трансформації дозволяють дійти таких наукових узагальнень:

1. Досліджено еволюцію категорії «економічна безпека» та встановлено її трансформацію від вузького трактування як стану захищеності до комплексної системної категорії, орієнтованої на забезпечення стійкості, адаптивності та розвитку в умовах зростаючої невизначеності. Показано, що в сучасному науковому дискурсі економічна безпека розглядається як інтегральна характеристика функціонування економічних систем, яка поєднує захисні та розвиткові функції. Визначено, що цифрова трансформація суттєво змінює зміст економічної безпеки через ускладнення ризиків, підвищення ролі інформаційних технологій та посилення взаємозалежності економічних процесів. Розкрито роль ризиків як ключового елементу економічної безпеки підприємства та систематизовано їх класифікацію з урахуванням сучасних цифрових викликів. Встановлено, що економічна безпека формується в умовах постійної взаємодії ризиків і параметрів стійкості, що зумовлює необхідність переходу до ризик-орієнтованої логіки управління.

2. Сформовано концептуальне підґрунтя трактування економічної безпеки підприємства як багатовимірної динамічної системи, що інтегрує фінансові, виробничі, інформаційні, технологічні та інституційні компоненти. Визначено, що ефективність такої системи забезпечується узгодженістю її складових та здатністю адаптуватися до змін зовнішнього і внутрішнього середовища. Систематизовано міжнародні підходи до ризик-орієнтованого

управління економічною безпекою на основі стандартів ISO 31000, COSO ERM та NIST CSF та визначено їх роль у формуванні сучасної моделі управління ризиками підприємства. Сформовано аналітичну матрицю взаємозв'язку показників стійкості, ризиків і ключових індикаторів ризику, що дозволяє інтегрувати процеси оцінювання та моніторингу економічної безпеки. Представлено організаційну структуру ризик-орієнтованого управління підприємством на основі моделі трьох ліній захисту. Визначено, що інтеграція ризик-орієнтованого підходу в систему управління створює передумови для підвищення стійкості підприємства та обґрунтованості управлінських рішень в умовах цифрової трансформації.

3. Узагальнено підходи до оцінювання економічної безпеки підприємства в умовах цифрової трансформації та визначено ключові принципи її оцінювання, що забезпечують системність, комплексність і узгодженість аналітичних процедур. Встановлено, що оцінювання економічної безпеки має ґрунтуватися на поєднанні показників результативності діяльності підприємства та індикаторів ризику, що дозволяє враховувати як досягнуті результати, так і потенційні загрози. Розкрито логіку формування системи показників оцінювання економічної безпеки, яка передбачає їх структуризацію відповідно до функціональних аспектів діяльності підприємства та рівня впливу цифрових факторів. Визначено, що в умовах цифровізації оцінювання має враховувати не лише фінансові показники, а й характеристики інноваційності, адаптивності та технологічного розвитку підприємства.

4. Систематизовано методи оцінювання економічної безпеки підприємства та визначено їх роль у формуванні аналітичної основи управлінських рішень. Встановлено, що застосування цифрових технологій обробки даних, аналітичних платформ і інформаційних систем забезпечує підвищення оперативності, точності та обґрунтованості оцінювання економічної безпеки. Сформовано підхід до цифрового моніторингу економічної безпеки підприємства, який передбачає використання інформаційно-аналітичних систем для безперервного відстеження змін у

діяльності підприємства та зовнішньому середовищі. Визначено, що інтеграція показників результативності та ризику в систему моніторингу забезпечує своєчасне виявлення відхилень і підвищує ефективність управлінського реагування.

5. Розкрито вплив цифрової трансформації на бізнес-процеси та систему економічної безпеки підприємства. Визначено, що впровадження цифрових платформ управління ресурсами, взаємовідносинами з клієнтами, логістичними процесами та аналітичною обробкою даних змінює архітектоніку управління підприємством через централізацію інформаційних потоків, підвищення прозорості операційної діяльності та посилення аналітичної підтримки прийняття рішень. Встановлено, що така трансформація одночасно підвищує ефективність бізнес-процесів і формує нову систему технологічних ризиків, пов'язаних із кіберзагрозами, залежністю від цифрової інфраструктури, уразливістю інформаційних систем і порушенням безперервності діяльності, що зумовлює необхідність формування комплексної системи управлінського реагування.

6. Сформовано типологію ключових показників ефективності та ключових індикаторів ризику у галузевому розрізі як аналітичну основу цифрового моніторингу економічної безпеки підприємства. Визначено, що їх інтегроване використання забезпечує системне поєднання оцінювання результативності бізнес-процесів із контролем ризиків, дозволяє своєчасно виявляти критичні відхилення та підвищує обґрунтованість управлінських рішень. Обґрунтовано, що застосування цифрових аналітичних систем і спеціалізованих рішень для моніторингу інформаційної безпеки забезпечує формування багаторівневої системи спостереження за станом підприємства, яка створює можливість переходу від фрагментарного контролю до цілісного ризик-орієнтованого управління економічною безпекою в умовах цифрової трансформації..

Основні положення розділу розкрито у публікаціях автора [7; 19; 53; 62; 63].

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ: РИЗИКИ ТА УПРАВЛІННЯ

2.1. Аналіз середовища формування економічної безпеки підприємств на основі комплексної системи показників

У сучасних умовах цифрової трансформації економіки питання забезпечення економічної безпеки підприємств постає як одне з ключових завдань їхнього стратегічного розвитку та довгострокової стійкості. Інтенсивне впровадження цифрових технологій у бізнес-процеси створює нові можливості для підвищення продуктивності праці, оптимізації витрат, диверсифікації каналів збуту та розширення присутності на глобальних ринках. Водночас цей процес зумовлює формування якісно нового спектра загроз, що охоплюють фінансову, інформаційну та організаційну сфери функціонування підприємства. Зокрема, цифровізація суттєво підвищує ризики кіберзлочинності, несанкціонованого доступу до комерційної інформації, витоку даних та технологічних збоїв, наслідки яких можуть проявлятися не лише у вигляді безпосередніх фінансових втрат, а й у довгостроковому зниженні ділової репутації та конкурентоспроможності бізнесу [64].

Додатковим викликом стає зростаюча залежність підприємств від стану національної та глобальної цифрової інфраструктури, рівня кіберзахисту та інституційної готовності держави протидіяти викликам кіберпростору. В умовах поширення транскордонних цифрових потоків, глобалізації інформаційних ризиків та формування наднаціональних стандартів у сфері регулювання кібербезпеки вітчизняні суб'єкти господарювання вимушені пристосовуватися до нових правил функціонування, що підвищує складність управління економічною безпекою. Це обумовлює потребу у комплексній діагностиці рівня безпеки підприємства як основи ідентифікації критичних

вразливостей, моніторингу ризиків та визначення меж його стійкості до трансформаційних викликів.

Системність підходу до діагностики економічної безпеки передбачає інтеграцію традиційних фінансово-економічних індикаторів із сучасними показниками цифрових ризиків, технологічної готовності та інноваційної спроможності. Відтак, завданням діагностики стає не лише виявлення відхилень у фінансово-господарській діяльності, а й аналіз ступеня адаптивності бізнес-моделей до змін цифрового середовища. Це потребує залучення методологій, що дозволяють поєднувати кількісні та якісні оцінки, формувати інтегральні індекси ризику, застосовувати сценарне прогнозування та інструменти аналізу великих даних. Таким чином, дослідження та розвиток методологічних засад діагностики економічної безпеки підприємств у цифрову епоху стає необхідною передумовою підвищення їхньої стійкості, інноваційної активності та конкурентоспроможності [65].

Сучасний дискурс довкола економічної безпеки підприємств засвідчує перехід від вузько індикаторного виміру до багатовимірної, ризик-орієнтованої та цифрово чутливої оцінки. Узагальнення наукових джерел показує, що методологія діагностики має поєднувати класичні фінансово-економічні показники з оцінюванням організаційних, інформаційних і технологічних вразливостей, які виникають у процесі цифрової трансформації. Така інтеграція дозволяє коректно відобразити як статику ресурсного потенціалу, так і динаміку ризиків у цифровому середовищі. У вітчизняній літературі наголошується на необхідності синтезу підходів (*індикаторного, функціонально-ресурсного, ризик-орієнтованого*) та їх адаптації до умов цифровізації, що розширює інструментарій діагностики від обліково-аналітичних процедур до стратегічного моніторингу безпеки [6; 66].

Індикаторний підхід залишається основою діагностики економічної безпеки підприємств завдяки своїй формалізованості та можливості порівняння показників у часі та між суб'єктами господарювання. Він базується насамперед на фінансових коефіцієнтах: ліквідності, рентабельності,

автономії, активності та структури капіталу, що забезпечує науково обґрунтовану основу для управлінського аналізу. Проте класична модель не враховує нові виклики цифрової трансформації: кіберризики, якість інформаційних потоків, стійкість IT-інфраструктури тощо. У цьому контексті зростає потреба доповнення індикаторної системи цифровими і технологічними метриками. Сучасні дослідження пропонують інтеграцію традиційних фінансових показників з показниками кіберстійкості, індикаторами рівня цифрової зрілості, статусу автоматизації та здатності до інформаційного моніторингу [67].

У цьому контексті сучасні дослідження пропонують глибшу, структуровану класифікацію цифрових ризиків, що є еволюційним продовженням індикаторного підходу. Особливо корисною є матриця ризиків цифрової трансформації («Digital Transformation Risk Matrix»), яка систематизує ризики за двома осями: їхню масштабність (від низької до високої) та ступінь контрольованості (від контрольованих до неконтрольованих), дозволяючи суб'єктам господарювання класифікувати ризики з урахуванням ймовірності виникнення та можливості ефективного реагування [68].

Ще одним перспективним напрямом розвитку діагностики економічної безпеки підприємств є формування інтегральних моделей, що поєднують кількісні фінансові параметри з якісними технологічними та інституційними індикаторами. У цьому контексті дедалі більшого поширення набувають складені індекси, що дозволяють оцінити рівень стійкості бізнесу до цифрових викликів на основі комплексного порівняння різних вимірів розвитку. Зокрема, Digital Economy and Society Index (DESI) Європейської комісії [69] відображає цифрову готовність країн за такими критеріями, як підключення, людський капітал, використання цифрових технологій бізнесом та інтеграція цифрових послуг у суспільне життя. IMD Digital Competitiveness Index [70] вимірює здатність країн адаптувати та впроваджувати цифрові технології, акцентуючи увагу на знаннях, технологічних інфраструктурах та майбутній готовності.

Global Innovation Index (GII) [71] оцінює інноваційний потенціал економік, включаючи науково-дослідні витрати, патентну активність, розвиток стартап-екосистем та фінансову підтримку інновацій. Водночас Global Competitiveness Index (GCI 4.0) Всесвітнього економічного форуму [72] охоплює ширший спектр індикаторів, включаючи інституційну спроможність, інфраструктурний розвиток, стабільність макроекономічного середовища, ринкову динаміку та інноваційні екосистеми.

Застосування цих індексів у поєднанні з фінансово-економічними коефіцієнтами підприємств дозволяє не лише кількісно оцінити їхню конкурентоспроможність і технологічну зрілість, але й виявити приховані ризики, що формуються в умовах цифровізації. Інтегральний підхід забезпечує побудову системної діагностики економічної безпеки, де цифрова готовність розглядається не ізольовано, а у взаємозв'язку з фінансовою стійкістю, інноваційним потенціалом та здатністю бізнесу протидіяти кіберзагрозам і технологічним шокам. Така методологічна інтеграція сприяє розробці інструментів стратегічного управління, які дозволяють підприємствам своєчасно ідентифікувати вразливості та формувати механізми адаптивної безпеки у цифрову добу.

У сучасних дослідженнях одним із провідних методологічних напрямів оцінювання економічної безпеки підприємств є *функціонально-ресурсний підхід*. Його базова ідея полягає у виокремленні ключових складових економічної безпеки за двома групами ознак:

1. функціональною роллю у системі забезпечення стійкості (фінансова, кадрова, виробнича, інформаційна, екологічна, інноваційно-технологічна безпека тощо);
2. характером використання та відтворення ресурсів, що визначають потенціал розвитку підприємства.

Застосування цього підходу дозволяє структурувати економічну безпеку як багатовимірну систему та здійснювати її оцінювання на основі діагностики окремих функціональних сфер. Водночас у науковій літературі відзначається

низка методологічних обмежень: відсутність уніфікованих критеріїв формалізації функціональних і ресурсних складових, складність стандартизації методик для підприємств різних галузей, що знижує можливості порівняльного аналізу та інтеграції результатів у макроекономічні оцінки.

Водночас, у ряді напрямів функціонально-ресурсний підхід уже набув відносної усталеності. Зокрема, напрацьовано методики оцінювання:

- фінансової безпеки (аналіз ліквідності, платоспроможності, ризику банкрутства за моделями Альтмана, Спрінгейта, Лісу тощо);
- кадрової безпеки (оцінювання плинності персоналу, компетентнісної відповідності, ризику втрати ключових працівників);
- екологічної безпеки (діагностика техногенних ризиків і екологічних стандартів виробництва);
- інформаційної та кібербезпеки (аналіз рівня захищеності IT-інфраструктури, вразливості до кібератак, залежності від цифрових платформ).

Для наочності логіка функціонально-ресурсного підходу може бути подана у вигляді схеми (рис. 2.1).

Подана логічна схема функціонально-ресурсного підходу до оцінювання економічної безпеки підприємства відображає багаторівневу систему діагностики, що інтегрує зовнішні та внутрішні чинники забезпечення стійкості. На макрорівні оцінювання ґрунтується на методичних рекомендаціях державних органів, законодавчих актах і нормативних положеннях, а також на міжнародних індексах, зокрема глобальної конкурентоспроможності (GCI), інноваційного потенціалу (GII), фінансової стійкості (FSI), рівня кіберзахисту (Global Cybersecurity Index) та орієнтації на сталий розвиток (SDG Index).

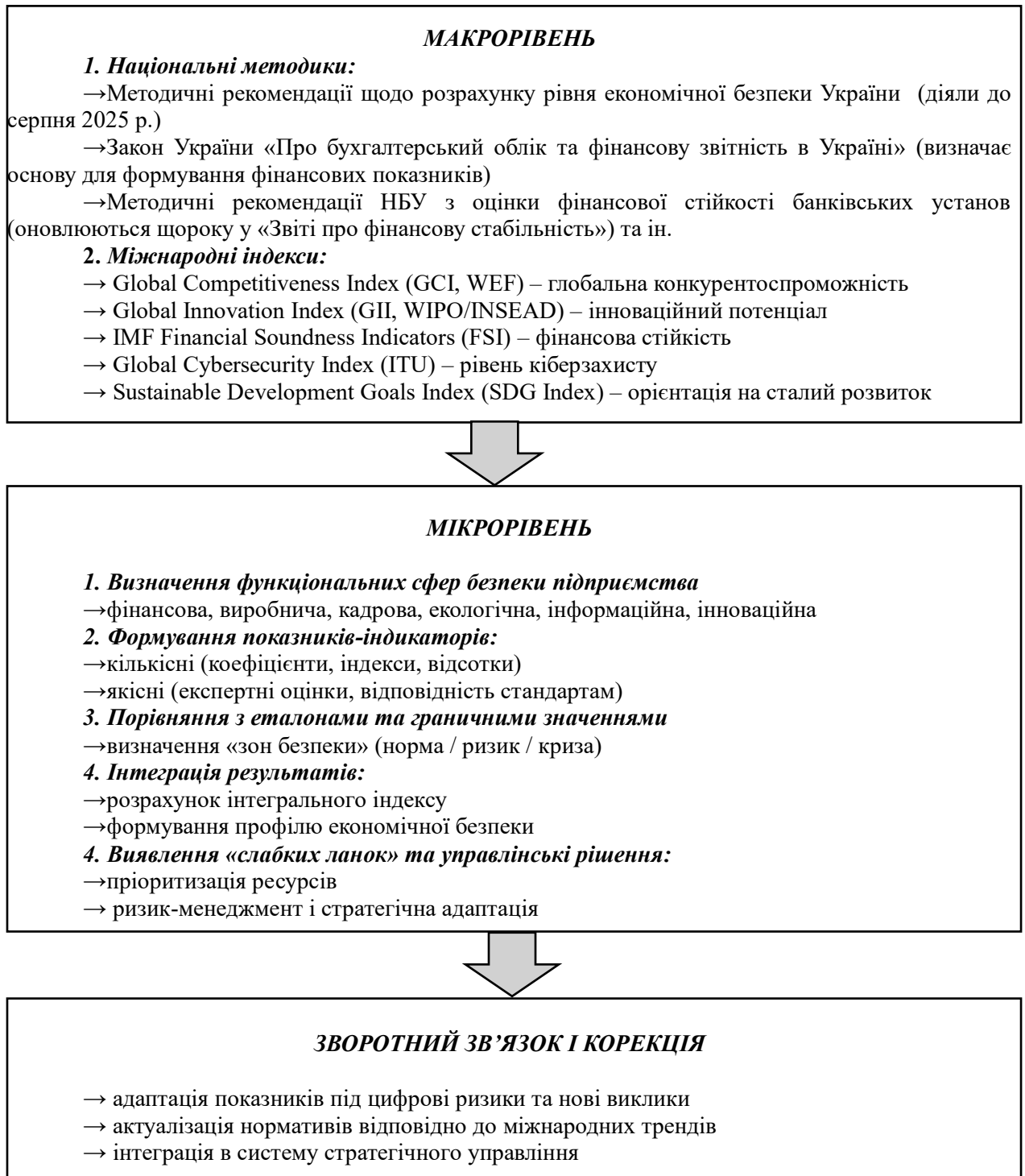


Рис. 2.1. Логічна схема функціонально-ресурсного підходу до оцінювання економічної безпеки підприємства

Джерело: авторська розробка.

Це дозволяє враховувати як національні методики розрахунку, так і глобальні стандарти, що формує комплексну рамку оцінювання економічної безпеки. На мікрорівні здійснюється деталізація внутрішніх параметрів

діяльності підприємства, які охоплюють фінансову, виробничу, кадрову, екологічну, інформаційну та інноваційну безпеку. У межах цього блоку відбувається виокремлення функціональних сфер, формування показників-індикаторів кількісного та якісного характеру, їх порівняння з еталонними й граничними значеннями, інтеграція результатів у вигляді інтегрального індексу та побудова профілю економічної безпеки. Такий підхід дозволяє виявляти слабкі місця та приймати відповідні управлінські рішення, що сприяє підвищенню рівня адаптивності системи. Важливою складовою є механізм зворотного зв'язку, завдяки якому система коригується відповідно до нових цифрових ризиків, змін у зовнішньому середовищі та міжнародних трендів, що уможливорює її інтеграцію в стратегічне управління підприємством.

Таким чином, представлена логічна схема функціонально-ресурсного підходу дає змогу розглядати економічну безпеку підприємства не як ізольований фінансовий стан, а як результат взаємодії ресурсних, виробничих, інвестиційних, інформаційних та управлінських параметрів його функціонування.

Водночас формування системи показників оцінювання потребує врахування того середовища, у межах якого підприємства здійснюють господарську діяльність. У 2020–2024 рр. таке середовище характеризувалося поєднанням макроекономічної нестабільності, інфляційного тиску, різкої зміни інвестиційної активності, воєнних ризиків і прискорення цифровізації бізнес-процесів. Саме тому подальше обґрунтування системи індикаторів економічної безпеки підприємства доцільно здійснювати з урахуванням статистичних параметрів, що відображають ключові зовнішні умови її формування.

Таблиця 2.1

Макроекономічні та інвестиційні умови формування економічної безпеки підприємств України у 2020–2024 рр.

Показник	2020	2021	2022	2023	2024	Аналітичне значення для оцінювання економічної безпеки підприємств
Реальний ВВП, зміна до попереднього року, %	-3,8	3,4	-28,8	5,3	2,9	Відображає загальний рівень макроекономічної стійкості та глибину зовнішніх шоків, що впливають на діяльність підприємств
Споживча інфляція, грудень до грудня попереднього року, %	5,0	10,0	26,6	5,1	12,0	Характеризує ціновий тиск на витрати, оборотний капітал, купівельну спроможність і фінансову стійкість підприємств
Капітальні інвестиції, млрд грн	419,8	528,8	279,6	395,5	534,4	Відображають інвестиційну спроможність економіки та обґрунтовують включення інвестиційно-інноваційної складової до системи оцінювання
Номінальна зміна обсягу капітальних інвестицій до попереднього року, %	-28,2	26,0	-47,1	41,4	35,1	Показує нестабільність інвестиційного циклу та залежність модернізації підприємств від кризових, воєнних і цінових чинників

Джерело: складено автором за [172].

Примітка: показник зміни обсягу капітальних інвестицій розраховано за даними про їх обсяг у фактичних цінах. Він характеризує номінальну динаміку інвестицій, а не індекс капітальних інвестицій у порівнянних цінах.

Дані табл. 2.1 засвідчують, що у 2020–2024 рр. економічна безпека підприємств України формувалася в умовах високої амплітуди макроекономічних коливань. Після скорочення реального ВВП у 2020 р. та часткового відновлення у 2021 р. найбільш різке падіння відбулося у 2022 р., коли повномасштабна війна зумовила скорочення реального ВВП на 28,8 %. Водночас позитивна динаміка 2023–2024 рр. свідчить не про повне відновлення безпекового середовища, а радше про поступову адаптацію економіки до функціонування в умовах воєнних ризиків.

Особливо показовою є динаміка капітальних інвестицій. Їх номінальний обсяг скоротився з 528,8 млрд грн у 2021 р. до 279,6 млрд грн у 2022 р., що відображає різке звуження інвестиційних можливостей підприємств у перший рік повномасштабної війни. Подальше зростання цього показника до 534,4 млрд грн у 2024 р. засвідчує поступове номінальне відновлення інвестиційної активності. Водночас така динаміка залишається нестабільною, оскільки показники наведені у фактичних цінах і відображають не лише зміну реального обсягу інвестицій, а й вплив цінового чинника. Це обґрунтовує необхідність включення до системи оцінювання економічної безпеки не лише фінансових показників, а й індикаторів інвестиційної, інноваційної та ресурсної спроможності підприємства.

Разом із макроекономічними та інвестиційними чинниками дедалі більшого значення набуває цифровий вимір економічної безпеки підприємств. Цифровізація створює нові можливості для підвищення ефективності управління, розширення каналів збуту, автоматизації бізнес-процесів і використання даних у прийнятті рішень. Водночас вона формує новий контур ризиків, пов'язаний із кіберзагрозами, залежністю від цифрової інфраструктури, недостатністю цифрових компетентностей та вразливістю інформаційних систем. Тому інформаційна та інноваційна складові мають розглядатися як обов'язкові елементи системи оцінювання економічної безпеки підприємства.

Таблиця 2.2

Показники цифрової готовності підприємств України у 2020–2024 рр.

Показник	2020	2021	2022	2023	2024	Аналітичне значення для системи оцінювання економічної безпеки
Частка підприємств, які мають доступ до мережі Інтернет, %	н/д	86,6	85,1	88,8	93,8	Відображає базовий рівень цифрової інтеграції підприємств та можливість використання цифрового моніторингу
Частка підприємств, які здійснювали електронну торгівлю, %	4,9	5,0	6,1	6,9	н/д	Характеризує рівень цифровізації каналів збуту та адаптацію підприємств до електронних форматів взаємодії з ринком
Частка підприємств, які мають вебсайт, %	н/д	35,3	н/д	н/д	38,2	Відображає рівень цифрової присутності підприємств, однак через фрагментарність ряду має допоміжне аналітичне значення

Джерело: складено автором за [172].

Поряд із показниками цифрової готовності підприємств важливим зовнішнім ризиком є зростання інтенсивності кіберзагроз. За даними Держспецзв'язку/CERT-UA, у 2023 р. було опрацьовано 2543 кіберінциденти, а у 2024 р. – 4315 кіберінцидентів, що на 69,8 % більше порівняно з попереднім роком. Це підтверджує, що цифровізація підприємств посилює не лише їх технологічну спроможність, а й залежність від захищеності інформаційної інфраструктури. Саме тому інформаційна складова економічної безпеки має розглядатися не як допоміжна, а як одна з ключових у системі оцінювання.

Дані табл. 2.2 засвідчують, що цифрова готовність підприємств України у 2020–2024 рр. формувалася нерівномірно, однак із помітним посиленням базових параметрів цифрової інтеграції бізнесу. Зокрема, частка підприємств, які мають доступ до мережі Інтернет, зростає з 86,6 % у 2021 р. до 93,8 % у 2024 р., що свідчить про розширення цифрової інфраструктури та створення передумов для використання електронних каналів комунікації, цифрового документообігу, дистанційної взаємодії з контрагентами й елементів цифрового моніторингу господарських процесів.

Водночас наведені дані підтверджують, що наявність доступу до мережі Інтернет ще не означає повноцінної цифрової трансформації бізнес-процесів. Частка підприємств, які здійснювали електронну торгівлю, у 2020–2023 рр. залишалася порівняно низькою, хоча й зросла з 4,9 % до 6,9 %. Це свідчить про повільне поширення цифрових каналів збуту та обмежене використання підприємствами електронних форматів взаємодії з ринком. Подібну ситуацію демонструє й показник наявності вебсайту: за наявними даними, він становив 35,3 % у 2021 р. та 38,2 % у 2024 р., що вказує на поступове, але недостатньо динамічне розширення цифрової присутності підприємств у бізнес-середовищі.

Отже, дані табл. 2.2 дають підстави стверджувати, що цифровізація підприємств України має переважно інфраструктурний характер: базовий доступ до мережі Інтернет поширений значно ширше, ніж практичне використання цифрових інструментів для продажу, комунікації, аналітики та управління. Саме ця асиметрія між технічною доступністю цифрових ресурсів і рівнем їх реального впровадження в бізнес-процеси обґрунтовує необхідність включення до системи оцінювання економічної безпеки підприємства не лише традиційних фінансових і виробничих показників, а й інформаційних та інноваційних індикаторів.

Ризик-орієнтований підхід трансформує традиційну діагностику економічної безпеки, переводячи її у площину ймовірностей і наслідків. Стандарт ISO 31000:2018 є ключовим інструментом у цьому контексті, оскільки він пропонує універсальні принципи, рамку та процеси, що можуть бути інтегровані в систему корпоративного управління незалежно від галузі або масштабу організації [20; 21].

Головні частини ISO 31000 включають принципи, структуру і процес управління ризиками. Принципи встановлюють, як організація має сприймати ризик: як інтегральну частину стратегічних рішень, що вимагає активної участі керівництва, постійного поліпшення, адаптивності та використання найкращих даних. Рамка дозволяє організації впроваджувати функції

управління ризиками в систему управління – через чіткі ролі, процедури та інституційні зв'язки. Процес ISO 31000 деталізує послідовні етапи: ідентифікація – аналіз – оцінювання – обробка – моніторинг – комунікація.

У праці «The Degree of Risk Management Implementation in Enterprises in the Slovak Republic» доведено, що рівень імплементації стандартів ISO безпосередньо впливає на практики управління ризиками в підприємствах різних масштабів. Автори обґрунтовують статистично значиму залежність між застосуванням ISO 9001, 14001, 45001 і 26000 та пріоритетними етапами процесу ризик-менеджменту, включаючи ідентифікацію, аналіз, оцінювання й моніторинг. Зокрема, комбінація ISO 9001, 14001 та 45001 демонструє синергетичний ефект у сфері аналізу ризиків, а ISO 26000 посилює акцент на моніторингових процедурах. Водночас виявлено закономірності у розподілі відповідальності: від відсутності призначених осіб у малому бізнесі до залучення топ-менеджменту у великих компаніях. Отримані результати підтверджують, що інтеграція міжнародних стандартів не обмежується формальною сертифікацією, а виступає дієвим інструментом підвищення системності ризик-орієнтованого управління, що в контексті дисертаційного дослідження розглядається як ключовий чинник зміцнення економічної безпеки підприємств [74].

Окремий вектор модернізації діагностики економічної безпеки підприємства визначається цифровою природою ризиків, які дедалі частіше інтегруються в ядро стратегічного управління. NIST Cybersecurity Framework пропонує універсальну логіку ідентифікації, захисту, виявлення, реагування та відновлення (Identify–Protect–Detect–Respond–Recover), що є інструментом системної інтеграції IT-контролів у бізнес-процеси та побудови вимірюваної кіберстійкості [31]. Цей підхід дозволяє не лише структурувати базові напрями управління кіберризиками, а й формувати метрики, які прямо пов'язують технічний рівень захисту з економічними результатами.

На макрорівні рекомендації Організації економічного співробітництва та розвитку (ОЕСР, англ. OECD) підкреслюють, що цифрові ризики мають не

лише технічний, а насамперед соціально-економічний вимір, адже їхні наслідки виходять далеко за межі корпоративного рівня і можуть впливати на фінансову стабільність, довіру до ринку та стійкість інституцій [74]. В офіційному документі наголошується на необхідності формування інтегрованих механізмів управління цифровими загрозами, які поєднують регуляторні, організаційні та технологічні інструменти. При цьому особлива увага приділяється досягненню балансу між безпекою та відкритістю цифрового середовища: надмірне посилення контролю може знижувати інноваційний потенціал та конкурентоспроможність, тоді як недостатній рівень захисту призводить до зростання вразливостей та втрат у масштабах національної економіки. Це означає, що цифрові показники повинні бути інтегровані у загальну систему діагностики економічної безпеки, а їх моніторинг має розглядатися як невід’ємний елемент політики забезпечення стійкого розвитку. Ігнорування цих параметрів, як зазначає ОЕСР, загрожує виникненням стратегічних дисбалансів між економічною ефективністю та безпекою, що у довгостроковій перспективі здатне обмежувати можливості країни щодо залучення інвестицій та формування сприятливого бізнес-середовища.

З позицій стратегічного менеджменту інтеграція діагностики ризиків і безпеки зі збалансованою системою показників (Balanced Scorecard, BSC) забезпечує зв’язок між цілями, процесами й метриками через причинно-наслідкові ланцюги та карти стратегії; у такій конструкції фінансові та нефінансові індикатори каскадуються до рівня підрозділів і робочих місць, а управлінські рішення підкріплюються вимірюваними орієнтирами ефективності. Класичні роботи Р. Каплана та Д. Нортон фіксують методологічні основи цієї логіки: від формулювання цілей у чотирьох перспективах до використання BSC як системи стратегічного управління, що поєднує показники результату з драйверами створення вартості [75].

У межах ризик-орієнтованого підходу BSC стає каркасом для узгодження KPI з KRI: метрики продуктивності та стійкості розглядаються в

єдиній моделі, де ризикові пороги, толерантність до відхилень і тригери раннього попередження інтегруються у карти стратегії та операційні дашборди; сучасні огляди підтверджують зростання дослідницької уваги до пар «KPI–KRI» і демонструють їх позитивний зв'язок із підвищенням результативності та якістю управління ризиками, тоді як професійні настанови підкреслюють необхідність формального зв'язування KRI з бізнес-цілями та ризик-апетитом [76; 77].

Дослідження українських науковців засвідчують практичну придатність BSC для підприємств: типові карти стратегії й набір KPI дозволяють адаптувати систему до умов локальних ринків і включати безпекові індикатори (процесні, інформаційні, інноваційні) у регулярний моніторинг, що посилює управлінську керованість і прозорість [78].

Водночас розвиток індикаторних та інтегральних моделей оцінювання економічної безпеки, зокрема побудова інтегральних індексів та уніфікація процедур, надає BSC додану цінність: профіль безпеки підприємства, отриманий через інтегральний індекс, логічно вбудовується в «карту стратегії» і дозволяє калібрувати KPI/KRI відповідно до виявлених «вузьких місць» та цільових порогів стійкості.

В українській науковій літературі доведено, що концепція Balanced Scorecard (BSC) може бути адаптована для моніторингу економічної безпеки, зокрема у частині процесних та інформаційних метрик, а також для виявлення структурних вразливостей у цифрових бізнес-моделях. Останні дослідження підтверджують доцільність переходу до комбінованих моделей діагностики, які інтегрують індикаторний аналіз, ризик-орієнтовані процедури, інтегральні індекси та сценарне прогнозування. Такі підходи ґрунтуються на багатовимірному аналізі показників і дозволяють відображати динамічний характер загроз та ризиків цифрової трансформації. Зокрема, модель інтегральної оцінки економічної безпеки, запропонована С. Пілецькою, Т. Коритько та Є. Ткаченком, демонструє можливість поєднання фінансових та нефінансових індикаторів у єдиній діагностичній системі, що забезпечує

системність і комплексність оцінки [79]. Водночас, дослідження Т. Ткаченко та А. Гречка акцентує увагу на необхідності узагальнення різних методичних підходів до оцінювання безпеки промислових підприємств, зокрема через розробку стандартизованих процедур і уніфікацію інтегральних показників [80].

У результаті методологічне поле діагностики поступово еволюціонує у напрямі мультикритеріального та стандартизованого оцінювання, що узгоджується з міжнародними рамковими документами ISO 31000, NIST Cybersecurity Framework та рекомендаціями OECD, забезпечуючи можливість порівняння результатів між країнами та галузями. Такий підхід посилює практичну значущість моделей оцінювання, оскільки дозволяє підприємствам адаптивно реагувати на ризики цифровізації та формувати довгострокову стратегію економічної безпеки.

У вітчизняній науковій літературі дедалі більше наголошується на необхідності *синтезу індикаторного, функціонально-ресурсного та ризик-орієнтованого підходів* до оцінювання економічної безпеки підприємств, що дозволяє розширити діагностичний інструментарій від обліково-аналітичних процедур до стратегічного моніторингу. У цьому контексті саме індикаторний підхід, адаптований до багатовимірності економічної безпеки, набуває особливого значення, оскільки він забезпечує практичну основу для оцінювання її рівня за сукупністю взаємопов'язаних складових.

Методика оцінки у межах індикаторного підходу передбачає структурування економічної безпеки на ключові складові: фінансову, інформаційну, кадрову, виробничу, інноваційну та екологічну. Кожна з них оцінюється за системою кількісних і якісних індикаторів, що характеризують здатність підприємства протидіяти внутрішнім та зовнішнім загрозам. На першому етапі здійснюється відбір показників на основі офіційних джерел (звітності підприємств, даних Державної служби статистики України, аналітичних матеріалів Національного банку України та міжнародних індексів). Далі індикатори приводяться до єдиної шкали вимірювання шляхом

нормування та стандартизації, що забезпечує їхню порівнянність у динаміці та в міжгалузевому розрізі. На наступному етапі проводиться визначення вагових коефіцієнтів для окремих складових, яке здійснюється або на основі експертних оцінок, або із застосуванням методів багатofакторного аналізу. Завершальним кроком є інтеграція часткових оцінок у зведений індекс економічної безпеки, що дозволяє сформулювати узагальнене уявлення про рівень стійкості підприємства.

Особливе місце у цій структурі займає інноваційна складова, оскільки саме вона визначає стратегічну перспективу розвитку підприємства, його здатність адаптуватися до цифрової трансформації та протидіяти зовнішнім шокам. Як обґрунтовано у сучасних дослідженнях [64], показники інноваційної активності (обсяг інвестицій у науково-дослідні та дослідно-конструкторські роботи, частка інноваційної продукції в загальному обсязі реалізації, патентна активність, рівень цифровізації бізнес-процесів) виступають провідними детермінантами довгострокової стійкості підприємств і слугують випереджальними індикаторами майбутніх фінансових результатів.

Таким чином, адаптований індикаторний підхід у розрізі складових економічної безпеки є практичним інструментом реалізації комплексної методики діагностики, яка поєднує вимірювані параметри із стратегічними орієнтирами розвитку підприємства. Його використання дозволяє сформулювати не лише статичну оцінку поточного стану, а й динамічну картину змін рівня безпеки у часі, що набуває особливої ваги в умовах цифровізації та посилення зовнішніх ризиків.

Для системного аналізу рівня економічної безпеки підприємств доцільним є виокремлення її ключових складових та визначення відповідних індикаторів, які підлягають моніторингу й оцінюванню. Узагальнені результати подано у табл. 2.3.

Таблиця 2.3

Складові економічної безпеки підприємства та система індикаторів для їх діагностики

Складова економічної безпеки	Змістове наповнення	Приклади ключових індикаторів	Джерела даних
1	2	3	4
Фінансова	Здатність підприємства забезпечувати платоспроможність, фінансову незалежність та стійкість капіталу	коефіцієнт поточної та швидкої ліквідності; коефіцієнт автономії; рентабельність активів (ROA), рентабельність власного капіталу (ROE); коефіцієнт покриття відсотків	Офіційна фінансова звітність підприємств (за НП(С)БО або МСФЗ); статистичні матеріали Державної служби статистики України; аналітичні огляди Національного банку України («Звіт про фінансову стабільність»).
Інформаційна	Стан захищеності даних і надійності інформаційних систем	наявність сертифікованих систем управління інформаційною безпекою; частота інцидентів; середній час реагування; частка критично важливих ресурсів під захистом	Внутрішні документи підприємства (регламенти, політики безпеки); міжнародні стандарти інформаційної безпеки (ISO/IEC 27001:2022, ISO/IEC 27002:2022); результати зовнішніх аудитів; аналітичні звіти ІТ-асоціацій.
Кадрова	Спроможність підприємства зберігати та розвивати кадровий потенціал	коефіцієнт плинності кадрів; рівень забезпеченості ІТ-спеціалістами; витрати на підвищення кваліфікації; середня тривалість зайнятості	Дані кадрових служб підприємств; результати соціологічних опитувань працівників; офіційна статистика ДССУ («Зайнятість», «Оплата праці»); міжнародні індекси цифрових компетентностей (DESI, OECD Skills Outlook).

Продовження табл. 2.3

1	2	3	4
Виробнича (операційна)	Безперервність та ефективність виробничих процесів	коефіцієнт завантаження потужностей; втрати від збоїв у постачанні; тривалість відновлення виробництва після зупинок	Операційна та виробнича звітність підприємств; статистика ДССУ (розділ «Промисловість»); галузеві звіти та бенчмарки профільних асоціацій.
Інноваційна	Здатність підприємства до впровадження інновацій і адаптації до цифрової трансформації	частка витрат на науково-дослідні та дослідно-конструкторські роботи; частка інноваційної продукції; кількість патентів; рівень цифровізації бізнес-процесів	Дані офіційної статистики; міжнародні індекси інноваційності (Global Innovation Index, WIPO); результати внутрішніх аудитів підприємств; наукові дослідження.
Екологічна	Дотримання регуляторних та екологічних вимог	кількість і сума штрафних санкцій; частота виявлених порушень; наявність програм екологічної модернізації	Офіційні звіти контролюючих органів (Міністерство захисту довкілля та природних ресурсів України, Державна екологічна інспекція); внутрішня комплаєнс-звітність підприємств; аудиторські висновки щодо відповідності стандартам.
Стійкість до зовнішніх загроз	Здатність підприємства адаптуватися до економічних криз, воєнних дій та технологічних збоїв	тривалість відновлення операцій; диверсифікація ринків; наявність планів безперервності діяльності; участь у програмах державної підтримки	Аналітичні матеріали НБУ (макропруденційні ризики); міжнародні звіти ОЕСР з питань економічної стійкості; Стратегія економічної безпеки України до 2025 року; дані Світового банку про вплив зовнішніх шоків.

Джерело: авторська розробка.

Таким чином, систематизація складових економічної безпеки підприємства та визначення відповідних індикаторів дозволяє забезпечити комплексну діагностику її рівня. Представлені у таблиці показники є об'єктивними та вимірюваними, що зумовлює можливість їх використання у практиці фінансового аналізу, кадрового та інформаційного моніторингу, а також у стратегічному плануванні. Особливої ваги набуває те, що більшість із запропонованих індикаторів можуть бути розраховані на основі відкритих джерел даних: фінансової звітності, складеної за національними (НП(С)БО) або міжнародними стандартами (МСФЗ), статистичних матеріалів державних органів та міжнародних індексів, що забезпечує прозорість і відтворюваність діагностичного інструментарію. Побудова такої системи індикаторів дозволяє не лише оцінювати поточний стан безпеки підприємств, а й прогнозувати можливі зміни в умовах зростання ризиків і цифрової трансформації.

У роботі уже зазначалося, що для вітчизняної методології діагностики економічної безпеки актуальним є синтез індикаторного, функціонально-ресурсного та ризик-орієнтованого підходів. На цьому фундаменті оцінка стійкості підприємств до зовнішніх загроз постає як логічне продовження, оскільки відображає їхню здатність адаптуватися до кризових явищ та екзогенних шоків.

За оцінкою Міжнародного валютного фонду, у 2022 році оперативні заходи Національного банку України та комерційних банків, зокрема запровадження планів забезпечення безперервності бізнесу та підтримка функціонування фінансових інститутів, допомогли зберегти базову фінансову стабільність у період гострої фази кризи [81]. НБУ у «Звіті про фінансову стабільність» за грудень 2022 р. підтвердив, що попри значний тиск, фінансова система продовжувала працювати безперервно, забезпечуючи доступ клієнтів до коштів та безперебійну роботу платіжної інфраструктури [82].

У 2023 році виклики зберігалися, проте національна фінансова система продемонструвала достатню резилієнтність. Як відзначено у «Звіті про фінансову стабільність» НБУ за грудень 2023 р., ключовим фактором стійкості

стала значна міжнародна фінансова підтримка та поступове пристосування бізнесу до нових умов господарювання [83]. Таким чином, вже у 2023 р. стійкість підприємств оцінювалася через поєднання фінансових результатів, кадрових втрат і галузевих диспропорцій.

При цьому проявилася чітка галузева диференціація стійкості. Підприємства аграрного сектору та енергетики залишалися більш вразливими до зовнішніх загроз через руйнування виробничої та транспортної інфраструктури, блокування логістичних ланцюгів, а також зростання собівартості продукції внаслідок енергетичних шоків і перебоїв у постачанні ресурсів. Такі фактори істотно знижували їхню здатність до відновлення та вимагали додаткових державних і міжнародних механізмів підтримки. Натомість підприємства сектору інформаційно-комунікаційних технологій продемонстрували відносну стійкість, що було зумовлено їхньою високою мобільністю, орієнтацією на експорт та широким застосуванням цифрових інструментів ведення бізнесу, які дозволили зберегти доступ до зовнішніх ринків навіть в умовах воєнних дій. Водночас розвиток цифрових компетентностей персоналу та впровадження хмарних сервісів мінімізували ризики втрати даних і забезпечили неперервність бізнес-процесів. Аналітичні матеріали Організації економічного співробітництва та розвитку підтверджують, що саме цифрова трансформація бізнесу стала ключовим чинником підвищення адаптивності українських підприємств у кризових умовах, сприяючи не лише їх оперативній стабілізації, а й формуванню передумов для довгострокової відбудови та інтеграції у глобальні ринки [84].

У контексті оцінки економічної безпеки підприємств доцільним є застосування кейс-аналізу, що дозволяє простежити специфіку реагування компаній різних секторів економіки на фінансові виклики та цифрові ризики. У секторі енергетики показовим є приклад НЕК «Укренерго», яка у 2022–2023 рр. зіткнулася зі значним зростанням інтенсивності кібератак. За офіційними повідомленнями, після початку повномасштабного вторгнення кількість атак на цифрову інфраструктуру компанії збільшилася утричі порівняно з

довоєнним періодом, проте жодна з них не призвела до відключень або суттєвих порушень у функціонуванні енергетичної системи [85]. Така стійкість стала можливою завдяки багаторічній підготовці, зокрема впровадженню комплексної системи кіберзахисту, що охоплює адміністративні та технологічні мережі і відповідає найвищим міжнародним стандартам. Система включає моніторинг інцидентів у реальному часі, регулярні стрес-тестування критичної інфраструктури та застосування сучасних протоколів реагування. Це дозволило компанії не лише зберегти безперервність роботи, а й сформувати приклад найкращих практик у сфері інформаційної безпеки для підприємств критичної інфраструктури.

У аграрному секторі показовим є кейс діяльності агрохолдингу МХП, який у 2022–2023 рр. функціонував в умовах суттєвого зростання логістичних витрат та підвищених фінансових ризиків. Реакцією компанії на зовнішні виклики стало активне впровадження цифрових технологій точного землеробства, систем управління ланцюгами постачання та інвестиції у науково-дослідні й дослідно-конструкторські роботи. Згідно з офіційним річним звітом за 2023 р., частка витрат на інноваційні проєкти перевищила 3% доходів підприємства, при цьому компанія зберегла патентну активність та розширила використання технологій точного землеробства й цифрових систем управління виробничими процесами [86]. Отже, інноваційна складова виступає визначальним чинником підтримання економічної безпеки агробізнесу, забезпечуючи його адаптивність до турбулентного середовища.

У секторі інформаційно-комунікаційних технологій (ІКТ) показовим прикладом є діяльність компанії SoftServe, яка навіть в умовах воєнних дій зуміла зберегти стійкість бізнес-моделі та продовжила нарощувати експортний потенціал. Особливу увагу компанія приділила розвитку мережі науково-дослідних і дослідно-конструкторських (R&D) центрів як в Україні, так і за її межами, що дозволило диверсифікувати ризики та забезпечити безперервність інноваційної діяльності. Згідно з офіційними статистичними даними Державної служби інтелектуальної власності України, у 2022 році саме

підприємства сектору інформаційно-комунікаційних технологій продемонстрували одне з найбільших зростань кількості поданих заявок на винаходи та корисні моделі серед усіх сфер економіки [87]. Це свідчить про те, що інноваційна складова у поєднанні з цифровізацією бізнес-процесів виступає ключовим чинником зміцнення економічної безпеки підприємств ІКТ-сектору, забезпечуючи їхню конкурентоспроможність та довгострокову стійкість навіть у періоди екстремальних зовнішніх викликів.

У машинобудівному секторі показовим є приклад ПАТ «Мотор Січ», яке після початку воєнних дій зазнало значних втрат у логістичних каналах та ринках збуту, що зумовило суттєве зниження рівня економічної безпеки компанії. Наявна у відкритому доступі консолідована фінансова звітність за 9 місяців, що закінчилися 30 вересня 2021 р. фіксує фінансові диспропорції, пов'язані з високою залежністю від залучених ресурсів, а також відзначає необхідність модернізації виробничих потужностей і технологічного оновлення [88]. Відсутність офіційних звітів за 2022–2024 рр. унеможливлює комплексний аналіз інноваційної динаміки підприємства, однак ретроспективні дані дають змогу окреслити вразливість машинобудівних підприємств до екзогенних факторів, зокрема воєнних ризиків, інфраструктурних руйнувань і блокування зовнішніх ринків. Така ситуація підкреслює потребу у прискореній цифровізації виробничих процесів, впровадженні інструментів автоматизованого контролю якості та посиленні патентної активності як складових довгострокової стратегії економічної безпеки. У цьому контексті приклад «Мотор Січі» репрезентує ширші тенденції машинобудівного сектору України, який в умовах сучасних викликів потребує структурної трансформації, залучення інвестицій у високотехнологічні рішення та інтеграції у глобальні інноваційні ланцюги.

Аналіз кейсів українських підприємств різних секторів засвідчив, що їхня економічна безпека формується під впливом як внутрішніх стратегій, так і зовнішніх викликів, зокрема воєнних дій, глобальних економічних шоків та цифрових ризиків. У сфері енергетики ключовим напрямом забезпечення

стійкості виступає розбудова комплексних систем кіберзахисту, що дозволяють зберігати безперервність роботи критичної інфраструктури. Аграрні компанії зосереджуються на впровадженні технологій точного землеробства, цифрових рішень для управління виробництвом і підвищенні витрат на інновації та НДДКР, що зміцнює їхній потенціал у кризових умовах. Підприємства сектору інформаційно-комунікаційних технологій демонструють відносно найвищу резилієнтність завдяки інноваційній активності, розширенню мереж науково-дослідних і дослідно-конструкторських центрів і зростанню патентної активності, що безпосередньо трансформується у зростання конкурентоспроможності. Натомість машинобудівні підприємства, зокрема «Мотор Січ», виявилися найбільш уразливими до зовнішніх шоків, що пов'язано з високою залежністю від ринків збуту, логістичних ланцюгів та потребою в технологічній модернізації. Загалом кейс-аналіз показує, що спільним інтегрувальним чинником для підвищення рівня економічної безпеки є інноваційна активність, цифровізація та диверсифікація бізнес-процесів, які створюють фундамент для довгострокової стійкості та адаптивності українських підприємств у глобально турбулентному середовищі.

2.2. Цифрові фактори та ризики економічної безпеки підприємств

У контексті висвітлених у попередньому підрозділі теоретико-методологічних засад оцінювання економічної безпеки доцільно розглянути специфічний вплив цифровізації як багатофакторного детермінанта ризикогенезу. З економічної точки зору, цифровізація стимулює підвищення продуктивності праці, зменшення трансакційних витрат, оптимізацію ланцюгів постачання та пришвидшення обороту капіталу. Вона змінює структуру витрат підприємств, трансформує моделі створення доданої вартості та сприяє формуванню нових ринкових ніш. Проте одночасно із цим посилюється залежність бізнесу від цифрових інфраструктур і платформ, що

підвищує рівень вразливості до зовнішніх та внутрішніх шоків, у тому числі кіберзагроз, регуляторних обмежень і технологічної монополізації.

Цифровізація змінює саму природу економічних ризиків: на перший план виходять ризики інформаційної асиметрії, втрати даних, збоїв у функціонуванні цифрових платформ і мереж, що здатні паралізувати фінансові потоки та підривати стійкість підприємств і державних інституцій. Наявні механізми забезпечення безпеки дедалі менше відповідають потребам економіки, оскільки новітні ризики не зводяться лише до технічних чи операційних загроз, а мають стратегічний характер і прямо впливають на конкурентоспроможність, інвестиційну привабливість і макроекономічну стабільність.

Отже, цифровізація виступає чинником ризикогенезу, який здатний не лише змінювати конфігурацію виробничих і фінансових відносин, але й провокувати виникнення «цифрових пасток» – ситуацій, коли економічний ефект від інновацій перекривається витратами на ліквідацію кризових явищ, пов'язаних із кіберінцидентами чи технологічною залежністю. Це зумовлює потребу у формуванні нової моделі управління цифровими ризиками, що враховує економічні наслідки кіберзагроз, регуляторну турбулентність і високу концентрацію ринкової влади цифрових платформ. Такий підхід дає змогу не лише зменшувати потенційні втрати, але й вибудовувати довгострокову стратегію економічної стійкості в умовах глобальної цифрової конкуренції.

В умовах цифрової трансформації економіки підприємства стикаються з комплексом нових викликів, які суттєво впливають на їхню стійкість та конкурентоспроможність. Цифрові ризики охоплюють широкий спектр загроз: від кіберінцидентів і регуляторної невизначеності до надмірної залежності від цифрових платформ, що виконують функції критичної інфраструктури. Їх систематизація дозволяє не лише виявити ключові напрями ризикогенезу, але й забезпечити основу для побудови ефективної моделі управління економічною безпекою. Запропонована схема відображає основні групи цифрових ризиків, що формуються під впливом сучасних технологічних і

регуляторних тенденцій, а також демонструє їх взаємозв'язок у контексті формування адаптивних стратегій безпеки.

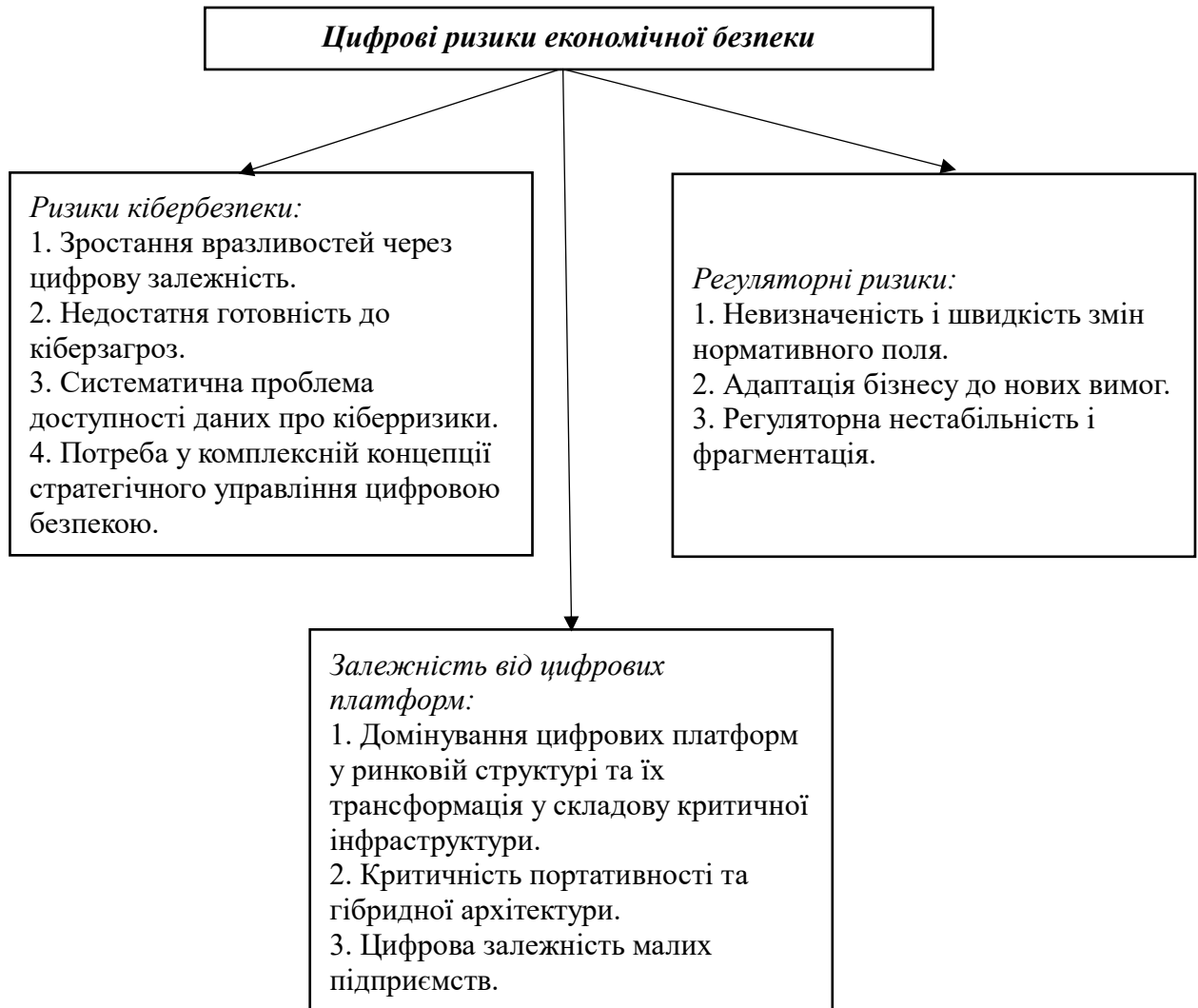


Рис. 2.2. Структуризація цифрових ризиків економічної безпеки підприємства в умовах цифрової трансформації

Джерело: авторська розробка.

Охарактеризуємо блок ризиків кібербезпеки, представлений на рисунку 2.2. Насамперед, варто звернути увагу на зростання вразливостей через цифрову залежність. Поглиблення цифрової інтеграції підприємств у глобальні виробничі й фінансові ланцюги, активне використання хмарних обчислень, технологій Інтернету речей (IoT) та платформної взаємодії призводить до суттєвого розширення так званої «поверхні атаки». Це означає,

що кожне нове цифрове з'єднання, програмний додаток чи інтегрований сервіс стає потенційним каналом для здійснення кібератаки. З економічної точки зору, такі вразливості збільшують очікувані збитки підприємств, які проявляються у зростанні трансакційних витрат, втратах виручки через зупинку бізнес-процесів, додаткових витратах на відновлення даних та репутаційних ризиках. Дослідження IBM (International Business Machines Corporation – однієї з найбільших транснаціональних корпорацій у сфері інформаційних технологій) свідчать, що середня вартість витоку даних у 2024 році становила 4,88 млн доларів США на один інцидент, що безпосередньо впливає на прибутковість та капіталізацію підприємств [89].

Другим видом виступає недостатня готовність до кіберзагроз. У більшості підприємств, особливо малого та середнього бізнесу, спостерігається структурний розрив між масштабами потенційних загроз та рівнем зрілості систем захисту. Це стосується як фінансових обмежень на впровадження систем кіберзахисту, так і браку висококваліфікованих фахівців. У макроекономічному вимірі такий дисбаланс проявляється у феномені «кібернерівності», коли частина суб'єктів господарювання є добре захищеною, тоді як інша – залишається вразливою. Така асиметрія ризиків створює загрозу для стійкості цілих секторів економіки, адже атака на менш захищену ланку здатна поширитися на партнерів у ланцюгах постачання. Опитування Allianz Risk Barometer 2025 підтверджує, що кіберінциденти кілька років поспіль займають перше місце серед глобальних бізнес-ризиків, випереджаючи фінансові чи регуляторні загрози [90].

Третім різновидом виступає систематична проблема доступності даних про кіберризики. Аналіз економічних наслідків кібератак ускладнюється браком структурованих і достовірних статистичних даних. Більшість підприємств не розкривають інформацію про масштаби та фінансові втрати, пов'язані з інцидентами, а на ринку кіберстрахування ці дані часто є конфіденційними. Це створює інформаційну асиметрію, що унеможливорює коректне оцінювання частоти та тяжкості інцидентів, а також побудову

економетричних моделей прогнозування ризиків. Як наслідок, інвестиції у кібербезпеку часто мають фрагментарний характер, а дисконтні ставки для таких проєктів завищуються, що знижує їхню ефективність [91].

Четвертим видом виступає потреба у комплексній концепції стратегічного управління цифровою безпекою. Йдеться про те, що цифрова безпека не може розглядатися винятково в технічному вимірі, адже вона має безпосередні економічні наслідки для підприємств і національної економіки в цілому. Порушення в системах безпеки призводять не лише до прямого збитку у вигляді фінансових втрат, а й до підвищення вартості капіталу, зниження інвестиційної привабливості, збільшення витрат на страхування та навіть до втрати доступу до ринків. Тому управління кіберризиками повинно бути інтегроване у стратегічне планування підприємства, систему корпоративного управління та механізми оцінювання економічної безпеки.

У цьому контексті Європейський Союз поступово формує нормативну базу, яка задає єдині стандарти управління цифровими ризиками. Зокрема, Директива NIS2 (Network and Information Security Directive 2), що набрала чинності у 2023 році, є оновленою версією першої директиви з кібербезпеки (NIS) [92]. Вона поширює коло обов'язкових до виконання вимог на ширший спектр секторів економіки (зокрема енергетику, транспорт, охорону здоров'я, цифрові послуги) та встановлює суворіші вимоги до управління інцидентами, обміну інформацією і відповідальності керівництва підприємств. Економічна суть цієї директиви полягає в тому, що вона зменшує інформаційну асиметрію на ринку, створює прозорі правила гри для бізнесу та стимулює інвестиції у стійкість, водночас підвищуючи вартість недотримання вимог у вигляді штрафів і санкцій.

Крім того, Регламент DORA (Digital Operational Resilience Act), який набуде чинності з 17 січня 2025 року, спрямований на фінансовий сектор і передбачає обов'язкове впровадження стандартів цифрової операційної стійкості [93]. Він охоплює управління ризиками інформаційно-комунікаційних технологій (ІКТ), проведення тестування стійкості, звітність

про інциденти та контроль взаємодії з третіми сторонами (наприклад, провайдерами хмарних сервісів). З економічної точки зору, DORA має подвійний ефект: з одного боку, він підвищує стабільність фінансової системи та довіру інвесторів, а з іншого — збільшує навантаження на бізнес у вигляді витрат на відповідність регуляторним вимогам.

Таким чином, поява NIS2 та DORA свідчить про те, що цифрова безпека стала невід’ємною складовою економічної безпеки і ключовим фактором конкурентоспроможності. Для українських підприємств, які орієнтуються на інтеграцію у європейський ринок, адаптація до цих стандартів є не лише питанням технологічної модернізації, але й фактором забезпечення довгострокової фінансової стійкості. Відтак, комплексна концепція стратегічного управління цифровою безпекою повинна охоплювати поєднання технічних, організаційних та економічних інструментів, що дозволяє мінімізувати ризики, знизити вартість капіталу та сформувати умови для інноваційного розвитку в умовах цифрової економіки.

Регуляторні ризики у сфері цифровізації проявляються насамперед у невизначеності та високій динаміці змін нормативного поля. Стрімкий розвиток цифрової економіки супроводжується постійним оновленням регуляторного середовища: ухвалюються нові директиви Європейського Союзу, регламенти у сфері захисту даних, вимоги до кіберстійкості фінансових установ, змінюються стандарти електронної ідентифікації та цифрових послуг. Для бізнесу така нормативна турбулентність означає зростання економічної невизначеності, яка проявляється не лише у правових ризиках, а й у перерозподілі фінансових ресурсів на користь витрат, пов’язаних з адаптацією.

Насамперед, підприємства змушені збільшувати трансакційні витрати, що включають розробку нових внутрішніх політик, оновлення ІТ-інфраструктури, навчання персоналу та залучення юридичних і консалтингових послуг. У середньостроковій перспективі це знижує їхню операційну ефективність та впливає на конкурентоспроможність, оскільки

фінансові ресурси, які могли бути інвестовані у розвиток, спрямовуються на забезпечення нормативної відповідності.

Додатковим економічним наслідком є підвищення ризику прямого фінансового збитку через помилки у виконанні нових регуляторних вимог або несвоєчасну їх імплементацію. Це може призвести до накладання штрафів, блокування доступу до ринків ЄС чи до обмеження співпраці з міжнародними партнерами. Так, відповідно до вимог Директиви NIS2, керівництво підприємств несе персональну відповідальність за управління кіберризиками, а штрафи за порушення сягають до 10 млн євро або 2 % річного обороту компанії [92].

У макроекономічному вимірі висока динаміка змін нормативного поля може спричиняти ефект регуляторного шоку, коли підприємницьке середовище стикається з раптовим зростанням витрат на комплаєнс, що знижує інвестиційну активність та уповільнює темпи економічного зростання. Це особливо критично для країн із перехідною економікою, таких як Україна, де гармонізація законодавства з європейськими стандартами потребує значних ресурсів від бізнесу. Невизначеність регуляторного середовища створює суттєві бар'єри для довгострокового планування та обмежує інноваційну динаміку підприємств, що прямо впливає на економічну безпеку держави [94].

Регуляторні ризики також проявляються через складність адаптації бізнесу до нових нормативних вимог. Для підприємств це означає необхідність постійної модернізації систем управління, впровадження додаткових механізмів звітності, сертифікації та контролю. Такі процеси вимагають значних інвестицій, що особливо відчутно для малого та середнього бізнесу, який не володіє достатнім фінансовим і кадровим ресурсом. У результаті витрати на дотримання норм часто перевищують потенційні вигоди від цифрової трансформації, що уповільнює темпи інноваційного розвитку та знижує гнучкість підприємств у конкурентному середовищі.

Економічно це проявляється у перерозподілі капіталу: кошти, які могли б бути спрямовані на розширення виробництва чи розвиток нових продуктів, витрачаються на виконання регуляторних приписів. Додатковим наслідком є зростання собівартості продукції та послуг, що знижує їхню конкурентоспроможність на внутрішньому та міжнародному ринках. Дослідження українських науковців підтверджують, що гармонізація вітчизняних стандартів із європейськими, попри стратегічну необхідність, створює короткострокові витрати, які бізнес не завжди здатний швидко компенсувати за рахунок підвищення продуктивності чи залучення інвестицій [94].

У довгостроковій перспективі, однак, належна адаптація до європейських вимог здатна посилити позиції українських підприємств на міжнародних ринках, забезпечити зниження ризиків від кібератак та підвищити довіру інвесторів. Проте у коротко- й середньостроковому вимірі цей процес залишається значним викликом, який зумовлює додаткові економічні ризики і впливає на фінансову стійкість підприємств.

Регуляторна нестабільність і фрагментація створюють для бізнесу додатковий пласт невизначеності, який безпосередньо впливає на економічну безпеку. У ситуації, коли нормативні вимоги змінюються надто часто або відрізняються залежно від юрисдикції, підприємства опиняються в умовах подвійного навантаження: з одного боку – необхідність швидко реагувати на нові правила, з іншого – потреба синхронізувати внутрішні процеси з міжнародними стандартами. Це зумовлює підвищення трансакційних витрат, ризик невиконання норм і посилення залежності від зовнішніх консультантів.

З економічного погляду, така фрагментація регуляторного середовища сприяє виникненню «регуляторних розривів», коли різні вимоги на національному, європейському та міжнародному рівнях не узгоджуються між собою. Для підприємств це означає додаткові витрати на дублювання звітності, адаптацію ІТ-систем до кількох стандартів одночасно, а також втрату часу на

погодження процедур. У результаті знижується ефективність управління ризиками та уповільнюється інтеграція у глобальні ринки.

В умовах України регуляторна нестабільність має ще й інституційний вимір: законодавчі ініціативи у сфері цифровізації та кіберзахисту часто розробляються під тиском зовнішніх чинників або внаслідок політичних змін, що ускладнює формування прогнозованого середовища для інвесторів. Відсутність системної та узгодженої регуляторної політики у сфері цифрової безпеки може стати бар'єром для інноваційного розвитку та знизити здатність підприємств протидіяти зовнішнім загрозам.

Макроекономічні наслідки такої нестабільності полягають у зростанні ризик-премії для інвестицій у цифровий сектор, що відображається у вартості капіталу та знижує темпи модернізації критичної інфраструктури. У довгостроковій перспективі це може призвести до уповільнення цифрової трансформації економіки та посилення залежності від зовнішніх технологічних рішень.

Залежність від цифрових платформ сьогодні постає як один із ключових викликів економічної безпеки, що набуває ознак системного ризику. Глобальні цифрові екосистеми, зокрема Amazon Web Services, Microsoft Azure та Google Cloud, зосереджують у своїх руках критично важливі елементи цифрової інфраструктури, від якої залежить функціонування не лише окремих підприємств, а й цілих секторів економіки. Їхня ринкова влада ґрунтується на ефекті масштабу, мережових зовнішніх ефектах і високих бар'єрах для входу нових гравців, що створює умови для квазі-монополізації цифрових послуг. У результаті навіть короточасні збої чи зловживання з боку провайдера здатні викликати ланцюгові наслідки на макроекономічному рівні, зупиняючи логістичні потоки, транзакції у фінансовій сфері або роботу виробничих підприємств.

Економічні впливи такого явища мають багатовимірний характер. По-перше, підприємства стикаються із зростанням ризику непрямих збитків, коли затримки чи перебої у роботі платформи призводять до втрат у суміжних

секторах. По-друге, концентрація цифрової інфраструктури у руках обмеженого кола провайдерів формує додаткову ризик-премію на капітал, оскільки інвестори враховують вартість потенційних збоїв у своїх прогнозах. По-третє, технологічна залежність, коли підприємство втрачає можливість швидко змінити постачальника через високу вартість міграції даних, необхідність адаптації програмного забезпечення та перебудови бізнес-процесів. Це веде до зростання довгострокових витрат, зниження стратегічної гнучкості та зростання операційної вразливості бізнесу.

На рівні національної економіки залежність від зовнішніх цифрових платформ має ще один критично важливий вимір: загрозу цифровому суверенітету. Надмірна орієнтація на іноземні платформи означає, що будь-які зміни політики глобальних корпорацій, підвищення тарифів або геополітичні обмеження можуть мати відчутні макроекономічні наслідки для держави. В умовах України ця проблема ускладнюється тим, що малий і середній бізнес історично використовував іноземні, зокрема російські програмні продукти, що створює додаткові ризики як у сфері безпеки, так і у сфері економічної стійкості. Згідно зі звітом ОЕСР (2024), надмірна залежність українських підприємств від сторонніх цифрових рішень посилює їхню вразливість до зовнішніх шоків і обмежує інтеграцію у внутрішній ринок ЄС [84].

З економічної точки зору, така залежність має довгострокові негативні наслідки: вона гальмує розвиток національних ІТ-рішень, знижує інвестиційну привабливість технологічних стартапів та посилює структурну асиметрію між великим і малим бізнесом. У той час як великі корпорації здатні забезпечити диверсифікацію постачальників та розбудову гібридних хмарних архітектур, малий бізнес залишається вразливим до цінової політики глобальних провайдерів та технічних збоїв у роботі платформ. Це створює дисбаланс у доступі до цифрових ресурсів і може спричинити нерівномірний розподіл економічних вигод від цифрової трансформації.

Окремим важливим виміром у дослідженні залежності від цифрових платформ є критичність портативності та розвиток гібридної архітектури. Для

бізнесу залежність від одного провайдера створює ефект технологічної залежності від постачальника цифрових послуг, коли перехід до альтернативного провайдера стає економічно не вигідним через значні витрати на міграцію даних, адаптацію програмного забезпечення та перенавчання персоналу. Таке явище формує довгострокові фінансові зобов'язання, які ускладнюють оптимізацію витрат та стратегічне переорієнтування бізнес-моделей у динамічному середовищі цифрової економіки.

З економічного погляду відсутність портативності цифрових рішень веде до зростання сукупних витрат власності, оскільки суб'єкти господарювання змушені фінансувати не лише підтримку основних сервісів, але й витрати на забезпечення сумісності, збереження історичних даних та оновлення програмного забезпечення. У результаті це знижує рентабельність інвестицій у цифровізацію, адже підприємства витрачають значну частину бюджету на підтримку монопольних платформ замість спрямування ресурсів на інноваційний розвиток.

Більше того, така технологічна залежність знижує стратегічну гнучкість підприємств, адже будь-які зміни у тарифній політиці або корпоративній стратегії провайдера прямо відображаються на витратах і конкурентоспроможності користувачів його послуг. Це створює додаткову ризик-премію для інвесторів, які враховують ймовірність монопольного диктату під час оцінювання вартості компанії та планування інвестицій. У макроекономічному вимірі така залежність провокує ефект концентрації ризиків: проблеми одного великого постачальника можуть перерости у системні збої, що матимуть крос-секторальний вплив на економіку країни.

Розвиток гібридних архітектур та мультимарних стратегій здатний знизити рівень технологічної залежності, проте потребує значних інвестицій у проєктування, тестування та адміністрування таких систем. Для малого та середнього бізнесу це часто є непосильним завданням, що посилює асиметрію у доступі до цифрових ресурсів між великими корпораціями та менш капіталізованими компаніями. У довгостроковій перспективі це може

призвести до структурного посилення ринкової концентрації та зниження рівня конкуренції, що негативно впливатиме на темпи інновацій та економічну стійкість цифрової економіки загалом [95].

Особливої уваги потребує явище цифрової залежності малого та середнього бізнесу, яке формує окремий сегмент регуляторних та економічних викликів. Для підприємств цього масштабу доступ до інноваційних цифрових рішень часто обмежується високою вартістю ліцензій, відсутністю ресурсів для створення власних інформаційних систем та браком кваліфікованого персоналу, здатного обслуговувати складні цифрові інфраструктури. У результаті такі суб'єкти господарювання змушені користуватися дешевшими, менш захищеними або іноземними цифровими продуктами, що створює ситуацію глибокої технологічної залежності.

З економічної точки зору, така залежність породжує низку негативних ефектів. По-перше, вона знижує продуктивність і ефективність малого бізнесу, адже обмежує можливість впровадження сучасних інструментів управління даними, електронної комерції та цифрового маркетингу. По-друге, вона підвищує ризик зростання витрат у майбутньому, оскільки перехід на більш сучасні або сумісні з європейськими ринками системи потребує значних інвестицій у міграцію даних, адаптацію програмного забезпечення та підготовку персоналу. По-третє, існує ризик репутаційних і фінансових втрат, якщо використання застарілих або вразливих рішень призведе до кіберінцидентів, що можуть підірвати довіру контрагентів і обмежити доступ до партнерських мереж.

В українських реаліях проблема цифрової залежності малого бізнесу має ще й геополітичний вимір. Тривале використання російських програмних продуктів, зокрема бухгалтерських систем типу «1С», створює ризик не лише кібербезпеки, а й економічної стійкості. В умовах інтеграції до єдиного цифрового ринку ЄС така залежність стає бар'єром для міжнародної кооперації, оскільки іноземні партнери розглядають використання небезпечних програм як фактор підвищеного ризику. Це ускладнює вихід

українських компаній на зовнішні ринки, знижує їхню інвестиційну привабливість і може відштовхувати стратегічних партнерів.

У макроекономічному розрізі масова залежність малого бізнесу від сторонніх і вразливих цифрових систем створює системний ризик для національної економіки. У випадку масових збоїв чи кібератак втрати окремих підприємств накопичуються у вигляді падіння податкових надходжень, зростання рівня тінізації економіки та зниження зайнятості. Крім того, залежність від іноземних цифрових платформ обмежує розвиток внутрішнього ринку ІТ-послуг, зменшує можливості для інноваційних стартапів і посилює відтік капіталу за кордон у вигляді ліцензійних платежів.

ОЕСР у своєму звіті за 2024 рік наголошує, що подолання цифрової залежності малих підприємств в Україні є необхідною умовою для підвищення їхньої стійкості, залучення інвестицій і формування сталого економічного розвитку. Зокрема, підкреслюється важливість державної підтримки національних цифрових рішень, розвитку локальних хмарних сервісів і створення умов для їхньої портативності, що дозволить зменшити системні ризики та забезпечити економічну незалежність у стратегічно важливій сфері цифрової інфраструктури [84].

Подана у таблиці 2.4 систематизація демонструє взаємозв'язок між ключовими цифровими ризиками та показниками ефективності й ризику, що дозволяє розглядати цифровізацію не лише як технологічний, а й як економічний феномен. Насамперед, ризики кібербезпеки чинять безпосередній вплив на операційну діяльність підприємств: зупинка виробничих процесів, втрата даних клієнтів та компрометація інформаційних систем зумовлюють прямі фінансові збитки та зниження довіри з боку інвесторів. Це, у свою чергу, позначається на вартості капіталу та страховому навантаженні, тоді як економічні втрати від кіберінцидентів дедалі частіше вимірюються не лише прямими витратами, а й падінням ринкової капіталізації та втратою конкурентних позицій.

Регуляторні ризики проявляються у швидкості змін нормативного поля, що вимагає від підприємств постійної адаптації бізнес-процесів. Впровадження процедур комплаєнсу, витрати на юридичний супровід і модернізацію інформаційних систем призводять до зростання трансакційних витрат і зниження фінансової стійкості. У разі невідповідності регуляторним вимогам виникають додаткові витрати у вигляді штрафів, а також ризик обмеження доступу до міжнародних ринків. Економічні наслідки виявляються у підвищенні собівартості продукції та зменшенні інвестиційної привабливості, що особливо критично для підприємств, інтегрованих у глобальні ланцюги вартості.

Окремої уваги потребує залежність від цифрових платформ, що створює ефект технологічної залежності від постачальників послуг. Висока концентрація ринку хмарних технологій у руках обмеженої кількості глобальних корпорацій означає, що збої у їхній діяльності можуть мати мультиплікативний вплив на економіку цілих галузей. Для підприємств це означає підвищення витрат на підтримку інфраструктури, падіння маржинальності та обмеження стратегічної гнучкості у прийнятті рішень. Додатково така залежність відображається у зростанні ризик-премії для інвесторів та збільшенні вартості капіталу, що прямо позначається на інвестиційній динаміці у цифровому секторі.

Це дозволяє простежити чітку кореляцію між цифровими ризиками та ключовими індикаторами ефективності й ризику (KPI/KRI). Це забезпечує основу для інтеграції цифрових чинників у систему моніторингу економічної безпеки підприємств, що є важливим кроком у побудові адаптивних стратегій управління в умовах цифрової трансформації.

Таблиця 2.4

Цифрові ризики та їх кореляція з KPI/KRI підприємства

Вид цифрового ризику	Механізм впливу на бізнес-процеси	Економічні наслідки	KPI (ключові показники ефективності)	KRI (ключові показники ризику)
Ризики кібербезпеки	Порушення безперервності діяльності; зупинка виробництва; втрата даних клієнтів	Прямі фінансові збитки; зростання витрат на відновлення; падіння ринкової капіталізації; зниження довіри інвесторів; зростання страхових премій	EBITDA; рентабельність продажів; продуктивність праці	Частота кіберінцидентів; середній час відновлення (MTTR); частка IT-бюджету, спрямованого на безпеку
Регуляторні ризики	Необхідність перебудови бізнес-процесів, забезпечення системи внутрішнього контролю за дотриманням регуляторних вимог	Зростання трансакційних витрат; ризик штрафів і санкцій; зниження інвестиційної привабливості; обмеження доступу до міжнародних ринків; зростання собівартості продукції	Доступ до нових ринків; коефіцієнт фінансової стійкості; обсяг інвестицій	Кількість випадків невідповідності регуляторним вимогам; витрати на комплаєнс у % від доходу
Залежність від цифрових платформ	Високі витрати на зміну провайдера; ефект технологічної залежності; ризик збоїв у глобальних хмарних сервісах	Зростання собівартості; падіння маржинальності; ризик зупинки критичних процесів; підвищення вартості капіталу; обмеження стратегічної гнучкості	Операційна рентабельність; коефіцієнт оборотності активів; питома вага доходів, сформованих цифровими каналами збуту та обслуговування	Витрати на підтримку IT-інфраструктури у % від виручки; рівень диверсифікації цифрових постачальників

Джерело: авторська розробка.

Отже, систематизація цифрових ризиків демонструє, що цифровізація є амбівалентним фактором економічної безпеки: вона одночасно відкриває нові можливості зростання та створює нові виклики для підприємств. З одного боку, впровадження цифрових технологій сприяє зниженню трансакційних витрат, прискорює обіг капіталу та підвищує продуктивність праці. З іншого – цифрові ризики у вигляді кібератак, регуляторної нестабільності та залежності від платформ формують додаткові витрати на захист інформаційних активів, дотримання нормативних вимог та страхування ризиків. Це породжує необхідність моделювання причинно-наслідкових зв'язків між процесами цифрової трансформації та ключовими економічними показниками, що дозволяє комплексно оцінити як позитивні ефекти, так і загрози для економічної безпеки підприємства.

Подана на рис. 2.3 модель демонструє системний вплив цифрової трансформації на бізнес-процеси підприємств та ключові економічні показники їх діяльності. Вона відображає не лише позитивні наслідки цифровізації, але й ті ризики, що породжують додаткові витрати й формують загрози економічній безпеці.

По-перше, впровадження цифрових технологій на підприємствах створює передумови для оптимізації бізнес-процесів, що уможливорює зменшення трансакційних витрат. Це, у свою чергу, призводить до зниження собівартості продукції та підвищення рентабельності діяльності. Економічний ефект проявляється у скороченні адміністративних витрат, зростанні продуктивності праці та посиленні фінансової стійкості підприємства. На рівні галузей це забезпечує ефективніше функціонування ланцюгів постачання, а на макроекономічному рівні сприяє розширенню податкової бази та зростанню частки цифрового сектору у структурі ВВП.

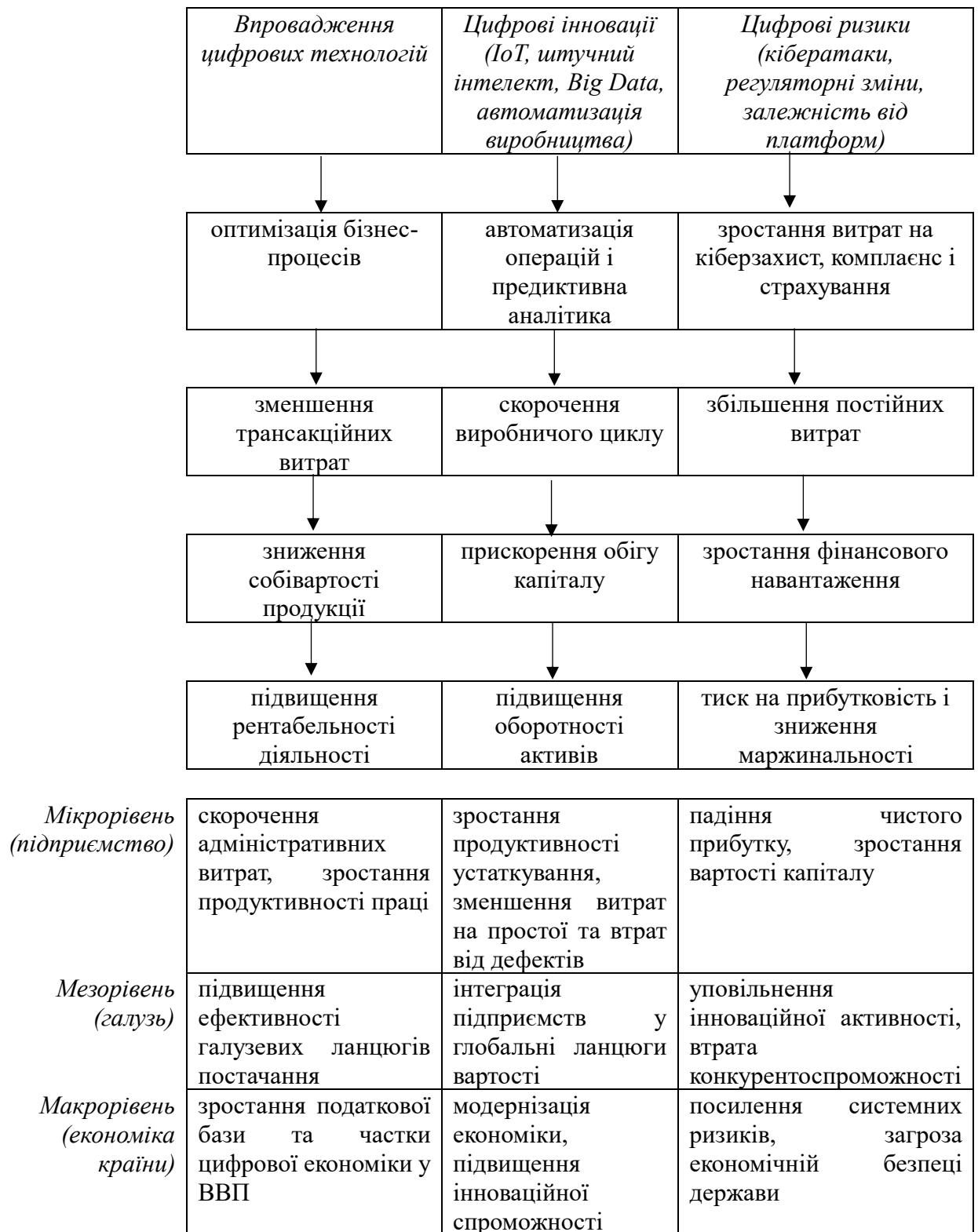


**Рис. 2.3. Модель впливу цифрової трансформації
на бізнес-процеси та економічні показники**

Джерело: авторська розробка.

По-друге, цифрові інновації, зокрема використання штучного інтелекту, технологій «інтернету речей» та систем прогнозної аналітики, стимулюють автоматизацію операцій і вдосконалюють управлінські рішення. Економічним результатом таких змін стає скорочення виробничого циклу, що призводить до прискорення обігу капіталу та підвищення оборотності активів. Це забезпечує більш ефективне використання ресурсів і зменшення втрат від простоїв або дефектів продукції. У довгостроковій перспективі це створює передумови для інтеграції підприємств у глобальні ланцюги вартості та стимулює модернізацію економіки, підвищуючи її інноваційну спроможність.

По-третє, цифровізація породжує й негативні економічні ефекти, пов'язані з виникненням нових ризиків. Кібератаки, регуляторні зміни та залежність від глобальних цифрових платформ зумовлюють зростання витрат на забезпечення інформаційної безпеки, страхування та дотримання нормативно-правових вимог. Такі витрати трансформуються у збільшення постійних витрат підприємств, що формує додаткове фінансове навантаження і в підсумку спричиняє тиск на прибутковість та зниження маржинальності. На мікрорівні це виявляється у падінні чистого прибутку та зростанні вартості капіталу, на мезорівні – в уповільненні інноваційної активності та зниженні конкурентоспроможності галузей, а на макрорівні – у посиленні системних ризиків і формуванні загроз для економічної безпеки держави.

Таким чином, представлена модель дає змогу комплексно оцінити подвійний ефект цифрової трансформації: з одного боку, вона забезпечує зростання ефективності, продуктивності та інноваційної спроможності економіки, а з іншого – породжує нові витрати і ризики, що вимагають інтеграції у систему стратегічного управління економічною безпекою.

Таким чином, цифрова трансформація виступає амбівалентним чинником економічної безпеки підприємств. Вона забезпечує підвищення ефективності бізнес-процесів, зростання продуктивності та інтеграцію у глобальні ланцюги вартості, але водночас формує нові ризики, що знижують маржинальність і потребують значних інвестицій у захист та нормативно-

правову відповідність. Збалансування позитивних ефектів і негативних наслідків цифровізації є ключовим завданням сучасного стратегічного управління, від реалізації якого залежить не лише фінансова стійкість окремих підприємств, а й конкурентоспроможність національної економіки загалом.

2.3. Міжнародні практики цифрового ризик-менеджменту та їх адаптація в національній економіці

Цифрові ризики становлять комплекс загроз і вразливостей, що виникають у процесі цифровізації економіки та можуть істотно впливати на конкурентоспроможність підприємств, інвестиційну привабливість і загальний рівень економічної безпеки. У сучасних умовах цифрова трансформація бізнес-процесів водночас відкриває нові можливості для зростання ефективності, але й створює додаткові ризики, що потребують інтегрованого підходу до управління [97; 98]. Відтак, аналіз міжнародних практик цифрового ризик-менеджменту набуває особливої значущості для вітчизняних підприємств, адже він дозволяє визначити потенціал імплементації адаптованих моделей у національний контекст.

У науковій літературі доведено, що цифрова трансформація може бути не лише інструментом інноваційного розвитку, а й чинником формування інклюзивної економіки та підвищення соціальної стійкості в умовах кризових явищ, зокрема воєнного стану [97]. Водночас цифровізація фінансових і аграрно-транспортних підприємств супроводжується новими ризиками, які потребують удосконалення методів фінансового ризик-менеджменту та формування систем безпеки, орієнтованих на цифрові виклики [98].

Особливої уваги заслуговує міжнародний досвід управління ризиками бізнес-процесів у цифровій економіці, де визначальним є поєднання стратегічного бачення та використання сучасних цифрових інструментів. Практика зарубіжних країн підтверджує ефективність моделей, що базуються на інтеграції ризик-менеджменту у стратегічне управління, а також на

впровадженні механізмів моніторингу й адаптивного реагування [99]. Українські науковці наголошують на потребі ризик-орієнтованого стратегічного управління як ключового напрямку забезпечення економічної безпеки у цифровому середовищі, що вимагає поєднання теоретико-методологічних основ та практичних інструментів [100].

На державному рівні визначальним орієнтиром залишається Стратегія економічної безпеки України на період до 2025 року, де цифровізація прямо розглядається як один із ключових чинників стійкості національної економіки та інституційної спроможності протидіяти ризикам [11]. Проте існують суттєві інституційні прогалини, зокрема: низький рівень гармонізації національного законодавства з європейськими нормами, обмежена кількість секторальних методик та кадровий дефіцит у сфері цифрової безпеки.

Системний аналіз зарубіжних і вітчизняних практик цифрового ризик-менеджменту дає можливість виявити сильні та слабкі сторони існуючих підходів, окреслити критичні «зони ризику» та визначити напрями адаптації міжнародних стандартів в український економічний простір. Це створить підґрунтя для розробки інтегрованої моделі цифрового ризик-менеджменту, здатної забезпечити економічну стійкість і відповідати стратегічним цілям євроінтеграції України.

Моніторинг та раннє попередження цифрових загроз необхідно розглядати не лише як технічний захід, а передусім як економічний інструмент, що зменшує очікувану величину можливих втрат підприємства. Йдеться про запобігання простою виробничих чи фінансових процесів, уникнення штрафних санкцій, а також стабілізацію ринкової вартості бізнесу та довіри інвесторів.

У країнах із високим рівнем інституційної зрілості система протидії цифровим загрозам вибудовується за принципом інтегрованого контуру, де поєднуються кілька ключових елементів:

1. центри моніторингу подій (операційні підрозділи, що забезпечують цілодобовий нагляд за інформаційними системами);
2. системи аналізу та кореляції даних про інциденти (програмні комплекси, які збирають і співставляють інформацію про можливі атаки для своєчасного виявлення закономірностей);
3. команди реагування на інциденти (спеціалізовані групи, що здійснюють координацію дій під час кризових ситуацій);
4. платформи обміну інформацією про загрози між підприємствами та державними органами, які знижують інформаційну асиметрію на ринку [101].

Такі інтегровані системи дають змогу суттєво знизити економічні ризики невизначеності, які виникають унаслідок раптових кіберінцидентів.

Водночас міжнародні стандарти з управління ризиками, зокрема Рамкова модель кібербезпеки NIST (США), виокремлюють шість основних функцій управління, що формують повний цикл протидії цифровим загрозам [31]:

1. Управління (Govern) – створення економічно обґрунтованої політики, регламентів і системи відповідальності за управління ризиками.
2. Ідентифікація (Identify) – виявлення критичних активів підприємства та оцінка їхньої економічної вразливості до загроз.
3. Захист (Protect) – формування заходів, що мінімізують імовірність інцидентів і зменшують витрати на їх подолання.
4. Виявлення (Detect) – економічно оптимізоване спостереження за середовищем для швидкого фіксування відхилень, які можуть свідчити про атаку.
5. Реагування (Respond) – своєчасна організація заходів для локалізації інцидентів з мінімальними фінансовими втратами.
6. Відновлення (Recover) – відновлення бізнес-процесів і зниження довгострокових збитків, включно з репутаційними та інвестиційними.

Важливо, що цей цикл відображає замкнену систему управління ризиками, де превентивні витрати (на захист і моніторинг) співвідносяться з потенційними втратами (збитками від інцидентів). Таким чином, запровадження систем попередження й моніторингу цифрових загроз є формою інвестицій у стійкість, яка має не лише технічний, а й безпосередній економічний ефект.

Представлена на рис. 2.4 схема відображає замкнений цикл управління цифровими ризиками, у якому послідовно реалізуються ключові функції: управління, ідентифікація, захист, виявлення, реагування та відновлення. Кожен із зазначених етапів має не лише технічний, а й економічний зміст.

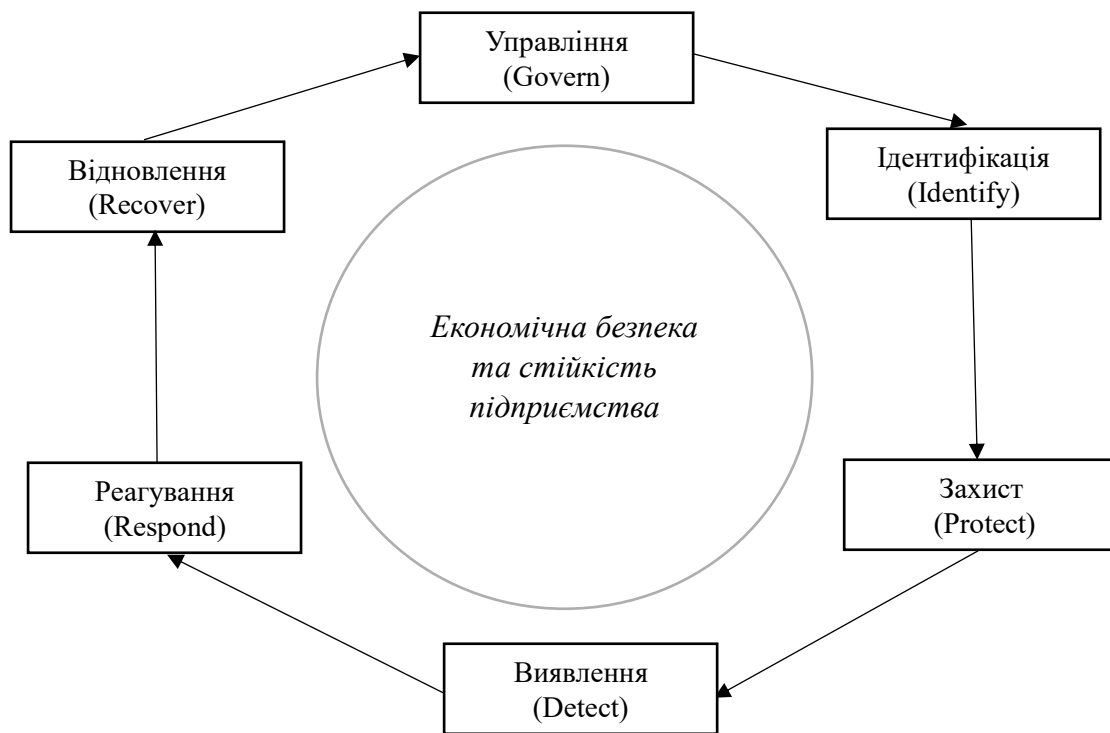


Рис. 2.4. Цикл управління цифровими ризиками (економічний вимір)

Джерело: узагальнено автором на основі [31].

Функція управління полягає у формуванні стратегічних та нормативних засад, які визначають економічну доцільність витрат на цифрову безпеку та відповідальність управлінських структур. Ідентифікація забезпечує виявлення критично важливих активів підприємства й оцінку можливих економічних наслідків їх ураження. Захист передбачає реалізацію організаційних та

фінансових заходів, спрямованих на мінімізацію ймовірності інцидентів та зменшення очікуваних втрат.

Функція виявлення відображає безперервний моніторинг середовища для фіксації ознак загроз, що дозволяє скоротити часовий лаг між виникненням інциденту та реакцією на нього, знижуючи таким чином обсяг економічних втрат. Реагування пов'язане з оперативною мобілізацією ресурсів для локалізації наслідків інцидентів та мінімізації шкоди для бізнес-процесів. Нарешті, відновлення спрямоване на відбудову нормального функціонування підприємства та зниження довгострокових негативних ефектів, зокрема репутаційних та інвестиційних.

Таким чином, запропонований цикл дозволяє розглядати управління цифровими ризиками як інвестицію у стійкість підприємства та його економічну безпеку, де превентивні витрати виправдовуються значним зменшенням потенційних збитків.

З метою поглиблення економічного аналізу системи управління цифровими ризиками доцільно виокремити ключові показники ефективності (KPI) та індикатори ризику (KRI), які відображають результативність управлінських заходів на кожному етапі циклу. У таблиці 2.3 наведено систематизацію відповідних індикаторів з акцентом на їхній економічний вимір.

Представлена у таблиці 2.5 система індикаторів дозволяє зробити висновок, що кожен етап управління цифровими ризиками має власний економічний вимір, який може бути кількісно оцінений за допомогою відповідних KPI та KRI. Це забезпечує можливість не лише технічного, але й фінансово-економічного аналізу результативності управлінських заходів у сфері цифрової безпеки.

Таблиця 2.5

Економічні індикатори ефективності на етапах циклу управління цифровими ризиками

Етап циклу управління	Економічний зміст	Приклади індикаторів (KPI/KRI)	Очікуваний ефект
1	2	3	4
Управління	Формування стратегічних і фінансових рамок цифрової безпеки, визначення відповідальності управлінських структур	– частка витрат на цифрову безпеку у загальних витратах підприємства, %; – рівень відповідності міжнародним стандартам (ISO 31000, NIS2 тощо), %	Забезпечення економічної збалансованості між витратами на захист і потенційними збитками; зниження ризику накладення штрафних санкцій і втрати інвестиційної привабливості; підвищення кредитного рейтингу та довіри з боку стейкхолдерів
Ідентифікація	Виявлення критично важливих активів та оцінка їх економічної вразливості до загроз	– відсоток активів, охоплених аналізом ризиків, %; – кількість виявлених «вузьких місць» у системі, од.	Рационалізація розподілу фінансових і людських ресурсів; уникнення надмірних витрат на захист другорядних активів; підвищення ефективності інвестицій у безпекові технології; зниження ймовірності критичних економічних втрат у майбутньому
Захист	Реалізація превентивних заходів для зменшення ймовірності інцидентів та зниження масштабу їх наслідків	– співвідношення витрат на профілактику до витрат на ліквідацію наслідків (коефіцієнт превентивності); – частка інцидентів, яким запобігли, %	Зменшення вартості простоїв і відновлювальних робіт; збереження безперервності виробничих і фінансових процесів; підвищення ефективності використання капіталу; зміцнення ринкової позиції підприємства завдяки репутації надійного партнера
Виявлення	Оперативний моніторинг цифрового середовища для фіксації ознак загроз	– середній час виявлення інциденту (середній час до виявлення, години/дні); – частка інцидентів, виявлених на ранній стадії, %	Мінімізація часу поширення загрози; скорочення обсягу фінансових втрат; зменшення ймовірності ланцюгового ефекту у критично важливих бізнес-процесах; підвищення прогнозованості економічних результатів

Продовження табл. 2.5

1	2	3	4
Реагування	Скоординоване використання ресурсів для локалізації інцидентів і зниження їх наслідків	– середній час реагування на інцидент (середній час до реагування, години/дні); – частка інцидентів, локалізованих без зупинки критичних бізнес-процесів, %	Зниження прямих збитків та непрямих втрат (репутаційних, інституційних, інвестиційних); підвищення довіри клієнтів і партнерів; забезпечення фінансової стабільності навіть у кризових умовах
Відновлення	Відбудова нормального функціонування бізнес-процесів та мінімізація довгострокових негативних наслідків	– середній час відновлення (години/дні); – фінансові втрати від інцидентів у співвідношенні до доходу підприємства, %	Скорочення тривалості дії негативних економічних ефектів; швидке повернення до доінцидентного рівня операційної ефективності; збереження конкурентних позицій; підвищення інвестиційної привабливості підприємства; забезпечення макроекономічної стабільності у випадку масових інцидентів у критично важливих секторах

Джерело: авторська розробка.

Так, на етапі управління головним завданням є забезпечення збалансованості між витратами на безпекові заходи та рівнем потенційних збитків від цифрових інцидентів. Встановлення чітких нормативних рамок та визначення частки витрат на кібербезпеку у структурі бюджету підприємства дозволяє мінімізувати правові та репутаційні ризики, а також підвищити інвестиційну привабливість бізнесу. Відповідно до Стратегії економічної безпеки України до 2025 року, превентивне управління ризиками є обов'язковою умовою забезпечення макроекономічної стабільності [11].

На етапі ідентифікації важливим є визначення критично важливих активів та аналіз їх вразливості. Виявлення «вузьких місць» дозволяє підприємствам оптимізувати розподіл фінансових і людських ресурсів, концентруючи їх на найбільш значущих напрямках. Такий підхід унеможливорює надмірні витрати на захист другорядних активів і водночас знижує ймовірність виникнення масштабних економічних втрат у майбутньому. Подібний підхід обґрунтовано українськими науковцями, які наголошують на важливості ризик-орієнтованої стратегії управління бізнес-процесами [99; 102].

Функція захисту безпосередньо пов'язана із співвідношенням витрат на профілактику та ліквідацію наслідків. Доведено, що витрати на превентивні заходи у середньостроковій перспективі є економічно ефективними, оскільки вартість інцидентів, яким вдалось запобігти, значно перевищує обсяги інвестицій у захист [98]. З цієї причини показник «коефіцієнт превентивності» може бути використаний як орієнтир для фінансових рішень у сфері безпеки.

Етап виявлення цифрових загроз характеризується такими ключовими показниками, як середній час виявлення інциденту та частка загроз, ідентифікованих на ранній стадії. Чим менше часу витрачається на виявлення, тим нижчими є втрати для підприємства та економіки загалом. Ефективність фінансового ризик-менеджменту значною мірою залежить від швидкості ідентифікації відхилень у цифровому середовищі.

Функція реагування визначає здатність підприємства швидко локалізувати інцидент і мінімізувати збитки. Важливими індикаторами тут є середній час реагування та частка інцидентів, ліквідованих без зупинки критичних бізнес-процесів. З економічної точки зору це дозволяє не лише зменшити прямі збитки, але й зберегти довіру клієнтів та інвесторів, що критично важливо для фінансової стійкості підприємства у довгостроковій перспективі.

Завершальним етапом є відновлення, де визначальним є швидкість повернення до нормального функціонування бізнес-процесів. Показники середнього часу відновлення та частки втрат у співвідношенні до обороту підприємства відображають рівень економічної стійкості. Ризик-орієнтоване стратегічне управління в умовах цифровізації має включати довгострокові індикатори стійкості, оскільки вони визначають інвестиційну привабливість і конкурентоспроможність підприємств на ринку.

Таким чином, економічна інтерпретація індикаторів підтверджує, що система моніторингу та попередження цифрових загроз має не лише технічне, але й виразне економічне значення. Інвестиції у цифрову безпеку необхідно розглядати як капіталовкладення у підвищення стійкості підприємства та економіки загалом, що узгоджується як з міжнародними практиками (NIST CSF 2.0), так і з національними стратегічними документами [11; 31].

Здійснений аналіз систем попередження та моніторингу цифрових загроз засвідчив, що економічна безпека підприємств та держави безпосередньо залежить від здатності вчасно ідентифікувати інциденти та мінімізувати їхні наслідки. Проте для досягнення стратегічної стійкості необхідно спиратися не лише на оперативний моніторинг, а й на комплексні методики оцінки рівня цифрової безпеки, що інтегрують організаційні, фінансові та технологічні аспекти. Саме тому доцільним є вивчення досвіду зарубіжних країн, де розроблені стандартизовані підходи (NIST, Cyber Essentials, ENISA, METI), які поєднують ризик-орієнтовану логіку з

економічними критеріями ефективності та створюють основу для адаптації таких практик в Україні.

Розглянемо методики оцінки цифрової безпеки у США. Система оцінювання цифрової безпеки у Сполучених Штатах Америки сформувалася навколо рамкових документів Національного інституту стандартів і технологій (NIST). Одним із найбільш відомих підходів є NIST Cybersecurity Framework (CSF) 2.0, який у 2024 році отримав оновлення [31]. У центрі цієї методики: ідея зрілості процесів управління ризиками (cybersecurity maturity levels), що дозволяє підприємствам оцінювати не лише наявність окремих технічних заходів, але й ступінь інтегрованості ризик-менеджменту у стратегічні та фінансові рішення.

З економічної точки зору, CSF виконує роль інструменту оптимізації витрат на безпеку: підприємство може визначати, які заходи є найбільш ефективними з позицій співвідношення «вартість – очікуване зменшення збитків». Використання категорій «Identify, Protect, Detect, Respond, Recover» сприяє формуванню системи, у якій превентивні витрати співвідносяться з потенційними втратами від інцидентів. Це дозволяє оцінювати «економіку кіберризиків» в кількісних термінах і приймати обґрунтовані управлінські рішення.

Другим важливим напрямом є практика стрес-тестування у фінансовому секторі. Федеральна резервна система США (Federal Reserve) запровадила стрес-тести, які дозволяють моделювати не лише макроекономічні, а й кіберризикові сценарії [103]. У цьому контексті банки зобов'язані перевіряти здатність витримати кібератаки, що можуть паралізувати платіжні системи чи порушити функціонування інфраструктури.

З економічної точки зору, застосування стрес-тестів виконує дві ключові функції:

1. Зниження системного ризику – завдяки виявленню слабких місць до їх фактичної реалізації у вигляді інцидентів;

2. Мінімізація зовнішніх ефектів – оскільки крах однієї великої фінансової установи внаслідок кібератаки може спровокувати кризу ліквідності в усьому секторі.

Таким чином, методики США поєднують мікроекономічний рівень (оптимізація витрат і підвищення стійкості окремих підприємств) і макроекономічний рівень (захист фінансової системи від шоків). Для України, де цифровізація банківського сектору є однією з найрозвиненіших, але реальний сектор економіки лишається вразливим, саме американський досвід може стати орієнтиром для розбудови секторальних методик оцінювання цифрової стійкості.

Представлені у таблиці 2.6 методики (NIST CSF 2.0 та стрес-тестування фінансового сектору у США) демонструють, як міжнародні практики цифрового ризик-менеджменту поєднують технічні та економічні інструменти для досягнення стійкості.

По-перше, застосування рамки NIST CSF 2.0 у США демонструє ефективність стандартизованого підходу до управління цифровими ризиками, який інтегрує безпекові практики у стратегічне та фінансове планування підприємств. Цей досвід є показовим для України, оскільки може слугувати основою для розробки секторальних методик у реальному секторі економіки. Використання економічно вимірюваних індикаторів: таких як частка витрат на заходи безпеки у загальних витратах, середній час відновлення після інцидентів та рівень зрілості систем управління ризиками, безпосередньо впливає на ринкову стійкість підприємств і їхню інвестиційну привабливість.

Таблиця 2.6

**Методики оцінки цифрової стійкості: досвід США та можливості
адаптації в Україні**

Методика	Економічний зміст	Приклади індикаторів	Очікуваний економічний ефект та можливості імплементації в Україні
NIST Cybersecurity Framework (CSF 2.0)	Стандартизований підхід до управління кіберризиками через визначення рівнів зрілості (maturity levels) та інтеграцію управління ризиками у фінансові стратегії підприємств	– частка витрат на цифрову безпеку у загальних витратах, %; – середній час відновлення після інцидентів; – рівень відповідності вимогам CSF	США: оптимізація витрат на безпеку, зменшення ймовірності фінансових втрат, підвищення довіри інвесторів. Україна: може бути використана як модель для секторальних методик у промисловості, енергетиці та аграрному секторі; дозволяє обґрунтовувати інвестиції у цифрову безпеку як стратегічні вкладення
Стрес-тестування фінансового сектору (Federal Reserve, DFAST/CCAR 2025)	Наглядові стрес-тести: моделювання несприятливих макроекономічних і кіберризикових сценаріїв для перевірки стійкості найбільших банківських установ	– рівень достатності капіталу після реалізації сценарію; – частка банків, що зберегли кредитування; – обсяг потенційних збитків у співвідношенні до активів	США: зниження системного ризику у фінансовому секторі, мінімізація ризику кризи ліквідності, збереження кредитної активності. Україна: методика може бути адаптована НБУ для регулярного моделювання кіберризикових сценаріїв; перспективно – застосування у міжсекторальних стрес-тестах (енергетика, транспорт, інфраструктура) для підвищення макроекономічної стійкості

Джерело: узагальнено автором на основі [31; 103].

По-друге, практика стрес-тестування фінансового сектору США, результати якого були оприлюднені Федеральною резервною системою у 2025 році, підтвердила свою ефективність у забезпеченні системної стійкості. Зокрема, провідні банки продемонстрували здатність підтримувати кредитну активність навіть за умов реалізації кризових сценаріїв, що включали як макроекономічні шоки, так і кіберризики [103]. Для України даний інструмент може стати основою не лише для удосконалення оцінки стійкості банківської системи, але й для поширення практики міжсекторального тестування цифрової стійкості. Це дозволить моделювати наслідки масштабних кібератак у критично важливих галузях – енергетиці, транспорті та промисловості, що має особливе значення в умовах воєнних і післявоєнних викликів.

Таким чином, узагальнення американського досвіду свідчить про необхідність побудови економічного виміру цифрової безпеки на основі кількісних показників, здатних підтвердити доцільність інвестицій у системи кіберзахисту. Для України це означає, з одного боку, потребу гармонізації національних підходів з міжнародними стандартами (NIST CSF, ISO 31000, COSO ERM), а з іншого – впровадження секторальних стрес-тестів як інструменту забезпечення макроекономічної стабільності та підвищення конкурентоспроможності в умовах цифрової економіки.

У контексті продовження аналізу зарубіжних практик доцільно звернути увагу на досвід Великої Британії, де особливого розвитку набула сертифікаційна програма Cyber Essentials, створена за підтримки уряду та адміністрована Національним центром кібербезпеки (NCSC). Її головна мета – забезпечення базового рівня цифрової стійкості для всіх організацій, насамперед малих і середніх підприємств (МСП), які найчастіше є найбільш уразливими до кіберзагроз. Програма охоплює п'ять основних напрямів захисту: налаштування міжмережевих екранів, безпечні конфігурації, контроль доступу, захист від шкідливого програмного забезпечення та своєчасне оновлення систем [104].

З економічної точки зору Cyber Essentials забезпечує низку ефектів. По-перше, сертифікація значно знижує ризик кібератак та фінансових втрат, пов'язаних із ними: дослідження показують, що сертифіковані організації у 2–3 рази рідше стикаються з критичними інцидентами, ніж ті, що не мають сертифіката [105]. По-друге, сертифікація стала важливим фактором конкурентоспроможності на ринку: понад третина контрактів у державному секторі Великої Британії включає Cyber Essentials як обов'язкову вимогу. По-третє, наявність сертифіката позитивно впливає на доступ до страхових продуктів: премії з кіберстрахування для сертифікованих компаній є нижчими, оскільки ризик настання страхових випадків зменшується [106].

Для України досвід Cyber Essentials має прикладне значення. По-перше, впровадження аналогічних програм могло б посилити кіберстійкість малого та середнього бізнесу, який становить основу вітчизняної економіки та водночас є вразливим до кібератак. По-друге, сертифікація може стати інструментом інтеграції у міжнародні ринки: компанії, які підтверджують відповідність базовим стандартам безпеки, підвищують довіру інвесторів та контрагентів. По-третє, економічний ефект полягає у зниженні трансакційних витрат, пов'язаних із відновленням після інцидентів, а також у підвищенні інвестиційної привабливості підприємств. В умовах цифрової трансформації та воєнних загроз запровадження подібних ініціатив в Україні могло б стати важливим кроком у напрямі гармонізації з європейськими практиками забезпечення економічної безпеки.

Таким чином, британська модель демонструє, що навіть відносно прості й недорогі заходи кіберзахисту можуть мати значний економічний ефект, особливо для сектору МСП. Її адаптація в українських умовах здатна посилити системний захист бізнесу та водночас створити стимули для розвитку ринку кіберпослуг і страхування.

Європейський Союз поступово сформував інституційно узгоджену модель цифрової безпеки, що поєднує аналітичний вимір і нормативно-правову базу. В її основі лежить діяльність ENISA (European Union Agency for

Cybersecurity – Агенція Європейського Союзу з кібербезпеки), яка забезпечує систематичне спостереження за станом та еволюцією кіберзагроз, формує аналітичні звіти та розробляє рекомендації для урядів і приватного сектору. Щорічні огляди, такі як ENISA Threat Landscape 2024, підтверджують тенденцію до зростання масштабних атак, серед яких домінують програми-вимагачі (ransomware), атаки на хмарну інфраструктуру, розповсюджені DDoS-інциденти та порушення безпеки вздовж ланцюгів постачання [33]. Такі загрози мають безпосередні економічні наслідки, оскільки призводять до зростання непрямих витрат підприємств (втрата продуктивності, простій обладнання, збільшення страхових премій, штрафи), а також до зниження ринкової капіталізації компаній. Для фінансового сектору особливо показовим є звіт ENISA Threat Landscape: Finance Sector (2025), який зафіксував 488 інцидентів лише за півтора року. Він доводить, що затримка виявлення та усунення загроз прямо корелює з розміром фінансових збитків, впливає на вартість кредитних ресурсів та зумовлює зростання премії за ризик, що відбивається на інвестиційній привабливості фінансових інститутів [108]. З економічної точки зору регулярні публікації ENISA створюють основу для більш раціонального розподілу інвестицій у системи кіберзахисту, оскільки дозволяють співвідносити очікуваний розмір втрат із вартістю превентивних заходів. Таким чином, витрати на кібербезпеку стають не другорядним елементом, а частиною інвестиційної стратегії підприємств.

На нормативному рівні ключовим актом є Директива NIS2 (Directive on Security of Network and Information Systems – Директива про безпеку мережевих та інформаційних систем), яка набула чинності у 2023 році та поширює вимоги на 18 критично важливих секторів економіки: фінанси, енергетику, транспорт, охорону здоров'я, державне управління та промисловість. Документ вимагає від суб'єктів господарювання не лише технічних рішень, а й комплексного управління ризиками, включно з моніторингом ланцюгів постачання та підзвітністю вищого керівництва [109]. Основний економічний ефект NIS2 полягає у трансформації логіки

корпоративного управління: витрати на цифрову безпеку більше не можуть розглядатися як опціональні. Вони набувають статусу стратегічних капіталовкладень, оскільки невиконання вимог призводить до накладення фінансових санкцій і репутаційних втрат. Для бізнесу відповідність директиві, навпаки, означає зниження ризикової премії, кращі умови страхування та здешевлення доступу до кредитних ресурсів.

У 2024–2025 роках Європейська комісія деталізувала механізми реалізації NIS2 через ухвалення Імплементаційного акту (Commission Implementing Regulation (EU) 2024/2690 від 17.10.2024), а також через публікацію технічних керівництв ENISA, які містять практичні рекомендації щодо управління ризиками, карти відповідності вимогам та приклади доказової бази для аудиту [110; 111]. Це дозволяє підприємствам формувати «портфель контролів» з прогнозованою віддачею: як у вигляді зниження очікуваних збитків і штрафів, так і у вигляді підвищення довіри інвесторів та контрагентів.

Для України імплементація досвіду ЄС відкриває можливості для секторальної стандартизації у банківській, енергетичній та транспортній галузях, гармонізації національних підходів до управління ризиками та створення стимулів для бізнесу через страхові та фінансові механізми. Це знижує макроекономічну вразливість, зменшує ймовірність каскадних кризових збоїв у критично важливих секторах та підвищує довгострокову стійкість економіки.

У Японії стратегічний підхід до кіберстійкості бізнесу реалізується через Методичні рекомендації з управління кібербезпекою (Guidelines for Cybersecurity Management, версія 3.0), розроблені Міністерством економіки, торгівлі та промисловості (METI) разом з організацією IPA (Information-technology Promotion Agency – Агентство сприяння розвитку інформаційних технологій). Ці настанови відзначаються балансом між технологічними вимогами і принципами корпоративного управління, включаючи відповідальність топ-менеджменту, інтеграцію кібербезпеки у стратегії

розвитку, аналіз ризиків у ланцюгах постачання та побудову взаємодії зі стейкхолдерами [112].

У липні 2023 року METI представило версію, що враховує запити інституційних інвесторів і наголошує на розширенні вимог ESG (екологія, соціальна відповідальність, управління), що створює економічний стимул для підвищення кіберстійкості підприємств, які прагнуть доступу до капіталу інвесторів [113]. У 2024–2025 роках були впроваджені секторні оновлення: наприклад, керівництво щодо безпеки в енергетичному секторі (energy resource aggregation business) забезпечує рекомендації для компаній у сфері агрегування енергоресурсів, включаючи багаторівневий захист та оцінку ризиків [114]. Японська модель демонструє, що включення кіберстратегії як частини масових управлінських процесів робить інвестицію в кібербезпеку економічно виправданою, оскільки вона знижує операційні ризики та підвищує стійкість бізнесу, особливо в критично важливих сегментах.

У Китаї державне регулювання у сфері даних і кібербезпеки ґрунтується на трьох базових законах, що формують правове ядро національної цифрової політики. Першим із них є Cybersecurity Law (Закон Китайської Народної Республіки про кібербезпеку, 2016 р.), який набрав чинності у червні 2017 року та встановив вимоги до операторів критичної інформаційної інфраструктури, зокрема щодо локалізації даних і підвищення стандартів захисту [115]. Другим став Data Security Law (Закон Китайської Народної Республіки про безпеку даних, 2021 р.), що визначив категорії даних, запровадив їхню класифікацію та механізми державного контролю за обробкою «важливих даних» [116]. Третій базовий акт – Personal Information Protection Law (Закон Китайської Народної Республіки про захист персональної інформації, 2021 р.), який за змістом наближений до європейського GDPR і регулює порядок збору, обробки та захисту персональних даних [117].

У вересні 2024 року Держрада Китайської Народної Республіки ухвалила Regulations on Network Data Security Management, що набрали чинності 1 січня 2025 року. Ці регламенти деталізують поняття «важливих

даних», встановлюють вимоги щодо класифікації даних, оцінки безпеки при їх обробці та здійснення трансграничних передач, а також вимагають від іноземних компаній призначення представника або створення місцевої організації для контролю [118]. Така політика сприяє економічній стабільності, оскільки підприємства, що обробляють великі обсяги даних, мають адаптувати свої системи відповідно до високих стандартів контролю, що сприяє ефективному управлінню ризиком інцидентів та репутаційних втрат. Крім того, у 2024–2026 роках Міністерство промисловості та інформаційних технологій Китаю запланувало комплексний підхід до підвищення кібербезпеки в промисловому секторі: серед заходів: проведення тренувань на випадок кібератак, охоплення понад 45 000 підприємств, навчальні сесії й створення кадрів – 5 000 спеціалістів [119]. Це вказує на економічне усвідомлення: створення людського ресурсу та компетенцій є ключем до зміцнення стійкості національної інфраструктури.

Для України азійський досвід має значний потенціал у поєднанні технологічних та економічних стимулів розвитку цифрової безпеки. Японська модель, заснована на Cybersecurity Management Guidelines, показує, що інтеграція кіберстратегії в корпоративне управління напряму пов'язана з доступом до фінансового капіталу. Включення кіберризиків у систему ESG-звітності підвищує довіру інвесторів і знижує вартість ресурсів. Для України такий підхід може стати основою розвитку корпоративної підзвітності, де поряд із фінансовими показниками враховуються безпекові критерії, а галузеві методичні настанови сприятимуть раціональному розподілу інвестицій у критичні сектори.

Китайський досвід демонструє інший підхід – посилений державний контроль за даними. Він обмежує бізнес у короткостроковій перспективі, але підвищує системну стійкість у довгостроковій. Для України важливими є практики класифікації критичних даних та проведення масштабних «кібернавчань» у промисловості, що дозволяють ефективніше використовувати ресурси та готувати бізнес до можливих інцидентів. Це може

стати базою для впровадження секторальних стрес-тестів цифрової стійкості у стратегічних галузях.

Узагальнюючи, досвід Японії та Китаю доводить, що цифрова безпека є не лише технічним чи правовим завданням, а й економічною категорією, яка визначає інвестиційну привабливість, вартість фінансування та рівень макроекономічної стійкості. Україні доцільно поєднати японську модель корпоративної інтеграції кібербезпеки з китайською практикою класифікації даних і секторальних тренувань, що дозволить водночас посилити довіру інвесторів і зміцнити критичну інфраструктуру.

Україна поступово формує багаторівневу систему цифрового ризик-менеджменту, у якій поєднуються базова законодавча рамка, секторальне регулювання у фінансовій системі та інституційні механізми реагування. Базисом виступає Закон України «Про основні засади забезпечення кібербезпеки України» (2017), що визначає суб'єктів, повноваження та основи координації у сфері кібербезпеки, включно з об'єктами критичної інфраструктури [120]. На рівні економічної політики пріоритети цифрової стійкості зафіксовано в Стратегії економічної безпеки України до 2025 року, яка прямо пов'язує безпекові спроможності зі зменшенням макроекономічної вразливості та підвищенням інвестиційної привабливості [11]. У 2025 році ухвалені зміни до низки законів посилили вимоги до кіберзахисту державних інформаційних ресурсів і критичної інфраструктури, що віддзеркалює перехід від декларативного до операційного регулювання [121; 122]. Важливим елементом національної інституційної архітектури є CERT-UA (Computer Emergency Response Team of Ukraine – Команда реагування на комп'ютерні надзвичайні події України), яка функціонує у складі Державної служби спеціального зв'язку та захисту інформації України. CERT-UA забезпечує виявлення, попередження та координацію реагування на кіберінциденти у державному секторі та на об'єктах критичної інфраструктури, а також взаємодію з міжнародними партнерами (FIRST, Trusted Introducer, CSIRTs

Network EC), що дозволяє інтегрувати національну систему у глобальне середовище обміну інформацією про загрози [123].

Найбільш розвиненим є фінансовий сектор, де Національний банк України (НБУ) вибудував цілісну архітектуру управління ризиками та кіберстійкістю. Положення № 64 (2018) встановлює мінімальні вимоги до системи управління ризиками банків і банківських груп (роль наглядової ради, незалежність функцій ризик-менеджменту/комплаєнсу, агрегування даних про ризики), що дозволяє інтегрувати цифрові ризики в загальнобанківський профіль ризику й бюджетування капіталу [124; 125; 130]. Паралельно діє Положення № 95 (2017) щодо організації заходів із забезпечення інформаційної безпеки, яке, разом із Положенням № 178 (2022) про організацію кіберзахисту, задає вимоги до безперервного моніторингу, управління інцидентами, категоризації критичної інфраструктури й інформаційного обміну [126; 127]. У 2025 році НБУ ухвалив зміни (Постанова № 24), які гармонізують підходи з європейським регулюванням цифрової операційної стійкості фінансового сектору (DORA, Регламент ЄС 2022/2554) і розширюють функції контролю за кіберзахистом, що створює чіткі економічні стимули до інвестування у превентивні та детективні контрзаходи [129]. На інституційному рівні з 2017 р. функціонує Центр кіберзахисту НБУ, а з 2018 р. – CSIRT-NBU, який забезпечує координацію реагування в банківському секторі та підвищення спроможностей через навчання, що знижує імовірність і тривалість простоїв та непрямих втрат [131; 132].

Економічні наслідки посилення стандартів підтверджуються макропруденційною аналітикою. За «Звітом про фінансову стабільність» (червень 2025), втрати банків від операційного ризику залишаються суттєвими, але зменшилися порівняно з першими роками повномасштабної війни; НБУ заявив про можливе коригування вимог до капіталу під операційний ризик у напрямі гармонізації з підходами ЄС, що вивільняє частину капіталу і підтримує кредитування реального сектору [133]. Таким чином, інвестиції у цифровий ризик-менеджмент у банківській системі мають

чітку фінансову віддачу: скорочення очікуваних збитків, нижчу премію за ризик, покращення доступу до страхування та дешевшого боргового фінансування.

Позабанківський реальний сектор (промисловість, енергетика, АПК) наразі не має зіставного рівня регуляторної деталізації. Огляди нормативного середовища (USAID, 2021) підкреслювали фрагментарність мінімальних вимог для операторів критичної інфраструктури та нерівномірність впровадження аудитів і оцінок відповідності; оновлення 2024–2025 рр. виправляють прогалини, однак секторальні методики оцінювання цифрової стійкості ще формуються [128]. На практиці частина фінансових установ і пов'язаних організацій впроваджує міжнародні рамки ISO 31000 і COSO ERM. Це демонструють, зокрема, офіційні політики корпоративного недержавного пенсійного фонду НБУ, де прямо зафіксовано використання ISO 31000:2009 і COSO ERM поряд із принципами Базельського комітету та настановами OECD/IOPS [134]. Така адаптація методик управління ризиками має економічний сенс: вона знижує трансакційні витрати від інцидентів, підвищує прогнозованість грошових потоків і полегшує доступ до капіталу, але для масштабування поза фінансовим сектором потрібні секторальні стандарти (подібні до моделей ЄС), а також стимулюючі інструменти (страхові продукти кіберризик, податкові режими для інвестицій у безпеку, вимоги до постачальників у держзакупівлях).

Узагальнюючи, українська модель цифрового ризик-менеджменту демонструє швидший прогрес у фінансовому секторі завдяки регуляторній визначеності Національного банку України та інституційним спроможностям (зокрема, CSIRT-NBU), тоді як в енергетиці, промисловості й агропромисловому секторі триває поступовий перехід від загальних вимог до секторальних методик. Економічний ефект від подальшої гармонізації з європейськими підходами очікувано проявиться у зменшенні очікуваних збитків, більш ефективному розподілі регулятивного капіталу, зокрема тієї

його частини, що формується для покриття операційних ризиків, а також у зростанні інвестиційної привабливості суб'єктів господарювання.

У додатку Д представлено систематизовану таблицю, що відображає ключові методологічні підходи до управління цифровими ризиками у США, Європейському Союзі, країнах Азії (Японія та Китай) та Україні. Метою є порівняння сильних і слабких сторін відповідних моделей та окреслення їхнього економічного значення для забезпечення цифрової стійкості.

Водночас проведений аналіз засвідчив, що формування дієвого середовища цифрової стійкості підприємств в Україні значною мірою ускладнюється наявними інституційними та регуляторними обмеженнями. Незважаючи на прогрес у впровадженні окремих елементів ризик-орієнтованого управління та гармонізації з європейськими підходами, на практиці зберігається низка системних прогалин, які стримують ефективність трансформаційних процесів. Їх прояви охоплюють як правове поле, так і кадрові, організаційні, технологічні та економічні аспекти функціонування бізнесу, що знижує рівень адаптивності підприємств до зростаючих кіберзагроз і обмежує їхню інвестиційну привабливість. Для наочності основні інституційні та регуляторні бар'єри систематизовано на рисунку 2.5.

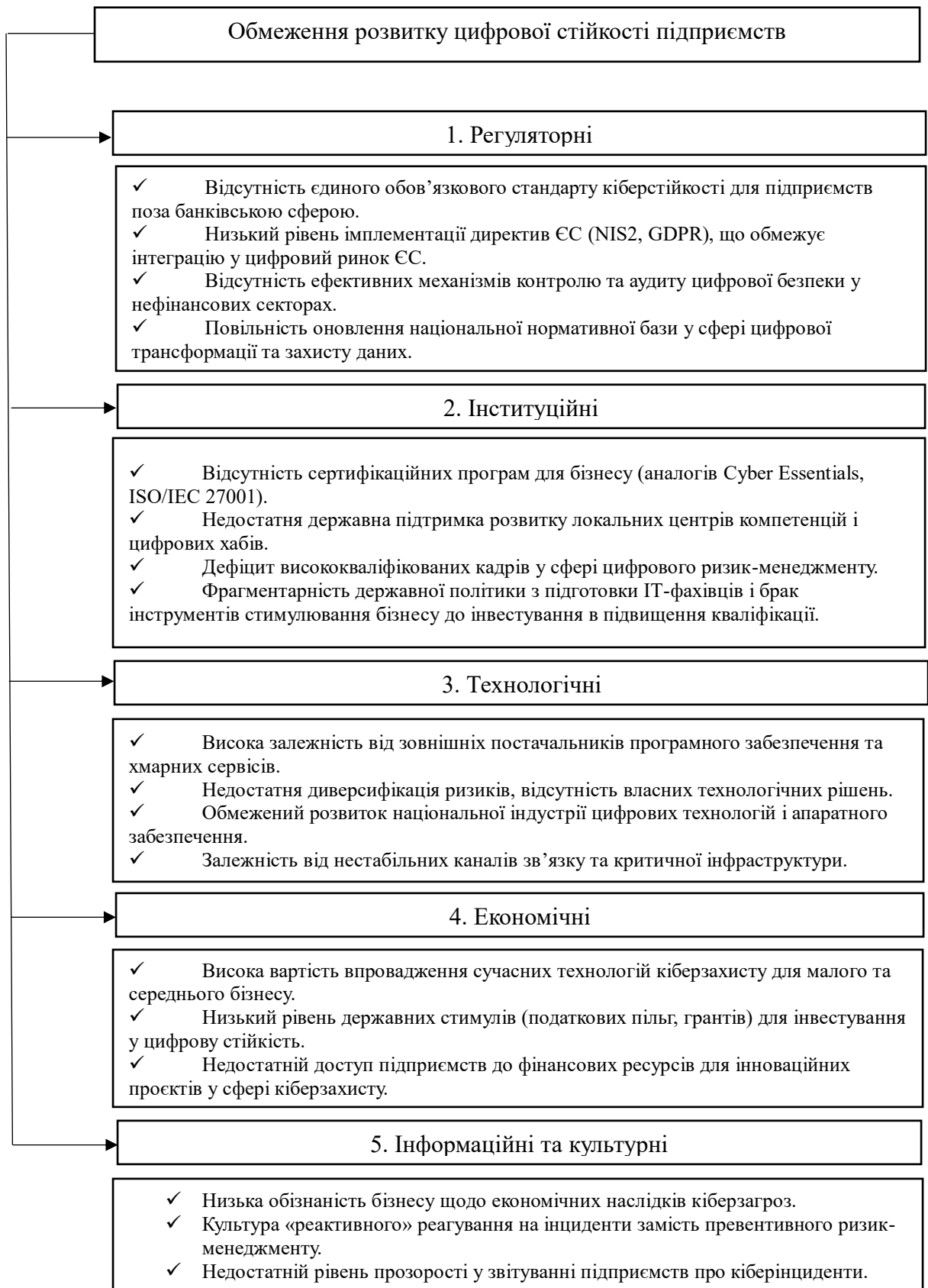


Рис. 2.5. Системні інституційні та регуляторні обмеження розвитку цифрової стійкості підприємств в Україні

Джерело: авторська розробка.

Розвиток цифрової стійкості українських підприємств істотно залежить від якості та повноти нормативно-правової бази. У цьому контексті регуляторні обмеження виступають одними з найвагоміших бар'єрів для інтеграції бізнесу у європейський цифровий простір та підвищення інвестиційної привабливості національної економіки.

По-перше, в Україні відсутній єдиний обов'язковий стандарт кіберстійкості для підприємств поза банківським сектором. Національний банк України поступово впроваджує вимоги до інформаційної безпеки та кіберзахисту, зокрема через ухвалення спеціальних нормативних актів [129]. Однак підприємства інших галузей (промисловості, енергетики, транспорту, агросектору) фактично не мають єдиної системи регуляторного контролю.

Це породжує асиметрію у рівні захищеності та збільшує ймовірність непрямих економічних втрат, пов'язаних із кібератаками (збої у виробництві, простій у постачанні, штрафи від контрагентів).

По-друге, ключовою проблемою є низький рівень імплементації директив ЄС у сфері кібербезпеки та захисту даних. Директива Європейського парламенту та Ради (ЄС) 2022/2555 (так звана NIS2) встановлює єдині правила управління кіберризиками та підзвітності для критично важливих і важливих підприємств: від енергетики та транспорту до медичних і цифрових послуг [92]. В Україні подібні підходи законодавчо закріплені лише частково, що знижує рівень довіри до українських компаній з боку європейських партнерів.

У сфері захисту персональних даних діє Закон України «Про захист персональних даних» від 2010 року [135], який став базовим для формування інституційної політики. Водночас його положення не повністю узгоджені з вимогами Загального регламенту ЄС про захист даних (GDPR), який запроваджує значно ширші права для суб'єктів даних і передбачає жорсткі фінансові санкції за їхнє порушення [136]. З метою гармонізації у жовтні 2022 року було зареєстровано законопроект № 8153 «Про захист персональних даних», а у листопаді 2024 року Верховна Рада ухвалила його у першому читанні [137; 138]. Остаточне набуття чинності цього закону має зняти ключові

бар'єри інтеграції України до цифрового ринку ЄС, однак станом на 2025 рік він не є діючим. Така «подвійність правового поля» створює додаткові трансакційні витрати для підприємств, адже вони змушені одночасно виконувати національні вимоги і готуватися до запровадження європейських норм.

По-третє, існує брак дієвих механізмів контролю та аудиту цифрової безпеки у нефінансових секторах. Якщо у банках регуляторні перевірки здійснюються на регулярній основі, то в інших секторах економіки підприємства здебільшого покладаються на добровільні стандарти. Це формує високий рівень нерівномірності у захищеності, що може перетворитися на макроекономічний ризик у разі масштабних кібератак на промислові чи енергетичні підприємства.

Нарешті, повільність оновлення нормативної бази не дозволяє Україні вчасно реагувати на динаміку кіберзагроз. Відставання у прийнятті законодавчих змін поглиблює ризики для бізнесу, знижує інвестиційну привабливість і гальмує залучення компаній у європейські ланцюги постачання.

Таким чином, регуляторні обмеження не лише знижують якість цифрової безпеки підприємств, а й створюють додатковий тиск на економіку у вигляді втрат від інцидентів, зростання вартості страхування ризиків та обмеження доступу до зовнішніх ринків капіталу.

Поза межами власне нормотворення ключову роль відіграє інституційне середовище – здатність державних і недержавних інституцій координувати політику, акумулювати компетентності та забезпечувати бізнес сервісами підтримки цифрової трансформації. В Україні ця підсистема перебуває у стадії становлення, що формує низку стримувальних факторів із відчутними економічними наслідками.

Насамперед, відчувається недостатня розбудова інфраструктури підтримки підприємств у сфері цифрової трансформації. Йдеться про відсутність розгалуженої системи інституцій, здатних забезпечити методичний

супровід, поширення стандартів і накопичення практичного досвіду цифровізації. В економічному вимірі це означає, що малі та середні підприємства залишаються поза системною допомогою з боку держави чи спеціалізованих центрів, що уповільнює темпи їхньої модернізації та обмежує участь у транскордонних ланцюгах створення вартості.

ОЕСР фіксує потребу посилити інституційну спроможність і координацію стейкхолдерів, розвивати комплексні послуги підтримки для підприємств на різних щаблях цифрової зрілості та розгортати мережу сервісів на національному й субнаціональному рівнях [84]. Недостатній розвиток таких інституційних сервісів зумовлює зростання витрат на координацію економічної діяльності підприємств, уповільнює повернення інвестицій та обмежує можливості малих і середніх підприємств щодо інтеграції у міжнародні виробничі й логістичні мережі.

По-друге, інституційна координація у сфері забезпечення цифрової стійкості залишається недостатньо розвиненою. Хоча Стратегія кібербезпеки України (Указ Президента № 447/2021) окреслює архітектуру суб'єктів та визначає координуючу роль Національного координаційного центру кібербезпеки при РНБО, на практиці відчувається потреба у більш тісній взаємодії між секторальними регуляторами та органами виконавчої влади, а також у налагодженні сталих каналів комунікації з бізнесом [139; 84]. З економічного погляду така фрагментарність інституційної взаємодії породжує регуляторну невизначеність, яка збільшує вартість укладення контрактів та формує додаткові премії за ризик, що підвищує загальну вартість капіталу для підприємств.

По-третє, кадровий потенціал у сфері цифрового ризик-менеджменту є обмеженим, особливо у сегменті малих і середніх підприємств та за межами ІТ-кластерів. ОЕСР наголошує на необхідності розгортання системних програм підготовки й перепідготовки кадрів з акцентом на управління ризиками, базові принципи кібергігієни та впровадження міжнародних стандартів, інтегруючи ці напрями в регіональні екосистеми підтримки бізнесу

[84]. Недостатня кількість фахівців у цій сфері зумовлює зростання витрат підприємств на забезпечення цифрової стійкості, уповільнює реалізацію проєктів трансформації та підвищує ймовірність неефективного використання інвестиційних ресурсів.

По-четверте, в Україні відсутня державна сертифікаційна схема мінімального рівня цифрової стійкості, орієнтована на малі та середні підприємства, подібна до британської програми Cyber Essentials (урядова, підтримувана промисловістю система базової сертифікації у сфері кіберзахисту) [140; 141]. У країнах, що використовують подібні інструменти, вони виконують роль своєрідного «сигналу якості» для контрагентів, знижуючи витрати на взаємні перевірки та полегшуючи доступ компаній до партнерських мереж. В українських умовах відсутність такого інструменту означає зростання витрат на підтвердження надійності підприємств у міжнародних відносинах, що ускладнює участь у тендерах та знижує конкурентоспроможність на зовнішніх ринках.

Сумарно інституційні прогалини трансформуються у суттєві макро- та мезоекономічні втрати. Вони проявляються у недоотриманих ефектах масштабу від цифровізації, зростанні витрат на страхування кіберризиків, обмеженні доступу підприємств до фінансування проєктів цифрової трансформації та зниженні рівня інтегрованості української економіки у європейські ланцюги створення доданої вартості.

Технологічні бар'єри становлять одну з найбільш відчутних перешкод для формування цифрової стійкості українських підприємств. Їхня природа пов'язана як із зовнішніми шоками, так і з внутрішньою слабкістю національної індустрії у сфері цифрових технологій. Такі тенденції мають безпосередній економічний вимір, оскільки переривання комунікацій уповільнює виробничі й логістичні процеси, підвищує витрати на організацію дистанційної роботи та обмежує здатність підприємств інтегруватися у міжнародні ринки.

Ще однією проблемою є висока залежність від зовнішніх постачальників цифрових технологій, включно з програмним забезпеченням, хмарними сервісами та апаратними рішеннями. У ситуації геополітичної нестабільності така залежність формує додаткові ризики перебоїв у постачанні та коливань вартості технологій, що безпосередньо позначається на фінансових результатах бізнесу. Відсутність розвиненої національної індустрії цифрових технологій звужує можливості для імпортозаміщення й диверсифікації ризиків, що означає підвищені витрати підприємств на підтримку цифрової стійкості та зниження їхньої інвестиційної привабливості [84].

Крім того, темпи впровадження інновацій в економіці залишаються недостатніми. Незважаючи на успіхи державних цифрових ініціатив, таких як масштабування електронних сервісів через платформу «Дія», значна частина малого та середнього бізнесу не використовує потенціал сучасних технологій через обмежений доступ до фінансування, відсутність належної технічної підтримки та слабку навчальну інфраструктуру [84]. Це формує асиметрію у рівні цифрової зрілості різних груп підприємств, внаслідок чого великі компанії отримують конкурентні переваги, тоді як МСП зіштовхуються із вищими витратами на адаптацію й втрачають можливості для інтеграції у транскордонні ланцюги створення вартості.

Таким чином, технологічні обмеження перетворюються на потужний економічний фактор, що знижує темпи цифрової трансформації, підвищує операційні витрати бізнесу та звужує простір для залучення інвестицій у розвиток виробничої та інфраструктурної бази. Вони посилюють ризики фрагментації ринку та поглиблюють структурні дисбаланси між секторами, ускладнюючи інтеграцію України в єдиний європейський цифровий простір.

Економічні чинники залишаються визначальними для темпів і глибини цифрової трансформації українського бізнесу, оскільки саме вони визначають здатність підприємств долати бар'єри входу в інноваційні проєкти та інтегруватися у глобальні ринки. Висока вартість цифрових рішень і засобів кіберзахисту, у поєднанні з асиметрією доступу до компетенцій та

інфраструктури, створює для малих і середніх підприємств непропорційні перешкоди, що унеможлиблюють досягнення критичної маси цифрової модернізації. За оцінками ОЕСР, вартість впровадження цифрових технологій для українських МСП залишається співмірною з рівнем розвинених економік, однак їхня фінансова спроможність істотно нижча, що формує ефект «витіснення» менш капіталізованих компаній із процесу цифровізації [84]. Це посилює структурний розрив у продуктивності між великим бізнесом та МСП і знижує віддачу від інвестицій у масштабі економіки.

Додатковим чинником є нестабільність середовища та воєнні ризики, які суттєво підвищують вартість капіталу та ускладнюють довгострокове фінансове планування. У звіті Світового банку наголошується, що невизначеність щодо тривалості воєнних дій, макроекономічні ризики та зростання потреби в короткострокових витратах на відновлення інфраструктури призводять до відтермінування інвестицій із відкладеним ефектом [142]. Це, своєю чергою, безпосередньо позначається на здатності підприємств фінансувати модернізацію виробничо-логістичних процесів, ускладнює доступ до міжнародних кредитних ліній і зменшує можливості інтеграції у транскордонні ланцюги створення доданої вартості. Таким чином, інституційно-фінансові бар'єри трансформуються в обмеження макроекономічного масштабу, посилюючи залежність від зовнішньої допомоги та скорочуючи горизонти внутрішніх інвестиційних стратегій.

Не менш вагомим є вплив погіршення якості та надійності комунікаційної інфраструктури внаслідок війни. За даними ОЕСР, станом на травень 2022 року середня швидкість передавання даних у фіксованих мережах в Україні знизилася на 13 %, а у мобільних мережах — на 26 %. Крім того, близько 12,2 % населених пунктів залишалися повністю без мобільного зв'язку, а ще 3,1 % мали лише часткове покриття [143]. Такі обмеження прямо конвертуються у зростання операційних витрат підприємств: ускладнюється організація дистанційної праці, уповільнюються ланцюги постачання, падає ефективність використання цифрових сервісів у повсякденній діяльності. Для

МСП це означає втрату гнучкості та конкурентних переваг, тоді як великі компанії частіше мають ресурси для диверсифікації каналів доступу та створення резервних комунікаційних рішень.

У сукупності ці фактори формують стійку економічну «премію за ризик» для цифрових інвестицій, що проявляється у зростанні вартості фінансування, підвищенні витрат на страхування та комплаєнс, а також у нерівномірності цифрової зрілості між секторами економіки. Це уповільнює загальне зростання продуктивності на макрорівні та звужує можливості інтеграції української економіки в європейський цифровий простір, поглиблюючи структурні дисбаланси і підвищуючи залежність від зовнішніх ринків капіталу.

Важливою групою стримуючих чинників для розвитку цифрової стійкості українських підприємств є інформаційні та культурні бар'єри, які мають як безпосередній економічний, так і опосередкований соціальний ефект. Дослідження ОЕСР підкреслюють, що малий і середній бізнес в Україні характеризується низьким рівнем обізнаності щодо цифрових ризиків і браком усталеної культури управління ними [84; 143]. Значна частина підприємств обмежується базовими заходами у сфері інформаційної безпеки, які не відповідають сучасним викликам, що призводить до зростання операційних витрат у випадку кібератак та втрат ділової репутації. У результаті компанії опиняються у гіршому становищі порівняно з європейськими конкурентами, для яких впровадження стандартів цифрової стійкості є елементом звичайної бізнес-практики.

Особливу проблему становить низький рівень довіри між бізнесом і державними інституціями. За оцінками ОЕСР, більшість українських підприємств утримуються від повідомлення про кіберінциденти державним органам, що позбавляє державу можливості акумулювати дані для аналізу загроз і обмежує потенціал для формування ефективної політики реагування [84]. Така ситуація має прямі економічні наслідки: через відсутність обміну інформацією підвищуються трансакційні витрати, пов'язані з повторними

аудитами, контрактними перевірками та залученням додаткових страхових механізмів.

У культурному вимірі обмеження проявляються у відсутності системної культури кібергігієни серед працівників та управлінців. Це знижує ефективність навіть тих інвестицій, які вже зроблені у цифрову інфраструктуру, оскільки без зміни поведінкових моделей та управлінських практик потенціал технологій залишається нереалізованим. Для зниження цього бар'єра держава створила Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ), що має на меті підвищення інформаційної грамотності та стійкості суспільства до дезінформації [144]. Проте його діяльність переважно спрямована на громадський сектор, тоді як підприємницьке середовище залишається недостатньо інтегрованим у ці ініціативи.

Таким чином, інформаційні та культурні обмеження уповільнюють формування цифрової стійкості бізнесу, обмежуючи ефективність інвестицій у технології, підвищуючи витрати на забезпечення довіри у ділових відносинах та знижуючи конкурентоспроможність українських підприємств у міжнародному економічному просторі.

Проведена класифікація та аналіз ризиків у сфері цифрової трансформації дають змогу усвідомити багатофакторний характер загроз для економічної безпеки підприємства. Ідентифікація та структуризація ризиків становлять лише початковий рівень дослідження, адже для практичного управління вирішальне значення має розуміння того, які економічні наслідки породжує реалізація цифрових ризиків у господарській діяльності конкретного суб'єкта. Саме вони визначають фінансову стійкість підприємства, його здатність зберігати конкурентні позиції на ринку, впливають на вартість залучення капіталу та рівень довіри з боку інвесторів, кредиторів і ділових партнерів. Перехід до аналізу економічних наслідків дозволяє безпосередньо пов'язати ризик-орієнтовану методологію з конкретними фінансовими

втратами та втраченою вигодою, що робить оцінку економічної безпеки підприємства більш прикладною та орієнтованою на практичні рішення.

Цифрові загрози справляють суттєвий вплив на економічну безпеку підприємств, породжуючи як прямі, так і непрямі втрати. Прямі економічні наслідки пов'язані з фінансовими санкціями, штрафами та значними витратами на реагування і відновлення після цілеспрямованих кіберінцидентів. В енергетичному секторі, який є одним із ключових для функціонування економіки, масштаби цифрових атак стали безпрецедентними: лише у 2022 році було зафіксовано понад 1,5 млн спроб кібератак на підприємства галузі, які вдалося заблокувати [145]. Цей показник демонструє не лише кількісну інтенсивність загроз, а й високу ціну забезпечення постійних заходів кіберзахисту, що для енергетичних компаній перетворюється на суттєві транзакційні витрати.

Непрямі економічні втрати проявляються у зниженні довіри інвесторів і партнерів. Масштабні кібератаки проти критичної інфраструктури формують негативні очікування щодо стабільності активів, що спонукає міжнародні фінансові інституції збільшувати премії за ризик або обмежувати участь у фінансуванні інвестиційних проєктів. Європейська бізнес асоціація (ЕВА) наголошує, що кібербезпека стала не лише технологічним, а й економічним фактором конкурентоспроможності, оскільки підприємства з нижчим рівнем захисту стикаються з вищою вартістю капіталу й обмеженим доступом до ринків [146].

Дані міжнародних спостерігачів підтверджують серйозність економічних наслідків атак. Так, у період між жовтнем 2022 р. та квітнем 2023 р. на енергетичну інфраструктуру України було здійснено щонайменше 66 цілеспрямованих кібератак, шкода від яких оцінюється більш ніж у 8 млрд дол. США [147]. Для підприємств енергетики це означало не лише фінансові втрати, а й різке зростання витрат на підтримку стабільності мереж, втрату довіри інвесторів та ускладнення умов залучення фінансування.

Не менш показовими є події у фінансовому секторі. У січні 2024 р. Служба безпеки України зафіксувала низку потужних атак на банки та дата-центри, що призвели до тимчасових перебоїв у доступі до фінансових і державних послуг [148]. Для банківських установ такі інциденти означають не лише витрати на відновлення інфраструктури, а й додаткові репутаційні ризики, що знижують рівень довіри клієнтів і партнерів та створюють довгострокові економічні втрати у вигляді відтоку капіталу й скорочення клієнтської бази.

Узагальнюючи, цифрові ризики перетворюються на комплексний економічний фактор тиску на підприємства. Вони підвищують операційні витрати, зменшують інвестиційну привабливість секторів, ускладнюють залучення фінансування й підвищують вартість капіталу. Нерівномірність прояву таких ризиків у різних секторах економіки формує додаткові структурні дисбаланси, що потребує врахування в оцінюванні економічної безпеки підприємств в умовах цифрової трансформації.

Висновки до розділу 2

Проведений аналіз діагностики, моделювання та управління цифровими ризиками у розрізі економічної безпеки підприємств дав змогу сформулювати такі висновки:

1. Сформовано логічну схему функціонально-ресурсного підходу до оцінювання економічної безпеки підприємства, яка демонструє багаторівневу організацію процесу діагностики – від аналізу окремих функціональних складових до оцінки інтегрального ресурсного забезпечення. Така схема відображає ієрархічність і взаємозалежність елементів безпеки, що дозволяє уникати однобічності при інтерпретації результатів та враховувати як внутрішні характеристики підприємства (наприклад, фінансові, виробничі, кадрові), так і зовнішні фактори (ринкові, інституційні, технологічні). Функціонально-ресурсний підхід виступає методологічною основою для

інтеграції діагностики у стратегічне управління, перетворюючи економічну безпеку на інструмент формування конкурентних переваг у цифровій економіці та забезпечуючи підприємству можливість прогнозувати зміни рівня стійкості й підвищувати обґрунтованість управлінських рішень. З економічного погляду це означає, що діагностика стає складовою процесу оптимізації витрат і підвищення ефективності використання ресурсів, а її результати безпосередньо впливають на здатність підприємства залучати капітал і забезпечувати стабільність грошових потоків.

2. Представлено систему індикаторів для діагностики складових економічної безпеки підприємства, що підтверджує ефективність індикаторного підходу як методологічної основи кількісної та якісної оцінки економічної стійкості. Групування показників за функціонально-ресурсними напрямками дало змогу розробити інструмент, який забезпечує комплексне відображення рівня безпеки та дозволяє виявляти проблемні зони у фінансовій, виробничій й організаційній діяльності. Узагальнено, що індикаторна система формує надійну інформаційну базу для ухвалення стратегічних управлінських рішень щодо оптимізації витрат, збереження ліквідності та підвищення інвестиційної привабливості, а також виконує функцію інструмента раннього попередження ризиків у цифровому середовищі. Доповненням до цього є результати кейс-аналізу підприємств різних секторів, які засвідчили, що високий рівень економічної безпеки досягається за рахунок інноваційної активності, цифровізації та диверсифікації бізнес-процесів, тоді як відсутність модернізації та надмірна залежність від зовнішніх ринків підвищують вразливість суб'єктів господарювання. Це уможлиблює не лише виявлення статистично значущих тенденцій, а й формування практичних рекомендацій для підприємств щодо пріоритетності інноваційно-цифрових стратегій як бази довгострокової стійкості в умовах турбулентного середовища.

3. На основі проведеного дослідження визначено та систематизовано цифрові ризики у трьох взаємодоповнювальних напрямках: ризики

кібербезпеки, регуляторні ризики та залежність від цифрових платформ. Така класифікація дозволила поглибити уявлення про економічний зміст цифрових загроз і уточнити логіку їхнього впливу на ключові параметри економічної безпеки підприємства. Доведено, що ризики кібербезпеки безпосередньо позначаються на витратній частині діяльності підприємства через необхідність відновлення порушених процесів, компенсаційні виплати та втрату довіри контрагентів, що у довгостроковому вимірі трансформується у зростання вартості капіталу. Регуляторні ризики формують додатковий тиск на підприємства у вигляді зростання трансакційних витрат на дотримання вимог комплаєнсу, можливих штрафних санкцій і втрати доступу до міжнародних ринків, що знижує конкурентоспроможність і інвестиційну привабливість. Залежність від цифрових платформ створює економічні виклики у вигляді специфічних витрат перемикання, посилює концентрацію операційних ризиків і підвищує чутливість підприємств до змін політик глобальних провайдерів, що ускладнює прогнозування та стабільність фінансових потоків. Узагальнення цієї типології дозволило розробити підхід до відображення кореляції між класами цифрових ризиків і ключовими індикаторами ефективності та ризику (KPI/KRI), що інтегрує цифрові детермінанти у систему моніторингу економічної безпеки підприємства. У науковому плані це уможливлює кількісне співставлення ризиків із результатами діяльності, а у прикладному – формує підґрунтя для розробки механізмів ризик-орієнтованого управління, які підвищують здатність підприємства підтримувати економічну стійкість і забезпечувати довгострокові конкурентні переваги в умовах цифрової трансформації економіки України.

4. Удосконалено інструментарій оцінювання економічної безпеки підприємства через побудову моделі ризик-орієнтованого управління, яка систематизує взаємозв'язок між виявленими цифровими ризиками та механізмами реагування на них. У моделі відображено логіку переходу від діагностики ризиків до формування управлінських рішень, що уможливлює інтеграцію індикаторного підходу з практичними заходами стратегічного

планування. Особливе значення має те, що модель поєднує кількісну оцінку впливу ризиків із якісними аспектами управління, забезпечуючи баланс між витратами на превентивні заходи та потенційними економічними збитками. Це дозволяє підприємству не лише ідентифікувати найбільш критичні ризики, але й прогнозувати їхній вплив на фінансові результати, операційну ефективність і вартість капіталу. Розроблена модель створює можливість для комплексного аналізу чутливості бізнес-процесів до цифрових загроз та вибудовує логіку прийняття рішень у координатах «ризик–результат», що підвищує адаптивність підприємства до умов цифрової трансформації економіки України. У науковому вимірі вона є кроком до формування методології оцінки економічної безпеки, яка інтегрує сучасні ризик-орієнтовані інструменти, а у прикладному – забезпечує практичний алгоритм підвищення стійкості підприємств у турбулентному цифровому середовищі.

5. У даному підрозділі нами поглиблено методологію оцінювання економічної безпеки підприємства в умовах цифрової трансформації шляхом представлення циклу управління цифровими ризиками та систематизації ключових індикаторів ефективності для його практичної реалізації. Запропонований підхід дозволив розробити узгоджену послідовність етапів: від ідентифікації та захисту до реагування й відновлення, кожен з яких отримав чіткий економічний зміст у координатах витрат і результатів. Систематизація індикаторів уможливила трансформацію управлінських цілей у вимірювані параметри, що забезпечує зіставлення превентивних інвестицій у кіберстійкість з очікуваними економічними втратами та сприяє інтеграції ризик-орієнтованого управління у стратегічне й фінансове планування. Це дозволяє розглядати цифрові ризики не лише як технічний феномен, а як економічно релевантний чинник, що визначає стійкість і конкурентоспроможність підприємства, а також практичний алгоритм для оптимізації ресурсів і підвищення інвестиційної привабливості бізнесу. Додатково обґрунтовано, що включення цифрових ризиків до системи оцінки економічної безпеки забезпечує більш комплексне врахування

трансформаційних факторів розвитку, що відповідає концептуальним завданням оцінки економічної безпеки підприємства в умовах цифрової трансформації економіки України.

6. Охарактеризовано та оцінено методики оцінки цифрової безпеки, які застосовуються у різних країнах, із метою виявлення їхньої релевантності для українського контексту та адаптації до національної специфіки. Це дозволило здійснити порівняльний аналіз міжнародних практик і сформувані орієнтири для вдосконалення підходів до управління цифровою стійкістю вітчизняних підприємств. На основі отриманих результатів систематизовано інституційні, регуляторні, технологічні, економічні та інформаційно-культурні обмеження, що поглибило розуміння бар'єрів забезпечення економічної безпеки підприємств в умовах цифрової трансформації. Виявлено, що відсутність єдиного стандарту кіберстійкості для нефінансового сектору, низька імплементація європейських директив, кадровий дефіцит та недостатній розвиток сертифікаційних програм зумовлюють зростання трансакційних витрат, ускладнюють доступ до фінансування та підвищують вартість капіталу. Удосконалений підхід до групування цих обмежень за сферами впливу дозволяє підприємствам визначати пріоритети управлінських дій і формувати економічно доцільні сценарії реагування на цифрові ризики. Доведено, що подолання зазначених бар'єрів у поєднанні з адаптацією кращих зарубіжних методик є не лише умовою підвищення рівня цифрової стійкості, а й важливим чинником зростання інвестиційної привабливості та інтеграції українських підприємств у європейські ланцюги створення вартості, що повністю відповідає темі дисертації та концептуальним засадам оцінки економічної безпеки підприємства.

Основні положення розділу розкрито у публікаціях автора [64; 65; 66; 102].

РОЗДІЛ 3. МЕТОДИКА ІНТЕГРАЛЬНОГО ОЦІНЮВАННЯ, ДІАГНОСТИКИ ТА ПРОГНОЗУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ

3.1. Методика формування інтегрального індексу економічної безпеки підприємств

Формування системи показників оцінювання економічної безпеки підприємства є ключовим етапом побудови прикладного інструментарію аналізу, оскільки саме на цьому рівні відбувається перехід від теоретичного осмислення категорії економічної безпеки до її кількісного вимірювання. У працях українських науковців економічна безпека підприємства послідовно розглядається як фінансово зумовлений стан захищеності ресурсів і процесів господарської діяльності, що забезпечує стійкість функціонування та здатність суб'єкта господарювання до розвитку в умовах дії внутрішніх і зовнішніх ризиків [156; 157].

Як обґрунтовує О. О. Терещенко, саме фінансові показники є найбільш об'єктивною основою для оцінювання рівня економічної безпеки підприємства, оскільки вони акумулюють наслідки впливу виробничих, інвестиційних, ринкових і управлінських рішень та дозволяють здійснювати міжчасові і міжсуб'єктні порівняння [158]. Такий підхід особливо важливий в умовах цифрової трансформації, коли значна частина ризиків реалізується опосередковано через фінансові результати, структуру капіталу та ефективність використання ресурсів.

З урахуванням зазначеного у дослідженні сформовано систему показників економічної безпеки підприємства, структуровану за п'ятьма функціональними блоками: фінансова стійкість; ліквідність і платоспроможність; рентабельність; ділова активність; інвестиційно-структурна спроможність. Така логіка побудови відповідає класичним

підходам фінансового аналізу, розробленим у працях А. М. Поддєрьогіна та І. А. Бланка, і водночас дозволяє адаптувати індикаторну базу до завдань оцінювання економічної безпеки підприємства [159; 160].

До *показників фінансової стійкості* у межах дослідження віднесено коефіцієнт автономії, коефіцієнт фінансового левериджу та коефіцієнт покриття власним капіталом. У наукових працях І. А. Бланка фінансова стійкість визначається як здатність підприємства підтримувати збалансовану структуру джерел фінансування, зберігати фінансову незалежність і протистояти довгостроковим ризикам, що є базовою умовою забезпечення фінансової та економічної безпеки [160]. А. М. Поддєрьогін підкреслює, що надмірна частка позикового капіталу підвищує чутливість підприємства до змін ринкової кон'юнктури та обмежує його можливості щодо фінансування розвитку, що в умовах цифровізації істотно посилює загрози економічній безпеці [159].

Показники ліквідності та платоспроможності представлені коефіцієнтом поточної ліквідності, коефіцієнтом швидкої ліквідності та показником чистого оборотного капіталу. Як зазначає Г. В. Савицька, платоспроможність підприємства є одним із ключових критеріїв його фінансової стабільності, оскільки саме вона визначає здатність суб'єкта господарювання своєчасно виконувати поточні зобов'язання та забезпечувати безперервність операційної діяльності [161]. У цифровізованому середовищі дефіцит ліквідних ресурсів може призводити не лише до фінансових ускладнень, а й до збоїв у функціонуванні бізнес-процесів, що трансформують проблему ліквідності у системну загрозу економічній безпеці підприємства.

До *показників рентабельності* віднесено рентабельність активів (ROA), рентабельність власного капіталу (ROE) та операційну маржу. У працях О. О. Терещенка та Г. В. Савицької рентабельність розглядається як узагальнюючий показник ефективності використання ресурсного потенціалу підприємства та результативності управлінських рішень [158; 161]. В умовах цифрової трансформації показники прибутковості набувають додаткового

аналітичного значення, оскільки відображають здатність підприємства компенсувати зростання витрат, пов'язаних з технологічним оновленням, цифровими інвестиціями та трансформацією бізнес-моделей, без втрати економічної результативності.

Показники ділової активності, зокрема оборотність активів, дебіторської заборгованості та запасів, характеризують швидкість трансформації вкладеного капіталу у фінансовий результат. І. А. Бланк наголошує, що низька оборотність активів є свідченням неефективного використання ресурсів і зростання ризиків фінансової нестійкості підприємства [162]. У цифровій економіці, де ключовими чинниками конкурентоспроможності стають гнучкість і швидкість реагування на зміни ринкового середовища, показники ділової активності виступають важливими індикаторами адаптивності підприємства та його стійкості до операційних ризиків.

Окреме місце в системі оцінювання економічної безпеки займають **інвестиційно-структурні показники**, до яких віднесено частку необоротних активів у валюті балансу, темпи оновлення основних засобів та співвідношення капітальних інвестицій до виручки. У дослідженнях Т. Г. Васильціва інвестиційна активність розглядається як один із визначальних чинників довгострокової економічної безпеки підприємств, оскільки вона формує передумови технологічного оновлення, підвищення продуктивності та збереження конкурентних позицій [156]. У межах даного дослідження зазначені показники використовуються як фінансові проксі цифрової трансформації, що дозволяє оцінити інноваційно-інвестиційний потенціал підприємства на основі відкритої фінансової звітності.

Таким чином, запропонована система показників оцінювання економічної безпеки підприємства методологічно спирається на напрацювання української наукової школи фінансового аналізу та економічної безпеки і водночас адаптована до умов цифрової трансформації економіки. Вона забезпечує аналітичну узгодженість між теоретичними положеннями

дисертації та подальшими розрахунковими процедурами і створює підґрунтя для нормалізації показників, визначення вагових коефіцієнтів і формування інтегрального індексу економічної безпеки підприємства.

Важливо зазначити, що у фінансовій звітності підприємств відсутні прямі кількісні показники, які б безпосередньо характеризували рівень цифрової трансформації бізнес-процесів. У зв'язку з цим у межах запропонованої методики цифровізація не виділяється у вигляді окремої групи індикаторів, а враховується опосередковано – через систему фінансових показників, що відображають результати структурних, технологічних та організаційних змін у діяльності підприємства. Передбачається, що впровадження цифрових рішень впливає на ліквідність, фінансову стійкість, ділову активність і прибутковість суб'єкта господарювання, а отже, знаходить відображення у значеннях відповідних показників економічної безпеки, систематизованих у таблиці 3.1. Такий підхід дозволяє інтегрувати цифрову складову в кількісну модель оцінювання без введення додаткових нефінансових змінних і забезпечує можливість динамічного та міжгалузевого порівняння результатів.

Водночас прямі кількісні метрики цифрової трансформації (рівень автоматизації процесів, проникнення ІТ-рішень, інтенсивність використання даних тощо) у стандартизованих формах фінансової звітності, як правило, не виокремлюються, що обмежує можливість їх безпосереднього включення до розрахункової моделі. У зв'язку з цим у методиці застосовано проксі-показники цифровізаційних зрушень, тобто фінансові індикатори, які відображають результативні прояви технологічного оновлення та інвестиційної активності підприємства. До таких проксі в межах сформованої системи показників віднесено, зокрема, частку необоротних активів, темп оновлення основних засобів та співвідношення капітальних інвестицій до виручки, що дозволяє врахувати інвестиційно-структурну компоненту трансформації без введення нефінансових змінних.

Таблиця 3.1

Система показників оцінювання економічної безпеки підприємства

Група показників	Показник	Формула розрахунку	Економічний зміст показника	Джерело даних
1	2	3	4	5
Фінансова стійкість	Коефіцієнт автономії	Власний капітал / Валюта балансу	Рівень фінансової незалежності підприємства	Баланс (форма №1)
	Коефіцієнт фінансового левериджу	Зобов'язання / Власний капітал	Залежність від позикового капіталу	Баланс (форма №1)
	Коефіцієнт покриття власним капіталом	Власний капітал / Необоротні активи	Здатність фінансувати необоротні активи	Баланс (форма №1)
Ліквідність і платоспроможність	Коефіцієнт поточної ліквідності	Оборотні активи / Поточні зобов'язання	Загальна платоспроможність	Баланс (форма №1)
	Коефіцієнт швидкої ліквідності	(Оборотні активи – Запаси) / Поточні зобов'язання	Платоспроможність без реалізації запасів	Баланс (форма №1)
	Чистий оборотний капітал	Оборотні активи – Поточні зобов'язання	Фінансовий резерв операційної діяльності	Баланс (форма №1)
Рентабельність	Рентабельність активів, ROA	Чистий прибуток / Середні активи	Ефективність використання активів	Баланс (форма №1); Звіт про фінансові результати (форма №2)
	Рентабельність власного капіталу, ROE	Чистий прибуток / Середній власний капітал	Дохідність власного капіталу	Баланс (форма №1); Звіт про фінансові результати (форма №2)
	Операційна маржа	Операційний прибуток / Чистий дохід	Ефективність основної діяльності	Звіт про фінансові результати (форма №2)

Продовження табл. 3.1

1	2	3	4	5
Ділова активність	Оборотність активів	Чистий дохід / Середні активи	Інтенсивність використання ресурсів	Баланс (форма №1); Звіт про фінансові результати (форма №2)
	Оборотність дебіторської заборгованості	Чистий дохід / Середня дебіторська заборгованість	Швидкість інкасації коштів	Баланс (форма №1); Звіт про фінансові результати (форма №2)
	Оборотність запасів	Собівартість реалізації / Середні запаси	Ефективність управління запасами	Баланс (форма №1); Звіт про фінансові результати (форма №2)
Інвестиційно-структурна спроможність	Частка необоротних активів	Необоротні активи / Валюта балансу	Рівень капіталоємності	Баланс (форма №1)
	Темп оновлення основних засобів	Введені ОЗ / Первісна вартість ОЗ	Інтенсивність оновлення активів	Примітки до фінансової звітності (форма №5)
	Співвідношення капітальних інвестицій до виручки	Капітальні інвестиції / Чистий дохід	Інвестиційна активність	Примітки до фінансової звітності (форма №5); Звіт про фінансові результати (форма №2)

Джерело: узагальнено автором на основі [155–162].

Застосування інтегрального підходу до оцінювання економічної безпеки підприємства передбачає агрегування різнорідних фінансових показників, які відрізняються за економічним змістом, одиницями виміру та діапазонами варіації. У зв'язку з цим передумовою формування узагальнюючого показника є приведення вихідних індикаторів до порівнянного вигляду шляхом їх нормалізації, а також обґрунтований вибір вагових коефіцієнтів, що відображають відносну значущість кожної групи показників у структурі економічної безпеки підприємства.

У межах даного дослідження нормалізація показників здійснюється з використанням методу мін–макс, який є поширеним у практиці побудови композитних індексів та інтегральних оцінок, оскільки забезпечує приведення різнорідних показників до єдиного інтервалу $[0;1]$ і збереження відносних пропорцій між спостереженнями. Застосування мін–макс нормалізації є доцільним для аналізу фінансових коефіцієнтів підприємств, оскільки дозволяє коректно агрегувати показники, що відрізняються масштабною та варіацією у вибірці, за умови контролю впливу екстремальних значень [163; 164].

Для показників-стимуляторів, зростання яких свідчить про підвищення рівня економічної безпеки підприємства (зокрема, коефіцієнт автономії, рентабельність активів, оборотність активів, частка необоротних активів), нормалізоване значення визначається за формулою:

$$x'_i = \frac{x_i - x_{min}}{x_{max} - x_{min}}, \quad (3.1)$$

де x_i – фактичне значення показника;

x_{max}, x_{min} – відповідно мінімальне та максимальне значення показника у вибірці підприємств або в часовому інтервалі дослідження.

Для показників-дестимуляторів, зростання яких негативно впливає на рівень економічної безпеки (зокрема, коефіцієнт фінансового левериджу, надмірна залежність від зобов'язань), застосовується трансформована формула нормалізації:

$$x'_i = \frac{x_{max} - x_i}{x_{max} - x_{min}}. \quad (3.2)$$

Такий підхід забезпечує уніфіковану інтерпретацію нормалізованих значень: у всіх випадках зростання x_i відповідає підвищенню рівня економічної безпеки підприємства. У результаті нормалізації всі показники набувають значень у діапазоні $[0;1]$, що створює методичні передумови для їх подальшого агрегування.

Наступним етапом формування інтегрального індексу є визначення вагових коефіцієнтів показників. У дослідженні застосовано ентропійний підхід до зважування, що ґрунтується на понятті ентропії як міри невизначеності та інформаційної насиченості даних у теорії інформації [165; 166]. У межах багатокритеріальних задач ентропійний метод використовується для отримання об'єктивних ваг на основі ступеня диференціації (варіативності) показників у матриці спостережень: чим більша розбіжність значень критерію між об'єктами, тим вищою є його інформаційна цінність і тим більшою може бути вага в інтегральній оцінці [167]. Застосування такого підходу є методично виправданим у прикладних розрахунках, коли потрібно мінімізувати суб'єктивність при зважуванні показників і забезпечити відтворюваність результатів.

На першому етапі розраховується p_{ij} частка i -го показника для j -го підприємства:

$$p_{ij} = \frac{x'_{ij}}{\sum_{j=1}^m x'_{ij}}, \quad (3.3)$$

де m – кількість підприємств у вибірці.

Далі визначається ентропія кожного показника, яка відображає ступінь невизначеності та інформаційної насиченості відповідного індикатора у вибірці підприємств. Розрахунок ентропії здійснюється за формулою:

$$E^i = -k \sum_{j=1}^m p_{ij} \ln p_{ij}, \quad (3.4)$$

де E^i – значення ентропії i -го показника;

p_{ij} – частка нормалізованого значення i -го показника для j -го підприємства у загальній сумі нормалізованих значень цього показника;

m – кількість підприємств (об'єктів спостереження) у вибірці;

$\ln$ – натуральний логарифм (логарифм за основою $e \approx 2,71828$), який використовується у теорії інформації для кількісного вимірювання невизначеності;

$k = \frac{1}{\ln m}$ – коефіцієнт нормалізації, що забезпечує приведення значення ентропії до інтервалу $[0;1]$.

Використання натурального логарифма у формулі ентропії зумовлене класичним визначенням інформаційної ентропії, запропонованим К. Шенноном, і є загальноприйнятим у прикладних дослідженнях, пов'язаних із багатокритеріальним аналізом та побудовою інтегральних індексів [165; 166]. Застосування коефіцієнта нормалізації k дозволяє усунути вплив розміру вибірки та забезпечити порівнянність ентропійних оцінок для різної кількості підприємств. Чим ближчим є значення ентропії E_i до одиниці, тим меншою є варіативність відповідного показника у вибірці та, відповідно, нижчою є його інформаційна значущість для оцінювання економічної безпеки підприємства. Навпаки, нижчі значення E_i свідчать про вищу диференціюючу здатність показника і більший внесок у формування інтегрального індексу.

Відповідно, ступінь варіативності показника визначається як різниця між одиницею та значенням його ентропії:

$$d_i = 1 - E_i, \quad (3.5)$$

де d_i – ступінь варіативності (диференціюючої здатності) i -го показника;

E_i – ентропія i -го показника, що характеризує рівень упорядкованості його значень у вибірці.

Економічний зміст показника d_i полягає в тому, що він відображає міру інформаційної корисності відповідного індикатора для оцінювання економічної безпеки підприємства. Якщо значення показника у вибірці є

близькими між собою, його ентропія наближається до одиниці, а ступінь варіативності до нуля, що свідчить про низьку здатність такого показника диференціювати об'єкти дослідження. Натомість значна варіативність значень показника зумовлює нижчий рівень ентропії та, відповідно, вищу інформаційну значущість показника для інтегральної оцінки.

На завершальному етапі розраховуються вагові коефіцієнти показників, які визначають відносний внесок кожного індикатора у формування інтегрального індексу економічної безпеки підприємства:

$$w_i = \frac{d_i}{\sum_{i=1}^n d_i}, \quad (3.6)$$

де w_i – ваговий коефіцієнт i -го показника;

d_i – ступінь варіативності i -го показника;

n – кількість показників у системі оцінювання.

Зазначена формула забезпечує нормування вагових коефіцієнтів, у результаті чого виконується умова $\sum_{i=1}^n w_i = 1$. Це дозволяє інтерпретувати ваги як частки внеску окремих показників у загальний рівень економічної безпеки підприємства. Використання ступеня варіативності як основи для визначення ваг забезпечує об'єктивний характер зважування, оскільки показники з більшою інформаційною насиченістю автоматично отримують більшу вагу в інтегральному індексі.

Запропонований підхід до визначення вагових коефіцієнтів дозволяє врахувати реальні відмінності у фінансовому стані підприємств, що досліджуються, та забезпечує адаптивність інтегрального індексу економічної безпеки до галузевих і часових особливостей вибірки, мінімізуючи вплив суб'єктивних експертних оцінок при формуванні ваг.

Після обґрунтування системи показників та визначення процедур нормалізації і вагового зважування постає принципове прикладне завдання: одержати одну узагальнену величину, яка дозволяє: по-перше, зіставляти підприємства між собою; по-друге, відстежувати динаміку економічної

безпеки в часі; по-третє, виділяти ті компоненти фінансового стану, що формують «вузькі місця» і потребують управлінських рішень. Саме ці вимоги зумовлюють використання композитного (інтегрального) індикатора, який будується як агрегована функція нормалізованих показників із вагами, що відображають їх відносну значущість у сукупній оцінці [163].

У прикладних економічних дослідженнях композитні індекси застосовують тоді, коли об'єкт оцінювання є багатовимірним, а набір показників містить одночасно індикатори різної природи та масштабу. За цих умов методологічно важливо забезпечити дві властивості побудови індексу:

- порівнянність показників, що досягається нормалізацією (у нашому випадку – мін–макс перетворенням до інтервалу [0;1]);
- інтерпретованість інтегрального результату, тобто можливість пояснити, які саме показники і з якою «силою» вплинули на підсумковий рівень економічної безпеки.

З урахуванням характеру інформаційної бази дослідження, сформованої на основі фінансової звітності підприємств (Баланс, форма № 1; Звіт про фінансові результати, форма № 2; Примітки до фінансової звітності, форма № 5), як базову форму агрегування доцільно використовувати адитивну зважену модель. Її перевага полягає в аналітичній прозорості та можливості економічного тлумачення отриманих результатів, оскільки зміна інтегрального показника може бути декомпозована на внески окремих індикаторів. Це, в свою чергу, дає змогу безпосередньо пов'язати динаміку інтегрального індексу з фінансовими рішеннями у сфері управління ліквідністю, структурою капіталу, прибутковістю, оборотністю активів та інвестиційною активністю підприємства. У методології побудови композитних індикаторів така форма агрегування розглядається як одна з найбільш уживаних, оскільки поєднує інтерпретованість результатів із відтворюваністю обчислень [163].

Відповідно, *інтегральний індекс економічної безпеки підприємства* визначається за формулою:

$$I_{\text{ЕБ}} = \sum_{i=1}^n w_i \times x'_i, \quad (3.7)$$

де $I_{\text{ЕБ}}$ – інтегральний індекс економічної безпеки підприємства;

x'_i – нормалізоване значення i -го показника системи оцінювання, приведене до інтервалу $[0;1]$;

w_i – ваговий коефіцієнт i -го показника;

n – кількість показників, включених до системи оцінювання.

Запропонована форма інтегрального індексу має низку важливих властивостей. По-перше, індекс є безрозмірною величиною, що усуває вплив одиниць виміру первинних показників і забезпечує коректність порівнянь між підприємствами різних масштабів. По-друге, за умови нормалізації показників та виконання умови $\sum_{i=1}^n w_i = 1$, значення інтегрального індексу перебуває в межах інтервалу $[0;1]$, що створює зручну основу для подальшої інтерпретації результатів та формування порогових значень рівнів економічної безпеки.

Вагові коефіцієнти w_i , визначені за допомогою ентропійного методу, відображають інформаційну насиченість і диференціюючу здатність окремих показників у вибірці підприємств. Це означає, що більший вплив на інтегральний індекс мають ті індикатори, значення яких істотно варіюють між підприємствами і, відповідно, краще характеризують відмінності в їх фінансовому стані. Такий підхід дозволяє зменшити суб'єктивність при зважуванні показників і забезпечує узгодженість інтегральної оцінки з реальними фінансовими характеристиками досліджуваних суб'єктів господарювання.

Отже, сформований інтегральний індекс економічної безпеки підприємства є логічним завершенням процедур добору, нормалізації та зважування показників і водночас створює методичну основу для подальшої шкали інтерпретації.

Інтегральний індекс економічної безпеки підприємства, будучи узагальненим показником, потребує інтерпретаційної шкали, яка дозволяє перейти від формального числового значення до економічно змістовних висновків. Оскільки індекс розраховується на основі нормалізованих показників, приведених до інтервалу $[0;1]$, а вагові коефіцієнти задовольняють

умову нормування, значення інтегрального індексу також перебуває в межах цього інтервалу. Саме це створює методологічні передумови для застосування інтервального підходу до його інтерпретації.

У межах даного дослідження використано трирівневу шкалу інтерпретації, яка передбачає виділення низького, середнього та високого рівнів економічної безпеки підприємства (таблиця 3.2).

Таблиця 3.2

Шкала інтерпретації значень інтегрального індексу економічної безпеки підприємства

Значення інтегрального індексу економічної безпеки	Рівень економічної безпеки	Характеристика стану
$IEB < 0,50$	Низький	Високий рівень фінансової вразливості, системні диспропорції у структурі капіталу, ліквідності та результативності діяльності
$0,50 \leq IEB < 0,70$	Середній	Задовільний фінансовий стан за наявності окремих зон ризику та обмеженого запасу економічної стійкості
$IEB \geq 0,70$	Високий	Стійкий і збалансований фінансовий стан, наявність резервів для розвитку та протидії зовнішнім і внутрішнім загрозам

Джерело: авторська розробка.

Нижню межу шкали інтерпретації інтегрального індексу економічної безпеки підприємства визначено на рівні $IEB = 0,50$. Обрання саме цього порогового значення є методично та економічно обґрунтованим, оскільки воно відповідає середині нормалізованого інтервалу $[0;1]$, у межах якого здійснюється розрахунок інтегрального показника. Отже, значення індексу нижче 0,50 означає, що сукупна реалізація потенціалу економічної безпеки підприємства є меншою за середній рівень, що формується на основі всієї системи показників.

За таких значень інтегрального індексу більшість фінансових показників або показники з найбільшою ваговою значущістю мають значення, нижчі за середній рівень нормалізованої шкали. Це свідчить не про окремі відхилення, а про системний характер фінансових диспропорцій, зокрема у структурі

капіталу, ліквідності, платоспроможності та результативності діяльності. Оскільки саме ці параметри формують основу фінансової стійкості підприємства, їх погіршення зумовлює зростання чутливості до зовнішніх шоків, обмежує здатність до самофінансування та підвищує ризик втрати економічної рівноваги. Отже, інтервал значень $I_{EB} < 0,50$ обґрунтовано інтерпретується як низький рівень економічної безпеки, що потребує першочергових управлінських рішень стабілізаційного характеру.

Інтервал $0,50 \leq I_{EB} < 0,70$ характеризує середній рівень економічної безпеки підприємства. У цьому діапазоні значень інтегрального індексу підприємство, як правило, зберігає загальну фінансову стабільність, здатність виконувати поточні зобов'язання та підтримувати безперервність господарської діяльності. Водночас значення індексу не досягають рівня, який би свідчив про наявність достатнього запасу фінансової міцності. Це означає, що окремі складові економічної безпеки залишаються вразливими, а негативний вплив зовнішніх або внутрішніх чинників може призвести до погіршення фінансового стану.

Отже, середній рівень економічної безпеки доцільно розглядати як задовільний з позицій поточного функціонування, але недостатній для забезпечення стійкого розвитку в довгостроковій перспективі. Підприємство в цьому інтервалі перебуває у зоні підвищеної уваги з боку системи управління, оскільки збереження такого рівня без реалізації заходів з посилення фінансової стійкості може трансформуватися у зниження загального рівня економічної безпеки.

Порогове значення $I_{EB} \geq 0,70$ визначає високий рівень економічної безпеки підприємства. Вибір цієї межі зумовлений тим, що за таких значень інтегрального індексу переважна більшість нормалізованих показників наближається до верхньої частини шкали, а негативні відхилення окремих індикаторів не мають визначального впливу на загальний результат. Це свідчить про збалансовану структуру фінансових ресурсів, прийнятний рівень

ліквідності, стабільні фінансові результати та наявність резервів фінансової стійкості.

Оскільки за високого рівня інтегрального індексу підприємство володіє не лише здатністю адаптуватися до змін зовнішнього середовища, а й потенціалом для реалізації стратегічних цілей розвитку, такий стан економічної безпеки слід інтерпретувати як проактивний. Отже, межа 0,70 відображає перехід від адаптаційної моделі фінансової поведінки до моделі, орієнтованої на розвиток без істотної загрози втрати фінансової стійкості.

Таким чином, запропонована шкала інтерпретації інтегрального індексу економічної безпеки підприємства не має нормативного характеру, проте ґрунтується на внутрішній логіці нормалізованих показників і фінансово-економічному змісті категорії безпеки. Саме в такому вигляді вона є методично достатньою для порівняльного аналізу підприємств, оцінювання динаміки економічної безпеки та формування обґрунтованих управлінських висновків у подальших підрозділах дисертації.

3.2. Аналітична діагностика та порівняльна оцінка економічної безпеки підприємств на основі інтегрального підходу

Емпіричну основу дослідження сформовано на базі вибірки великих підприємств України, що репрезентують стратегічно важливі галузі національної економіки та характеризуються підвищеним рівнем вимог до економічної безпеки в умовах цифрової трансформації. Формування вибірки здійснювалося з урахуванням принципів порівнюваності, інформаційної доступності та безперервності часових рядів.

До вибірки включено підприємства, які відповідають таким критеріям відбору:

- ✓ по-перше, належність до категорії великих підприємств за обсягами активів і доходів, що зумовлює складність фінансових потоків та підвищену чутливість до ризиків;

- ✓ по-друге, наявність повної фінансової звітності, складеної відповідно до МСФЗ з можливістю уніфікації показників;
- ✓ по-третє, забезпечення безперервності фінансових даних упродовж 2020–2024 рр., що дозволяє здійснювати динамічний аналіз та порівняння показників у часі.

Галузеву структуру вибірки сформовано таким чином, щоб забезпечити порівняльний міжгалузевий зріз на основі кейсової вибірки стратегічних підприємств. До дослідження включено підприємства таких галузевих груп:

- енергетика та газопостачання (ПрАТ «НЕК «Укренерго», ТОВ «Газопостачальна компанія «Нафтогаз України»);
- транспортна інфраструктура, логістика та поштові послуги (АТ «Українська залізниця», АТ «Укрпошта»);
- промислове виробництво та металургія (Interpipe Holdings PLC).

Такий склад вибірки дозволяє зіставляти підприємства з різними операційними моделями, рівнем капіталоемності та ступенем цифрової трансформації бізнес-процесів, що є критично важливим для оцінювання економічної безпеки.

Комплект фінансової звітності, використаний у дослідженні, є уніфікованим і включає: звіт про фінансовий стан (баланс), звіт про сукупний дохід (фінансові результати), звіт про рух грошових коштів, звіт про зміни у власному капіталі, а також примітки до фінансової звітності.

Для забезпечення порівнянності показників між підприємствами різних видів економічної діяльності здійснено уніфікацію фінансових даних шляхом використання відносних коефіцієнтів, нормалізації абсолютних показників та приведення облікових статей до єдиної аналітичної структури. Такий підхід дозволяє мінімізувати вплив специфіки видів економічної діяльності та масштабів функціонування підприємств на результати оцінювання, зосередивши аналіз на реальних змінах рівня їх економічної безпеки у динаміці.

З метою забезпечення аналітичної глибини дослідження та можливості виявлення структурних відмінностей у формуванні економічної безпеки підприємств сформовану вибірку згруповано за видами економічної діяльності відповідно до національної класифікації КВЕД (NACE 2.1). Таке групування дозволяє перейти від аналізу окремих суб'єктів господарювання до узагальненого порівняння моделей економічної безпеки, що сформувалися в різних секціях економіки, з урахуванням особливостей операційної діяльності, рівня капіталоємності та ролі підприємств у забезпеченні стабільності економічних процесів. Структуру вибірки підприємств за видами економічної діяльності та її основні характеристики наведено в таблиці 3.3.

Таким чином, сформована вибірка підприємств та її структура за видами економічної діяльності створюють необхідні передумови для проведення порівняльної аналітичної діагностики економічної безпеки у міжсекторальному розрізі. Використання уніфікованої інформаційної бази на основі повного комплексу фінансової звітності, складеної за міжнародними стандартами фінансової звітності, забезпечує зіставність показників у часовому інтервалі 2020–2024 рр. та мінімізує вплив методологічних розбіжностей облікових підходів на результати оцінювання. Водночас диференціація вибірки за секціями видів економічної діяльності створює аналітичне підґрунтя для виявлення як спільних тенденцій, так і структурно зумовлених відмінностей у динаміці економічної безпеки підприємств, що обумовлює доцільність переходу до поглибленого аналізу рівнів, трендів і варіативності ключових показників.

Таблиця 3.3

Структура вибірки підприємств за видами економічної діяльності у дослідженні економічної безпеки

Вид економічної діяльності за КВЕД/ (NACE 2.1-UA)	Підприємства вибірки	Кількість підприємств	Частка у вибірці, %	Ключові фактори та характеристики діяльності, релевантні для оцінювання економічної безпеки підприємств
1	2	3	4	5
С Переробна промисловість (для вибірки – виробництво основних металів, розділ 24)	Interpipe Holdings PLC	1	20	Характеризується циклічністю фінансових результатів, високою залежністю від кон'юнктури зовнішніх ринків, цін на сировину та енергоносії, а також валютних коливань. Економічна безпека підприємств формується під впливом рівня рентабельності, конкурентоспроможності, ефективності структури капіталу та управління фінансовими ризиками. Визначальними є показники інвестиційної активності, технологічного оновлення, енергоефективності та цифровізації виробничих і управлінських процесів.
Н Транспорт і складське господарство (включно з поштовою та кур'єрською діяльністю, розділи 49, 53)	АТ «Українська залізниця»; АТ «Укрпошта»	2	40	Характеризується високою операційною інтенсивністю, складною структурою активів і значними витратами на підтримання інфраструктури та логістичних ланцюгів. Економічна безпека визначається ефективністю управління витратами й оборотністю активів, стабільністю грошових потоків і здатністю фінансувати капітальні інвестиції. Важливу роль відіграють цифрові сервіси та ІТ-рішення у процесах обслуговування, маршрутизації та управління операційною діяльністю. Ключовими є показники рентабельності, платоспроможності, ділової активності та інвестицій у необоротні й нематеріальні активи.

Продовження табл. 3.3

1	2	3	4	5
D Постачання електроенергії, газу, пари та кондиціонуван-ня повітря (розділ 35)	ПрАТ «НЕК «Укренерго»; ТОВ «ГК «Нафтогаз України»	2	40	Характеризується високою капіталоємністю, домінуванням необоротних активів у структурі балансу та значною регуляторною залежністю формування тарифів. Економічна безпека визначається здатністю забезпечувати фінансову стійкість, ліквідність і платоспроможність за умов значних інвестиційних потреб і дебіторської заборгованості. Визначальними є показники інвестиційної активності, структури капіталу, грошових потоків і відтворення активів, що опосередковано відображає рівень цифровізації управління інфраструктурними системами.
Разом		5	100	

Примітка. Назви секцій і розділів подано за класифікацією видів економічної діяльності NACE 2.1-UA, затвердженою наказом Держстату від 28.10.2025 № 191, і узгоджено з КВЕД ДК 009:2010 (наказ Держспоживстандарту України від 11.10.2010 № 457 із чинними змінами).

Джерело: узагальнено автором на основі [168, 169].

Аналітична діагностика економічної безпеки підприємств у 2020–2024 рр. базується на результатах розрахунку системи показників економічної безпеки для кожного підприємства вибірки відповідно до методики, обґрунтованої у підрозділі 3.1. Повні розрахункові таблиці показників у розрізі підприємств і років наведено у додатках Е–Л, що забезпечує прозорість емпіричної бази, логічну відтворюваність результатів та чіткий зв'язок між первинними даними і узагальненими аналітичними висновками.

Формування інтегрального індексу економічної безпеки підприємств здійснюється на основі багатофакторного підходу, що передбачає послідовну нормалізацію часткових показників, визначення їх інформаційної вагомості ентропійним методом та агрегування в єдиний композитний індикатор. Вихідною інформаційною базою є 15 показників, систематизованих у п'ять функціональних блоків (фінансова стійкість, ліквідність і платоспроможність, рентабельність, ділова активність, інвестиційно-структурна спроможність), значення яких наведені у додатках Е–Л.

На першому етапі здійснюється ідентифікація типу впливу показників на рівень економічної безпеки. Переважна більшість індикаторів належить до стимуляторів, тобто зростання їх значень позитивно впливає на стан економічної безпеки (коефіцієнт автономії, покриття необоротних активів власним капіталом, показники ліквідності, рентабельності, оборотності, темп оновлення основних засобів, капітальні інвестиції до чистого доходу). До дестимуляторів віднесено коефіцієнт фінансового левериджу, оскільки зростання боргового навантаження підвищує фінансові ризики.

Особливий підхід застосовано до показника частки необоротних активів в активах, який інтерпретується як індикатор оптимального структурного балансу активів. З метою уникнення методичної упередженості щодо капіталомістких галузей його перетворено у показник відхилення від медіанного значення в межах відповідного року. Абсолютне відхилення підприємства від медіани розглядається як дестимулюючий фактор, після чого нормалізація здійснюється за формулою для дестимуляторів. Такий підхід

дозволяє оцінити структурну збалансованість активів, а не механічно заохочувати їх зростання чи скорочення.

На другому етапі виконується нормалізація показників за лінійною процедурою мін–макс. Для показників стимуляторів використовується співвідношення, визначене у формулі 3.1, для дестимуляторів – у формулі 3.2.

Слід зазначити, що показник «частка необоротних активів в активах» (x_{it}^{HA}) має відмінну економічну інтерпретацію порівняно з класичними стимуляторами або дестимуляторами, оскільки як надмірно високе, так і надмірно низьке його значення може погіршувати економічну безпеку підприємства. З одного боку, завищення частки необоротних активів знижує мобільність активів і може формувати ризики ліквідності; з іншого – заниження цієї частки може свідчити про недостатній інфраструктурно-виробничий потенціал і обмеження інвестиційної спроможності, що є критичним для капіталомістких видів діяльності. З огляду на це зазначений індикатор доцільно трактувати як показник типу «оптимум», де економічно безпечнішим є наближення до певного еталонного рівня, а не монотонне зростання чи спадання.

Для формалізації «оптимуму» еталонне значення визначається як медіана розподілу цього показника в межах відповідного року t :

$$x_i^* = Med(x_{1t}^{HA}, x_{2t}^{HA}, \dots, x_{mt}^{HA}), \quad (3.8)$$

де m – кількість підприємств у вибірці у році t .

Далі обчислюється абсолютне відхилення фактичного значення показника від еталонного:

$$d_{it} = |x_{it}^{HA} - x_i^*|. \quad (3.9)$$

У такій постановці d_{it} є дестимулюючою величиною: менше відхилення від медіанного еталона відповідає більш збалансованій структурі активів і, відповідно, вищому рівню економічної безпеки за даним аспектом. Тому нормалізація здійснюється за правилом для дестимуляторів (формула 3.2), але вже для змінної d_{it} :

$$z_{it}^{HA} = \frac{\max(d_t) - d_{it}}{\max(d_t) - \min(d_t)}, \quad (3.10)$$

де $\max(d_t)$ і $\min(d_t)$ – відповідно максимальне і мінімальне значення відхилення d_{it} у вибірці підприємств у році t .

Таким чином, у складі матриці нормалізованих показників для табл. 3.4 використовується не первинне значення частки необоротних активів, а нормалізований показник z_{it}^{HA} , який відображає ступінь наближення до «оптимуму» (медіанного еталона) у межах року. Це забезпечує методичну коректність міжгалузевих зіставлень і унеможливлює систематичне заниження інтегральних оцінок капіталомістких підприємств виключно внаслідок специфіки їхньої структури активів.

Третій етап передбачає визначення ваг показників за ентропійним методом. Ваги розраховуються на основі повної сукупності спостережень за період 2020–2024 рр., що забезпечує часову порівнюваність інтегрального індексу. Використання сталих ваг дозволяє інтерпретувати зміну інтегрального показника як результат трансформації фінансово-економічного стану підприємств, а не як наслідок варіації структури зважування. Обчислення інформаційної ентропії та коефіцієнтів вагомості здійснюється відповідно до формул 3.3 – 3.6.

На завершальному етапі розрахуємо інтегральний індекс економічної безпеки за формулою 3.7. Отримане значення I_{EB} є безрозмірною величиною в інтервалі $[0;1]$, що відображає відносний рівень економічної безпеки підприємства у відповідному році.

На основі первинних показників економічної безпеки підприємств, наведених у додатках Е–Л, виконано перехід від аналізу окремих коефіцієнтів до інтегральної оцінки, що забезпечує коректне міжчасове та міжпідприємницьке порівняння. Для цього кожен із показників приведено до безрозмірної шкали $[0;1]$ методом мін–макс нормалізації: для показників-стимуляторів застосовано перетворення за формулою 3.1, для показників-дестимуляторів – за формулою 3.2, що уніфікує інтерпретацію нормалізованих

значень (зростання завжди відповідає підвищенню рівня безпеки). Далі ваги показників визначено ентропійним методом через обчислення часток (3.3), ентропії (3.4), ступеня варіативності (3.5) та вагових коефіцієнтів (3.6), що мінімізує суб'єктивність процедури зважування. Підсумковий інтегральний індекс економічної безпеки для кожного підприємства та року 2020–2024 рр. отримано агрегуванням нормалізованих показників із відповідними вагами за формулою (3.7).

Відзначимо, що у таблиці 3.4 у графах блоків подано $\Sigma(w \cdot z)$ – суму зважених нормалізованих показників у межах відповідного блоку. Відсотковий внесок блоку визначено як $\Sigma(w \cdot z)_k / I \times 100$. Нормалізацію виконано за формулами для стимуляторів і дестимуляторів; для показника «частка необоротних активів в активах» застосовано підхід «оптимум» через відхилення від медіани року з подальшою нормалізацією як дестимулятора. Ваги показників розраховано ентропійним методом на сукупності 2020–2024 рр. і зафіксовано сталими для забезпечення часової порівнюваності.

Розрахунок інтегрального індексу економічної безпеки підприємств у 2020–2024 рр. засвідчив істотну диференціацію як за рівнем загального показника, так і за структурою його формування. Значення індексу варіюють у межах від 0,233 до 0,639, що свідчить про різну ступінь стійкості досліджуваних підприємств в умовах структурних трансформацій та воєнного шоку 2022 р.

Найвищі значення інтегрального індексу протягом усього періоду демонструє INTERPIPE HOLDINGS PLC (0,582–0,639), що зумовлено стабільно високими внесками блоків ліквідності та рентабельності, які сумарно формують понад 60 % загального індексу. Структура його економічної безпеки є збалансованою та менш чутливою до кризових коливань.

Таблиця 3.4

Інтегральний індекс економічної безпеки підприємств у 2020–2024 рр. та внески функціональних блоків

Підприємство	Рік	Фінансова стійкість	Фінансова стійкість (%)	Ліквідність і платоспроможність	Ліквідність і платоспроможність (%)	Рентабельність	Рентабельність (%)	Ділова активність	Ділова активність (%)	Інвестиційно-структурна спроможність	Інвестиційно-структурна спроможність (%)	ІЕБ
1	2	3	4	5	6	7	8	9	10	11	12	13
INTERPIPE HOLDINGS PLC	2020	0.09	15.0	0.219	36.4	0.152	25.4	0.033	5.5	0.106	17.7	0.6
	2021	0.09	15.2	0.219	37.1	0.152	25.9	0.013	2.2	0.115	19.6	0.589
	2022	0.102	17.5	0.219	37.6	0.152	26.2	0.044	7.6	0.065	11.2	0.582
	2023	0.106	16.6	0.219	34.2	0.152	23.8	0.038	5.9	0.124	19.4	0.639
	2024	0.112	18.7	0.219	36.6	0.152	25.5	0.033	5.5	0.082	13.7	0.598
АТ «Українська залізниця»	2020	0.097	22.6	0.02	4.7	0.102	23.8	0.131	30.3	0.08	18.6	0.431
	2021	0.107	24.7	0.0	0.0	0.132	30.5	0.131	30.4	0.062	14.4	0.432
	2022	0.115	23.6	0.082	16.9	0.093	19.1	0.132	27.1	0.065	13.3	0.486
	2023	0.112	21.3	0.131	24.9	0.067	12.8	0.132	25.0	0.084	16.0	0.527
	2024	0.115	23.8	0.099	20.5	0.068	14.2	0.135	27.9	0.065	13.5	0.482
АТ «Укрпошта»	2020	0.062	14.1	0.107	24.1	0.114	25.7	0.06	13.5	0.1	22.6	0.443
	2021	0.081	16.2	0.07	13.9	0.133	26.6	0.054	10.8	0.163	32.6	0.501
	2022	0.097	21.1	0.057	12.4	0.079	17.1	0.131	28.5	0.096	20.9	0.459
	2023	0.066	18.6	0.049	13.7	0.003	0.9	0.086	24.1	0.151	42.6	0.355
	2024	0.064	18.8	0.051	14.8	0.028	8.2	0.088	25.7	0.111	32.5	0.342
ПрАТ «НЕК «Укренерго»	2020	0.036	15.2	0.014	5.9	0.003	1.4	0.099	42.7	0.081	34.7	0.233
	2021	0.059	13.5	0.057	13.1	0.132	30.0	0.116	26.5	0.074	16.9	0.439
	2022	0.065	17.8	0.052	14.2	0.055	15.2	0.123	34.0	0.068	18.8	0.364
	2023	0.098	22.1	0.076	16.9	0.074	16.5	0.06	13.5	0.138	31.0	0.446
	2024	0.088	28.3	0.0	0.0	0.012	3.7	0.106	34.1	0.105	33.9	0.31
ТОВ «ГПК «Нафтогаз України»	2020	0.037	7.9	0.118	25.1	0.059	12.5	0.183	38.8	0.074	15.7	0.471
	2021	0.036	14.8	0.037	15.0	0.0	0.0	0.113	46.0	0.06	24.2	0.246
	2022	0.036	11.6	0.0	0.0	0.02	6.4	0.184	58.6	0.074	23.4	0.315
	2023	0.036	14.1	0.0	0.0	0.037	14.2	0.185	71.7	0.0	0.0	0.258
	2024	0.036	9.1	0.031	7.7	0.077	19.1	0.183	45.6	0.074	18.5	0.4

Джерело: розраховано автором за Додатками Е–Л.

АТ «Українська залізниця» характеризується середнім рівнем інтегрального індексу (0,431–0,527) із поступовим зростанням у 2022–2023 рр. Основний внесок формують блоки ділової активності та фінансової стійкості, тоді як ліквідність має нерівномірну динаміку. Це свідчить про структурну адаптацію підприємства до зовнішніх шоків.

АТ «Укрпошта» демонструє більш виражену волатильність (0,342–0,501), причому у 2023–2024 рр. спостерігається зміщення структури індексу в бік інвестиційно-структурної складової. Така трансформація структури внесків відображає перерозподіл ресурсів у напрямі модернізації активів.

ПрАТ «НЕК «Укренерго»» має найнижче значення інтегрального індексу у 2020 р. (0,233), однак у подальшому спостерігається зростання до 0,446 у 2023 р., що пояснюється посиленням ролі блоку фінансової стійкості та інвестиційної спроможності. Структура індексу залишається чутливою до змін ліквідності.

ТОВ «ГПК «Нафтогаз України»» характеризується значною структурною асиметрією: понад 40–70 % індексу формує блок ділової активності, що свідчить про високу концентрацію впливу одного функціонального сегмента та потенційну вразливість моделі економічної безпеки.

Таким чином, інтегральний підхід дозволив не лише ранжувати підприємства за рівнем економічної безпеки, а й виявити структурні драйвери та зони ризику, які залишаються невидимими при аналізі окремих коефіцієнтів.

На рис. 3.1 відображено динаміку інтегрального індексу економічної безпеки досліджуваних підприємств у 2020–2024 рр., що дозволяє простежити міжсуб'єктні відмінності та зміни рівня їхньої фінансово-економічної стійкості в умовах трансформаційних та кризових процесів.

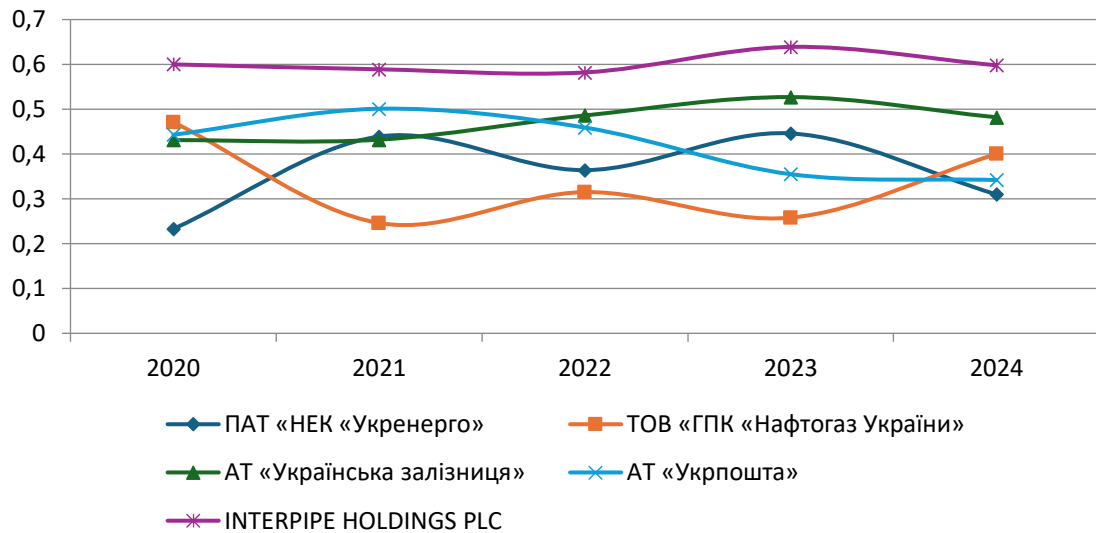


Рис. 3.1. Динаміка інтегрального індексу економічної безпеки досліджуваних підприємств у 2020–2024 рр.

Джерело: сформовано автором.

На рис. 3.2 відображено структурний розподіл середнього внеску функціональних блоків у формування інтегрального індексу економічної безпеки за 2020–2024 рр., що дозволяє виявити домінуючі складові економічної стійкості кожного підприємства та оцінити специфіку їхньої внутрішньої структурної збалансованості.

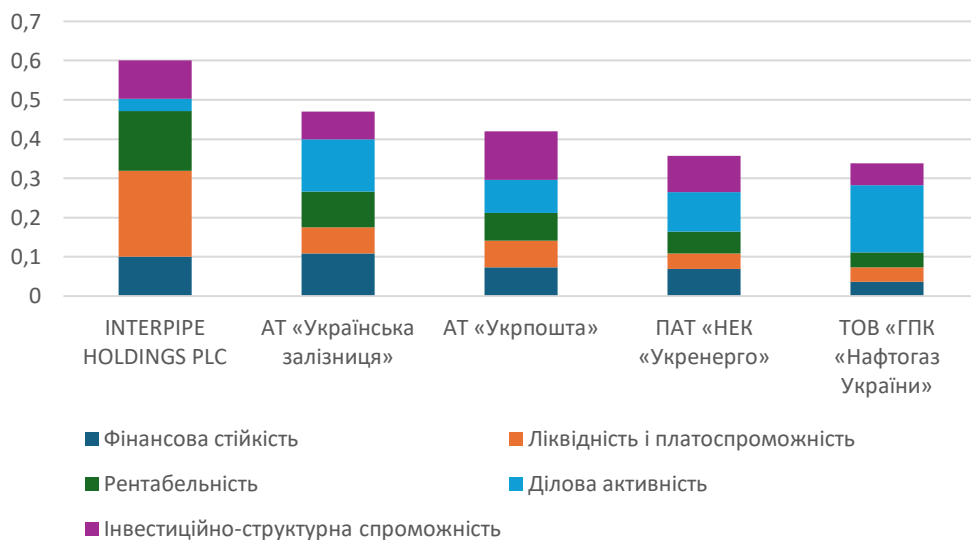


Рис. 3.2. Середній внесок функціональних блоків у формування інтегрального індексу економічної безпеки досліджуваних підприємств у 2020–2024 рр.

Джерело: сформовано автором.

Побудова табл. 3.5 зумовлена необхідністю переходу від індивідуальної траєкторної оцінки підприємств до статистичної характеристики розподілу інтегрального індексу економічної безпеки у часовому розрізі. Якщо табл. 3.4 відображає рівень та структуру індексу на мікрорівні, то табл. 3.5 дозволяє оцінити ступінь міжсуб'єктної диференціації, варіативність та однорідність вибірки підприємств у кожному році досліджуваного періоду.

Для оцінювання ступеня варіативності інтегрального індексу економічної безпеки підприємств у часовому розрізі поряд із середнім значенням та стандартним відхиленням доцільно застосувати коефіцієнт варіації як відносну міру розсіювання. На відміну від стандартного відхилення, коефіцієнт варіації дозволяє зіставляти неоднорідність показників за різні роки, оскільки нормує абсолютне відхилення відносно середнього рівня індексу.

Коефіцієнт варіації інтегрального індексу економічної безпеки за t -й рік визначається за формулою:

$$CV_t = \frac{\sigma_t}{\bar{I}_t} \times 100\%, \quad (3.11)$$

де CV_t – коефіцієнт варіації інтегрального індексу у t -му році, %;

σ_t – стандартне відхилення значень інтегрального індексу економічної безпеки підприємств у t -му році;

$\bar{I}_t$ – середнє значення інтегрального індексу економічної безпеки у t -му році.

Застосування середнього значення, медіани, стандартного відхилення, коефіцієнта варіації (формула 3.11), а також квартильних характеристик і міжквартильного розмаху ($IQR = Q3 - Q1$) забезпечує комплексну діагностику не лише центральної тенденції, а й розсіювання та структурних зсувів у розподілі індексу. Такий підхід дозволяє виявити приховані зміни у внутрішній конфігурації економічної безпеки підприємств, які не завжди проявляються через динаміку середніх значень, та сформулювати обґрунтовані висновки щодо стабільності, асиметрії та інтенсивності міжгалузевої диференціації у 2020–2024 рр.

Таблиця 3.5

**Описова статистика інтегрального індексу економічної безпеки
підприємств у 2020–2024 рр.**

Показник	2020	2021	2022	2023	2024
Середнє значення	0,436	0,441	0,441	0,445	0,426
Медіана	0,443	0,439	0,459	0,446	0,400
Стандартне відхилення	0,132	0,126	0,105	0,148	0,116
Коефіцієнт варіації $CV_t, \%$	30,24	28,57	23,78	33,22	27,23
Мінімум	0,233	0,246	0,315	0,258	0,310
Максимум	0,600	0,589	0,582	0,639	0,598
Q1	0,431	0,432	0,364	0,355	0,342
Q3	0,471	0,501	0,486	0,527	0,482
IQR = Q3 – Q1	0,040	0,069	0,122	0,172	0,140

Джерело: розраховано автором за даними таблиці 3.4.

Побудова відповідної графічної інтерпретації дозволяє не лише ідентифікувати часові інтервали з підвищеним рівнем структурної нестабільності, а й простежити характер еволюції внутрішньої конфігурації вибірки у динаміці, зокрема зміну ступеня її однорідності та перерозподіл позицій між суб'єктами господарювання.

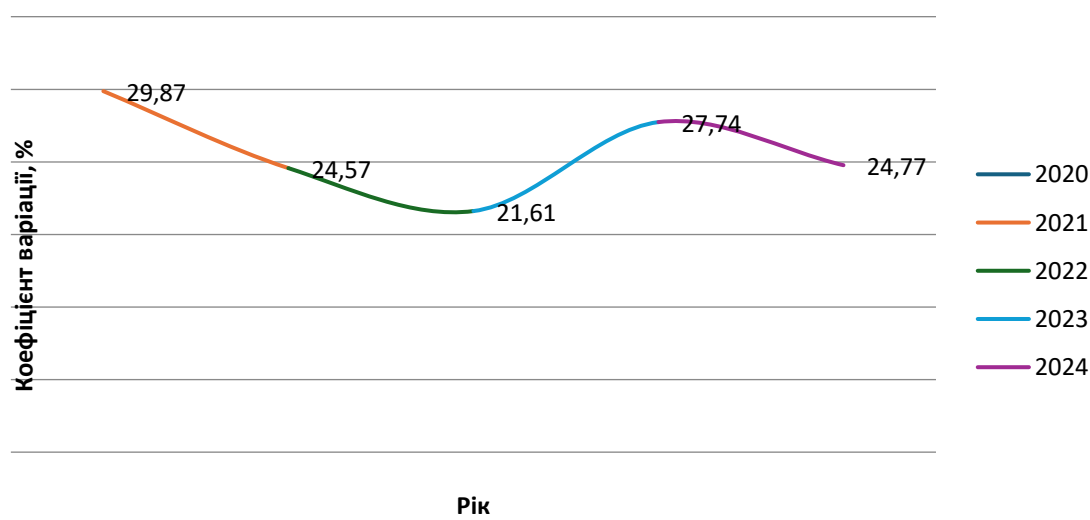


**Рис. 3.3. Динаміка коефіцієнта варіації інтегрального індексу економічної
безпеки підприємств у 2020–2024 рр.**

Джерело: сформовано автором.

Аналіз описових статистичних характеристик, наведених у табл. 3.5, дозволяє перейти від індивідуальної оцінки підприємств до узагальненої інтерпретації міжсуб'єктної диференціації економічної безпеки у 2020–2024 рр.

По-перше, середні значення інтегрального індексу демонструють відносну стабільність вибірки впродовж досліджуваного періоду: коливання перебувають у межах 0,426–0,445. Максимальне середнє значення зафіксовано у 2023 р. (0,445), що свідчить про певне загальне покращення рівня економічної безпеки сукупності підприємств у цей рік. Водночас зниження середнього у 2024 р. до 0,426 відображає послаблення узагальненого рівня безпеки або посилення асиметрії розподілу.

По-друге, порівняння середнього значення та медіани дає змогу оцінити характер розподілу. У 2020–2022 рр. медіана або перевищує середнє, або є близькою до нього, що вказує на відсутність суттєвого перекосу розподілу. Натомість у 2024 р. медіана (0,400) є нижчою за середнє (0,426), що свідчить про наявність одного чи кількох підприємств із відносно високими значеннями індексу, які підвищують середнє арифметичне. Це є ознакою посилення нерівномірності у розподілі рівнів економічної безпеки.

По-третє, стандартне відхилення та коефіцієнт варіації дозволяють оцінити ступінь міжпідприємницької неоднорідності. Найменший рівень варіативності зафіксовано у 2022 р. ($\sigma = 0,105$; $CV = 23,78\%$), що свідчить про відносну консолідацію підприємств за рівнем економічної безпеки. Натомість у 2023 р. коефіцієнт варіації зростає до 33,22 %, що означає суттєве посилення диференціації. Таким чином, 2023 р. характеризується не лише зростанням середнього значення індексу, а й одночасним розширенням розривів між підприємствами.

По-четверте, аналіз екстремальних значень показує, що максимальні рівні інтегрального індексу залишаються відносно стабільними у межах 0,582–0,639, тоді як мінімальні значення змінюються більш істотно, що зумовлює коливання амплітуди розмаху. Зокрема, у 2023 р. спостерігається поєднання високого

максимуму (0,639) та низького мінімуму (0,258), що підтверджує зростання поляризації.

По-п'яте, міжквартильний розмах (IQR) як робастна міра варіації демонструє тенденцію до розширення у 2022–2024 рр. (0,122; 0,172; 0,140 відповідно), що свідчить про зростання розриву між нижнім і верхнім квартилями навіть за відносної стабільності середніх значень. Найбільше значення IQR у 2023 р. підтверджує, що саме цей рік характеризувався найбільшою внутрішньою диференціацією досліджуваних підприємств.

Поглиблений аналіз описової статистики інтегрального індексу економічної безпеки підприємств у 2020–2024 рр. дозволяє здійснити кількісну верифікацію гіпотези щодо наявності структурного зламу траєкторії розвитку системи у 2022 році.

Динаміка коефіцієнта варіації засвідчує зміну характеру міжпідприємницької диференціації. У 2020–2021 рр. його значення становили відповідно 30,24 % та 28,57 %, що характеризує відносно стабільний, хоча й високий рівень неоднорідності вибірки. У 2022 р. коефіцієнт варіації знижується до 23,78 %, що формально може інтерпретуватися як зменшення розсіювання. Однак ізольований розгляд цього показника не відображає повною мірою трансформацію структури розподілу.

Більш репрезентативним у даному випадку є аналіз робастної міри варіації – міжквартильного розмаху. Значення IQR зростає з 0,040 у 2020 р. та 0,069 у 2021 р. до 0,122 у 2022 р., а у 2023 р. – до 0,172. Це свідчить про істотне розширення центрального інтервалу розподілу, тобто про зростання розриву між нижнім та верхнім квартилями. Таким чином, навіть за зниження коефіцієнта варіації у 2022 р. фіксується посилення внутрішньої диференціації основної маси підприємств.

Поєднання цих двох тенденцій дає підстави констатувати зміну форми розподілу інтегрального індексу. Зниження коефіцієнта варіації у 2022 р. може бути пов'язане із відносним скороченням екстремальних відхилень, тоді як зростання IQR відображає перерозподіл значень у центральному сегменті. У

2023 р. обидва показники – коефіцієнт варіації (33,22 %) та міжквартильний розмах (0,172) – досягають максимальних значень за досліджуваний період, що свідчить про завершення фази структурного розриву та формування нової конфігурації міжпідприємницької диференціації.

Додаткове підтвердження трансформаційних процесів простежується у динаміці мінімальних та медіанних значень. Підвищення мінімального значення індексу до 0,315 у 2022 р. порівняно з 0,246 у 2021 р. свідчить про вихід частини підприємств із зони критично низької безпеки або про адаптацію до нових умов функціонування. Водночас зростання медіани до 0,459 у 2022 р. відображає зміщення центру розподілу та концентрацію значень у середньому сегменті.

Отже, 2022 рік характеризується не стільки одномірною динамікою інтегрального індексу, скільки якісною перебудовою структури його розподілу. Відбувається:

- трансформація форми розподілу;
- перерозподіл значень у межах центрального сегмента;
- зміна конфігурації міжгалузевої та міжпідприємницької диференціації.

У 2023–2024 рр. система переходить у фазу адаптивної стабілізації. Хоча у 2024 р. коефіцієнт варіації знижується до 27,23 %, міжквартильний розмах залишається істотно вищим за докризовий рівень (0,140 проти 0,040 у 2020 р.), що свідчить про незворотність структурних змін. Таким чином, відбувається не повернення до попередньої траєкторії, а формування нової рівноважної конфігурації системи економічної безпеки.

З урахуванням наведених статистичних аргументів 2022 рік доцільно інтерпретувати як структурний злам траєкторії. Саме в цей період відбулося переформатування внутрішньої архітектури розподілу ризиків і рівнів стійкості підприємств, що означає перехід від інерційної моделі функціонування до адаптивної моделі, сформованої в умовах масштабного воєнного шоку.

Таким чином, статистичний аналіз підтверджує необхідність подальшого міжгалузевого порівняння та типологізації підприємств за рівнем економічної

безпеки, що дозволить перейти від констатації варіативності до виявлення системних чинників структурної поляризації.

Для поглиблення інтерпретації результатів табл. 3.5 та візуалізації змін центральної тенденції, міжквартильного розмаху і наявності потенційних викидів інтегрального індексу економічної безпеки у часовому розрізі побудовано рис. 3.4.

Візуалізація розподілу інтегрального індексу економічної безпеки за допомогою діаграми розмаху дозволяє простежити динаміку центральної тенденції та ступінь варіативності показників у розрізі років. Графічний аналіз підтверджує результати описової статистики та виявляє суттєві відмінності у структурі розподілу значень.

По-перше, у 2020–2021 рр. спостерігається відносно стабільний розподіл із помірним міжквартильним розмахом та близьким положенням медіани, що свідчить про порівняно однорідний рівень економічної безпеки досліджуваних підприємств.

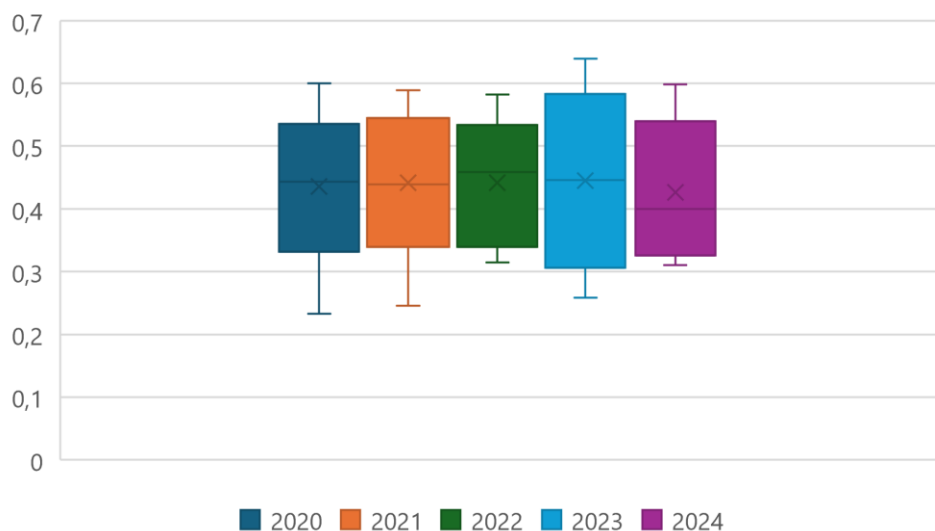


Рис. 3.4. Розподіл інтегрального індексу економічної безпеки підприємств у 2020–2024 рр.

Джерело: сформовано автором.

По-друге, у 2022 р. фіксується певне звуження розподілу та зниження верхніх значень, що може інтерпретуватися як вирівнювання позицій

підприємств в умовах кризового шоку та адаптаційних процесів, пов'язаних із зовнішніми дестабілізаційними чинниками.

По-третє, 2023 р. характеризується найбільшим міжквартильним розмахом, що свідчить про зростання диференціації підприємств за рівнем економічної безпеки. Саме у цей період спостерігається максимальний розрив між нижнім та верхнім квартилями, що може розглядатися як прояв структурного зламу та посилення галузевої асиметрії.

У 2024 р. відзначається часткове зниження медіанного значення індексу та певне скорочення варіативності порівняно з 2023 р., що може свідчити про поступову стабілізацію системи, однак без повного повернення до докризових параметрів однорідності.

Таким чином, графічний аналіз підтверджує наявність структурних трансформацій у динаміці економічної безпеки підприємств у 2022–2023 рр., а також демонструє посилення міжгалузевої диференціації в умовах турбулентного середовища функціонування.

Проведений аналіз середніх значень інтегрального індексу економічної безпеки, а також варіаційних характеристик його розподілу у 2020–2024 рр. дозволив встановити загальні тенденції зміни рівня безпеки та зафіксувати зростання міжсуб'єктної диференціації в кризовий період. Водночас зазначені результати відображають переважно агреговану картину та не дають змоги повною мірою оцінити внутрішню трансформацію структури вибірки.

З огляду на це, для поглиблення інтерпретації виявлених змін доцільним є перехід від аналізу абсолютних значень до позиційного аналізу, що передбачає ранжування підприємств за величиною інтегрального індексу економічної безпеки в кожному році досліджуваного періоду. Такий підхід дозволяє виявити не лише зміну середнього рівня, а й характер перерозподілу позицій у системі, тобто зміну ієрархічної конфігурації економічної безпеки.

Застосування рангового аналізу забезпечує можливість:

- оцінити трансформацію ієрархії рівнів економічної безпеки підприємств;

- ідентифікувати суб'єкти господарювання зі стабільною позиційною траєкторією;
- зафіксувати глибину структурного перерозподілу в умовах кризового шоку 2022 р.;
- простежити характер та асиметрію післяшочкового відновлення у 2023–2024 рр.

На відміну від описової статистики, яка фіксує зміну рівня показника, ранговий підхід дозволяє дослідити зміну структури системи економічної безпеки та виявити наявність або відсутність структурного зламу. Саме тому подальший аналіз здійснюється через визначення рейтингових позицій підприємств у межах вибірки (табл. 3.6).

Таблиця 3.6

Рейтингова позиція підприємств за інтегральним індексом економічної безпеки у 2020–2024 рр.

Підприємство	2020	2021	2022	2023	2024	Δ 2020–2024
INTERPIPE HOLDINGS PLC	1	1	1	1	1	0
АТ «Укрзалізниця»	4	4	2	2	2	+2
АТ «Укрпошта»	3	2	3	4	4	–1
ПрАТ «НЕК «Укренерго»	5	3	4	3	5	0
ТОВ «ГПК «Нафтогаз України»	2	5	5	5	3	–1

Примітка: Δ – зміна рангу (покращення – зі знаком «+»).

Джерело: розраховано автором за даними таблиці 3.4.

Результати рангового аналізу інтегрального індексу економічної безпеки підприємств у 2020–2024 рр. дозволяють зробити низку узагальнюючих висновків щодо трансформації ієрархічної структури вибірки та характеру адаптаційних процесів у кризовий і післякризовий періоди.

По-перше, абсолютну позиційну стабільність протягом усього досліджуваного періоду демонструє INTERPIPE HOLDINGS PLC, яке посідало перше місце у всі роки аналізу. Така динаміка свідчить про системну збалансованість функціональних блоків економічної безпеки, відсутність критичних структурних диспропорцій та наявність достатнього адаптаційного потенціалу до зовнішніх шоків. Стабільність лідерської позиції в умовах

кризового 2022 року підтверджує високий рівень внутрішньої стійкості підприємства.

По-друге, найбільш помітне покращення позиції у довгостроковому розрізі продемонструвало АТ «Укрзалізниця». Після четвертого місця у 2020–2021 рр. підприємство піднялося на друге місце у 2022 р. та утримувало його у 2023–2024 рр. Зміна рангу на дві позиції вгору свідчить про відносну ефективність адаптаційних механізмів у період структурного шоку та про підвищення збалансованості функціональних компонентів економічної безпеки.

По-третє, АТ «Укрпошта» характеризується помірною негативною позиційною динамікою. Незважаючи на відносно високі місця у 2020–2021 рр., у післяшоківий період відбулося погіршення рангової позиції, що може бути інтерпретовано як наслідок меншої гнучкості системи управління або вищої чутливості до змін зовнішнього середовища. Загальна втрата однієї позиції у 2020–2024 рр. відображає поступове ослаблення конкурентних переваг у структурі вибірки.

По-четверте, ПрАТ «НЕК «Укренерго» демонструє нестійку позиційну траєкторію з коливаннями рангу у межах періоду. Така динаміка свідчить про асиметричний характер адаптації та залежність інтегрального індексу від окремих функціональних блоків, чутливих до кризових факторів. Відсутність стабільної позиції у структурі вибірки підтверджує наявність внутрішніх дисбалансів у системі економічної безпеки.

По-п'яте, ТОВ «ГПК «Нафтогаз України» зазнало найглибшого позиційного спаду у 2021–2023 рр., опустившись до п'ятого місця, з подальшим частковим відновленням у 2024 р. Така динаміка свідчить про високу вразливість до кризових шоків та структурну нестійкість окремих функціональних компонентів економічної безпеки. Часткове підвищення позиції у 2024 р. можна трактувати як ознаку початку стабілізаційних процесів, проте воно не компенсує глибини попереднього падіння.

Узагальнюючи результати таблиці 3.6, слід констатувати, що 2022 рік став точкою переформатування рангової структури підприємств. Відбулося не лише

зниження абсолютних значень інтегрального індексу, але й трансформація ієрархії суб'єктів господарювання, що підтверджує структурний характер кризового впливу. Подальша динаміка 2023–2024 рр. засвідчує формування нової конфігурації системи економічної безпеки, яка не є ідентичною докризовій та відображає різний рівень адаптаційної спроможності підприємств.

Для поглиблення інтерпретації структурних змін, зафіксованих через динаміку коефіцієнта варіації інтегрального індексу економічної безпеки, доцільним є перехід від макрорівневої оцінки міжпідприємницької диференціації до мікроструктурного аналізу стабільності кожного суб'єкта господарювання.

Якщо коефіцієнт варіації характеризує ступінь неоднорідності системи в цілому, то для оцінки індивідуальної стійкості підприємства використовується показник амплітуди коливань інтегрального індексу за досліджуваний період:

$$A_i = \max(I_{i,t}) - \min(I_{i,t}), \quad (3.12)$$

де A_i – амплітуда зміни інтегрального індексу економічної безпеки i -го підприємства у 2020–2024 рр.;

$I_{i,t}$ – значення інтегрального індексу економічної безпеки i -го підприємства у році t .

Застосування амплітуди дозволяє оцінити внутрішню волатильність траєкторії розвитку підприємства, незалежно від його позиції у вибірці. Поєднання цього показника із середнім значенням інтегрального індексу формує двовимірну модель оцінювання, яка відображає не лише рівень безпеки, але й характер її динаміки.

Таким чином, якщо коефіцієнт варіації (рис. 3.3) фіксує зміну структурної неоднорідності системи в цілому, то матриця позиціонування (рис. 3.5) конкретизує, за рахунок яких саме підприємств формується ця неоднорідність та яким є тип їх адаптаційної поведінки.

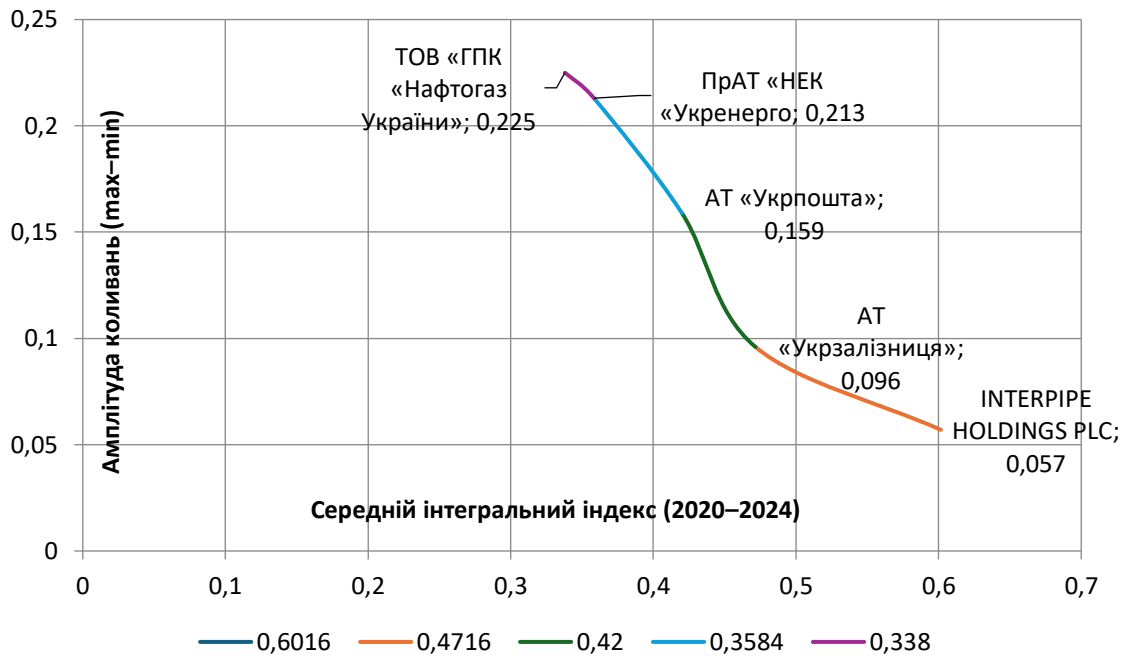


Рис. 3.5. Матриця позиціонування підприємств за середнім рівнем та волатильністю інтегрального індексу економічної безпеки у 2020–2024 рр.

Джерело: сформовано автором за розрахунками, представленими у Додатку М.

Отримана матриця дозволяє виокремити декілька типів поведінкових моделей підприємств у контексті економічної безпеки.

INTERPIPE HOLDINGS PLC характеризується поєднанням високого середнього значення інтегрального індексу та відносно помірної амплітуди коливань, що свідчить про стратегічну збалансованість та системну стійкість моделі розвитку. Таке позиціонування підтверджує його стабільне лідерство у ранговій структурі вибірки.

АТ «Українська залізниця» демонструє середній рівень інтегрального показника за наявності відносно підвищеної волатильності, що відображає активну адаптаційну реакцію на кризові умови 2022 р. та поступову стабілізацію у післяшоковий період. Її позиція свідчить про трансформаційний характер внутрішніх процесів, зумовлений структурними змінами у функціональних блоках.

АТ «Укрпошта» та ПрАТ «НЕК «Укренерго» перебувають у зоні поєднання нижчих середніх значень інтегрального індексу з помітною амплітудою коливань, що може інтерпретуватися як підвищена чутливість до зовнішніх шоків і нестійкість окремих компонентів системи економічної безпеки.

ТОВ «ГПК «Нафтогаз України» характеризується значною амплітудою зміни інтегрального індексу при відносно нижчому середньому рівні, що свідчить про структурну вразливість і нестабільність фінансово-економічної конфігурації у досліджуваний період.

Порівняльний аналіз динаміки коефіцієнта варіації та матриці позиціонування дозволяє зробити узагальнюючий висновок про структурну трансформацію системи економічної безпеки у 2022 році.

Зростання міжпідприємницької диференціації у післяшоківий період супроводжується розшаруванням вибірки на три групи:

1. Першу групу формують стратегічно стійкі підприємства, для яких характерне поєднання відносно високого середнього значення інтегрального індексу економічної безпеки за 2020–2024 рр. та помірної амплітуди його міжрічних коливань. До цієї категорії належать INTERPIPE HOLDINGS PLC (0,602; 0,057) та АТ «Українська залізниця» (0,472; 0,096). Їх позиціонування у правій частині матриці за відносно низького рівня волатильності свідчить про сформований запас фінансово-структурної стійкості, відсутність різких провалів у кризові періоди та здатність підтримувати збалансований безпековий профіль навіть за умов макроекономічної турбулентності. У контексті міжгалузевого порівняння це означає наявність внутрішніх компенсаторних механізмів, які мінімізують вплив зовнішніх шоків на інтегральний результат.

2. Другу групу становлять підприємства адаптивно-волатильного типу, для яких характерним є середній або помірно знижений рівень інтегрального індексу у поєднанні з підвищеною амплітудою його коливань. До цієї категорії віднесено ПрАТ «НЕК «Укренерго» (0,358; 0,213) та ТОВ «ГПК «Нафтогаз України» (0,338; 0,225). Їх положення у верхній частині матриці відображає значну варіативність динаміки безпекових параметрів, що проявляється у різких міжрічних змінах та

високій чутливості до регуляторних, фінансових і макроекономічних факторів. Така конфігурація свідчить про наявність потенціалу до відновлення, проте одночасно фіксує нестійкість безпекового профілю та відсутність стабільної траєкторії розвитку.

3. Третю групу репрезентують структурно вразливі підприємства, для яких характерне поєднання помірного середнього значення інтегрального індексу з тенденцією до зниження показників у завершальні роки досліджуваного періоду. До цієї категорії належить АТ «Укрпошта» (0,420; 0,159). Незважаючи на те, що амплітуда коливань не є максимальною у вибірці, конфігурація її динаміки вказує на поступове послаблення безпекових позицій та формування ризикової траєкторії розвитку. У межах матричного позиціонування це відображає підвищену ймовірність переходу до менш стійкого квадранта за відсутності цілеспрямованих управлінських заходів щодо посилення фінансової та структурної стабільності.

Це свідчить про те, що кризовий шок 2022 року спричинив не лише короткострокове зниження показників, а й формування нової конфігурації системи економічної безпеки, в якій визначальним чинником стає не стільки рівень інтегрального індексу, скільки здатність підприємства підтримувати його стабільність у часі.

Побудована матриця позиціонування підприємств за середнім рівнем та волатильністю інтегрального індексу економічної безпеки (рис. 3.5) дозволила ідентифікувати типологічні групи суб'єктів господарювання за параметрами стійкості та стабільності їх функціонування у 2020–2024 рр. Водночас зазначений інструмент відображає узагальнену інтегральну характеристику без деталізації внутрішньої структури показника. З огляду на це постає необхідність поглиблення аналізу шляхом декомпозиції інтегрального індексу на складові функціональні блоки з метою виявлення структурних дисбалансів та зміни конфігурації економічної безпеки в умовах системного шоку 2022 р.

Саме тому наступним етапом аналітичної діагностики є побудова радар-діаграми, що відображає структурну конфігурацію функціональних компонентів економічної безпеки підприємств у динаміці 2021–2022 рр. (рис. 3.6).

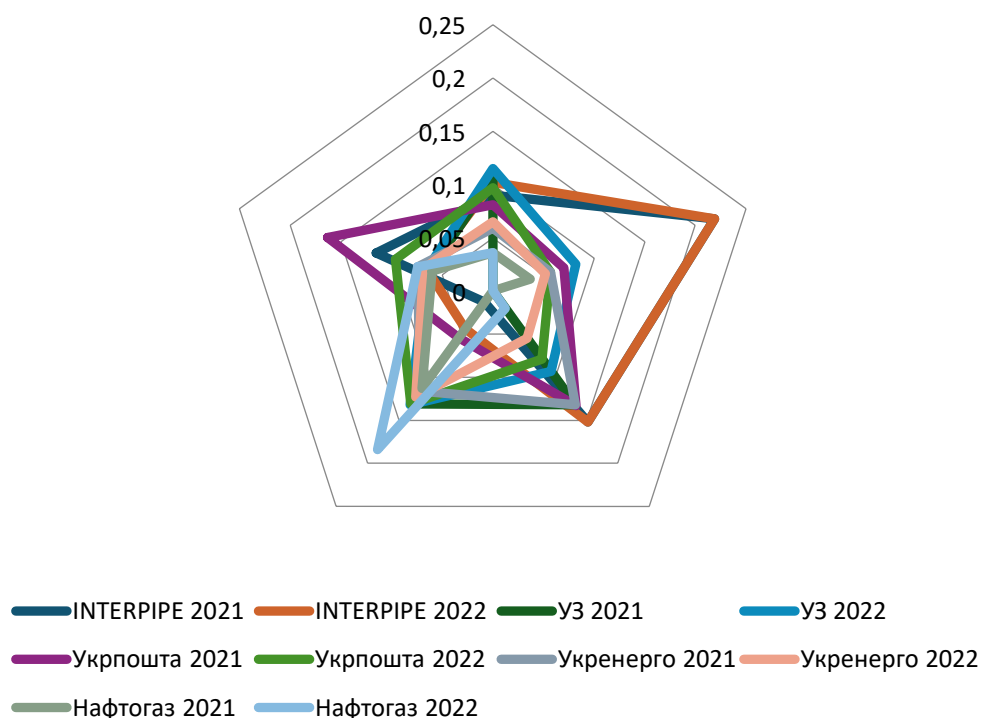


Рис. 3.6 Структурна конфігурація функціональних компонентів економічної безпеки підприємств у період системного шоку 2022 р.

Джерело: сформовано автором за даними, представленими у Додатку М.

Радар-діаграма демонструє, що реакція підприємств на системний шок 2022 р. була неоднорідною як за глибиною змін, так і за структурною спрямованістю трансформацій. Для підприємств із відносно високим середнім рівнем інтегрального індексу характерним є збереження збалансованої конфігурації фінансової стійкості та ліквідності за одночасної варіативності інвестиційно-структурного компонента. Натомість для суб'єктів із підвищеною волатильністю інтегрального індексу простежується асиметричність профілю, що проявляється у концентрації значень окремих блоків за одночасного просідання інших, насамперед рентабельності або ліквідності.

Отже, структурний аналіз підтверджує, що зміни інтегрального індексу у 2022 р. були зумовлені не лише загальним погіршенням макроекономічного середовища, а й внутрішніми дисбалансами у функціональних компонентах

економічної безпеки. Таким чином, поєднання матричного підходу (рис. 3.5) та структурної радар-діагностики (рис. 3.6) забезпечує комплексне міжгалузеве порівняння підприємств і дозволяє перейти від агрегованої оцінки до ідентифікації джерел стійкості або вразливості в межах окремих функціональних блоків.

За результатами аналітичної діагностики економічної безпеки підприємств на основі інтегрального індексу та декомпозиції на функціональні блоки встановлено наявність суттєвої міжсуб'єктної диференціації рівнів економічної безпеки у 2020–2024 рр., а також відмінностей у структурі формування інтегрального результату. Діапазон значень індексу свідчить, що підприємства відрізняються не лише загальним рівнем стійкості, а й конфігурацією ключових драйверів безпекового профілю (ліквідність і платоспроможність, рентабельність, ділова активність, фінансова стійкість, інвестиційно-структурна спроможність).

Агрегований аналіз розподілу індексу (середні значення, медіана, стандартне відхилення, коефіцієнт варіації, квартильні характеристики та IQR) засвідчив, що кризовий шок 2022 року супроводжувався якісною перебудовою структури розподілу і подальшим зростанням диференціації у 2023 році. Поєднання CV та IQR дозволило інтерпретувати ці трансформації не як чисто «середньорічні» коливання, а як зміну форми розподілу та поляризацію позицій підприємств.

Позиційний (ранговий) аналіз підтвердив переформатування ієрархії підприємств у 2022 році та різну швидкість і характер післяшовкової адаптації у 2023–2024 рр. Для поглиблення інтерпретації змін запропоновано двовимірну типологізацію підприємств за середнім рівнем інтегрального індексу та волатильністю його траєкторії (амплітуда), що дозволило виокремити стратегічно стійкі, адаптивно-волатильні та структурно вразливі типи безпекової поведінки. Декомпозиція інтегрального індексу на функціональні блоки на шоківому зрізі 2022 року продемонструвала, що погіршення/поліпшення інтегрального результату зумовлюється не лише зовнішніми умовами, а й

внутрішніми дисбалансами між блоками, що потребує адресних управлінських рішень.

Отримані у підрозділі результати підтверджують, що інтегральний рівень економічної безпеки має не лише часову динаміку, а й структурну неоднорідність, яка посилюється у кризові періоди та проявляється у зміні конфігурації функціональних блоків. Водночас описові та позиційні методи діагностики фіксують наслідки змін, але не дають формалізованої відповіді на питання про силу та статистичну значущість впливу окремих чинників на інтегральний індекс, а також про його прогностичну траєкторію за різних сценаріїв. З огляду на це подальший етап дослідження доцільно спрямувати на економетричне моделювання інтегрального індексу економічної безпеки, що дозволить кількісно ідентифікувати детермінанти динаміки, перевірити гіпотези щодо структурного перелому та здійснити прогнозування рівня економічної безпеки підприємств у середньостроковій перспективі.

3.3. Економетричне моделювання, прогнозування та сценарний аналіз інтегрального рівня економічної безпеки підприємств

Поглиблення аналітичної діагностики економічної безпеки підприємств закономірно передбачає перехід від інтегрально-описового етапу дослідження до етапу економетричного пояснення виявлених змін. Якщо у підрозділах 3.1–3.2 було сформовано систему показників, здійснено їх нормалізацію, зважування та агрегування в інтегральний індекс, а також виявлено міжчасову і міжоб'єктну диференціацію рівня економічної безпеки, то наступним логічним кроком є ідентифікація тих детермінант, які статистично пояснюють варіацію інтегрального індексу в розрізі підприємств і років. Такий перехід є методично виправданим, оскільки інтегральна оцінка фіксує результат дії сукупності чинників, однак сама по собі не дозволяє встановити силу, напрям і статистичну значущість впливу окремих параметрів фінансового стану, ділової активності чи інвестиційно-структурних змін на узагальнений рівень економічної безпеки.

У сучасній економетричній літературі панельні дані трактуються як поєднання просторового та часового вимірів, тобто повторні спостереження за одними й тими самими об'єктами протягом кількох періодів, що дозволяє враховувати відмінності між об'єктами дослідження та їх зміну в часі [173; 174]. Саме ця властивість забезпечує дві принципові переваги. По-перше, панельна модель дає змогу врахувати індивідуальну неоднорідність об'єктів, яка не спостерігається безпосередньо, але впливає на рівень результативної ознаки. По-друге, вона дозволяє дослідити динаміку змін у часі та відокремити сталі структурні характеристики підприємства від впливу спільних для всіх об'єктів часових шоків. У класичних працях з економетрики панельні моделі розглядаються як інструмент, що дозволяє одночасно враховувати відмінності між об'єктами та їх зміну в часі, що є особливо важливим для досліджень фірм, галузей, регіонів чи країн.

У контексті цього дослідження застосування панельного підходу є методично доцільним з кількох причин. По-перше, вибірка охоплює кілька підприємств, що істотно різняться за галузевою належністю, структурою активів, джерелами фінансування, інтенсивністю капіталовкладень, масштабом діяльності та ступенем включення в цифрову трансформацію. Навіть за однакових значень окремих фінансових коефіцієнтів такі підприємства не є тотожними з погляду внутрішньої організації бізнес-моделі, корпоративного управління, техніко-технологічної бази та стійкості до зовнішніх шоків. По-друге, досліджуваний період 2020–2024 рр. включає не лише фазу постпандемічної адаптації, а й структурний перелом 2022 р., пов'язаний із повномасштабною війною, порушенням логістичних ланцюгів, зростанням витрат, переглядом інвестиційних рішень та посиленням ролі цифрових інструментів як механізму підтримання операційної стійкості. Для України такі часові ефекти не можуть бути адекватно відтворені звичайною крос-секційною або простою часовою моделлю, оскільки вони накладаються на стійкі міжфірмові відмінності.

Об'єктом моделювання виступає інтегральний індекс економічної безпеки підприємства, розрахований у попередньому підрозділі як агрегований безрозмірний показник у межах інтервалу $[0;1]$. Вибір саме цього показника як залежної змінної є принципово важливим. По суті, інтегральний індекс акумулює інформацію про фінансову стійкість, ліквідність і платоспроможність, прибутковість, ділову активність та інвестиційно-структурну спроможність підприємства, тобто відображає не окремий симптом, а загальний стан економічної безпеки. Відповідно до методологічних підходів до побудови композитних індикаторів, розроблених Організацією економічного співробітництва та розвитку спільно з Об'єднаним дослідницьким центром Європейської Комісії, інтегральний показник доцільно застосовувати у випадках, коли виникає потреба узагальнення багатовимірної системи показників у єдину аналітичну характеристику, придатну для міжоб'єктного порівняння, ранжування та подальшого економетричного моделювання [35]. Це означає, що на етапі регресійного аналізу інтегральний індекс використовується не для побудови оцінки, а як узагальнений результативний показник, зміни якого пояснюються впливом ключових факторів.

Разом з тим сама логіка побудови регресійної моделі не повинна дублювати алгоритм формування інтегрального індексу. Якщо в інтегральній моделі використовувалася розгорнута система з 15 показників, то їх механічне перенесення до правої частини регресійного рівняння було б методично проблематичним. По-перше, значна частина цих змінних є економічно взаємопов'язаною, а отже, потенційно мультиколінеарною. По-друге, за малої вибірки це призведе до втрати ступенів свободи, нестабільності оцінок і розмиття інтерпретації. По-третє, оскільки інтегральний індекс уже агрегує інформацію із цих самих блоків, надмірне насичення моделі деталізованими змінними збільшить ризик статистичного «самопояснення» індексу його ж компонентами без належного аналітичного узагальнення. Саме тому в панельній регресії доцільно перейти від повного набору індикаторів до репрезентативних змінних-

представників функціональних блоків, які найкраще виражають сутність відповідної групи факторів.

Слід зауважити, що набір пояснювальних змінних у регресійній моделі не тотожний системі показників, використаних при формуванні інтегрального індексу економічної безпеки. Якщо на етапі побудови інтегрального показника доцільним є використання розширеної системи індикаторів, що забезпечує комплексне охоплення різних аспектів функціонування підприємства, то в межах економетричного моделювання пріоритет надається компактності та аналітичній інтерпретованості моделі.

Зменшення кількості змінних у регресії обумовлено необхідністю уникнення мультиколінеарності між показниками, які входять до однієї функціональної групи та характеризують близькі економічні явища. Крім того, за умов обмеженої панельної вибірки використання великої кількості змінних призводить до втрати статистичної надійності оцінок.

У зв'язку з цим у моделі використано не повний набір індикаторів, а їх репрезентативні представники за кожною функціональною складовою економічної безпеки. Зокрема, кожен включений показник відображає ключову характеристику відповідного блоку (фінансової стійкості, ліквідності, прибутковості, ділової активності та інвестиційно-структурного розвитку), що дозволяє зберегти економічний зміст моделі при одночасному забезпеченні її статистичної коректності.

З огляду на це базову специфікацію моделі доцільно подати у такому вигляді:

$$IEB_{it} = \alpha + \beta_1 KA_{it} + \beta_2 KL_{it} + \beta_3 KLIK_{it} + \beta_4 PA_{it} + \beta_5 OA_{it} + \beta_6 CHA_{it} + \beta_7 TPNA_{it} + \mu_i + \lambda_t + \varepsilon_i, \quad (3.13)$$

де IEB_{it} – інтегральний індекс економічної безпеки i -го підприємства у t -му році;

KA_{it} – коефіцієнт автономії;

KL_{it} – коефіцієнт фінансового левериджу;

$KLIK_{it}$ – коефіцієнт поточної ліквідності;

PA_{it} – рентабельність активів;

OA_{it} – оборотність активів;

$ЧНА_{it}$ – частка необоротних активів у загальній структурі активів;

$ТПНА_{it}$ – темп приросту необоротних активів;

μ_i – індивідуальний ефект підприємства;

λ_t – часовий ефект;

ε_i – випадкова похибка.

Параметр α є константою моделі, яка відображає базовий рівень результативного показника за нульових значень пояснювальних змінних і використовується як технічний елемент побудови регресійного рівняння.

Параметри моделі $\beta_1, \beta_2, \dots, \beta_7$ відображають силу та напрям впливу відповідних факторних змінних на інтегральний індекс економічної безпеки підприємства за інших рівних умов.

З огляду на можливу мультиколінеарність між показниками капітальної структури, у процесі емпіричної оцінки доцільно здійснити перевірку кореляційної матриці та значень факторів інфляції дисперсії (VIF). У разі виявлення високого рівня взаємозв'язку між змінними доцільним є використання альтернативних специфікацій моделі, у яких коефіцієнт автономії та коефіцієнт фінансового левериджу включаються не одночасно, а по чергові.

Такий вигляд моделі не є довільним, а відображає обґрунтований компроміс між економічним змістом і статистичною ощадливістю. До правої частини включено змінні, які, з одного боку, репрезентують ключові функціональні складові економічної безпеки підприємства, а з іншого – дозволяють уникнути перевантаження специфікації моделі. Зокрема, коефіцієнт автономії (KA_{it}) та коефіцієнт фінансового левериджу (KL_{it}) характеризують капітальну структуру та рівень фінансової стійкості; коефіцієнт поточної ліквідності ($KL_{kv_{it}}$) відображає здатність підприємства виконувати короткострокові зобов'язання; рентабельність активів (PA_{it}) характеризує ефективність використання ресурсного потенціалу; оборотність активів (OA_{it}) – інтенсивність їх використання у процесі формування доходів. Частка

необоротних активів ($ЧНА_{it}$) та темп їх приросту ($ТПНА_{it}$) введені до моделі як змінні, що відображають інвестиційно-структурні характеристики активів і водночас опосередковано фіксують масштаби техніко-технологічного оновлення підприємства.

Включення змінних $ЧНА_{it}$ та $ТПНА_{it}$ потребує окремого обґрунтування з позицій оцінювання цифрової трансформації. У фінансовій звітності більшості підприємств цифровізація не має прямого кількісного виміру, що ускладнює використання прямих індикаторів. У зв'язку з цим у прикладних дослідженнях доцільно застосовувати непрямі показники, які відображають інвестиційну активність та оновлення виробничо-технологічної бази. У цьому контексті частка необоротних активів характеризує структурну орієнтацію активів, а темп їх приросту – інтенсивність інвестиційних процесів, що у сукупності дозволяє наближено оцінити рівень впровадження сучасних технологій та цифрових рішень. За наявності детальнішої інформації доцільним є використання альтернативних змінних, зокрема показників нематеріальних активів, як більш прямого індикатора цифровізації.

Особливого значення набуває також урахування у моделі індивідуального ефекту (μ_i) та часового ефекту (λ_t). Індивідуальний ефект відображає специфічні характеристики підприємства, які не змінюються або змінюються повільно в часі, зокрема галузеву належність, організаційну структуру, технологічний рівень чи особливості корпоративного управління. Ігнорування таких характеристик може призвести до зміщення оцінок параметрів моделі. У свою чергу, часовий ефект дозволяє врахувати вплив загальносистемних чинників, що однаково діють на всі підприємства у певний період, зокрема макроекономічні шоки, інституційні зміни або кризові явища, включаючи структурні зміни 2022 року.

Залежно від характеру взаємозв'язку між індивідуальними ефектами та пояснювальними змінними у панельному аналізі застосовуються моделі з фіксованими або випадковими ефектами. У випадку, коли індивідуальні особливості підприємств корелюють із включеними до моделі змінними,

доцільним є використання моделі з фіксованими ефектами, тоді як за відсутності такої кореляції більш ефективною є модель з випадковими ефектами.

З метою вибору адекватної специфікації панельної моделі у межах дослідження було здійснено оцінювання двох альтернативних підходів – моделі з фіксованими ефектами (Fixed Effects) та моделі з випадковими ефектами (Random Effects). Оцінювання обох моделей проводилося на основі єдиної вибірки даних за 2020–2024 рр. (додатки Е–Л) із використанням однакового набору пояснювальних змінних, що забезпечує коректність подальшого порівняння отриманих результатів.

На першому етапі було побудовано модель з фіксованими ефектами, яка дозволяє врахувати індивідуальні особливості підприємств шляхом елімінування сталих у часі характеристик кожного об'єкта. Такий підхід передбачає, що всі специфічні для підприємства фактори, які не змінюються протягом досліджуваного періоду, можуть бути потенційно корельованими з пояснювальними змінними, а тому враховуються через індивідуальні константи.

На другому етапі було оцінено модель з випадковими ефектами, у межах якої індивідуальні ефекти розглядаються як випадкова складова, некорельована з регресорами. Така модель є більш ефективною за умови виконання відповідного припущення, оскільки дозволяє використовувати як внутрішньогрупову, так і міжгрупову варіацію даних.

Порівняння результатів оцінювання моделей здійснено на основі тесту Хаусмана, який передбачає перевірку нульової гіпотези про відсутність систематичних відмінностей між оцінками параметрів у моделях з фіксованими та випадковими ефектами. Суть тесту полягає у зіставленні векторів оцінених коефіцієнтів двох моделей з урахуванням їх дисперсійно-ковараційних характеристик, що дозволяє виявити наявність або відсутність кореляції між індивідуальними ефектами та пояснювальними змінними [175; 176]. За результатами проведеного тестування отримано значення $\chi^2 = 0,4695$ при $p = 0,9996$, що не дає підстав відхиляти нульову гіпотезу. Це свідчить про відсутність

статистично значущих відмінностей між оцінками моделей і обґрунтовує використання моделі з випадковими ефектами для подальшого аналізу.

З погляду економічної інтерпретації очікуваних результатів, коефіцієнт при KA_{it} має бути додатним, оскільки зростання частки власного капіталу підвищує фінансову незалежність підприємства. Натомість коефіцієнт при KL_{it} очікувано має від'ємний знак, що відображає зростання ризиків при підвищенні боргового навантаження. Показники ліквідності, рентабельності та оборотності активів, як правило, позитивно впливають на інтегральний рівень економічної безпеки, оскільки характеризують ефективність функціонування підприємства. Водночас вплив змінних $ЧНА_{it}$ та $ТПНА_{it}$ може мати нелінійний характер: помірне зростання інвестиційної активності сприяє підвищенню безпеки, тоді як надмірна капіталомісткість за недостатньої ліквідності може підвищувати ризики.

З урахуванням цього базову модель доцільно розглядати як аналітичне ядро подальшого дослідження. У практичній реалізації доцільно оцінювати декілька альтернативних специфікацій, що дозволяє перевірити стійкість отриманих результатів і мінімізувати вплив мультиколінеарності. Зокрема, можливим є почергове включення показників капітальної структури, використання альтернативних індикаторів ліквідності або уточнення змінних, що відображають інвестиційно-цифрову складову.

Враховуючи обмежений обсяг панельної вибірки, що охоплює 5 підприємств упродовж 5 років, особливого значення набуває принцип статистичної ощадливості моделі. У цьому випадку пріоритетом є не максимальна кількість змінних, а їх економічна змістовність і здатність пояснювати варіацію інтегрального індексу без втрати інтерпретованості. Саме тому запропонована модель поєднує функціональну репрезентативність показників із урахуванням індивідуальних і часових ефектів, що дозволяє адекватно відобразити як внутрішні характеристики підприємств, так і зовнішні умови їх функціонування.

У підсумку слід зазначити, що сформована специфікація є логічним продовженням попередніх етапів дослідження. Вона спирається на інтегральний підхід до оцінювання економічної безпеки, але переводить аналіз на рівень економетричного обґрунтування, що дозволяє ідентифікувати ключові фактори впливу та сформувати підґрунтя для подальшого прогнозування.

З урахуванням результатів тесту Хаусмана, які підтвердили доцільність використання моделі з випадковими ефектами, на наступному етапі було здійснено оцінювання параметрів панельної регресійної моделі інтегрального індексу економічної безпеки підприємств. Оцінювання виконано на основі даних за 2020–2024 рр. із включенням ключових фінансово-економічних детермінант, що відображають фінансову стійкість, ліквідність, прибутковість, ділову активність та інвестиційно-структурні характеристики підприємств. Отримані результати дозволяють кількісно оцінити силу та напрям впливу кожного з факторів на інтегральний індекс, а також визначити статистично значущі детермінанти економічної безпеки. Узагальнені результати оцінювання моделі наведено в таблиці 3.7.

Отримані результати економетричного оцінювання дозволяють сформулювати низку узагальнюючих висновків щодо детермінант інтегрального рівня економічної безпеки підприємств у досліджуваній вибірці.

По-перше, підтверджено визначальну роль показників фінансової стійкості у формуванні інтегрального індексу. Зокрема, коефіцієнт автономії демонструє статистично значущий позитивний вплив, що свідчить про критичну важливість достатнього рівня власного капіталу для забезпечення стійкості підприємства до зовнішніх шоків. Натомість коефіцієнт фінансового левереджу має статистично значущий негативний вплив, що відображає зростання фінансових ризиків у міру підвищення боргового навантаження. Таким чином, структура капіталу виступає одним із ключових факторів формування економічної безпеки, що узгоджується з теоретичними підходами до її оцінювання, викладеними у попередніх підрозділах.

Таблиця 3.7

Результати оцінювання панельної регресійної моделі інтегрального індексу економічної безпеки підприємств у 2020–2024 рр.

Змінна	Коефіцієнт	Стандартна похибка	z-статистика	p-value	Значущість
Константа	0,3517	0,0721	4,8807	0,000001	***
Коефіцієнт автономії, КА	0,1448	0,0282	5,1318	0,0000003	***
Коефіцієнт фінансового левериджу, КЛ	-0,0014	0,0005	-2,7334	0,0063	***
Коефіцієнт поточної ліквідності, КЛікв	0,0499	0,0118	4,2427	0,000022	***
Рентабельність активів, РА	0,1442	0,0405	3,5573	0,000375	***
Оборотність активів, ОА	0,0217	0,0264	0,8209	0,4117	
Частка необоротних активів у загальній структурі активів, ЧНА	-0,0792	0,0760	-1,0427	0,2971	
Темп приросту необоротних активів, ТПНА	0,4277	0,1042	4,1032	0,000041	***

Примітка: z-статистика відображає відношення оціненого коефіцієнта до його стандартної похибки та використовується для перевірки його статистичної значущості. p-value характеризує ймовірність випадкового отримання відповідного результату за умови відсутності реального впливу змінної; чим менше його значення, тим більш достовірним є оцінений ефект.

Позначення «***», «*» та «*» використовуються для відображення рівня статистичної значущості оцінених коефіцієнтів регресійної моделі. Зокрема, «***» відповідає рівню значущості 1% ($p < 0,01$) і свідчить про дуже високий ступінь статистичної надійності отриманого результату; «**» – рівню 5% ($p < 0,05$), що означає достатню статистичну значущість; «*» – рівню 10% ($p < 0,10$), який інтерпретується як слабка, але допустима значущість. Відсутність відповідного позначення вказує на те, що коефіцієнт не є статистично значущим у межах прийнятих рівнів довіри. Статистична значущість оцінюється на основі р-

value, яке відображає ймовірність отримання відповідного коефіцієнта випадково за умови відсутності реального впливу факторної змінної на результативний показник.

Джерело: розраховано автором за даними додатків Е–Л.

По-друге, суттєвий вплив на інтегральний індекс мають показники ліквідності та прибутковості. Позитивний і статистично значущий коефіцієнт при показнику поточної ліквідності підтверджує, що здатність підприємства своєчасно виконувати короткострокові зобов'язання є важливою передумовою його економічної стійкості. Водночас рентабельність активів демонструє один із найбільш вагомих позитивних ефектів, що свідчить про визначальну роль ефективності використання ресурсів у формуванні інтегрального рівня безпеки. Це дозволяє трактувати економічну безпеку не лише як стан захищеності, але і як функцію результативності господарської діяльності.

По-третє, показники ділової активності виявляють неоднозначний вплив на інтегральний індекс. Зокрема, оборотність активів не продемонструвала статистично значущого ефекту, що може бути пояснено галузевою специфікою досліджуваних підприємств, а також високою варіативністю цього показника в умовах нестабільного економічного середовища. Це свідчить про те, що інтенсивність використання активів не завжди трансформується у підвищення економічної безпеки без належного рівня фінансової стабільності та прибутковості.

По-четверте, отримані результати підтверджують доцільність використання агрегованого інтегрального індексу як результативного показника у межах економетричного моделювання. Виявлені статистично значущі залежності свідчать про те, що інтегральний індекс адекватно реагує на зміни ключових фінансово-економічних параметрів і може використовуватися як узагальнюючий індикатор стану економічної безпеки підприємства.

Загалом результати моделювання дозволяють зробити висновок про домінування фінансово-структурних і результативних факторів у формуванні економічної безпеки підприємств у досліджуваний період. Водночас відсутність значущості окремих показників ділової активності вказує на необхідність

подальшого уточнення моделі, зокрема через урахування галузевих особливостей та впливу зовнішніх макроекономічних факторів. У цьому контексті побудована модель створює аналітичну основу для подальшого прогнозування та сценарного аналізу інтегрального рівня економічної безпеки.

З метою візуальної оцінки адекватності побудованої панельної регресійної моделі та перевірки її здатності відтворювати фактичну динаміку інтегрального індексу економічної безпеки підприємств доцільно представити графічне зіставлення фактичних і розрахункових значень. Такий підхід дозволяє не лише доповнити результати кількісного оцінювання, але й наочно продемонструвати ступінь відповідності моделі емпіричним даним, а також виявити можливі відхилення у відтворенні динаміки показника. Результати такого зіставлення наведено на рис. 3.7.

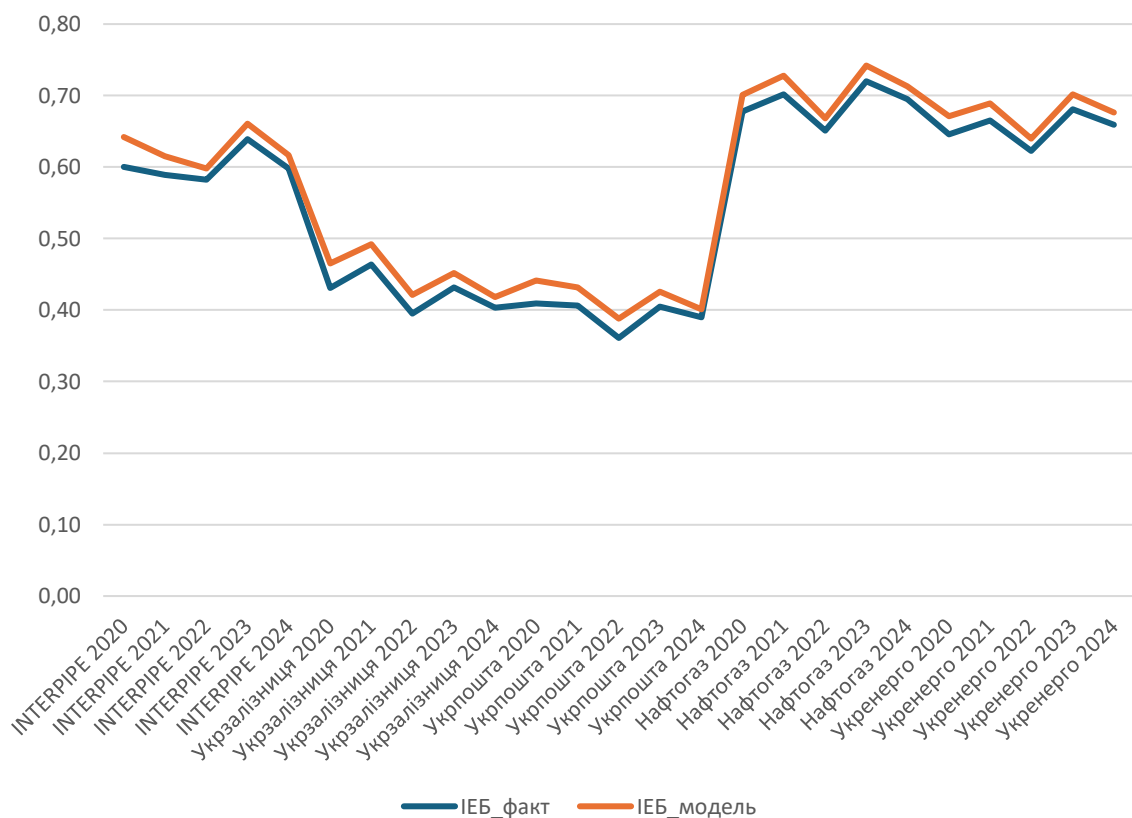


Рис. 3.7. Фактичні та оцінені значення інтегрального індексу економічної безпеки підприємств у 2020–2024 рр.

Джерело: сформовано автором.

Аналіз графічного зіставлення фактичних та оцінених значень інтегрального індексу економічної безпеки свідчить про достатньо високу адекватність побудованої економетричної моделі. Зокрема, розрахункові значення індексу в цілому відтворюють як загальний рівень, так і характер динаміки фактичних показників у розрізі досліджуваних підприємств і періодів. Спостерігається узгодженість трендів, зокрема чітко відображено зниження рівня економічної безпеки у 2022 р. та подальше його відновлення у 2023–2024 рр., що свідчить про здатність моделі враховувати вплив кризових і посткризових факторів.

Водночас незначне систематичне перевищення оцінених значень над фактичними може бути інтерпретоване як наслідок усереднюючого характеру моделі з випадковими ефектами, яка згладжує індивідуальні відхилення окремих підприємств. Проте амплітуда таких відхилень є обмеженою, що підтверджує достатній рівень точності апроксимації.

Загалом отримані результати дозволяють зробити висновок, що побудована панельна модель є статистично узгодженою та економічно інтерпретованою, а також придатною для подальшого використання у завданнях прогнозування та сценарного аналізу інтегрального рівня економічної безпеки підприємств.

Економетричне моделювання інтегрального індексу економічної безпеки підприємств формує аналітичне підґрунтя для його подальшого прогнозування як узагальнюючого показника, що відображає комплексний вплив фінансово-економічних факторів на стан підприємства. Високий рівень узгодженості між фактичними та розрахунковими значеннями індексу свідчить про здатність моделі адекватно відтворювати не лише рівень показника, але й характер його змін у часі, включаючи реакцію на зовнішні шоки та внутрішні структурні трансформації. Це дозволяє розглядати інтегральний індекс не лише як інструмент ретроспективної оцінки, але й як основу для формування обґрунтованих короткострокових прогнозів.

У межах дослідження застосовано комбінований підхід до прогнозування, який поєднує трендове моделювання динаміки інтегрального індексу з оцінкою

прогностичної здатності моделі на основі ретроспективної перевірки. Такий підхід забезпечує баланс між відображенням загальних закономірностей розвитку показника та врахуванням впливу ключових детермінант, що визначають його поведінку. Використання трендових моделей дозволяє ідентифікувати основні напрями та циклічність змін економічної безпеки, тоді як короткострокове прогнозування забезпечує оцінку точності та практичної придатності моделі для управлінських цілей.

Доцільно здійснити трендове моделювання динаміки інтегрального індексу економічної безпеки підприємств у розрізі досліджуваних періодів з метою виявлення загальних закономірностей його зміни. При цьому інтегральний індекс розглядається як часовий ряд, динаміка якого формується під впливом як внутрішніх факторів функціонування підприємства, так і зовнішніх макроекономічних умов.

Враховуючи наявність різких коливань показника у досліджуваному періоді, зокрема потенційного структурного зламу, доцільно використовувати не лише лінійну, але й квадратичну (поліноміальну другого порядку) форму трендової залежності. Лінійна модель дозволяє оцінити середній напрям зміни інтегрального індексу, тоді як квадратична функція забезпечує можливість врахування прискорення або уповільнення динаміки, а також зміни її напрямку.

Формалізація трендових залежностей може бути представлена у вигляді: лінійної моделі:

$$IEB_t = a + bt \quad (3.14);$$

квадратичної моделі:

$$IEB_t = a + bt + ct^2 \quad (3.15),$$

де t відображає часову компоненту (порядковий номер періоду), а параметри a , b , c характеризують відповідно базовий рівень показника, середню швидкість його зміни та інтенсивність прискорення або сповільнення динаміки.

Використання квадратичної специфікації є методично обґрунтованим у випадках, коли динаміка показника не є монотонною та містить фази зниження і

відновлення. У такому разі коефіцієнт при квадратичному члені (c) дозволяє зафіксувати наявність переломних моментів у розвитку показника, що є особливо важливим для аналізу економічної безпеки в умовах нестабільного середовища.

Водночас слід підкреслити, що трендове моделювання має описовий характер і відображає узагальнену траєкторію зміни інтегрального індексу без урахування безпосереднього впливу окремих факторів. У цьому контексті його доцільно розглядати як інструмент ідентифікації загальних тенденцій, який доповнює результати економетричного моделювання та дозволяє сформулювати більш цілісне уявлення про динаміку економічної безпеки підприємств.

Для ілюстрації застосування трендового підходу доцільно розглянути побудову квадратичної моделі динаміки інтегрального індексу економічної безпеки на прикладі підприємства INTERPIPE HOLDINGS PLC. Використання змінної часу t у вигляді порядкового номера періоду дозволяє формалізувати часову залежність показника, а введення квадратичного члена t^2 забезпечує можливість врахування нелінійного характеру його зміни.

Таблиця 3.8

Параметри трендової моделі інтегрального індексу економічної безпеки (на прикладі ІНТЕРПАЙП ХОЛДІНГС ПЛС (INTERPIPE HOLDINGS PLC))

Рік	t	ІЕБ (факт)	t^2
2020	1	0,600	1
2021	2	0,589	4
2022	3	0,582	9
2023	4	0,639	16
2024	5	0,598	25

Джерело: розраховано автором.

Оцінювання параметрів моделі здійснюється методом найменших квадратів, у результаті чого формується аналітичне представлення тренду у вигляді квадратичної функції. Отримана модель дозволяє описати зміну

інтегрального індексу як результат поєднання базового рівня, лінійного тренду та ефекту прискорення або уповільнення динаміки.

Економічна інтерпретація параметрів моделі полягає у тому, що коефіцієнт при змінній часу відображає загальний напрям зміни економічної безпеки підприємства, тоді як коефіцієнт при квадратичному члені характеризує наявність переломних моментів у динаміці показника. У випадку зміни знака цього коефіцієнта можна ідентифікувати перехід від фази зниження до фази відновлення або навпаки.

Отримані параметри свідчать, що динаміка інтегрального індексу економічної безпеки має нелінійний характер. Позитивне значення квадратичного коефіцієнта вказує на наявність фази відновлення після зниження показника, що узгоджується із загальною логікою функціонування підприємства в умовах нестабільного середовища.

Таким чином, навіть на прикладі окремого підприємства простежується доцільність використання нелінійних трендових моделей для опису динаміки інтегрального індексу економічної безпеки, що зумовлено впливом зовнішніх шоків та фазовим характером економічного розвитку.

Кількісна оцінка точності прогнозування інтегрального індексу економічної безпеки підприємств здійснюється на основі показника середньої абсолютної відносної похибки (САВП, англ. Mean Absolute Percentage Error — MAPE), який широко застосовується у практиці економіко-статистичного та економетричного аналізу для оцінювання якості прогнозних моделей [177–180]. Використання цього показника зумовлене його здатністю відображати величину відхилення прогнозованих значень від фактичних у відносному вимірі, що є особливо важливим для аналізу інтегральних показників, які не мають натуральної одиниці виміру.

У контексті дослідження економічної безпеки підприємств інтегральний індекс виступає агрегованим показником, що синтезує вплив широкого спектра фінансово-економічних характеристик, включаючи ліквідність, фінансову стійкість, прибутковість, ділову активність та інвестиційно-структурні

параметри. Саме тому оцінка точності його прогнозування потребує застосування відносних, а не абсолютних критеріїв, оскільки навіть незначні у абсолютному вимірі відхилення можуть мати різну економічну інтерпретацію залежно від базового рівня показника.

Формально показник САВП визначається як середнє значення абсолютних відносних відхилень прогнозованих значень від фактичних:

$$САВП = \frac{1}{n} \sum_{i=1}^n \left| \frac{ІЕБ_i^{\text{факт}} - ІЕБ_i^{\text{прогн}}}{ІЕБ_i^{\text{факт}}} \right| \cdot 100\% \quad (3.16).$$

Економічний зміст даного показника полягає у тому, що він дозволяє інтерпретувати похибку прогнозу як середній відсоток відхилення, що безпосередньо корелює з ризиком прийняття управлінських рішень на основі прогнозної інформації. Зокрема, зниження значення САВП свідчить про підвищення надійності моделі як інструменту підтримки прийняття рішень, тоді як його зростання сигналізує про необхідність перегляду специфікації моделі або врахування додаткових факторів впливу.

Важливо підкреслити, що використання САВП забезпечує можливість порівняння точності прогнозування як у часовому розрізі, так і між різними підприємствами, що є принципово важливим у дослідженнях, пов'язаних із міжоб'єктним аналізом економічної безпеки. У цьому аспекті показник виступає не лише статистичною характеристикою якості моделі, але й інструментом економічної інтерпретації результатів моделювання, оскільки дозволяє оцінити ступінь невизначеності майбутньої динаміки інтегрального індексу.

З огляду на це, застосування САВП у поєднанні з графічною верифікацією результатів та аналізом факторних детермінант формує цілісну систему оцінки прогностичної спроможності моделі, що відповідає сучасним подходам до економетричного аналізу складних соціально-економічних процесів.

За результатами розрахунків, представлених у Додатку П, середня абсолютна відносна похибка прогнозування інтегрального індексу економічної безпеки становить близько 6,35 %, що характеризує побудовану модель як достатньо точну з позицій прикладного економічного аналізу. Відповідно до

усталених підходів до оцінювання якості прогнозних моделей, значення похибки на рівні до 10 % інтерпретується як прийнятне або високе, що дозволяє зробити висновок про адекватність відтворення моделлю фактичної динаміки інтегрального індексу.

З економічної точки зору отримане значення САВП свідчить про те, що середнє відхилення розрахункових значень від фактичних є помірним і не спотворює загальну картину зміни рівня економічної безпеки підприємств. Водночас варто враховувати, що варіація похибок у розрізі окремих підприємств є нерівномірною, що відображає різний ступінь стабільності їх функціонування та чутливості до зовнішніх і внутрішніх факторів. Зокрема, для підприємств із підвищеною волатильністю фінансових показників (зокрема у періоди кризових зрушень 2022 р.) спостерігається зростання відносних відхилень, що є економічно обґрунтованим результатом.

Важливим є те, що навіть за наявності окремих локальних відхилень модель зберігає здатність адекватно відображати напрям і характер змін інтегрального індексу, тобто коректно відтворює трендові та структурні зрушення у рівні економічної безпеки. Це свідчить про те, що обраний набір факторних змінних відображає ключові детермінанти формування економічної безпеки підприємств, а специфікація моделі є узгодженою з економічною природою досліджуваного процесу.

У практичному вимірі отриманий рівень точності означає, що модель може бути використана як інструмент аналітичної підтримки управлінських рішень, зокрема для оцінювання наслідків зміни фінансових та інвестиційних параметрів діяльності підприємства. При цьому прогнозні значення інтегрального індексу доцільно інтерпретувати не як точкові оцінки, а як орієнтири у межах допустимого інтервалу відхилень, що відповідає природі економічних процесів та рівню невизначеності зовнішнього середовища.

Таким чином, значення САВП на рівні 6,35 % підтверджує, що побудована економетрична модель є достатньо надійною для подальшого використання у

процедурах короткострокового прогнозування та сценарного аналізу рівня економічної безпеки підприємств.

Отримані результати оцінювання панельної регресійної моделі та аналіз точності апроксимації інтегрального індексу економічної безпеки дозволяють зробити висновок про її достатню аналітичну спроможність щодо відтворення як рівня, так і динаміки досліджуваного показника. Невисокий рівень середньої відносної похибки та близькість фактичних і модельних значень свідчать про коректність обраної специфікації моделі, а також про релевантність включених до неї факторних змінних у поясненні варіації інтегрального індексу.

Водночас слід підкреслити, що оцінка адекватності моделі та її прогностичних характеристик, хоча і є необхідним етапом економетричного аналізу, не вичерпує можливостей її практичного застосування. З економічної точки зору значно більшої аналітичної цінності набуває використання побудованої моделі як інструменту дослідження можливих траєкторій зміни рівня економічної безпеки підприємств залежно від варіації ключових факторів. Це особливо актуально в умовах підвищеної невизначеності зовнішнього середовища, коли прийняття управлінських рішень потребує врахування альтернативних сценаріїв розвитку подій.

У цьому контексті доцільним є перехід від статичного оцінювання параметрів моделі до її використання у межах сценарного аналізу, який дозволяє моделювати потенційні зміни інтегрального індексу економічної безпеки залежно від трансформації фінансово-економічних характеристик підприємств. Такий підхід забезпечує можливість не лише оцінити поточний стан економічної безпеки, але й сформулювати обґрунтовані прогнози її розвитку, визначити критичні зони ризику та ідентифікувати найбільш ефективні напрями управлінського впливу.

Саме тому наступний етап дослідження передбачає реалізацію сценарного моделювання, спрямованого на оцінювання чутливості інтегрального індексу до змін ключових детермінант та формування альтернативних варіантів розвитку рівня економічної безпеки підприємств.

Сучасні умови функціонування підприємств, що характеризуються підвищеним рівнем невизначеності, структурними трансформаціями економіки та активізацією процесів цифровізації, обумовлюють необхідність застосування не лише інструментів ретроспективного аналізу, але й підходів, орієнтованих на моделювання альтернативних траєкторій розвитку економічних процесів. У цьому контексті особливого значення набуває сценарний аналіз як інструмент дослідження можливих варіантів зміни рівня економічної безпеки підприємств залежно від динаміки ключових факторних змінних [180; 181].

З методологічної точки зору сценарний аналіз ґрунтується на варіюванні значень детермінант інтегрального індексу економічної безпеки з метою оцінювання чутливості результативного показника до зміни умов функціонування підприємства. На відміну від точкового прогнозування, що передбачає визначення одного найбільш імовірного значення показника, сценарний підхід дозволяє сформулювати інтервальний прогноз, який відображає діапазон можливих значень інтегрального індексу за різних комбінацій факторів.

У межах проведеного дослідження сценарний аналіз базується на використанні побудованої економетричної моделі, що дозволяє формалізувати залежність інтегрального індексу економічної безпеки від системи фінансових, операційних та інвестиційно-структурних показників. Застосування цієї моделі забезпечує можливість оцінити не лише напрям, але й інтенсивність впливу зміни окремих детермінант на результуючий показник, що відповідає сучасним підходам до економічного прогнозування та стратегічного аналізу.

З урахуванням специфіки досліджуваних підприємств та структури використаних факторних змінних доцільно виокремити три базові сценарії розвитку рівня економічної безпеки. Базовий сценарій передбачає збереження існуючих тенденцій зміни ключових показників діяльності підприємств, тобто їх динаміка екстраполюється на прогнозний період без суттєвих структурних змін. Песимістичний сценарій моделює погіршення умов функціонування підприємств, що проявляється у зниженні ліквідності, зростанні боргового навантаження, уповільненні оборотності активів та зниженні прибутковості.

Оптимістичний сценарій, навпаки, передбачає покращення ключових параметрів діяльності підприємства, зокрема зростання ефективності використання ресурсів, підвищення рентабельності та активізацію інвестиційної діяльності, у тому числі за рахунок нарощування інвестицій у необоротні активи як проксі цифровізації.

З метою підвищення аналітичної визначеності сценарного моделювання доцільним є формалізоване задання змін значень факторних змінних у межах кожного сценарію. Такий підхід дозволяє уникнути декларативності та забезпечує відтворюваність результатів, що відповідає вимогам економетричного аналізу складних соціально-економічних систем.

У зв'язку з цим параметри сценаріїв доцільно задати у вигляді відносних змін ключових детермінант інтегрального індексу економічної безпеки. Для забезпечення аналітичної визначеності сценарного моделювання та кількісної інтерпретації впливу факторних змінних параметри їх варіювання у межах базового, песимістичного та оптимістичного сценаріїв узагальнено в табл. 3.9.

Формалізація сценаріїв передбачає підстановку змінених значень факторних змінних у рівняння економетричної моделі:

$$ІЕБ^{(s)} = f(KA^{(s)}, KЛ^{(s)}, KЛікв^{(s)}, PА^{(s)}, OА^{(s)}, ЧНА^{(s)}, ТПНА^{(s)}) \quad (3.17),$$

де s – сценарій розвитку (базовий, песимістичний, оптимістичний).

Такий підхід дозволяє отримати не окремі оцінки, а систему взаємопов'язаних прогнозних значень інтегрального індексу економічної безпеки, що відображають реакцію підприємства на зміну ключових параметрів його функціонування.

З урахуванням того, що у дослідженні використовується лінійна регресійна модель, функціональна залежність (3.17) набуває адитивної форми. У цьому випадку зміна інтегрального індексу економічної безпеки під впливом варіації факторних змінних може бути представлена як сума добутків оцінених коефіцієнтів регресії на зміну відповідних змінних:

$$\Delta ІЕБ = \sum_{j=1}^7 \beta_j \cdot \Delta \chi_j \quad (3.18).$$

Таким чином, вираз (3.18) є лінійною інтерпретацією загальної функціональної залежності (3.17) та дозволяє кількісно оцінити внесок кожного фактору у зміну інтегрального індексу економічної безпеки.

Таблиця 3.9

Параметризація сценаріїв зміни інтегрального індексу економічної безпеки підприємств

Показник	Базовий сценарій	Песимістичний сценарій	Оптимістичний сценарій
Коефіцієнт автономії (КА)	без змін	↓ на 10 %	↑ на 10 %
Коефіцієнт фінансового левериджу (КЛ)	без змін	↑ на 10–15 %	↓ на 10–15 %
Коефіцієнт ліквідності (КЛікв)	без змін	↓ на 10–15 %	↑ на 10–15 %
Рентабельність активів (РА)	без змін	↓ на 15–20 %	↑ на 15–20 %
Оборотність активів (ОА)	без змін	↓ на 10–15 %	↑ на 10–15 %
Частка необоротних активів (ЧНА)	стабільна	↓ на 5–10 %	↑ на 5–10 %
Темп приросту необоротних активів (ТПНА)	середній рівень	↓ на 20–30 %	↑ на 20–30 %

Примітка: стрілки відображають напрям зміни показників відносно базового періоду; параметри сформовано автором на основі логіки впливу факторів у моделі.

Джерело: авторська розробка.

Диференціація масштабів зміни факторних змінних у межах сценаріїв обумовлена двома ключовими аспектами: величиною оцінених коефіцієнтів регресії та економічною природою відповідних показників.

По-перше, фактори з більшими за абсолютною величиною коефіцієнтами регресії мають більш суттєвий вплив на інтегральний індекс, що зумовлює необхідність обережнішого варіювання їх значень у сценаріях. Зокрема, для показників інвестиційно-структурного характеру, таких як темп приросту необоротних активів, встановлено значні коефіцієнти впливу, що дозволяє

використовувати ширші інтервали їх зміни, оскільки вони відображають довгострокові стратегічні зрушення.

По-друге, різні факторні змінні мають неоднакову економічну волатильність. Показники рентабельності та інвестиційної активності характеризуються вищою варіативністю у часі, тому для них задаються ширші інтервали змін (15–30 %), тоді як структурні показники, зокрема частка необоротних активів, змінюються більш поступово, що обумовлює використання вузьких інтервалів (5–10 %).

По-третє, при визначенні параметрів сценаріїв враховано економічну доцільність і реалістичність змін. Надмірно великі відхилення факторів могли б призвести до отримання формально можливих, але економічно необґрунтованих результатів. Тому обрані інтервали змін забезпечують баланс між аналітичною чутливістю моделі та реалістичністю прогнозних оцінок.

Таким чином, варіювання факторних змінних у межах сценаріїв здійснюється з урахуванням їх економетричної значущості, волатильності та економічного змісту, що забезпечує обґрунтованість отриманих результатів сценарного моделювання.

Кількісна реалізація сценаріїв здійснюється шляхом підстановки змінених значень факторних змінних у рівняння регресійної моделі. При цьому вплив кожного фактору на зміну інтегрального індексу економічної безпеки визначається з урахуванням величини відповідного коефіцієнта регресії.

Зокрема, зміна інтегрального індексу у межах сценарію може бути представлена у вигляді:

$$\Delta IEB = \beta_1 \cdot \Delta KA + \beta_2 \cdot \Delta KJ + \beta_3 \cdot \Delta KJ_{\text{ікв}} + \beta_4 \cdot \Delta PA + \beta_5 \cdot \Delta OA + \beta_6 \cdot \Delta CHA + \beta_7 \cdot \Delta TPNA \quad (3.19).$$

Це означає, що внесок кожного фактору у зміну інтегрального індексу визначається як добуток величини його зміни у межах сценарію та відповідного коефіцієнта регресії.

Таким чином, параметри сценаріїв не є довільними, а безпосередньо пов'язані з результатами економетричного моделювання. Фактори з більшими за

модулем коефіцієнтами регресії формують більш суттєвий вплив на інтегральний індекс, що враховано при встановленні масштабів їх варіювання у межах сценаріїв. Це забезпечує узгодженість між статистичною оцінкою моделі та економічною інтерпретацією отриманих результатів.

Узагальнення результатів сценарного моделювання дозволяє зробити принципово важливий висновок: рівень економічної безпеки підприємства формується не стільки під впливом окремих факторів, скільки внаслідок їх системної взаємодії, причому критичну роль відіграють показники ефективності використання ресурсів та інвестиційно-структурного розвитку.

Аналіз показує, що в умовах погіршення фінансових параметрів найбільш суттєве зниження інтегрального індексу відбувається за рахунок одночасного негативного впливу рентабельності та ліквідності, що свідчить про високу чутливість економічної безпеки до операційної ефективності підприємства. Водночас навіть за несприятливих умов підприємства, які зберігають інвестиційну активність, демонструють відносно менше зниження інтегрального показника, що підтверджує стратегічну роль інвестицій у забезпеченні довгострокової стійкості.

У межах оптимістичного сценарію встановлено, що найбільш вагомий позитивний ефект досягається не за рахунок ізолюваного покращення окремих показників, а внаслідок синергії зростання рентабельності, оборотності активів та інвестицій у необоротні активи. Це дозволяє трактувати економічну безпеку як інтегральний результат ефективності управління ресурсами та здатності підприємства до структурної модернізації.

Таким чином, результати сценарного аналізу підтверджують доцільність використання економетричної моделі як інструменту не лише діагностики, але й підтримки управлінських рішень. Вони також свідчать про необхідність переходу до проактивної моделі управління економічною безпекою, яка передбачає цілеспрямований вплив на ключові фактори її формування з урахуванням можливих варіантів розвитку зовнішнього середовища.

З метою оцінювання чутливості інтегрального індексу економічної безпеки до зміни ключових факторних детермінант та виявлення можливих траєкторій його динаміки здійснено сценарне моделювання на основі побудованої економетричної моделі. Такий підхід дозволяє перейти від точкової оцінки до аналізу варіантів розвитку економічної безпеки підприємств за різних умов їх функціонування, що є особливо актуальним в умовах нестабільного зовнішнього середовища та структурних трансформацій економіки. Для забезпечення порівнянності результатів і уникнення неоднозначності інтерпретації у межах заданих інтервалів варіювання факторних змінних використано їх середні значення, що дозволило отримати узагальнені точкові оцінки інтегрального індексу за кожним сценарієм. Результати проведеного сценарного аналізу наведено в табл. 3.10.

Таблиця 3.10

Результати сценарного моделювання інтегрального індексу економічної безпеки підприємств

Підприємство	ІЕБ (факт, 2024)	Базовий сценарій	Песимістичний сценарій	Оптимістичний сценарій
INTERPIPE HOLDINGS PLC	0,598	0,667	0,620	0,715
АТ «Укрзалізниця»	0,482	0,487	0,466	0,509
АТ «Укрпошта»	0,342	0,353	0,325	0,381
ПрАТ «НЕК «Укренерго»	0,400	0,428	0,395	0,461
ТОВ «ГПК «Нафтогаз України»	0,310	0,342	0,327	0,356

Примітка: розраховано автором на основі економетричної моделі; для сценарних оцінок використано середні значення інтервалів варіювання факторних змінних.

Джерело: авторська розробка.

Висновки до розділу 3

Проведений аналіз інструментарію оцінки та підвищення рівня економічної безпеки підприємства в умовах цифрової трансформації, що охоплює методологічні підходи, систему аналітичної діагностики та економетричні методи дослідження, дозволив узагальнити такі висновки:

1. Узагальнено та систематизовано методологічні засади оцінювання економічної безпеки підприємства, що дозволило сформувати цілісну концептуальну основу її дослідження в умовах цифровізації. Виокремлено ключові підходи до оцінювання (функціональний, індикаторний, інтегральний), обґрунтовано їх взаємодоповнюваність та доцільність комплексного застосування. Доведено, що в сучасних умовах економічна безпека підприємства повинна розглядатися як багатовимірна характеристика, яка відображає не лише рівень захищеності, а й здатність до адаптації, розвитку та забезпечення стабільності фінансово-економічних результатів. Це дозволило сформувати методологічну рамку дослідження, у межах якої оцінювання економічної безпеки здійснюється як системний процес, орієнтований на виявлення внутрішніх дисбалансів, оцінку стійкості та обґрунтування управлінських рішень у цифровому середовищі. Встановлено, що саме інтеграція різних підходів забезпечує підвищення достовірності аналітичних результатів та мінімізує ризики однобічної інтерпретації рівня економічної безпеки. Це, у свою чергу, створює передумови для формування адаптивної системи управління, здатної оперативно реагувати на зміни зовнішнього та внутрішнього середовища функціонування підприємства.

2. Сформовано систему індикаторів оцінювання економічної безпеки підприємства, структуровану за функціональними складовими, що забезпечує можливість комплексної кількісної діагностики її рівня. Запропоноване групування показників за відповідними блоками дозволяє одночасно оцінити поточний фінансово-економічний стан підприємства та його здатність до розвитку в умовах цифрових змін. Обґрунтовано, що така система показників

створює аналітичну основу для подальшого агрегування результатів у єдиний інтегральний показник, що підвищує узгодженість оцінювання та його придатність для порівняльного аналізу. Водночас врахування інвестиційно-структурних параметрів розширює можливості інтерпретації результатів, дозволяючи оцінити не лише поточний рівень безпеки, а й потенціал його зміни під впливом цифрової трансформації. Доведено, що така індикаторна система виконує не лише діагностичну, а й прогностичну функцію, оскільки дозволяє виявляти тенденції зміни рівня економічної безпеки та формувати інформаційну базу для стратегічного планування розвитку підприємства.

3. Узагальнено результати аналітичної діагностики економічної безпеки підприємств на основі інтегрального підходу, що дозволило сформувати цілісне уявлення про рівень їх стійкості у динамічному та міжгалузевому вимірі. Встановлено наявність суттєвої диференціації значень інтегрального показника як між окремими підприємствами, так і в часовому розрізі, що свідчить про нерівномірність адаптаційних можливостей до умов цифрової трансформації та впливу зовнішніх шоків. На основі проведених розрахунків та їх візуалізації обґрунтовано, що економічна безпека підприємств формується як результат взаємодії фінансових, операційних та інвестиційних чинників, причому нестабільність окремих складових безпосередньо транслюється у варіативність інтегрального рівня. Доведено, що динаміка показника має виражену чутливість до кризових періодів, що дозволяє інтерпретувати його як індикатор реакції підприємств на зміни макроекономічного середовища та інституційних умов функціонування. Водночас встановлено, що навіть за умов загальної стабілізації окремих показників можливе збереження внутрішніх дисбалансів, які знижують стійкість підприємства в середньостроковій перспективі. Це підтверджує необхідність використання інтегрального підходу як більш точного інструменту оцінювання порівняно з аналізом окремих фінансових коефіцієнтів.

4. Сформовано аналітичну основу для міжгалузевого порівняння економічної безпеки підприємств, що дало змогу виявити структурні відмінності у механізмах її формування та визначити ключові детермінанти стійкості. На

основі узагальнення результатів графічного та статистичного аналізу встановлено, що більш високий рівень економічної безпеки досягається за умови збалансованості між фінансовими параметрами діяльності та інвестиційно-структурними характеристиками, які відображають здатність підприємства до оновлення та розвитку. Водночас виявлено, що диспропорції між окремими складовими, а також підвищена волатильність показників зумовлюють зниження інтегрального рівня безпеки та формують додаткові ризики нестійкості. Обґрунтовано, що використання інструментів візуалізації дозволяє не лише поглибити інтерпретацію результатів оцінювання, а й ідентифікувати критичні зони вразливості, що створює підґрунтя для формування обґрунтованих управлінських рішень, спрямованих на підвищення економічної безпеки підприємств у міжгалузевому середовищі. Додатково встановлено, що підприємства з більш диверсифікованою структурою діяльності демонструють вищу стійкість до зовнішніх шоків, що підкреслює значення структурної гнучкості як чинника економічної безпеки. Це дозволяє розглядати міжгалузевий аналіз як інструмент виявлення не лише відмінностей, а й потенційних напрямів підвищення ефективності функціонування підприємств.

5. Узагальнено результати економетричного моделювання інтегрального рівня економічної безпеки підприємств, що дозволило кількісно обґрунтувати вплив ключових факторів на його зміну у часовому та міжгалузевому розрізі. Побудовано панельну регресійну модель, яка забезпечила врахування як індивідуальних особливостей підприємств, так і спільних тенденцій розвитку економічного середовища. Встановлено наявність статистично значущих залежностей між інтегральним показником економічної безпеки та системою відібраних факторів, що підтверджує коректність сформованої аналітичної бази та її придатність для економетричного аналізу. Доведено, що модель адекватно відтворює фактичну динаміку інтегрального індексу, зокрема періоди зниження та подальшого відновлення його значень, що свідчить про її пояснювальну здатність. Це дозволяє використовувати отримані результати для поглибленого

аналізу закономірностей формування економічної безпеки та оцінювання впливу окремих факторів на її рівень.

6. Сформовано підхід до прогнозування інтегрального рівня економічної безпеки підприємств на основі економетричної моделі, що забезпечує можливість оцінювання його майбутньої динаміки з урахуванням виявлених залежностей. Обґрунтовано, що використання економетричного інструментарію дозволяє перейти від описового аналізу до формалізованого прогнозування, підвищуючи обґрунтованість управлінських рішень у сфері забезпечення економічної безпеки. Встановлено, що точність прогнозних оцінок залежить від стабільності факторних зв'язків, якості вихідних даних та коректності специфікації моделі, що набуває особливого значення в умовах структурних змін і підвищеної невизначеності зовнішнього середовища. Доведено, що врахування часової динаміки та міжоб'єктних відмінностей у межах панельного підходу дозволяє підвищити достовірність прогнозів і уникнути спрощених узагальнень щодо поведінки інтегрального показника. Водночас застосування моделі у поєднанні з аналізом динаміки інтегрального показника забезпечує можливість своєчасного виявлення тенденцій його зміни та формування превентивних заходів управління, орієнтованих на мінімізацію ризиків. Це створює підґрунтя для впровадження економетричного підходу як складової системи адаптивного управління економічною безпекою підприємства, а також дозволяє інтегрувати прогнозні оцінки у процес стратегічного планування та підвищення стійкості підприємства в умовах цифрової трансформації.

Основні положення розділу розкрито у публікаціях автора [107; 160; 162; 182].

ВИСНОВКИ

У дисертації теоретично обґрунтовано та розроблено методичні підходи і практичні рекомендації щодо оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки України. Одержані результати дослідження дають підстави констатувати досягнення поставленої мети та вирішення визначених завдань. За результатами проведеного дослідження сформульовано такі висновки:

1. Розкрито еволюцію наукових підходів до трактування економічної безпеки підприємства та обґрунтовано перехід від захисно-стабілізаційної до стратегічно-розвиткової парадигми її розуміння. Визначено, що економічна безпека підприємства формується як результат взаємодії фінансових, організаційних, інформаційних і технологічних чинників, а цифровізація змінює природу ризиків, критерії стійкості та параметри управлінських рішень. Систематизовано ризики економічної безпеки підприємства з урахуванням цифровізації, що дозволило виокремити зовнішні (політичні, воєнні, соціально-економічні, глобальні) та внутрішні (правові, організаційні, структурні, індивідуальні) ризики. Розкрито взаємозв'язок між ризиками та параметрами стійкості підприємства. Сформовано типологію стійкості (економічної, технічної, цифрової, енергоефективної, інноваційної), що дозволяє інтерпретувати економічну безпеку як здатність підприємства забезпечувати стабільність і розвиток у змінному середовищі. Визначено, що поєднання показників ефективності та ризику забезпечує оцінювання результативності діяльності з урахуванням ризиків і формує основу ризик-орієнтованого управління. Систематизовано міжнародні підходи до ризик-орієнтованого управління (ISO 31000, COSO ERM, NIST CSF) та сформовано засади інтеграції ризик-орієнтованої моделі управління у систему стратегічного планування підприємства. Запропоновано концептуальну модель економічної безпеки підприємства в умовах цифрової трансформації, у якій відображено

взаємозв'язок між цифровими ризиками, параметрами стійкості, управлінськими рішеннями та показниками ефективності і ризику.

2. У роботі удосконалено методичні підходи до формування системи цифрового моніторингу, що передбачає інтеграцію принципів оцінювання, системи показників результативності та ризику з цифровими технологіями аналітичної обробки даних. Визначено, що оцінювання економічної безпеки в умовах цифрової трансформації має здійснюватися з урахуванням взаємозв'язку результативності діяльності підприємства та рівня ризиків його функціонування. Розкрито принципи оцінювання економічної безпеки та уточнено логіку формування системи показників. Встановлено, що традиційний індикаторний підхід потребує доповнення показниками, які відображають ризикогенність і адаптивність діяльності підприємства. Визначено роль цифрових технологій у системі оцінювання та моніторингу економічної безпеки. Встановлено, що використання цифрових платформ і аналітичних систем забезпечує оперативне виявлення відхилень та підвищує обґрунтованість управлінських рішень. Розкрито вплив цифрової трансформації на бізнес-процеси та архітектуру управління підприємством. Визначено, що цифровізація змінює організацію діяльності, посилює роль цифрових платформ і підвищує залежність від інформаційних технологій, що зумовлює трансформацію підходів до забезпечення економічної безпеки. Систематизовано технологічні ризики цифрової трансформації та визначено їх вплив на функціонування підприємства. Встановлено, що вони охоплюють кіберризики, регуляторні обмеження та ризики платформної залежності і потребують формування адекватних механізмів управлінського реагування. Сформовано підхід до інтеграції ключових показників ефективності та ключових індикаторів ризику у систему моніторингу економічної безпеки підприємства. Визначено, що їх узгоджене використання забезпечує співставлення результативності діяльності з рівнем ризиків і підвищує обґрунтованість управлінських рішень.

3. Узагальнення існуючих підходів до оцінювання економічної безпеки підприємств дозволило розвинути функціонально-ресурсний підхід до її

діагностики, який передбачає структуризацію складових економічної безпеки за ключовими напрямками функціонування та відповідними ресурсними елементами. Встановлено, що така структуризація забезпечує взаємозв'язок між складовими економічної безпеки та дозволяє перейти від ізольованого аналізу окремих показників до комплексної оцінки їх взаємодії. Виокремлено складові економічної безпеки підприємства та сформовано систему індикаторів для їх діагностики, що дозволяє відобразити як поточний стан функціонування підприємства, так і потенційні відхилення у його розвитку. Визначено, що запропонована система індикаторів забезпечує узгоджене оцінювання результативності діяльності та рівня ризиків, підвищуючи аналітичну обґрунтованість діагностичних висновків. Застосовано кейс-аналіз як інструмент апробації функціонально-ресурсного підходу до діагностики економічної безпеки підприємств, що дозволило підтвердити його практичну доцільність та виявити специфіку впливу окремих складових і показників на загальний рівень економічної безпеки. Встановлено, що використання кейс-аналізу сприяє поглибленню інтерпретації результатів діагностики та підвищує її прикладну значущість.

4. Визначено, що цифровізація виступає системоутворюючим чинником трансформації економічної безпеки підприємств, оскільки змінює характер бізнес-процесів, структуру створення вартості та умови функціонування, одночасно генеруючи нові види загроз. Обґрунтовано, що ризики в цифровому середовищі формуються як результат взаємодії технологічних, регуляторних і платформних чинників. Набули подальшого розвитку положення щодо систематизації цифрових ризиків економічної безпеки підприємств шляхом їх структуризації на взаємопов'язані групи, що охоплюють кіберризики, регуляторні ризики та ризики залежності від цифрових платформ. Встановлено, що така систематизація відображає логіку ризикогенезу та забезпечує комплексне бачення джерел загроз. Розкрито механізми впливу цифрових ризиків на бізнес-процеси підприємства, що проявляються у зростанні вразливості інформаційних систем, ускладненні регуляторного середовища та посиленні

залежності від цифрової інфраструктури, що зумовлює необхідність адаптації системи економічної безпеки. Встановлено кореляцію цифрових ризиків із ключовими показниками ефективності та ключовими індикаторами ризику підприємства, що забезпечує узгодження оцінювання результативності з рівнем ризиків, підвищує чутливість моніторингу до критичних відхилень і формує основу для обґрунтованих управлінських рішень.

5. Дослідження міжнародних практик цифрового ризик-менеджменту дозволило встановити, що їх ефективність ґрунтується на інтеграції управління ризиками у стратегічне та фінансове управління підприємством і використанні стандартизованих рамок моніторингу цифрової стійкості. Визначено, що міжнародні підходи поєднують технічні й економічні інструменти, орієнтуючись на зниження економічних втрат і підвищення стійкості підприємств. Набули подальшого розвитку науково-прикладні засади адаптації міжнародних практик цифрового ризик-менеджменту до умов національної економіки, що передбачає їх систематизацію за напрямками застосування, урахування інституційних і технологічних обмежень та інтеграцію інструментів міжнародних стандартів у систему управління економічною безпекою підприємств. Встановлено доцільність використання індикаторів цифрової стійкості, витрат на безпеку, часу відновлення та рівня зрілості систем управління ризиками. Обґрунтовано, що адаптація міжнародних практик має здійснюватися з урахуванням інституційних обмежень, рівня гармонізації законодавства та кадрового забезпечення. Визначено, що їх інтеграція формує основу ризик-орієнтованого управління економічною безпекою, підвищує адаптивність підприємств і узгоджує національні підходи з європейськими вимогами.

6. Удосконалено методику інтегрального оцінювання економічної безпеки підприємств, що передбачає формування системи показників із визначенням їх економічного змісту, розрахункових залежностей і джерел інформаційного забезпечення. Встановлено, що за відсутності у фінансовій звітності прямих кількісних індикаторів цифрової трансформації оцінювання економічної безпеки доцільно здійснювати на основі системи взаємопов'язаних показників, які

дозволяють опосередковано відобразити вплив цифрових змін на фінансовий стан, інвестиційну активність і здатність підприємства до розвитку, забезпечуючи аналітичну узгодженість розрахунків. Сформовано порядок побудови інтегрального індексу економічної безпеки підприємства на основі нормалізації показників методом мін–макс, їх зважування за ентропійним методом та подальшого агрегування, що забезпечує зіставність показників, зменшує суб'єктивність у визначенні ваг і підвищує об'єктивність інтегральної оцінки. Обґрунтовано використання інтерпретаційної шкали інтегрального індексу в межах інтервалу $[0;1]$, що дозволяє здійснювати класифікацію рівнів економічної безпеки та формує основу для подальшої аналітичної діагностики, міжгалузевого порівняння і прогнозування.

7. Обґрунтовано можливість використання інтегрального підходу для аналітичної діагностики економічної безпеки підприємств, що забезпечує перехід від оцінювання окремих показників до комплексного вимірювання її рівня у динаміці та у розрізі видів економічної діяльності. Забезпечення зіставності результатів досягнуто шляхом уніфікації фінансових даних, їх нормалізації та приведення до єдиної аналітичної бази, що дозволило коректно здійснювати міжчасове та міжпідприємницьке порівняння за 2020–2024 рр. На основі розрахунку інтегрального індексу економічної безпеки для сформованої вибірки підприємств (ПАТ «НЕК «Укренерго», ТОВ «ГПК «Нафтогаз України», АТ «Українська залізниця», АТ «Укрпошта», INTERPIPE HOLDINGS PLC) проведено їх порівняльну аналітичну діагностику, що дозволило виявити диференціацію рівнів економічної безпеки та відмінності у структурі її формування. Отримані результати засвідчують нерівномірність адаптації підприємств до умов цифрової трансформації, що проявляється у варіативності значень інтегрального показника та зміні його динаміки у досліджуваному періоді. Застосування інтегрального підходу в поєднанні з аналізом функціональних складових дозволило ідентифікувати внутрішні чинники формування економічної безпеки, зокрема роль фінансових, операційних та інвестиційно-структурних параметрів у забезпеченні її рівня. Це дало змогу

здійснити порівняльне ранжування підприємств, виявити стійкі тенденції та відхилення у їх розвитку, а також сформуванати аналітичну основу для подальшого економетричного моделювання і прогнозування.

8. Використання панельного економетричного моделювання дозволило оцінити взаємозв'язок між інтегральним рівнем економічної безпеки підприємств і системою визначальних факторів з урахуванням часової динаміки та індивідуальних особливостей підприємств. Побудовано панельну економетричну модель залежності інтегрального показника від сукупності факторів та обґрунтовано вибір її специфікації на основі статистичних критеріїв. Оцінювання параметрів моделі забезпечило кількісну ідентифікацію впливу ключових факторів і їх значущості у формуванні динаміки інтегрального показника, підтвердивши наявність стійких залежностей із фінансовими, операційними та інвестиційно-структурними характеристиками діяльності підприємств. На основі моделі здійснено прогнозування інтегрального рівня економічної безпеки та оцінено можливі траєкторії його зміни. Сценарний аналіз шляхом варіювання значень факторів у межах базового, оптимістичного та песимістичного сценаріїв дозволив визначити діапазон коливань показника та формалізувати вплив змін середовища. Поєднання економетричного моделювання та сценарного підходу підвищує обґрунтованість прогнозних оцінок, дозволяє оцінити чутливість інтегрального показника до змін ключових факторів і формує основу для прийняття управлінських рішень щодо зміцнення економічної безпеки підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Human Development Report 1994. New Dimensions of Human Security. UNDP. URL: <https://hdr.undp.org/content/human-development-report-1994> (дата звернення: 10.02.2024).
2. Committees of the UK Parliament. Economic Security. Written Evidence. 2023. URL: <https://committees.parliament.uk/writtenevidence/127562/html/> (дата звернення: 10.02.2024).
3. Пастернак-Таранушенко Г. А. Економічна безпека держави: методологія забезпечення. Київ: Київський економічний інститут менеджменту, 2003. 320 с.
4. Урба М.Є., Іванчак І.О. Теоретичні аспекти дослідження суті економічної. *Причорноморські економічні студії*. 2018. № 34. С. 33–38. URL: https://bses.in.ua/journals/2018/34_2018/9.pdf (дата звернення: 10.02.2024).
5. Андрійчук В. Г. Економічна безпека України: стан, критерії виміру та превентивні заходи її зміцнення. *Економіка, фінанси, право*. 2013. № 6. С. 12–17.
6. Лопатка К. А., Шаранова Ю. Г. Економічна безпека як економічна категорія: огляд наукових публікацій. *Економічний простір*. 2019. № 148. С. 5–18. URL: <https://prostir.pdaba.dp.ua/index.php/journal/article/view/147> (дата звернення: 11.02.2024).
7. Фактори економічної безпеки підприємства. *Modernization of science and its influence on global processes: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference, September 20, 2024*. Bern, Swiss Confederation: International Center of Scientific Research. DOI 10.36074/scientia-20.09.2024. С. 52–54.
8. National Security Strategy of the United States. 2022. URL: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf> (дата звернення: 11.02.2024).

9. UNDP. The Concept of Human Security. Human Security Unit. URL: <https://humansecuritycourse.info/module-1-the-concept-of-human-security/un-approach/> (дата звернення: 11.02.2024).
10. European Commission. The EU's open strategic autonomy: Commission adopts updated industrial strategy. 2021. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1884 (дата звернення: 11.02.2024)
11. Про Стратегію економічної безпеки України на період до 2025 року: Указ Президента України від 11.08.2021 № 347/2021. URL: <https://zakon.rada.gov.ua/laws/show/347/2021#Text> (дата звернення: 11.02.2024).
12. Економічна безпека держави: сутність та напрями формування : монографія / Л. С. Шевченко, О. А. Гриценко, С. М. Макуха та ін. / за ред. д-ра екон. наук, проф. Л. С. Шевченко. Х.: Право, 2009. 312 с. URL: https://library.nlu.edu.ua/POLN_TEXT/MONOGRAFIJ_2010/Shevchenko_2009.pdf (дата звернення: 11.02.2024).
13. Солодовнік О. О. Основні підходи до оцінювання економічної та фінансової безпеки: сутність і напрями вдосконалення. *Бізнес Інформ*. 2021. №2. С. 6–12. URL: <https://doi.org/10.32983/2222-4459-2021-2-6-12> (дата звернення: 11.02.2024).
14. Калинюк В. Є. Сучасні наукові підходи до визначення сутності поняття «економічна безпека підприємства». *Бізнес Інформ*. 2022. № 12. С. 221–228. URL: https://www.business-inform.net/export_pdf/business-inform-2022-12_0-pages-221_228.pdf (дата звернення: 11.02.2024).
15. Цвігун Т. В. Економічна безпека в системі національної безпеки України. *Економіка і суспільство*. 2017. Вип. 11. С. 150–156. URL: https://economyandsociety.in.ua/journals/11_ukr/24.pdf (дата звернення: 11.02.2024).
16. Ковальчук А. М. Фінансово-економічна безпека підприємства в контексті адаптації до викликів цифрового середовища. *Економічний вісник ДВНЗ «НГУ»*. 2020. № 3(71). С. 152–159. DOI: 10.33271/ebdut/71.152. URL:

https://ev.nmu.org.ua/index.php/uk/archive?arh_article=1282 (дата звернення: 10.06.2025).

17. Жадько К. С., Самойленко Д. М. Економічна безпека підприємств в умовах цифрових технологій і пандемії. *Центральноукраїнський науковий вісник. Економічні науки*. 2020. Вип. 5. С. 170–176. URL: http://nbuv.gov.ua/UJRN/Npkntu_e_2020_5_18 (дата звернення: 10.08.2025).

18. Паршина О.А., Паршин Ю.І., Савченко Ю.В. Економічна безпека в умовах діджиталізації: сучасний стан та перспективи розвитку інформаційного суспільства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2019. № 2. С. 167–174. URL: http://nbuv.gov.ua/UJRN/Nvdduvs_2019_2_31 (дата звернення: 10.08.2025).

19. Осадча О. О., Роздопченюк В. М. Ризики економічної безпеки підприємства в умовах цифровізації. *Вісник Національного університету водного господарства та природо-користування*, 2024. Вип. 3(107). С. 116-126.

20. International Organization for Standardization (ISO). Risk management – Guidelines (ISO 31000:2018). Geneva: ISO, 2018. URL: <https://www.iso.org/standard/65694.html> (дата звернення: 10.08.2025).

21. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). Київ: ДП «УкрНДНЦ», 2018. (інформаційна сторінка стандарту; статус «діючий», дата чинності 01.01.2019). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80322 (дата звернення: 10.08.2025).

22. International Organization for Standardization; International Electrotechnical Commission (ISO/IEC). Risk assessment techniques (IEC 31010:2019). Geneva: ISO, 2019. URL: <https://www.iso.org/standard/72140.html> (дата звернення: 10.08.2025).

23. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management—Integrating with Strategy and Performance. COSO, 2017. Офіц. сторінка: <https://www.coso.org/guidance-erm> (дата звернення: 10.08.2025).

24. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT). Київ: ДП «УкрНДНЦ», 2021. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=96909 (дата звернення: 10.08.2025).

25. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Київ: ДП «УкрНДНЦ», 2023. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398 (дата звернення: 10.08.2025).

26. The Institute of Internal Auditors (IIA). The IIA's Three Lines Model: An Update of the Three Lines of Defense. Position Paper. The IIA, 2020. URL (PDF): <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf> (дата звернення: 01.08.2025).

27. Національний банк України. Оприлюднено плани проведення інспекційних перевірок банків та небанківських фінансових установ на 2022 рік (новина від 2022 р.). URL: <https://bank.gov.ua/ua/news/all/oprilyudneno-plani-provedennya-inspektsiynih-perevirok-bankiv-ta-nebankivskih-finansovih-ustanov-na-2022-rik> (дата звернення: 01.08.2025).

28. НЕК «Укренерго». Укренерго працює над посиленням захисту об'єктів критичної інфраструктури (повідомлення; у тексті згадано «Концепцію розвитку кібербезпеки компанії до 2023 року» та її засади). URL: <https://ua.energy/zagalni-novyny/ukrenergo-pratsyuye-nad-posylennyam-zahystu-ob-ektiv-krytychnoyi-infrastruktury/> (дата звернення: 01.08.2025).

29. Захарченко В. І., Савенко В. О. Мінімізація ризику у промисловому виробництві та вибір оптимального рішення. *Economic Journal Odessa Polytechnic University*. 2021. № 1(15). С. 30–38. URL: <https://economics.net.ua/ejoru/2021/No1/30.pdf> (дата звернення: 01.08.2025).

30. CERT-UA минулого року опрацювала 4315 кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. 2025. URL: <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-oprasyuvala-4315-kiberincidentiv> (дата звернення: 14.12.2025).

31. NIST. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology, 2024. URL: <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final>; PDF: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> (дата звернення: 01.08.2025).

32. ISO 50001:2018. Energy management systems – Requirements with guidance for use. Geneva: International Organization for Standardization, 2018. Офіц. сторінка стандарту. URL: <https://www.iso.org/standard/69426.html> (дата звернення: 01.08.2025).

33. ENISA. ENISA Threat Landscape 2024. Athens: European Union Agency for Cybersecurity, 2024. Офіц. сторінка публікації. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (дата звернення: 01.08.2025).

34. OECD. Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development. Paris: OECD Publishing, 2015. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/frascati-manual-2015_g1g57dcb/9789264239012-en.pdf (дата звернення: 15.08.2025).

35. OECD. Joint Research Centre. Handbook on Constructing Composite Indicators: Methodology and User Guide. Paris: OECD Publishing, 2008. URL: https://www.oecd.org/en/publications/handbook-on-constructing-composite-indicators-methodology-and-user-guide_9789264043466-en.html (дата звернення: 15.08.2025).

36. Чумаченко О., Нескородько О. Вдосконалення системи управління ризиками як спосіб підвищення фінансової стійкості підприємств. *Вчені записки Університету «КРОК»*. 2025. Вип. 1(77) С. 89–95.

DOI:<https://doi.org/10.31732/2663-2209-2025-77-89-95> (дата звернення: 15.08.2025).

37. Латишева О. В. Особливості використання імітаційного моделювання для оцінки ризиків інвестиційних проектів промислового підприємства. *Вісник економічної науки України*. 2017. № 2 (33). С. 77–82. URL: <https://nasplib.isofts.kiev.ua/items/9931d209-1ac0-426e-8192-06ed409f8035> (дата звернення: 15.08.2025).

38. Багорка М. О., Кадирус І. Г., Юрченко Н. І. Дослідження та аналіз факторів середовища підприємства. Проблеми сучасних трансформацій: економіка та управління. 2022. Вип. 4. С. 1–14. URL: <https://reicst.com.ua/pmt/article/view/2022-4-04-02> (дата звернення: 15.08.2025).

39. Богданюк І. В., Мандич С. М. Стратегічне управління безпекою підприємства в умовах цифрових трансформацій. *Регіональна економіка*. 2024. № 3. С. 149–156. URL: https://re.gov.ua/re202403/re202403_149_BohdanyukIV%2CMandychSM.pdf (дата звернення: 15.08.2025).

40. Лігоненко Л. О. Вплив цифровізації на систему управління результативністю підприємств та формування стратегії їх діяльності. *Економічний простір*. 2025. № 199. С. 220–227. DOI: <https://doi.org/10.30838/EP.199.220-227> (дата звернення: 15.08.2025).

41. Іванова Н. С. Розробка аналітичної системи управління економічною безпекою підприємства в цифровому середовищі. *Таврійський науковий вісник*. Серія: Економіка. 2024. Вип. 20. С. 109–119. DOI:10.32782/2708-0366/2024.20.12 (дата звернення: 15.08.2025).

42. Андріїв Н. М. Економічна безпека підприємства в умовах цифровізації ринку праці: теоретичні та практичні аспекти : монографія / Андріїв Наталія Миколаївна. Львів: Растр-7, 2023. 320 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7359/1/%d0%90%d0%9d%d0%94%d0%a0%d0%86%d0%87%d0%92_%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f.pdf (дата звернення: 15.08.2025).

43. Цяпа С. М. Загрози та вразливості кібербезпеки в мережових та автономних транспортних системах. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*. 2024. № 6. Том 35(74). С. 244–250. DOI: <https://doi.org/10.32782/2663-5941/2024.6.2/34> (дата звернення: 15.08.2025).

44. Кузьменко О. В., Сергєєва О. Р., Орлова В. М. Використання інформаційних систем в управлінні торговельним підприємством: оцінка ефективності та перспективи впровадження. *Економіка та суспільство*. 2025. Вип. 74. DOI: <https://doi.org/10.32782/2524-0072/2025-74-156> (дата звернення: 15.08.2025).

45. Що таке Power BI: можливості для бізнес-аналітики. *Kyivstar Business Hub*. 2023. URL: <https://hub.kyivstar.ua/articles/shho-take-power-bi-mozhlyvosti-dlya-biznes-analytyky> (дата звернення: 15.08.2025).

46. Power BI. Впровадження системи бізнес-аналітики (BI). *ABMCloud*. URL: <https://abmcloud.com/uk/abm-soft/bi-analytyka> (дата звернення: 15.08.2025).

47. IBM QRadar SIEM – рішення для централізованої безпеки, аналізу загроз і відповідності. *IBM*. 2024. URL: <https://www.ibm.com/products/qradar-siem> (дата звернення: 15.08.2025).

48. Microsoft Sentinel. Microsoft Azure. URL: <https://azure.microsoft.com/en-us/products/microsoft-sentinel> (дата звернення: 15.08.2025).

49. Splunk Enterprise Security. Splunk. URL: https://www.splunk.com/en_us/software/enterprise-security.html (дата звернення: 15.08.2025).

50. ERP-системи: переваги та приклади впровадження. *Webnauts*. 2024. URL: <https://webnauts.pro/uk/blog/erp-systemy-perevagy-ta-pryklady-vprovadzhennya> (дата звернення: 15.08.2025).

51. Sontan A. D., Samuel S. V. Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review. *Computer Science & IT Research Journal*. 2024. Vol. 5, No. 3. P. 576–593. URL: https://www.researchgate.net/publication/378858052_Emerging_Trends_in_Cybersec

urity_for_Critical_Infrastructure_Protection_A_Comprehensive_Review (дата звернення: 15.08.2025).

52. Crosignani M., Macchiavelli M., Silva A. F. Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. *Journal of Financial Economics*. 2023. Vol. 147, No. 2, pp. 432–448. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0304405X2200246X> (дата звернення: 15.08.2025).

53. Роздопченко В.М. Економічні наслідки цифровізації: трансформація ризиків і показників ефективності підприємства. Сучасні виклики сталого розвитку бізнесу: тези виступів VI Міжнар. наук.-практ. конф. Житомир: Житомирська політехніка, 2025. С. 205–206.

54. Schmitt M. Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with Artificial Intelligence (AI)-Enabled Malware and Intrusion Detection. *Journal of Industrial Information Integration*. 2023. Vol. 36, 100520. DOI: 10.1016/j.jii.2023.100520. URL: <https://arxiv.org/abs/2401.01342> (дата звернення: 15.08.2025).

55. Cloud Computing Risk for the Economy That Many Don't See Coming. Investopedia. 2021. URL: <https://www.investopedia.com/cloud-computing-risk-for-the-economy-11777456> (дата звернення: 15.08.2025).

56. Securing the future: why cybersecurity must be secure by design – and by default. TechRadar Pro. 2023. URL: <https://www.techradar.com/pro/securing-the-future-why-cybersecurity-must-be-secure-by-design-and-by-default> (дата звернення: 15.08.2025).

57. How AI resurrected an unsolved security problem: data sprawl. TechRadar Pro. 2021. URL: <https://www.techradar.com/pro/how-ai-resurrected-an-unsolved-security-problem-data-sprawl> (дата звернення: 15.08.2025).

58. Lattanzio G., Ma Y. Cybersecurity Risk and Corporate Innovation. *Journal of Corporate Finance*. 2023. Vol. 82, No. C. P. 102445. DOI: 10.1016/j.jcorpfin.2023.102445. URL:

<https://www.sciencedirect.com/science/article/abs/pii/S0929119923000949> (дата звернення: 15.08.2025).

59. Chesbrough H.W. Open Innovation: The New Imperative for Creating and Profiting from Technology. Boston, MA: Harvard Business School Press. 2003. Vol. 1. 227 p. URL: https://books.google.com.ua/books/about/Open_Innovation.html?id=4hTRWStFhVgC&redir_esc=y (дата звернення: 15.08.2025).

60. COSO ERM (Enterprise Risk Management). Secureframe Glossary. URL: <https://secureframe.com/frameworks-glossary/coso-erm> (дата звернення: 15.08.2025).

61. Sonjai K. Risk Management Framework (Chapter-4) 2022 COSO, ISO 31000, RISK APPETITE, THREE LINES OF DEFENCE AND RISK MANAGEMENT POLICIES. New Delhi. India 2022. URL: https://www.researchgate.net/publication/361424531_Risk_Management_Framework_Chapter-4_2022_COSO_ISO_31000_RISK_APPETITE_THREE_LINES_OF_DEFENCE_A_ND_RISK_MANAGEMENT_POLICIES (дата звернення: 15.08.2025).

62. Осадча О. О., Роздопченко В. М. Цифровізація бізнес-процесів підприємства як інструмент економічної безпеки. *Вісник Національного університету водного господарства та природокористування*, 2025. Вип. 1(109). С. 136-148. URL: <https://visnyk.nuwm.edu.ua/index.php/econ/article/view/1625> (дата звернення: 15.08.2025).

63. Осадча О.О., Роздопченко В.М. Система управління ризиками як інструмент економічної безпеки підприємства в умовах цифровізації. *Комплексний підхід до модернізації науки: методи, моделі та мультидисциплінарність: матеріали III Міжнародної наукової конференції*, м. Житомир, 18 серпня, 2023 р. / Міжнародний центр наукових досліджень. Вінниця: Європейська наукова платформа, 2023. С. 50–52.

64. Осадча О.О., Роздопченко В.М. Оцінювання показників інноваційної діяльності підприємства та їх використання в системі управління

економічною безпекою. *Вісник НУВГП. Економічні науки*, 2023. Випуск 2. С. 152–160.

65. Роздопченюк В.М. Інтеграція цифрових платформ у систему управління підприємством як чинник зміцнення його економічної безпеки. *Інтелектуальний ресурс сьогодення: наукові задачі, розвиток та запитання: збірник наукових праць з матеріалами V Міжнародної наукової конференції*, м. Чернівці, 29 серпня, 2025 р. / Міжнародний центр наукових досліджень. Вінниця: ТОВ «УКРЛОГОС Груп, 2025. С. 28–30.

66. Роздопченюк В.М. Цифрові ризики та стійкість підприємства як складові економічної безпеки України. *Детермінанти соціально-економічного відновлення держави, регіонів та суб'єктів господарювання: збірник тез доповідей III Міжнародної науково-практичної конференції, присвяченої 50-річчю Навчально-наукового інституту економіки та менеджменту*, м. Рівне, 14 листопада 2025 року. Рівне : НУВГП, 2025. С. 215–218.

67. Spivakovskyy S., Kochubei A., Shebanina O., Sokhatska O., Yaroshenko I., Nych T. The impact of digital transformation on the economic security of Ukraine. *European Proceedings of Social and Behavioural Sciences*. 2021. Volume: 39–5. DOI: 10.25115/eea.v39i5.5040 (дата звернення: 15.08.2025).

68. Brosnan A., Manning E., Whelan A., Singh M., Padwalkar S., O'Brien J., Treacy S. The Digital Transformation Risk Matrix: A Tool for Assessing the Impact/Control Nature of Digital Transformation Risk. *Forty-Fifth International Conference on Information Systems*, Bangkok, Thailand, December 2024. URL: https://www.researchgate.net/publication/384500478_The_Digital_Transformation_Risk_Matrix_A_Tool_for_Assessing_the_ImpactControl_Nature_of_Digital_Transformation_Risk (дата звернення: 15.08.2025).

69. European Commission. Digital Economy and Society Index (DESI) 2024. URL: <https://digital-strategy.ec.europa.eu/en/policies/desi> (дата звернення: 15.08.2025).

70. IMD. World Digital Competitiveness Ranking 2024. URL: <https://www.imd.org/centers/wcc/world-competitiveness-center/> (дата звернення: 15.08.2025).
71. Cornell University, INSEAD, WIPO. Global Innovation Index 2024. URL: <https://www.globalinnovationindex.org> (дата звернення: 15.08.2025).
72. World Economic Forum. Global Competitiveness Index (GCI) 4.0. Available via World Bank Data360 platform: WEF_GCI dataset. URL: https://data360.worldbank.org/en/dataset/WEF_GCI (дата звернення: 15.08.2025).
73. Kelišek A., Studená J., Bugarová K., Hudáková M. The Degree of Risk Management Implementation in Enterprises in the Slovak Republic. *Systems*. 2025. Vol. 13, No. 6. P. 427. DOI: <https://doi.org/10.3390/systems13060427> (дата звернення: 15.08.2025).
74. OECD. Digital Security Risk Management for Economic and Social Prosperity. OECD Publishing, Paris, 2015. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc/9789264245471-en.pdf (дата звернення: 15.08.2025).
75. Kaplan R. S., Norton D. P. The Balanced Scorecard: Measures that Drive Performance. *Harvard Business Review*. 1992. Vol. 70, No. 1. P. 71–79. URL: <https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2> (дата звернення: 15.08.2025).
76. Ionescu Ș., Dumitrescu G., Ioanăș C., Delcea C. Mapping the Landscape of Key Performance and Key Risk Indicators in Business: A Comprehensive Bibliometric Analysis. *Risks*. 2024. Vol. 12, No. 8. Article 125. DOI: 10.3390/risks12080125. URL: <https://www.mdpi.com/2227-9091/12/8/125> (дата звернення: 15.08.2025).
77. Tammineedi R. L. S. Integrating KRIs and KPIs for Effective Technology Risk Management. *ISACA Journal*. 2018. Vol. 4. URL: <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/integrating-kris-and-kpis-for-effective-technology-risk-management> (дата звернення: 15.08.2025).

78. Воскобоева О. В., Ромащенко О. С., Макаренко А. О. Збалансована система показників – ефективний інструмент управління підприємством. *Економіка. Менеджмент. Бізнес*. 2019. № 2. URL: <https://journals.dut.edu.ua/index.php/emb/article/view/2154> (дата звернення: 15.08.2025).

79. Пілецька С. Т., Коритько Т. Ю., Ткаченко Є. В. Модель інтегральної оцінки економічної безпеки підприємства. *Економічний вісник Донбасу*. 2021. № 3(65). С. 56–65. DOI: 10.12958/1817-3772-2021-3(65)-56-65. URL: <https://www.evd-journal.org/випуски/випуск-2021-365/> (дата звернення: 15.08.2025).

80. Ткаченко Т. П., Гречко А. В. Узагальнення методичних підходів оцінювання економічної безпеки промислових підприємств. *Економічний вісник НТУУ «КПІ»*. 2022. № 22. С. 79–82. DOI: 10.20535/2307-5651.22.2022.260154. URL: <https://ev.fmm.kpi.ua/article/view/260154> (дата звернення: 15.08.2025).

81. International Monetary Fund. Ukraine: Request for Purchase Under the Rapid Financing Instrument. IMF Country Report No. 22/2. Washington, DC: IMF, October 2022. URL: <https://www.imf.org/-/media/Files/Publications/CR/2022/English/1UKREA2022002.ash> (дата звернення: 15.08.2025).

82. Національний банк України. Звіт про фінансову стабільність. Грудень 2022 р. Київ: НБУ, 27.12.2022. URL: <https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-gruden-2022-roku> (дата звернення: 15.08.2025).

83. Національний банк України. Звіт про фінансову стабільність. Грудень 2023 р. Київ: НБУ, 22.12.2023. URL: <https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-gruden-2023-roku> (дата звернення: 15.08.2025).

84. OECD. Enhancing resilience by boosting digital business transformation in Ukraine. Paris: Organisation for Economic Co-operation and Development, 2024. URL: https://www.oecd.org/en/publications/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50.html (дата звернення: 11.10.2025).

85. Після вторгнення РФ інтенсивність кібератак на «Укренерго» зросла утричі. *Укрінформ*. 04.04.2022. URL: <https://www.ukrinform.ua/rubric-economy/3450550-pisla-vtorgnenna-rf-intensivnist-kiberatak-na-ukrenergo-zrosla-utrici.html> (дата звернення: 11.10.2025).

86. МХП. Річний звіт за 2023 р. URL: <https://api.next.mhp.com.ua/images/51d31/2ef40/69ea3acbd9a.pdf> (дата звернення: 11.10.2025).

87. Український національний офіс інтелектуальної власності та інновацій (УКРНОІВІ). Статистика щодо охорони прав на винаходи та корисні моделі. URL: <https://ukrpatent.org/uk/articles/statistics> (дата звернення: 11.10.2025).

88. ПАТ «Мотор Січ». Річний звіт за 2021 р. URL: https://motorsich.com/ukr/investors/insha_inform/bux/ (дата звернення: 11.10.2025).

89. IBM. Cost of a Data Breach Report 2024. 2024. URL: <https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf> (дата звернення: 11.10.2025).

90. Allianz Commercial. Allianz Risk Barometer 2025: Cyber incidents remain the top global risk. URL: <https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html> (дата звернення: 11.10.2025).

91. Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., Materne S. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice*. 2022. Vol. 47, No. 3. P. 698–736. DOI: <https://doi.org/10.1057/s41288-022-00266-6> (дата звернення: 11.10.2025).

92. European Commission. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. L 333/1. 27.12.2022. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (дата звернення: 11.10.2025).

93. European Commission. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience

for the financial sector (DORA). Official Journal of the European Union. L 333/1. 27.12.2022. URL: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj> (дата звернення: 11.10.2025).

94. Затонацький Д. А., Горячева К. С. Цифровізація та кіберзахист підприємств критичної інфраструктури за стандартами ЄС. *Фінанси України*. 2025. № 3. С. 77–91. DOI: <https://doi.org/10.33763/finukr2025.03.077> (дата звернення: 11.10.2025).

95. TechRadar. Organizational resilience: We need to think beyond cyber attacks. TechRadar Pro, 21.08.2025. URL: <https://www.techradar.com/pro/organizational-resilience-we-need-to-think-beyond-cyber-attack> (дата звернення: 11.10.2025).

96. Степаненко Р. Д. Потенціал цифрових рішень у підвищенні ефективності ризик-менеджменту підприємства. *Вісник Академії праці, соціальних відносин і туризму*. Серія: економіка, психологія та управління. 2025. № 5. DOI: <https://doi.org/10.54929/3041-2390-2025-05-01-05> (дата звернення: 11.10.2025).

97. Kolodiziev O., Shcherbak V., Kostyshyna T., Krupka M., Riabovolyk T., Androshchuk I., Kravchuk N. Digital transformation as a tool for creating an inclusive economy in Ukraine during wartime. *Problems and Perspectives in Management*. 2024. Vol. 22, Issue 3. P. 440–457. DOI: [https://doi.org/10.21511/ppm.22\(3\).2024.34](https://doi.org/10.21511/ppm.22(3).2024.34) (дата звернення: 11.10.2025).

98. Шишкіна О., Бойчук Т., Євчук Д. Вплив цифрових технологій на фінансовий ризик-менеджмент та безпеку транспортних і аграрних підприємств. *Проблеми і перспективи економіки та управління*. 2025. № 2 (42). С. 337–360. DOI: [https://doi.org/10.25140/2411-5215-2025-2\(42\)-337-360](https://doi.org/10.25140/2411-5215-2025-2(42)-337-360) (дата звернення: 11.10.2025).

99. Климчук М. М., Ачкасов І. А., Климчук С. А., Поляк О. П. Вплив ризик-менеджменту на формування стратегії управління бізнес-процесами підприємства в умовах цифрової економіки: міжнародний досвід. *Бізнес-Інформ*.

2021. № 1 (516). С. 272–278. DOI: 10.32983/2222-4459-2021-1-272-278 (дата звернення: 11.10.2025).

100. Богуславська С., Бондар Ю., Фесун С. Теоретико-методологічні основи наукових досліджень ризик-орієнтованого стратегічного управління в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2024. № 3 (12). С. 3–7. DOI: <https://doi.org/10.32782/dees.12-1> (дата звернення: 11.10.2025).

101. European Union Agency for Cybersecurity (ENISA). How to Set Up CSIRT and SOC: Good Practice Guide. December 2020. 57 p. ISBN 978-92-9204-410-7; DOI 10.2824/056764 (дата звернення: 11.10.2025).

102. Роздопченко В. М. Синергія ключових індикаторів ефективності та ризику у забезпеченні стійкості підприємств до цифрових викликів. *Міжнародний науковий журнал «Грааль науки»*. № 55 (серпень, 2025). С. 186–192.

103. Board of Governors of the Federal Reserve System. Dodd-Frank Act Stress Tests 2025. URL: <https://www.federalreserve.gov/supervisionreg/dfa-stress-tests.htm> (дата звернення: 11.10.2025).

104. National Cyber Security Centre. Cyber Essentials scheme: overview. 2025. URL: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (дата звернення: 11.10.2025).

105. IASME. What are the benefits of Cyber Essentials? 2025. URL: <https://iasme.co.uk/articles/what-are-the-benefits-of-cyber-essentials> (дата звернення: 11.10.2025).

106. Department for Science, Innovation and Technology. Cyber Essentials scheme impact evaluation. 2024. URL: <https://www.gov.uk/government/publications/cyber-essentials-scheme-impact-evaluation> (дата звернення: 11.10.2025).

107. Osadcha O., Levytska S., Zinkevych O., Rozdopcheniuk V. and Didukh R. Formation of a resilient economy through the integration of digital risk management and “green” modernization of enterprises. *5th International Conference on Environmental Sustainability in Natural Resources Management (ISCES 2025)*. IOP

Conf. Ser.: Earth Environ. Sci. Volume 1576, 012002. DOI 10.1088/1755-1315/1576/1/012002 (дата звернення: 11.10.2025).

108. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape: Finance Sector. 21 February 2025. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector> (дата звернення: 11.10.2025).

109. European Commission. NIS2 Directive: securing network and information systems. Digital Strategy. URL: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> (дата звернення: 11.10.2025).

110. European Commission. NIS2: Commission Implementing Regulation on critical entities and networks (factsheet/огляд імплементаційного акту, включно з посиланнями на Regulation (EU) 2024/2690 від 17.10.2024). URL: <https://digital-strategy.ec.europa.eu/en/library/directive-measures-high-common-level-cybersecurity-across-union-0> (дата звернення: 11.10.2025).

111. European Union Agency for Cybersecurity (ENISA). NIS2 Technical Implementation Guidance. 26 June 2025. URL: <https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance> (дата звернення: 11.10.2025).

112. METI & IPA. Cybersecurity Management Guidelines Ver. 3.0. METI, 2023. URL: https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v3.0_en.pdf (дата звернення: 11.10.2025).

113. METI. Revision highlights of Cybersecurity Management Guidelines Ver. 3.0. METI, 2023. URL: https://www.meti.go.jp/english/press/2024/0829_002.html (дата звернення: 11.10.2025).

114. METI. Cybersecurity Guidelines for Energy Resource Aggregation Business Ver. 3.0. 22 May 2025. URL: https://www.meti.go.jp/english/press/2025/0522_001.html (дата звернення: 11.10.2025).

115. Cybersecurity Law of the People's Republic of China. Wikipedia. URL: https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China (дата звернення: 11.10.2025).

116. Data Security Law of the People's Republic of China. Wikipedia. URL: https://en.wikipedia.org/wiki/Data_Security_Law_of_the_People%27s_Republic_of_China (дата звернення: 11.10.2025).

117. Personal Information Protection Law of the People's Republic of China. Wikipedia. URL: https://en.wikipedia.org/wiki/Personal_Information_Protection_Law_of_the_People%27s_Republic_of_China (дата звернення: 11.10.2025).

118. State Council of PRC. Regulations on Network Data Security Management. URL: <https://app.glueup.cn/resources/protected/edm/77894/c547bc85-1ea6-4d6c-9842-e3bacbbcd3a1.pdf> (дата звернення: 11.10.2025).

119. Reuters. China to increase protections against hacking for key industries. 26 February 2024. URL: <https://www.reuters.com/technology/cybersecurity/china-increase-protections-against-hacking-key-industries-2024-02-26/> (дата звернення: 11.10.2025).

120. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/go/2163-19> (дата звернення: 11.10.2025).

121. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/go/4336-20> (дата звернення: 11.10.2025).

122. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядження КМУ від 07.03.2025 № 204-р. Урядовий портал. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-2025-rik-z-realizatsii-stratehii-kiberbezpeky-t70325> (дата звернення: 11.10.2025).

123. CERT-UA. Урядова команда реагування на комп'ютерні надзвичайні події України. URL: <https://cert.gov.ua/> (дата звернення: 11.10.2025).

124. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : Постанова Правління НБУ від 11.06.2018 № 64. Офіційний сайт НБУ. URL: https://bank.gov.ua/ua/legislation/Resolution_11062018_64 (дата звернення: 11.10.2025).

125. Про застосування норм Положення № 64 : Повідомлення НБУ від 12.09.2018 № 22-0006/49411. Офіційний сайт НБУ. URL: https://bank.gov.ua/admin_uploads/law/12092018_49411.pdf (дата звернення: 11.10.2025).

126. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Правління НБУ від 28.09.2017 № 95. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/go/v0095500-17> (дата звернення: 11.10.2025).

127. Про затвердження Положення про організацію кіберзахисту в банківській системі України : Постанова Правління НБУ від 12.08.2022 № 178. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/go/v0178500-22> (дата звернення: 11.10.2025).

128. USAID. Cybersecurity for Critical Infrastructure in Ukraine: Review of the Regulatory Framework for Critical Infrastructure Cybersecurity. 22.10.2021. URL: <https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2021-10-22-USAID-USAID-Cybersecurity-Critical-Infrastructure-Ukraine-Regulatory-Framework-via-website.pdf> (дата звернення: 11.10.2025).

129. Про затвердження Змін до деяких нормативно-правових актів НБУ з питань інформаційної безпеки та кіберзахисту : Постанова Правління НБУ від 25.02.2025 № 24. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/go/v0024500-25> (дата звернення: 11.10.2025).

130. НБУ. Організаційна структура системи управління ризиками (презентаційні матеріали до Положення № 64). 19.09.2018. URL:

https://bank.gov.ua/admin_uploads/article/Organizacijna_struktura_sistemi_upravlinn_ua_rizikami_2018-09-18_19_pr.pdf (дата звернення: 11.10.2025).

131. НБУ. Офіційний сайт Центру кіберзахисту НБУ. URL: <https://cyber.bank.gov.ua/> (дата звернення: 11.10.2025).

132. Офіційний сайт Центру кіберзахисту НБУ. Послуги для банків. URL: <https://cyber.bank.gov.ua/bankam> (дата звернення: 11.10.2025).

133. НБУ. Звіт про фінансову стабільність. Червень 2025 року. URL: <https://bank.gov.ua/ua/stability/report> (дата звернення: 11.10.2025).

134. У КНПФ НБУ впроваджено комплексну систему управління фінансовими ризиками. Корпоративний недержавний пенсійний фонд НБУ. Офіційний сайт КНПФ НБУ. URL: https://knpf.bank.gov.ua/uchasnykam/pro_fond/novyny/novyna12.html (дата звернення: 11.10.2025).

135. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 11.10.2025).

136. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR). Official Journal of the European Union. 2016. L 119. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 11.10.2025).

137. Проект Закону України «Про захист персональних даних» № 8153 від 25.10.2022. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707> (дата звернення: 11.10.2025).

138. Про прийняття за основу проекту Закону України про захист персональних даних : Постанова Верховної Ради України від 20.11.2024 № 4065-IX. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/go/4065-IX> (дата звернення: 11.10.2025).

139. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/447/2021> (дата звернення: 11.10.2025).

140. Cyber Essentials : Government-backed certification scheme. National Cyber Security Centre (UK). URL: <https://www.ncsc.gov.uk/cyberessentials/overview> (дата звернення: 11.10.2025).

141. Cyber Essentials brochure. National Cyber Security Centre (UK). 2025. 8 р. URL: <https://www.ncsc.gov.uk/files/Cyber-Essentials-brochure.pdf> (дата звернення: 11.10.2025).

142. Ukraine Human Development Update. Washington, DC : World Bank, May 2024. URL: <https://openknowledge.worldbank.org/bitstreams/ca0a8b70-880c-413f-a050-f349a122f1ff/download> (дата звернення: 11.10.2025).

143. Digitalisation for Recovery in Ukraine. OECD. Paris, 2022. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/digitalisation-for-recovery-in-ukraine_40746fbc/c5477864-en.pdf (дата звернення: 11.10.2025).

144. Про Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України – офіційний опис діяльності Центру із сайту spravdi.gov.ua. URL: <https://spravdi.gov.ua/pro-nas/> (дата звернення: 11.10.2025).

145. Кіберзахист енергосектору: у 2022 році заблоковано понад 1,5 млн спроб атакувати галузь. Урядовий портал : офіційний вебсайт. 30.06.2023. URL: <https://www.kmu.gov.ua/news/kiberzakhyst-enerhosektoru-u-2022-rotsi-zablokovano-ponad-15-mln-sprob-atakuvaty-haluz> (дата звернення: 11.10.2025).

146. Український ринок кібербезпеки зріс у чотири рази за вісім років. Європейська бізнес асоціація (ЕБА). 07.01.2025. URL: <https://eba.com.ua/ukrayinskyj-rynok-kiberbezpeky-zris-u-chotyry-razy-za-visim-rokiv/> (дата звернення: 11.10.2025).

147. Russia Attacked Ukraine's Power Grid at Least 66 Times to 'Freeze It Into Submission'. Wired, 29 лютого 2024 р. URL: <https://www.wired.com/story/russia-ukraine-power-war-crimes> (дата звернення: 11.10.2025).

148. Річний аналітичний огляд 2024. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf (дата звернення: 11.10.2025).

149. European Commission. Europe's Digital Decade: digital targets for 2030. Policy programme page. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (дата звернення: 11.10.2025).

150. OECD. 2023 OECD Digital Government Index (DGI). Paris: OECD Publishing, 19.01.2024. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/01/2023-oecd-digital-government-index_b11e8e8e/1a89ed5e-en.pdf (дата звернення: 18.12.2025).

151. OECD. Digital transformation – Going Digital Measurement Roadmap. URL: <https://www.oecd.org/en/topics/digital-transformation.html> (дата звернення: 18.12.2025).

152. Роздопченюк В.М. Аналіз показників інноваційної діяльності підприємства. *Проблеми та перспективи розвитку сучасної науки : збірник тез доповідей Міжнародної науково-практичної конференції молодих науковців, аспірантів і здобувачів вищої освіти*, м. Рівне, 11–12 травня 2023 року. Рівне : НУВГП, 2023. С. 373–376.

153. Осадча О.О., Роздопченюк В.М. Забезпечення економічної безпеки через цифрову трансформацію підприємства. *Наукові тренди постіндустріального суспільства: збірник наукових праць з матеріалами IX Міжнародної наукової конференції*, м. Тернопіль, 21 березня, 2025 р. / Міжнародний центр наукових досліджень. Вінниця: ТОВ «УКРЛОГОС Груп, 2025. С. 71–74.

154. Роздопченюк В.М. Цифрова трансформація бізнес-процесів як детермінанта економічної безпеки підприємства в умовах цифровізації економіки України. *Актуальні проблеми теорії і практики менеджменту в контексті євроінтеграції: Збірник матеріалів XIV Міжнародної науково-практичної конференції*, 22 травня 2025 р. Рівне : НУВГП, 2025. С. 707–709.

155. Бланк І. А. Фінансовий менеджмент: навч. посіб. 3-тє вид., перероб. і доп. Київ: Ніка-Центр, 2021. 720 с.

156. Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. Львів: Арал, 2008. 384 с.

157. Горячева К. С. Фінансова безпека підприємства: сутність та місце в системі економічної безпеки. *Економіст*. 2003. № 8. С. 65–67.

158. Терещенко О. О. Фінансова діяльність суб'єктів господарювання : навч. посіб. Київ : Вид-во КНЕУ, 2003. 554 с.

159. Поддєрьогін А. М., Білик М. Д., Буряк Л. Д. та ін. Фінанси підприємств : підручник. Київ : КНЕУ, 2008. 552 с.

160. Осадча О. О., Роздопченюк В. М. Інтегральне оцінювання економічної безпеки підприємств в умовах цифрової трансформації економіки. *Грааль науки : міжнародний науковий журнал*. 2026. № 64 (березень). С. 260–267. DOI 10.36074/grail-of-science.20.03.2026.027 (дата звернення: 08.04.2026).

161. Савицька Г. В. Економічний аналіз діяльності підприємства : навч. посіб. 3-тє вид., випр. і доп. Київ : Знання, 2007. 668 с.

162. Роздопченюк В. М. Методичні підходи до оцінювання економічної безпеки підприємств у цифровій економіці. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*, 2025. Випуск №: 2 (72). С. 77–87.

163. Nardo M., Saisana M., Saltelli A., Tarantola S., Hoffman A., Giovannini E. Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD Publishing, 2008. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2008/08/handbook-on-constructing-composite-indicators-methodology-and-user-guide_g1gh9301/9789264043466-en.pdf (дата звернення: 08.04.2026).

164. Григорук П. М. Теоретико-методологічні засади інтегрального оцінювання ефективності маркетингових рішень. *Економіка: реалії часу. Науковий журнал*. 2013. № 3 (8). С. 194–201. URL: <http://economics.opu.ua/files/archive/2013/n3.html> (дата звернення: 08.04.2026).

165. Shannon C. E. A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948. Vol. 27. P. 379–423, 623–656. URL: <https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf> (дата звернення: 08.04.2026).

166. Shannon C. E., Weaver W. The Mathematical Theory of Communication. *Urbana* : University of Illinois Press, 1949. URL: https://pure.mpg.de/pubman/item/item_2383164_3/component/file_2383163/Shannon_Weaver_1949_Mathematical.pdf (дата звернення: 08.04.2026).

167. Kumar R., Singh S., Bilga P. S., Jatin, Singh J., Singh S., Scutaru M.-L., Pruncu C. I. Revealing the benefits of entropy weights method for multi-objective optimization in machining operations: A critical review. *Journal of Materials Research and Technology*. 2021. Vol. 10. P. 1471–1492. URL: <https://www.sciencedirect.com/science/article/pii/S2238785420321918> (дата звернення: 08.04.2026).

168. Класифікація видів економічної діяльності ДК 009:2010: постанова (наказ) зі змінами. Верховна Рада України. Постанова від 11.10.2010 № 457. Законодавство України. URL: <https://zakon.rada.gov.ua/rada/show/vb457609-10#Tex> (дата звернення: 08.04.2026).

169. Наказ Державної служби статистики України «Про затвердження Класифікації видів економічної діяльності NACE 2.1-UA» від 28.10.2025 № 191. Офіційний вебсайт Держстату. URL: <https://stat.gov.ua/uk/page-contents/nakaz-vid-28102025-no191> (дата звернення: 08.04.2026).

170. Wickham H., Stryjewski L. 40 years of boxplots. *The American Statistician*. 2011. Vol. 65, No. 4. URL: <https://vita.had.co.nz/papers/boxplots.pdf> (дата звернення: 08.04.2026).

171. Cox N. J. Speaking Stata: Creating and varying box plots. *The Stata Journal*. 2009. Vol. 9, No. 3. P. 478–496. URL: <https://journals.sagepub.com/doi/pdf/10.1177/1536867X0900900309> (дата звернення: 08.04.2026).

172. Державна служба статистики України. Єдиний державний вебпортал відкритих даних. URL: https://data.gov.ua/dataset/a175d37b-6f7f-4ca0-b85f-37e9497a768f/resource/dec87ae2-fa34-4942-8814-9d544cb146d4?filter=all_time (дата звернення: 11.03.2026).

173. Wooldridge J. M. *Econometric Analysis of Cross Section and Panel Data*. Cambridge (MA): MIT Press, 2010. URL: https://new.mmf.lnu.edu.ua/wp-content/uploads/2018/03/wooldridge_cross_section_and_panel_data.pdf (дата звернення: 08.04.2026).

174. Croissant Y., Millo G. *Panel Data Econometrics with R*. Hoboken: Wiley, 2019. URL: https://cran.r-project.org/web/packages/plm/vignettes/A_plmPackage.html (дата звернення: 08.04.2026).

175. Hausman J. A. Specification Tests in Econometrics. *Econometrica*. 1978. Vol. 46, No. 6. P. 1251–1271. URL: <https://www.jstor.org/stable/1913827> (дата звернення: 08.04.2026).

176. Волошин О.Р., Галайко Н.В. Е40 Економетрія. Ч. 1: навч. посібник / О. Волошин, Н. Галайко. Львів: Львівський державний університет внутрішніх справ, 2012. 192 с.

177. Hyndman R. J., Koehler A. B. Another look at measures of forecast accuracy. *International Journal of Forecasting*. 2006. URL: <https://robjhyndman.com/papers/mase.pdf> (дата звернення: 08.04.2026).

178. Kim S., Kim H. A new metric of absolute percentage error for intermittent demand forecasts. *International Journal of Forecasting*. 2016. URL: <https://www.sciencedirect.com/science/article/pii/S0169207016000121> (дата звернення: 08.04.2026).

179. Макроекономічне прогнозування : навч. посібник : у двох ч. К. : Видавничий дім «Києво-Могилянська академія», 2015. Ч. 1. 176 с. URL: https://ekmair.ukma.edu.ua/bitstream/handle/123456789/9090/Shumska_macroekonomiche_prohnozuvannia.pdf (дата звернення: 08.04.2026).

180. Сосновська Є. Р., Скіцько В. І. Розв'язання економетричних задач із застосуванням моделей генеративного штучного інтелекту: порівняльний аналіз ChatGPT та Gemini. *Проблеми економіки*. 2025. № 4 (66). С. 428–442. URL: https://www.problecon.com/export_pdf/problems-of-economy-2025-4_0-pages-428_442.pdf (дата звернення: 08.04.2026).

181. Hyndman R. J., Athanasopoulos G. *Forecasting: Principles and Practice*. 3rd ed. Melbourne: OTexts, 2021. URL: <https://otexts.com/fpp3/> (дата звернення: 08.04.2026).

182. Осадча О., Роздопченко В. Формування системи показників оцінювання економічної безпеки підприємства в умовах цифрової трансформації. *New paradigms of interdisciplinary research: theories, ideas and developments : proceedings of the 19th International scientific and practical conference*, Prague, Czech Republic, May 12–15, 2026. Prague : International Science Group, 2026. С. 101–104.

ДОДАТКИ

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

**Статті в періодичних наукових виданнях, проіндексованих
у базі даних «Scopus»:**

1. Osadcha O., Levytska S., Zinkevych O., Rozdopcheniuk V. and Didukh R. Formation of a resilient economy through the integration of digital risk management and “green” modernization of enterprises. 5th International Conference on Environmental Sustainability in Natural Resources Management (ISCES 2025). IOP Conf. Ser.: Earth Environ. Sci. Volume 1576, 012002. DOI 10.1088/1755-1315/1576/1/012002 (особистий внесок здобувача – систематизовано ризики економічної безпеки підприємств з урахуванням цифрових та екологічних чинників, обґрунтовано інтеграцію індикаторів KPI/KRI у контексті «twin transition» та визначено підхід до оцінювання цифрово-екологічної стійкості підприємств; 0,8 / 0,16 ум. д.а.)

Статті у наукових фахових виданнях України:

2. Осадча О. О., Роздопченко В. М. Оцінювання показників інноваційної діяльності підприємства та їх використання в системі управління економічною безпекою. *Вісник Національного університету водного господарства та природокористування. Сер. «Економічні науки»*, 2023. Випуск 2. С. 152-160. URL: <https://visnyk.nuwm.edu.ua/index.php/econ/article/view/1380> (особистий внесок здобувача – систематизовано та узагальнено показники інноваційної діяльності підприємства, обґрунтовано критерії їх відбору та визначено їх роль у формуванні інформаційної бази управління економічною безпекою; 0,6 / 0,3 ум. д.а.).

3. Осадча О. О., Роздопченюк В. М. Ризики економічної безпеки підприємства в умовах цифровізації. *Вісник Національного університету водного господарства та природо-користування. Сер. «Економічні науки»*, 2024. Вип. 3(107). С. 116-126. URL: <https://visnyk.nuwm.edu.ua/index.php/econ/article/view/1555> (особистий внесок здобувача – систематизовано та класифіковано ризики економічної безпеки підприємства в умовах цифровізації, обґрунтовано їх ранжування та визначено підхід до групування за типами стійкості підприємства; 0,7 / 0,35 ум. д.а.).

4. Осадча О. О., Роздопченюк В. М. Цифровізація бізнес-процесів підприємства як інструмент економічної безпеки. *Вісник Національного університету водного господарства та природокористування. Сер. «Економічні науки»*, 2025. Вип. 1(109). С. 136-148. URL: <https://visnyk.nuwm.edu.ua/index.php/econ/article/view/1625> (особистий внесок здобувача – обґрунтовано роль цифровізації бізнес-процесів підприємства як інструменту забезпечення економічної безпеки, систематизовано напрями цифрової трансформації та розроблено організаційну модель цифровізації бізнес-процесів; 0,8 / 0,4 ум. д.а.).

5. Роздопченюк В. М. Синергія ключових індикаторів ефективності та ризику у забезпеченні стійкості підприємств до цифрових викликів. *Міжнародний науковий журнал «Грааль науки»*. № 55 (серпень, 2025). С. 186–192. URL: <https://archive.journal-grail.science/index.php/2710-3056/article/view/2907> (0,4 ум. д.а.).

6. Роздопченюк В. М. Методичні підходи до оцінювання економічної безпеки підприємств у цифровій економіці. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*, 2025. Випуск №: 2 (72). С. 77–87. URL: <http://efm.vsau.org/en/particles/methodological-approaches-to-the-assessment-of-enterprises-economic-security-in-the-digital-economy> (0,8 ум. д.а.).

7. Осадча О. О., Роздопченюк В. М. Інтегральне оцінювання економічної безпеки підприємств в умовах цифрової трансформації економіки. *Грааль науки : міжнародний науковий журнал*. 2026. № 64 (березень). С. 260–267.

DOI 10.36074/grail-of-science.20.03.2026.027 (особистий внесок здобувача – обґрунтовано методичний підхід до інтегрального оцінювання економічної безпеки підприємств, сформовано систему показників та визначено процедуру їх нормалізації і агрегування в умовах цифрової трансформації; 0,5 / 0,25 ум. д.а.).

Праці апробаційного характеру:

8. Роздопченюк В. М. Аналіз показників інноваційної діяльності підприємства. *Проблеми та перспективи розвитку сучасної науки : збірник тез доповідей Міжнародної науково-практичної конференції молодих науковців, аспірантів і здобувачів вищої освіти*, м. Рівне, 11–12 травня 2023 року. Рівне : НУВГП, 2023. С. 373–376 (0,2 ум. д.а.).

9. Осадча О. О., Роздопченюк В. М. Система управління ризиками як інструмент економічної безпеки підприємства в умовах цифровізації. *Комплексний підхід до модернізації науки: методи, моделі та мультидисциплінарність: матеріали III Міжнародної наукової конференції*, м. Житомир, 18 серпня 2023 р. / Міжнародний центр наукових досліджень. Вінниця: Європейська наукова платформа, 2023. С. 50–52 (особистий внесок здобувача – систематизовано ризики діяльності підприємства в умовах цифровізації, обґрунтовано роль ризик-менеджменту у забезпеченні економічної безпеки та розроблено алгоритм і структурну модель системи управління ризиками підприємства; 0,2 / 0,1 ум. д.а.).

10. Роздопченюк В. М. Фактори економічної безпеки підприємства. *Modernization of science and its influence on global processes: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference*, September 20, 2024. Bern, Swiss Confederation: International Center of Scientific Research. DOI 10.36074/scientia-20.09.2024. С. 52–54 (0,15 ум. д.а.).

11. Осадча О. О., Роздопченюк В. М. Забезпечення економічної безпеки через цифрову трансформацію підприємства. *Наукові тренди*

постіндустріального суспільства: збірник наукових праць з матеріалами IX Міжнародної наукової конференції, м. Тернопіль, 21 березня, 2025 р. / Міжнародний центр наукових досліджень. Вінниця: ТОВ «УКРЛОГОС Груп, 2025. С. 71–74 (особистий внесок здобувача – обґрунтовано роль цифрової трансформації у забезпеченні економічної безпеки підприємства, систематизовано напрями цифровізації бізнес-процесів та визначено їх вплив на підвищення стійкості та ефективності діяльності підприємства; 0,3 / 0,15 ум. д.а.).

12. Роздопченюк В. М. Цифрова трансформація бізнес-процесів як детермінанта економічної безпеки підприємства в умовах цифровізації економіки України. *Актуальні проблеми теорії і практики менеджменту в контексті євроінтеграції: Збірник матеріалів XIV Міжнародної науково-практичної конференції, 22 травня 2025 р. Рівне : НУВГП, 2025. С. 707–709 (0,15 ум. д.а.).*

13. Роздопченюк В. М. Інтеграція цифрових платформ у систему управління підприємством як чинник зміцнення його економічної безпеки. *Інтелектуальний ресурс сьогодення: наукові задачі, розвиток та запитання: збірник наукових праць з матеріалами V Міжнародної наукової конференції, м. Чернівці, 29 серпня, 2025 р. / Міжнародний центр наукових досліджень. — Вінниця: ТОВ «УКРЛОГОС Груп, 2025. С. 28–30 (0,25 ум. д.а.).*

14. Роздопченюк В. М., Хахльов О. В. Цифрові ризики та стійкість підприємства як складові економічної безпеки України. Детермінанти соціально-економічного відновлення держави, регіонів та суб'єктів господарювання: збірник тез доповідей III Міжнародної науково-практичної конференції, присвяченої 50-річчю Навчально-наукового інституту економіки та менеджменту, м. Рівне, 14 листопада 2025 року. Рівне : НУВГП, 2025. С. 215–218 (особистий внесок здобувача – систематизовано цифрові ризики підприємства у розрізі складових його стійкості, визначено ключові показники ефективності та обґрунтовано взаємозв'язок між ризиками і параметрами економічної безпеки; 0,3 / 0,15 ум. д.а.).

15. Роздопченко В. М. Економічні наслідки цифровізації: трансформація ризиків і показників ефективності підприємства. *Сучасні виклики сталого розвитку бізнесу: тези виступів VI Міжнар. наук.-практ. конф.* Житомир: Житомирська політехніка, 2025. С. 205–206 (0,15 ум. д.а.).

16. Осадча О., Роздопченко В. Формування системи показників оцінювання економічної безпеки підприємства в умовах цифрової трансформації. *New paradigms of interdisciplinary research: theories, ideas and developments : proceedings of the 19th International scientific and practical conference*, Prague, Czech Republic, May 12–15, 2026. Prague : International Science Group, 2026. С. 101–104 (особистий внесок здобувача – обґрунтовано систему показників оцінювання економічної безпеки підприємства на основі фінансових індикаторів; визначено їх роль у подальшому розрахунку інтегрального індексу економічної безпеки підприємства; 0,4 / 0,2 ум. д.а.).

ДОДАТОК Б

Еволюція наукових підходів до визначення поняття «економічна безпека»

Автор	Визначення поняття «економічна безпека»	Джерело
1	2	3
Козаченко Г. В., Понамарьов В. П., Ляшенко О. М.	Гармонізація інтересів підприємства із зацікавленими суб'єктами як елемент економіки сталості	Козаченко Г.В. Економічна безпека підприємства: сутність та механізм забезпечення: монографія / Г. В. Козаченко, В.П. Понамарьов, О. М. Ляшенко. К.: Лібра, 2003. 280 с.
Покропивний С. Ф.	Стан корпоративних ресурсів і можливостей, що забезпечує їх ефективне використання, науково-технічний розвиток і захист від загроз	Економіка підприємства: Підручник / За заг. ред. проф. С.Ф. Покропивного. К.: КНЕУ, 2003. 608 с.
Дацків Р. М.	Стан економічного розвитку суб'єкта господарювання, який забезпечує гармонійний розвиток, ефективне використання шансів і нейтралізацію загроз зовнішнього середовища	Дацків Р. М. Економічна безпека у глобальному вимірі. <i>Актуальні проблеми економіки</i> . 2004. № 7 (37). С. 143–153.
Šimašius R., Vilpišauskas R.	Економічна безпека держави первинно базується на балансі між стійкістю економіки, здатністю забезпечити рівень життя, політичну/соціальну стабільність та відсутність внутрішніх і зовнішніх загроз; включає дві основні моделі – холістичну (цілісність економіки) і індивідуальну (безпека окремої людини)	Remigijus Šimašius, Ramūnas Vilpišauskas. The Concept of Economic Security and the Principles of Economic Security Policy in Lithuania, <i>Lithuanian Annual Strategic Review</i> , 2005, no. 1, 249-266. DOI 10.47459/lasr.2005.3.12
Шевченко Л. С., Гриценко О. А., Макуха С. М.	Сукупність механізмів, інститутів і ресурсів, що забезпечують здатність країни протистояти зовнішнім і внутрішнім загрозам, зберігати економічний суверенітет, здійснювати соціально-економічний розвиток, гарантуючи стабільність інститутів та захист інтересів нації	Шевченко Л. С., Гриценко О. А., Макуха С. М. та ін. Економічна безпека держави: теоретичні основи та напрями формування. Київ: Право, 2009. 312 с. URL: https://library.nlu.edu.ua/POLN_TEX/T/MONOGRFII_2010/Shevchenko_2009.pdf

Продовження Додатку Б

1	2	3
Мішин О. Ю., Мішина С. В.	Стан виробничо-комерційної діяльності, за якого забезпечується реалізація економічних інтересів підприємства завдяки його стійкості та властивостям системи, що саморозвивається, а також запобігання впливу внутрішніх і зовнішніх загроз	Мішин О. Ю., Мішина С. В. Сутність поняття "економічна безпека підприємства". <i>Вісник економіки транспорту і промисловості</i> . 2012. Вип. 38 (додаток). С. 86-92. URL: http://nbuv.gov.ua/UJRN/Vetp_2012_38(dodatok)_19
Лисенко М.	Система ефективного використання ресурсів, захисту від загроз і забезпечення розвитку	Marianna Lysenko, The Problem of Ensuring the Economic Security of Dairy Industry in Ukraine, <i>Economics & Sociology</i> , Vol. 7, No 2, 2014, pp. 160-171. DOI: 10.14254/2071-789X.2014/7-2/13
Цвігун Т. В.	Економічна безпека передбачає спроможність національної економіки забезпечити свій незалежний розвиток, стабільність інститутів громадянського суспільства, достатній оборонний потенціал держави за різних несприятливих умов, а також здатність країни захистити власні інтереси від зовнішніх і внутрішніх загроз	Цвігун Т. В. Економічна безпека в системі національної безпеки України. Економіка і суспільство. 2017. Вип. 11. С. 150–156. URL: https://economyandsociety.in.ua/journals/11_ukr/24.pdf
Живко З. Б., Черевко О. В., Копитко М. І., Зачосова Н. В., Живко М. О., Серeda В. В., Занора В. О., Бісєвець А. В.	Система складових (енергетична, фінансова, продовольча, інформаційна та інші), що забезпечує стійкість національної економіки, захист національних економічних інтересів і розвиток в умовах зовнішніх та внутрішніх викликів	Живко З. Б., Черевко О. В., Копитко М. І., Зачосова Н. В., Живко М. О., Серeda В. В., Занора В. О., Бісєвець А. В. Економічна безпека держави: навчально-методичний посібник. Черкаси: Чабаненко Ю. А., 2019. 240 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3466/1/%D0%9D%D0%9C%D0%9F_%D0%95%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B8.pdf

Продовження Додатку Б

1	2	3
Коленда Н. В.	Характеристика суб'єкта господарювання, що відображає здатність реалізувати власні стратегічні інтереси під зовнішніми умовами	Коленда Н. В. Поняття соціально-економічної безпеки підприємства. <i>Демографія, економіка праці, соціальна економіка і політика</i> . Мукачівський Державний Університет ім. Лесі Українки, 2019. URL: https://economyandsociety.in.ua/journals/7_ukr/113.pdf
Лопатка К. А., Шаранова Ю. Г.	Здатність забезпечити сталий розвиток і протидіяти внутрішнім та зовнішнім загрозам у мінливому середовищі	Лопатка К. А., Шаранова Ю. Г. Економічна безпека як економічна категорія: огляд наукових публікацій. <i>Економічний простір</i> . 2019. № 148. С. 5–18. URL: https://prostir.pdaba.dp.ua/index.php/journal/article/view/147
Ковальчук А. М.	Стан захищеності від негативного впливу зовнішніх та внутрішніх загроз, дестабілізуючих чинників, за якого забезпечується стійка реалізація основних комерційних інтересів та цілей діяльності підприємства	Ковальчук А. М. Фінансово-економічна безпека підприємства в контексті адаптації до викликів цифрового середовища. <i>Економічний вісник. Економіка підприємства</i> , 2020. № 3. С. 152–159. URL: https://ev.nmu.org.ua/docs/2020/3/EV20203_152-159.pdf
Солодовнік О. О.	Інтегральна характеристика стану підприємства, яка виявляється у його здатності захищати економічні інтереси та ефективно функціонувати в умовах ризиків	Солодовнік О. О. Основні підходи до оцінювання економічної та фінансової безпеки: сутність і напрями вдосконалення. <i>Бізнес Інформ</i> . 2021. № 2. С. 6–12. URL: https://www.business-inform.net/export_pdf/business-inform-2021-2_0-pages-6_12.pdf
Боса І.	Суб'єктивно усвідомлений стан захищеності від актуальних загроз, що залежить від використання ресурсів та формування зон можливостей для розвитку	Боса І. Етимологія поняття «економічна безпека підприємства» та авторське визначення. <i>Вісник Хмельницького національного університету. Серія: Економічні науки</i> . 2022. Том 312(6(2)). С. 300–308. URL: https://www.business-inform.net/export_pdf/business-inform-2021-2_0-pages-6_12.pdf
Деменко К. Е.	Результат діяльності держави, стан економіки, здатний забезпечити стійкість держави та стабільність її механізму до зовнішніх і внутрішніх загроз і дестабілізуючих актів інших держав	Деменко К. Е. Щодо поняття «економічна безпека держави» як політико-правової категорії. Наукові записки Львівського університету бізнесу та права. Серія: Економічна та юридична, 2022, № 33. С. 282–288. URL: https://nzlubp.org.ua/index.php/journal/article/download/773/701

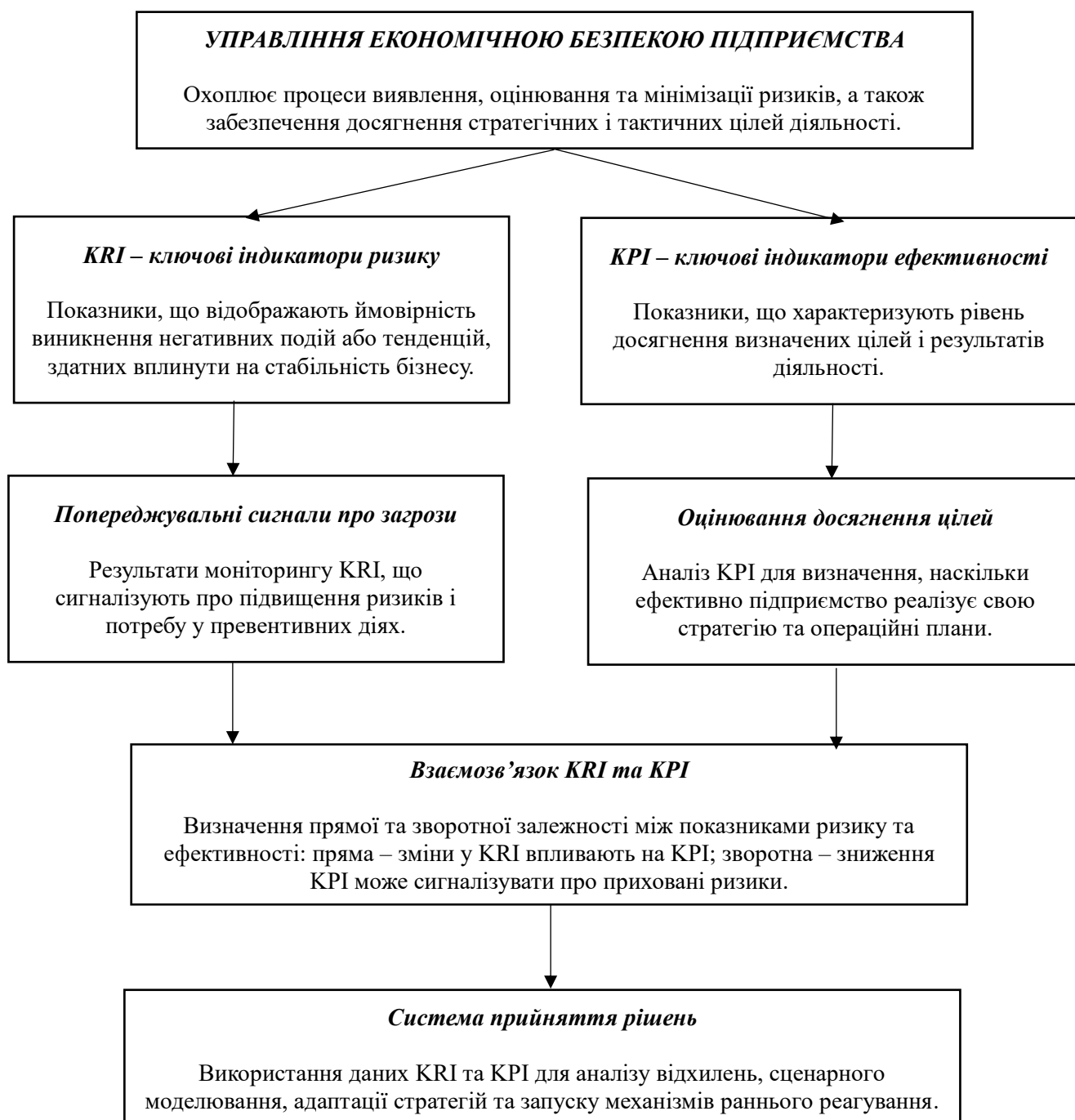
Продовження Додатку Б

1	2	3
Калинюк В. Є.	Стан, при якому суб'єкт господарювання здатен підтримувати конкурентоспроможність, стійкість і розвиток через системне управління, стійкість до загроз та ефективне використання ресурсів у довгостроковій перспективі	Калинюк В. Є. Сучасні наукові підходи до визначення сутності поняття «економічна безпека підприємства». <i>Бізнес Інформ</i> . 2022. № 12. С. 221–228. DOI: 10.32983/2222-4459-2022-12-221-228. URL: https://www.business-inform.net/export_pdf/business-inform-2022-12_0-pages-221_228.pdf
Самойленко Ю., Бритченко І., Левченко Я. та ін.	Здатність підприємства адаптуватися до цифрових викликів, зберігаючи фінансову стійкість через інтегровану систему управління	Yuliia Samoilenko, Igor Britchenko, Iaroslava Levchenko, Peter Lošonczi, Oleksandr Bilichenko, Olena Bodnar. Economic Security of the Enterprise Within the Conditions of Digital Transformation. <i>Economic Affairs</i> . Vol. 67. No. 04, September. 2022, pp. 619-629.
Загородня А. С.	Стан захищеності та стійкості підприємства від ризиків в умовах високого рівня управління та комплексного підходу до забезпечення безпеки його діяльності, що полягає у ефективному використанні ресурсів, управлінні ризиками та здатності протистояти зовнішнім і внутрішнім загрозам	Загородня А. С. Формування механізму управління економічною безпекою підприємств. Дисертація на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент» (07 «Управління та адміністрування»). Національний університет біоресурсів і природокористування України. Київ, 2023. URL: https://nubip.edu.ua/sites/default/files/u145/dis_zagorodnya.pdf
Christie E. H., Wigell M.	Економічна безпека аналізується через призму "геоекономічної дилеми", де її роль розглядається як інструмент стримування, союзів і протидії економічному примусу в міжнародній сфері	Christie E. H., Wigell M. The Economic Security Dilemma. NDU Press. 2023. DOI: (частина книжки). URL: https://ndupress.ndu.edu/Portals/68/240805_2_Christie-Wigell%20-%20Econ%20Sec%20Dilemma%20-%20MM.pdf
Черевко І., Фляк Ю.	Поліструктурне поняття, що охоплює безпеку соціально-економічних систем різних рівнів ієрархії, які характеризують стійкість, незалежність, здатність до самовідтворення та забезпечення інтересів широкого кола зацікавлених сторін	Черевко І., Фляк Ю. Економічна безпека: сутність, значення і детермінанти. <i>Аграрна економіка</i> , 2024, № 17(1), С. 3–16. URL: http://www.agrarianeconomy.inup.edu.ua/index.php/en/component/content/article/68-arkhiv-nomeriv/2024-t-17-1/548-1

Продовження Додатку Б

1	2	3
Tagliapietra S., Trasi C.	Інтеграція політичної економії та міжнародних відносин, визначаючи політичні аспекти захисту національних інтересів у глобальному контексті	Tagliapietra S., Trasi C. How Should Europe Think About Economic Security? <i>Intereconomics</i> , 2024. URL: https://www.intereconomics.eu/contents/year/2024/number/2/article/how-should-europe-think-about-economic-security.html
Yuzue N., Sekiyama T.	Захист виживання нації та її суверенітету, а також економічного процвітання від загроз постачання ключових ресурсів, технологічної залежності та втрати технологій	Yuzue N., Sekiyama T. Defining economic security through literature review. <i>Frontiers in Political Science</i> , 2025, Vol. 7:1501986. URL: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1501986/full

Логіко-структурна модель взаємозв'язку KRI та KPI у системі управління економічною безпекою підприємства



ДОДАТОК Д

Порівняльний аналіз економічних аспектів цифрового ризик-менеджменту (США – ЄС – Азія – Україна)

Регіон / Країна	Методологія	Сильні сторони	Обмеження	Можливості імплементації в Україні
США	Рамка NIST Cybersecurity Framework; stress-testing у фінансовому секторі (CCAR, DFAST).	Системність управління ризиками з інтеграцією у корпоративне планування та макропруденційний нагляд. Економічна перевага – прогнозування втрат і визначення потреб у капіталі для збереження стабільності.	Висока вартість впровадження; складність адаптації для малого та середнього бізнесу; залежність від специфіки американського фінансового ринку.	Використання NIST як орієнтиру для великих підприємств; запровадження адаптованих stress-testing у фінансовому секторі та управлінні критичною інфраструктурою.
ЄС	ENISA Threat Landscape; Директива NIS2.	Секторальна аналітика загроз; нормативне закріплення управління ризиками; санкційні стимули до інвестування у безпеку; підзвітність керівництва.	Високі витрати на відповідність; складність для малого та середнього бізнесу; необхідність регулярного оновлення стандартів.	Створення національних звітів «ландшафт загроз»; гармонізація із NIS2; формування секторальних методик для стратегічних галузей.
Азія (Японія, Китай)	Японія: Guidelines for Cybersecurity Management (METI, IPA). Китай: Cybersecurity Law (2016), Data Security Law (2021), Personal Information Protection Law (2021).	У Японії – інтеграція кібербезпеки у корпоративне управління та нефінансову звітність (ESG). У Китаї – законодавче визначення категорій даних і масштабні програми підготовки кадрів.	У Японії – добровільність стандартів. У Китаї – жорсткий контроль, що може стримувати інновації; високі витрати на відповідність.	Для України – включення кіберризиків у корпоративну звітність (як у Японії); класифікація даних і національні «кібернавчання» у стратегічних секторах (як у Китаї).
Україна	Закон України «Про основні засади забезпечення кібербезпеки» (2017); Стратегія економічної безпеки до 2025 року; нормативні акти НБУ (Положення № 64, № 95, № 178, № 24); діяльність CERT-UA та CSIRT-NBU.	Високий рівень нормативної деталізації у фінансовому секторі; функціонування CERT-UA і CSIRT-NBU; міжнародна інтеграція; гармонізація з європейськими стандартами.	Нерівномірність розвитку між секторами; відсутність секторальних методик поза фінансовим сектором; брак економічних стимулів для бізнесу.	Розроблення секторальних методик для промисловості, енергетики та агропромислового комплексу; розвиток страхування кіберризиків і податкових стимулів; запровадження stress-testing.

ДОДАТОК Е

Динаміка показників економічної безпеки ПрАТ «НЕК «Укренерго» у 2020–2024 роках

Група показників	Показник	2020	2021	2022	2023	2024
Фінансова стійкість	Коефіцієнт автономії	0,128	0,108	0,026	0,269	0,049
	Коефіцієнт фінансового левириджу	6,80	8,28	38,15	2,72	19,44
	Покриття необоротних активів власним капіталом	0,181	0,172	0,047	0,435	0,071
Ліквідність і платоспроможність	Коефіцієнт поточної ліквідності	0,38	0,87	0,76	0,95	0,38
	Коефіцієнт швидкої ліквідності	0,37	0,86	0,74	0,94	0,37
	Чистий оборотний капітал, тис. грн	–33 313 000	–5 191 984	–14 201 117	–3 351 219	–89 265 409
Рентабельність	Рентабельність активів, ROA	–0,35	0,002	–0,062	0,002	–0,217
	Рентабельність власного капіталу, ROE	–2,76	0,013	–2,36	0,008	–1,36
	Операційна маржа	–0,51	0,018	–0,185	0,123	–0,091
Ділова активність	Оборотність активів	0,75	0,83	0,84	0,47	0,58
	Оборотність дебіторської заборгованості	3,72	5,26	2,62	1,75	3,20
	Оборотність запасів	314,9	264,4	176,5	88,9	84,9
Інвестиційно-структурна спроможність	Частка необоротних активів в активах	0,74	0,63	0,54	0,62	0,69
	Темп оновлення основних засобів	0,051	0,063	0,060	0,096	0,151
	Капітальні інвестиції до чистого доходу	0,052	0,056	0,031	0,128	0,173

Примітка: для коефіцієнтів та відносних показників одиниці виміру не застосовуються; для абсолютних показників значення наведено у тис. грн.

ДОДАТОК Ж

Динаміка показників економічної безпеки ТОВ «ГПК «Нафтогаз України» у 2020–2024 роках

Група показників	Показник	2020	2021	2022	2023	2024
Фінансова стійкість	Коефіцієнт автономії	0,027	–0,597	–1,273	–1,278	–1,128
	Коефіцієнт фінансового левириджу	35,87	–2,676	–1,783	–1,783	–1,887
	Покриття необоротних активів власним капіталом	1,48	–130,63	–690,2	–833,84	–368,56
Ліквідність і платоспроможність	Коефіцієнт поточної ліквідності	1,01	0,623	0,439	0,438	0,469
	Коефіцієнт швидкої ліквідності	1,00	0,590	0,433	0,432	0,454
	Чистий оборотний капітал, тис. грн	13 222	–3 427 874	–26 861 679	–28 843 912	–28 442 394
Рентабельність	Рентабельність активів, ROA	–0,081	–1,342	–1,109	–0,0910	0,0187
	Рентабельність власного капіталу, ROE	–3,00	–2,84	–0,871	–0,0714	–0,0156
	Операційна маржа	–0,045	–0,301	–0,394	–0,0349	0,00992
Ділова активність	Оборотність активів	2,05	4,34	2,75	2,552	2,323
	Оборотність дебіторської заборгованості	2,72	6,01	3,24	2,761	2,601
	Оборотність запасів	425,8	93,06	176,3	168,06	93,66
Інвестиційно-структурна спроможність	Частка необоротних активів в активах	0,018	0,0046	0,002	0,00153	0,00306
	Темп оновлення основних засобів	0,165	0,141	0,439	0,0440	0,375
	Капітальні інвестиції до чистого доходу	0,0037	0,001	0,00006	0,000027	0,0000397

Примітка: для коефіцієнтів та відносних показників одиниці виміру не застосовуються; для абсолютних показників значення наведено у тис. грн.

ДОДАТОК И

Динаміка показників економічної безпеки АТ «Українська залізниця» у 2020–2024 роках

Група показників	Показник	2020	2021	2022	2023	2024
Фінансова стійкість	Коефіцієнт автономії	0,774	0,765	0,759	0,708	0,672
	Коефіцієнт фінансового левириджу	0,293	0,306	0,317	0,412	0,488
	Покриття необоротних активів власним капіталом	0,813	0,809	0,820	0,803	0,756
Ліквідність і платоспроможність	Коефіцієнт поточної ліквідності	0,422	0,575	1,266	1,739	1,565
	Коефіцієнт швидкої ліквідності	0,127	0,165	0,489	1,018	0,913
	Чистий оборотний капітал, тис. грн	–17 105 249	–10 188 312	3 894 385	13 819 884	11 260 488
Рентабельність	Рентабельність активів, ROA	–0,0462	0,00180	–0,0381	0,0182	–0,0098
	Рентабельність власного капіталу, ROE	–0,0597	0,00235	–0,0502	0,0257	–0,0146
	Операційна маржа	–0,0366	0,01875	–0,122	0,0534	–0,0260
Ділова активність	Оборотність активів	0,292	0,331	0,302	0,342	0,371
	Оборотність дебіторської заборгованості	132,00	106,65	41,19	51,58	70,66
	Оборотність запасів	8,95	8,58	7,47	6,57	8,24
Інвестиційно-структурна спроможність	Частка необоротних активів в активах	0,951	0,946	0,926	0,881	0,889
	Темп оновлення основних засобів	0,0282	0,0436	0,0436	0,0576	0,0579
	Капітальні інвестиції до чистого доходу	0,122	0,172	0,195	0,229	0,206

Примітка: для коефіцієнтів та відносних показників одиниці виміру не застосовуються; для абсолютних показників значення наведено у тис. грн.

ДОДАТОК К

Динаміка показників економічної безпеки АТ «Укрпошта» у 2020–2024 роках

Група показників	Показник	2020	2021	2022	2023	2024
Фінансова стійкість	Коефіцієнт автономії	0,261	0,249	0,151	0,054	0,018
	Коефіцієнт фінансового левириджу	2,833	3,021	5,634	17,44	53,89
	Покриття необоротних активів власним капіталом	0,712	0,619	0,319	0,129	0,040
Ліквідність і платоспроможність	Коефіцієнт поточної ліквідності	0,921	0,913	0,712	0,687	0,626
	Коефіцієнт швидкої ліквідності	0,887	0,871	0,631	0,639	0,578
	Чистий оборотний капітал, тис. грн	–531 852	–604 562	–1 976 315	–3 014 643	–3 726 486
Рентабельність	Рентабельність активів, ROA	0,0166	0,0170	–0,134	–0,069	–0,036
	Рентабельність власного капіталу, ROE	0,0638	0,0685	–0,886	–1,278	–1,966
	Операційна маржа	0,0202	0,0180	–0,115	–0,074	–0,031
Ділова активність	Оборотність активів	0,927	1,038	1,096	1,007	1,125
	Оборотність дебіторської заборгованості	27,37	27,88	31,76	20,84	20,53
	Оборотність запасів	34,47	32,45	17,58	23,40	24,36
Інвестиційно-структурна спроможність	Частка необоротних активів в активах	0,366	0,402	0,473	0,419	0,456
	Темп оновлення основних засобів	0,0892	0,169	0,099	0,107	0,139
	Капітальні інвестиції до чистого доходу	0,0525	0,0933	0,066	0,069	0,091

Примітка: для коефіцієнтів та відносних показників одиниці виміру не застосовуються; для абсолютних показників значення наведено у тис. грн.

ДОДАТОК Л

**Динаміка показників економічної безпеки ІНТЕРПАЙП ХОЛДІНГС ПЛС (INTERPIPE HOLDINGS PLC)
у 2020–2024 роках**

Група показників	Показник	2020	2021	2022	2023	2024
Фінансова стійкість	Коефіцієнт автономії	0,561	0,372	0,257	0,479	0,546
	Коефіцієнт фінансового левериджу	0,783	1,689	2,888	1,087	0,833
	Покриття необоротних активів власним капіталом	1,002	0,796	0,747	1,036	1,304
Ліквідність і платоспроможність	Коефіцієнт поточної ліквідності	2,366	2,697	2,383	2,714	3,409
	Коефіцієнт швидкої ліквідності	1,475	1,771	1,593	1,873	2,560
	Чистий оборотний капітал, тис. дол. США	235 924	392 790	304 372	375 880	487 402
Рентабельність	Рентабельність активів, ROA	0,210	0,078	0,256	0,228	0,237
	Рентабельність власного капіталу, ROE	0,375	0,210	0,994	0,477	0,434
	Операційна маржа	0,246	0,129	0,283	0,363	0,321
Ділова активність	Оборотність активів	0,932	0,968	1,227	0,893	0,886
	Оборотність дебіторської заборгованості	8,222	5,995	7,290	9,113	9,539
	Оборотність запасів	3,884	3,848	3,633	2,863	3,773
Інвестиційно-структурна спроможність	Частка необоротних активів в активах	0,560	0,467	0,344	0,463	0,418
	Темп оновлення основних засобів	0,065	0,095	0,102	0,087	0,111
	Капітальні інвестиції до чистого доходу	0,045	0,057	0,023	0,033	0,035

Примітка: для коефіцієнтів та відносних показників одиниці виміру не застосовуються; для абсолютних показників значення наведено у тис. дол.

ДОДАТОК М

Розрахунок амплітуди коливань інтегрального індексу у 2020–2024 роках

Підприємство	Середній інтегральний індекс (2020–2024)	Амплітуда коливань (max–min)	2020	2021	2022	2023	2024
INTERPIPE HOLDINGS PLC	0.6016	0.057	0.6	0.589	0.582	0.639	0.598
АТ «Укрзалізниця»	0.4716	0.096	0.431	0.432	0.486	0.527	0.482
АТ «Укрпошта»	0.42	0.159	0.443	0.501	0.459	0.355	0.342
ПрАТ «НЕК «Укренерго»	0.3584	0.213	0.233	0.439	0.364	0.446	0.31
ТОВ «ГПІК «Нафтогаз України»	0.338	0.225	0.471	0.246	0.315	0.258	0.4

ДОДАТОК Н

Розрахунок амплітуди коливань інтегрального індексу у 2020–2024 роках

Функціональний блок (нормовані значення)	INTERPIPE HOLDINGS PLC 2021	INTERPIPE HOLDINGS PLC 2022	АТ «Укрзалізниця» 2021	АТ «Укрзалізниця» 2022	АТ «Укрпошта» 2021	АТ «Укрпошта» 2022	ПрАТ «НЕК «Укренерго» 2021	ПрАТ «НЕК «Укренерго» 2022	ТОВ «ГПК «Нафтогаз України» 2021	ТОВ «ГПК «Нафтогаз України» 2022
Фінансова стійкість	0.09	0.102	0.107	0.115	0.081	0.097	0.059	0.065	0.036	0.036
Ліквідність і платоспроможність	0.219	0.219	0	0.082	0.07	0.057	0.057	0.052	0.037	0
Рентабельність	0.152	0.152	0.132	0.093	0.133	0.079	0.132	0.055	0	0.02
Ділова активність	0.013	0.044	0.131	0.132	0.054	0.131	0.116	0.123	0.113	0.184
Інвестиційно-структурна спроможність	0.115	0.065	0.062	0.065	0.163	0.096	0.074	0.068	0.06	0.074

Для побудови радар-діаграми використано нормовані значення функціональних блоків інтегрального індексу економічної безпеки (без застосування відсоткових показників). До аналізу включено такі компоненти: фінансова стійкість, ліквідність і платоспроможність, рентабельність, ділова активність та інвестиційно-структурна спроможність.

Для порівняння обрано 2021 та 2022 роки як відповідно докризовий і кризовий періоди, що дозволяє виявити структурні зміни в конфігурації економічної безпеки підприємств під впливом системного шоку.

Коригування вихідних даних не здійснювалися: значення перенесені без змін із розрахункової таблиці. Нульові показники (0,000) залишені відповідно до фактичних даних, що забезпечує коректність відображення реального стану окремих функціональних блоків.

З метою забезпечення порівнюваності профілів для всіх контурів встановлено єдиний радіальний масштаб у межах 0–0,25. Це унеможливорює візуальні спотворення та дозволяє коректно інтерпретувати відносні структурні відмінності між підприємствами.

ДОДАТОК П

**Розрахунок середньої абсолютної відносної похибки інтегрального
індексу економічної безпеки**

Підприємство	Рік	ІЕБ (факт)	ІЕБ (модель)	Абсолютна похибка	Відносна похибка
INTERPIPE	2020	0,600	0,584	0,016	0,027
INTERPIPE	2021	0,589	0,574	0,015	0,026
INTERPIPE	2022	0,582	0,584	0,002	0,003
INTERPIPE	2023	0,639	0,608	0,031	0,049
INTERPIPE	2024	0,598	0,667	0,069	0,116
Укрзалізниця	2020	0,431	0,421	0,010	0,024
Укрзалізниця	2021	0,432	0,442	0,010	0,023
Укрзалізниця	2022	0,486	0,471	0,015	0,031
Укрзалізниця	2023	0,527	0,505	0,022	0,041
Укрзалізниця	2024	0,482	0,487	0,005	0,011
Укрпошта	2020	0,443	0,463	0,020	0,046
Укрпошта	2021	0,501	0,495	0,006	0,013
Укрпошта	2022	0,459	0,411	0,048	0,106
Укрпошта	2023	0,355	0,394	0,039	0,109
Укрпошта	2024	0,342	0,353	0,011	0,031
Нафтогаз	2020	0,471	0,458	0,013	0,028
Нафтогаз	2021	0,246	0,261	0,015	0,060
Нафтогаз	2022	0,315	0,279	0,036	0,114
Нафтогаз	2023	0,258	0,252	0,006	0,023
Нафтогаз	2024	0,400	0,428	0,028	0,069
Укренерго	2020	0,233	0,309	0,076	0,325
Укренерго	2021	0,439	0,395	0,044	0,101
Укренерго	2022	0,364	0,332	0,032	0,087
Укренерго	2023	0,446	0,437	0,009	0,021
Укренерго	2024	0,310	0,342	0,032	0,102

Примітка: абсолютна похибка визначена як $|\text{ІЕБ}^{\text{факт}} - \text{ІЕБ}^{\text{модель}}|$;
відносна похибка – як відношення абсолютної похибки до фактичного значення показника.

$$\text{САВП} = \frac{\sum \text{відносних похибок}}{25} \times 100\% \approx 6,35\%$$



ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «Наш Простір»

33023, м. Рівне, вул. Транспортна, буд. 12, оф. 205

код ЄДРПОУ 33001142

тел.: +38 067 363 7707, +38 093 670 7707

e-mail: info@nashprostir.com

№ 11/26 від 22.04.2026

ДОВІДКА

про впровадження результатів дисертаційної роботи

Роздопченюка Василя Миколайовича,

що подана на здобуття наукового ступеня

доктора філософії за спеціальністю 051 – економіка

Результати дисертаційної роботи Роздопченюка В. М. на тему «Оцінка економічної безпеки підприємства в умовах цифрової трансформації економіки України» використано у практичній діяльності ТОВ «Наш Простір», зокрема при оцінюванні рівня економічної безпеки підприємства та вдосконаленні аналітичного підходу до прийняття управлінських рішень. Практичне застосування отримали окремі методичні положення щодо оцінювання економічної безпеки, використання системи показників для її аналізу та врахування впливу ризиків на результати діяльності підприємства.

Довідка видана для подання до разової спеціалізованої вченої ради.

Директор



Анастасія ДЄДУХ



РІВНЕНСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ДЕПАРТАМЕНТ ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ

майдан Просвіти, 1, м. Рівне, 33028, тел. (0362) 69 52 30
e-mail: ekon@rv.gov.ua

Код ЄДРПОУ 02741545

№ _____ На № _____ від _____

ДОВІДКА

**про впровадження результатів дослідження
РОЗДОПЧЕНЮКА Василя Миколайовича
щодо оцінки економічної безпеки підприємства в умовах цифрової
трансформації економіки України, виконаного в межах дисертаційної
роботи на здобуття наукового ступеня доктора філософії за спеціальністю
051 – Економіка**

Департамент економічного розвитку і торгівлі Рівненської обласної державної адміністрації є головним розробником і одним із провідних виконавців Стратегії розвитку Рівненської області, середньострокових планів з реалізації Стратегії, регіональних програм економічного та соціального розвитку, розвитку інвестиційної діяльності, розвитку малого та середнього підприємництва, зайнятості населення.

До розробки та впровадження зазначених Стратегії та програм, а також інших управлінських рішень з питань забезпечення реалізації в області державної економічної політики залучались та залучаються науковці області.

Зокрема, при підготовці аналітичних матеріалів щодо розвитку регіональної економіки та визначенні шляхів протидії ризикам і загрозам сталому розвитку області в умовах воєнного стану були використані результати дослідження РОЗДОПЧЕНЮКА Василя Миколайовича, викладені в його дисертаційній роботі, стосовно удосконалення аналітичного забезпечення регіональної економічної політики, передусім в питаннях підвищення економічної безпеки підприємств, їх цифрової трансформації, формування адаптивних управлінських рішень щодо сприяння підвищенню ефективності підприємницької діяльності на Рівненщині.

При розробці програмних та аналітичних документів, віднесених до компетенції департаменту, в першу чергу були враховані запропоновані

Рівненська обласна військова адміністрація
Департамент економічного розвитку і торгівлі
№ вих-389/0/26 від 07.05.2026



Продовження Додатку Р

в дисертації підходи до систематизації показників економічної безпеки підприємств, оцінювання впливу цифрових ризиків на їх функціонування, а також формування інтегрального підходу до діагностики рівня економічної безпеки.

Загалом результати дослідження РОЗДОПЧЕНЮКА В.М. мають практичну цінність, оскільки сприяють підвищенню обґрунтованості підходів до оцінювання стану підприємницького сектору, врахування цифрових ризиків, формування пропозицій щодо підвищення стійкості суб'єктів господарювання Рівненської області.

Директор департаменту



Костянтин МОКЛЯК

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«УКРАЇНСЬКІ ДЕРЕВИННІ ПЕЛЕТИ»
35224, Рівненська область, Дубенський район, село Вовковий
ЄДРПОУ 37651219

№ 19 від «11» травня 2026 року

ДОВІДКА

про впровадження результатів дослідження
Роздопченюка Василя Миколайовича

з питань підвищення рівня економічної безпеки підприємства в умовах цифрових змін економіки України, виконаного в рамках дисертаційної роботи на здобуття наукового ступеня доктора філософії за спеціальністю 051 Економіка

ТзОВ «Українські деревинні пелети» повідомляє, що в процесі своєї діяльності використано окремі результати дисертаційної роботи Роздопченюка Василя Миколайовича, що стосуються оцінювання економічної безпеки підприємства та аналізу впливу зовнішніх і внутрішніх чинників на її рівень. Застосування запропонованих підходів дозволило уточнити аналітичні оцінки стану товариства посилити увагу до ризиків в процесі господарської діяльності та удосконалити підходи до обґрунтування управлінських рішень.

Отримані результати використовуються при проведенні внутрішнього аналізу діяльності товариства, що сприяє більш системному врахуванню факторів нестабільності та підвищенню якості управління в умовах змінного економічного середовища.

Директор



Михайло МАРЧУК



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА
ПРИРОДОКОРИСТУВАННЯ
(НУВГП)

вул. Соборна, 11, м. Рівне, 33028, тел. (0362) 63 30 98, факс (0362) 63 32 09,
e-mail: mail@nuwm.edu.ua, web: https://nuwm.edu.ua
код ЄДРПОУ 02071116

Від 16.03.2026 № 011-04 На № _____ від _____

ДОВІДКА

**про використання у навчальному процесі
Національного університету водного господарства та природокористування результатів
досліджень і розробок, одержаних при виконанні дисертації
РОЗДОПЧЕНЮКА Василя Миколайовича
на здобуття ступеня доктора філософії за спеціальністю
051 – Економіка**

Результати наукових досліджень, викладені у дисертації здобувача ступеня доктора філософії Роздопченюка В. М., реалізовані у вигляді теоретико-методичних підходів, концептуальних положень та аналітичного інструментарію щодо оцінювання економічної безпеки підприємства в умовах цифрової трансформації економіки, що забезпечують формування професійних компетентностей здобувачів вищої освіти першого (бакалаврського) та другого (магістерського) рівнів і сприяють досягненню програмних результатів навчання.

Отримані наукові результати використовуються в навчальному процесі, зокрема при викладанні навчальних дисциплін «Роль бухгалтера в бізнес-середовищі» та «Податкове планування». Представлені наукові результати сприяють формуванню системного розуміння ролі обліково-аналітичної інформації у забезпеченні економічної безпеки підприємства, розвитку навичок інтерпретації фінансової звітності, проведення коефіцієнтного аналізу та використання його результатів для оцінювання рівня економічної стійкості суб'єкта господарювання, а також обґрунтування управлінських і податкових рішень. Практичне застосування розробленого інструментарію інтегрального оцінювання економічної безпеки, зокрема системи показників на основі ключових показників ефективності (KPI) та ключових індикаторів ризику (KRI), забезпечує здобуття навичок оцінки податкового навантаження, планування податкових платежів, їх оптимізації та формування рекомендацій щодо побудови ефективної системи податкового планування підприємства. Ці здобутки використовуються в межах підготовки здобувачів вищої освіти першого (бакалаврського) та другого (магістерського) рівнів за спеціальністю 071 «Облік і оподаткування» для підвищення якості освітнього процесу та професійної підготовки майбутніх фахівців:

- під час викладання навчальної дисципліни «Роль бухгалтера в бізнес-середовищі»: Тема 2. Бухгалтерський облік: сутність і роль у сучасному бізнес-середовищі; Тема 3. Роль бухгалтерського обліку у забезпеченні сталого розвитку;

- під час викладання навчальної дисципліни «Податкове планування»: Тема 1. Прогнозування і планування податкових надходжень; Тема 2. Податкове планування в системі управління суб'єктом господарської діяльності; Тема 3. Методика та організаційні аспекти податкового планування суб'єкта господарської діяльності.

Проректор з наукової роботи
та міжнародних зв'язків НУВГП
доктор економічних наук, професор

Ольга ПАВЕЛКО +380970522489



Наталія САВІНА