

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»**

Кваліфікаційна наукова  
праця на правах рукопису

**БІЛИЧЕНКО МАКСИМ МИКОЛАЙОВИЧ**

УДК 658:004(043.5)

**ДИСЕРТАЦІЯ**

**СИСТЕМА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В  
УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ**

за спеціальністю 051 «Економіка»  
галузь знань 05 «Соціальні та поведінкові науки»

Подається на здобуття наукового ступеня доктора філософії

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

М.М. Біличенко

Науковий керівник Смерічевський Сергій Францович  
доктор економічних наук, професор

Київ – 2026

## АНОТАЦІЯ

Біличенко М.М. Система економічної безпеки підприємства в умовах цифрової трансформації.

Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 05 «Соціальні та поведінкові науки» зі спеціальності 051 «Економіка». Державний університет «Київський авіаційний інститут» Міністерства освіти і науки України, Київ, 2026.

Дисертація присвячена розв'язанню наукового завдання щодо розвитку теоретико-методичних підходів і формування прикладного інструментарію управління системою економічної безпеки підприємства в умовах цифрової трансформації, що забезпечує комплексне оцінювання стану фінансової, кадрової та техніко-технологічної підсистем безпеки на основі економіко-математичного моделювання та сучасних цифрових інструментів, підвищуючи обґрунтованість управлінських рішень щодо нейтралізації загроз і забезпечення стійкого функціонування підприємства в умовах невизначеності й зростання кіберризиків.

У вступі обґрунтовано актуальність теми дисертації та визначено її зв'язок з науковими програмами, планами і тематикою досліджень. Показано, що попри значну кількість наукових праць, присвячених теоретичним засадам і прикладним аспектам забезпечення економічної безпеки підприємства, переважно найбільше з них обґрунтовується на статичних моделях, орієнтованих на ретроспективну фінансову звітність, що не дозволяє адекватно ідентифікувати специфічні вразливості цифровізованого середовища. слідом до сформульованої мети конкретизовано завдання дослідження, визначено наукову новину та практичне значення отриманих результатів, надано відомості про особистість внесок автора, апробацію основних положень дисертації та перелік наукових публікацій.

У першому розділі «Теоретичні основи управління економічною безпекою підприємства в умовах цифровізації економіки» здійснено

теоретичне узагальнення та обґрунтування концептуальних засад управління економічною безпекою підприємства в умовах інтенсифікації цифрових трансформацій.

Досліджено еволюцію наукових підходів до визначення сутності та структури економічної безпеки підприємства – від вузькоспрямованих захисно-регламентних трактів до системних, стратегічно орієнтованих концепцій. На основі узагальнення домінуючих підходів запропоновано авторське визначення поняття «економічна безпека підприємства», яке інтегрує захисну, ресурсну, адаптивну та стратегічну складову та трактує її як динамічну резистентність суб'єкта господарювання до деструктивних впливів, що забезпечує конвергентне функціонування ключових підсистем під наскрізним регулюванням цифрової безпеки як детермінанти міжсистемної стійкості.

Розкрито зміст цифрової трансформації як багатовимірного процесу фундаментальної перебудови операційної моделі підприємства. Систематизовано підходи вітчизняних і зарубіжних науковців та провідних міжнародних корпорацій до трактування поняття «цифрова трансформація підприємства». Встановлено подвійний характер її впливу на систему економічної безпеки: поряд із підвищенням операційної ефективності, конкурентоспроможності та адаптивності до ринкових змін, цифрова трансформація породжує нові категорії ризиків – зростання кіберзагроз, ризики витоку конфіденційної інформації, стійкість оцінки результатів трансформацій та нестабільність кіберфізичних систем.

Проаналізовано диференційований вплив цифровізації на три ключові підсистеми безпеки: фінансову, де цифровізація відкриває нові канали монетизації, проте одночасно формує залежність від сторонніх цифрових сервісів; кадрову, де автоматизація продуктивності, але посилює ризики інсайдерських загроз; та техніко-технологічну, де інтеграцію IoT, SCADA-систему та цифрових двійників забезпечує ефективність виробництва, проте розширює поверхню кіберфізичних атак.

Визначено концептуальну модель інтегрованої системи економічної безпеки підприємства, яка поєднує функціональні підсистеми в єдиний безпековий контур з виокремленням цифрової безпеки як наскрізного компонента, що інтегрується в усі функціональні підсистеми та обслуговує зв'язуючим елементом між ними. Обґрунтовано, що базисом для вибору стратегічного орієнтиру розвитку системи має служити інтегральна оцінка рівня безпеки, яка дозволяє формалізувати стан захищеності через сукупність якісних та якісних показників і забезпечує перехід від реактивного до проактивного управління.

У другому розділі «Аналіз системи економічної безпеки сучасного підприємства» здійснено аналіз методичних підходів та інструментарію оцінки рівня економічної безпеки підприємства, розглянуто підходи до моделювання складових системи в умовах цифрової економіки та розроблено інформаційну модель управління системою економічної безпеки.

На підставі аналізу наукових джерел досліджено еволюцію методології оцінювання економічної безпеки підприємства з виокремленням чотирьох етапів її розвитку, кожен з яких відповідав специфічним умовам господарювання та рівню розвитку економічної науки. Систематизовано індикаторний, ресурсно-функціональний, експертний та алгоритмічний підходи до оцінювання економічної безпеки, визначено їх переваги та обмеження. Встановлено, що традиційні статичні моделі, орієнтовані на ретроспективну фінансову звітність, втрачають ефективність у цифровому середовищі через неможливість врахування специфічних ІТ-ризиків та відсутність інструментарію для обробки великих даних. Обґрунтовано необхідність комплексного інструментарію, що поєднує кількісні методи з урахуванням нематеріальних активів і цифрових чинників.

Здійснено аналіз сучасних підходів до моделювання фінансової, кадрової та техніко-технологічної складових системи економічної безпеки. У сфері фінансової безпеки розглянуто еволюцію методів прогнозування банкрутства від класичних статистичних моделей до сучасних алгоритмів

машинного навчання. Обґрунтовано доцільність інтеграції традиційних фінансових індикаторів із авторською системою показників цифрової активності підприємств – інтернет-присутності, активності у соціальних мережах та розвиненості електронної комерції.

У сфері кадрової безпеки охарактеризовано підходи до моделювання інсайдерських ризиків і виявлення аномальної поведінки персоналу в корпоративному цифровому середовищі. Встановлено, що найбільш ефективними підходами є алгоритми виявлення аномалій, які дозволяють ідентифікувати несанкціоновані відхилення у поведінці персоналу через аналіз цифрових слідів активності у корпоративних мережах. Обґрунтовано методологічні засади семантичного збагачення поведінкових даних із застосуванням великих мовних моделей для динамічної контекстуальної класифікації вебактивності співробітників – підходу, що принципово відрізняється від статичних методів фільтрації трафіку.

Для техніко-технологічної підсистеми розроблено ієрархічну модель інтегрального оцінювання на основі авторської системи цифро-орієнтованих критеріїв: рівня автоматизації виробництва, захищеності ІТ-інфраструктури, частки цифрових технологій у технологічних процесах, стану технічного обладнання та інноваційної готовності, цифрової компетентності персоналу. Модель забезпечує формалізацію якісних характеристик цифрової зрілості підприємства шляхом їх перетворення в нормовані числові значення з подальшим зваженим агрегуванням в інтегральний індекс техніко-технологічної стійкості. Вагові коефіцієнти можуть встановлюватися індивідуально для кожного підприємства залежно від галузевої специфіки, рівня цифрової зрілості та технологічного укладу.

Розроблено інформаційну модель управління системою економічної безпеки підприємства як ключовий елемент системи підтримки прийняття рішень. Запропонована блочно-модульна архітектура забезпечує горизонтальну інтеграцію гетерогенних даних фінансового, кадрового та технологічного контурів, автоматизований моніторинг індикаторів безпеки та

раннє попередження про критичні відхилення. Обґрунтовано доцільність використання нелінійного інтегрального показника економічної безпеки, який, на відміну від традиційних адитивних методів згортання показників, враховує синергетичний ефект одночасної дії цифрових ризиків у різних підсистемах. Сформульовано принципи побудови інформаційної моделі.

У третьому розділі «Економіко-математичне моделювання системи економічної безпеки підприємства в умовах цифрової трансформації» здійснено економіко-математичне моделювання та апробацію розроблених методичних підходів на реальних об'єктах дослідження.

Для моделювання фінансової складової економічної безпеки сформовано репрезентативну вибірку підприємств переробної промисловості України, що охоплює 570 підприємств за період 2014–2020 рр. Базу даних сформовано шляхом поєднання офіційних судових реєстрів повідомлень про банкрутство та фінансової звітності підприємств, отриманої через аналітичний сервіс YouControl. Апробовано п'ять алгоритмів машинного навчання: логістичну регресію, SVM, Random Forest, нейронні мережі та XGBoost. Встановлено, що модель XGBoost з L1-регуляризацією забезпечує найвищу прогностичну точність порівняно з традиційними економетричними методами. Інтеграція трьох авторських змінних цифрової активності підвищила прогностичну спроможність моделі та емпірично довела статистичну значущість рівня цифровізації бізнес-процесів як важливого фактору прогнозування фінансової стійкості. Для інтерпретації нелінійних взаємозв'язків між факторами та рівнем фінансового ризику застосовано метод побудови графіків часткової залежності (PDP), що дозволило ідентифікувати порогові значення ключових індикаторів для прийняття превентивних управлінських рішень.

Для моделювання кадрової складової розроблено модель управління кадровою безпекою підприємства, спрямовану на виявлення інсайдерських ризиків та аномальної поведінки персоналу. На відміну від існуючих підходів, що базуються на статичних списках заблокованих доменів, розроблений метод

здійснює динамічну контекстуальну класифікацію вебресурсів за їх змістом, генеруючи нові бінарні семантичні ознаки ризикової поведінки, недоступні для стандартних систем фільтрації трафіку. Введено авторські композитні змінні поведінкового профілю, зокрема мультиплікативну змінну, що фіксує синергетичний ефект одночасного зростання пошукової активності на сайтах працевлаштування та збільшення підключень зовнішніх пристроїв. Застосування алгоритму Isolation Forest дозволило ідентифікувати латентні загрози на до-інцидентній стадії, реалізуючи принципово превентивний характер управління кадровою безпекою. Емпірично підтверджено, що критично високий рівень кадрових ризиків здатний нівелювати позитивний вплив фінансової стабільності, що обґрунтовує необхідність комплексного, а не ізольованого управління підсистемами безпеки.

Здійснено інтеграцію побудованих моделей фінансової, кадрової та техніко-технологічної підсистем у комплексну інформаційну систему управління економічною безпекою підприємства. Розроблено уніфіковану трирівневу шкалу оцінки ризику для забезпечення сумісності результатів моделей різних підсистем. Реалізовано прикладну інформаційну систему на платформі Streamlit із чотирьохмодульною архітектурою, що забезпечує наскрізну автоматизацію повного управлінського циклу: від завантаження первинних даних та їх інтелектуального аналізу до формування нелінійного інтегрального показника економічної безпеки та генерування диференційованих стратегічних і тактичних рекомендацій.

Апробацію розробленої комплексної системи оцінювання проведено на шести підприємствах різного профілю та форм власності. Результати апробації підтвердили практичну придатність розробленого інструментарію та дозволили виявити галузеву специфіку формування ризиків. Зокрема, встановлено пряму залежність між рівнем цифровізації підприємства та його загальною економічною стійкістю. Для високотехнологічних компаній цифрова трансформація виступає ключовим буфером проти макроекономічних ризиків, тоді як для підприємств традиційного індустріального сектору

критично низькі індекси технологічної безпеки у поєднанні з високим рівнем аномальних дій персоналу стають каталізаторами фінансової деградації. За результатами апробації сформовано узагальнені управлінські рекомендації для кожного підприємства з урахуванням виявлених зон ризику.

Практичне значення одержаних результатів полягає в доведенні основних наукових положень дисертації до рівня науково-методичних та практичних рекомендацій, які можуть застосовуватися на підприємствах різних галузей при формуванні та коригуванні управлінських рішень у сфері економічної безпеки в умовах цифрової трансформації.

**Ключові слова:** економічна безпека підприємства, управління економічною безпекою, цифрова безпека, фінансова безпека, кадрова безпека, техніко-технологічна безпека, цифровізація, індикатори безпеки, оцінка ризику, прогнозування банкрутства, машинне навчання, інтегральне оцінювання, система, системний підхід, інформаційна модель, стратегія.

## ABSTRACT

Bilichenko M.M. The system of economic security of an enterprise in the conditions of digital transformation.

Dissertation for the degree of Doctor of Philosophy in the field of knowledge 05 "Social and behavioral sciences" in the specialty 051 "Economics". State University "Kyiv Aviation Institute" of the Ministry of Education and Science of Ukraine, Kyiv, 2026.

The dissertation is devoted to solving the scientific problem of developing theoretical and methodological approaches and forming applied tools for managing the system of economic security of an enterprise in the conditions of digital transformation, which provides a comprehensive assessment of the state of financial, personnel and technical and technological security subsystems based on economic and mathematical modeling and modern digital tools, increasing the validity of

management decisions to neutralize threats and ensure the sustainable functioning of the enterprise in conditions of uncertainty and growth of cyber risks.

The introduction substantiates the relevance of the dissertation topic and determines its connection with scientific programs, plans and research topics. It is shown that despite the significant number of scientific works devoted to the theoretical principles and applied aspects of ensuring the economic security of an enterprise, most of them are based on static models focused on retrospective financial reporting, which does not allow for adequate identification of specific vulnerabilities of the digitalized environment. Following the formulated goal, the research tasks are specified, the scientific novelty and practical significance of the results obtained are determined, information about the author's personal contribution, approbation of the main provisions of the dissertation and a list of scientific publications are provided.

In the first section "Theoretical foundations of managing the economic security of an enterprise in the conditions of digitalization of the economy" a theoretical generalization and justification of the conceptual principles of managing the economic security of an enterprise in the conditions of intensification of digital transformations is carried out.

The evolution of scientific approaches to determining the essence and structure of the economic security of an enterprise is studied - from narrowly focused protective and regulatory tracts to systemic, strategically oriented concepts. Based on the generalization of dominant approaches, the author's definition of the concept of "economic security of an enterprise" is proposed, which integrates the protective, resource, adaptive and strategic components and interprets it as the dynamic resistance of a business entity to destructive influences, which ensures the convergent functioning of key subsystems under the end-to-end regulation of digital security as determinants of intersystem stability. The content of digital transformation is revealed as a multidimensional process of fundamental restructuring of the enterprise's operating model. The approaches of domestic and foreign scientists and leading international corporations to the interpretation of the

concept of "digital transformation of an enterprise" are systematized. The dual nature of its impact on the economic security system has been established: along with increasing operational efficiency, competitiveness and adaptability to market changes, digital transformation generates new categories of risks – the growth of cyber threats, risks of leakage of confidential information, the stability of the assessment of transformation results and the instability of cyber-physical systems.

The differentiated impact of digitalization on three key security subsystems has been analyzed: financial, where digitalization opens new channels of monetization, but at the same time creates dependence on third-party digital services; personnel, where productivity automation, but increases the risks of insider threats; and technical and technological, the integration of IoT, SCADA systems and digital twins ensures production efficiency, but expands the surface of cyber-physical attacks.

A conceptual model of an integrated system of economic security of an enterprise has been defined, which combines functional subsystems into a single security circuit with the isolation of digital security as a cross-cutting component that is integrated into all functional subsystems and serves as a connecting element between them. It is substantiated that the basis for choosing a strategic guideline for the development of the system should be an integrated assessment of the level of security, which allows formalizing the state of security through a set of qualitative and quantitative indicators and ensures the transition from reactive to proactive management.

In the second section, "Analysis of the economic security system of a modern enterprise", an analysis of methodological approaches and tools for assessing the level of economic security of an enterprise has been carried out, approaches to modeling the components of the system in the conditions of a digital economy have been considered, and an information model for managing the economic security system has been developed.

Based on the analysis of scientific sources, the evolution of the methodology for assessing the economic security of an enterprise has been investigated, with the

identification of four stages of its development, each of which corresponded to specific business conditions and the level of development of economic science. Indicator, resource-functional, expert and algorithmic approaches to assessing economic security, their advantages and limitations are determined. It is established that traditional static models focused on retrospective financial reporting lose their effectiveness in the digital environment due to the inability to take into account specific IT risks and the lack of tools for processing big data. The need for a comprehensive tool that combines quantitative methods considering intangible assets and digital factors is substantiated.

An analysis of modern approaches to modeling the financial, personnel and technical and technological components of the economic security system is carried out. In the field of financial security, the evolution of bankruptcy forecasting methods from classical statistical models to modern machine learning algorithms is considered. The feasibility of integrating traditional financial indicators with the author's system of indicators of digital activity of enterprises - Internet presence, activity in social networks and the development of e-commerce is substantiated.

Within the domain of personnel security, methodologies for modelling insider threats and identifying atypical employee behaviour in corporate digital environments are delineated. It was found that the most effective approaches are anomaly detection algorithms that allow identifying unauthorized deviations in personnel behavior through the analysis of digital traces of activity in corporate networks. The methodological principles of semantic enrichment of behavioral data using large language models for dynamic contextual classification of employee web activity are substantiated - an approach that is fundamentally different from static methods of traffic filtering.

For the technical and technological subsystem, a hierarchical model of integral assessment was developed based on the author's system of digitally oriented criteria: the level of production automation, IT infrastructure security, the share of digital technologies in technological processes, the state of technical equipment and innovation readiness, and digital competence of personnel. The model provides

formalization of qualitative characteristics of the enterprise's digital maturity by converting them into normalized numerical values with subsequent weighted aggregation into an integral index of technical and technological stability. Weighting factors can be set individually for each enterprise depending on the industry specifics, level of digital maturity and technological structure.

An information model for managing the economic security system of an enterprise has been developed as a key element of the decision-making support system. The proposed block-modular architecture provides horizontal integration of heterogeneous data of financial, personnel and technological circuits, automated monitoring of security indicators and early warning of critical deviations. The feasibility of using a nonlinear integral indicator of economic security has been substantiated, which, unlike traditional additive methods of index roll-up, takes into account the synergistic effect of the simultaneous action of digital risks in different subsystems. The principles of building an information model have been formulated.

In the third section "Economic and mathematical modeling of the economic security system of an enterprise in the conditions of digital transformation", economic and mathematical modeling and testing of the developed methodological approaches on real research objects have been carried out.

To model the financial component of economic security, a representative sample of Ukrainian processing industry enterprises was formed, covering 570 enterprises for the period 2014–2020. The database was formed by combining official court registers of bankruptcy notifications and financial statements of enterprises obtained through the analytical service YouControl. Five machine learning algorithms were tested: logistic regression, SVM, Random Forest, neural networks, and XGBoost. It was found that the XGBoost model with L1-regularization provides the highest predictive accuracy compared to traditional econometric methods. The integration of three author's digital activity variables increased the predictive ability of the model and empirically proved the statistical significance of the level of digitalization of business processes as a predictor of financial stability. To interpret the nonlinear relationships between factors and the

level of financial risk, the method of constructing partial dependency graphs (PDP) was used, which allowed identifying the threshold values of key indicators for making preventive management decisions.

To model the personnel component, a model of enterprise personnel security management was developed, aimed at identifying insider risks and anomalous behavior of personnel. Unlike existing approaches based on static lists of blocked domains, the developed method performs dynamic contextual classification of web resources by their content, generating new binary semantic features of risky behavior that are inaccessible to standard traffic filtering systems. The author introduced composite variables within the behavioral profile, notably a multiplicative variable. A synergistic effect was identified when both search activity on employment sites and the number of external device connections increased simultaneously. The use of the Isolation Forest algorithm allowed identifying latent threats at the pre-incident stage, implementing the fundamentally preventive nature of personnel security management. It has been empirically confirmed that a critically high level of personnel risks is able to offset the positive impact of financial stability, which justifies the need for comprehensive, rather than isolated, management of security subsystems. The built models of financial, personnel, and technical and technological subsystems have been integrated into a comprehensive information system for managing the economic security of the enterprise. A unified three-level risk assessment scale has been developed to ensure the compatibility of the results of models of different subsystems. An applied information system on the Streamlit platform with a four-module architecture was implemented, which provides end-to-end automation of the full management cycle: from loading primary data and their intelligent analysis to the formation of a nonlinear integral indicator of economic security and the generation of differentiated strategic and tactical recommendations.

The developed comprehensive assessment system was tested at six enterprises of various profiles and forms of ownership. The test results confirmed the practical applicability of the developed tools and allowed us to identify the industry-specific nature of risk formation. In particular, a direct relationship was established between

the level of digitalization of the enterprise and its overall economic stability. For high-tech companies, digital transformation acts as a key buffer against macroeconomic risks, while for enterprises in the traditional industrial sector, critically low technological security indices combined with a high level of anomalous personnel actions become catalysts for financial degradation. Based on the test results, generalized management recommendations were formed for each enterprise, taking into account the identified risk areas.

The practical significance of the results obtained lies in bringing the main scientific provisions of the dissertation to the level of scientific, methodological and practical recommendations that can be applied at enterprises of various industries in the formation and adjustment of management decisions in the field of economic security in the context of digital transformation.

**Keywords:** *economic security of the enterprise, economic security management, digital security, financial security, personnel security, technical and technological security, digitalization, security indicators, risk assessment, bankruptcy forecasting, machine learning, integrated assessment, system, systems approach, information model, strategy.*

## СПИСОК ОПУБЛКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

### *Статті у наукових виданнях, включених до наукометричних баз Scopus та/або Web of Science*

1. Bilychenko M., Kasianova N., Smerichevskyi S., Lavrynenko O., Kryvovyazyuk I. Development of a smart personnel security system using machine learning. *Cyber Security and Data Protection 2025 (CSDP 2025): proceedings* (Lviv, Ukraine, 31 Jul. 2025). 2025, 203-215.

*Особистий внесок Біличенка М.М.:* Запропоновано інноваційний підхід до збагачення поведінкових даних шляхом інтеграції великих мовних моделей. Обґрунтовано практичну придатність запропонованої моделі для реального моніторингу кадрової безпеки підприємства та визначено напрями її інтеграції в корпоративну інфраструктуру безпеки.

2. Kostyunik O., Andriienko M., Voinalovych I., Bosa I., Bilychenko M. Organizational support for the formation of the economic security system of enterprises in the conditions of intellectual and innovative development of society. *Management Theory and Studies for Rural Business and Infrastructure Development*, 2023, 45(4), 399–405. DOI: <https://doi.org/10.15544/mts.2023.39>

*Особистий внесок Біличенка М.М.:* Розроблено послідовність етапів проєктування інформаційної моделі управління системою економічної безпеки в умовах цифрової трансформації.

### *Статті у наукових фахових виданнях України:*

3. Біличенко М.М., Смерічевський С.Ф. Застосування штучного інтелекту для аналізу фінансової безпеки підприємства. *Підприємництво та інновації*. 2026, 39, 69-75. DOI: <https://doi.org/10.32782/2415-3583/39.10>

*Особистий внесок Біличенка М.М.:* Запропоновано інноваційний алгоритм використання великих мовних моделей штучного інтелекту для автоматизованого інтерпретування графіків PDP, виявлено та систематизовано ключові групи ризиків цифрової трансформації підприємства, визначено їх негативний вплив на

систему економічної безпеки підприємства.

*Особистий внесок Смерічевського С.Ф.:* Обґрунтовано використання пояснюваного підходу до прогнозування банкрутства підприємств України на основі сучасних методів штучного інтелекту

4. Bilychenko M.M. Modeling of the technical-technological component of economic security in the context of enterprise digitalization. *Economic Innovations*, 2025, 27(4(97)), 13-22. DOI [https://doi.org/10.31520/ei.2025.27.4\(97\).13-22](https://doi.org/10.31520/ei.2025.27.4(97).13-22)

5. Біличенко М. М. Концептуальна модель оцінки економічної безпеки підприємства в умовах цифрової трансформації. *Здобутки економіки: перспективи та інновації*, 2025, 18. DOI: <https://doi.org/10.5281/zenodo.15540326>

6 Біличенко М. М. Оцінка фінансової безпеки підприємства методами машинного навчання. *Цифрова економіка та економічна безпека*, 2024, 4 (13), 101-107. DOI: <https://doi.org/10.32782/dees.13-15>

7. Касьянова Н. В., Біличенко М. М., Севериненко А. О. Моделювання цифрової безпеки підприємства. *Modern Economics*, 2023, 39, 54-61. DOI: [https://doi.org/10.31521/modecon.V39\(2023\)-08](https://doi.org/10.31521/modecon.V39(2023)-08).

*Особистий внесок Біличенка М.М.:* Запропоновано класифікацію цифрових ризиків підприємства за детермінантами загроз та ключовими сферами управління. Обґрунтовано триєдиний підхід до побудови системи цифрової безпеки підприємства на основі концептуальної, математичної та функціональної моделей, що забезпечує системну взаємодію між технічними, організаційними та управлінськими елементами захисту.

*Особистий внесок Касьянкової Н.В.:* Розроблено концептуальну модель цифрової безпеки підприємства, яка формалізує взаємозв'язки між джерелами загроз, чинниками вразливості та інформаційними ресурсами і слугує методологічною основою для побудови комплексної системи економічної безпеки.

*Особистий внесок Севериненка А.О.:* Визначено теоретичні засади цифрової безпеки підприємства на макро- та мікрорівні та розроблено

математичну модель оцінки рівня ризику цифрових атак з урахуванням параметрів цифрового середовища та характеристик потенційного злоумисника.

8. Біличенко М. М., Касьянова Н. В. Вплив цифрової трансформації на формування системи економічної безпеки підприємства. *Бізнес Інформ*, 2023, 7, 83–91. DOI: <https://doi.org/10.32983/2222-4459-2023-7-83-91>

*Особистий внесок Біличенка М.М.:* Виявлено та систематизовано п'ять ключових груп ризиків цифрової трансформації підприємства та визначено їх негативний вплив на фінансову, технологічну, інформаційну, кадрову та інтелектуальну підсистеми системи економічної безпеки підприємства.

*Особистий внесок Касьянкової Н.В.:* Сформовано комплекс організаційно-технологічних ініціатив для забезпечення стабільного функціонування підприємства в умовах цифровізації, а також обґрунтовано три стратегічні орієнтири управління безпекою.

***Наукові праці, які додатково відображають наукові результати дисертації***

9. Bilychenko M. Information model for managing enterprise economic security under digital transformation. *Innovations and New Directions in Scientific Research: proceedings of the 2nd International Scientific Conference* (Manchester, United Kingdom, 20 Sept. 2025). 2025. P.21-24. DOI: 10.64076/iedc250920.07.

10. Bilychenko M. Modern approaches to evaluate company's financial security. *X International scientific and practical conference «Modern Trends in the Development of Scientific Space»* (February 14-16, 2024). Dresden, Germany, International Scientific Unity. 2024. P. 44-47

11. Біличенко М.М. Прогнозування банкрутства підприємства методами інтелектуального аналізу даних. *Матеріали V Міжнародної науково-практичної конференції «Розвиток економіки та бізнес-адміністрування: наукові течії та рішення»*. (11 листопада 2024 р.). К., ДУ «КАІ», 2024. С. 24-27

12. Біличенко М.М. Вплив цифрової трансформації на операційні та фінансові показники діяльності підприємств. *Матеріали IV міжнародної науково-практичної конференції «Бізнес-аналітика: моделі, інструменти та технології»*. (1-3 березня 2023 р.). К.: НАУ, 2023. С. 404-409.

13. Біличенко М.М. Еволюція методів прогнозування фінансово-економічної безпеки підприємства. *Матеріали XIV міжнародної науково-практичної конференції «Сучасні проблеми моделювання соціально-економічних систем»*. (6-7 квітня 2023 р.). Братислава Харків, ВШЕМ – ХНЕУ ім. С. Кузнеця, 2023. URL: <https://mpsesm.hneu.edu.ua/index.php/mpsesm/mpsesm-xiv/paper/view/1074>

14. Біличенко М.М. Особливості оцінки економічної безпеки підприємства в умовах цифрової трансформації. *Міжнародної науково-практичної конференції «Розвиток економіки та бізнес-адміністрування: наукові течії та рішення»* (16 листопада 2023 р.). К.: НАУ, 2023. С. 41-42.

15. Біличенко М. М., Касьянова Н. В. Економічна безпека підприємства в умовах цифрової економіки. *Матеріали XII міжнародної науково-практичної конференції «Сучасні проблеми економіки та бізнесу»*. (10-11 листопада 2022 р.). К.: НАУ, 2022. С. 85-88. (особистий внесок здобувача полягає в визначенні сутності та основних ризиків цифрової трансформації підприємств, їх впливі на систему економічної безпеки підприємства).

## ЗМІСТ

|                                                                                                                                                           |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ВСТУП .....                                                                                                                                               | 21  |
| РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ.....                                                 | 33  |
| 1.1. Теоретичні підходи до визначення сутності та структури економічної безпеки підприємства.....                                                         | 33  |
| 1.2. Особливості впливу цифрової трансформації на економічну безпеку підприємства.....                                                                    | 56  |
| 1.3. Концептуальні засади формування інтегрованої системи економічної безпеки підприємства в умовах цифрової трансформації.....                           | 75  |
| Висновки до першого розділу .....                                                                                                                         | 102 |
| РОЗДІЛ 2. МЕТОДИЧНІ ЗАСАДИ ОЦІНКИ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА .....                                                                | 104 |
| 2.1. Методичні підходи до оцінки рівня економічної безпеки підприємства                                                                                   | 104 |
| 2.2. Методичні підходи до моделювання окремих складових системи економічної безпеки в умовах цифрової економіки.....                                      | 124 |
| 2.3. Інформаційно-логічна модель системи підтримки прийняття рішень для управління системою економічною безпекою підприємства в умовах цифровізації ..... | 148 |
| Висновки до другого розділу .....                                                                                                                         | 170 |
| РОЗДІЛ 3. ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.....                                 | 172 |
| 3.1. Моделювання фінансової складової системи економічної безпеки підприємства.....                                                                       | 172 |
| 3.2. Формування моделі управління кадровою безпекою підприємства .....                                                                                    | 194 |
| 3.3. Реалізація прикладної інформаційної системи управління системою економічною безпекою підприємств .....                                               | 211 |
| Висновки до третього розділу .....                                                                                                                        | 228 |

|                                  |     |
|----------------------------------|-----|
| ВИСНОВКИ.....                    | 230 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ..... | 234 |
| ДОДАТКИ.....                     | 260 |

## ВСТУП

**Актуальність теми.** В умовах стрімкого розгортання четвертої промислової революції та масштабних цифрових перетворень, що охоплюють усі сфери господарської діяльності, забезпечення економічної безпеки підприємства набуває принципово нового змісту. Цифрова трансформація кардинально змінює операційні моделі, структуру ризиків і конкурентне середовище, водночас генеруючи нові категорії загроз, що не охоплюються класичним інструментарієм управління безпекою. Особливої гостроти ця проблематика набуває для українських підприємств, які змушені одночасно вирішувати завдання технологічної модернізації та адаптації до умов підвищеної економічної і безпекової нестабільності.

Незважаючи на значну кількість наукових праць, присвячених теоретичним засадам і прикладним аспектам забезпечення економічної безпеки підприємства, переважна більшість із них ґрунтується на статичних моделях, орієнтованих на ретроспективну фінансову звітність. Такий підхід не дозволяє адекватно ідентифікувати специфічні вразливості цифровізованого середовища, зокрема: загрози інформаційній інфраструктурі, ризики витоку даних внаслідок інсайдерської діяльності та нестабільність кіберфізичних систем. Відтак, розроблення інтегрованої системи економічної безпеки, адаптованої до умов цифрової трансформації та оснащеної інструментарієм предиктивного моніторингу, є нагальною науково-практичною потребою.

Питання формування системи економічної безпеки підприємства досліджували численні вітчизняні та зарубіжні науковці: О.В. Ареф'єва [106], Л.П. Артеменко [213], Ю.О. Бровкіна [118], Н.В. Касьянова [145], О.Ю. Мішин [162], Л.О. Матвійчук [158], Н.Й. Реверчук [180], Н.О. Пархоменко [172], С.Т. Пілецька [175], З.М. Побережна [176], Т.О. Сімкова [188], С.Ф. Смерічевський [189], С.Ю. Хамініч [195], Т.Б. Ши́ра [203], А.М. Штангрет [207]. Ці дослідники зробили вагомий внесок у розвиток теоретико-методологічного базису управління економічною безпекою, запропонували різноманітні підходи до

визначення її сутності та обґрунтували структуру функціональних складових системи безпеки. Однак, незважаючи на значну наукову базу, проблема системного переосмислення і адаптації концептуальних засад та методичного інструментарію економічної безпеки підприємства в контексті цифрової трансформації залишається недостатньо розробленою.

Специфіку цифрової трансформації як каталізатора нових бізнес-моделей і одночасно джерела системних ризиків досліджували С. Берман [15], Г. Віал [99], І. Гьокальп [42], В. Мартінес [42], Ф. Фіцджеральд [38], а серед вітчизняних науковців цією проблемою займались Ю.П. Воржакова [127], Г.В. Козаченко [148], Ю.О. Нікітін [165], С.Ю. Хамініч [196], І.М. Шопіна [205], А.М. Штангрет [208]. Прикладним аспектам прогнозування фінансової неспроможності з використанням методів машинного навчання присвячені праці Е. Альтмана [9], М. Хамді [43], Т. Новіанторо [75], Й. Хуанга [48], Т. Корола [59], Б. Самі [43], В. Серрет [14] та ін. Системи виявлення інсайдерських загроз кадрової безпеки розробляли М. Раїссі-Дехкорді [80], Т. Рашід [82], Г. Гаваї [41], Ю. Сонг [91], Д. С. Ле [62], Н. Зінджир-Хейвуд [35] та ін. Попри широту досліджень, практично відсутні роботи, які б цілісно інтегрували цифрові чинники в структуру системи оцінювання та управління економічною безпекою підприємства, що й обумовлює наукову новизну і практичну значущість даного дисертаційного дослідження.

Актуальність дослідження посилюється й прикладним виміром: переважна більшість вітчизняних підприємств характеризується поверхневим рівнем цифровізації, що створює реальні загрози технологічного відставання і зниження конкурентоспроможності. Водночас відсутність комплексного науково-методичного забезпечення, здатного синтезувати фінансові, кадрові та техніко-технологічні аспекти безпеки в єдиній інтегрованій системі з використанням сучасних методів штучного інтелекту та машинного навчання, стримує перехід підприємств від реактивного до проактивного управління ризиками.

## **Зв'язок роботи з науковими програмами, планами, темами.**

Дисертаційна робота виконувалась відповідно до планів науково-дослідних робіт кафедри економіки Державного університету «Київський авіаційний інститут» за темами:

«Моделювання складних систем в контексті цифрової трансформації економічних процесів» (номер державної реєстрації 0120U103263, 2020-2022 рр.). Особистий внесок здобувача в межах цієї теми полягає у формуванні концептуальної моделі управління економічною безпекою підприємства в умовах цифрової трансформації, яка враховує особливості впливу цифрових ризиків на ключові підсистеми функціонування підприємств;

«Розвиток соціально-економічних систем в умовах турбулентності світової економіки» (номер державної реєстрації 0123U100645, 2023-2025 рр.). У межах даної науково-дослідної роботи здобувачем обґрунтовано методичний підхід до моделювання цифрової безпеки підприємства, що дозволяє оцінити можливості підприємства протистояти цифровим ризикам та мінімізувати ймовірні збитки шляхом формування багаторівневої безпекової системи.

**Мета і задачі дослідження.** Мета дисертаційної роботи полягає в удосконаленні теоретичних положень, науково-методичних підходів та розробленні практичного інструментарію формування інтегрованої системи економічної безпеки підприємства, адаптованої до умов цифрової трансформації та забезпеченої сучасними методами економіко-математичного моделювання й прогностичного аналізу.

Для досягнення поставленої мети сформульовано та вирішено такі основні завдання:

- здійснити критичний аналіз та систематизацію існуючих наукових підходів до визначення сутності та структури економічної безпеки підприємства;
- систематизувати ключові інструменти цифрової трансформації підприємств та здійснити аналіз їхнього впливу на бізнес-процеси;

- обґрунтувати концептуальну модель формування інтегрованої системи економічної безпеки підприємства в умовах цифрової трансформації із виокремленням цифрової безпеки як наскрізного компонента;
- класифікувати існуючі методичні підходи до оцінювання рівня економічної безпеки підприємства, визначивши їхні переваги та обмеження в умовах цифрової економіки;
- розробити методичний інструментарій оцінювання фінансової, кадрової та техніко-технологічної підсистем економічної безпеки підприємства на основі алгоритмів машинного навчання та економіко-математичного моделювання;
- удосконалити інформаційну модель управління системою економічної безпеки підприємства на основі блочно-модульної архітектури з інтеграцією методів штучного інтелекту;
- побудувати та апробувати моделі прогнозування фінансової стійкості на основі даних українських підприємств;
- розробити модель управління кадровою безпекою підприємства на основі алгоритму виявлення аномалій та семантичного збагачення даних;
- реалізувати прикладну інформаційну систему комплексної оцінки та моніторингу стану економічної безпеки підприємства у форматі готового програмного рішення.

**Об’єктом дослідження** є процес формування та управління системою економічної безпеки підприємства в умовах цифрової трансформації.

**Предметом дослідження** є сукупність теоретичних, науково-методичних засад і практичних рекомендацій щодо побудови інтегрованої системи економічної безпеки підприємства, адаптованої до умов цифрової трансформації, з використанням методів економіко-математичного моделювання.

**Методи дослідження.** Методологічною основою дисертаційного дослідження є системний, комплексний, процесний та функціональний

підходи до вивчення економічних явищ і процесів у контексті управління економічною безпекою підприємства в умовах цифрової трансформації.

Для розв'язання поставлених завдань використано такі методи наукового дослідження: методи аналізу, синтезу та формалізації – для систематизації теоретичних підходів до визначення сутності економічної безпеки підприємства, поняття та інструментарію цифрової трансформації (пп. 1.1, 1.2, 1.3); морфологічного аналізу – для уточнення понятійно-категоріального апарату з проблеми дослідження (пп. 1.1, 1.2); графічний – для наочного подання теоретичного та методичного матеріалу (усі розділи); абстрактно-логічний – для теоретичних узагальнень і формулювання висновків; структурно-функціональний – для дослідження архітектури системи економічної безпеки, визначення ролі та взаємодії її складових (пп. 1.3, 2.1, 2.3); методи класифікації та порівняльного аналізу – для оцінювання існуючих методичних підходів до прогнозування банкрутства та виявлення інсайдерських загроз (пп. 2.2); метод аналізу ієрархій та апарат нечіткої логіки – для розроблення ієрархічної моделі оцінювання техніко-технологічної складової економічної безпеки (пп. 2.2); методи машинного навчання (логістична регресія, SVM, Random Forest, XGBoost, нейронні мережі, Isolation Forest) – для побудови моделей бінарної класифікації фінансових станів і виявлення аномальної поведінки персоналу (пп. 3.1, 3.2); методи пояснюваного штучного інтелекту (алгоритм побудови графіків часткової залежності, PDP) – для інтерпретації нелінійних взаємозв'язків і порогових значень факторів впливу (пп. 3.1); методи семантичного аналізу на основі великих мовних моделей – для класифікації вебактивності персоналу та збагачення даних корпоративного моніторингу (пп. 3.2); методи системного проектування – для розроблення блочно-модульної інформаційної моделі системи підтримки прийняття рішень та програмної реалізації прикладної системи на базі фреймворку Streamlit (пп. 2.3, 3.3).

**Інформаційною основою роботи** стали: офіційні статистичні дані Державної служби статистики України; судові реєстри повідомлень про

банкрутство підприємств за 2016–2020 роки; фінансова звітність підприємств за період 2014–2020 рр.; відкритий набір даних корпоративного моніторингу CERT Insider Threat Dataset 4.2 (Carnegie Mellon University); аналітичні матеріали міжнародних консалтингових компаній (Accenture, KPMG, IBM, Gartner); наукові публікації у фахових вітчизняних і зарубіжних виданнях; матеріали міжнародних наукових конференцій. Зазначена інформаційна база забезпечила необхідну широту емпіричного охоплення, об'єктивність результатів та можливість відтворення розроблених моделей у практичній діяльності підприємств.

**Наукова новизна одержаних результатів.** Наукова новизна одержаних результатів полягає в системному теоретичному узагальненні та розробці науково-методичних засад і практичних рекомендацій щодо формування та управління системою економічної безпеки промислових підприємства в умовах цифрової трансформації. Основні положення наукової новизни, що відображають авторський внесок здобувача та виносяться на захист, полягають у наступному:

*удосконалено:*

- концептуальну модель інтегрованої системи економічної безпеки підприємства в умовах цифрової трансформації, що, на відміну від існуючих моделей, у яких фінансова, кадрова та техніко-технологічна підсистеми розглядаються ізольовано, базується на принципі їхньої системної конвергенції у єдину захисну архітектуру з виокремленням цифрової безпеки як наскрізного регулятора стійкості. Удосконалена модель формалізує механізми каскадного міжпідсистемного поширення цифрових ризиків і ефекти їхньої взаємодії, що обґрунтовує необхідність переходу від дискретного захисту окремих складових до цілісного проактивного управління економічною безпекою підприємства;

- інструментарій оцінювання фінансової складової економічної безпеки підприємства, який, на відміну від існуючих, передбачає інтеграцію традиційних фінансових індикаторів із розробленою системою показників цифрової активності. Застосування алгоритму XGBoost з L1-регуляризациєю

та методів пояснюваного ШІ дозволило не лише констатувати рівень фінансового ризику, а й ідентифікувати нелінійні порогові значення факторів впливу для прийняття превентивних управлінських рішень, що розширює теоретичне розуміння детермінант фінансової безпеки в умовах цифрової трансформації економіки;

- методичний підхід до виявлення інсайдерських загроз у кадровому контурі безпеки підприємства на основі моделей виявлення поведінкових аномалій, що, на відміну від існуючих методів кадрового аналізу, які ґрунтуються на традиційних показниках плинності кадрів та продуктивності праці, дозволяє ідентифікувати несанкціоновані відхилення у поведінці персоналу через аналіз цифрових слідів активності у корпоративних мережах та забезпечує превентивне виявлення внутрішніх загроз до настання критичних наслідків;

- методичний підхід до формування загальної оцінки рівня економічної безпеки підприємства та визначення стратегічних орієнтирів її досягнення в умовах цифрової трансформації. На відміну від існуючих підходів, що використовують агрегування часткових показників підсистеми через традиційні адитивні моделі згортки без урахування міжпідсистемної взаємодії цифрових ризиків, пропонується підхід обґрунтовується на нелінійному інтегральному показнику, що фіксує синергетичний ефект одночасної дії загроз у фінансових, кадрових та техніко-технологічних підсистемах. Отримане інтегральне значення служить основою для диференційованого вибору стратегічного орієнтиру управління безпекою та забезпечує безпосередній зв'язок між результатами аналітичного оцінювання та управлінськими рішеннями та реалізує методологічний перехід від реактивного до проактивного управління економічною безпекою підприємства;

*набули подальшого розвитку:*

- наукове розуміння категорії «економічна безпека підприємства» шляхом його розширення відповідно до умов цифрової економіки. На відміну від існуючих дефініцій, сформованих у межах захисного, ресурсно-

функціонального, стійкісного та процесного підходів, що не враховують специфіку цифрового середовища, запропоноване визначення трактує економічну безпеку як динамічний стан резистентності суб'єкта господарювання до деструктивних впливів, що забезпечується конвергентним функціонуванням ключових підсистем під наскрізним регулюванням цифрової безпеки як детермінанти міжсистемної стійкості в умовах технологічної трансформації;

- класифікація цифрових ризиків підприємства у розрізі їхнього диференційованого впливу на ключові підсистеми економічної безпеки підприємства. Запропонована типологія структурує цифрові ризики за принципом їхнього каскадного поширення між фінансовою, кадровою та техніко-технологічною підсистемами, що формує теоретичне підґрунтя для обґрунтування необхідності комплексного, а не ізольованого управління економічною безпекою підприємства;

- методичний підхід до оцінювання техніко-технологічної складової економічної безпеки підприємства шляхом розроблення ієрархічної моделі інтегрального оцінювання, що базується на авторській системі цифрово-орієнтованих критеріїв, що забезпечує формалізацію якісних характеристик цифрової зрілості підприємства через їх перетворення в нормовані числові значення з подальшим зваженим агрегуванням в інтегральний індекс техніко-технологічної стійкості, що дозволяє здійснити кількісну діагностику підсистеми в умовах, коли традиційний метричний апарат не відображає специфіки цифрової трансформації технологічного середовища;

- інформаційно-логічна модель системи підтримки прийняття рішень в управлінні економічною безпекою підприємства, яка базується на застосуванні блочно-модульної архітектури та за допомогою принципу горизонтальної інтеграції результатів фінансового, кадрового та техніко-технологічного аналізу дозволяє побудувати єдиний нелінійний інтегральний показник економічної безпеки підприємства, що враховує синергетичний ефект одночасної дії цифрових ризиків у різних функціональних підсистемах.

**Практичне значення одержаних результатів.** Результати дисертаційного дослідження мають важливе прикладне значення та можуть бути використані підприємствами різних галузей для підвищення рівня економічної безпеки в умовах цифрової трансформації. Розроблені теоретичні положення, науково-методичні підходи та прикладний інструментарій орієнтовані на практичне впровадження в системи управління підприємств і вже пройшли апробацію на реальних об'єктах дослідження.

Розроблений методичний інструментарій управління кадровою безпекою підприємства, що включає механізм ідентифікації та аналізу ризиків у сфері управління персоналом, систему цифрового моніторингу поведінкових показників працівників у режимі реального часу та програму підвищення кваліфікації персоналу з питань кібергігієни, впроваджено у діяльність Приватного акціонерного товариства «Дружківський завод металевих виробів» (м. Дружківка). Зазначені розробки дозволили зміцнити систему управління персоналом підприємства з акцентом на цифрову безпеку, мінімізувати ризики витоку конфіденційної інформації та забезпечити стабільність кадрового потенціалу в умовах сучасних викликів цифровізації і людського фактору.

Прикладну модель фінансової безпеки підприємства, засновану на цифровому інструментарії інтелектуального аналізу даних і спрямовану на автоматизацію оцінки фінансових ризиків, моніторинг зовнішніх та внутрішніх загроз фінансовим ресурсам, а також прогнозування їхнього впливу на платоспроможність підприємства впроваджено у діяльність ТОВ «Видавництво Фоліо» (м. Харків). Використання зазначених науково-методичних розробок сприяло суттєвому підвищенню рівня фінансової стійкості підприємства, дозволило приймати більш обґрунтовані управлінські рішення щодо розподілу капіталу та підвищити рівень захищеності фінансових ресурсів від зовнішніх загроз.

Комплекс результатів наукового дослідження, що включає: економіко-математичну модель раннього попередження ризиків банкрутства, механізм

аналізу впливу цифрових технологій на економічну безпеку підприємства та інтегровану інформаційну модель підтримки прийняття як оперативних, так і стратегічних управлінських рішень, впроваджено у систему управління ПрАТ «Інститут керамічного машинобудування «Кераммаш»» (м. Слов'янськ). Впровадження зазначених розробок дозволило підвищити ефективність управлінських процесів, знизити рівень економічних ризиків та забезпечити стабільний розвиток підприємства.

Запропоновані автором наукові положення та практичні рекомендації використано в освітньому процесі при підготовці фахівців економічного профілю. Зокрема, матеріали дисертаційного дослідження впроваджено у навчальний процес Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»» при підготовці: фахівців зі спеціальності 051 «Економіка» за освітньо-професійною програмою «Економіка підприємства» під час викладання на першому (бакалаврському) рівні вищої освіти дисциплін «Інструменти Big Data для бізнесу»; на другому (магістерському) рівні – дисциплін «Моделювання та управління розвитком економічних систем», «Міжнародна економічна безпека».

**Особистий внесок здобувача.** Усі наукові положення, висновки та рекомендації, викладені у дисертаційній роботі, є результатом особистих досліджень здобувача. Самостійно обґрунтовано теоретико-методологічні підходи до визначення сутності та структури економічної безпеки підприємства в умовах цифрової трансформації, зокрема запропоновано авторське трактування зазначеної категорії як складного динамічного стану функціонування суб'єкта господарювання, що відображає здатність системи забезпечувати захищеність економічних інтересів, стійкий розвиток та адаптивність до деструктивних цифрових впливів.

Здобувачем особисто розроблено концептуальну модель формування та управління інтегрованою системою економічної безпеки підприємства, особливістю якої є виокремлення цифрової безпеки як наскрізного координаційного компонента, що пронизує фінансову, кадрову та техніко-

технологічну підсистему й мінімізує ризик виникнення цифрових загроз у суміжних сферах функціонування підприємства.

Особисто розроблено та апробовано методичний інструментарій оцінювання фінансової складової економічної безпеки підприємства на основі алгоритмів машинного навчання із інтеграцією цифрових індикаторів; сформовано авторський підхід до моделювання техніко-технологічної складової безпеки з використанням ієрархічної моделі та апарату нечіткої логіки. Самостійно запропоновано та реалізовано методичний підхід до управління кадровою безпекою підприємства на основі алгоритму виявлення аномалій із семантичним збагаченням даних корпоративного моніторингу.

Здобувачем особисто сформовано архітектуру інформаційної моделі системи підтримки прийняття рішень на основі блочно-модульної структури та розроблено прикладну інформаційну систему комплексної оцінки і моніторингу стану економічної безпеки підприємства на базі фреймворку Streamlit, що забезпечує замкнений цикл управління: від автоматизованого збору та інтелектуального аналізу даних до генерації адаптивних управлінських рекомендацій залежно від виявленого рівня ризику.

**Апробація результатів дисертаційного дослідження.** Основні положення і результати дисертаційного дослідження були апробовані на міжнародних та вітчизняних науково-практичних конференціях: «Сучасні проблеми економіки та бізнесу» (Київ, НАУ, 2022); «Сучасні проблеми моделювання соціально-економічних систем» (Братислава–Харків, ВШЕМ–ХНЕУ ім. С. Кузнеця, 2023); «Розвиток економіки та бізнес-адміністрування: наукові течії та рішення» (Київ, НАУ, 2023, 2024); «Modern Trends in the Development of Scientific Space» (Дрезден, Німеччина, 2024); «Innovations and New Directions in Scientific Research» (Манчестер, Велика Британія, 2025); «Cyber Security and Data Protection 2025» (Львів, Україна, 2025).

**Публікації.** Теоретичні та практичні результати дисертації викладено та опубліковано у 15 наукових працях загальним обсягом 9,95 друк. арк., у тому числі: 2 – у наукових виданнях, включених до наукометричних баз Scopus

та/або Web of Science, 6 –у наукових фахових виданнях України категорії Б, 7 публікацій у матеріалах науково-практичних конференцій. Загальний обсяг опублікованих праць, що належить особисто автору, становить 5,79 д. а.

**Структура та обсяг роботи.** Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 280 сторінок, із них: основний текст – 220 сторінок, список використаних джерел (213 найменувань) – 24 сторінки, 5 додатків на 21 сторінках. Дисертація містить 27 таблиць, 27 рисунків.

## **РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ**

### **1.1. Теоретичні підходи до визначення сутності та структури економічної безпеки підприємства**

Поняття економічної безпеки підприємства є складною, багатоаспектною та міждисциплінарною категорією, стосовно якої в науковій спільноті досі не сформовано єдиного, загальновизнаного підходу до її трактування. У сучасній економічній літературі представлено велику кількість дефініцій цього терміну, що зумовлено відмінностями у наукових школах, методологічних підходах та предметно-об'єктних площинах досліджень.

Протягом останніх десятиліть простежується чітка еволюція наукових поглядів на економічну безпеку підприємства: від вузького трактування, що зосереджувалося переважно на необхідності захисту від зовнішніх і внутрішніх загроз, – до системного, комплексного бачення, у якому економічна безпека виступає не лише як інструмент захисту, а й як основа забезпечення сталого функціонування, розвитку, конкурентоспроможності та адаптації підприємства до змінного середовища.

У науковому дискурсі питання сутності та структури економічної безпеки підприємства є предметом численних досліджень. Вчені пропонують різноманітні підходи до трактування цього поняття, що відображають відмінності в акцентах на мету, завдання, функціональні компоненти та інституційні умови функціонування системи економічної безпеки. Ці підходи умовно можна класифікувати за їх методологічними ознаками, що, у свою чергу, дає змогу узагальнити ключові напрями дослідницького осмислення даної категорії.

Узагальнення існуючих наукових підходів дозволяє систематизувати домінуючі трактування поняття «економічна безпека підприємства» та

виявити різноманітність аналітичних ракурсів, у межах яких розглядається ця категорія. У табл. 1.1 наведено класифікацію підходів до визначення економічної безпеки підприємства із зазначенням їх сутнісних характеристик і відповідних науковців, що представляють ці напрями.

Таблиця 1.1

Підходи до визначення поняття «економічна безпека підприємства»

| Назва підходу              | Суть підходу                                                                                                                                                               | Представники                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1. Захисний                | Економічна безпека як стан захищеності підприємства від внутрішніх та зовнішніх загроз, мінімізація можливих втрат.                                                        | Н.Й. Реверчук [180]<br>О.Ю. Мішин, С.В. Мішина<br><br>[162], А. Іаніогло та Т. Поляєва [49] |
| 2. Ресурсно-функціональний | Ефективне використання ресурсів підприємства (фінансових, кадрових, інформаційних тощо) для забезпечення стабільного функціонування.                                       | С. Ф. Покропивний [134], О.Ф. Яременко [211], Л.І. Донець [131]                             |
| 3. Стійкісний              | Безпека як здатність підприємства витримувати потрясіння, адаптуватися до змін і забезпечувати стабільний розвиток у довгостроковій перспективі.                           | С.П. Дубецька [133], Т.Б. Шири [203]                                                        |
| 4. Гармонізаційний         | Акцент на балансі між інтересами підприємства та зовнішнього середовища (партнери, споживачі, держава), інтеграція в ринкову екосистему.                                   | Г.В. Козаченко [147], Л.Г. Шемаєва [201]                                                    |
| 5. Процесний               | Економічна безпека як безперервний динамічний процес управління ризиками, ресурсами та взаємодією з оточенням; фокус на моніторинг і адаптацію.                            | Ю.О. Бровкіна [118], Л.О. Матвійчук [158],                                                  |
| 6. Динамічний              | Трактування безпеки як динамічного стану функціонування, що забезпечує своєчасне запобігання загрозам, беззбитковість та стабільність результатів через адаптацію до змін. | О. В. Ареф'єва [106], Н. О. Пархоменко [54]                                                 |

Джерело: складено автором

Розглянемо основні визначення економічної безпеки підприємства, які репрезентують підходи, згруповані в табл. 1.1.

Захисний підхід фокусується переважно на убезпеченні життєво важливих інтересів та ресурсів підприємства від деструктивного впливу

внутрішніх і зовнішніх загроз. У межах цього підходу економічну безпеку підприємства доцільно інтерпретувати як сукупність превентивних заходів, що мають на меті нівелювання ризиків та недопущення деструктивного впливу на ресурсний потенціал. Зокрема, у науковому доробку Н. Реверчук [180] акцентовано увагу на функціонуванні системи активної протидії матеріальним, кадровим та фінансовим втратам, за якої фактичні або потенційні збитки не перевищують критично допустимих меж. Зазначене трактування базується на концепції нормативної граничності шкоди, що визначає здатність суб'єкта господарювання зберігати стабільність за умов зовнішнього тиску.

Подальша еволюція теоретичних поглядів представлена у працях О.Ю. Мішина та С.В. Мішиної [162], де категорію «економічна безпека підприємства» розглянуто через призму захищеності бізнес-процесів та їхнього ресурсного базису. Авторами обґрунтовано, що превенція внутрішніх і зовнішніх загроз створює підґрунтя для стабільної операційної діяльності та забезпечує умови для розширеного відтворення з мінімізацією втрат. Такий підхід дозволяє інтегрувати оперативний та стратегічний аспекти управління системою безпеки підприємства в сучасних умовах.

Цікавим є підхід, запропонований А. Іаніогло та Т. Поляєвою [49], які, провівши аналіз еволюції підходів до розуміння поняття, визначають економічну безпеку підприємства як таку, що включає три ключові елементи: економічну незалежність, стійкість до загроз та здатність до розвитку. Таким чином, у межах захисного підходу також поступово формується уявлення про економічну безпеку як структуровану категорію, що поєднує як стани, так і процеси.

Ресурсно-функціональний підхід, який є одним із найпоширеніших у сучасному науковому середовищі, інтерпретує економічну безпеку переважно через ефективне управління ресурсним потенціалом підприємства. Так, С. Ф. Покропивний [134] визначає економічну безпеку як певний стан ресурсів та бізнес-можливостей, за якого забезпечується їх найбільш ефективне

використання для стійкого функціонування і розвитку підприємства з одночасною нейтралізацією внутрішніх і зовнішніх негативних впливів.

У наукових розробках О.Ф. Яременка [211] економічну безпеку визначено як специфічний стан функціонування суб'єкта господарювання, за якого завдяки гранично ефективній експлуатації наявних ресурсів забезпечується нівелювання, демпфування або територіальна локалізація загроз. При цьому наголошується, що в умовах конкурентного середовища реалізація стратегічних цілей підприємства безпосередньо залежить від імплементації інструментарію сучасного менеджменту. Зазначений підхід дає змогу простежити детермінований зв'язок між якістю організаційної системи управління та рівнем захищеності корпоративних інтересів.

У свою чергу, Л.І. Донець [131] наголошує на ефективному використанні ресурсів як передумові стабільного функціонування та сталого розвитку підприємства у майбутньому, чим підкреслює стратегічний аспект ресурсного підходу до безпеки.

Окрему увагу в науковій літературі привертає гармонізаційний підхід, що ґрунтується на розумінні підприємства як відкритої системи, функціонування якої значною мірою залежить від взаємодії із зовнішнім середовищем. У межах цього підходу економічна безпека визначається не лише внутрішнім станом стабільності, а й ступенем узгодженості економічних інтересів підприємства із зовнішніми суб'єктами, а саме партнерами, державними органами, споживачами, тощо.

У науковому доробку Г. В. Козаченко [147] економічну безпеку запропоновано розглядати як міру часової та просторової гармонізації економічних інтересів підприємства з інтересами контрагентів та інших суб'єктів зовнішнього середовища. Такий підхід акцентує увагу на необхідності підтримання динамічної рівноваги та стабільної економічної взаємодії в умовах мінливої ринкової кон'юнктури.

Розвиваючи зазначену концепцію, Л. Г. Шемаєва [201] інтерпретує економічну безпеку як процес забезпечення реалізації стратегічних

пріоритетів підприємства через ефективне використання релевантних можливостей зовнішнього середовища та розбудову продуктивної взаємодії з його суб'єктами. Зазначене трактування зміщує фокус із суто захисної функції на стратегічно-орієнтовану співпрацю, що є необхідною умовою досягнення довгострокових цілей розвитку.

Іншим вагомим напрямом є стійкісний підхід, у межах якого економічна безпека ототожнюється із здатністю підприємства зберігати стабільність та здатність до розвитку навіть за умов деструктивних впливів. Представники цього підходу наголошують на ролі стійкості системи у протидії кризовим явищам.

У наукових розробках С.П. Дубецької [133] економічну безпеку підприємства інтерпретовано як специфічний стан об'єкта в архітектурі його системних зв'язків, що оцінюється через здатність до самовиживання та безперервного розвитку під впливом деструктивних внутрішніх і зовнішніх чинників, зокрема непередбачуваних та складних для прогнозування факторів. У межах зазначеного підходу акцентовано увагу на адаптивності суб'єкта господарювання як фундаментальних передумовах його стабільного функціонування.

Подібну наукову позицію поділяє Т.Б. Шири [203], розглядаючи економічну безпеку як досягнення детермінованого стану підприємства, що забезпечує резистентність до несприятливих екзогенних та ендегенних впливів. Отже, до ключових характеристик даного підходу віднесено збереження внутрішньої цілісності системи та її здатність до саморегуляції.

Ще один важливий науковий напрям – процесний підхід, представники якого наголошують на тому, що економічна безпека не є статичним станом, а динамічним і безперервним процесом управлінської діяльності. У рамках цього підходу забезпечення економічної безпеки включає постійний моніторинг загроз, адаптацію до змін середовища, управління ресурсами та підтримання стабільності підприємства.

Ю. О. Бровкіна [118] прямо вказує на необхідність розглядати економічну безпеку саме як процес, що протікає постійно та безперервно. Така позиція відображає сучасні уявлення про необхідність адаптивного менеджменту у сфері ризиків і стійкості.

У науковому доробку Л. О. Матвійчук [158] представлено комплексне бачення економічної безпеки підприємства як динамічного процесу трансформації суб'єкта господарювання у стан, що характеризується резистентністю до ендегенних та екзогенних деструктивних чинників. У межах цього підходу акцентовано увагу на формуванні конкурентних переваг через оптимізацію використання ресурсного потенціалу, що сприяє просторовій та часовій гармонізації інтересів підприємства із запитам суб'єктів зовнішнього середовища. Така концептуалізація дозволяє забезпечити стабільність операційної діяльності в короткостроковому періоді та сформувати базис для стратегічного розвитку в майбутньому. Отже, застосування процесного підходу дозволяє синтезувати ресурсну, функціональну та гармонізаційну компоненти в єдину аналітичну модель управління.

Логічним розвитком процесного бачення є динамічний підхід, у межах якого економічна безпека розглядається не лише як послідовність дій, а як здатність системи утримувати цільові параметри функціонування у мінливому середовищі. У науковому доробку Т.О. Сімкової та Ю.Ю. Копчі економічну безпеку інтерпретовано як динамічний стан функціонування підприємства, що характеризується здатністю до своєчасного запобігання загрозам зовнішнього середовища та забезпеченням беззбитковості діяльності [188]. Зазначений підхід дозволяє акцентувати увагу на оперативності реагування системи безпеки, що є критично важливим для підтримання фінансово-економічної стійкості в умовах високої волатильності ринків.

Подібна наукова позиція обґрунтовується у працях Н. О. Пархоменко, де під економічною безпекою розуміється динамічний стан суб'єкта господарювання, що забезпечує стабільність результатів його діяльності через

механізми адаптації до варіативних змін ендогенного та екзогенного походження [54]. Таким чином, у межах динамічного підходу акцент зміщується з констатації захищеності на параметри гнучкості та швидкості трансформації системи.

Підсумовуючи викладене, слід зазначити, що наукові підходи до визначення поняття «економічна безпека підприємства» охоплюють як статичні, так і динамічні аспекти функціонування підприємства, враховуючи внутрішні ресурси, зовнішнє середовище, взаємодію з іншими суб'єктами та довгострокову стійкість. Кожне з поданих трактувань відображає специфічний ракурс дослідження та розкриває ті або інші аспекти безпеки – від захисту до розвитку й адаптації. Узагальнена класифікація наведених визначень представлена в табл. 1.2.

Таблиця 1.2

Економічна безпека підприємства як економічна категорія

| Автори                                | Підхід / Визначення                                                                                                                                          |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Захисний підхід</b>                |                                                                                                                                                              |
| Н.Й. Реверчук [180]                   | Система активного захисту від можливих утрат, у якій збитки не перевищують установлених норм.                                                                |
| О.Ю. Мішин, С.В. Мішина [162]         | Стан захищеності бізнес-процесів та ресурсного забезпечення, що дає змогу запобігати загрозам і забезпечує стабільне функціонування з мінімальними втратами. |
| А. Іаніогло, Т. Поляєва [49]          | Економічна безпека включає три елементи: незалежність, стійкість та розвиток.                                                                                |
| <b>Ресурсно-функціональний підхід</b> |                                                                                                                                                              |
| С.Ф. Покропивний [134]                | Стан корпоративних ресурсів і можливостей, що забезпечує їх ефективне використання для розвитку з одночасною нейтралізацією загроз.                          |
| О.Ф. Яременко [211]                   | Стан, за якого ефективне використання ресурсів дозволяє уникати або локалізувати загрози в умовах конкуренції.                                               |
| Л. І. Донець [131]                    | Ефективне використання ресурсів, що забезпечує стабільне функціонування і розвиток у майбутньому.                                                            |
| <b>Гармонізаційний підхід</b>         |                                                                                                                                                              |
| Г.В. Козаченко [147]                  | Міра гармонізації економічних інтересів підприємства та суб'єктів зовнішнього середовища у часі й просторі.                                                  |
| Л.Г. Шемаєва [201]                    | Реалізація стратегічних інтересів підприємства через продуктивну взаємодію із зовнішнім середовищем.                                                         |
| <b>Стійкісний підхід</b>              |                                                                                                                                                              |
| С.П. Дубецька [133]                   | Стан підприємства з погляду його стійкості до загроз і здатності до саморозвитку в умовах дестабілізації.                                                    |
| Т. Б. Шири [203]                      | Досягнення підприємством такого стану, який забезпечує йому здатність протидіяти несприятливим впливам.                                                      |

| <b>Процесний підхід</b>  |                                                                                                                                                                                                                                                      |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ю.О. Бровкіна [118]      | Економічна безпека як безперервний процес моніторингу, аналізу і реагування на загрози для збереження стабільності.                                                                                                                                  |
| Л.О. Матвійчук [158]     | Процес досягнення стану стійкості до загроз, конкурентних переваг і гармонізації інтересів підприємства з його зовнішнім середовищем у коротко- та довгостроковій перспективі.                                                                       |
| <b>Динамічний підхід</b> |                                                                                                                                                                                                                                                      |
| О. В. Ареф'єва [106]     | Динамічний стан функціонування, спрямований на своєчасне запобігання загрозам та забезпечення беззбитковості діяльності підприємства.                                                                                                                |
| Н. О. Пархоменко [54]    | Динамічний стан підприємства, що забезпечує стабільність результатів діяльності на основі адаптації до варіативних змін.                                                                                                                             |
| Авторський підхід        | Складний динамічний стан функціонування підприємства, що через сукупність кількісних та якісних індикаторів відображає здатність системи забезпечувати захищеність економічних інтересів, стійкий розвиток та адаптивність до деструктивних впливів. |

Джерело: складено автором

На основі проведеного аналізу запропоновано розглядати економічну безпеку підприємства як складний динамічний стан його функціонування, що характеризується сукупністю кількісних та якісних показників (індикаторів) здатності системи забезпечувати захищеність економічних інтересів, стійкий розвиток та адаптивність до деструктивних впливів середовища. Це створює методологічне підґрунтя для подальшого використання методів економіко-математичного моделювання, зокрема адаптивних моделей та алгоритмів машинного навчання, з метою прогнозування траєкторії безпечного розвитку підприємства в умовах цифрової трансформації.

Розглянувши сутнісні характеристики економічної безпеки підприємства, доцільним наступним кроком є аналіз чинників, які безпосередньо зумовлюють необхідність її формування – тобто загроз. Саме загрози виступають ключовим елементом, що ініціює потребу в побудові цілісної системи економічної безпеки, визначає її структуру та функціональне наповнення.

У науковій літературі загроза зазвичай розглядається як реально або потенційно можливий вплив, дія чи стан, який порушує нормальні умови функціонування підприємства шляхом заподіяння матеріальної шкоди – прямої або опосередкованої, що, у свою чергу, призводить до фінансових втрат,

у тому числі, у вигляді упущеної вигоди [154]. У цьому контексті запобігання, виявлення, локалізація та нейтралізація загроз економічній безпеці становлять змістовне ядро всієї системи економічної безпеки підприємства.

Причини виникнення загроз економічній безпеці можна умовно поділити за рівнями їхнього походження. З одного боку, вони можуть бути зумовлені зовнішніми макроекономічними, політичними чи інституційними чинниками, що одночасно впливають на широке коло суб'єктів господарювання. У такому випадку загрози набувають системного характеру й стосуються не лише окремого підприємства, а й національної економіки в цілому. До зовнішніх загроз економічній безпеці підприємства традиційно відносять [135]:

- несприятливі зміни політичної ситуації в країні чи регіоні;

- зміну законодавства, що істотно впливає на умови господарської діяльності;

- макроекономічні шоки – інфляцію, фінансово-економічні кризи, розрив виробничо-логістичних ланцюгів;

- втрату ринків збуту або джерел постачання ресурсів;

- недобросовісну конкуренцію, включаючи використання демпінгових цін;

- загрози з боку кримінальних структур;

- шантаж, залякування чи фізичний тиск на керівників підприємств.

З іншого боку, загрози можуть мати мікроекономічну природу й бути наслідком внутрішніх дисфункцій, таких як неефективне управління, кадрові помилки, організаційна нестабільність тощо. У цьому випадку причини криються в управлінських рішеннях самого підприємства або в недосконалості внутрішніх процесів [123; 135]: Серед них можна виокремити:

- низький професійний рівень управлінської ланки;

- порушення трудової дисципліни;

- перевищення повноважень з боку керівників;

- вибір ненадійних контрагентів;

порушення режиму збереження комерційної таємниці;  
масовий відтік кваліфікованих кадрів;  
зниження рівня професійної компетентності персоналу;  
відсутність чіткої системи кар'єрного зростання та мотивації;  
технологічну відсталість;  
зношеність основних фондів;  
недоступність фінансування інноваційних проєктів та відсутність ефективних механізмів кредитування;  
недалекоглядне планування;  
ігнорування ринкових тенденцій або несвоєчасне оновлення бізнес-моделі.

У сукупності розглянуті загрози формують складне та динамічне ризик-середовище, в межах якого функціонує сучасне підприємство. Це середовище характеризується високим ступенем невизначеності, зростанням як зовнішніх, так і внутрішніх ризиків, що зумовлює необхідність розроблення дієвої системи реагування на загрози. У зв'язку з цим система економічної безпеки підприємства розглядається як концептуальна управлінська категорія, яка визначає стратегічні межі і механізми ідентифікації, оцінювання, попередження та нейтралізації загроз економічному функціонуванню організації.

За визначенням З.С. Варналія, економічна безпека підприємства як системне явище характеризується такими загальними властивостями, як розвиток, стійкість, адаптивність, незалежність і інерційність [119]. Ці ознаки дозволяють підприємству зберігати функціональну цілісність, реагувати на зміни середовища та забезпечувати стратегічну орієнтацію. У свою чергу, Т. М. Іванюта та А. О. Заїчковський [141] підкреслюють, що система економічної безпеки повинна мати низку критично важливих характеристик: бути унікальною (відповідною до особливостей конкретного підприємства), самостійною (структурно завершеною), комплексною (такою, що охоплює всі сфери функціонування), дієвою (здатною до практичної реалізації) та

ефективною (орієнтованою на досягнення очікуваних результатів). Наявність цих характеристик забезпечує не лише ліквідацію негативних наслідків реалізованих загроз, а й формує потенціал для попередження нових, ще не ідентифікованих ризиків, сприяючи таким чином стабільному розвитку підприємства.

Узагальнення теоретичних підходів дозволяє констатувати, що система економічної безпеки підприємства репрезентує собою складну сукупність детермінованих елементів: об'єктів, суб'єктів, функціональних складових, методологічного інструментарію оцінювання, а також превентивних і реактивних заходів, реалізація яких забезпечує стабільність, стратегічний розвиток та конкурентоспроможність суб'єкта господарювання. Відповідно до логіки дослідження, архітектуру такої системи доцільно представити у вигляді комплексної схеми (рис. 1.1), що візуалізує взаємозв'язок між її структурними компонентами.

Об'єктом системи економічної безпеки підприємства в узагальненому розумінні виступає його збалансований економічний стан у короткостроковій та стратегічній перспективах [132].

У межах системного підходу будь-який елемент, на який спрямовується управлінський вплив з метою нівелювання загроз, розглядається як об'єкт захисту, формуючи керовану підсистему. Деталізація об'єктів здійснюється за такими напрямками:

- за видами ресурсного забезпечення: фінансові, техніко-технологічні, матеріальні, кадрові, управлінські, а також інтелектуально-інформаційні ресурси, що набувають особливої ваги в умовах цифровізації;

- за сферами функціонування: виробнича, комерційна, інвестиційно-інноваційна та маркетингова діяльність;

- за цільовими показниками: сукупність індикаторів, що підлягають стабілізації або оптимізації для зміцнення загальної економічної резистентності.

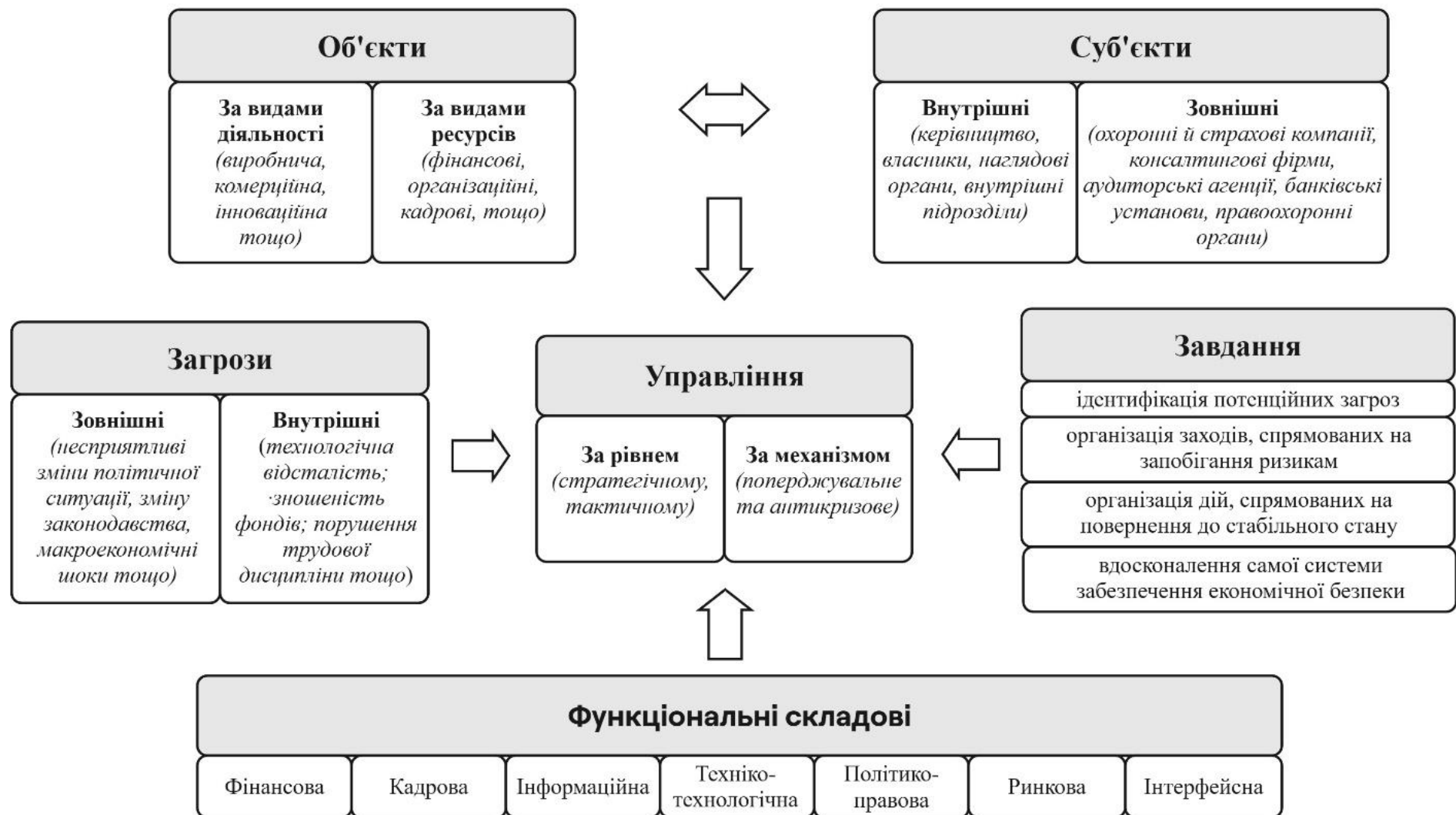


Рис. 1.1. Система економічної безпеки підприємства.

Джерело: складено автором.

Таким чином, об'єкти системи економічної безпеки охоплюють не лише традиційні фактори виробництва, а й бізнес-процеси, організаційні структури та результуючі параметри діяльності підприємства .

Суб'єкти системи економічної безпеки, які формують керуючу підсистему, мають складнішу й більш варіативну природу, оскільки охоплюють як внутрішніх, так і зовнішніх учасників процесу забезпечення безпеки. До внутрішніх суб'єктів зазвичай відносять керівництво підприємства, власників, наглядові органи, внутрішні підрозділи, які безпосередньо виконують функції моніторингу та протидії загрозам. У межах внутрішнього середовища суб'єкти поділяють також за рівнем спеціалізації: спеціалізовані, напівспеціалізовані (юридичні, маркетингові підрозділи) та загальні органи управління [152].

До зовнішніх суб'єктів належать як державні, так і недержавні структури, які сприяють або безпосередньо беруть участь у забезпеченні безпеки підприємства, зокрема охоронні й страхові компанії, консалтингові фірми, аудиторські й кадрові агенції, банківські установи, а також правоохоронні органи, державні регуляторні служби, судові та інші інститути публічної влади, науково-дослідні й освітні організації. Участь зовнішніх суб'єктів забезпечує доступ до спеціалізованих знань, ресурсів і правових механізмів, а також сприяє підвищенню рівня прозорості, підзвітності та легітимності заходів безпеки.

Головною метою системи управління економічною безпекою підприємства є не лише реагування на вже наявні загрози, а насамперед – прогнозування та випередження можливих деструктивних впливів, які можуть призвести до кризового стану. Особливе значення в цій системі відіграє антикризове управління, орієнтоване на локалізацію наслідків негативних подій, стабілізацію діяльності підприємства, мінімізацію економічних втрат та забезпечення швидкого відновлення. У цьому контексті ключовим завданням системи економічної безпеки є формування механізмів раннього

попередження загроз, своєчасного ухвалення рішень і практичної реалізації превентивних заходів економіко-правового та організаційного характеру.

Система економічної безпеки реалізує свою функцію шляхом виконання низки інтегрованих завдань, які забезпечують її ефективність і комплексність. До таких завдань належать [129]:

- ідентифікація потенційних загроз і слабких місць у функціонуванні підприємства, тобто прогнозування сценаріїв дестабілізації.
- організація заходів, спрямованих на запобігання ризикам, що передбачає впровадження систем моніторингу, аналізу зовнішнього середовища та розроблення резервних стратегій.
- оперативне виявлення, аналіз і оцінювання вже реалізованих загроз, що дозволяє швидко реагувати на ситуації, які загрожують безперервності бізнесу.
- організація комплексу дій, спрямованих на реагування, ліквідацію наслідків і повернення до стабільного функціонування.
- вдосконалення самої системи забезпечення економічної безпеки шляхом інституційних змін, оновлення політик, стандартів, процедур і впровадження сучасних управлінських технологій.

Розглянувши сутнісні аспекти поняття економічна безпека підприємства, доцільним наступним кроком є аналіз її внутрішньої структури, зокрема функціональних складових. Саме через вивчення складових економічної безпеки можливо конкретизувати її зміст, визначити напрями управління та створити підґрунтя для побудови дієвої системи забезпечення безпеки на підприємстві.

Функціональні складові економічної безпеки підприємства можна визначити як сукупність відносно самостійних, але взаємопов'язаних напрямів, що відображають окремі сфери економічного життя підприємства, захист і розвиток яких є необхідною умовою стабільного функціонування суб'єкта господарювання. Оскільки саме поняття економічної безпеки

трактується науковцями по-різному, відповідно відрізняються й підходи до визначення її складових.

Аналіз наукових джерел свідчить про значну варіативність поглядів на структурну побудову системи економічної безпеки. Дослідники подають як узагальнені, так і деталізовані переліки складових, інтерпретуючи їх відповідно до обраної методології, предметного поля дослідження та зовнішньоекономічного контексту.

Так, Й. М. Петрович [173] пропонує детальну структуру, що включає такі складові: екологічну, енергетичну, інтелектуальну, інтерфейсну, інформаційну, кадрову, політико-правову, ресурсну, ринкову, силову, соціальну, техніко-технологічну та фінансову. Такий підхід дозволяє охопити широку палітру аспектів безпеки підприємства, однак водночас ускладнює їх системне інтегрування в єдину модель управління.

Ю.О. Ярова та Л.П. Артеменко [213] також поділяють систему економічної безпеки на ряд складових, зокрема: фінансову, інтелектуальну, кадрову, соціальну, технічну, технологічну, юридичну, ринкову, інтерфейсну, інформаційну, екологічну, силову, енергетичну та інноваційну. Представлене бачення орієнтоване на повне охоплення як внутрішніх, так і зовнішніх факторів, що впливають на стабільність підприємства.

У дослідженнях О.В. Арєф'євої та Т.Б. Кузенко [106] структура економічної безпеки представлена через такі складові, як фінансова, інтелектуальна, техніко-технологічна, політико-правова, ресурсна, екологічна, соціальна, інформаційна, силова та безпека праці. Авторки акцентують увагу на збереженні виробничого потенціалу, підтримці правової захищеності та забезпеченні безпечних умов праці як ключових функціональних напрямків безпеки.

На думку Л. М. Худолія [199], ефективна система економічної безпеки потребує концентрації на п'яти базових складових, а саме: фінансовій, інформаційній, техніко-технологічній, кадровій та правовій. Такий підхід

спрямований на забезпечення керованості та фокусування управлінських рішень на найбільш уразливих зонах підприємницької діяльності.

В. Г. Алькема [161] виокремлює інформаційну, кадрову, фізичну, техніко-технологічну та фінансову складові. Цей підхід передбачає системну інтеграцію організаційних, ресурсних і технологічних аспектів у єдине поле безпеки.

М. Журавель [138] пропонує ієрархізовану модель економічної безпеки залежно від рівня реалізації: на поточному рівні – фінансова, морально-психологічна, силова та інформаційна складові; на тактичному – виробничо-технічна, кадрова, комерційна та правова; на стратегічному – інноваційно-технологічна, інтелектуальна, ринкова, екологічна та безпека репутації. Такий підхід дозволяє врахувати не лише функціональну різноманітність, але й часовий горизонт впливу безпекових чинників.

Окремі науковці також висувують додаткові пропозиції щодо розширення структури економічної безпеки. Наприклад, О. Ф. Яременко [212] підкреслює значення міжнародної складової, яка набуває особливої актуальності у контексті євроінтеграційних процесів і глобалізації. За її визначенням, така складова покликана забезпечувати безпеку зовнішньоекономічної діяльності підприємства. І.Н. Карпунь [143], у свою чергу, доповнює класифікацію техногенною та інтерфейсною складовими, що відображають загрози, пов'язані з технічними ризиками та організаційною взаємодією.

Разом з тим, надмірна деталізація структури економічної безпеки, що включає морально-психологічну чи силову складові, викликає певні застереження. На наш погляд, включення елементів, які мають переважно соціальний або опосередковано економічний характер, ускладнює управлінське оперування системою безпеки.

Проаналізувавши наявні підходи, вважаємо обґрунтованим виділення таких базових функціональних складових системи економічної безпеки підприємства:

- фінансову
- кадрову,
- техніко-технологічну,
- інформаційну,
- політико-правову,
- ринкову,
- інтерфейсну.

Кожна зі складових відіграє специфічну роль у забезпеченні загальної стійкості суб'єкта господарювання.

Фінансова складова традиційно розглядається як фундамент економічної безпеки, що полягає у забезпеченні стабільної платоспроможності, фінансової незалежності та здатності підприємства акумулювати ресурси для виконання стратегічних завдань. Водночас в умовах цифрової трансформації її зміст доповнюється необхідністю управління специфічними цифровими активами, підвищенням швидкості фінансових транзакцій та забезпеченням стійкості до кіберзагроз у платіжних і банківських системах.

Кадрова складова спрямована на формування якісного кадрового потенціалу, забезпечення ефективної системи мотивації та запобігання відтоку кваліфікованих працівників. У цифровій парадигмі акцент зміщується на розвиток специфічних цифрових компетенцій персоналу та протидію внутрішнім загрозам, що пов'язані з методами соціальної інженерії та порушенням кібергігієни в умовах дистанційної роботи.

Техніко-технологічна складова відображає ступінь відповідності виробничої бази сучасному рівню науково-технічного прогресу та здатність до модернізації основних засобів. Для підприємств, що проходять стадію цифровізації, ця складова еволюціонує в бік безпеки кіберфізичних систем, де критичного значення набуває стабільність інтегрованих програмно-апаратних комплексів, технологій Індустрії 4.0 та Інтернету речей.

Інформаційна складова у класичному розумінні забезпечує захист комерційної таємниці та якісне наповнення управлінських рішень

достовірними даними. В умовах цифровізації вона стає системоутворюючим елементом, оскільки економічна стійкість тепер прямо залежить від здатності обробляти «великі дані» у реальному часі та забезпечувати високу здатність до відновлення усієї інформації підприємства.

Політико-правова складова фокусується на забезпеченні юридичної чистоти діяльності, дотриманні норм законодавства та захисті прав власності й інтересів підприємства в судовому порядку.

Ринкова складова характеризує здатність підприємства утримувати та розширювати свою частку на ринку, забезпечувати конкурентоспроможність продукції та стабільність каналів збуту.

Інтерфейсна складова орієнтована на формування верифікованої системи взаємодії з контрагентами, інституціями державної влади та іншими суб'єктами екзогенного середовища з метою гармонізації сукупних економічних інтересів.

Таким чином, запропонована автором структура функціональних складових економічної безпеки підприємства дозволяє здійснювати комплексне оцінювання як поточного рівня його захищеності, так і адаптивного потенціалу розвитку в умовах високої волатильності ринкового середовища. Наукова новизна підходу полягає у переосмисленні пріоритетності складових та їх змістовного наповнення крізь призму цифрової трансформації, що дозволяє ідентифікувати специфічні вразливості, які раніше не враховувалися в класичних моделях безпеки, а саме: необхідність інтеграції ризиків цифровізації активів у систему забезпечення фінансової стійкості, гарантування безпеки кіберфізичних систем та стабільності програмно-апаратних комплексів, пріоритетність формування цифрових компетенцій персоналу для нейтралізації внутрішніх загроз і витоку даних, а також забезпечення цілісності та достовірності інформаційних ресурсів в умовах активізації зовнішніх втручань (рис. 1.2).



Рис. 1.2. Структура системи економічної безпеки підприємства в умовах цифровізації.

Джерело: складено автором на основі [213, 164]

Це створює необхідне методологічне підґрунтя для подальшого деталізованого аналізу кожної зі складових з позицій їх інструментального забезпечення, діагностики та економіко-математичного моделювання процесів управління ризиками в умовах інтенсивної цифровізації бізнес-процесів.

Управління економічною безпекою підприємства інтерпретується як безперервний багаторівневий процес, орієнтований на підтримання стабільного функціонування суб'єкта господарювання в детермінованих та стохастичних умовах мінливого зовнішнього середовища. Цільова спрямованість зазначеного процесу полягає у забезпеченні фінансової рівноваги, систематизації отримання прибутку, реалізації стратегічних пріоритетів, а також зміцненні конкурентних позицій та створенні передумов для інтенсивного розвитку на всіх етапах життєвого циклу організації. Управління економічною безпекою постає як системна діяльність, що інтегрує механізми оперативного реагування на виклики, прогностичне оцінювання потенційних ризиків, адаптацію до динаміки ринкової кон'юнктури та перманентну оптимізацію внутрішніх бізнес-процесів [164].

Процес управління безпекою зазвичай розглядається у двох ієрархічних вимірах – стратегічному та тактичному. На стратегічному рівні управління економічною безпекою охоплює довгострокове планування, оцінку загроз підприємства, формування системи стратегій реагування на ризики, а також забезпечення реалізації управлінських рішень через узгодження з місією, цілями та ресурсним потенціалом організації. Стратегічне управління передбачає комплексний аналіз зовнішнього середовища, моніторинг конкурентної ситуації, визначення критичних вразливих точок і розробку інтегрованих моделей забезпечення безпеки, орієнтованих на стійкий розвиток [183].

У науковій літературі простежуються різні підходи до класифікації стратегій управління економічною безпекою. Наприклад, Т.М. Іванюта та А. О. Заїчковський [141] виокремлюють три базові типи стратегій: стратегії раптового реагування, що передбачають швидке усунення вже реалізованих

загроз; стратегії прогнозування небезпек, які акцентують на системному вивченні ситуації як усередині підприємства, так і в його оточенні; а також стратегії відшкодування, що спрямовані на мінімізацію втрат та відновлення стійкості. Більш розширену класифікацію пропонує Т.Г. Васильців та співавтори [121], які виокремлюють такі види стратегій: швидкого реагування, послідовного зміцнення, системного планового забезпечення, комплексного гарантування, відшкодування збитків, раптового реагування, сегментованого забезпечення, часткового врахування, а також делегування функцій.

Узагальнюючи зазначене, можна виділити три функціональні групи стратегій управління економічною безпекою:

- спрямовані на попередження загроз;
- реалізуються з метою усунення вже існуючих ризиків;
- зосереджені на відновленні належного рівня безпеки після настання деструктивних подій.

Для обґрунтованого вибору стратегії необхідним є глибокий аналіз внутрішнього стану підприємства, зокрема його ресурсного забезпечення, організаційної структури, а також особливостей зовнішнього середовища.

Реалізація тактичного рівня управління економічною безпекою здійснюється в межах операційної діяльності суб'єкта господарювання та виступає механізмом імплементації стратегічних орієнтирів у релевантних ринкових умовах. Зазначений рівень передбачає проектування альтернативних сценаріїв розвитку подій, проведення компаративного оцінювання рівня економічної безпеки за кожним із них, обґрунтування оптимальної траєкторії та розроблення відповідного оперативного плану заходів. Такі плани, на відміну від стратегічних, містять як якісні, так і кількісні параметри: конкретні заходи, строки їх реалізації, відповідальних осіб, очікувані результати [206]. У межах тактичного управління здійснюється оперативне реагування на загрози, приймаються антикризові рішення та реалізуються превентивні дії у короткостроковій перспективі.

Забезпечення ефективного управління економічною безпекою суб'єкта господарювання є визначальним чинником підтримки гомеостазу економічної системи, а також превенції соціальних, трудових та організаційних колізій, здатних деструктивно вплинути на її цілісність. У межах функціонування зазначеної системи пріоритетне значення має реалізація комплексного інструментарію практичних заходів, орієнтованих на нівелювання ризиків та формування сприятливого середовища для стабільної динаміки розвитку. Відповідно до класифікації, запропонованої О. В. Васильєвим та В. І. Мейтою [120], такі заходи можуть бути структуровані за напрямками:

- правові (забезпечення відповідності діяльності підприємства чинному законодавству),
- фінансово-економічні (зміцнення фінансової самостійності, зростання вартості активів, посилення ринкових позицій),
- силові (захист ресурсів підприємства від фізичних загроз і неправомірних дій),
- інформаційні (моніторинг зовнішнього та внутрішнього середовища, аналітична підтримка управлінських рішень),
- техніко-технологічні (впровадження сучасних технологій та оновлення матеріально-технічної бази),
- інноваційні (застосування новітніх рішень для забезпечення стійкої конкурентоспроможності).

Важливою концептуальною категорією в межах управління економічною безпекою є механізм її забезпечення (рис. 1.3). Його слід розуміти як впорядковану сукупність процесів, процедур і управлінських рішень, які забезпечують досягнення цілей системи безпеки та її динамічну стабільність [184]. Структурно доцільно поділяти механізм управління на два основні підвиди – попереджувальне (превентивне) управління та антикризове реагування [179].



Рис. 1.3. Механізм забезпечення економічної безпеки підприємства.

Джерело: складено автором на основі [183, 184, 120].

Попереджувальне управління ґрунтується на стратегічному аналізі, прогнозуванні змін у зовнішньому і внутрішньому середовищі, виявленні потенційних ризиків і розробленні заходів щодо їх недопущення. Воно включає планування розвитку підприємства з урахуванням вразливостей, системне оновлення управлінських процедур, інвестиції в інновації, інформаційні технології та організаційну культуру.

Антикризове управління є реакцією на вже реалізовані загрози. Воно передбачає оперативне ухвалення рішень, мобілізацію ресурсів, ліквідацію наслідків та стабілізацію основних параметрів функціонування підприємства. Його ефективність визначається здатністю підприємства швидко скоротити втрати, відновити рівновагу та повернутися до стійкого розвитку.

Таким чином, управління системою економічної безпеки підприємства охоплює стратегічне передбачення і прогнозування, тактичну реалізацію управлінських рішень, а також динамічну побудову механізмів реагування. Її ефективність залежить від наявності злагодженої системи цілей, процедур, організаційних структур та інформаційно-аналітичного забезпечення, що дозволяє підприємству функціонувати в умовах невизначеності, адаптуватися до зовнішніх викликів і реалізовувати потенціал сталого розвитку.

## **1.2. Особливості впливу цифрової трансформації на економічну безпеку підприємства**

Цифрові технології стрімко інтегрувалися у більшість сфер суспільного життя, охоплюючи освіту, засоби масової інформації, робоче середовище, повсякденні побутові практики, торгівлю, спорт, охорону здоров'я та розваги. Формування цифрового суспільства передбачає створення складної, проте цілковито трансформованої екосистеми, у якій технології та люди співіснують у нових формах спільного життя та взаємодії.

Процес цифрової трансформації характеризується високим рівнем ресурсомісткості, часовою тривалістю та складністю імплементації, що є особливо критичним для суб'єктів малого та середнього підприємництва. Зазначені обставини зумовлюють необхідність чіткої формалізації цифрових стратегій із детермінацією пріоритетних векторів трансформаційних змін. Відповідно до визначених пріоритетів, підприємства мають адаптувати внутрішню архітектуру та впроваджувати інноваційні рішення як

технологічного, так і методологічного спрямування. Доведено, що в умовах цифрової трансформації забезпечення економічної безпеки підприємства потребує переходу до моделі адаптивного управління бізнес-процесами на основі інформаційно-комунікаційних технологій, що дозволяє модернізувати технології управління відповідно до динамічних ринкових умов та підвищити рівень довіри стейкхолдерів до діяльності суб'єкта господарювання. Попри потенційний позитивний ефект, імплементація таких рішень генерує специфічні загрози та ризики, що потребує інтеграції механізмів гарантування економічної безпеки на рівні всіх функціональних підсистем організації.

У сучасному науковому дискурсі спостерігається значна варіативність дефініцій «цифрова трансформація підприємства», що пояснюється багатоаспектністю цього феномену. Загалом цифровізація розглядається як багатовимірний процес, що інтегрує технологічні, управлінські, соціокультурні та стратегічні вектори функціонування суб'єктів господарювання.

Згідно з позицією С. Бермана [15], цифрова трансформація постає як послідовність загальноорганізаційних трансформацій у системі менеджменту та інформаційних технологій, що реалізуються у відповідь на динамічні виклики екзогенного середовища. Водночас Г. Віал [99] інтерпретує цифрову трансформацію як процес, у якому цифрові технології виступають тригером стратегічного збурення. Це змушує організації переосмислювати існуючі моделі створення цінності, адаптуючись до нових конкурентних умов шляхом нівелювання організаційних бар'єрів та здійснення структурних перебудов.

Інші науковці, зокрема І. Гьокальп і В. Мартінес [42], наголошують на революційному характері цифрової трансформації, вбачаючи в ній каталізатор появи нових бізнес-моделей та операційних підходів у різних секторах економіки. Також вагомий внесок у розвиток цього поняття зробили Ф. Фіцджеральд та інші [38], які акцентують увагу на прикладному аспекті, визначаючи цифрову трансформацію як впровадження цифрових технологій (штучний інтелект, соціальні мережі, мобільні пристрої, аналітика) з метою

вдосконалення бізнес-процесів, поліпшення клієнтського досвіду або оптимізації бізнес-моделей. Лю та інші дослідники [67] підкреслюють, що цифрова трансформація виходить за межі простого редизайну бізнес-процесів або інтеграції новітніх технологій, передбачаючи фундаментальне переосмислення операційної діяльності підприємства, спрямоване на максимальне використання його конкурентних переваг шляхом застосування цифрових рішень.

Значна частина визначень також формується в практичній площині на основі підходів провідних міжнародних корпорацій. Так, компанія IBM [76] визначає цифрову трансформацію як ініціативу бізнес-стратегії, що охоплює всі напрями діяльності організації та передбачає модернізацію її процесів, продуктів, операцій і технологічного стеку задля забезпечення швидких і клієнтоорієнтованих інновацій. Згідно з трактуванням Salesforce [100], цифрова трансформація є процесом створення або зміни існуючих бізнес-процесів, культури та клієнтського досвіду за допомогою цифрових технологій у відповідь на динаміку ринку. У свою чергу, Hewlett Packard Enterprise [32] акцентує увагу на інтеграції цифрових підходів до традиційних бізнес-методів, що супроводжується трансформацією організаційної культури, постійним експериментуванням та адаптацією до нових умов.

Українські науковці також зробили помітний внесок у розвиток теорії цифрової трансформації. Так, Ю.П. Воржакова та О.І. Хлебінська [127] визначають її як перехід підприємства на новий рівень функціонування шляхом трансформації моделей управління, бізнес-процесів та загальної структури діяльності із залученням цифрових технологій. Ю.О. Нікітін та О.І. Кульчицький [165] підкреслюють, що цифрова трансформація – це не лише впровадження інновацій, а цілісний процес змін, що базується на стратегічному партнерстві між усіма учасниками, розробці цифрових сервісів і програмного забезпечення, а також на постійному оцінюванні її ефективності. На думку І. М. Шопіної [205], цифрова трансформація є процесом глибокого перетворення організації, управлінських функцій,

інформаційної культури та свідомості учасників ринку за допомогою цифрових інструментів. Узагальнення всіх визначень цього поняття наведене у табл. 1.3.

Таблиця 1.3

Узагальнення підходів до трактування поняття «цифрова трансформація підприємства»

| Автор                                 | Визначення поняття «цифрова трансформація»                                                                                                                                                                                                                     |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| С. Берман [15]                        | Серія загальноорганізаційних змін в інформаційних технологіях та управлінні, що відбуваються у відповідь на зміни у зовнішньому середовищі.                                                                                                                    |
| Г. Віал [99]                          | Процес, у якому цифрові технології виступають чинником стратегічного збурення, що змушує організації переосмислювати моделі створення цінності, адаптуючись до нових умов шляхом подолання організаційних бар'єрів і впровадження структурних змін.            |
| І. Гьокальп, В. Мартінес [42]         | Технологічне революційне досягнення, яке є каталізатором появи нових бізнес-моделей та операційних підходів у різних секторах економіки.                                                                                                                       |
| Ф. Фіцджеральд та інші [38]           | Впровадження цифрових технологій з метою вдосконалення бізнес-процесів, покращення клієнтського досвіду або оптимізації бізнес-моделей.                                                                                                                        |
| Д. Лю та інші [67]                    | Фундаментальне переосмислення операційної діяльності підприємства для повного використання його конкурентних переваг шляхом цифрових рішень.                                                                                                                   |
| IBM [76]                              | Бізнес-ініціатива, яка охоплює всі напрями діяльності організації та передбачає модернізацію процесів, продуктів, операцій і технологічного стеку.                                                                                                             |
| Salesforce [100]                      | Процес створення або зміни бізнес-процесів, культури та клієнтського досвіду за допомогою цифрових технологій у відповідь на зміну ринкових умов.                                                                                                              |
| Hewlett Packard Enterprise [32]       | Процес зміни традиційних бізнес-методів шляхом інтеграції цифрових підходів у діяльність організації та зміни способу створення цінності.                                                                                                                      |
| Ю.П. Воржакова, О.І. Хлебінська [127] | Трансформація суб'єкта господарювання на якісно новий щабель функціонування, що реалізується через модифікацію управлінських моделей, реінжиніринг бізнес-процесів та перебудову структури операційної діяльності на основі імплементації цифрових технологій. |
| Ю. О. Нікітін, О.І. Кульчицький [165] | Комплексний процес організаційних перетворень, підґрунтям якого є розбудова партнерської взаємодії між учасниками екосистеми, генерування цифрових сервісів, проектування програмних рішень та моніторинг результативності впроваджених інновацій.             |
| І. М. Шопіна [205]                    | Процес глибокого перетворення організації, управлінських функцій, інформаційної культури та свідомості учасників ринку через використання цифрових інструментів.                                                                                               |

Джерело: складено автором

Доповнюючи наведені дефініції, слід врахувати підхід А. М. Штангрета та І. М. Підгородецького [207], які стверджують, що сучасне сприйняття економічної безпеки підприємства вимагає формування єдиного системного підходу, що не втрачає актуальності у зв'язку із постійними змінами в умовах діяльності економічних суб'єктів та необхідністю адаптації до них. Це дозволяє розглядати цифрову трансформацію не лише як сукупність технологічних змін, а як фундамент для розбудови цілісної та гнучкої системи безпеки.

Таким чином, аналіз наукових і прикладних підходів до трактування цифрової трансформації свідчить про багатовимірність цього феномену, що охоплює як технологічні, так і управлінські, організаційні та культурні аспекти розвитку підприємства. Це створює необхідне підґрунтя для подальшого аналізу впливу цифрової трансформації на окремі компоненти системи економічної безпеки підприємства.

Отже, аналіз різних підходів до визначення цифрової трансформації підприємства дозволяє зробити висновок, що цей процес безпосередньо пов'язаний із впровадженням сучасних цифрових технологій з метою вдосконалення існуючих або створення нових бізнес-процесів.

Цифрова трансформація не є уніфікованим процесом, оскільки вона може реалізовуватися різними шляхами залежно від специфіки підприємства, його цілей, ресурсної бази та стратегічного бачення. У цьому контексті важливо не лише визначити сам факт цифрових змін, а й чітко окреслити інструментарій, за допомогою якого відбувається така трансформація. Як свідчать аналітичні дослідження компанії Accenture [3], найбільш масштабне впровадження цифрових рішень у сучасних організаціях відбувається завдяки хмарним технологіям, штучному інтелекту та Інтернету речей. У межах даного дослідження було здійснено систематизацію ключових інструментів цифрової трансформації підприємства та охарактеризовано їхній потенційний вплив на бізнес-процеси, що узагальнено у табл. 1.4.

**Основні інструменти цифрової трансформації підприємства та їх вплив на  
бізнес-процеси**

| <b>№</b> | <b>Технологія</b>                 | <b>Визначення</b>                                                                                                  | <b>Потенційний вплив на бізнес-процеси</b>                                                                           |
|----------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| 1        | Хмарні технології                 | Гнучкі, масштабовані та безпечні сервіси для зберігання, обробки й управління даними, що доступні через інтернет   | Зменшення витрат на ІТ-інфраструктуру, прискорення цифрової трансформації, централізований доступ до даних і систем. |
| 2        | Інтернет речей (IoT)              | Мережа фізичних пристроїв з вбудованими сенсорами, які збирають та обмінюються даними.                             | Автоматизація обліку та обслуговування, підвищення ефективності виробництва, аналітика в режимі реального часу.      |
| 3        | Мобільні технології               | Застосування смартфонів, планшетів, AR- та VR-додатків для бізнес-операцій, маркетингу та навчання.                | Підвищення взаємодії з клієнтами, інноваційне навчання персоналу, розширення цифрових каналів продажів і підтримки.  |
| 4        | Робототехніка та RPA              | Робототехніка – фізичні пристрої для автоматизації; RPA – програмні агенти для рутинних офісних задач.             | Зниження витрат і помилок, підвищення продуктивності, звільнення персоналу для стратегічних завдань.                 |
| 5        | Big Data та штучний інтелект (AI) | Інструменти для збирання, зберігання, аналізу великих обсягів даних у поєднанні з алгоритмами прогнозування та ML. | Підвищення точності управлінських рішень, прогнозування попиту, адаптивне управління, персоналізація сервісу.        |

Джерело: складено автором на основі [178, 84, 170]

Загалом, упровадження інформаційно-комунікаційних технологій, штучного інтелекту, Інтернету речей та хмарних сервісів сприяє формуванню інтегрованого цифрового середовища, у якому бізнес-процеси здійснюються з мінімальними витратами часу та ресурсів. Таке середовище не лише забезпечує автоматизацію рутинних операцій, а й дозволяє використовувати аналітику великих даних для підтримки управлінських рішень, активно розвивати канали електронної комерції та поглиблювати взаємодію з клієнтами.

Процеси цифровізації охоплюють широке коло напрямів, серед яких ключовими є: удосконалення виробничих і управлінських процесів, створення

нових цифрових продуктів і сервісів, розроблення гнучких бізнес-моделей [212]. Дослідження показують, що найбільш відчутний вплив цифрові технології справляють на такі елементи бізнес-процесів, як: взаємодія з клієнтами, формування ціннісної пропозиції, а також управління внутрішньою інфраструктурою підприємства [139].

Значущість та масштабність трансформаційних процесів у цифровій площині підтверджуються динамічними показниками розвитку відповідного глобального ринку. За результатами аналітичного звіту компанії Fortune Business Insights, обсяг світового ринку цифрової трансформації у 2023 році становив 1961,30 млрд дол. США. Очікується, що до 2032 року цей показник зросте до 10944,65 млрд дол. США. Таким чином, середньорічний темп приросту протягом прогностного періоду оцінюється на рівні 22%, що свідчить про інтенсифікацію впровадження цифрових рішень у світову економіку [33].

Такі темпи зростання зумовлені стрімким впровадженням концепцій «Індустрії 4.0», активним розвитком хмарних обчислень, аналітики великих даних, інтернету речей, а також інших інноваційних цифрових рішень. Ці технології формують нові підходи до побудови бізнес-моделей та сприяють підвищенню гнучкості підприємств в умовах цифрової економіки. Наприклад, лише чотири провідні американські компанії планують інвестувати протягом 2025 року близько 320 млрд дол. США у розвиток технологій штучного інтелекту, що підкреслює стратегічну важливість цієї технології для прискорення цифрової трансформації та забезпечення конкурентних переваг [92].

Європейський Союз також демонструє позитивну динаміку цифровізації бізнесу. У 2023 році 59 % підприємств країн ЄС досягли принаймні базового рівня цифрової інтенсивності. Варто зазначити, що серед малих і середніх підприємств цей показник становив 58 %, тоді як серед великих підприємств – 91 % [47]. Згідно з методологією індексу цифрової інтенсивності, базовий рівень передбачає використання щонайменше 4 з 12 цифрових технологій, серед яких: хмарні обчислення, CRM-системи, присутність в соціальних

мережах, електронна комерція або технології штучного інтелекту. У межах реалізації програми Digital Decade, однією з цілей ЄС є досягнення показника не менше 90 % МСП із базовим рівнем цифрової інтенсивності до 2030 року [37].

Аналогічні процеси спостерігаються і в інших регіонах світу. Зокрема, за даними дослідження «Аналіз цифрової трансформації малих і середніх підприємств», у 2021 році близько 79 % МСП у Китаї перебували на початковій стадії цифрової трансформації [89]. Це свідчить про глобальний характер викликів цифровізації бізнесу, зокрема для малого та середнього сегменту.

Цифрова трансформація в Україні має свої особливості, зумовлені як стратегічним баченням держави, так і соціально-економічним контекстом. Зокрема, цифровізація визначена одним із пріоритетів державної політики в аспекті посилення економічної безпеки та модернізації публічного управління. За даними Всесвітнього банку та Організації економічного співробітництва та розвитку, Україна активно впроваджує цифрові інструменти в межах ініціативи «Держава у смартфоні», що має на меті розширення доступу до електронних адміністративних послуг, спрощення регуляторних процедур, підвищення прозорості державного управління та зменшення адміністративного тиску на бізнес. Згідно з Індексом розвитку електронного урядування ООН за 2024 рік, Україна посіла 5-те місце серед 193 країн світу за рівнем розвитку цифрових державних послуг, демонструючи суттєвий прогрес порівняно з 102-ою позицією у 2018 році [36]. Така динаміка свідчить про послідовне втілення національної цифрової стратегії та вагомі результати в частині цифрового реформування державного сектора. Разом з тим, як зазначають А. М. Штангрет та інші [208], попри успіхи державного сектору, низька ініціативність вітчизняного бізнесу та вимушене гальмування інвестиційних процесів в умовах воєнної агресії суттєво послаблюють конкурентні позиції підприємств. Авторами обґрунтовано, що цифрова трансформація в Україні є об'єктивною необхідністю для виживання та підготовки до післявоєнної відбудови, коли внутрішній ринок стане більш

відкритим для іноземних конкурентів, що вимагатиме від національних виробників випереджального формування цифрового фундаменту.

Утім, розвиток цифрової інфраструктури в корпоративному секторі України супроводжується рядом системних викликів. Це, зокрема, стосується низького рівня цифрової зрілості більшості підприємств, обмеженої інтеграції цифрових інструментів у господарську діяльність, а також нестачі інвестицій у цифрову модернізацію виробничих і управлінських процесів. Ілюстрацією цього є частка підприємств, що використовували окремі цифрові технології в Україні станом на 2024 рік (рис. 1.4).



Рис. 1.4. Рівень використання цифрових технологій підприємствами України у 2024 році.

Джерело: складено автором на основі [124]

Як видно з наведених даних, частка підприємств, що застосовують ключові цифрові інструменти такі як електронна торгівля, штучний інтелект та інструменти ВІ залишається відносно низькою та не перевищує 10% від всіх підприємств. Найбільш поширеним цифровим елементом є лише базова наявність фіксованого доступу до мережі Інтернет (93,8%), в той час як базовий вебсайт мають лише третина всіх українських підприємств, що

свідчить про поверхневий рівень цифровізації. Це вказує на те, що загальний рівень цифрової готовності українського бізнесу є недостатнім для повноцінного використання потенціалу цифрової економіки. Подолання цього розриву потребує цілеспрямованої державної політики підтримки цифровізації підприємств, особливо у сегменті малого та середнього бізнесу.

Враховуючи наведені вище статистичні дані та особливості цифрової трансформації в Україні, постає необхідність глибше розглянути її вплив на діяльність підприємств. Цифровізація господарських процесів не лише змінює підходи до управління ресурсами, виробництвом та взаємодією з клієнтами, а й формує нову парадигму конкурентної поведінки на ринку. Проте, як і будь-яке системне нововведення, цифрова трансформація має як переваги, так і певні обмеження, які потребують всебічного аналізу.

У подальшому викладі буде розглянуто основні переваги цифрової трансформації, що проявляються в підвищенні ефективності операційної діяльності, зміцненні конкурентних позицій, адаптивності до зовнішніх змін, якості взаємодії з клієнтами та розвитку інноваційних бізнес-моделей.

1. Підвищення операційної ефективності. Запровадження цифрових технологій дозволяє підприємствам суттєво зменшити транзакційні витрати, пов'язані з координацією діяльності, комунікацією та реалізацією бізнес-процесів [7]. Використання інтернет-інструментів прискорює пошук постачальників, клієнтів та працівників, що сприяє скороченню виробничих витрат і розширенню ринків збуту [28]. Особливо значущі результати спостерігаються у виробничих секторах та сферах із високою часткою рутинних операцій. Автоматизація таких процесів за допомогою інформаційно-комунікаційних технологій забезпечує зростання продуктивності праці [72].

Додатково, інтеграція інструментів аналітики великих даних дозволяє оптимізувати управління активами компанії, забезпечуючи гнучке використання ресурсів та зменшення їх простоїв. Згідно з дослідженнями, підприємства, які впровадили цифрові рішення, вже протягом першого року

демонструють позитивну динаміку: зокрема, обіг активів зростає на 3-9 % упродовж трьох років порівняно з компаніями, які не здійснюють цифрову трансформацію [23].

Окрім того, використання сучасних цифрових технологій дозволяє підвищити ефективність виробничих і управлінських процесів, забезпечити більш раціональне використання ресурсів та мінімізувати ймовірність помилок, спричинених людським фактором. У підсумку підприємства отримують можливість пришвидшити виробничі цикли, підвищити загальну продуктивність і скоротити операційні витрати, що є визначальними чинниками економічної стійкості в умовах високої конкуренції.

2. Підвищення конкурентоспроможності. Підприємства, які послідовно впроваджують цифрові технології в управлінську та виробничу діяльність, мають суттєві стратегічні переваги. Оптимізація бізнес-процесів, розширення каналів комунікації та вдосконалення ІТ-інфраструктури сприяють підвищенню адаптивності до ринкових змін та забезпечують основу для довгострокового зростання.

Дослідження підтверджують, що цифровізація дозволяє не лише підвищити ефективність внутрішніх операцій, а й зміцнити кооперацію між підприємствами, постачальниками та іншими учасниками бізнес-екосистеми [25]. Це, у свою чергу, підвищує здатність підприємства створювати додаткову цінність, зміцнювати ринкові позиції та підвищувати рівень економічної безпеки.

3. Швидка адаптація до змін у зовнішньому середовищі. Однією з ключових переваг цифрової трансформації є підвищення адаптивності підприємства до динамічних умов зовнішнього середовища. Використання автоматизованих систем, алгоритмів машинного навчання та інших інструментів штучного інтелекту дозволяє ефективно виконувати рутинні та регламентовані операції з високим рівнем точності й швидкості. Це, своєю чергою, звільняє людські ресурси для вирішення більш складних, творчих або

аналітичних завдань, що потребують стратегічного мислення та гнучкого підходу [192].

Завдяки цьому підприємства отримують змогу оперативно реагувати на ринкові зміни, адаптувати бізнес-моделі до нових умов, інтегрувати інновації у виробничо-управлінські процеси та швидко переглядати тактичні й стратегічні рішення. Таким чином, цифровізація сприяє формуванню стійких організаційних структур, здатних ефективно функціонувати в умовах невизначеності, високої конкуренції та технологічної турбулентності.

4. Покращення клієнтського досвіду. У цифрову епоху клієнтоорієнтованість стає одним із головних чинників конкурентоспроможності підприємства. Сучасні споживачі очікують індивідуального підходу, безперервного доступу до послуг та гнучкої взаємодії через зручні для них канали. Цифрова трансформація дозволяє підприємствам відповідати цим очікуванням шляхом впровадження інтелектуальних інструментів персоналізації обслуговування. Зокрема, використання технологій машинного навчання та штучного інтелекту забезпечує можливість глибокого аналізу клієнтських даних, виявлення поведінкових шаблонів та формування персоналізованих рекомендацій щодо товарів і послуг. Такі рішення підвищують релевантність комунікацій зі споживачами, що в свою чергу сприяє зростанню задоволеності, підвищенню лояльності та збільшенню тривалості взаємодії клієнтів з компанією [40].

5. Стимулювання інновацій у бізнес-моделях. Цифрова трансформація відкриває нові можливості для перегляду існуючих бізнес-моделей та впровадження інноваційних підходів до створення вартості. Зміна поведінки споживачів і нові ринкові вимоги спонукають компанії до інтеграції цифрових рішень у процеси розробки продуктів, сервісів і систем монетизації.

Як зазначають Г. Коломієць та інші [58], розвиток цифрових інструментів сприяє появі нових бізнес-моделей, таких як дропшипінг, SaaS сервіси, платформні екосистеми, які базуються на використанні аналітики даних і автоматизованих процесів для прийняття рішень у реальному часі.

Незважаючи на суттєві преференції, процеси цифрової трансформації супроводжуються низкою ризиків та деструктивних обмежень, здатних чинити вагомий вплив на рівень стабільності та результативності функціонування суб'єктів господарювання. Зазначені виклики мають комплексний характер і охоплюють як економічні, так і технологічні домінанти. Розглянемо ключові з них більш детально.

1. Високий рівень інвестиційних витрат. Запровадження цифрових технологій супроводжується суттєвими фінансовими витратами, особливо на початкових етапах. Підприємства змушені інвестувати у модернізацію IT-інфраструктури, перенавчання персоналу, зміну бізнес-процесів і впровадження нових систем управління. Згідно з даними дослідження International Data Corporation [50], середня вартість реалізації проєкту цифрової трансформації становить 27,5 млн дол. США, що свідчить про високу капіталомісткість подібних ініціатив.

Особливо вразливими в цьому контексті є малі та середні підприємства, які мають обмежений доступ до інвестиційних ресурсів. На ранніх етапах цифровізації гранична вигода може перевищувати витрати, однак надалі внаслідок ефекту дифузії маржинальна ефективність інвестицій знижується [103].

Також, варто зазначити, що в умовах цифрової трансформації для забезпечення належного рівня фінансової безпеки підприємствам необхідно здійснювати значні інвестиції у створення, впровадження та підтримку інформаційних систем, розробку спеціалізованого програмного забезпечення, а також у засоби кіберзахисту для запобігання несанкціонованим доступам і витокам конфіденційної інформації.

2. Складність оцінки результатів цифрової трансформації. Нерідко вартість впровадження цифрових технологій та заходів кіберзахисту значно перевищує початкові очікування підприємств. За даними [12], 70 % проєктів цифрової трансформації перевищили заплановані бюджети, а 7 % – обійшлися компаніям удвічі дорожче, ніж передбачалося. Більш того, згідно з

дослідженням McKinsey [88], лише 31 % очікуваного фінансового результату вдається реалізувати на практиці (рис. 1.5). Інше дослідження [39] також підтверджує, що лише третина проєктів цифровізації досягає або перевищує заплановані цілі.

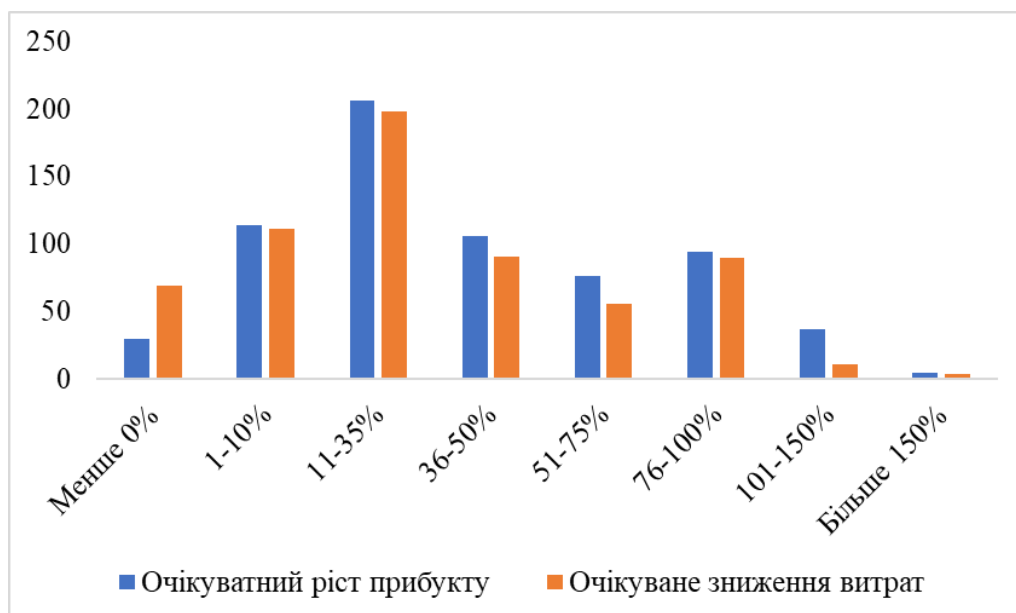


Рис. 1.5. Частка реалізованого фінансового прибутку та зниження витрат від цифрової трансформації.

Джерело: складено автором на основі [88].

У контексті цифрової трансформації менеджмент фінансових ризиків екстраполюється у фундаментальний інструментарій підтримання загального рівня економічної безпеки суб'єкта господарювання. Інтенсифікація капітальних видатків на цифровізацію та зростання рівня стохастичності щодо очікуваної результативності зумовлюють необхідність імплементації інтегрованих систем управління фінансовими ризиками, що базуються на принципах проактивності. Зазначений підхід передбачає застосування предиктивних моделей прогнозування, динамічне оцінювання рентабельності цифрових проєктів упродовж їхнього життєвого циклу, а також використання розширених механізмів диверсифікації ризиків, детермінованих впровадженням інноваційних технологій. Реалізація такої стратегії дозволяє

забезпечити фінансову резистентність підприємства та нівелювати ймовірність збитків від неефективних цифрових ініціатив.

3. Зростання кіберризиків. Паралельно з розвитком цифрових технологій та масштабним впровадженням цифрових рішень зростають і пов'язані з цим загрози, насамперед у сфері кібербезпеки. Сучасні цифрові інфраструктури, які об'єднують великі обсяги даних, автоматизовані системи управління, хмарні сервіси та інтернет речей, створюють численні вектори вразливості, що активно експлуатуються зловмисниками. Інтеграція складних технологічних рішень підвищує рівень технологічної залежності підприємств, що робить їх функціонування вразливим до технічних збоїв і цілеспрямованих атак.

Умовна стійкість бізнес-процесів значною мірою залежить від безперебійної роботи цифрової інфраструктури. Будь-які перебої в роботі хмарних сервісів, зараження виробничих систем шкідливим програмним забезпеченням чи злам мереж автоматизації можуть призвести до тимчасового або повного паралічу операційної діяльності, що тягне за собою суттєві фінансові втрати, порушення договірних зобов'язань і репутаційні ризики.

Згідно зі звітом Всесвітнього економічного форуму [95], кібератаки, витоки даних та інші прояви кіберзлочинності входять до переліку десяти найбільш небезпечних глобальних ризиків як у короткостроковій, так і в довгостроковій перспективі. Особливо вразливими до таких загроз є підприємства, що функціонують у критично важливих галузях, зокрема в енергетиці, сільському господарстві, фінансах, транспорті, водопостачанні та телекомунікаціях, де відмова систем може призвести до масштабних економічних та соціальних наслідків. За аналітичними оцінками, лише у 2023 році кількість зареєстрованих кіберінцидентів зросла на 72 % порівняно з 2021 роком [1]. Така динаміка свідчить про те, що процес цифровізації, поряд з очевидними перевагами, породжує і нові системні виклики, що потребують посилення заходів інформаційної безпеки.

4. Ризики витоку конфіденційної інформації. Цифрова трансформація передбачає активну обробку персональних і комерційно чутливих даних, що

створює додаткові ризики. Недостатній рівень кібергігієни, помилки персоналу, атаки соціальної інженерії та внутрішні загрози можуть призводити до серйозних витоків інформації. За даними IBM Security [26], середня глобальна вартість ліквідації наслідків витоку даних у 2024 році досягла 4,88 млн дол. США, що є рекордним показником за останні вісім років (рис. 1.6). Згідно з Thales Data Threat Report [93], 45 % опитаних компаній зазнали витоку даних, з яких 14 % – протягом останнього року.

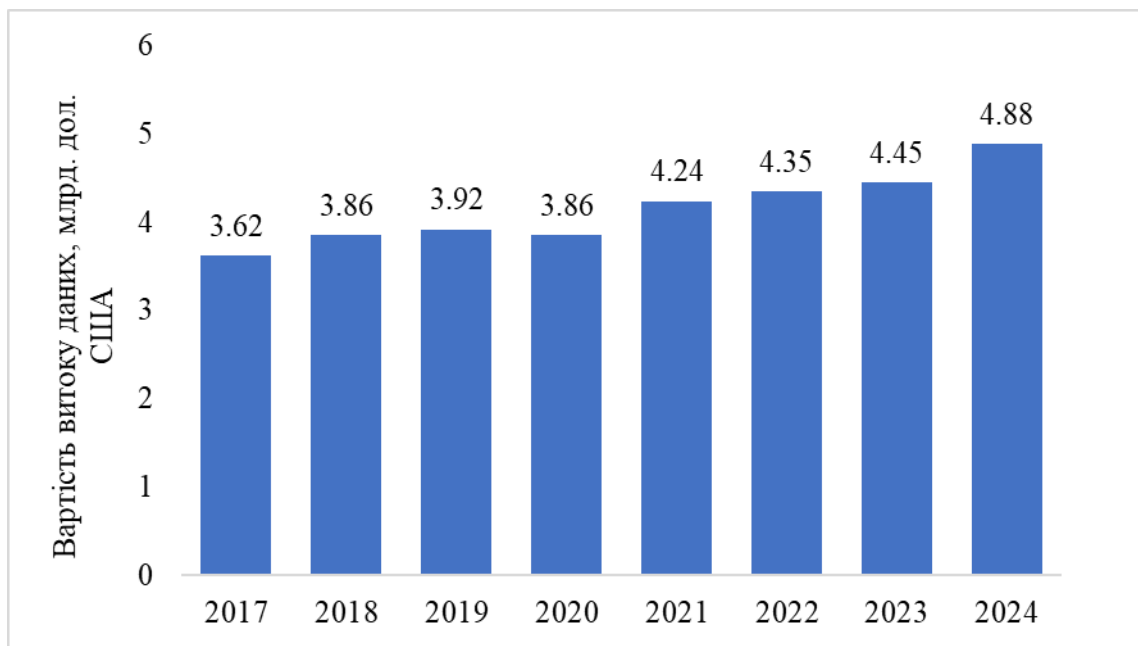


Рис. 1.6. Середня глобальна вартість витоку даних у 2017–2024 роках, млн дол. США.

Джерело: складено автором на основі [26].

Крім фінансових збитків, витoki даних негативно впливають і на ринкову капіталізацію компаній. Наприклад, після оприлюднення інформації про інцидент витоку даних у компанії Окта у 2022 році, її ринкова вартість зменшилася майже на 6 млрд дол. США протягом одного тижня [93].

Особливої актуальності набуває проблема внутрішніх кіберзагроз в умовах поширення дистанційного режиму роботи, використання мобільних пристроїв та гнучких форматів взаємодії з інформаційними системами. У таких умовах підвищується ризик несанкціонованого доступу до критично

важливих даних, що вимагає від підприємств реалізації комплексної політики цифрової безпеки. Це передбачає, зокрема, регламентування рівнів доступу, впровадження систем постійного моніторингу активності користувачів, а також автоматизованих процедур шифрування, резервного копіювання та реагування на інциденти безпеки.

У сукупності зазначені фактори підтверджують, що ефективне управління ризиками витоків даних має стати пріоритетним напрямом цифрової стратегії підприємства, інтегрованим у загальну систему економічної безпеки.

5. Нестача кваліфікованого персоналу. Цифрова трансформація підприємств вимагає не лише технологічної модернізації, але й формування потужного людського капіталу, здатного ефективно впроваджувати, підтримувати та масштабувати цифрові рішення. Водночас стрімкий розвиток цифрових технологій зумовлює динамічну еволюцію вимог до професійних компетенцій, що, у свою чергу, спричиняє суттєвий розрив між потребами бізнесу та наявними ресурсами на ринку праці.

У сучасних умовах цифровізація зумовлює зростання рівня складності та абстрактності завдань, які виконує персонал. Це вимагає від працівників постійного оновлення знань, гнучкості мислення та здатності до міждисциплінарної взаємодії. Однак на практиці все більш відчутним стає дефіцит висококваліфікованих спеціалістів, зокрема у сфері інформаційної безпеки, аналітики даних, управління цифровими проектами, ІТ-архітектури та бізнес-аналітики [74].

Цей кадровий розрив є однією з головних перешкод на шляху ефективної цифровізації підприємств, особливо в умовах високої конкуренції за технічні таланти на глобальному ринку праці. За результатами дослідження Всесвітнього економічного форуму у межах ініціативи «Робота майбутнього» [94], саме нестача кваліфікованого персоналу була визнана найбільш критичним бар'єром, який стримує впровадження новітніх цифрових технологій в майже 55% організацій (рис. 1.7).



Рис. 1.7. Основні бар'єри впровадження цифрових технологій за оцінкою бізнесу.

Джерело: складено автором на основі [94].

Невідповідність між потребами цифрової економіки та наявним кадровим потенціалом потребує системних рішень на рівні державної політики, системи освіти та корпоративного управління знаннями.

Таким чином, цифрова трансформація справляє комплексний вплив на діяльність підприємств, відкриваючи широкі можливості для підвищення ефективності, інноваційності та конкурентоспроможності. Водночас вона супроводжується низкою викликів, зокрема фінансових, організаційних та інформаційно-безпекових [115]. Для узагальнення результатів проведеного аналізу доцільно систематизувати основні переваги та недоліки цифрової трансформації підприємства, що наведено у табл. 1.5.

Аналіз виявлених загроз дозволяє стверджувати, що в умовах цифрової трансформації традиційний контур економічної безпеки доповнюється специфічною складовою – цифровою безпекою. Під цифровою безпекою підприємства автором запропоновано розуміти стан захищеності інтересів

суб'єкта господарювання у цифровому просторі, що забезпечується здатністю системи управління своєчасно ідентифікувати, нейтралізувати та прогнозувати деструктивні впливи на інформаційні активи, цифрові інфраструктури та бізнес-процеси з метою збереження конкурентних переваг і забезпечення безперервності діяльності.

Таблиця 1.5

Основні переваги та недоліки цифрової трансформації підприємства

| <b>Переваги цифрової трансформації</b>                                                                    | <b>Недоліки цифрової трансформації</b>                                                  |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Підвищення операційної ефективності за рахунок автоматизації та аналітики даних                           | Високі інвестиційні витрати на впровадження технологій та інфраструктурні зміни         |
| Зміцнення конкурентоспроможності завдяки оптимізації бізнес-процесів і новим каналам взаємодії            | Складність оцінки результатів і невідповідність очікуваних та фактичних вигод           |
| Швидка адаптація до змін зовнішнього середовища та ринкових умов                                          | Зростання кіберризиків і уразливість до атак на критичну цифрову інфраструктуру         |
| Покращення клієнтського досвіду через персоналізацію, багатоканальність та обробку даних у реальному часі | Ризики витоку конфіденційної інформації, що спричиняють фінансові та репутаційні втрати |
| Стимулювання інновацій у бізнес-моделях (платформи, підписки, дропшипінг тощо)                            | Нестача кваліфікованого персоналу для реалізації та підтримки цифрових ініціатив        |

Джерело: складено автором

На відміну від суто технічного розуміння кібербезпеки, цифрова безпека в економічному контексті акцентує увагу на мінімізації фінансових втрат та збереженні стратегічної стійкості підприємства в умовах стохастичності цифрового середовища [144].

Узагальнюючи результати проведеного аналізу, можна зробити висновок, що цифрова трансформація підприємств є складним, багатовимірним та багатоетапним процесом, який охоплює не лише впровадження інформаційно-комунікаційних технологій, але й глибоку трансформацію бізнес-процесів, управлінських моделей, способів взаємодії з клієнтами та загальної архітектури функціонування підприємства.

Цифровізація виступає ключовим фактором модернізації економіки та однією із головних причин підвищення конкурентоспроможності підприємств, забезпечуючи зростання продуктивності, оперативності управлінських

рішень, адаптивності до ринкових змін та клієнтоорієнтованості. Водночас масове впровадження цифрових рішень супроводжується виникненням нових викликів і ризиків, зокрема зростанням інвестиційного навантаження, посиленням кіберзагроз, ризиків витоку конфіденційної інформації, а також нестачею кваліфікованого персоналу.

Зазначене зумовлює необхідність ревізії традиційних парадигм формування системи економічної безпеки суб'єкта господарювання. Сучасна архітектура економічної безпеки має характеризуватися динамічністю, адаптивністю та здатністю до превентивного нівелювання загроз, генерованих цифровим середовищем. Пріоритетними векторами розвитку системи постають менеджмент цифрових ризиків, інтеграція кібернетичної безпеки в контур стратегічного планування, нарощення цифрових компетенцій людського капіталу, а також розроблення аналітичного інструментарію для прогнозування результативності інвестицій у цифрові активи.

З огляду на викладене, актуальною науково-практичною задачею є формування нової концептуальної моделі системи економічної безпеки підприємства, яка враховуватиме специфіку функціонування в умовах цифрової економіки, а також характер і масштаб новітніх ризиків, породжених цифровізацією. Саме така модель повинна стати основою для забезпечення сталого розвитку підприємств в умовах цифрових трансформацій.

### **1.3. Концептуальні засади формування інтегрованої системи економічної безпеки підприємства в умовах цифрової трансформації**

У науковій літературі представлено численні підходи до визначення поняття системи економічної безпеки підприємства, які були детально проаналізовані в попередніх розділах. Проте, стрімкий розвиток цифрових технологій, що супроводжує сучасні трансформаційні процеси в економіці, зумовлює необхідність переосмислення традиційних підходів до побудови

такої системи. У контексті переходу до концепції «Індустрія 4.0» економічна безпека підприємства зазнає істотної трансформації, що вимагає розгляду нових ризиків, можливостей і форм взаємодії між технологічними та організаційними складовими підприємства.

Цифровізація господарських процесів, зокрема запровадження інноваційних інформаційно-комп'ютерних технологій, кардинально змінює підходи до управління підприємствами. Ці зміни охоплюють не лише виробничу, логістичну чи управлінську сфери, а й безпосередньо впливають на формування та функціонування систем економічної безпеки. З одного боку, цифрова трансформація сприяє підвищенню прозорості, ефективності управлінських рішень і оптимізації витрат, але з іншого вона породжує низку нових загроз, пов'язаних із кібербезпекою, витоком конфіденційної інформації, залежністю від зовнішніх ІТ-постачальників, а також посиленням регуляторних вимог.

У цьому контексті заслуговує на увагу дослідження Ю. Самойленка та співавторів [84], у якому обґрунтовано доцільність заміни застарілого терміну «інформаційна безпека» на більш сучасне поняття «цифрова безпека підприємства». Такий підхід дозволяє охопити ширший спектр загроз, притаманних цифровому середовищу. Автори здійснили аналіз різних країн, що продемонстрував залежність рівня цифрової безпеки від специфіки інституційного середовища та розміру підприємств у межах країн Європейського Союзу, чим суттєво розширено традиційне трактування поняття економічної безпеки підприємства.

Крім того, важливий внесок у формування новітніх підходів до концепції економічної безпеки зроблено у праці [145], де представлено системну класифікацію цифрових ризиків, притаманних промисловим підприємствам. Зокрема, в роботі підкреслено важливість багаторівневого аналізу ризиків з урахуванням їх впливу на ключові підсистеми підприємства таких як фінансову, кадрову, техніко-технологічну тощо. Такий підхід сприяє побудові

більш адаптивних і гнучких моделей управління економічною безпекою в умовах цифрової економіки.

Проблематика адаптації системи економічної безпеки підприємства до умов цифрової трансформації знайшла ґрунтовне відображення у роботі К. Полупанова, О. Хаджунова та З. Сіманавіцієне [78]. У дослідженні здійснено узагальнення базових принципів адаптації системи безпеки та представлено структурну модель, що враховує трансформаційні впливи цифровізації на внутрішні бізнес-процеси. Зазначена модель є важливим етапом на шляху до формалізації цифрових аспектів у структурі економічної безпеки, проте, водночас, вона має певні обмеження. Зокрема, у ній відсутні інструменти кількісної оцінки рівня безпеки, що ускладнює практичне застосування представленої концепції в реальному управлінні.

Доповненням до зазначених підходів є наукова позиція Сімкової Т. та Копчі Ю. [188], які розглядають адаптивне управління та цифрову трансформацію як ключові стратегічні імперативи, що забезпечують стійкість бізнес-моделі підприємства в умовах високої невизначеності та інноваційно-орієнтованого розвитку. Такий підхід дозволяє змістити акцент з пасивного захисту на активне формування стратегічної стійкості через впровадження інноваційних моделей управління

Інший важливий аспект цифрової трансформації розкрито у дослідженні А. Гарагуліа, В. Суслова та О. Горової [44], в якому акцентовано увагу на сучасних інструментах стратегічного управління економічною безпекою в умовах глобальної нестабільності, зокрема війни в Україні. Автори детально проаналізували можливості інтеграції таких інструментів як страхування ризиків, прогнозування загроз та аналітичне моделювання у загальну систему безпекового менеджменту підприємства. Ці практики набувають особливої актуальності в умовах зростання невизначеності та швидких змін бізнес-середовища.

Таким чином, сучасна наукова думка демонструє поступовий перехід від ізольованого розгляду окремих компонентів системи безпеки до побудови

комплексних моделей, які охоплюють усі ключові підсистеми підприємства, зокрема фінансову, кадрову, техніко-технологічну та інформаційну, з урахуванням викликів цифрової економіки. Такий інтегрований підхід сприяє формуванню цілісного уявлення про природу ризиків і механізми їх нейтралізації.

На основі узагальнення наукових джерел та практичних кейсів цифрової трансформації, можна виокремити низку проблем і ризиків, що супроводжують діяльність підприємств у цифровому середовищі. Ці ризики мають багатогранний і міждисциплінарний характер, охоплюючи як технічні, так і організаційно-управлінські аспекти функціонування підприємств. Зокрема, найбільш характерними ризиками цифрової епохи є кіберризики, ризики витоку конфіденційної інформації, інсайдерські ризики, ризики технологічного старіння, цифрове шахрайство, тощо. Детальний список нових ризиків в епоху цифровізації, приклади цих ризиків та вплив на підсистеми економічної безпеки представлені в табл. 1.6. Усі перелічені фактори створюють суттєві загрози для стійкості системи економічної безпеки та вимагають перегляду традиційних підходів до її формування і підтримання.

Як засвідчує аналіз сучасних досліджень представлених (п. 1.2), цифровізація господарської діяльності зумовлює появу нових типів ризиків, що суттєво відрізняються від традиційних загроз економічній безпеці. Усе більше науковців виокремлюють поняття цифрової безпеки підприємства як самостійну складову загальної системи економічної безпеки. Такий підхід обумовлений потребою захисту підприємств від негативних наслідків, що виникають у разі реалізації цифрових загроз, зокрема втрат інформації, фінансових збитків, порушення конфіденційності та зниження репутаційної вартості. Переважна більшість загроз для економічної стабільності підприємств на сучасному етапі мають саме цифрову природу або реалізуються через цифрові канали. Отже, в умовах динамічної цифровізації економіки формування ефективної системи цифрової безпеки є не лише

актуальним, а й критично необхідним завданням для забезпечення стійкості підприємства.

Таблиця 1.6

Типологія цифрових ризиків у системі економічної безпеки

| Назва ризику                      | Приклади ризику                                         | Вплив на підсистему економічної безпеки | Ступінь критичності |
|-----------------------------------|---------------------------------------------------------|-----------------------------------------|---------------------|
| Кіберризик                        | Злам інформаційних систем, атаки програм-вимагачів      | Інформаційна, фінансова                 | Високий             |
| Ризик конфіденційності            | Витік комерційних або персональних даних                | Фінансова, інформаційна                 | Високий             |
| Інсайдерський ризик               | Несанкціоновані дії співробітників                      | Кадрова, інформаційна                   | Середній            |
| Технічний збій                    | Відмова ІТ-інфраструктури, обриви зв'язку, втрати даних | Техніко-технологічна, фінансова         | Середній            |
| Шахрайство в цифровому середовищі | Використання ботів для фальсифікації транзакцій         | Фінансова                               | Високий             |
| Ризик некомпетентності            | Недостатній рівень цифрових навичок персоналу           | Кадрова, інформаційна                   | Середній            |
| Ризик технологічного старіння     | Використання застарілого програмно забезпечення         | Техніко-технологічна                    | Середній            |
| Стрес та вигорання                | Емоційне вигорання, зниження мотивації                  | Кадрова                                 | Середній            |

Джерело: складено автором

Розроблення такої системи потребує комплексного врахування низки об'єктивних факторів. Зокрема, до основних елементів, які мають бути обов'язково проаналізовані при проектуванні системи цифрової безпеки, належать:

- загрози цифрової безпеки, їхня природа, інтенсивність, ймовірність виникнення та реалізації;
- вразливості цифрової інфраструктури, включаючи інформаційні системи, які можуть бути використані для несанкціонованого доступу, знищення або модифікації даних;
- ризики та потенційні збитки, що виникають у разі реалізації цифрової загрози, зокрема як прямі втрати (наприклад, фінансові), так і непрямі наслідки (репутаційні втрати, зниження конкурентоспроможності, втрата клієнтів).

У цьому контексті ключовим етапом стало створення концептуальної моделі цифрової безпеки підприємства [144], яка виступає методологічною основою для подальшої розробки комплексної моделі системи економічної безпеки. Така модель є універсальною і може бути застосована на підприємствах незалежно від галузі чи масштабу діяльності. Вона дозволяє формалізувати підхід до управління цифровими загрозами та забезпечити системну взаємодію між технічними, організаційними та управлінськими елементами. Представлена модель на рис. 1.8 є логічним підґрунтям для побудови інструментів практичного забезпечення цифрової безпеки та формування стратегії протидії цифровим загрозам в умовах цифрової економіки.

Ця модель дозволяє візуалізувати основні взаємозв'язки між джерелами загроз, чинниками вразливості, інформаційними ресурсами, а також потенційними наслідками реалізації цифрових ризиків. Згідно з моделлю, вихідною точкою є джерела загроз, які класифіковано на три основні групи:

- людський фактор (наприклад внутрішні зловмисники, персонал, конкуренти),
- збої обладнання (помилки користувачів, відмова апаратного або програмного забезпечення),
- природні чинники (стихійні лиха, біологічні загрози тощо).

Ці джерела породжують загрози, що у свою чергу можуть активізувати вразливості інформаційних систем підприємства. Вразливість зумовлюється наявністю технічних недоліків, людських помилок або процедурної неузгодженості в роботі ІТ-інфраструктури. У моделі підкреслюється, що чим вищий рівень вразливості, тим більша ймовірність реалізації ризику. В свою чергу, інформаційні ресурси (дані, документація, апаратне та програмне забезпечення) є об'єктами, які піддаються впливу загроз і вразливостей, але в той же час мають відповідну цінність для підприємства.

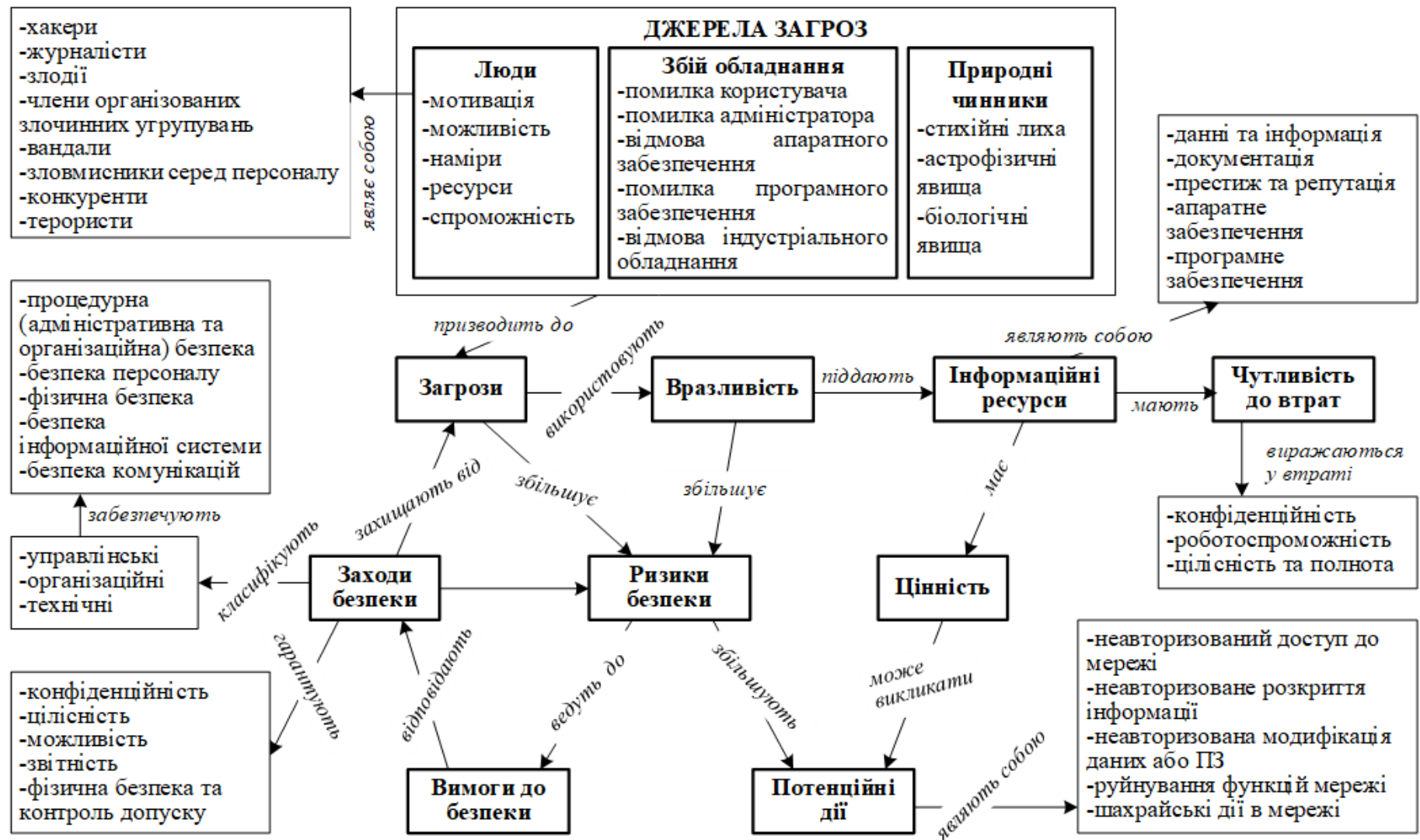


Рис. 1.8. Модель цифрової безпеки підприємства.

Джерело: розроблено автором [144].

Відтак, оцінка чутливості до втрат дозволяє визначити рівень потенційної шкоди в разі несанкціонованих дій. Чутливість до втрат виражається у трьох основних показниках:

- конфіденційність – здатність запобігати несанкціонованому доступу до інформації;
- працездатність – забезпечення безперебійної роботи систем;
- цілісність і повнота даних – запобігання їх модифікації або знищенню.

Порушення цих показників призводить до потенційних дій, що виражаються у формі несанкціонованого доступу, модифікації чи знищення інформації, порушення функцій мережі або цифрового шахрайства. Відповіддю на наявність загроз і вразливостей є заходи безпеки, що поділяються на:

- управлінські (політики, регламенти, аудит),
- організаційні (контроль доступу, розмежування повноважень),
- технічні (захисне програмне забезпечення, шифрування, резервування даних).

Зазначений комплекс заходів детермінує вимоги до безпекового контуру, імплементація яких є необхідною для досягнення цільових параметрів захищеності, насамперед забезпечення конфіденційності, цілісності та інваріантності доступу до інформаційних ресурсів. Узагальнюючи, дана модель цифрової безпеки постає фундаментальним базисом для проектування інтегрованої системи економічної безпеки, проведення багатокритеріальної оцінки релевантних ризиків та розроблення стратегічних сценаріїв реагування в умовах глобальної цифровізації економічних процесів.

У цілому, ця концептуальна модель демонструє системний підхід до цифрової безпеки, в якому ризики розглядаються як результат взаємодії між загрозами, вразливостями та ціннісними характеристиками інформаційних ресурсів. Такий підхід дозволяє не лише ідентифікувати ключові зони ризику, а й структурувати заходи протидії відповідно до ієрархії факторів ризику.

Водночас, цифрова безпека є лише однією з ключових, але не єдиною складовою загальної системи економічної безпеки підприємства в умовах цифрової трансформації. Система економічної безпеки за своєю суттю є складною, багаторівневою структурою, що включає взаємопов'язані підсистеми, кожна з яких відіграє визначальну роль у забезпеченні сталості й життєздатності підприємства. Для ефективного управління економічною безпекою надзвичайно важливо розуміти логіку взаємозв'язків між цими підсистемами та аналізувати, яким чином цифровізація впливає на кожну з них.

Застосування системного підходу до формування економічної безпеки в умовах цифрової трансформації дозволяє розглядати підприємство як цілісний об'єкт, у якому всі елементи безпеки – фінансова, техніко-технологічна, кадрова, інформаційна та інші – функціонують у єдиному управлінському полі з метою досягнення спільної стратегічної цілі: забезпечення стійкого, безпечного й адаптивного розвитку підприємства в цифровій економіці. У контексті цифрової трансформації системний підхід набуває особливої актуальності, оскільки дає змогу:

- забезпечити всебічне охоплення ризиків, які охоплюють фінансову, виробничу, інноваційну, екологічну, кадрову та інформаційну сфери;
- ідентифікувати нові види загроз, що виникають внаслідок цифровізації бізнес-процесів, зокрема: витоки даних, атаки програм-вимагачів, порушення ланцюгів постачання, інциденти у сфері конфіденційності [153];
- налагодити міжпідсистемну взаємодію на основі єдиних стандартів управління ризиками, що дозволяє уникнути каскадного ефекту;
- підвищити адаптивність і гнучкість системи економічної безпеки, забезпечуючи її здатність до швидкого реагування на зміни у зовнішньому середовищі;
- інтегрувати інноваційні цифрові технології в управління безпековими процесами, включаючи штучний інтелект, машинне навчання, блокчейн, великі дані для побудови систем моніторингу, виявлення та прогнозування

загроз. За даними дослідження McKinsey Global Institute, підприємства, які впровадили AI-рішення в системи управління ризиками, підвищили швидкість виявлення інцидентів на 30–50 % [96];

– сформувати корпоративну культуру безпеки, яка ґрунтується на усвідомленні ролі кожного працівника у захисті підприємства від ризиків і загроз.

Отже, системний підхід до управління економічною безпекою підприємства дає змогу не лише структурувати захисні заходи, але й вибудовувати інтегровану й динамічну модель, що здатна адаптуватись до викликів цифрової епохи. Така модель передбачає постійний моніторинг середовища, аналіз нових загроз, корекцію внутрішніх процесів та оперативну реакцію на інциденти.

Зважаючи на викладене, системна побудова економічної безпеки підприємства в умовах цифрової трансформації має спиратися не лише на узагальнені принципи, а й на глибокий аналіз впливу цифровізації на окремі підсистеми. Адже кожна підсистема економічної безпеки по-різному реагує на цифрові виклики, має власні вразливості та потребує специфічних інструментів управління ризиками. Такий аналітичний підхід дозволяє адаптувати систему безпеки не лише до загальних змін у цифровому середовищі, а й до структурних особливостей підприємства, його галузевої специфіки, масштабів діяльності та цифрової зрілості.

У науковій літературі спостерігається певна варіативність у підходах до структурування економічної безпеки. Так, Мацеха Д.С. [159] пропонує деталізовану систему показників, що охоплює фінансовий, управлінський, інформаційний, кадровий, соціальний, техніко-технологічний, інноваційний, політико-правовий, екологічний, антикризовий, ринково-інтерфейсний та силовий складники. Автор також акцентує увагу на вимогах до побудови системи показників та їх взаємозв'язку в межах загальної діагностичної моделі, простоти, доступності та здатності охоплювати ключові загрози для функціонування підприємства.

Інший підхід демонструє Вахлакова В. В. [122], яка зосереджує основну увагу на фінансовій та ринковій складових, трактуючи їх як синтетичні компоненти, що акумулюють ризики з інших сфер. Відповідно до її підходу, оцінювання економічної безпеки підприємства здійснюється в два етапи: спочатку окремо за кожною з двох ключових складових, а далі через їх інтегровану оцінку у вигляді сценаріїв економічної безпеки.

Попри різноманіття підходів, більшість сучасних досліджень і практичних моделей вказують на критичне значення окремих підсистем. На нашу думку, саме фінансова, кадрова та техніко-технологічна складові зазнають найпотужнішого впливу цифрових трансформацій. Це пояснюється як їхнім ключовим значенням у забезпеченні стабільного функціонування підприємства, так і високим ступенем чутливості до цифрових ризиків, таких як автоматизація фінансових операцій, трансформація трудових процесів або технологічна модернізація виробництва. У подальшому буде показано, що саме ці три підсистеми є найбільш вразливими до цифрових загроз і вимагають особливої уваги в межах цифрової безпеки підприємства.

1. У цифрову епоху фінансова підсистема підприємства зазнає істотної трансформації під впливом впровадження інформаційно-комунікаційних технологій. Цифровізація відкриває нові можливості для зростання доходів, оптимізації витрат і підвищення ефективності фінансового управління, але водночас супроводжується появою нових ризиків, які ускладнюють забезпечення фінансової безпеки.

Серед позитивних аспектів цифрового впливу на фінансову систему підприємства можна виділити:

- створення нових каналів продажів через електронну комерцію, що сприяє розширенню ринків збуту, підвищенню обороту та зменшенню транзакційних витрат;
- використання цифрового маркетингу, що забезпечує персоналізацію пропозицій і таргетовану взаємодію з цільовими аудиторіями, підвищуючи коефіцієнт конверсії та рентабельність інвестицій у комунікації;

– монетизацію цифрових активів і послуг (зокрема програмних продуктів, онлайн-сервісів, цифрових платформ), яка створює нові джерела доходу та підвищує фінансову гнучкість підприємства.

Проте негативні ефекти цифровізації також мають суттєвий вплив у контексті фінансової безпеки:

– залежність від цифрових сервісів (зокрема платіжних платформ, хмарних бухгалтерських систем або аналітичних сервісів) робить фінансову систему вразливою до технічних збоїв, перебоїв у роботі постачальників сервісів або змін їхньої політики;

– зростання шахрайства у цифрових каналах продажів, включаючи фішингові атаки, підміну платіжних реквізитів і маніпуляції з електронними транзакціями, що призводить до прямих фінансових втрат і погіршення репутації компанії.

Таким чином, формування сучасної фінансової безпеки передбачає збереження фінансової стійкості підприємства в умовах цифрової економіки, а також своєчасне реагування на зміни у середовищі за допомогою аналітичних інструментів. У цьому контексті оцінювання фінансової підсистеми економічної безпеки дедалі частіше здійснюється із використанням моделювання та прогнозування, орієнтованих на виявлення кризових станів та розробку систем фінансового раннього попередження.

Слід зауважити, що в умовах цифрової трансформації фінансова безпека вже не може розглядатися у відриві від технологічних, поведінкових і мережевих змін. Саме тому результати оцінювання фінансової підсистеми базуються не лише на класичних фінансових індикаторах, а й на цифрових показниках – індексах цифрової зрілості, рівнях залежності від ІТ-рішень, швидкості обробки інформації тощо. Інтеграція цифрових чинників у моделі прогнозування банкрутства, платоспроможності та фінансової стабільності є необхідною умовою ефективного управління ризиками. Таке поєднання дозволяє забезпечити актуальність фінансової аналітики, адаптивність до

цифрових змін і підвищити загальну резистентність підприємства до кризових явищ.

2. У структурі економічної безпеки підприємства кадрова підсистема відіграє стратегічну роль, оскільки персонал є не лише основним джерелом продуктивності, але й потенційним носієм ризиків. В умовах цифрової трансформації ця підсистема зазнає глибоких змін, зумовлених впровадженням цифрових технологій у процеси управління людськими ресурсами, зміною форм зайнятості, вимог до кваліфікації працівників і зміщенням акцентів у системі мотивації та контролю. Цифровізація, з одного боку, відкриває нові можливості для підвищення ефективності використання трудових ресурсів, а з іншого створює нові загрози для кадрової стабільності, що безпосередньо впливають на рівень економічної безпеки підприємства.

Серед позитивних ефектів цифрової трансформації на кадрову підсистему можна виокремити:

- підвищення продуктивності праці за рахунок автоматизації рутинних операцій і перенаправлення зусиль працівників на більш складні, креативні або аналітичні завдання;
- гнучкість у форматах зайнятості – дистанційна, гібридна або проектна робота, що сприяє підвищенню задоволеності працівників, оптимізації витрат на фізичну інфраструктуру та розширенню географії пошуку талантів;
- цифрова аналітика в HR-сфері, що дозволяє формувати персоналізовані траєкторії розвитку працівників, прогнозувати ризики плинності кадрів і планувати стратегічне управління талантами.

Однак негативні прояви цифровізації у кадровій сфері також мають системний характер:

- ризик витоку конфіденційної інформації з боку працівників, що мають доступ до критичних даних або комерційної таємниці (інсайдерська загроза);
- уразливість цифрових HR-систем до кібератак або помилок адміністрування, що загрожує порушенням конфіденційності персональних даних;

– дефіцит кваліфікованих кадрів у сфері ІТ, кібербезпеки, цифрової аналітики, що ускладнює адаптацію підприємства до нових технологічних реалій і посилює конкуренцію на ринку праці.

У зв'язку з цим, забезпечення кадрової безпеки в умовах цифрової трансформації потребує комплексного підходу, що включає:

- внутрішній контроль та поведінковий моніторинг;
- розвиток цифрових компетентностей персоналу;
- формування культури інформаційної гігієни;

Важливим напрямом сучасного підходу до оцінювання кадрової безпеки є використання інтелектуальних моделей аналізу поведінкових шаблонів, які дозволяють виявляти потенційно ризиковану активність працівників у цифровому середовищі. У цьому контексті аналітика аномалій стає основою для побудови інтегрального показника безпеки, який охоплює як технічні аспекти (доступ, логування, захист систем), так і поведінкові характеристики персоналу (частота та тип дій, відхилення від нормальної поведінки).

Таким чином, оцінювання рівня безпеки кадрової підсистеми підприємства в умовах цифрової трансформації має здійснюватися з урахуванням як нових типів загроз, так і розширених можливостей, які формуються в цифровому середовищі. До таких загроз належать, зокрема, інсайдерські атаки, витоки даних, маніпуляції з інформацією та зниження лояльності персоналу внаслідок цифрового перевантаження. Зважаючи на це, особливої актуальності набуває використання інтелектуальних моделей, здатних здійснювати глибокий аналіз поведінкових шаблонів працівників у корпоративному інформаційному середовищі. Такі моделі, що базуються на методах машинного навчання, дозволяють ідентифікувати нетипові дії, що потенційно свідчать про зміни у поведінці персоналу, які можуть становити загрозу для економічної безпеки підприємства. Такий підхід дає змогу сформувати інтегральний показник кадрової безпеки, який включає як технічні аспекти захисту інформації (доступ до систем, автентифікація, контроль активності), так і поведінкові характеристики персоналу (аналітика цифрової

активності, зміна комунікаційних шаблонів, рівень залученості). У результаті підприємство отримує інструмент для більш точного управління кадровими ризиками в умовах цифрової економіки.

3. Цифрова трансформація значною мірою змінює техніко-технологічну основу функціонування підприємств, сприяючи переходу до інтелектуалізованих виробничих систем, автоматизованих процесів управління, впровадження штучного інтелекту в технологічні ланцюги та підвищеної гнучкості операційної діяльності. У сучасних умовах саме техніко-технологічна підсистема виступає критично важливою для забезпечення операційної стійкості, ефективності та здатності підприємства адаптуватися до високодинамічного ринкового середовища.

Серед ключових позитивних ефектів цифровізації цієї підсистеми можна виділити:

- створення адаптивних виробничих систем, які завдяки застосуванню інтелектуальних цифрових технологій здатні оперативно перебудовувати процеси залежно від змін попиту, постачання або ресурсних обмежень;

- оптимізація використання ресурсів, що забезпечується автоматизованим моніторингом, використанням прогностичної аналітики, IoT-платформ і машинного навчання, що дозволяє знижувати виробничі витрати, підвищувати ефективність і екологічну сталість виробництва;

- інтеграція цифрового дублювання та симуляційних моделей, які дають змогу заздалегідь тестувати технологічні зміни та прогнозувати можливі відмови систем без необхідності реального втручання в операційний процес.

- Однак цифровізація технологічної бази підприємства породжує і нові ризики, які суттєво ускладнюють забезпечення техніко-технологічної безпеки:

- вразливість до кібератак на промислові системи управління, яка зростає у зв'язку з підключенням виробничих елементів до загальної цифрової мережі;

- ризик тимчасової зупинки виробництва внаслідок помилок програмного забезпечення, відмови цифрових компонентів або втрати зв'язку між елементами інфраструктури;

- прискорене моральне старіння технологій, яке вимагає регулярної модернізації, що, у свою чергу, передбачає зростання інвестиційного навантаження та підвищення залежності від зовнішніх постачальників технологій.

Таким чином, цифрова трансформація техніко-технологічної підсистеми є двостороннім процесом: вона водночас підвищує ефективність і адаптивність, але створює нові технічні, кіберфізичні та інвестиційні ризики. У такому контексті оцінка стану техніко-технологічної безпеки підприємства набуває особливого значення, оскільки саме ця підсистема забезпечує безперервність виробництва, технологічну резистентність і інноваційну спроможність підприємства.

Водночас, слід враховувати, що підприємства значно відрізняються між собою за рівнем автоматизації, структурою основних фондів, ступенем впровадження цифрових рішень і рівнем ІТ-захисту. Створення універсальної кількісної моделі оцінювання техніко-технологічної підсистеми є ускладненим через велику кількість якісних чинників, обмеженість уніфікованих метрик і високу невизначеність цифрового середовища. У зв'язку з цим, доцільним є застосування нечітких методів оцінювання, здатних враховувати багатofакторність, експертні судження, а також якісні характеристики технічного стану. На практиці це забезпечується побудовою інтегрального показника техніко-технологічної безпеки, що виступає агрегованою характеристикою поточного стану підсистеми. Такий показник дозволяє:

- здійснювати моніторинг технічної стійкості;
- приймати інвестиційні рішення щодо модернізації;
- планувати підвищення рівня кіберстійкості та автоматизації в умовах швидкоплинних змін цифрового середовища.

З метою узагальнення аналітичних висновків щодо трансформації ключових підсистем економічної безпеки в умовах цифрової економіки доцільно представити порівняльну характеристику позитивного та негативного впливу цифровізації. Такий підхід дозволяє більш системно оцінити як потенціал, так і ризики, притаманні кожній підсистемі, та обґрунтувати напрями подальшого вдосконалення системи управління безпекою. Порівняльну характеристику впливу цифрових змін на фінансову, кадрову та техніко-технологічну підсистеми наведено в табл. 1.7.

Таблиця 1.7

Порівняльна характеристика впливу цифрової трансформації на підсистеми економічної безпеки підприємства

| Підсистема           | Позитивний вплив                                                                                                                                                       | Негативний вплив                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Фінансова            | Нові канали продажів (e-commerce), що зменшують транзакційні витрати;<br>Персоналізація за допомогою цифрового маркетингу;<br>Монетизація цифрових активів і сервісів. | Залежність від сторонніх цифрових сервісів (хмарні бухгалтерії, платіжні системи);<br>Шахрайство у цифрових каналах, фішинг, атаки на платіжні інструменти.                           |
| Кадрова              | Автоматизація рутинних задач і зростання продуктивності;<br>Гнучкі формати зайнятості (дистанційна/гібридна робота);<br>Цифрова HR-аналітика/                          | Інсайдерські ризики та витік конфіденційної інформації;<br>Уразливість цифрових кадрових систем до атак;<br>Дефіцит фахівців із цифровими навичками.                                  |
| Техніко-технологічна | Гнучкі виробничі системи, адаптація до змін ринку;<br>Оптимізація ресурсів завдяки IoT, аналітиці та автоматизації;<br>Можливість цифрового дублювання та симуляції.   | Уразливість промислових IT-систем до кібератак;<br>Збої у виробництві через технічні відмови цифрових елементів;<br>Моральне старіння технологій та високе інвестиційне навантаження. |

Джерело: складено автором

На підставі здійсненого оцінювання фінансової, кадрової та техніко-технологічної підсистем економічної безпеки доцільним є формування єдиної

інтегральної оцінки, яка слугуватиме кількісним індикатором загального рівня економічної безпеки підприємства. Такий підхід забезпечує:

- узагальнення впливу окремих факторів ризику в межах системи;
- уніфіковану основу для прийняття стратегічних і тактичних управлінських рішень;
- можливість динамічного моніторингу безпеки в умовах цифрової трансформації.

Таким чином, економічна безпека підприємства формується як багатфакторна, взаємозалежна система, у якій ефективне функціонування кожної підсистеми залежить від стабільності інших. У цифрову епоху особливої важливості набуває інтеграція цифрової безпеки в усі рівні управління безпекою, що дозволяє не лише локалізувати окремі загрози, а й забезпечити цілісну захисну архітектуру підприємства. Порушення взаємозв'язків між підсистемами може мати мультиплікативний ефект, коли окремий інцидент призводить до каскадного поширення ризиків на суміжні сфери. Цифрова безпека, як наскрізний компонент, відіграє роль зв'язуючого елемента між підсистемами, оскільки більшість сучасних загроз реалізуються через цифрове середовище. Її ефективне функціонування є необхідною умовою збереження цілісності всієї системи економічної безпеки.

Найбільш значущі вектори взаємного впливу підсистем в умовах цифрової трансформації можна охарактеризувати так:

Вплив цифрової безпеки на фінансову підсистему. Порушення цифрової безпеки, зокрема кібератаки на фінансові системи, маніпуляції з електронними транзакціями або витоки конфіденційної фінансової інформації, призводять до прямих фінансових збитків, втрати ліквідності, штрафних санкцій та пошкодження репутації. Усе це негативно позначається на інвестиційній привабливості підприємства та його стійкості в конкурентному середовищі.

Вплив цифрової безпеки на техніко-технологічну підсистему. У виробничих системах, що інтегрують ІТ-рішення, IoT і кіберфізичні платформи, компрометація цифрової безпеки може спричинити збої в

операційних процесах, пошкодження обладнання, перерви в ланцюгах постачання, зниження якості продукції та зупинку виробництва. Відтак, технологічна стабільність підприємства стає прямо залежною від рівня цифрової захищеності.

Вплив кадрової підсистеми на цифрову безпеку. Людський фактор залишається одним із ключових джерел ризику в цифровому середовищі. Низький рівень цифрової грамотності, відсутність навичок кібергігієни, нехтування правилами безпечної роботи з конфіденційною інформацією або навмисні дії працівників (інсайдерські атаки) значною мірою підвищують вразливість цифрової інфраструктури. Саме тому кадрова безпека виступає важливим фактором підтримки цифрової стійкості.

Вплив фінансової підсистеми на техніко-технологічну безпеку. Нестача фінансових ресурсів або пріоритетне спрямування коштів на інші напрямки може обмежити можливості підприємства щодо оновлення технологічної бази, впровадження систем захисту, модернізації обладнання чи закупівлі сучасного програмного забезпечення. У результаті підприємство опиняється в умовах технологічного відставання, що знижує його здатність протистояти зовнішнім і внутрішнім викликам.

Таким чином, економічна безпека підприємства формується як багатофакторна, взаємозалежна система, у якій ефективне функціонування кожної підсистеми залежить від стабільності інших.

Забезпечення ефективного управління економічною безпекою підприємства в умовах цифрової трансформації потребує не лише аналізу окремих підсистем, а й узагальнення результатів оцінювання в єдиний інтегрований показник. Такий підхід дозволяє не лише виявити слабкі місця системи, а й забезпечити її стратегічну цілісність, своєчасно виявляти критичні відхилення та приймати зважені управлінські рішення.

Інтегральна оцінка дозволяє сформувати загальне уявлення про рівень економічної безпеки підприємства на основі комплексного моніторингу його фінансової, кадрової, техніко-технологічної підсистем, а також цифрової

безпеки. Це особливо важливо для попередження кризових ситуацій та загроз банкрутства, адже навіть незначне зниження стійкості в одній із підсистем може спровокувати системну дестабілізацію. Комплексний підхід до оцінювання дозволяє зменшити ризики недооцінки загроз і забезпечити превентивне реагування на їх прояви.

У більшості сучасних досліджень узагальнення стану підсистем реалізується через побудову інтегрального індексу економічної безпеки, що поєднує в собі ключові показники всіх підсистем та трансформує їх у єдине числове значення. Такий індекс виступає зручним і об'єктивним інструментом для оцінювання рівня захищеності підприємства, з можливістю подальшого порівняння між підприємствами, періодами чи секторами економіки.

Наприклад, у роботі Г. Жаворонкової та В. Жмуденко [137] було запропоновано методику побудови інтегрального показника економічної безпеки підприємств аграрного сектора. У моделі було виділено чотири підсистеми: виробничо-фінансову, матеріально-технічну, соціально-економічну та еколого-техногенну. Найбільшу питому вагу в оцінці безпеки, згідно з експертними опитуваннями, отримали виробничо-фінансова (0,31–0,35) та матеріально-технічна (0,29–0,32) складові, що свідчить про їхню критичну роль у формуванні загальної стійкості підприємств.

Подібний підхід реалізовано і в дослідженні С. Пілецької та інші [175], де на основі системного підходу розроблено модель інтегральної оцінки економічної безпеки підприємства, що охоплює фінансову, кадрову, техніко-технологічну та виробничо-збутову складові. Модель дає змогу не лише оцінити поточний стан підприємства, а й спрогнозувати його динаміку розвитку, визначаючи напрямки корекційної політики.

Окрему увагу заслуговує робота Л. Лелик та інші [63], у якій застосовано ресурсно-функціональний підхід до побудови інтегрального індексу безпеки. Дослідження демонструє, що навіть при задовільному загальному рівні безпеки (індекс 7,04 з 10), аналіз компонентного складу може виявити критично низькі значення окремих підсистем (наприклад, фінансової – 0,452,

інформаційної – 0,554, правової – 0,647). Це підкреслює важливість не лише інтегральної оцінки, а й деталізації результатів, які дозволяють приймати точкові управлінські рішення.

У цифрову епоху особливої важливості набуває інтеграція цифрової безпеки у всі рівні моделі економічної безпеки, оскільки більшість сучасних ризиків мають цифрову природу або реалізуються через цифрові канали. Побудова інтегрального індексу економічної безпеки із врахуванням цифрової компоненти дозволяє сформувати цілісну захисну архітектуру, орієнтовану на мінімізацію технологічних, фінансових, організаційних та кадрових ризиків.

Узагальнюючи викладене, у межах цього дослідження автором запропоновано системну композицію ключових елементів системи економічної безпеки підприємства в умовах цифровізації бізнес-процесів (рис. 1.9). На відміну від традиційних статичних структур, представлена композиція базується на принципах динамічної адаптивності та інтеграції цифрової складової як наскрізного чинника впливу на всі ключові підсистеми. Запропонована схема візуалізує ієрархію взаємозалежностей, де цифрова трансформація виступає не лише джерелом нових загроз, а й інструментальним базисом для підвищення загальної резистентності підприємства.

Розроблення ефективної стратегії управління економічною безпекою постає фінальною стадією аналітичного циклу, що має на меті гарантування стабільної життєдіяльності суб'єкта господарювання в парадигмі цифрової економіки. У сучасних наукових розробках поширеною є класифікація стратегічних альтернатив управління безпекою відповідно до фаз життєвого циклу організації [198], яка диференціює їх на:

- стратегії випереджаючого зростання (орієнтовані на інтенсифікацію інноваційного розвитку та розширення ринкової присутності);
- стратегії адаптивної стабілізації (спрямовані на підтримання наявних параметрів захищеності та збереження ресурсного потенціалу);

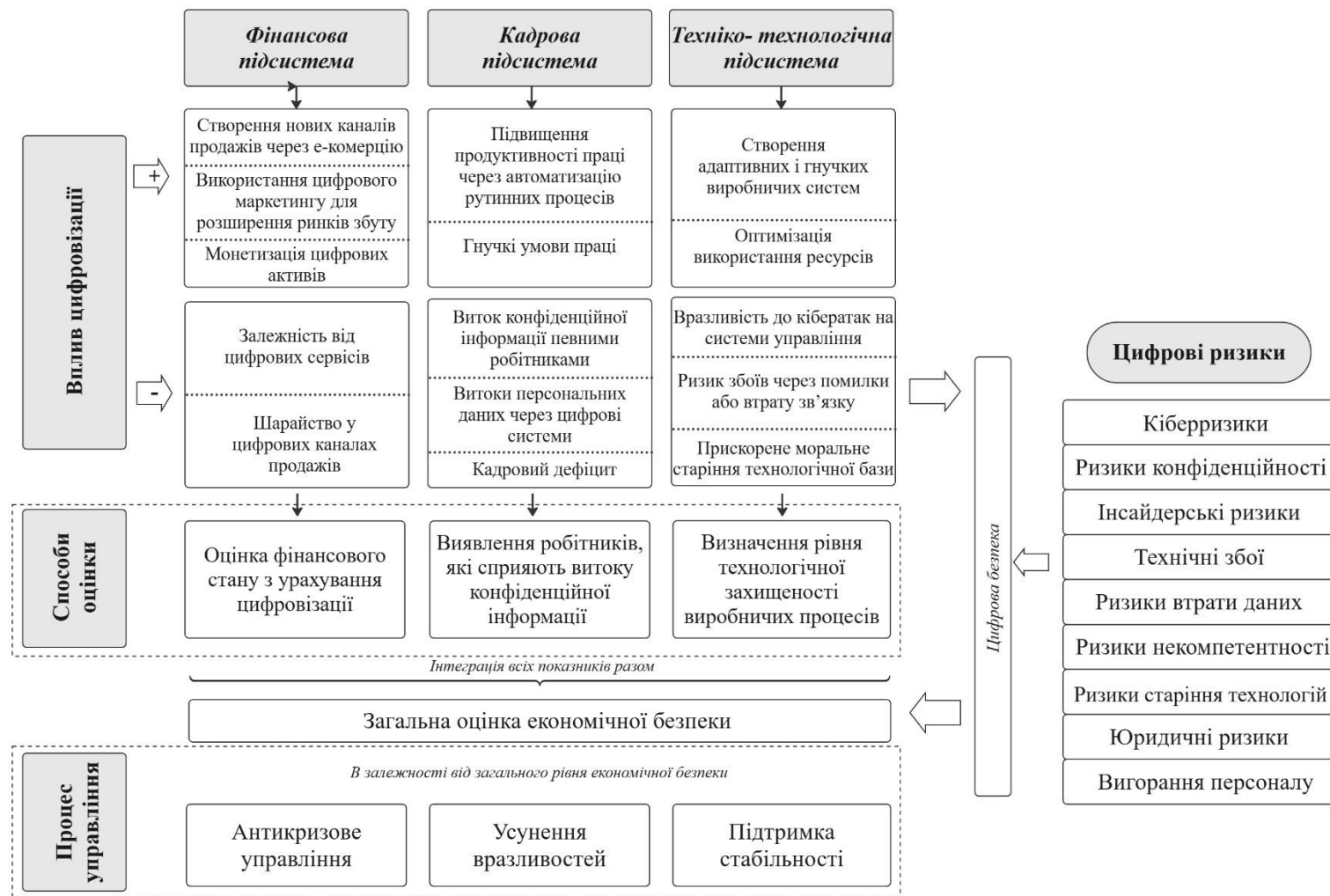


Рис. 1.9. Системна композиція ключових елементів системи економічної безпеки підприємства в умовах цифровізації бізнес-процесів. Джерело: складено автором [111]

– стратегії антикризової реструктуризації або санації (актуалізуються за умов виникнення критичних деструктивних впливів та необхідності системних трансформацій).

Як зазначає О. Роженко [181], концептуальний підхід до побудови стратегій економічної безпеки передбачає розробку нової моделі управління, що враховує динамічні зміни зовнішнього середовища, цифрові ризики, інституційні обмеження та внутрішній потенціал підприємства. У рамках цієї концепції стратегія безпеки повинна не лише нейтралізувати загрози, а й ідентифікувати можливості зростання, трансформуючи функцію безпеки з реактивної на проактивну.

Враховуючи побудовану модель економічної безпеки, яка інтегрує оцінки фінансової, кадрової, техніко-технологічної та цифрової підсистем, доцільно формувати стратегію безпеки підприємства відповідно до виявленого рівня ризику. На основі цього було розроблену наступні рекомендаційні стратегічні орієнтири:

Антикризове управління – застосовується за низького рівня безпеки, що свідчить про високі ризики банкрутства, технологічну деградацію або критичну кадрову нестабільність. Основна мета стратегії – локалізація загроз, фінансова стабілізація, зниження цифрових вразливостей, реструктуризація активів.

Усунення вразливостей – доцільне за середнього рівня безпеки, коли підприємство не перебуває в кризі, але існують суттєві точки ризику в окремих підсистемах. Стратегія передбачає таргетоване підсилення слабких ланок, оновлення технічної бази, посилення контролю над цифровою інфраструктурою, підвищення кваліфікації персоналу.

Підтримка стабільності – рекомендована за високого рівня безпеки, що характеризує підприємство як достатньо стійке до внутрішніх і зовнішніх загроз. У цьому випадку стратегія фокусується на підтриманні досягнутого рівня, адаптивності до нових викликів та інвестиціях у цифрову інфраструктуру, що підвищують довгострокову стійкість.

Застосування таких стратегій забезпечує зв'язок між аналітичним оцінюванням та управлінськими рішеннями, дозволяючи трансформувати результати діагностики у реальні заходи з підвищення безпеки. Це особливо важливо в умовах цифрової трансформації, де ризики виникають швидко, масштабуються миттєво й вимагають адаптивних підходів до управління.

У межах реалізації стратегії управління економічною безпекою підприємства важливим етапом є визначення конкретних організаційно-технологічних ініціатив, спрямованих на підвищення стійкості до загроз цифрового середовища. Для забезпечення стабільного функціонування підприємства та мінімізації впливу зовнішніх і внутрішніх ризиків у процесі цифрової трансформації, доцільно впроваджувати комплекс заходів, які охоплюють як технічну, так і організаційну площину функціонування системи економічної безпеки [114].

По-перше, важливим напрямом є впровадження інтегрованих автоматизованих систем управління, які забезпечують цифрову взаємодію між усіма рівнями управлінської і виробничої діяльності. Йдеться про системи підготовки виробництва, управління проектними даними, відносинами з клієнтами тощо [193]. Такі рішення не лише сприяють централізації зберігання та обробки інформації в режимі реального часу, але й дозволяють оперативно реагувати на зміни у внутрішньому та зовнішньому середовищі.

По-друге, використання хмарних обчислень і моделей типу Software-as-a-Service забезпечує гнучке масштабування ІТ-ресурсів, підвищує доступність сучасних цифрових інструментів для малих і середніх підприємств, мінімізуючи потребу в капітальних витратах. Автоматичне оновлення безпекових модулів, резервне копіювання та функції відновлення даних у разі інцидентів забезпечують підвищену кіберстійкість навіть в умовах надзвичайних ситуацій.

По-третє, до критичних елементів цифрової трансформації належить організація внутрішнього навчання персоналу. Розробка методичних матеріалів, політик цифрової етики, інструкцій з використання нових ІТ-

систем та стандартів інформаційної безпеки формує цифрову компетентність персоналу, яка є основою кадрової безпеки в умовах нових викликів. Освітній компонент має охоплювати як базову цифрову грамотність, так і навички роботи з аналітичними системами, управління даними та реагування на кіберінциденти.

Важливою передумовою стійкого цифрового розвитку є також модифікація організаційної структури управління, зокрема перехід від жорстко ієрархічних моделей до адаптивних структур, які забезпечують більшу гнучкість, децентралізацію повноважень і прискорене прийняття рішень. У таких моделях менеджери цифрової трансформації відіграють ключову роль як координатори інноваційних змін та лідери міждисциплінарної взаємодії.

Окремої уваги заслуговує налагодження співпраці з технологічними партнерами, зокрема постачальниками програмного забезпечення, ІТ-консультантами та системними інтеграторами. Така взаємодія дозволяє скоротити строки впровадження цифрових рішень, забезпечити високу якість технологічної інтеграції, а також мінімізувати ризики, пов'язані з помилками у виборі рішень або відсутністю внутрішньої технічної експертизи. Залучення зовнішніх фахівців також посилює відповідність вимогам інформаційної безпеки.

Зрештою, формування внутрішньої культури інновацій та адаптивності є довгостроковим, але критично важливим елементом стратегії економічної безпеки. Заохочення ініціативності, підтримка експериментування, відкритість до змін і залучення персоналу до вдосконалення процесів дозволяє створити гнучку організацію, здатну швидко реагувати на технологічні, ринкові та регуляторні виклики.

Таким чином, реалізація комплексного набору ініціатив дозволяє підприємству не лише забезпечити свою економічну безпеку, а й формувати конкурентні переваги в цифровій економіці, адаптуючись до динамічних умов середовища. В рамках дослідження було розроблено загальну схему

управління системою економічної безпеки в умовах цифрової трансформації, яка показана на рис. 1.10.



Рис. 1.10. Схема управління системою економічної безпеки підприємства в умовах цифрової трансформації.

Джерело: складено автором

На основі проведеного критичного аналізу існуючих теоретико-методологічних підходів та враховуючи трансформаційний вплив цифровізації на господарську діяльність, було розроблено концептуальну модель системи економічної безпеки підприємства в умовах цифрової трансформації (рис. 1.11).

Таким чином, удосконалено концептуальну модель системи економічної безпеки підприємства, яка, на відміну від існуючих, базується на принципах системної конвергенції фінансової, кадрової та техніко-технологічної

підсистем у єдину захисну архітектуру з визначенням цифрової безпеки як наскрізного регулятора стійкості, що дозволяє формалізувати підсистемні взаємозв'язки в умовах динамічної трансформації середовища, забезпечити перехід до проактивного управління на основі інтегрального оцінювання вразливостей та обґрунтувати вибір адаптивних стратегічних ініціатив в парадигмі цифровізації підприємства.

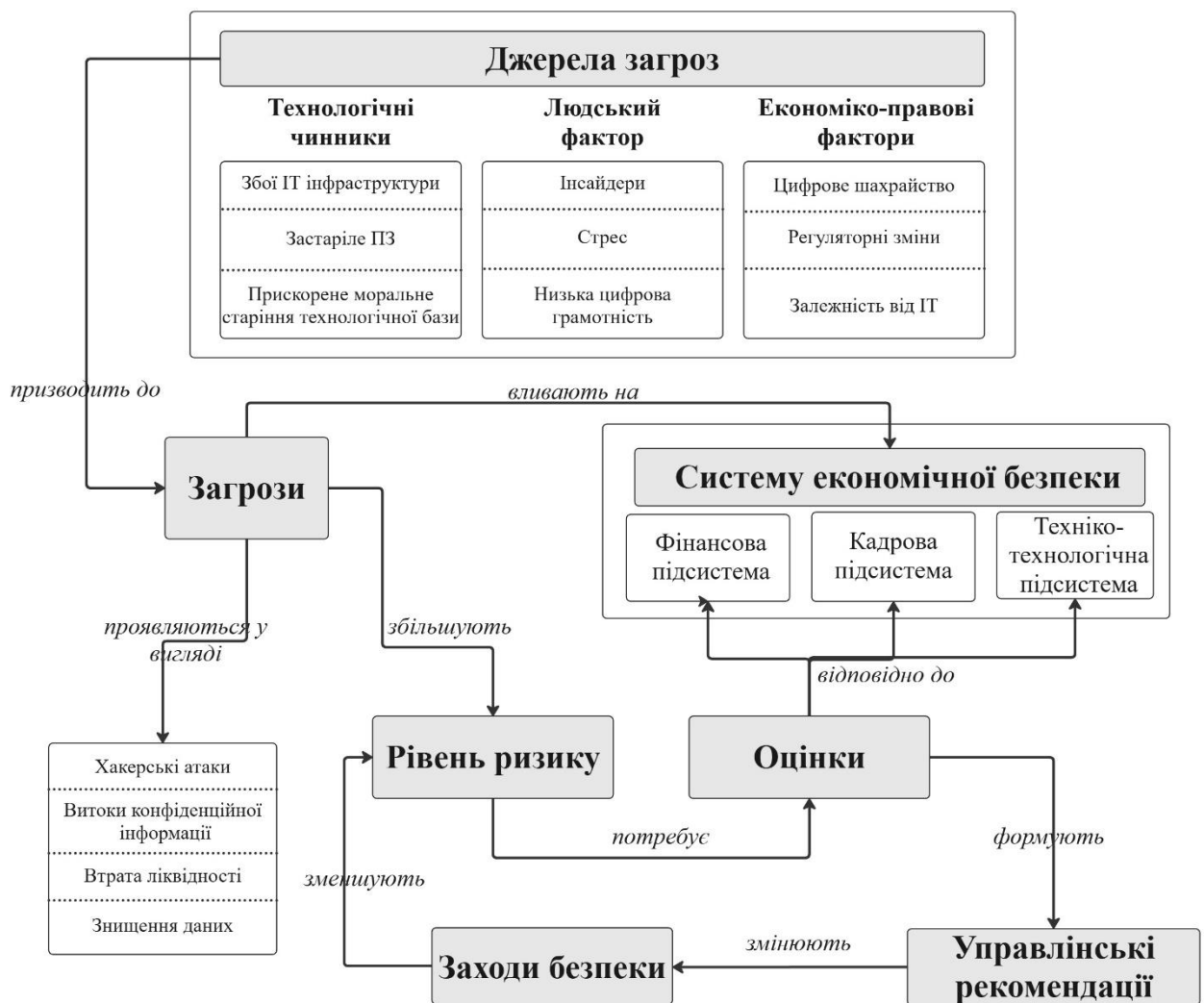


Рис. 1.11. Концептуальна модель системи економічної безпеки підприємства в умовах цифрової трансформації.

Джерело: складено автором

## Висновки до першого розділу

У першому розділі здійснено теоретичне узагальнення та обґрунтування концептуальних засад управління економічною безпекою підприємства в умовах інтенсифікації цифрових трансформацій. Отримані результати дозволили сформулювати такі висновки:

1. Встановлено, що категорія «економічна безпека підприємства» пройшла суттєву еволюцію від вузькоспрямованої захисної концепції до системного інструментарію забезпечення сталого розвитку. Систематизація наукових підходів дозволила інтерпретувати економічну безпеку як динамічний стан суб'єкта господарювання, що характеризується резистентністю до деструктивних впливів та здатністю до розширеного відтворення в мінливому екзогенному середовищі.

2. Сформовано архітектуру системи економічної безпеки, яку представлено як сукупність взаємопов'язаних функціональних складових. Доведено, що в умовах цифровізації фінансова, кадрова, техніко-технологічна та інформаційна підсистеми набувають ознак пріоритетності, оскільки саме вони формують базис цифрової резистентності підприємства. При цьому ефективність функціонування системи безпосередньо залежить від злагодженості механізмів превентивного та антикризового управління.

3. Визначено, що цифрова трансформація є багатовимірним процесом фундаментальної перебудови операційної моделі підприємства, де цифрові технології виступають каталізатором генерування нових бізнес-моделей. Встановлено дуальність впливу цифрових інновацій: поряд із підвищенням операційної ефективності та клієнтоорієнтованості, вони зумовлюють зростання капіталомісткості бізнесу та підвищують рівень його вразливості до специфічних кіберзагроз.

4. З'ясовано, що поточний стан цифровізації вітчизняного бізнесу характеризується переважно поверхневим рівнем, що створює ризики технологічного відставання та зниження конкурентоспроможності на

глобальних ринках. Зазначене обґрунтовує необхідність розроблення нової концептуальної моделі системи економічної безпеки, адаптованої до викликів четвертої промислової революції.

5. Систематизовано типологію цифрових ризиків, що дозволило уточнити вектори їхнього деструктивного впливу на ключові компоненти стійкості підприємства. На цій основі розроблено концептуальний підхід до формування системи економічної безпеки, специфічною особливістю якої є виокремлення цифрової безпеки як наскрізного компонента, що інтегрується у всі функціональні підсистеми.

6. Обґрунтовано, що базисом для вибору стратегічного орієнтиру розвитку системи має слугувати інтегральна оцінка рівня безпеки, яка дозволяє формалізувати стан захищеності через сукупність кількісних та якісних показників. Доведено, що результативність запропонованої системи детермінується впровадженням комплексу організаційно-технологічних ініціатив, спрямованих на гармонізацію інтересів підприємства в умовах цифрового простору.

Наукові результати дослідження висвітлено у роботах [109, 111, 114, 115, 144].

## **РОЗДІЛ 2. МЕТОДИЧНІ ЗАСАДИ ОЦІНКИ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА**

### **2.1. Методичні підходи до оцінки рівня економічної безпеки підприємства**

Дослідження методологічних засад оцінювання економічної безпеки підприємства доцільно розпочати з ретроспективного аналізу її формування та еволюції. Історичні передумови розвитку цієї наукової категорії засвідчують, що, хоча концептуальні елементи економічної безпеки опосередковано розглядалися в рамках теорій економічної стійкості, ризик-менеджменту та антикризового управління ще у другій половині XX століття, систематизоване вивчення економічної безпеки підприємств як окремого об'єкта дослідження активізувалося лише з початку 1990-х років.

Згідно з аналізом наукових джерел, процес розвитку методології оцінювання економічної безпеки підприємства умовно можна поділити на чотири етапи, кожен із яких мав свої характерні риси, наукову парадигму та інструментальний супровід:

Початковий етап (1990–1999 рр.). Цей період позначився формуванням базових уявлень про сутність економічної безпеки як об'єкта дослідження. Основна увага зосереджувалася на запозиченні методів з фінансового аналізу та суміжних галузей знань, що обумовило домінування індикативного підходу. Економічна безпека підприємства трактувалася переважно як фінансова стабільність і платоспроможність, без достатнього врахування інших складових та системного підходу до оцінювання загроз.

Етап диференціації (2000–2009 рр.). Відбувся якісний зсув у науковому дискурсі: понятійний апарат ЕБП було суттєво розширено, а сама концепція - деталізована через виокремлення основних функціональних складових економічної безпеки: фінансової, виробничої, кадрової, інформаційної,

екологічної, техніко-технологічної тощо. Методологічний апарат зазнав трансформацій через появу ресурсно-функціонального підходу, що дозволив враховувати специфіку різних аспектів діяльності підприємств та зовнішніх загроз.

Етап інтеграції (2010–2019 рр.). Цей період ознаменувався формуванням комплексних систем оцінювання економічної безпеки підприємства, що поєднували кількісні та якісні методи, а також статичні й динамічні показники. Акцент робився на адаптацію методик до галузевих особливостей, формувалася основа для побудови універсальних моделей, здатних відображати взаємозв'язки між складовими безпеки в умовах змінного економічного середовища.

Сучасний етап (з 2020 р.). Поточний етап розвитку характеризується впровадженням цифрових технологій в інструментарій оцінювання економічної безпеки підприємства. Застосовуються інструменти штучного інтелекту, нейронних мереж і методів машинного навчання для прогнозування загроз і виявлення аномальних тенденцій у діяльності підприємств. Активно розробляються адаптивні системи моніторингу, які забезпечують вчасне реагування на кризові явища, що особливо актуально в умовах зростання нестабільності й невизначеності в глобальному економічному середовищі.

Кожен із зазначених етапів розвитку методології оцінювання економічної безпеки підприємства відповідав специфічним умовам господарювання, рівню розвитку економічної науки та наявним інституційним обмеженням. У сукупності вони формують підґрунтя для подальшого удосконалення теоретико-методичних підходів, орієнтованих на комплексну оцінку економічної безпеки в умовах динамічного ризикового середовища.

У науковій літературі представлено широкий спектр підходів до моделювання та оцінювання економічної безпеки підприємства, які відображають різні наукові школи, дослідницькі традиції та прикладні завдання. За результатами аналізу вітчизняних і зарубіжних джерел, доцільно виділити чотири основні методологічні підходи: індикативний, ресурсно-

функціональний, експертний та алгоритмічний. Кожен із них має власну концептуальну базу, переваги та обмеження, що визначає можливість їх застосування в різних умовах функціонування підприємств.

Індикативний підхід ґрунтується на використанні системи кількісних показників, які відображають стан різних функціональних сфер діяльності підприємства. Оцінювання рівня економічної безпеки підприємства здійснюється шляхом порівняння фактичних значень цих показників із наперед визначеними пороговими значеннями (індикаторами). Відхилення від нормативу інтерпретується як потенційна загроза: чим більше відхилення – тим нижчий рівень економічної безпеки.

Так, у підході, запропонованому М.М. Єрмошенко, у якості критерію оцінки пропонується використовувати прибуток підприємства [136]. Однак цей підхід має певні обмеження, оскільки прибуток є абсолютним показником, значення якого слід інтерпретувати в контексті інших фінансових індикаторів, зокрема ліквідності, рентабельності та платоспроможності.

Більш деталізовану методику пропонує Г.В. Козаченко [149], яка рекомендує оцінювати економічну безпеку через співвідношення бруто-інвестицій підприємства та обсягу інвестиційних ресурсів, необхідних для забезпечення безпечного функціонування:

$$K = \frac{I_{\text{брутто}}(t)}{I_{\text{необх}}(t)},$$

де

$I_{\text{брутто}}(t)$  – фактичні інвестиції у році  $t$ , грош. од.,

$I_{\text{необх}}(t)$  – необхідні інвестиції для забезпечення економічної безпеки у тому ж періоді, грош. од. чим ближче цей коефіцієнт до одиниці, тим вищий рівень безпеки.

Автором запропоновано диференційовану шкалу рівнів безпеки: до 0,05 – підтримуючий; 0,06-0,10 – мінімальний; 0,11-0,19 – дуже низький; 0,20-0,29 – низький; 0,30-0,49 – середній; 0,50-0,70 – високий; понад 0,70 – дуже високий. Ця шкала демонструє глибину опрацювання питання, однак

основним викликом залишається об'єктивне визначення обсягу «необхідних інвестицій», що часто є оціночним показником [149].

У дослідженні О.М. Чернеги [200] індикативний підхід базується на визначенні порогових значень ключових показників, що характеризують фінансову стійкість та платоспроможність підприємства. Авторка сформувала перелік індикаторів, які дозволяють вимірювати рівень фінансової безпеки підприємства за такими напрямками, як ліквідність, ділова активність, рентабельність та загальна фінансова стійкість.

Ще один варіант реалізації індикаторного підходу запропонований В.Т. Шлемком [204], який застосовує графічний метод зіставлення фактичних та граничних значень індикаторів. На основі цього зіставлення виділяються три зони: нормального, критичного та передкризового стану економічної безпеки. Граничні значення показників встановлюються з урахуванням мінімально припустимого рівня функціонування, порушення якого сигналізує про входження підприємства до зони ризику.

Перевагами індикаторного підходу є його простота, можливість оперативної реалізації, порівняльна дешевизна та зручність для регулярного моніторингу. Він не потребує великих обсягів інформації та може бути впроваджений навіть за умов обмеженої аналітичної бази. Водночас, його ефективність значною мірою залежить від обґрунтованості обраної системи показників, адекватності порогових значень та врахування галузевої специфіки. Серед недоліків варто зазначити високий рівень суб'єктивності у встановленні індикаторів і складність адаптації системи оцінки до динамічних змін у зовнішньому середовищі.

Ресурсно-функціональний підхід розглядає економічну безпеку підприємства крізь призму ефективності використання внутрішніх ресурсів у межах ключових функціональних підсистем. Методологічним підґрунтям цього підходу є припущення, що раціональне управління ресурсним потенціалом дозволяє мінімізувати ризики, своєчасно реагувати на

деструктивні впливи та створювати умови для стабільного розвитку підприємства в довгостроковій перспективі.

У науковій практиці ресурсно-функціональний підхід нерідко поєднується з комплексним підходом, у результаті чого формується ієрархічна структура оцінювання. Згідно з цим підходом, економічна безпека трактується як система функціональних блоків, кожен з яких, у свою чергу, представлений набором специфічних показників. Це дозволяє здійснювати як локальну оцінку стану окремих сфер безпеки, так і інтегральну оцінку загального рівня захищеності підприємства.

Так, у працях О. В. Ареф'євої [106] економічна безпека підприємства трактується як стан ефективного використання корпоративних ресурсів та наявних ринкових можливостей, що дозволяє нейтралізувати внутрішні та зовнішні загрози і забезпечувати тривале виживання та стійкий розвиток суб'єкта господарювання. В межах ресурсно-функціонального підходу авторка пропонує здійснювати оцінювання через систему локальних інтегральних індикаторів за ключовими складовими (фінансовою, кадровою, техніко-технологічною, інформаційною тощо), що розраховуються шляхом нормування та зважування часткових показників діяльності. Важливою особливістю цього підходу є акцент на аналізі рівнів безпеки виключно в динаміці, що дозволяє інтегрувати результати оцінки в механізм стратегічного планування та адаптивного управління потенціалом підприємства.

У роботі С.Ф. Покропивного [177] представлена методика оцінювання економічної безпеки підприємства на основі інтегрального показника, де значення окремих функціональних критеріїв визначаються шляхом зіставлення ймовірної величини потенційних збитків із сумою витрат на впровадження превентивних заходів. Такий підхід дозволяє пов'язати рівень безпеки з ефективністю запобіжних дій і ресурсоемністю механізмів протидії ризикам.

Інший варіант реалізації ресурсно-функціонального підходу запропонований С. Ілляшенком [148], який розглядає економічну безпеку

підприємства як синтез чотирьох функціональних компонентів: фінансової, ринкової, інтерфейсної та інтелектуальної. Згідно з автором, оцінка загального рівня безпеки повинна здійснюватися шляхом інтегрування індивідуальних показників, при цьому вагові коефіцієнти кожної складової визначаються з використанням евристичних методів.

Розвиваючи цей підхід, О.М. Вовк [125] пропонує використовувати вартісно-орієнтовану послідовність оцінок, що дозволяє визначити рівень безпеки через оцінку резервів для забезпечення безперервності виробництва та інвестиційної привабливості. Такий підхід є особливо актуальним для підприємств із тривалим виробничим циклом, оскільки враховує галузеву специфіку та необхідність сертифікації.

У статті І.П. Оттенка та І.А. Яртим [169] наголошується, що однією з ключових вимог до забезпечення належного рівня економічної безпеки підприємств є обґрунтований вибір як методів її оцінювання, так і релевантних критеріїв. Запропонований авторами підхід базується на багатокритеріальному оцінюванні рівня економічної безпеки розвитку підприємства з урахуванням значущості окремих факторів та характеру їх змін. Формування системи показників здійснюється на основі фінансової та статистичної звітності, що забезпечує вищу ступінь достовірності даних та мінімізує ймовірність суперечливих оцінок. Це дозволяє використовувати результати оцінювання як аналітичну базу для прийняття стратегічних управлінських рішень, формування програм розвитку та здійснення ефективного контролю за їх реалізацією.

У продовження цього підходу, у роботі Н. Гавлонської та інших [128] запропоновано методику інтегрального оцінювання рівня економічної безпеки підприємства, що також базується на функціональному структуруванні складових. Інтегральний показник формується шляхом агрегування оцінок за такими функціональними компонентами, як: ресурсна, фінансово-економічна, організаційно-правова, управлінська, технологічна, інформаційна, кадрова та соціальна. Такий підхід дозволяє забезпечити комплексний огляд внутрішніх і

зовнішніх ризиків, а також оперативне реагування на потенційні загрози з боку підрозділів економічної безпеки.

Інструментальною базою для обчислення інтегрального показника слугує метод відстаней, який передбачає визначення ступеня відхилення поточних значень показників від їх еталонних (порогових) значень. Формально інтегральна оцінка  $I_i$  за  $i$ -ою функціональною компонентою визначається за формулою:

$$I_i = \sqrt{\sum_{j=1}^k w_j \left(1 - \frac{x_j}{x_{max}}\right)^2},$$

де:

$I_i$  – інтегральна оцінка функціональної компоненти економічної безпеки,

$w_j$  – питома вага  $j$ -го індикатора у структурі компоненти,

$x_j$  – фактичне значення  $j$ -го показника,

$x_{max}$  – еталонне (максимально бажане) значення  $j$ -го показника,

$k$  – кількість індикаторів, що входять до функціональної компоненти.

Важливо зазначити, що за цією методикою нижче значення інтегрального показника інтерпретується як сигнал про більш високий рівень небезпеки для підприємства.

Ресурсно-функціональний підхід має низку важливих переваг, що обумовлюють його популярність у наукових дослідженнях і практичному застосуванні. Його головною перевагою є системність, що дозволяє розглядати економічну безпеку підприємства як сукупність взаємопов'язаних функціональних складових. Такий підхід забезпечує комплексне охоплення основних сфер діяльності підприємства, що сприяє повноті оцінки. Важливою перевагою також є адаптивність до галузевих особливостей: система індикаторів може бути модифікована відповідно до специфіки конкретного підприємства. Простота розрахунків та орієнтація на фінансову і статистичну

звітність забезпечують зручність реалізації та аналітичну обґрунтованість отриманих результатів.

Водночас застосування цього підходу супроводжується низкою обмежень. Зокрема, відсутність уніфікованого переліку функціональних складових економічної безпеки зумовлює варіативність методик і ускладнює стандартизацію оцінювання. Крім того, орієнтація переважно на ретроспективні показники знижує прогностичну цінність такого підходу в умовах динамічного середовища. Часто економічні ризики залишаються поза увагою або враховуються недостатньо повно, що знижує точність оцінки. Також спостерігається низький рівень залученості функціональних підрозділів підприємства до процесу оцінювання, що може негативно впливати на ефективність впровадження результатів аналізу у практику управління.

Експертний підхід до оцінювання рівня економічної безпеки підприємства базується на залученні фахівців із відповідною кваліфікацією, знаннями та досвідом. Його особливість полягає в можливості якісного аналізу складних і слабоформалізованих характеристик безпеки, які не піддаються точному кількісному вимірюванню. Методика реалізації включає послідовні етапи: формулювання цілей оцінки, добір експертів, визначення критеріїв, оцінювання їхньої значущості (через ранжування, бальну оцінку або попарні порівняння), вагове нормування результатів і подальше агрегування для отримання інтегральної оцінки. У практиці експертного оцінювання використовуються різні методи: метод рангових оцінок, метод бальної шкали, метод попарних порівнянь, а також метод Дельфі, який передбачає багатетапне узгодження суджень експертів із наданням зворотного зв'язку. Їх застосування забезпечує гнучкість у виборі підходу залежно від цілей і контексту дослідження.

Значний внесок у розвиток експертного підходу зробили Г.В. Козаченко та Ю.С. Погорєлов [148], які наголошують на доцільності його використання у випадках, коли неможливо отримати достовірну або повну інформацію про стан об'єкта, а формалізація досліджуваних процесів є обмеженою. У таких

умовах професійні судження фахівців стають ключовим джерелом знань для оцінки рівня безпеки.

Окрему увагу слід приділити підходу, запропонованому О.В. Мельніченко [160], яка стверджує, що оцінка фінансової безпеки підприємства не може ґрунтуватися виключно на кількісних показниках, отриманих із фінансової чи управлінської звітності. На думку авторки, ці показники часто відображають лише моментний стан і не враховують повноти ситуації. Водночас саме професійне судження експертів дозволяє інтегрувати як об'єктивну інформацію, так і суб'єктивні фактори, що формують реальний рівень безпеки підприємства. Проте важливо враховувати, що метод експертних оцінок має свої обмеження, пов'язані з можливою упередженістю, когнітивними викривленнями та неоднозначністю інтерпретації результатів.

Серед основних переваг експертного підходу слід виокремити його здатність враховувати чинники, що складно або взагалі не піддаються формалізації. У випадках, коли відсутня повна або достовірна інформація, саме експертна думка виступає джерелом якісної оцінки. Метод дозволяє отримати обґрунтовані результати завдяки залученню фахівців із відповідною компетенцією, а групова форма експертного оцінювання сприяє підвищенню надійності та об'єктивності висновків.

В той же час, експертний підхід має низку обмежень. Зокрема, характерною рисою є високий рівень суб'єктивізму, який зумовлений індивідуальними уявленнями, досвідом і когнітивними упередженнями експертів. Крім того, значний вплив на результати мають кваліфікація, галузева компетентність та мотивація залучених осіб. Узгодження оцінок між експертами може бути ускладненим, особливо при різноманітності думок, що потребує ретельної організації процесу та застосування відповідних методичних процедур.

Алгоритмічний підхід до оцінювання рівня економічної безпеки підприємства ґрунтується на використанні формалізованих математичних і статистичних методів, що дозволяють моделювати залежності між множиною

внутрішніх і зовнішніх факторів та інтегральним рівнем безпеки. Особливістю цього підходу є його здатність забезпечити об'єктивність, точність та прогностичну здатність оцінювання завдяки використанню кількісно вимірюваних змінних і статистичних закономірностей.

До основних методів, які використовуються в межах алгоритмічного підходу, належать:

- економіко-математичне моделювання, що дозволяє будувати функціональні залежності між ключовими показниками діяльності підприємства;
- теорія нечіткої логіки, яка дає змогу оперувати лінгвістичними змінними в умовах невизначеності;
- нейромережеве моделювання, здатне виявляти складні нелінійні взаємозв'язки між показниками;
- дискримінантний аналіз, що використовується для класифікації підприємств за рівнем економічної безпеки та діагностики ймовірності настання кризових подій.

Однією з ранніх реалізацій цього підходу є розробка багатофакторної лінійної моделі економічної безпеки, запропонованої Д. Ковальовим та І. Плетніковою [146]. В основі моделі лежить кількісне вираження економічної безпеки підприємства як функції від інших показників його господарської діяльності.

Особливу увагу в рамках алгоритмічного підходу приділяють моделям прогнозування банкрутства, які базуються на дискримінантному аналізі. У роботі О.В. Кучмей [155] здійснено критичний аналіз переваг і недоліків найбільш поширених моделей оцінки ймовірності банкрутства зокрема, моделей Альтмана, Спрінгейта, Ліса, Таффлера, Терещенка, Матвійчука, а також коефіцієнта Бівера. В цій роботі було обґрунтовано важливість ранньої діагностики фінансових ризиків як ключового чинника забезпечення економічної безпеки в умовах трансформації економіки.

Подібну спрямованість має також симулятивна модель системи фінансової безпеки, розроблена у [171]. На основі економіко-математичного моделювання здійснено оптимізацію обсягів виробництва, що дозволило визначити такі параметри діяльності підприємства, за яких максимізуються показники рентабельності, а отже – зміцнюється його внутрішня економічна безпека. Модель також має прикладне значення для прогнозування фінансових потоків і розробки управлінських рішень у сфері фінансової стабільності.

Сучасний розвиток цього підходу представлено у дослідженні С.Т. Пілецької та інших [174]. Автори пропонують методику стратегічного забезпечення безпеки, що базується на вимірюванні рівня розвитку цифрової економіки та ступеня її впливу на діяльність підприємства. Ключовим елементом тут виступає оцінка цифрової стійкості, що дозволяє адаптувати систему безпеки до вимог четвертого етапу глобалізації та оперативно реагувати на специфічні ІТ-ризики.

Окремий напрям алгоритмічного підходу представлений роботами Л.А. Останкова та Н.Ю. Шевченко [167], які пропонують оцінювати рівень економічної безпеки підприємства через визначення ступеня ризику його банкрутства із застосуванням методів нечіткого аналізу. У рамках дослідження запропоновано якісно-кількісну методику діагностики фінансового стану промислового підприємства, яка поєднує експертні судження та розрахункові процедури, що дозволяє враховувати як формалізовані, так і нечітко виражені характеристики загроз.

Застосування алгоритмічного підходу в оцінюванні економічної безпеки підприємства має низку вагомих переваг. Насамперед, його сильним боком є можливість дослідження статистичної значущості вхідних параметрів, що дозволяє ідентифікувати найбільш впливові фактори, які визначають рівень безпеки. Такий підхід забезпечує обґрунтованість висновків і підвищує точність класифікації підприємств за рівнем економічної безпеки. Крім того, моделі, побудовані в межах цього підходу, дозволяють адаптуватися до

специфічних умов функціонування окремих підприємств, що сприяє зростанню достовірності отриманих результатів.

Утім, алгоритмічний підхід має і певні обмеження. Його реалізація є досить трудомісткою, оскільки потребує формування значного обсягу якісних статистичних даних для навчання та перевірки моделей. Побудова математичних залежностей і їх валідація вимагають спеціалізованих знань і технічних ресурсів. Крім того, обмеженням є відносна інерційність моделей, оскільки внесення змін до структури або переліку вхідних параметрів часто потребує повного перегляду моделі або повторного навчання. Це знижує гнучкість у використанні підходу за умов швидкозмінного середовища.

Отже, класифікація існуючих підходів до оцінювання економічної безпеки підприємства може здійснюватися за різними критеріями: джерелами інформації (кількісні дані або експертні оцінки), рівнем формалізації (інтуїтивні або алгоритмічні) та складністю реалізації (від простих матричних схем до складних адаптивних моделей). Класичні підходи (індикативний, ресурсно-функціональний) є доступними для широкого застосування, тоді як сучасні підходи дедалі частіше включають методи математичного моделювання, штучного інтелекту й машинного навчання, що дозволяє підвищити точність прогнозування загроз і ефективність системи управління економічною безпекою підприємства. Узагальнена таблиця підходів, їх переваг та недоліків та відповідних методів оцінки рівня економічної безпеки наведено в табл. 2.1.

Проведений аналіз методичних підходів до оцінювання рівня економічної безпеки підприємства свідчить про необхідність використання комплексного інструментарію, адаптованого до умов конкретного підприємства, його галузевої специфіки, стратегічних пріоритетів та ризик-профілю. Незалежно від обраного підходу ключовим етапом у процесі оцінювання є формування системи показників, які кількісно відображають рівень безпеки в окремих функціональних підсистемах підприємства.

Таблиця 2.1

Характеристика основних підходів до оцінки економічної безпеки  
підприємства

| Назва підходу           | Суть                                                                                                                                    | Переваги підходу                                                                                       | Недоліки підходу                                                                                         | Вчені хто займався дослідженням                                                                                  |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Індикативний            | Оцінювання на основі порівняння фактичних значень показників з пороговими індикаторами.                                                 | Простота реалізації, можливість регулярного моніторингу, орієнтація на офіційні дані.                  | Суб'єктивізм у виборі індикаторів, складність адаптації до змін середовища, обмежене охоплення ризиків.  | М.М. Єрмошенко [136], Г.В. Козаченко [149], О.М. Чернега [200], В.Т. Шлемко [204]                                |
| Ресурсно-функціональний | Оцінка через ефективність використання ресурсів у межах функціональних підсистем підприємства.                                          | Системність, можливість урахування галузевої специфіки, комплексність оцінки, орієнтація на звітність. | Невизначеність складу функціональних компонент, обмежений облік ризиків.                                 | О.В. Ареф'єва [106], О.М. Вовк [125], С.Ф. Покропивний [177], С. Ілляшенко [142], І.П. Оттенко, І.А. Яртим [169] |
| Експертний              | Якісне оцінювання на основі професійного судження експертів.                                                                            | Урахування неформалізованих факторів, використання колективної думки, гнучкість застосування.          | Суб'єктивізм, когнітивні обмеження, залежність від кваліфікації експертів, складність узгодження оцінок. | С.Т. Пілецька та ін. [174], Г.В. Козаченко, Ю.С. Погорелов [148], О.В. Мельніченко [160]                         |
| Алгоритмічний           | Формалізоване моделювання залежностей між чинниками та рівнем економічної безпеки із застосуванням математичних і статистичних методів. | Ідентифікація впливових факторів, точність, адаптація до специфіки підприємств, прогнозування.         | Необхідність великого обсягу даних, складність реалізації.                                               | Д. Ковальов, І. Плетнікова [146], О.В. Кучмей [155], Л.А. Останков, Н.Ю. Шевченко [167]                          |

Джерело: складено автором

Однією з поширених практик є побудова системи показників, яка охоплює всі або вибрані підсистеми економічної безпеки – фінансову, кадрову, техніко-технологічну, інформаційну тощо. Варто підкреслити, що більшість наявних методик оцінювання економічної безпеки базується на обчисленні статичних коефіцієнтів, які відображають поточний стан підприємства в розрізі ключових функціональних сфер. Це дає змогу об'єктивно і стандартизовано оцінити рівень стійкості підприємства до потенційних загроз на основі формалізованих індикаторів. Найчастіше в науковій літературі при оцінці рівня економічної безпеки основну увагу зосереджують на фінансовій підсистемі, оскільки саме її показники мають найбільш прямий зв'язок із платоспроможністю, ліквідністю, інвестиційною привабливістю та загальною фінансовою стабільністю суб'єкта господарювання. У науковій літературі до найпоширеніших показників фінансової безпеки відносять коефіцієнт автономії капіталу, коефіцієнти поточної та швидкої ліквідності, рівень боргового, тощо. Високі значення ліквідності та автономії капіталу, у поєднанні з помірним борговим навантаженням і стабільною прибутковістю, свідчать про належний рівень фінансової безпеки підприємства. Як доводить Л. Докієнко [34], показники платоспроможності та фінансової стійкості мають високу кореляцію з інтегральним рівнем фінансової безпеки. У табл. 2.2 наведено типовий перелік показників, які найчастіше використовуються для оцінки фінансової складової економічної безпеки підприємства.

Після аналізу фінансових індикаторів, що традиційно є ядром оцінки економічної безпеки, доцільно розглянути кадрову підсистему, яка відіграє не менш важливу роль у забезпеченні стійкості підприємства. Саме персонал формує основу інтелектуального, операційного та управлінського потенціалу організації, тому стан кадрової сфери прямо впливає на здатність підприємства протистояти внутрішнім і зовнішнім викликам.

У сучасних підходах до оцінювання економічної безпеки все частіше підкреслюється важливість нематеріальних активів, зокрема людського капіталу, адаптивності трудових ресурсів до змін середовища, стабільності

команди та інституційної пам'яті. Аналіз цієї групи показників дозволяє оцінити вразливість підприємства до внутрішніх кадрових ризиків, таких як висока текучість кадрів, втрата ключових спеціалістів, незадоволення працівників умовами праці, конфліктність або низька мотивація.

Таблиця 2.2

Перелік основних показників фінансової підсистеми економічної безпеки підприємства.

| Показник                                            | Алгоритм розрахунку                                          | Економічна сутність показника                                                                                                                              |
|-----------------------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Коефіцієнт автономії                                | Власний капітал /<br>Загальна сума<br>фінансування           | Відображає ступінь фінансової незалежності підприємства від зовнішніх джерел фінансування. Чим вищий показник – тим менший ризик втрати платоспроможності. |
| Коефіцієнт фінансування                             | Залучені кошти /<br>Власний капітал                          | Характеризує структуру капіталу підприємства, зокрема, ступінь залежності від позикових коштів. Підвищене значення свідчить про фінансову вразливість.     |
| Коефіцієнт покриття                                 | Оборотні активи /<br>Поточні зобов'язання                    | Оцінює здатність підприємства покривати поточні зобов'язання за рахунок мобільних активів. Свідчить про платоспроможність у короткостроковій перспективі.  |
| Коефіцієнт оборотності дебіторської заборгованості  | Чиста виручка /<br>Середньорічна дебіторська заборгованість  | Показує, наскільки швидко підприємство отримує кошти за надані товари/послуги. Високе значення свідчить про ефективне управління дебіторами.               |
| Коефіцієнт оборотності кредиторської заборгованості | Чиста виручка /<br>Середньорічна кредиторська заборгованість | Характеризує швидкість погашення зобов'язань перед постачальниками. Показник впливає на репутацію та фінансову стійкість підприємства.                     |
| Коефіцієнт рентабельності діяльності                | Валовий прибуток /<br>Собівартість реалізованої продукції    | Визначає ефективність основної діяльності: скільки прибутку отримано з кожної гривні витрат.                                                               |

Джерело: складено автором на основі [202]

Низькі показники стабільності колективу та кваліфікації персоналу можуть бути індикаторами латентних загроз, які знижують адаптивність підприємства до викликів зовнішнього середовища. Водночас позитивна

динаміка витрат на навчання, зростання рівня задоволеності персоналу та зниження обороту кадрів можуть слугувати ознаками високого рівня кадрової безпеки. У табл. 2.3 наведено типовий перелік показників, які найчастіше використовуються для оцінювання кадрової підсистеми економічної безпеки підприємства.

Таблиця 2.3

Перелік основних показників кадрової підсистеми економічної безпеки підприємства.

| Показник                                  | Алгоритм розрахунку                                                         | Економічна сутність показника                                                                                                     |
|-------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Коефіцієнт плинності кадрів               | Кількість звільнених / Середньооблікова чисельність персоналу               | Відображає стабільність трудового колективу. Високе значення може свідчити про внутрішні проблеми або низьку мотивацію персоналу. |
| Продуктивність праці                      | Обсяг продукції / Обсяг витраченої праці                                    | Показує ефективність використання людських ресурсів.                                                                              |
| Коефіцієнт фондоозброєності праці         | Вартість основних фондів / Кількість працівників                            | Визначає рівень технічної оснащеності персоналу.                                                                                  |
| Коефіцієнт раціоналізаторської активності | Кількість раціоналізаторських пропозицій / Кількість працівників            | Відображає інноваційну активність персоналу, спрямовану на покращення процесів та результатів роботи.                             |
| Коефіцієнт кваліфікаційного рівня         | Кількість висококваліфікованих працівників / Загальна кількість працівників | Показує якісний рівень кадрового потенціалу підприємства.                                                                         |

Джерело: складено автором на основі [202]

Наступним важливим елементом у структурі оцінювання економічної безпеки є техніко-технологічна підсистема, яка відображає рівень забезпеченості підприємства технічними ресурсами, стан матеріально-технічної бази, ефективність використання обладнання, а також ступінь його оновленості. Ця складова особливо критична для підприємств реального сектору економіки, де виробничий процес тісно пов'язаний із фізичними активами, технологічними циклами та інноваційною інфраструктурою.

Порушення в техніко-технологічній сфері можуть мати кумулятивний негативний ефект, що проявляється у зниженні продуктивності, підвищенні собівартості, зростанні енергозатрат, частоті аварій чи простоїв. Високий ступінь зносу обладнання або неефективне використання виробничих потужностей можуть свідчити про критичний рівень технічної вразливості підприємства.

Оцінювання стану цієї підсистеми, як правило, здійснюється за допомогою таких ключових показників як коефіцієнт використання виробничої потужності, коефіцієнт зносу основних засобів, коефіцієнт фондівіддачі тощо. Аналіз зазначених показників дає змогу виявити як потенційні технологічні вузькі місця, так і точки зростання підприємства. Високі значення фондівіддачі та інтенсивності використання технічних ресурсів, у поєднанні з низьким рівнем зносу, свідчать про високий рівень технологічної стійкості. Натомість критично низький коефіцієнт використання виробничої потужності може свідчити про неефективне управління ресурсами або ризик втрати ринкових позицій. У табл. 2.4 представлено узагальнений перелік основних техніко-технологічних показників, що використовуються для оцінювання відповідної підсистеми економічної безпеки підприємства.

Попри наявність широкого спектра методик оцінювання економічної безпеки підприємства, значна частина з них ґрунтується на використанні статичних фінансово-економічних показників, які були актуальними в умовах стабільного середовища, але втрачають ефективність у сучасному цифровому контексті. Основним недоліком таких підходів є їхня орієнтація на ретроспективний аналіз, що не враховує динамічну природу змін, характерну для цифрової економіки. Зокрема, традиційні моделі не здатні відображати швидкоплинні технологічні зрушення, трансформацію бізнес-процесів, зростання ролі даних та підвищення уразливості до новітніх цифрових загроз.

Більшість класичних інструментів аналізу економічної безпеки зосереджуються на оцінці фінансового, виробничого чи кадрового стану підприємства в певний момент часу. Вони не дають змоги виявляти

довгострокові тренди, кризові сигнали або латентні ризики, які проявляються поступово і, як наслідок, такі підходи не є адаптивними до сучасних викликів, зокрема викликів цифрової трансформації.

Таблиця 2.4

Перелік основних показників техніко-технологічної підсистеми економічної безпеки підприємства.

| Показник                                        | Алгоритм розрахунку                                  | Економічна сутність показника                                                                                                      |
|-------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Коефіцієнт використання виробничої потужності   | Фонд робочого часу / Трудомісткість виробництва      | Показує рівень завантаження виробничих потужностей. Чим вищий показник – тим ефективніше використовується наявне обладнання.       |
| Коефіцієнт зносу основних засобів               | Сума зносу / Балансова вартість основних засобів     | Характеризує фізичну зношеність матеріально-технічної бази. Високі значення можуть свідчити про необхідність оновлення обладнання. |
| Коефіцієнт фондівіддачі                         | Обсяг виробництва / Середня вартість основних фондів | Відоображає ефективність використання основних фондів у виробничій діяльності.                                                     |
| Коефіцієнт інтенсивного використання обладнання | Обсяг продукції / Потужність обладнання              | Визначає реальний рівень використання наявних виробничих потужностей.                                                              |

Джерело: складено автором на основі [202]

Крім того, в існуючих моделях недостатньо враховано ризики, що виникають у цифровому середовищі, серед яких – збої IT-інфраструктури, витоки конфіденційної інформації, кіберзагрози, порушення регуляторних норм щодо обробки персональних або стратегічних даних. Як справедливо зазначають С. Шинкар та ін. [87], недостатня стандартизація підходів, відсутність погоджених вагових коефіцієнтів і критеріїв оцінки між галузями та підприємствами створюють суттєві бар'єри для аналітичної об'єктивності та порівнюваності результатів оцінювання.

Окрім цього, класичні методики практично ігнорують потенціал великих даних, машинного навчання та системного моніторингу в режимі реального часу, що суттєво знижує релевантність прийнятих управлінських рішень. У результаті підприємства не мають змоги оперативно виявляти й локалізувати

цифрові загрози, втрачають гнучкість в умовах швидкоплинного інформаційного середовища та не здатні формувати ефективні превентивні механізми безпеки.

Актуальним завданням сьогодення є розробка нових підходів до аналізу економічної безпеки, що враховували б актуальні загрози та зміни. Цифрова трансформація не лише змінює структуру підприємства, але й формує нові типи ризиків, які мають бути інтегровані в систему безпеки. Серед них – технологічні ризики (збої цифрових платформ), ризики конфіденційності (витоки даних), операційні ризики (недостатня автоматизація контрольних процедур), а також регуляторні ризики, що виникають унаслідок невідповідності вимогам цифрового законодавства [68].

У цьому контексті С. Ю. Хамініч [196] виокремлює п'ять ключових напрямів контролю економічної безпеки підприємства в умовах цифрової інфраструктури: оцінку цифрових ризиків, впровадження превентивних та реактивних стратегій протидії загрозам, аналіз фінансових показників у цифровому контексті, безперервний моніторинг індикаторів безпеки та математичне моделювання кризових сценаріїв. Дослідниця наголошує, що саме поєднання цих напрямів формує основу для адаптивної системи мінімізації загроз, здатної швидко реагувати як на планові зміни, так і на раптові цифрові кризи, що узгоджується з принципами проактивного управління, покладеними в основу пропонованого в цьому дослідженні методичного підходу.

Сучасні виклики цифрової трансформації вимагають комплексного переосмислення та переоснащення методології оцінювання економічної безпеки підприємства [112]. У нових умовах змінилися не лише джерела ризиків, а й самі принципи функціонування бізнесу, що вимагає інтеграції новітніх цифрових технологій в інструментарій аналітичної оцінки. Актуальним є створення інтелектуальних, гнучких і динамічних моделей, які дозволяють виявляти неочевидні загрози, прогнозувати розвиток критичних ситуацій і реагувати на них у режимі реального часу. У цьому контексті можна

виокремити чотири ключові напрями цифрового переоснащення системи економічної безпеки.

1. Впровадження алгоритмів аналітики великих даних та штучного інтелекту. Сучасне цифрове середовище генерує величезні обсяги різномірної інформації, яка може бути використана для побудови адаптивних моделей економічної безпеки. Алгоритми машинного навчання, методи інтелектуального аналізу даних, а також автоматизовані аналітичні системи на базі штучного інтелекту дозволяють не лише виявляти приховані закономірності у поведінці об'єктів аналізу, а й формувати прогностичні моделі на основі виявлених патернів. Це, в свою чергу, забезпечує високу точність оцінювання ризиків, ідентифікацію аномалій, виявлення вразливостей у внутрішніх процесах та прогнозування впливу зовнішніх факторів.

2. Вдосконалення систем кіберзахисту як ключового елемента економічної стабільності. В умовах зростання обсягу цифрових активів та інтеграції IT-рішень в операційні процеси підприємств кібербезпека стає центральною складовою економічної безпеки. Загрози, пов'язані з кібератаками, шкідливим програмним забезпеченням, витоками даних та порушенням доступу до інформаційних систем, безпосередньо впливають на операційну діяльність та фінансову стійкість підприємств. Згідно з результатами дослідження Microsoft, 62 % представників малого та середнього бізнесу вважають саме кіберзагрози головним викликом у процесі цифрової трансформації [102].

3. Постійний моніторинг системи економічної безпеки в режимі наближеному до реального часу. Традиційні підходи, які базуються на періодичному аналізі, не здатні забезпечити своєчасне реагування на раптові зміни в цифровому середовищі. Тому впровадження систем моніторингу в реальному часі є ключовим етапом побудови сучасної моделі економічної безпеки. Такі системи повинні забезпечувати оперативну фіксацію критичних подій, оцінку рівня вразливості та формування сценаріїв реагування.

4. Формування адаптивних стратегій управління ризиками. У цифровому середовищі ключовою перевагою є не стільки наявність захисних механізмів, скільки здатність системи швидко адаптуватися до нових типів загроз, що постійно еволюціонують. У цьому контексті виникає потреба у розробці гнучких, багаторівневих стратегій управління ризиками, які можуть бути масштабовані, трансформовані або переглянуті залежно від змін у зовнішньому середовищі. Як свідчать результати дослідження компанії KPMG, 60 % опитаних фахівців підтверджують необхідність оновлення методологій управління ризиками задля протидії новим цифровим загрозам [31].

Таким чином, застосування традиційних, статичних підходів без урахування факторів цифровізації, зростання даних, системної взаємозалежності загроз і об'єктивності оцінювання є методологічно застарілим та неадекватним сучасним викликам. У відповідь на це виникає необхідність розробки нових моделей, що ґрунтуються на принципах цифрової трансформації, використанні великих даних та алгоритмах системного аналізу. Все це передбачає необхідність побудови інтелектуальної системи моніторингу економічної безпеки, що забезпечуватиме як поточне оцінювання, так і превентивну ідентифікацію потенційних загроз з високим ступенем точності та адаптивності.

## **2.2. Методичні підходи до моделювання окремих складових системи економічної безпеки в умовах цифрової економіки**

Гарантування результативного функціонування системи економічної безпеки суб'єкта господарювання базується на засадах системного аналізу. Застосування системного підходу дозволяє інтерпретувати економічну безпеку не як дискретну сукупність заходів, а як інтегровану систему, що поєднує взаємозумовлені елементи, управлінські механізми, інструментарій оцінювання ризиків та засоби захисту ресурсного потенціалу підприємства.

Зазначений підхід сприяє поглибленому розумінню генези загроз та розробленню методів їхньої нейтралізації, а також врахуванню галузевої специфіки в парадигмі цифрової трансформації економіки.

Сучасне моделювання системи економічної безпеки передбачає ідентифікацію її базових функціональних складових, їх структурування та подальшу формалізацію у вигляді математичних, інформаційних або економетричних моделей. Кожен компонент відіграє специфічну роль у загальній безпековій архітектурі, що зумовлює необхідність проведення аналізу з урахуванням як внутрішніх бізнес-процесів, так і динаміки зовнішнього середовища.

У межах цього дослідження доцільно здійснити аналіз фундаментальних складових системи економічної безпеки крізь призму новітніх наукових концепцій щодо їх ідентифікації, вимірювання та менеджменту. Особливу увагу приділено ролі цифрових технологій, алгоритмів штучного інтелекту та інструментарію аналітики великих даних у процесі проектування адаптивних та предиктивних моделей, здатних до оперативного реагування на виклики та забезпечення резистентності підприємства за умов нестабільної ринкової кон'юнктури.

Фінансова безпека є однією з ключових складових системи економічної безпеки підприємства, оскільки вона безпосередньо пов'язана зі стійкістю фінансового стану, здатністю підприємства своєчасно виконувати свої зобов'язання та забезпечувати стабільність фінансових потоків. Порухи фінансової безпеки створює ризики ліквідності, неплатоспроможності, втрати платоспроможності та, в найгіршому випадку, банкрутства підприємства. Саме тому моделювання фінансової безпеки базується на глибокому аналізі фінансової звітності – балансу, звіту про фінансові результати, звіту про рух грошових коштів – з метою виявлення слабких місць, вразливостей і потенційних загроз.

Аналіз сучасних наукових досліджень свідчить про те, що ключовим напрямом моделювання фінансової безпеки є побудова прогнозних моделей,

які дозволяють оцінити ймовірність неспроможності підприємства продовжувати господарську діяльність. При цьому поняття «неспроможність» найчастіше ототожнюється з банкрутством, дефолтом або критичною неплатоспроможністю, хоча в літературі немає єдиного універсального визначення цієї події [98]. Деякі дослідники розглядають фінансові труднощі як цільову змінну, що підлягає моделюванню в рамках системи економічної безпеки підприємства.

Починаючи з класичного емпіричного дослідження Е. Альтмана [9], прогнозування банкрутства підприємств розглядається як задача бінарної класифікації, де компанії поділяються на дві категорії: ті, що збанкрутували, і ті, що продовжують свою діяльність. Такий підхід забезпечує формалізований критерій, який дозволяє застосовувати методи машинного навчання або статистичного аналізу для побудови моделей, що передбачають фінансову неспроможність. З цієї точки зору банкрутство є найбільш обґрунтованим та об'єктивно вимірюваним індикатором втрати фінансової безпеки, придатним для емпіричного моделювання.

Сучасні підходи до оцінки фінансової безпеки підприємства дедалі частіше ґрунтуються на методах моделювання та прогнозування. Ці методи дозволяють не лише виявляти ймовірність настання кризових явищ, а й формувати системи раннього попередження та надання рекомендацій щодо мінімізації ризиків. Їхня ефективність значно зросла завдяки розвитку цифрових технологій, зокрема аналітики великих даних та інструментів штучного інтелекту, що забезпечили доступ до масивів інформації та потужностей для її оперативного оброблення.

Загалом можна виокремити дві основні групи методів у межах цього підходу: моделі прогнозування банкрутства та моделі фінансового раннього попередження [19]. Перший підхід передбачає оцінку ймовірності банкрутства підприємства на основі історичних фінансових даних. Більшість таких методик були розроблені в умовах стабільних ринкових економік, де існувала усталена інституціоналізована процедура банкрутства [56]. Протягом останніх

десятиліть було запропоновано численні класифікаційні моделі прогнозування фінансових ризиків, які можна згрупувати в кілька категорій

- класичні статистичні моделі (дискримінантний аналіз, логістична регресія);
- методи штучного інтелекту (нейронні мережі, дерева рішень тощо)
- використання інших методів (case-based reasoning, fuzzy modeling) [77].

Зі вступом у добу економіки знань моделі фінансового раннього попередження набули широкого поширення, особливо у сфері електронної комерції. Їх головна мета – не лише передбачення негативних фінансових сценаріїв, а й своєчасне виявлення сигналів потенційної кризи. Побудова ефективної системи раннього фінансового попередження дозволяє оперативно діагностувати загрозу та вжити запобіжних заходів до її реалізації. Особливо перспективним напрямом у цьому контексті є використання глибокого навчання, яке дозволяє враховувати нелінійні залежності між фінансовими та нефінансовими показниками, тим самим підвищуючи точність моделювання [22]. Зростаюча складність фінансових процесів зумовлює активне впровадження методів машинного навчання та штучного інтелекту для підвищення точності моделей прогнозування. Міжнародна наукова спільнота демонструє значний інтерес до вдосконалення таких підходів.

У дослідженні М. Хамді та інші [43] здійснено порівняння ефективності п'яти моделей – лінійного дискримінантного аналізу, логістичної регресії, дерев рішень, методу опорних векторів (SVM) та Random forest – для прогнозування банкрутства туніських компаній. Крім того, застосовано модель нейронної мережі, яка продемонструвала найвищу точність порівняно з іншими моделями, у той час як модель Random forest виявилася найефективнішою серед класичних методів машинного навчання.

У логічному продовженні цього підходу, Т. Новіанторо та Й. Нуанг [75] застосували як машинне, так і глибинне навчання для прогнозування банкрутства тайванських компаній за період 1999–2009 років. Результати

дослідження виявили, що модель Random forest перевершує інші методи за точністю, F-score та AUC, а другим за ефективністю виявився підхід глибокого навчання.

У свою чергу, Шетту та інші [85] проаналізували 3728 бельгійських компаній, застосувавши глибокі нейронні мережі, метод XGBoost та метод опорних векторів. Всі методи продемонстрували приблизно однакову точність прогнозування банкрутства на рівні 82–83%, що свідчить про високий рівень узгодженості результатів при застосуванні різних технік.

Істотно інноваційний підхід запропонували Б. Самі та В. Серрет [14], які розробили модель Fuzzy Convolutional Neural Networks для прогнозування фінансової неспроможності. Результати дослідження свідчать про перевагу даної моделі над традиційними та класичними методами машинного навчання за низкою метрик, зокрема за чутливістю, точністю та AUC.

Розширення горизонту прогнозування продемонстрував Т. Корол [59], який створив динамічні моделі для оцінки ймовірності банкрутства європейських компаній з використанням методів нечітких множин, нейронних мереж, а також дерев рішень. Дослідження підтвердило переваги динамічних моделей над статичними та високу ефективність нечітких множин, особливо на довгостроковому прогнозному горизонті.

У контексті країн з нестабільною економічною ситуацією цікаве дослідження Ю. Акер та А. Каравардар [6], де було здійснено прогнозування банкрутства турецьких малих та середніх підприємств у 2015–2019 роках. Найвищу точність за один та два роки до фінансової неспроможності продемонструвала модель дерева рішень, а за три роки - наївний баєсівський класифікатор. Отримані результати також вказують на ключові фінансові чинники ризику, зокрема надмірне кредитування та зниження капіталу.

На прикладі підприємств хімічної промисловості Словаччини у дослідженні С. Летковскі та інших [64] було порівняно класичні статистичні та AI-методи, зокрема логістичну регресію, штучні нейронні мережі, методи опорних векторів та дерева рішень. Попри різноманіття використаних

підходів, усі моделі продемонстрували подібні результати, що, ймовірно, зумовлено якістю вхідних даних.

Окремої уваги заслуговує дослідження Г. Ан та інші [5], у якому було вдосконалено метод Case-Based Reasoning шляхом одночасної оптимізації ваг ознак і відбору прикладів з використанням генетичних алгоритмів. Запропонована модель забезпечує підвищення точності прогнозування, зберігаючи здатність до пояснення результатів, що є особливо важливим для банківських установ і фінансових аналітиків.

У дослідженні Р. Ангелова та Д. Стоянчева [10] проаналізовано вплив цифровізації на ефективність діяльності та ризик банкрутства сільськогосподарських підприємств Болгарії. На основі даних середніх і великих аграрних підприємств за п'ятирічний період авторки оцінили застосовність класичних моделей прогнозування банкрутства в галузевому контексті. За допомогою моделей фіксованих ефектів і пробіт-моделі встановлено, що підприємства з нижчою продуктивністю та вищим фінансовим навантаженням мають підвищену ймовірність банкрутства, тоді як вищий рівень цифровізації асоціюється зі зменшенням ризику фінансової неспроможності.

Узагальнений аналіз сучасних наукових праць щодо прогнозування банкрутства підприємств та їх результати наведено в табл. 2.5. На основі проведеного дослідження було визначено, що подальша побудова моделі прогнозування буде здійснюватися із використанням п'яти алгоритмів логістична регресія, SVM, нейронна мережа, RandomForest та XGBoost, оскільки:

- це дозволяє здійснити ґрунтовне порівняння ефективності різних підходів до прогнозування;
- обрані методи добре масштабуються для роботи з великими обсягами фінансових даних;
- виявлені моделі демонструють найвищу точність серед усіх досліджених у сучасній літературі;

Таблиці 2.5

## Порівняння досліджень прогнозування банкрутства з використанням сучасних методів машинного навчання

| Робота                                 | Використані моделі                                                                                                                            | Використані дані                                                            | Метрики для оцінки якості                | Короткі результати                                                                              |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------|
| М. Хамді та інші, 2024 [43]            | Методи лінійного дискримінантного аналізу, логістична регресія, дерева рішень, SVM та Random forest                                           | Туніс, 2011–2017, 25 фінансових індикаторів                                 | Accuracy, F1 score, AUC                  | RF краща за інші ML та статистичні моделі                                                       |
| Т. Новіанторо та Й. Нуанг, 2021 [75]   | Дерево рішень, випадковий ліс, алгоритм k найближчих сусідів, SVM, штучна нейронна мережа, наївний байєсівський алгоритм, логістична регресія | Тайвань, 1999–2009, 96 фінансових індикаторів                               | Accuracy, F1 score, AUC                  | RF найкраща за всіма метриками, нейронна мережа - на другому місці.                             |
| Шетту та інші, 2022 [85]               | Нейронна мережа, XGBoost, SVM                                                                                                                 | Бельгія, 2002–2012, 3 фінансових коефіцієнти                                | Precision, Recall, F1 score              | Всі моделі показали подібну точність (82–83%)                                                   |
| Б. Самі та В. Серрет, 2023 [14]        | Нечіткі згорткові нейронні мережі (FCNN)                                                                                                      | Франція, 2014–2017, 17 фінансових індикаторів                               | Sensitivity, AUC, ROC, F score, Accuracy | FCNN перевершує традиційні та ML моделі                                                         |
| Т. Корол, 2019 [59]                    | Нечіткі множини, багатошарова штучна нейронна мережа та дерева рішень                                                                         | ЄС, 2004-2017, 20 індикаторів                                               | Accuracy                                 | Fuzzy sets найкращі, динамічні моделі стабільніші за статичні                                   |
| Ю. Акер та А. Каравардар, 2023 [6]     | Логістична регресія, дерево рішень, випадковий ліс, SVM, метод k-найближчих сусідів та наївна байєсівська модель                              | Туреччина, 2015–2019, 8–9 фінансових індикаторів                            | Accuracy                                 | DT найкраща за 1-2 роки, Naive Bayes - за 3 роки                                                |
| С. Летковські та інші, 2024 [64]       | Логістична регресія, штучні нейронні мережі, SVM та дерева рішень                                                                             | Словаччина, 2019–2021, 11 індикаторів                                       | Accuracy, Recall, F1 score               | Усі моделі показали схожі результати                                                            |
| Г. Ан та інші, 2009 [5]                | Метод міркування на основі прецедентів з використанням генетичних алгоритмів                                                                  | Korea, 1996-2000                                                            | Accuracy                                 | Оптимізована CBR значно краща за звичайну                                                       |
| Р. Ангелова та Д. Стоянчева, 2023 [10] | Моделі з фіксованими ефектами, пробіт-модель                                                                                                  | Болгарія, 2017-2021, 3 фінансові індикатори і один індикатор діджиталізації | Accuracy                                 | Нижча продуктивність та нижчий рівень цифровізації призводить до вищої ймовірності банкрутства. |

– вони охоплюють як традиційні статистичні методи, так і сучасні алгоритми машинного та глибокого навчання, що забезпечує широту підходу й гнучкість адаптації моделі до різних економічних умов.

Кожен з цих підходів має специфічні переваги, математичну структуру та гіперпараметри, які дозволяють адаптувати модель до особливостей фінансових даних підприємств. Нижче подано розгорнутий опис кожного з методів.

1. Логістична регресія є класичним статистичним методом бінарної класифікації, який використовується для оцінки ймовірності настання певної події – у даному випадку, банкрутства підприємства. Її основна перевага полягає у простоті реалізації та високій інтерпретованості результатів: кожен коефіцієнт моделі має чітке економічне трактування, що дає змогу зрозуміти ступінь впливу відповідного фінансового показника на ризик банкрутства.

З математичної точки зору, модель описується логістичною функцією, що перетворює лінійну комбінацію незалежних змінних на ймовірність події:

$$P(y = 1 | X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \dots + \beta_n x_n)}}$$

де:

$P(y = 1 | X)$  – ймовірність банкрутства;

$x_i$  – змінні моделі, зазвичай фінансові індикатори;

$\beta_i$  – коефіцієнти моделі;

Однією з ключових особливостей моделі є чутливість до мультиколінеарності та масштабування змінних, що потребує попередньої обробки даних.

2. Метод опорних векторів (SVM) є одним з найбільш потужних інструментів для класифікації у випадках, коли дані мають складну структуру, високу вимірність або не є лінійно роздільними. У контексті прогнозування банкрутства, SVM дозволяє побудувати оптимальну гіперплощину, яка максимально відокремлює підприємства-банкрути від фінансово стійких підприємств, використовуючи для цього лише найбільш інформативні

спостереження. Особливо цінним є застосування ядрових функцій, які дозволяють здійснювати нелінійне перетворення простору ознак без втрати важливої інформації. Математична модель цього методу може бути представлена у наступному вигляді:

$$f(x) = \text{sign} \left( \sum_{i=1}^n \alpha_i y_i K(x_i, x) + b \right)$$

$$K(x_i, x_j) = \exp(-\gamma \|x_i - x_j\|^2)$$

де:

$x_i, x_j$  – вектори ознак;

$\gamma > 0$  – параметр, що визначає радіус впливу опорного вектора

$\alpha_i$  – множники Лагранжа;

3. Штучна нейронна мережа імітує структуру та функціонування біологічного мозку, що дозволяє їм ефективно моделювати складні та нелінійні залежності між вхідними фінансовими параметрами та ймовірністю банкрутства. У задачах фінансової безпеки це особливо важливо, оскільки значна частина закономірностей є прихованою та неочевидною для традиційних моделей. У загальному вигляді нейронна мережа складається з трьох типів шарів: вхідного, одного або декількох прихованих та вихідного. Кожен нейрон обчислює зважену суму входів, додає зміщення і передає результат через активаційну функцію. Математичну модель для одного шару можна описати наступною рівністю:

$$a^{(1)} = f \left( \sum_{i=1}^n (w_i x_i + b) \right)$$

де:

$a^{(1)}$  – вихід нейрона;

$f$  – активаційна функція;

$w_i$  – ваги;

$x_i$  – вхідні змінні.

Хоча нейронні мережі вимагають більших обчислювальних ресурсів і є менш прозорою в інтерпретації, вони демонструють високу точність, особливо в умовах наявності великих наборів даних з багатьма ознаками.

4. Random Forest (випадковий ліс) є ансамблевим методом, який поєднує велику кількість незалежних дерев рішень для отримання остаточного прогнозу шляхом більшості голосів. Такий підхід дозволяє зменшити дисперсію та уникнути перенавчання, що є типовими проблемами для окремих дерев рішень. Використання методу Random Forest у прогнозуванні банкрутства дає змогу отримати стабільні й достовірні результати навіть у випадках, коли вихідні фінансові дані є шумними, містять пропущені значення або мають складну структуру. Цей метод можна описати наступною функцією:

$$\hat{y} = \text{mode}(h_1(x), h_2(x), \dots, h_k(x))$$

де:

$h_i(x)$  – окреме дерево класифікації

$\hat{y}$  – прогноз банкрутства.

Основними параметрами, які підлягають налаштуванню, є кількість дерев (*n\_estimators*), максимальна глибина дерев (*max\_depth*) та мінімальна кількість зразків для поділу вузла (*min\_samples\_split*).

5. XGBoost є одним з найсучасніших і найефективніших алгоритмів, що базуються на градієнтному бустингу дерев рішень. Його особливістю є послідовне побудування дерев, де кожне наступне дерево спрямоване на зменшення помилок попередніх. У задачах прогнозування банкрутства XGBoost забезпечує високу точність, особливо при роботі з великою кількістю змінних і значними обсягами даних. Математична модель цього методу має наступний вигляд:

$$\hat{y}_i = \sum_{k=1}^K f_k(x_i), f_k \in \mathcal{F}$$

де:

$\hat{y}_i$  – прогноз для об'єкта *i*,

$f_k$  – функція, що відповідає *k*-му дереву

$\mathcal{F}$  – простір можливих дерев рішень з обмеженою глибиною.

Цільовою функцією оптимізації в цьому випадку буде мати наступний вигляд:

$$\mathcal{L}(\phi) = \sum_{i=1}^n l(y_i, \hat{y}_i) + \sum_{k=1}^K \Omega(f_k)$$

де:

$l(y_i, \hat{y}_i)$  – функція втрат (наприклад, логістична втрата для класифікації),

$\Omega(f) = \gamma T + \frac{1}{2} \lambda \|w\|^2$  – регуляризаційний член, який карає за складність моделі,

$T$  – кількість листків у дереві,

$w$  – ваги в листках,

$\gamma, \lambda$  – параметри регуляризації.

Кожне нове дерево  $f_k$  будується таким чином, щоб мінімізувати залишкову помилку попередніх моделей на основі градієнта втрат. Це забезпечує поступове вдосконалення загального прогнозу. Алгоритм дозволяє гнучко налаштовувати велику кількість параметрів, зокрема кількість дерев ( $n\_estimators$ ), швидкість навчання ( $learning\_rate$ ), глибину дерев ( $max\_depth$ ), а також регуляризаційні коефіцієнти ( $lambda, alpha$ ), які контролюють складність моделі.

Підсумовуючи, варто зазначити, що на сьогодні не існує універсального методу прогнозування банкрутства, який би був оптимальним за всіх умов. Кожен алгоритм має свої сильні сторони та обмеження, які зумовлені характером і структурою вхідних фінансових даних, галузевими особливостями, рівнем доступності інформації, а також метою аналізу. Отже, вибір методології моделювання фінансової безпеки підприємства має базуватися на комплексному врахуванні як характеристик даних, так і вимог до моделі – з погляду точності, інтерпретованості та обчислювальної ефективності [110].

Разом з тим, аналіз сучасної літератури дозволяє зробити важливе спостереження: переважна більшість досліджень фокусується на оптимізації точності моделей без урахування трансформаційних процесів, пов'язаних із цифровізацією економіки. Практично відсутні роботи, які б інтегрували цифрові чинники в структуру моделей прогнозування банкрутства. Це створює значну наукову прогалину, адже цифрові індикатори можуть суттєво впливати на фінансову стабільність підприємства. Відтак, обґрунтування необхідності розробки моделей, адаптованих до умов цифрової економіки, стає ключовим напрямом подальшого дослідження.

Узагальнюючи результати досліджень у сфері фінансової безпеки, стає очевидним, що цифровізація справляє суттєвий вплив не лише на фінансову стійкість підприємств, але й на інші ключові підсистеми загальної економічної безпеки. Однією з таких критично важливих складових є кадрова безпека, яка в умовах цифрової трансформації набуває нових ризиків, викликів та вимог до управління.

У класичному розумінні кадрова безпека розглядається як сукупність заходів, спрямованих на забезпечення стабільності кадрового потенціалу, належного кваліфікаційного рівня персоналу, ефективної мотивації працівників та запобігання внутрішнім загрозам. Проте стрімкий розвиток цифрових технологій зумовлює необхідність перегляду підходів до оцінювання й прогнозування стану цієї підсистеми. Зокрема, актуальності набуває застосування сучасних методів моделювання – від бальних оцінок рівня мотивованості до ієрархічних моделей, що базуються на методах нечіткої логіки. Такі підходи дають змогу аналізувати вплив змін у системі мотивації, навчання та управління персоналом на ймовірність виникнення трудових ризиків, а також визначати зони найбільшої вразливості.

Крім традиційних напрямів забезпечення кадрової безпеки, в умовах цифрової економіки особливу загрозу становлять інсайдерські ризики, пов'язані з витоком конфіденційної інформації, маніпуляціями з внутрішніми даними або навмисним порушенням цілісності інформаційних систем. Попри

наявність широкого спектру програмного забезпечення, що забезпечує базовий рівень захисту від зовнішнього втручання, саме внутрішні загрози (від співробітників або осіб з доступом до критичних систем) є найскладнішими для виявлення та нейтралізації. У сучасній науковій літературі спостерігається зміщення фокусу з питань загального функціонування кадрових систем у бік розробки інструментів превентивної аналітики, які дозволяють ідентифікувати потенційно небезпечну поведінку ще до настання критичних наслідків.

У цьому контексті особливу увагу привертає застосування методів інтелектуального аналізу даних для побудови адаптивних систем управління кадровими ризиками. Такі системи аналізують широкі масиви цифрових слідів працівників (наприклад, активність у внутрішніх мережах, доступ до інформаційних ресурсів, зміни в шаблонах поведінки), що дозволяє з високою точністю виявляти ознаки потенційних інсайдерських загроз. Відтак, цифрова трансформація не лише створює нові ризики у сфері кадрової безпеки, а й відкриває нові можливості для їх проактивного управління.

Системи виявлення загроз, що функціонують на основі виявлення аномалій, формують статистичні моделі типового використання ІТ-ресурсів працівниками. Відхилення від усталених патернів сигналізують про потенційні кадрові загрози. Так, М. Раїссі-Дехкорді та співавт. [80] запропонували мультиперспективну модель виявлення інсайдерських загроз, яка інтегрує дані з різних компонентів корпоративної мережі. У межах цієї архітектури використовується алгоритм однокласового SVM, що дозволяє зменшити кількість хибних спрацьовувань та покращити точність виявлення ризикованої поведінки з боку персоналу. В той час як такий підхід демонструє високу точність для колективних атак, можливість точного прогнозування індивідуальних інсайдерських ризиків залишається обмеженою.

Альтернативний підхід запропонували Т. Рашід та інші [82], використавши приховані марковські моделі для моделювання звичної поведінки працівників. Цей метод добре адаптований до аналізу часових рядів,

однак характеризується високою обчислювальною складністю при збільшенні розміру моделі.

У свою чергу, Ю. Сонг та співавт. [91] застосували моделі змішаних Гаусовських розподілів для побудови профілів користувачів і виявлення аномалій. Попри високу точність, підхід орієнтований переважно на біометричну ідентифікацію, а не на безпосередню діагностику інсайдерських загроз у корпоративному середовищі.

У дослідженні Г. Гаваї та інші [41] запропоновано модель виявлення інсайдерських загроз на основі аналізу поведінкових цифрових слідів працівників. Було сформовано 42 ознаки у п'яти категоріях: використання та зміст електронної пошти, логіни, програмна та веб-активність. Для виявлення відхилень від нормальної поведінки застосовано алгоритм Isolation Forest та Random forest. Модель дозволяє автоматизовано ідентифікувати співробітників із підвищеним ризиком через інтерактивну панель візуалізації, що сприяє прийняттю превентивних рішень у сфері кадрової безпеки. Основними перевагами є простота, динамічність та об'єктивність аналізу, однак відзначено нестабільність при великій кількості працівників, що потребує додаткового налаштування.

У роботі Д. С. Ле та Н. Зінджир-Хейвуд [62] запропоновано підхід до виявлення інсайдерських загроз на основі ансамблів алгоритмів неконтрольованого навчання, зокрема таких моделей, як Isolation Forest, Autoencoder, Local Outlier Factor (LOF) та Lightweight Online Detector of Anomalies (LODA). Найкращі результати отримано при використанні Autoencoder та LOF. Крім того, виявлено, що ансамблеве голосування моделей покращує точність та робастність системи.

Т. Аль-Шехарі та співавт. [8] запропонували підхід до виявлення інсайдерських загроз з використанням алгоритму Density-Based Local Outlier Factor, адаптованого для роботи з дисбалансованими даними CERT R4.2. На відміну від традиційних методів, DBLOF аналізує локальну густину, що дозволяє точно виявляти рідкісні, але небезпечні поведінкові аномалії. Метод

показав високі результати точності, ефективно ідентифікуючи потенційні загрози в умовах реального корпоративного середовища.

У роботі С. Сонг та інші [90] запропоновано Audit-LLM – мультиагентну систему виявлення інсайдерських загроз на основі журналів подій, яка використовує великі мовні моделі (LLM) для аналізу складних логів користувацької активності. Щоб подолати обмеження LLM, система інтегрує три агенти: Decomposer, Tool Builder та Executor, а також механізм багатоагентних дебатов для підвищення точності висновків. Високі результати точності виявлення інсайдерів підтверджують перевагу запропонованого підходу над існуючими рішеннями, зокрема в аспекті обґрунтованості пояснень та роботи з великими лог-файлами.

Аналіз сучасних досліджень у сфері виявлення інсайдерських загроз (табл. 2.6) свідчить, що серед різноманіття методів аномального аналізу найчастіше застосовуються алгоритми Isolation Forest та Local Outlier Factor (LOF). Ці моделі не лише продемонстрували високу ефективність у реальних умовах (зокрема на CERT-датасетах), але й мають добру здатність до узагальнення результатів за умов обмеженості або відсутності маркованих даних. З огляду на їхню поширеність, аналітичну гнучкість та обґрунтовану ефективність, саме ці два підходи обрано для подальшого моделювання системи кадрової безпеки в умовах цифрової трансформації підприємства.

Розглянемо математичні основи кожного з методів, починаючи з LOF. Алгоритм LOF ґрунтується на концепції локальної густини: замість порівняння кожного об'єкта із загальною сукупністю, як це відбувається у глобальних моделях, LOF порівнює об'єкт лише з його найближчим локальним оточенням. Основна ідея полягає в тому, що аномальна точка матиме суттєво нижчу густину, ніж її сусіди, тобто перебуватиме у «розрідженому» регіоні простору ознак. Математично алгоритм LOF реалізується через кілька послідовних етапів. Першим етапом є обчислення відстані до  $k$ -го найближчого сусіда:

$$k\text{-distance}(p) = \text{відстань до } k\text{-го найближчого сусіда точки } p$$

Порівняння досліджень виявлення інсайдерських ризиків з використанням сучасних методів машинного навчання

| Автор                                     | Використані моделі                       | Дані                                    | Короткі результати                                                                          |
|-------------------------------------------|------------------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------|
| М. Раїссі-Дехкорді та співавт., 2011 [80] | One-Class SVM                            | Симульовані данні з використанням OPNET | Висока точність для колективних атак, але середня точність для індивідуальних.              |
| Т. Рашід та інші, 2016 [82]               | Hidden Markov Models                     | CERT                                    | Проста у навчанні модель, але обчислювально складна при великій кількості параметрів        |
| Ю. Сонг та співавт., 2013 [91]            | Gaussian Mixture Models                  | Дані RUU дослідження                    | Висока точність, але з орієнтацією на біометричні показники.                                |
| Г. Гаваї та інші, 2015 [41]               | Isolation Forest, Random forests         | Vegas                                   | Isolation Forest показав найкраще результати                                                |
| Д. С. Ле та Н. Зінджир-Хейвуд, 2021 [62]  | Isolation Forest, Autoencoder, LOF, LODA | CERT R4.2, R6.2                         | Autoencoder та LOF показують найвищу точність.                                              |
| Т. Аль-Шехарі та співавт., 2024 [8]       | Density-Based Local Outlier Factor (LOF) | CERT R4.2                               | Висока точність моделі LOF для незбалансованих наборів даних, але низька інтерпретованість. |
| С. Сонг та інші, 2024 [90]                | LLM-based multi-agent system             | CERT R4.2, R5.2, PicoDomain             | Висока точність моделі та покращена обґрунтованість, але є обмеження масштабованості.       |

Цей параметр визначає радіус локального простору навколо об'єкта  $p$ , в якому здійснюється аналіз. Після цього відбувається оцінка досяжної відстані, яка запобігає появі занадто малих значень густини, зумовлених наявністю дуже близьких точок:

$$reach\_dist_k(p, o) = \max \{k\text{-distance}(o), dist(p, o)\}$$

Після цього проводиться оцінка локальної густини  $lrd$ :

$$lrd_k(p) = \left( \frac{\sum_{o \in N_k(p)} reach\_dist_k(p, o)}{|N_k(p)|} \right)^{-1}$$

Цей показник визначає, наскільки "щільно" точка  $p$  оточена своїми  $k$ -найближчими сусідами. І на останньому етапі відбувається розрахунок коефіцієнта  $LOF$ :

$$LOF_k(p) = \frac{\sum_{o \in N_k(p)} \frac{lrd_k(o)}{lrd_k(p)}}{|N_k(p)|}$$

Саме  $LOF$  визначає відношення середньої локальної густини сусідів до густини точки  $ppp$ . Якщо  $LOF_k(p) \approx 1$ , поведінка точки є нормальною; якщо  $LOF_k(p) \gg 1$ , точка є аномальною, тобто її густина значно менша, ніж у її оточення.

Іншим сучасним алгоритмом для виявлення аномалій є метод ізоляційних лісів (Isolation Forest, IForest). На відміну від більшості методів, які моделюють нормальну поведінку, Isolation Forest побудований на механізмі ізоляції. Ідея полягає в тому, що аномальні об'єкти розташовані далі від інших точок і тому потребують менше кроків для ізоляції при випадковому поділі простору. Модель Isolation Forest складається з ансамблю ізоляційних дерев. Кожне дерево створюється шляхом випадкового вибору ознаки та довільного значення розділу, за яким простір даних рекурсивно поділяється. Такий процес продовжується доти, поки об'єкт не буде повністю ізолюваний в окремому листі дерева. Глибина вузла, в якому ізолюється об'єкт, відображає легкість або складність його відокремлення.

Загальна схема цього алгоритму може бути описана наступним чином: у ізоляційному лісі ми можемо створити деревоподібну структуру, яка може ефективно ізолювати кожен окремий екземпляр (рис. 2.1). Завдяки якості чутливості до ізоляції, викиди виділяються ближче до кореня дерева, тоді як стандартні точки, як правило, виділяються на кінцях дерева. Принцип ізоляції тих, що залишились, допомагає розвивати цей метод, а сформована структура дерева називається деревом ізоляції або  $iTree$ . Ізоляційний ліс створює ансамбль  $iTrees$  для заданого набору даних, де аномаліями є ті екземпляри, які мають коротку середню довжину шляху на  $iTree$ .

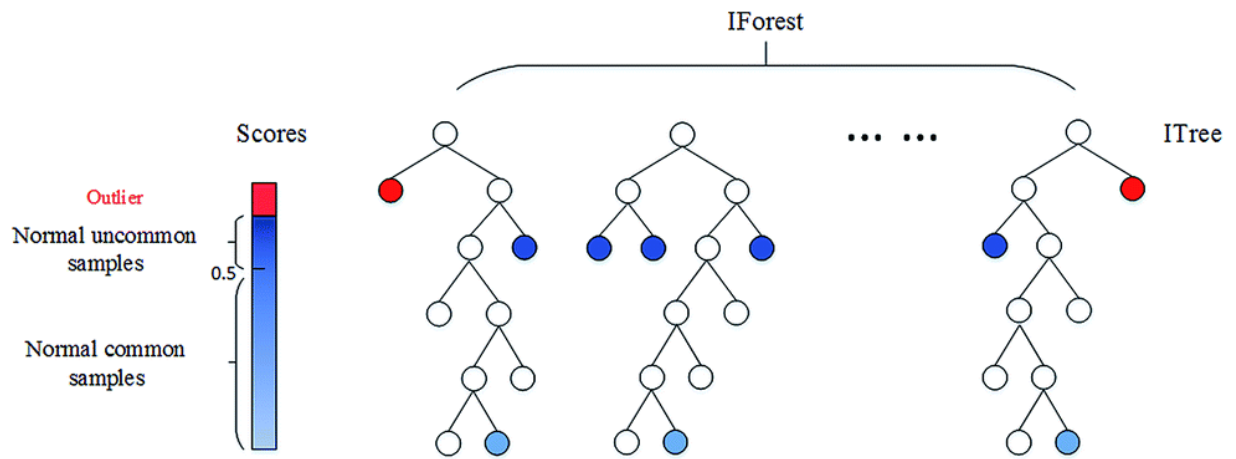


Рис. 2.1 Загальна схема алгоритму iForest.

Джерело: [24]

Математичну формалізацію цього алгоритму можна подати наступним чином. На першому етапі визначається очікувана довжина шляху ізоляції для точки  $x$  у дереві з  $n$  спостереженнями:

$$E[h(x)] \approx \log_2(n) + \gamma$$

де

$h(x)$  – довжина шляху до ізоляції точки  $x$ ,

$\gamma$  – константа для корекції (наближено 0.577 – стала Ейлера-Маскероні).

Після чого відбувається визначення коефіцієнта аномальності:

$$s(x, n) = 2^{-\frac{E[h(x)]}{c(n)}}$$

де  $c(n)$  – середня довжина шляху, яка у випадку для бінарного дерева може бути визначена наступним чином:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n}$$

а  $H(i)$  –  $i$ -те гармонійне число.

Інтерпретація результатів, отриманих за допомогою алгоритму Isolation Forest, ґрунтується на величині коефіцієнта аномальності  $s(x)$ , що набуває значень у межах від 0 до 1. Значення, близькі до одиниці  $s(x) \rightarrow 1$ , вказують на високу ймовірність того, що спостереження є аномальним, тобто поведінка відповідного об'єкта значно відрізняється від типової для решти вибірки.

Навпаки, значення  $s(x) < 0.5$  свідчать про «нормальність» поведінки, притаманної загальній множині спостережень. Значення, близькі до 0.5, потребують додаткового аналізу, оскільки можуть вказувати на пограничні або потенційно ризиковані випадки, які ще не перейшли в активну фазу порушень.

Узагальнюючи результати огляду, слід відзначити, що найбільш поширеними та ефективними підходами до виявлення інсайдерських загроз у системах кадрової безпеки є застосування алгоритмів Isolation Forest та Local Outlier Factor. Їх успішне використання базується на обробці поведінкових даних, отриманих з корпоративної мережі, зокрема журналів подій, логів доступу, активності в системах тощо. Ці алгоритми продемонстрували високу результативність у виявленні аномальної поведінки працівників, що потенційно може свідчити про внутрішні загрози безпеці підприємства.

Водночас, значна частина сучасних досліджень зосереджується переважно на оптимізації точності моделей, нехтуючи прикладними аспектами впровадження таких рішень у реальних умовах функціонування організацій. Зокрема, недостатньо розкритими залишаються питання адаптації моделей до змін середовища, масштабованості рішень та їх інтеграції в існуючу ІТ-інфраструктуру підприємств. Крім того, лише обмежене коло праць розглядає потенціал використання новітніх технологій, зокрема великих мовних моделей (LLM), які можуть істотно покращити масштабованість, швидкість обробки та інтерпретованість результатів у задачах виявлення загроз. З огляду на це, подальше дослідження буде зосереджене на поєднанні алгоритмів Isolation Forest і LOF із підходами, що базуються на LLM, з метою розробки сучасної, адаптивної, високоточної та масштабованої системи виявлення інсайдерських загроз, що буде орієнтована не лише на академічні метрики, а й на практичну придатність до впровадження в умовах реального підприємства.

За умов інтенсивної дифузії цифрових технологій та зростання рівня автоматизації операційних циклів техніко-технологічна підсистема економічної безпеки суб'єкта господарювання зазнає суттєвих структурно-функціональних трансформацій. Зазначена компонента детермінує

спроможність підприємства підтримувати стійкість виробничих процесів, забезпечуючи водночас технологічну надійність, нарощення інноваційного потенціалу та захищеність архітектури цифрової інфраструктури. У процесі цифровізації на техніко-технологічну підсистему чинять вплив як позитивні ефекти – підвищення ефективності, зниження витрат, прискорення виробничих циклів – так і нові загрози, пов'язані із цифровими ризиками. Серед основних джерел новітніх загроз можна виокремити індустріальний Інтернет речей, віддалене адміністрування та доступ до виробничих систем, використання цифрових двійників, кіберфізичні системи, а також інтеграцію розподілених сенсорних мереж. Такі рішення розширюють цифрову поверхню атаки та ускладнюють контроль над внутрішньовиробничими ризиками. У результаті цього виникає потреба в гнучких та адаптивних інструментах, здатних інтегрувати як кількісні, так і якісні характеристики, що мають високий рівень суб'єктивності та змінності.

Беручи до уваги значну диверсифікацію технологічного рівня підприємств, а також варіативність їхніх цифрових стратегій і ступеня ІТ-захисту, універсальні моделі оцінки техніко-технологічної безпеки є малоефективними або надто спрощеними. У такому контексті особливої актуальності набувають методи нечіткої логіки, які дозволяють ефективно опрацьовувати неструктуровані дані, експертні судження, а також невизначеність у значеннях показників. Застосування нечітких продукційних правил типу «якщо–то» із функціями належності дозволяє відобразити рівень ризику, технічну зношеність основних засобів, рівень технологічної модернізації та цифрової готовності підприємства в уніфікованому числовому вигляді. Такі моделі ефективно реалізують трансформацію експертних оцінок у числові інтервали, що є основою для подальшого аналізу та агрегування показників [151].

Таким чином, нечітке моделювання надає ефективний інструментарій для формалізації оцінок у складних техніко-технологічних умовах, де традиційні методи математичного аналізу втрачають точність або стають

непридатними. Це створює підґрунтя для побудови інтегральних індикаторів, що відображають реальний стан безпеки підприємства в умовах технологічної трансформації та цифрової інтеграції.

Сучасна наукова література також свідчить про ефективність інтегративних підходів, які поєднують методи нечіткої логіки з методами багатокритеріального прийняття рішень. Наприклад, використання нечіткого аналізу ієрархій, методу найгіршого кращого, нечіткої логіки дозволяє об'єктивно враховувати ваги критеріїв та взаємозалежності між ними. Такі підходи демонструють високу адаптивність до специфіки підприємств та контексту цифрової трансформації.

Так, у роботі П. Рані та інші [81] запропоновано гібридну модель оцінки ризиків цифрової трансформації підприємств, що поєднує метод ARAS та модель RANCOM у середовищі множин Picture Fuzzy Sets. Такий підхід дозволяє враховувати як кількісні, так і якісні чинники ризику, з урахуванням експертних оцінок і нечіткої інформації. Результати демонструють високу ефективність моделі у ранжуванні ризиків DT-проектів, що може бути застосовано для зміцнення техніко-технологічної безпеки підприємств.

Комплементарним до цього є підхід, представлений у праці Мазаракі А. [156], де запропоновано нечітко-множинну модель оцінки ризику виведення інноваційної продукції на ринок на основі концепції «RWW». Цей підхід дозволяє формалізувати якісні характеристики рішень та отримати інтегральну оцінку інноваційного ризику, що є особливо цінним в умовах цифрової модернізації виробничих процесів. Обидва підходи ілюструють перспективність поєднання нечіткої логіки з інструментами багатокритеріального аналізу як ефективного інструменту для зміцнення техніко-технологічної безпеки підприємств.

Вагоме значення в контексті нашого дослідження мають розробки Г. Тигач [194], де акцентовано увагу на тому, що саме техніко-технологічна компонента зазнає найбільш відчутних трансформацій під впливом цифровізації. Автором виокремлено розширення можливостей контролю

виробничих процесів, створення нових цифрових продуктів та масштабну автоматизацію як ключові драйвери розвитку. Водночас наголошується на необхідності адаптації системи безпеки до нових умов функціонування, що корелює з авторською тезою про потребу ревізії традиційних метрик та індикаторів оцінювання.

Таким чином, використання нечітких моделей у поєднанні з експертними методами та цифровими індикаторами є науково обґрунтованим підходом до оцінки техніко-технологічної підсистеми економічної безпеки [164]. Це дозволяє забезпечити комплексний аналіз стану підприємства з урахуванням цифрових ризиків, ступеня автоматизації, рівня інноваційної готовності обладнання, захищеності ІТ-інфраструктури та цифрових компетенцій персоналу.

Для того щоб оцінити загальний рівень техніко-технологічної підсистеми економічної безпеки поширеною практикою є використання інтегрального показника. Інтегральний індексний підхід передбачає приведення різномірних індикаторів до єдиного узагальненого показника. Кожному індикатору техніко-технологічної безпеки присвоюється вага  $w_i$  (відповідно до експертних оцінок важливості), після чого будується формула зваженої суми. Загальний рівень техніко-технологічної безпеки може розраховуватися, наприклад, як середньозважений інтегральний показник:

$$I_{mex} = \sum_{i=1}^n w_i I_i,$$

де  $I_i$  – нормований показник  $i$ -го індикатора.

Важливість показників  $w_i$  визначається експертно або статистичними методами такими як метод головних компонент чи аналіз ієрархічної структури.

У межах цього дослідження було запропоновано авторський підхід до формалізації техніко-технологічної підсистеми економічної безпеки підприємства шляхом побудови ієрархічної моделі інтегрального оцінювання. Запропонована система дозволяє обчислювати узагальнений інтегральний

індекс техніко-технологічної безпеки на основі агрегування окремих індикаторів, які формуються на нижньому рівні ієрархії [18].

Запропоновано структурований набір релевантних індикаторів, що відображають ключові параметри технічного та технологічного стану підприємства в умовах цифрової трансформації (табл. 2.7).

Таблиця 2.7

Перелік критеріїв оцінки техніко-технологічної підсистеми економічної безпеки.

| № | Критерій                                             | Підхід до оцінки                                                                                                            | Рівні оцінки (лінгвістичні)                                         | Відповідні числові значення |
|---|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------|
| 1 | Рівень автоматизації виробництва                     | Частка автоматизованих операцій у виробничому циклі (на основі стандартів IEC 62264, ISA-95)                                | Дуже низький / Низький / Середній / Високий / Дуже високий          | 0.1 / 0.3 / 0.5 / 0.7 / 0.9 |
| 2 | Захищеність IT-інфраструктури                        | Оцінюється за наявністю захисних систем, політик безпеки, стандартів ISO/NIST, частотою інцидентів                          | Дуже низька / Низька / Середня / Висока / Дуже висока               | 0.1 / 0.3 / 0.5 / 0.7 / 0.9 |
| 3 | Частка цифрових технологій у технологічних процесах  | Частка використання цифрових рішень (IoT, SCADA, цифрові двійники, тощо) у виробничих процесах                              | Менше 10% / 10–30% / 31–60% / 61–80% / Понад 80%                    | 0.1 / 0.3 / 0.5 / 0.7 / 0.9 |
| 4 | Стан технічного обладнання та інноваційна готовність | Середній вік обладнання, його відповідність стандартам цифрового виробництва (Industry 4.0), підключення до мереж           | Застаріле / Частково застаріле / Задовільне / Сучасне / Інноваційне | 0.1 / 0.3 / 0.5 / 0.7 / 0.9 |
| 5 | Цифрова компетентність персоналу                     | Частка працівників з цифровою освітою, наявність внутрішньої цифрової культури, доступ до тренінгів (DIGCOMP Framework 2.2) | Дуже низька / Низька / Середня / Висока / Дуже висока               | 0.1 / 0.3 / 0.5 / 0.7 / 0.9 |

Джерело: складено автором

До переліку індикаторів увійшли:

- рівень автоматизації виробництва;
- захищеність IT-інфраструктури;

- частка цифрових технологій у технологічних процесах;
- стан технічного обладнання та інноваційна готовність;
- цифрова компетентність персоналу.

Оцінювання кожного з індикаторів передбачається на шкалі рівнів (наприклад: низький, середній, високий) з урахуванням галузевих особливостей, нормативних вимог та експертної думки. Визначення значень здійснюється на основі статистичних даних підприємства або шляхом експертного опитування, а приклад відповідних опитувальних форм був розроблений і представлений в Додатку А.

У процесі інтегральної оцінки техніко-технологічної підсистеми економічної безпеки підприємства ваги критеріїв відіграють ключову роль, оскільки дозволяють урахувати нерівнозначний вплив кожного з них на загальний рівень безпеки. Нерівноважність обумовлена як різним ступенем критичності, так і особливостями цифрового середовища, яке трансформує роль класичних технічних факторів. Існує багато підходів до визначення ваг, зокрема метод експертних оцінок, аналіз чутливості або нормалізація ваг методом власного вектору [163, 126, 83]

Водночас у практичному застосуванні вагові коефіцієнти можуть встановлюватися індивідуально для кожного підприємства, залежно від галузевої специфіки, рівня цифрової зрілості, технологічного укладу, ступеня залежності від цифрових систем та актуальних викликів у сфері інформаційної безпеки. Наприклад, для підприємств із високим рівнем автоматизації та розвинутою цифровою інфраструктурою пріоритетними стають критерії, пов'язані із захищеністю ІТ-систем і цифровою компетентністю персоналу, адже збої в цих сферах можуть критично порушити виробничу безперервність. Натомість у підприємствах із традиційною технологічною базою домінуюче значення може мати стан основних фондів та інноваційна готовність, оскільки саме модернізація обладнання є необхідною умовою цифрового прориву. У випадках кадрового дефіциту вагомість цифрових навичок працівників може бути визначальною для забезпечення техніко-технологічної стійкості.

Таким чином, інтеграція кількісних і якісних параметрів у межах ієрархічної моделі дозволяє створити ефективний інструмент для моніторингу, діагностики та стратегічного управління техніко-технологічною підсистемою економічної безпеки підприємств.

### **2.3. Інформаційно-логічна модель системи підтримки прийняття рішень для управління системою економічною безпекою підприємства в умовах цифровізації**

В умовах інтелектуалізації економіки та стрімкого розвитку цифрових технологій ефективне управління та побудова системи економічної безпеки підприємства неможливе без чітко сформованої інформаційної моделі. Така модель виступає концептуальним та функціональним інструментом, що забезпечує взаємозв'язок між зовнішнім середовищем, внутрішніми ресурсами підприємства та оцінкою рівня його безпеки.

Інформаційна модель управління економічною безпекою підприємства є ключовою складовою системи підтримки прийняття рішень (СППР), яка в сучасних умовах цифрової трансформації набуває особливого значення. СППР представляє собою інтерактивну комп'ютерну систему, що поєднує апаратне та програмне забезпечення, бази даних і моделей, а також участь управлінського персоналу для підтримки процесу ухвалення рішень в умовах структурованих, слабоструктурованих або неструктурованих управлінських задач [187]. У західній науковій традиції широко використовується поняття *decision support systems* (DSS). Так, за визначенням С. Голсапл та А. Вінстон, системи підтримки рішень (DSS) – це системи, які підтримують як індивідуальне, так і колективне ухвалення управлінських рішень шляхом розширення здатності менеджерів працювати з різними видами знань [46]. Таким чином, СППР доцільно розглядати як інтерактивну комп'ютерну систему, що поєднує технічні засоби, програмне забезпечення, бази даних і

моделей, а також участь користувача в усіх фазах процесу прийняття управлінських рішень.

З огляду на це, в контексті системи економічної безпеки підприємства СППР виконує функції збору, структурування, зберігання, обробки та аналізу великого обсягу даних щодо внутрішнього стану підприємства та зовнішнього середовища. Це дає змогу формувати прогностичні сценарії розвитку подій, виявляти потенційні загрози та приймати обґрунтовані рішення щодо зниження ризиків.

Інформаційна модель є центральним елементом СППР, адже саме вона визначає набір даних, логіку їх структурування, способи трансформації первинної інформації у знання, необхідні для управління безпековими аспектами діяльності підприємства. Як зазначається у сучасній літературі, якість управлінських рішень безпосередньо залежить від якості інформаційно-аналітичного забезпечення. Узагальнюючи підходи до інформаційного забезпечення процесу управління, слід зазначити, що воно трактується як інструмент впливу, який забезпечує своєчасне надходження достовірних даних, їх верифікацію, обробку та доведення до відповідальних осіб [157, 197]. При цьому інформаційна модель повинна гарантувати повноту, актуальність та своєчасність інформаційних потоків, що використовуються в управлінні економічною безпекою.

Виконуючи функцію бази знань і моделей у складі СППР, інформаційна модель акумулює ключові показники фінансового, технічного, кадрового стану підприємства, а також формалізовані алгоритми оцінювання ризиків, прогнозування загроз, визначення зон вразливості. Вона забезпечує основу для інтелектуальної обробки інформації, включаючи використання штучного інтелекту, систем машинного навчання, нечіткої логіки та інших підходів сучасної аналітики.

З функціонального погляду, сучасна виконавча інформаційна система як варіант СППР включає такі основні підсистеми [186]:

- інтерфейс користувача;

- систему управління базами даних;
- систему управління математичними моделями;
- модулі комунікації та обміну інформацією.

У типових архітектурах систем підтримки прийняття рішень також виділяють [130]:

- лінгвістичну підсистему (відповідає за обробку запитів користувачів природною мовою),
- систему візуалізації даних та інформації,
- модулі постановки задач та генерації сценаріїв рішень,
- предметно-орієнтовані експертні підсистеми та бази знань.

На рис. 2.2 показан один з прикладів взаємодії елементів і структури системи підтримки прийняття рішень в рамках інформаційної системи.

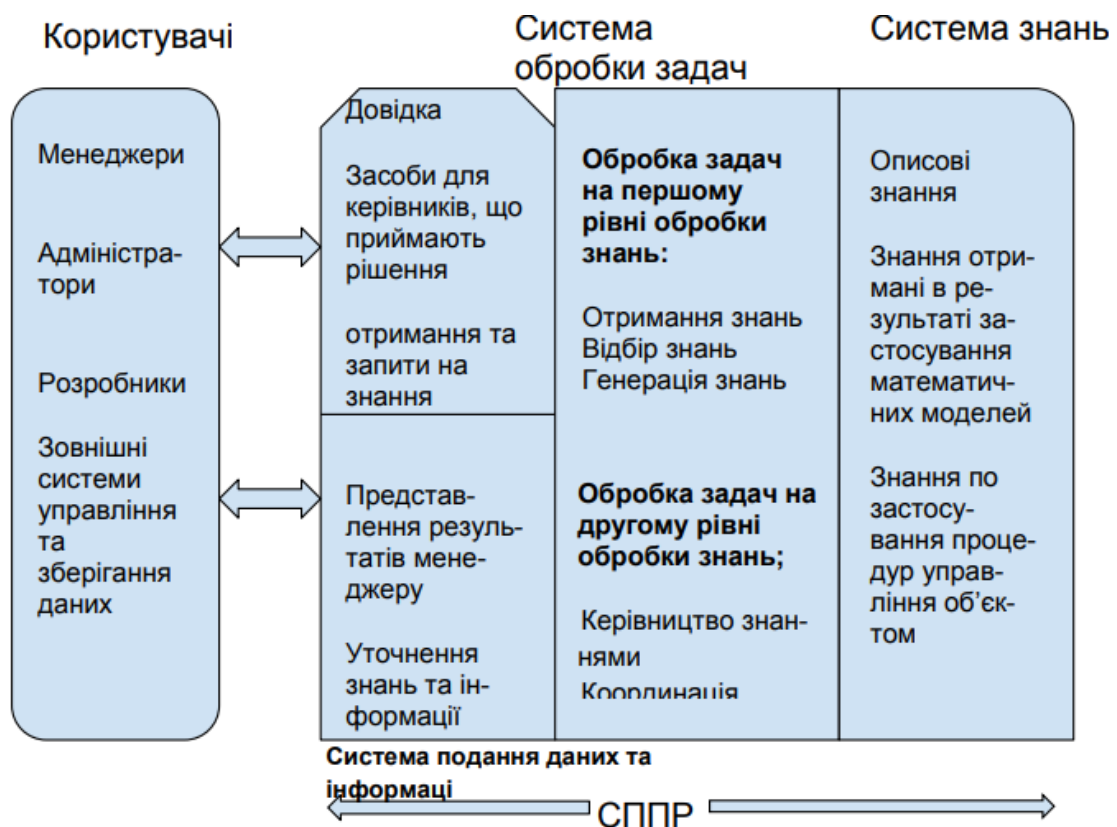


Рис. 2.2. Архітектура системи підтримки прийняття рішень. Джерело: [130]

Таким чином, побудова ефективної інформаційної моделі є основою забезпечення інтегральної економічної безпеки підприємства в умовах нестабільного зовнішнього середовища та зростаючих цифрових ризиків.

Процес розробки інформаційної моделі управління системою економічної безпеки підприємства повинен спиратися на систему науково обґрунтованих принципів. Їх дотримання є передумовою забезпечення ефективності, адаптивності та надійності моделі в умовах динамічного та часто непередбачуваного зовнішнього середовища.

До основних принципів побудови інформаційної моделі економічної безпеки належать такі положення [164]:

- принцип уніфікованості – інформаційну модель доцільно будувати на основі універсальних підходів, які дають змогу використовувати її для розв’язання широкого кола управлінських завдань;

- принцип системності – модель має бути цілісною та охоплювати всі ключові підсистеми економічної безпеки підприємства;

- принцип актуальності та розвитку – інформаційна модель повинна адаптуватися до змін зовнішнього середовища та забезпечувати можливість оновлення даних, методик і сценаріїв розвитку загроз;

- принцип сумісності – для ефективної взаємодії з іншими інформаційними системами підприємства модель має підтримувати стандартизовані інтерфейси та протоколи обміну даними;

- принцип стандартизації – використання галузевих стандартів у форматах даних, методах їх обробки та засобах візуалізації сприяє підвищенню якості й надійності моделі;

- принцип ефективності – розроблення та впровадження інформаційної моделі мають бути економічно обґрунтованими та забезпечувати підвищення якості управлінських рішень;

- принцип єдиної інформаційної бази – усі дані в системі повинні вводитися один раз і надалі багаторазово використовуватися в різних підсистемах;

– принцип достовірності та повноти – модель повинна ґрунтуватися на точних, повних, актуальних і релевантних даних.

Таким чином, дотримання зазначених принципів дозволяє сформувати інформаційну модель, яка відповідає як науковим вимогам, так і практичним потребам підприємства. Така модель не лише підтримує процеси аналізу та ухвалення рішень, а й сприяє підвищенню стійкості підприємства до загроз і викликів, зумовлених сучасними умовами господарювання.

Розробка ефективної інформаційної моделі підтримки прийняття рішень в управлінні економічною безпекою підприємства вимагає чіткого дотримання ряду критичних умов ще на початкових етапах проектування. Як зазначається у [107], успішна реалізація будь-якої комп'ютеризованої інформаційної системи значною мірою залежить від:

- повноти врахування потреб користувачів і специфіки середовища функціонування;
- обґрунтованого вибору інструментарію для реалізації технічної та програмної частини;
- належного рівня фінансової підтримки;
- забезпечення доступу до релевантних джерел інформації.

Ці фактори формують підґрунтя для створення функціонально збалансованої та адаптивної системи, яка має бути не лише технологічно сучасною, а й практично дієвою. На основі узагальнення сучасних досліджень і галузевих рекомендацій [3, 30] сформульовано такі початкові вимоги до ІСППР в управлінні економічною безпекою підприємства:

- підтримка обробки слабоструктурованих і нечітких даних, тобто система повинна працювати не лише з чітко формалізованими показниками, а й з експертними оцінками, аналітичними матеріалами та іншою інформацією, яку складно подати у строго визначеній формі;
- моделювання та прогнозування економічних ризиків, тобто ІСППР має допомагати оцінювати ймовірність виникнення ризиків і можливі наслідки їх реалізації за допомогою статистичних та прогнозних методів;

- підтримка всіх фаз процесу прийняття рішень, тобто система повинна супроводжувати користувача на всіх етапах від виявлення проблеми та збору інформації до розроблення альтернатив і вибору найбільш доцільного рішення;

- автоматизований моніторинг ключових індикаторів безпеки, тобто система має постійно відстежувати основні фінансові, кадрові й технологічні показники та своєчасно сигналізувати про потенційно небезпечні зміни;

- інтеграція з існуючими інформаційними системами підприємства, тобто ІСППР повинна без суттєвих труднощів обмінюватися даними з іншими цифровими платформами, які вже використовуються на підприємстві;

- зручний та гнучкий інтерфейс, тобто користувачі повинні мати можливість легко користуватися системою у щоденній роботі, а також налаштовувати її відповідно до своїх потреб і функціональних обов’язків;

- масштабованість і висока продуктивність, тобто система повинна стабільно працювати навіть за умови зростання обсягів даних і збільшення кількості користувачів без помітного зниження швидкості чи якості роботи;

- можливість еволюційного розвитку, тобто ІСППР має бути побудована так, щоб у подальшому можна було оновлювати її компоненти, розширювати функціонал і впроваджувати нові аналітичні інструменти без порушення загальної логіки роботи;

- підвищення ефективності управління економічною безпекою, тобто впровадження системи повинно сприяти прийняттю більш обґрунтованих рішень, своєчасному реагуванню на загрози та загальному зниженню рівня ризику для підприємства.

Таким чином, формування вимог до інформаційної системи не є лише технічним етапом, а виступає стратегічною основою її ефективності. Їх дотримання забезпечує відповідність системи як на рівні технологічної архітектури, так і з точки зору досягнення цілей економічної безпеки.

Після визначення ключових вимог побудови інформаційної моделі необхідним кроком є формування загальної архітектурної схеми та алгоритму

її реалізації. У контексті цифровізації та високої динаміки бізнес-середовища побудова ефективної інформаційної моделі управління системою економічної безпеки потребує чіткого структурування процесу розробки.

Процес проєктування інформаційної моделі доцільно розглядати як послідовність взаємопов'язаних етапів, кожен з яких виконує специфічну функцію у забезпеченні загальної цілісності та адаптивності системи. Узагальнена схема такої побудови представлена на рис. 2.3 [60].

Перший етап передбачає формування інформаційно-аналітичної бази щодо стану внутрішнього та зовнішнього середовища підприємства. Оскільки будь-яка господарська діяльність здійснюється у конкурентному полі, інформація про стан ринку, дії конкурентів, поведінку споживачів є критично важливою умовою для формування ефективної системи економічної безпеки.

Другий етап охоплює оцінювання та аналітичну обробку зібраної інформації. На цьому етапі здійснюється ідентифікація поточного стану підприємства, визначаються його сильні та слабкі сторони, а також наявні зовнішні загрози і потенційні можливості.

Третій етап полягає у визначенні поточного рівня економічної безпеки підприємства на основі попередніх аналітичних розрахунків. Це дозволяє отримати інтегральне уявлення про рівень захищеності підприємства від внутрішніх та зовнішніх деструктивних впливів.

Четвертий етап передбачає моделювання прогностичних показників діяльності підприємства з урахуванням виявлених загроз, резервів та вузьких місць. У результаті здійснюється прогнозування ймовірного рівня конкурентних позицій підприємства на внутрішньому та зовнішньому ринках за умов ефективної реалізації політики безпеки.

П'ятий етап включає розробку альтернативних сценаріїв розвитку подій (сценарний аналіз), з урахуванням бажаних напрямів взаємодії між усіма учасниками виробничо-економічних відносин. Такий підхід забезпечує врахування інтересів усіх зацікавлених сторін.

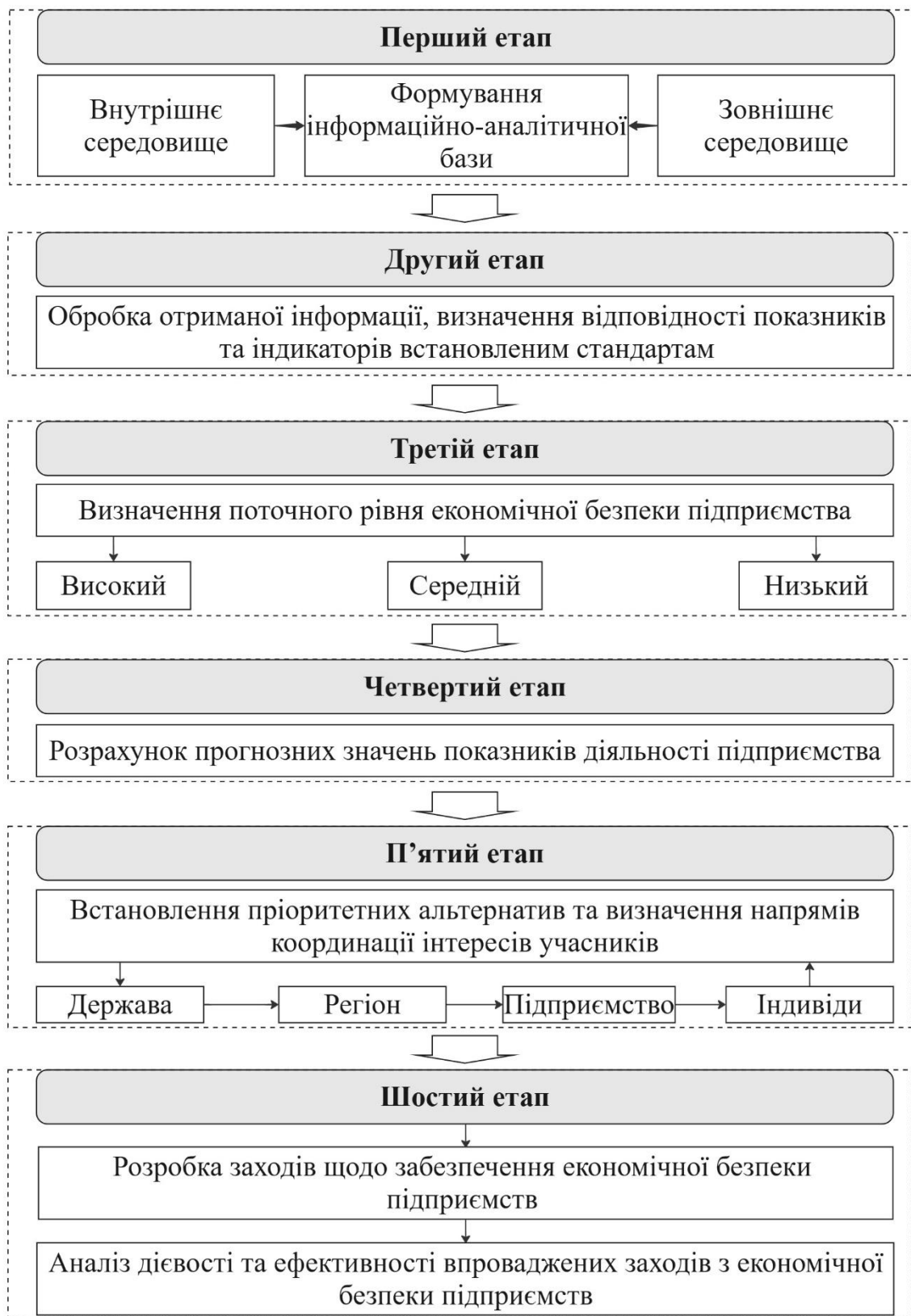


Рис. 2.3. Процес проектування інформаційної моделі системи підтримки прийняття рішень управління системою економічної безпеки.

Джерело: [60]

Шостий етап полягає у безпосередньому формуванні системи економічної безпеки підприємства, включаючи розробку механізмів реалізації, моніторинг ефективності її функціонування на визначених часових інтервалах та можливість коригування цільових показників для досягнення бажаного ефекту.

На основі концептуальної моделі економічної безпеки підприємства в умовах цифрової трансформації була розроблена інформаційна модель управління, яка поєднує системно-інтегративний підхід із сучасними технологіями штучного інтелекту. В основі її побудови лежить принцип модульності, що дозволяє забезпечити гнучкість, масштабованість і адаптивність системи відповідно до потреб конкретного підприємства.

На основі аналізу наукових праць та найкращих практик проєктування СППР [169] було визначено, що оптимальним варіантом побудови такої системи є блочно-модульна структура. Вона передбачає наявність трьох взаємопов'язаних функціональних підсистем – фінансової, кадрової та техніко-технологічної – та інтерфейсу взаємодії з користувачами.

Архітектура інформаційної моделі включає такі структурні елементи [16]:

Вхідний модуль. Забезпечує первинне введення даних і знань про підприємство, включаючи внутрішні звітні показники, регламентовані документи, дані з внутрішньої бази даних, а також зовнішню аналітичну інформацію.

Модуль попередньої обробки даних. Виконує перевірку, очищення, нормалізацію, уніфікацію та кодування даних для подальшого аналітичного оброблення.

Модуль моделювання та обробки результатів. Реалізує математичні моделі оцінювання стану підсистем, побудову трендів і прогнозів із застосуванням методів машинного навчання.

Модуль інтеграції оцінок. Забезпечує агрегацію результатів окремих підсистем і формування єдиного інтегрального індексу економічної безпеки підприємства.

Вихідний модуль. Формує результати оцінювання, звіти, візуалізації, рекомендації та попереджувальні сигнали. Результати подаються у зрозумілій формі для управлінців різного рівня.

Інтерфейс користувача. Забезпечує взаємодію користувача з системою, включаючи введення параметрів, запуск модулів, перегляд звітів і прийняття рішень. Інтерфейс орієнтований на інтуїтивність, доступність та адаптацію до рівня цифрових компетенцій користувача.

Важливо зазначити, що запропонована інформаційна модель системи економічної безпеки розроблена з урахуванням умов цифрової трансформації підприємства. Це дозволяє здійснювати ефективний контроль за новими цифровими ризиками, які виникають у зв'язку з інтенсивним впровадженням цифрових технологій, автоматизацією бізнес-процесів та використанням великих даних. Інформаційна система інтегрує цифрові показники у всі ключові підсистеми, забезпечуючи цілісне сприйняття цифрових загроз та своєчасне реагування на них.

Кожна з підсистем (фінансова, кадрова, техніко-технологічна) функціонує незалежно на етапах збору та попереднього аналізу даних. Водночас їх результати об'єднуються у єдиній інтеграційній частині, що дозволяє враховувати взаємозалежність окремих елементів системи економічної безпеки. Деталізований опис кожного з цих модулів наведено нижче.

Вхідний модуль є стартовим елементом інформаційної системи та відповідає за агрегацію вхідних даних із різних джерел. Основними джерелами інформації виступають корпоративні бази даних, файли формату CSV, а також документація підприємства, що включає політики безпеки, інструкції, технологічні описи тощо. Модуль виконує функцію форматування та попередньої верифікації даних перед їх передачею до відповідних підсистем,

при цьому забезпечується можливість інтеграції з внутрішніми та зовнішніми джерелами інформації, що дозволяє актуалізувати моделі відповідно до змін у цифровому середовищі підприємства.

Модуль попередньої обробки даних фінансової підсистеми реалізує функцію обробки та трансформації даних фінансової звітності. На цьому етапі здійснюється завантаження фінансових показників з бухгалтерських систем або інших джерел, а також введення показників цифрового розвитку підприємства. Після збирання даних модуль виконує очищення, нормалізацію та розрахунок проміжних фінансових індикаторів, що включають різні коефіцієнти ліквідності, фінансової стійкості, тощо. Результатом роботи цього модуля є підготовлений масив структурованих даних для моделювання ризиків фінансової підсистеми.

Модуль моделювання фінансової підсистеми активується після завершення підготовки фінансових індикаторів. Він реалізує модель прогнозування ймовірності банкрутства підприємства, що базується на сучасних алгоритмах машинного навчання на попередньо створеній і навченій відповідній моделі. Вхідними змінними є сформовані фінансові індикатори, а вихідним результатом є імовірнісна оцінка банкрутства.

Модуль обробки результатів фінансової підсистеми формує оцінку ризику фінансової безпеки на основі результатів моделювання. На цьому етапі відбувається трансформація прогнозовної ймовірності банкрутства у зручний формат оцінки рівня ризику відповідної підсистеми.

Модуль попередньої обробки даних кадрової підсистеми забезпечує завантаження, структурування та верифікацію корпоративних даних про працівників. До таких даних можуть належати журнали активності, історія доступів до систем, шаблони входу/виходу, зміни у правах доступу, а також дані про поведінкові аспекти.

Модуль моделювання кадрової підсистеми відповідає за виявлення поведінкових аномалій серед працівників, які можуть свідчити про інсайдерські загрози. У модулі реалізуються алгоритми пошуку аномалій, а

результатом є кількісна оцінка аномальних дій, яка надалі використовується для обчислення кадрового ризику.

Модуль обробки результатів кадрової підсистеми виконує інтерпретацію результатів аналізу кількості аномалій, при цьому оцінка кадрового ризику ґрунтується на кількості виявлених відхилень. Отримані значення кількості аномальних дій трансформуються в зрозумілі для всіх користувачів значення оцінки рівня ризику кадрової підсистеми.

Модуль попередньої обробки техніко-технологічної підсистеми акумулює дані з технічних джерел підприємства таких як аудиторські звіти, описи ІТ-інфраструктури, технічної документації. Оцінка техніко-технологічної підсистеми базується на ключових індикаторах, що відображають здатність підприємства впроваджувати та захищати цифрові технології в рамках виробничих і управлінських процесів. Модуль допомагає користувачам визначити рівень технічної цифрової готовності на основі відповідних критеріїв. Також тут визначаються вагові коефіцієнти для кожного критерію за допомогою експертних або алгоритмічних підходів.

Модуль моделювання техніко-технологічної підсистеми забезпечує розрахунок інтегрального показника технічної безпеки. Значення індикаторів кожного критерію агрегуються із урахуванням ваг, після чого формується комплексна оцінка здатності підприємства ефективно функціонувати в умовах цифрової трансформації.

Модуль обробки результатів техніко-технологічної підсистеми консолідує результати моделювання у форматі, придатному для включення в інтегральну модель економічної безпеки.

Модуль формування інтегрального показника та рекомендацій об'єднує результати трьох підсистем, обчислюючи загальний індекс економічної безпеки підприємства. Крім того, модуль генерує персоналізовані управлінські рекомендації, орієнтовані на зменшення ризиків та підвищення загального рівня захищеності підприємства.

Останній вихідний модуль побудованої інформаційної системи формує кінцеві результати роботи системи, зокрема: оцінки рівнів ризику кожної підсистеми, загальний індекс безпеки, а також текстові рекомендації щодо заходів управління ризиками. Ці результати можуть бути представлені у вигляді звітів або візуалізованих дашбордів.

Схему розробленої інформаційної моделі системи економічної безпеки в умовах цифрової трансформації можна побачити на рис. 2.4.

Незважаючи на те, що детальний опис моделей окремих підсистем наведено у п. 2.2, критично важливим етапом проектування інформаційної моделі залишається формалізація логіки роботи модуля формування інтегрального показника та стратегічних рекомендацій. Оскільки кожна підсистема генерує дані різної природи, виникає потреба у створенні уніфікованого математичного алгоритму, який би синтезував ці результати у єдиний аналітичний сигнал.

Для вирішення цього завдання автором запропоновано наступну формулу визначення інтегрального показника економічної безпеки підприємства  $I_s$ :

$$I_s = w_1 \cdot (1 - K_f) + w_2 \cdot \left(1 - \frac{K_k}{K_k + 1}\right) + w_3 \cdot K_t$$

де:

$K_f$  – прогнозована ймовірність банкрутства, розрахована на основі моделі банкрутства.

$K_k$  – нормалізована кількість аномальних дій працівників, отримана з моделі виявлення інсайдерських загроз.

$K_t$  – інтегральний індекс техніко-технологічної безпеки, що охоплює цифрову стійкість підприємства та рівень захищеності технологічних процесів.

$w_1, w_2, w_3$  – вагові коефіцієнти кожного компоненту, які відображають відносну значущість відповідної підсистеми.

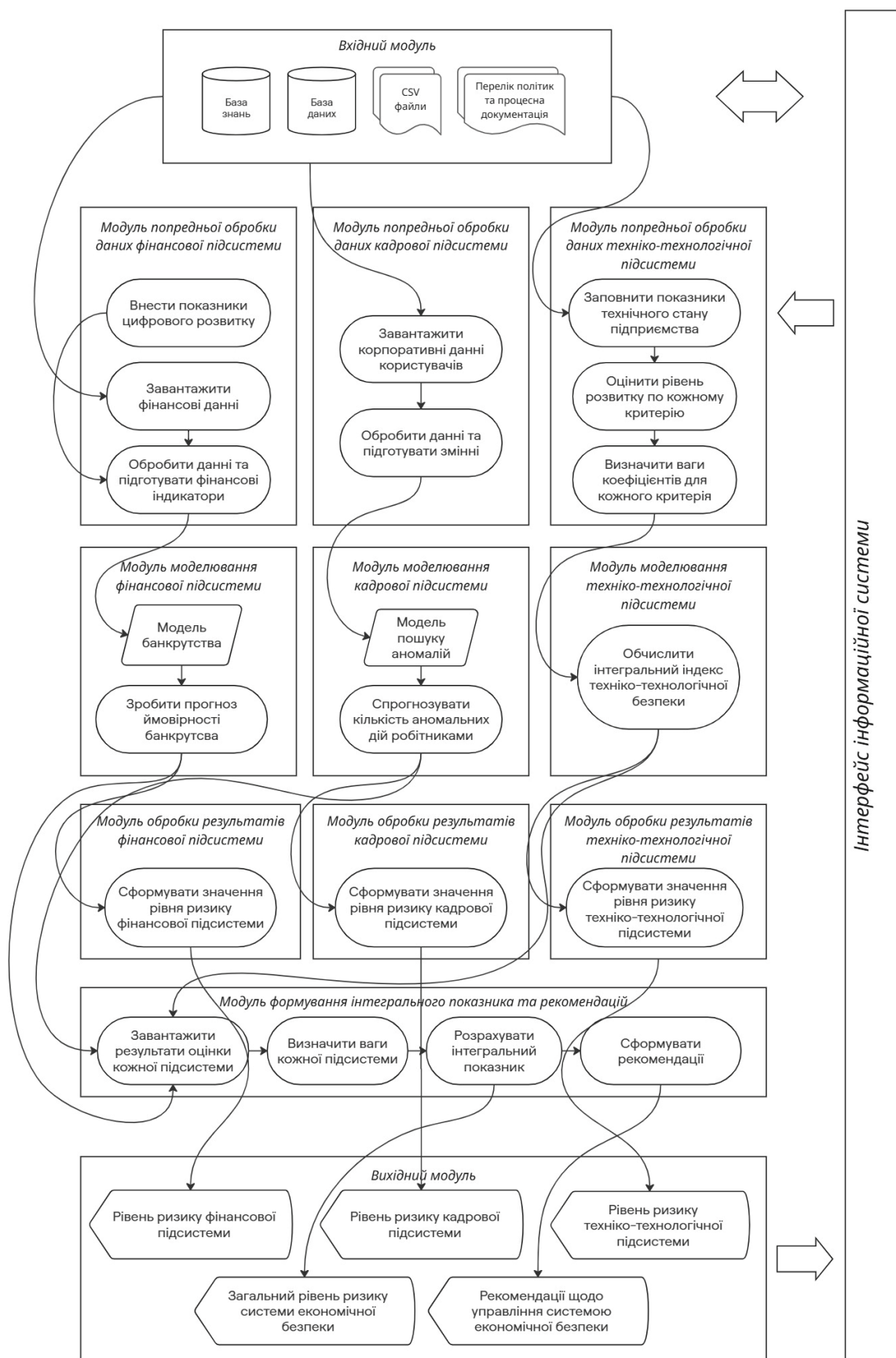


Рис. 2.4. Інформаційна системи економічної безпеки підприємства в умовах цифрової трансформації.

Джерело: складено автором.

У даному контексті здійснюється детальний аналіз кожної з компонент інтегрального показника, з подальшим обґрунтуванням доцільності вибору саме запропонованої формули. Використання комплементарної форми дозволяє подати фінансову стійкість як зростаючу функцію (чим нижча ймовірність банкрутства, тим вищий рівень загального рівня економічної безпеки  $I_s$ ). Це інтуїтивно узгоджується з логікою систем оцінки – вища фінансова стабільність повинна збільшувати інтегральну оцінку безпеки. Обрана форма фракції для кадрової підсистеми забезпечує асимптотичне згасання: при малих значеннях  $K_k$  (мала кількість аномальних дій) внесок компоненти до  $I_s$  буде наближений до 1, а при збільшенні  $K_k$  – швидко зменшуватиметься. Це дозволяє уникнути лінійної залежності та надає гнучкість у реакції системи на кадрові ризики. Індекс  $K_t$  побудований як зважена сума нормалізованих індикаторів. Його значення змінюється в інтервалі  $[0;1]$ , де 1 означає повну технологічну захищеність. В цьому випадку вибір прямої залежності між цим показником та рівнем  $I_s$  є логічно обґрунтованим.

Особливу увагу в процесі моделювання слід приділити визначенню вагових коефіцієнтів. В сучасній науковій літературі представлено чимало підходів до розв'язання цієї задачі. Зокрема, В. Алькема та М. Копитко [104], досліджуючи підприємства автомобілебудівної галузі, пропонують диференціювати ваги залежно від функціональних складових (фінансова – 0,35; кадрова – 0,20; техніко-технологічна – 0,20 тощо). Такий розподіл базується на експертних оцінках менеджменту та галузевій специфіці. У свою чергу, С. Пілецька [175] використовує метод побудови узагальнюючого показника на основі статистичної значущості груп індикаторів.

Проте, враховуючи динамічність цифрової трансформації, у межах цього дослідження запропоновано відмовитися від фіксації єдиного набору «жорстких» вагових коефіцієнтів. Замість цього розроблено тривимірну модель, яка дозволяє візуалізувати весь фазовий простір можливих станів системи.

Для аналітичного представлення взаємозв'язку між підсистемами було побудовано тривимірну сітку, що охоплює весь діапазон значень вхідних змінних. Результати моделювання «гіперпростору» станів економічної безпеки представлено на рис. 2.5. Кожна точка у сформованому об'ємі відповідає конкретному поєднанню станів фінансової, кадрової та технологічної підсистем, а її колір відображає підсумкове значення індексу економічної безпеки згідно з колірною шкалою від червоного (критичний рівень) до зеленого (високий рівень безпеки).

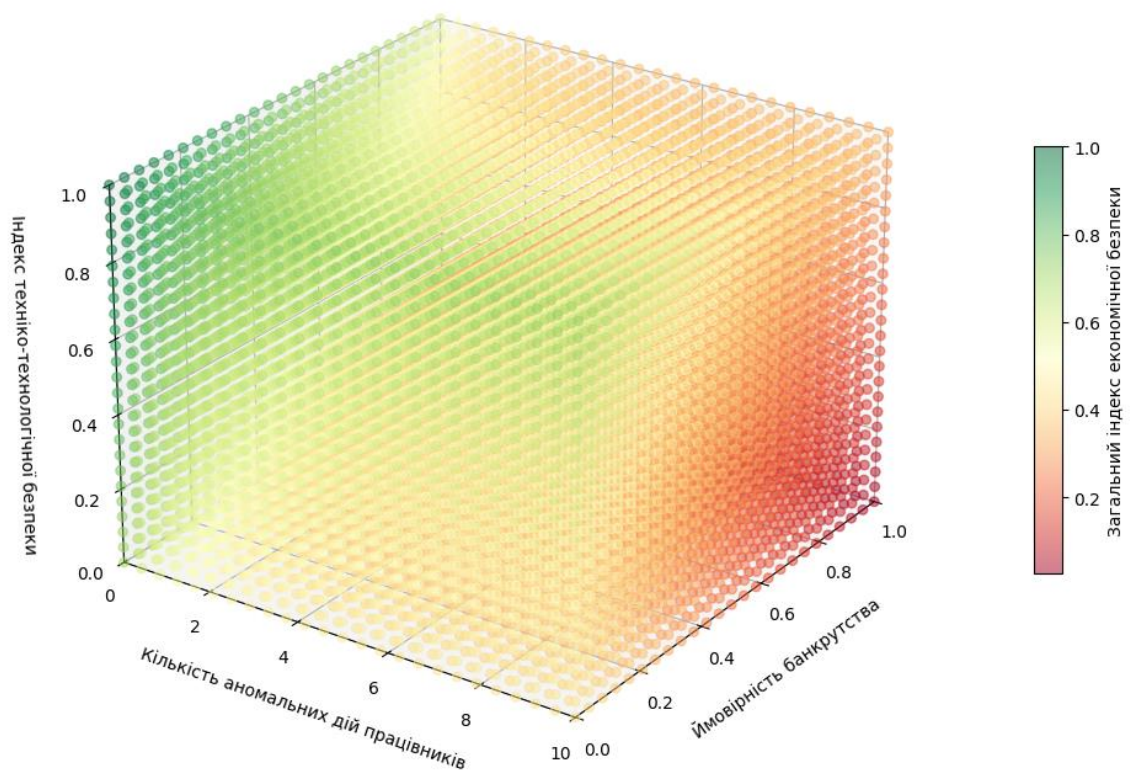


Рис. 2.5. Гіперпростір станів інтегрального індексу економічної безпеки підприємства.

Джерело: побудовано автором.

Аналіз отриманої графічної моделі дозволяє сформулювати підкреслити зони стратегічного ризику: скупчення точок у червоному спектрі (нижній правий кут простору) ілюструє синергетичний ефект накладання високої ймовірності банкрутства на низький рівень технологічної захищеності, що

призводить до стрімкого падіння  $I_s$  незалежно від стану кадрової безпеки. Також, за допомогою цього підходу можна проаналізувати чутливість моделі: градієнт кольорів демонструє, що інтегральний індекс найбільш чутливий до змін у фінансовій складовій, проте висока концентрація аномальних дій персоналу здатна перевести підприємство із «зеленої» зони до «жовтої» навіть за умови стабільного фінансового стану.

Водночас слід зауважити, що суто чисельне значення інтегрального індексу (у межах від 0 до 1) без належної інтерпретації може мати обмежений прикладний ефект для прийняття управлінських рішень. Для того, щоб результати моделювання стали зрозумілим сигналом для менеджменту, автором обґрунтовано необхідність приведення вихідних показників до уніфікованої шкали значень. Такий перехід до єдиного аналітичного простору є обов'язковою умовою побудови комплексної системи оцінювання.

Доцільність впровадження уніфікованої шкали зумовлена наступними ключовими аспектами:

1. По-перше, моделі, побудовані для окремих підсистем, оперують різними за природою показниками, які мають неоднорідні одиниці вимірювання, діапазони значень та вагові характеристики. Без уніфікації їх поєднання в межах єдиної системи призводило б до некоректності результатів і втрати об'єктивності аналізу. Уніфікована шкала дозволила стандартизувати дані, що, у свою чергу, забезпечило методологічну узгодженість інтегрованої оцінки.

2. По-друге, використання спільної шкали значень сприяє підвищенню інтерпретованості результатів аналізу, що дає змогу наочно відображати рівень економічної безпеки як в розрізі підсистем, так і на загальному рівні, що істотно полегшує процес прийняття управлінських рішень. Застосування візуально зрозумілих шкал ризику з чітко визначеними пороговими значеннями дозволяє оперативно ідентифікувати критичні стани та своєчасно реалізовувати заходи реагування.

3. Останнім вагомим аспектом є забезпечення гнучкості та масштабованості інформаційної системи. Іншими словами, завдяки приведенню до уніфікованої шкали, система здатна до подальшої адаптації шляхом інтеграції нових підсистем, що не потребує суттєвих змін у її структурі або логіці функціонування.

З метою переведення вихідних показників до кількісного формату застосовуються лінгвістичні оцінки, що ґрунтуються на узгоджених шкалах. Зокрема, І. Отенко [168] пропонує трирівневу шкалу для визначення рівня економічної безпеки підприємства. Аналогічний підхід використовують В. Алькема та М. Копитко [104], які виділяють низький, достатній та високий рівні безпеки. Подібна градація знайшла відображення і в положеннях Міжнародного стандарту з управління ризиками ISO 31000, де встановлено порогові рівні ризику – високий, середній та низький – для забезпечення пріоритезації загроз [52].

Таким чином, із урахуванням наукових підходів та практичної доцільності, в інформаційній системі управління економічною безпекою було реалізовано одну з найпоширеніших у науковій літературі трирівневу шкалу ризику. Така шкала дозволяє класифікувати загрози за ступенем їх імовірності реалізації та рівнем потенційного впливу, що є критично важливим для обґрунтованого прийняття управлінських рішень в умовах динамічного ризикового середовища. Відповідна шкала має включати наступні значення рівнів ризику:

- низький рівень ризику – відсутність суттєвих загроз або низька ймовірність виникнення негативних наслідків;
- середній рівень ризику – наявність окремих потенційних загроз, які за певних умов можуть призвести до помірного негативного впливу;
- високий рівень ризику – висока ймовірність реалізації значущих загроз, що можуть мати серйозні негативні наслідки для фінансової стабільності та функціонування підприємства.

У моделі фінансової безпеки визначення рівня ризику ґрунтувалося на прогнозованій ймовірності банкрутства підприємства. З урахуванням поширених аналітичних підходів до оцінювання кредитоспроможності та ризику неплатоспроможності, зокрема методології BNI 4.0 [13], були визначені такі порогові значення:

- низький ризик – якщо ймовірність банкрутства становить менше ніж 30%;
- середній ризик – у межах від 30% до 70%;
- високий ризик – понад 70%.

Застосування такого підходу має низку важливих переваг. По-перше, він дозволяє оперативно ідентифікувати рівень загроз для фінансової стабільності підприємства та сформулювати відповідну систему раннього попередження. По-друге, чітке розмежування рівнів ризику спрощує процес ухвалення управлінських рішень: керівництво може своєчасно адаптувати фінансову стратегію, коригувати поточні дії або впроваджувати запобіжні заходи відповідно до класу ризику. По-третє, такий підхід сприяє стандартизації оцінювання в межах підприємства, забезпечуючи узгодженість між різними підрозділами та підвищуючи прозорість фінансового моніторингу.

У моделі кадрової безпеки оцінювання рівня ризику здійснювалося на основі агрегованих місячних даних щодо поведінкових аномалій працівників, які можуть свідчити про потенційні внутрішні загрози для підприємства. Такий підхід дозволяє виявляти відхилення в поведінці персоналу, що мають характер системних або повторюваних порушень, які, у свою чергу, можуть бути ознаками нелояльності, зниження дисципліни або наміру спричинити шкоду. З метою формалізації оцінки ризику була визначена наступна градація:

- низький рівень ризику – протягом місяця не зафіксовано жодної аномальної поведінкової дії;
- середній рівень ризику – виявлено одну аномальну дію, яка може свідчити про поодинокий інцидент або тимчасове відхилення;

– високий рівень ризику – зафіксовано дві або більше аномальних дій, що вказує на системну поведінкову проблему або наявність внутрішньої загрози.

Застосування такої моделі дозволяє реалізувати механізм раннього виявлення ризикованих тенденцій у поведінці персоналу, що є важливим елементом у системі проактивного управління економічною безпекою. Це, у свою чергу, сприяє своєчасному реагуванню на потенційні внутрішні загрози, зменшенню їхнього впливу на операційну діяльність підприємства та зміцненню корпоративної стабільності.

Оцінювання стану техніко-технологічної безпеки підприємства здійснювалося на основі інтегрального показника  $I_{tex}$ , який об'єднує оцінки за п'ятьма ключовими критеріями, що представлені в п. 2.2. З метою формалізації рівнів ризику була застосована шкала, яка базується на оберненій відповідності числового значення інтегрального показника певним пороговим межах. Відповідно до цього підходу, було визначено таку градацію:

- низький рівень ризику – значення інтегрального показника перевищує 0,7
- середній рівень ризику – значення показника в межах від 0,3 до 0,7;
- високий рівень ризику – значення показника менше або дорівнює 0,3.

Застосування запропонованого підходу дозволяє оперативно ідентифікувати критичні зони технологічної уразливості та формує об'єктивне підґрунтя для прийняття обґрунтованих управлінських рішень щодо технічної модернізації, підвищення цифрової зрілості підприємства та розвитку цифрових компетенцій персоналу. Для забезпечення практичної реалізації моделі в межах СППР автором розроблено шкалу відповідності рівнів ризику результатам моделювання кожної підсистеми (табл. 2.8).

Заключним етапом функціонування розробленої моделі є формування диференційованих прикладних рекомендацій залежно від ідентифікованого рівня ризику кожної зі складових. Необхідність впровадження саме диференційованих стратегій управління пояснюється тим, що в умовах

цифрової трансформації загрози втрачають ізольований характер. Висока взаємозалежність внутрішніх процесів призводить до того, що локальні порушення (наприклад, критична вразливість в ІТ-інфраструктурі або аномальна поведінка системного адміністратора) можуть миттєво набути системних масштабів і спровокувати фінансову дестабілізацію підприємства.

Таблиця 2.8.

Відповідність рівня ризику результатам моделей економічної безпеки підприємства

| Підсистема економічної безпеки | Критерій оцінювання                             | Низький ризик | Середній ризик | Високий ризик |
|--------------------------------|-------------------------------------------------|---------------|----------------|---------------|
| Фінансова безпека              | Прогнозована ймовірність банкрутства            | < 30%         | 30% – 70%      | > 70%         |
| Кадрова безпека                | Кількість зафіксованих аномальних дій за місяць | 0             | 1              | ≥ 2           |
| Техніко-технологічна безпека   | Значення інтегрального показника                | < 0.7         | 0.3-0.7        | < 0.3         |

Джерело: складено автором

Традиційний інструментарій управління, зорієнтований на компенсацію наслідків «постфактум», у сучасному ризиковому середовищі вже не забезпечує належного рівня адаптивності. Саме тому ключовою перевагою розробленої інформаційної системи є її здатність до динамічної трансформації управлінської стратегії у відповідь на найменші коливання вхідних індикаторів (рис. 2.6).

Таким чином, розроблена інформаційно-логічна система підтримки прийняття рішень враховує як інтегральний стан економічної безпеки підприємства, так і специфічні ризики кожної підсистеми.

Це надає менеджменту варіативний перелік рекомендаційних дій, спрямованих на випереджальне зниження загрози та мінімізацію потенційних втрат у найбільш критичних точках. Деталізований перелік таких заходів, структурований за рівнями ризику, представлено у Додатку В.

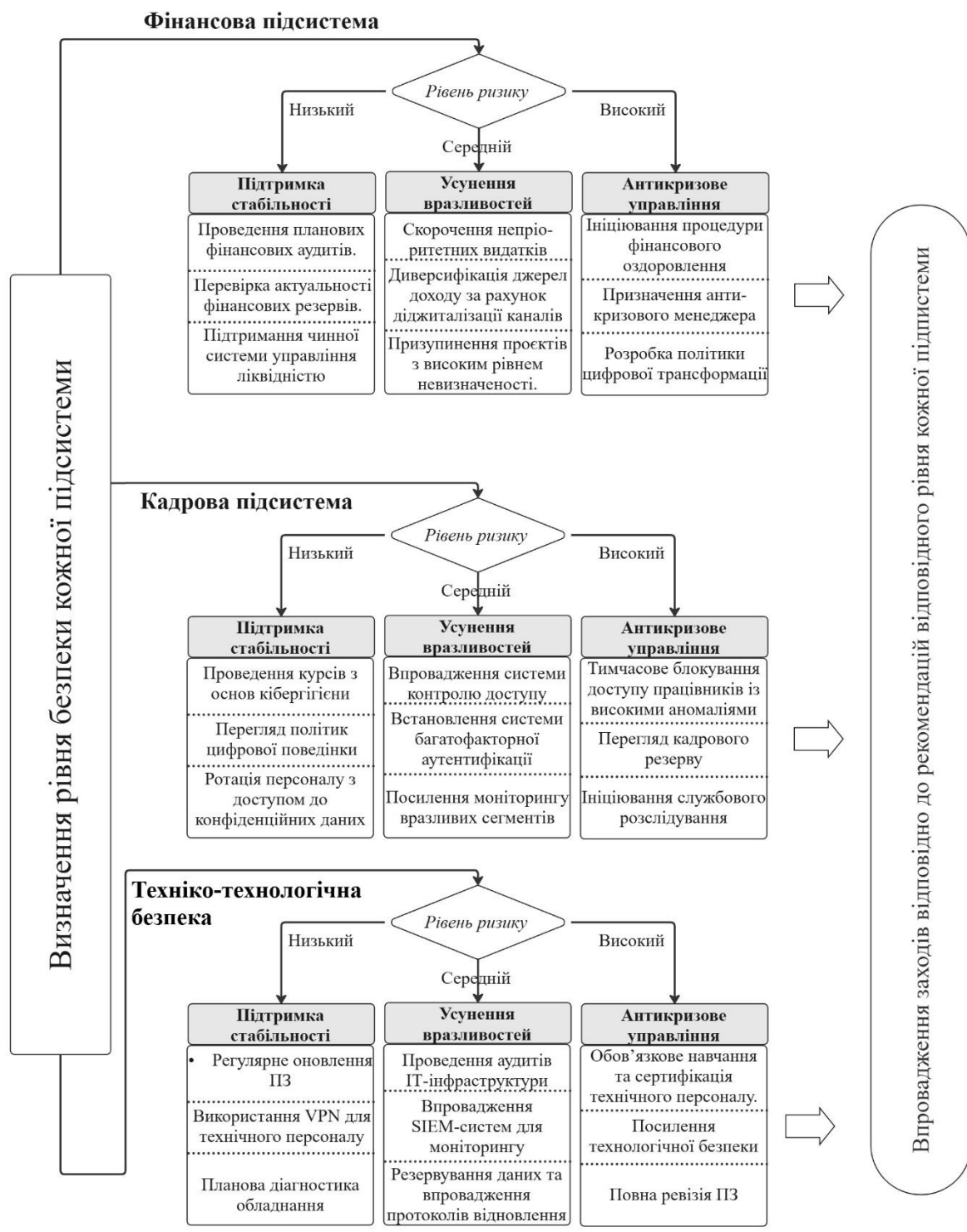


Рис. 2.6. Схема управління системою економічної безпеки підприємства на основі розробленої інформаційної системи.

Джерело: складено автором

Узагальнюючи результати другого розділу, слід зазначити, що запропонована інформаційна модель виступає не лише технічним інструментом обробки даних, а й стратегічним ресурсом зміцнення стійкості підприємства. Її впровадження дозволяє здійснити методологічний перехід від реактивного до проактивного управління ризиками, що є критично важливим для збереження конкурентоспроможності в умовах цифрової економіки.

### **Висновки до другого розділу**

На основі результатів проведеного дослідження у другому розділі, що присвячений аналізу та моделюванню системи економічної безпеки підприємства в умовах цифровізації, сформульовано такі загальні висновки:

1. Узагальнено еволюцію методичних підходів до оцінювання економічної безпеки, у межах якої виявлено закономірний перехід від описового індикативного аналізу до інтелектуальних систем підтримки прийняття рішень. Встановлено, що традиційні статичні моделі, орієнтовані на ретроспективну фінансову звітність, втрачають ефективність у цифровому середовищі через неможливість врахування специфічних ІТ-ризиків та відсутність інструментарію для обробки великих даних у режимі реального часу.

2. Доведено необхідність трансформації математичного апарату моделювання складових економічної безпеки. Обґрунтовано, що для підвищення прогностичної здатності системи класичні статистичні моделі прогнозування банкрутства мають бути інтегровані з алгоритмами машинного навчання. При цьому ідентифікація інсайдерських загроз у кадровому контурі безпеки найбільш достовірно реалізується через моделі виявлення аномалій, що дозволяє фіксувати несанкціоновані відхилення у поведінці персоналу.

3. Розроблено методичний підхід до оцінювання техніко-технологічної складової безпеки на основі ієрархічної моделі та апарату нечіткої логіки, що

забезпечує можливість формалізації якісних експертних оцінок щодо цифрової стійкості підприємства та їх переведення у кількісний інтегральний індекс, що є критично важливим за умов високої невизначеності технологічного середовища.

4. Сформовано архітектуру інформаційної моделі управління економічною безпекою, яка виступає центральним елементом системи підтримки прийняття рішень. Запропонована блочно-модульна структура моделі забезпечує її високу адаптивність із існуючими ERP-системами підприємства, створюючи умови для автоматизованого збору, очищення та аналітичної обробки даних.

5. Обґрунтовано доцільність використання нелінійного інтегрального показника економічної безпеки, який інтегрує результати роботи окремих модулів. Встановлено, що такий підхід дозволяє отримати адекватну оцінку загального стану підприємства, враховуючи синергетичний ефект цифрових ризиків, що не може бути досягнуто за допомогою традиційних адитивних методів згортання показників.

6. Визначено, що перспективним напрямом розвитку розробленого інструментарію є інтеграція великих мовних моделей з існуючими аналітичними модулями, що дозволить підвищити рівень інтерпретованості результатів моделювання для менеджменту та забезпечити генерацію текстових управлінських рекомендацій у режимі реального часу.

Наукові результати дослідження висвітлено у роботах [16, 19, 18, 60, 110, 112].

### **РОЗДІЛ 3. ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ**

#### **3.1. Моделювання фінансової складової системи економічної безпеки підприємства**

У сучасних умовах стрімкої цифровізації економіки та посилення конкурентних викликів, забезпечення економічної безпеки підприємств набуває особливої актуальності. Особливо це стосується фінансової складової, що виступає фундаментом стабільного функціонування та розвитку підприємств. Враховуючи значний вплив цифрових технологій на бізнес-процеси, виникає необхідність комплексного аналізу економічної безпеки підприємств із залученням як фінансових, так і цифрових параметрів.

Першим кроком у дослідженні було формування репрезентативної вибірки підприємств, що дозволяє адекватно відобразити стан фінансової безпеки в секторі переробної промисловості України. Для цього була здійснена систематична робота з офіційними судовими реєстрами, зокрема, із повідомленнями про банкрутство, зареєстрованими у період 2016-2020 років. Вибірка банкрутів сформована на основі типу повідомлень «Повідомлення про визнання боржника банкрутом і відкриття ліквідаційної процедури», що є офіційним підтвердженням кризового стану підприємства [166]. В результаті було ідентифіковано понад 4500 компаній із зазначенням року визнання банкрутства, що дозволило отримати достатньо широку базу для подальшого аналізу. Паралельно із цим, для створення контрольної групи було сформовано вибірку діючих підприємств переробної промисловості відповідно до класифікації КВЕД-2010. Ця база містила понад 78 тисяч компаній із чітко визначеним основним видом діяльності, що забезпечило можливість узгодженого порівняння з підприємствами-банкрутами.

Об'єднання двох баз даних здійснено за унікальним ідентифікатором ЄДРПОУ, що гарантувало коректність ідентифікації підприємств та виключило дублікати. Для подальшого аналізу було обрано підрозділи КВЕД-2010: 10, 11, 13–18, 20, 22–33, які характеризують переробну промисловість. Відбір підрозділів базувався на аналізі частки банкрутств у кожному розділі та їх відносного співвідношення до загальної кількості підприємств, що забезпечило репрезентативність вибірки та збалансованість між кризовими та стабільними підприємствами. З метою забезпечення збалансованості вибірки було відібрано всі компанії-банкрути, а також рівну кількість діючих підприємств, що дало можливість уникнути перекосу в моделюванні та підвищити точність класифікації.

Для побудови моделі прогнозування фінансової безпеки підприємств виникла необхідність у залученні високоякісних та достовірних фінансових даних, що відображають реальний стан компаній протягом певного історичного періоду. Як основне джерело інформації було використано фінансову звітність українських підприємств, отриману за допомогою аналітичного сервісу YouScore від компанії YouControl [11]. Для врахування всіх факторів та побудови універсальної моделі періодом дослідження був обраний від 2014-2020 роки. Обраний часовий діапазон охоплює як відносно стабільний економічний період, так і фазу наростання фінансово-економічної кризи, що забезпечує ширший контекст для аналізу факторів, здатних впливати на фінансову стійкість або, навпаки, призводити до банкрутства суб'єктів господарювання. З огляду на об'єктивні обмеження доступу до актуальної фінансової інформації внаслідок запровадження воєнного стану в Україні та істотного порушення звичних економічних процесів у післякризові роки, дані за 2021 рік і пізніше були свідомо виключені з аналізу. Такий підхід дозволив забезпечити високу якість вхідних даних, уникнути спотворень у результатах і зосередитися на стабільнішому та системно доступному інформаційному масиві.

Для підприємств-банкрутів були відібрані дані за період від чотирьох до двох років до дати банкрутства, що відповідає міжнародним практикам досліджень банкрутства [6, 53, 57], і дозволяє оцінити фінансовий стан підприємств у найбільш критичний період. Для діючих підприємств використано всю доступну інформацію за цей період, що дало змогу сформувати повний профіль фінансового стану кожного підприємства. Зібрані дані включали показники з форм №1 («Баланс») та №2 («Звіт про фінансові результати»), які були основою для формування фінансових індикаторів. Кожен запис у базі відповідав одному рядку звітності окремої компанії за певний рік, загальна кількість записів склала близько 100 тисяч, що забезпечило статистичну надійність проведеного аналізу.

З метою надання побудованій моделі прикладного змісту, а також забезпечення консистентності та однорідності вхідних даних, на наступному етапі було прийнято рішення використовувати лише один часовий зріз (один рік спостереження) для кожного підприємства у вибірці. Такий підхід дозволяє адаптувати результати дослідження до практичних умов функціонування реального бізнесу, де аналітичні рішення та рекомендації формуються, як правило, на основі найсвіжіших наявних фінансових даних.

Для підприємств, що зазнали банкрутства, було обрано фінансову звітність за два роки до офіційно зафіксованої дати банкрутства. Такий часовий відступ дозволяє уникнути спотворень, які можуть виникати в останній рік перед банкрутством через маніпулятивне управління фінансовою звітністю або суттєві зовнішні впливи, що вже є наслідками критичного фінансового стану. Водночас, обрання саме двохрічного інтервалу дозволяє моделі виявляти передумови фінансової дестабілізації з достатнім часовим горизонтом для реагування. Для компаній, які не потрапили до категорії банкрутів, рік для включення у вибірку було обрано таким чином, щоб забезпечити досягти балансу в розподілі підприємств за роками та уникнути статистичної упередженості, що підтверджується даними, наведеними в табл. 3.1. Таким чином, обраний підхід до формування вибірки сприяв

створенню більш стійкої та прикладної моделі прогнозування, результати якої можуть бути легко інтерпретовані й застосовані в реальному управлінському та фінансовому середовищі.

Таблиця 3.1

Розподіл компаній за роками на основі яких будувались моделі

| Рік  | Кількість компаній не банкрутів | Кількість компаній банкрутів |
|------|---------------------------------|------------------------------|
| 2014 | 82                              | 70                           |
| 2015 | 64                              | 65                           |
| 2016 | 60                              | 50                           |
| 2017 | 67                              | 35                           |
| 2018 | 46                              | 31                           |

Джерело: складено автором

На наступному етапі дослідження здійснюється формування набору фінансових показників, які стануть основою для побудови фінансових індикаторів. Ці індикатори, у свою чергу, виступатимуть ключовими змінними у процесі моделювання рівня фінансової безпеки підприємств. Формування цього набору є критично важливим, оскільки саме вибір вхідних змінних значною мірою визначає якість і прогностичну здатність побудованої моделі.

Для забезпечення релевантності та повноти вибірки було визначено 17 базових фінансових показників, які будуть слугувати основою для побудови фінансових індикаторів. Відповідно до цього, було використано дані форм фінансової звітності №1 (Баланс) та №2 (Звіт про фінансові результати). Їх відповідність офіційній фінансовій звітності наведена в додатку Б. Це дозволяє гарантувати узгодженість даних та їхню відповідність офіційно затвердженій фінансовій документації підприємств.

Заключним етапом підготовки є побудова фінансових індикаторів – узагальнених метрик, що акумулюють інформацію з окремих показників і краще відображають структурні характеристики фінансового стану підприємства. Вибір цих індикаторів здійснювався на основі критичного аналізу і вітчизняних досліджень з проблеми прогнозування банкрутства, а

також відповідних наукових публікацій щодо оцінювання фінансової безпеки, який наведений у п. 2.1. Додатковим орієнтиром слугували емпіричні дослідження, що демонстрували вплив окремих фінансових характеристик на здатність підприємства зберігати стійкість до зовнішніх та внутрішніх ризиків, що були проаналізовані у п. 2.2. У результаті був сформований узагальнений список ключових індикаторів, представлений у табл. 3.2.

Таблиця 3.2

Фінансові змінні моделі прогнозування банкрутств українських компаній

| Змінна | Формула                                                                                         | Економічна сутність                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| X1     | Чистий прибуток /<br>Загальна вартість активів                                                  | Є вимірником ефективності використання активів підприємства, і показує дохід, одержаний на грошову одиницю активів.    |
| X12    | Валовий прибуток /<br>Загальні поточні зобов'язання                                             | Показує, наскільки компанія здатна покрити свої короткострокові зобов'язання за рахунок валового прибутку.             |
| X18    | Валовий прибуток /<br>Загальна вартість активів                                                 | Показує ефективність використання загальних активів компанії для генерування валового прибутку.                        |
| X19    | Валовий прибуток /<br>Загальний виторг                                                          | Показує частку валового прибутку у загальному обсязі продажів, що свідчить про здатність компанії генерувати прибуток. |
| X20    | Запаси / Загальний виторг                                                                       | Допомагає оцінити ефективність управління запасами та швидкість їх обертання                                           |
| X21    | Загальний виторг<br>поточного року /<br>Загальний виторг<br>минулого року                       | Показує темп зростання продажів, дозволяючи оцінити динаміку розвитку бізнесу                                          |
| X23    | Чистий прибуток /<br>Загальний виторг                                                           | Відображає прибутковість компанії після вирахування всіх витрат і податків.                                            |
| X24    | Валовий прибуток за 3<br>роки / Загальний виторг                                                | Відображає ефективність використання активів для генерування прибутку в середньостроковій перспективі                  |
| X3     | (Загальні оборотні активи<br>- Загальні поточні<br>зобов'язання) / Загальна<br>вартість активів | Відображає здатність компанії покривати свої зобов'язання за рахунок найбільш ліквідних активів.                       |
| X30    | (Загальні пасиви - Гроші<br>та їх еквіваленти) /<br>Загальний виторг                            | Допомагає оцінити навантаження на виручку компанії з боку її боргових зобов'язань.                                     |
| X4     | Загальні оборотні активи<br>/ Загальні поточні<br>зобов'язання                                  | Відображає короткострокову фінансову стійкість та ліквідність компанії                                                 |
| X47    | Запаси / Собівартість<br>реалізованої продукції                                                 | Показує ефективність управління запасами відносно витрат на виробництво продукції                                      |

|     |                                                                     |                                                                                                                                                           |
|-----|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| X50 | Загальні оборотні активи / Загальні зобов'язання                    | Показує здатність компанії покривати свої загальні зобов'язання за рахунок поточних активів                                                               |
| X52 | Загальні поточні зобов'язання / Собівартість реалізованої продукції | Дозволяє оцінити, яка частка витрат фінансується за рахунок короткострокових зобов'язань                                                                  |
| X53 | Загальний власний капітал / Основні засоби                          | Відображає, якою мірою власний капітал покриває довгострокові інвестиції компанії                                                                         |
| X59 | Загальні довгострокові зобов'язання / Загальний власний капітал     | Відображає рівень рентабельності власного капіталу за різних варіантів структури капіталу                                                                 |
| X60 | Загальний виторг / Запаси                                           | Відображає ефективність управління запасами і швидкість їх реалізації                                                                                     |
| X61 | Загальний виторг / Дебіторська заборгованість                       | Показує, як ефективно компанія управляє своєю дебіторською заборгованістю                                                                                 |
| X64 | Загальний виторг / Основні засоби                                   | Відображає продуктивність необоротних активів у створенні доходів                                                                                         |
| X74 | Гроші та їх еквіваленти / Загальні поточні зобов'язання             | Показує здатність компанії покривати свої короткострокові зобов'язання виключно за рахунок наявних грошових коштів                                        |
| X8  | Загальний власний капітал / Загальні пасиви                         | Показує, наскільки компанія фінансується власними коштами порівняно з залученими зобов'язаннями, що є показником її фінансової стійкості та незалежності. |
| X9  | Загальний виторг / Загальна вартість активів                        | Характеризує ефективність використання ресурсів, залучених для організації виробництва                                                                    |

До нього увійшли, зокрема:

- індикатори динаміки розвитку компанії, зокрема річне зростання обсягів продажу та прибутковості за останні три роки;
- показники прибутковості, як-от коефіцієнт фінансової незалежності та загальний коефіцієнт рентабельності;
- індикатори ефективності використання капіталу, включаючи коефіцієнт фінансового левериджу та коефіцієнт поточної ліквідності;
- інші допоміжні показники, що відображають платоспроможність, рівень боргового навантаження тощо.

Варто зазначити, що змінна, пов'язана зі сферою діяльності підприємств (згідно з кодами КВЕД-2010), не була включена до остаточного переліку змінних. Причиною цього стала обмеженість обсягів вибірки: наявна кількість

компаній не дозволяла отримати статистично значущі висновки для кожної групи видів економічної діяльності.

Обробка даних передбачала очищення від змінних із понад 30% пропущених значень, що дозволило уникнути викривлення результатів через недостатню інформацію. Решта пропущених значень була заповнена медіаною відповідних змінних, що є стандартною практикою в обробці фінансових даних та зменшує вплив екстремальних значень [55, 86].

З метою уніфікації масштабів змінних було проведено стандартизацію, що є необхідним кроком для коректної роботи алгоритмів машинного навчання, особливо тих, що чутливі до масштабу даних [45]. У даному дослідженні стандартизацію було здійснено із використанням методу StandardScaler, який є одним із найбільш поширених способів нормалізації даних у статистичному аналізі та машинному навчанні. Суть методу полягає у перетворенні кожного значення змінної таким чином, щоб отриманий набір мав нульове середнє значення, та стандартне відхилення ( $\sigma$ ), яке дорівнює 1. Для цього використовується наступна формула:

$$z_i = \frac{x_i - \mu}{\sigma}$$

де

$x_i$  – початкове значення змінної,

$\mu$  – середнє значення,

$\sigma$  – стандартне відхилення вибірки,

$z_i$  – стандартизоване значення змінної.

Одним із ключових етапів побудови якісної моделі фінансової складової системи економічної безпеки підприємства є перевірка статистичних припущень щодо вихідних змінних, зокрема виявлення та усунення проблеми мультиколінеарності. Мультиколінеарність виникає у випадках, коли дві або більше незалежні змінні в моделі мають між собою сильний лінійний зв'язок, що призводить до викривлення оцінок регресійних коефіцієнтів та зниження точності прогнозування [182]. Попередній аналіз кореляційної структури

даних дозволив ідентифікувати змінні з високим ступенем парної кореляції ( $|r| > 0.8$ ), що свідчило про наявність потенційної мультиколінеарності. Для її усунення було застосовано метод скорочення змінних на основі кореляційної матриці. Зокрема, змінні з надмірною взаємною залежністю були виключені з моделі, натомість залишено ті, що забезпечують найвищу інформаційну насиченість при збереженні статистичної стабільності. Такий підхід дозволив зменшити ризик надлишкового включення пов'язаних показників та підвищити надійність результатів подальшого аналізу (рис. 3.1).

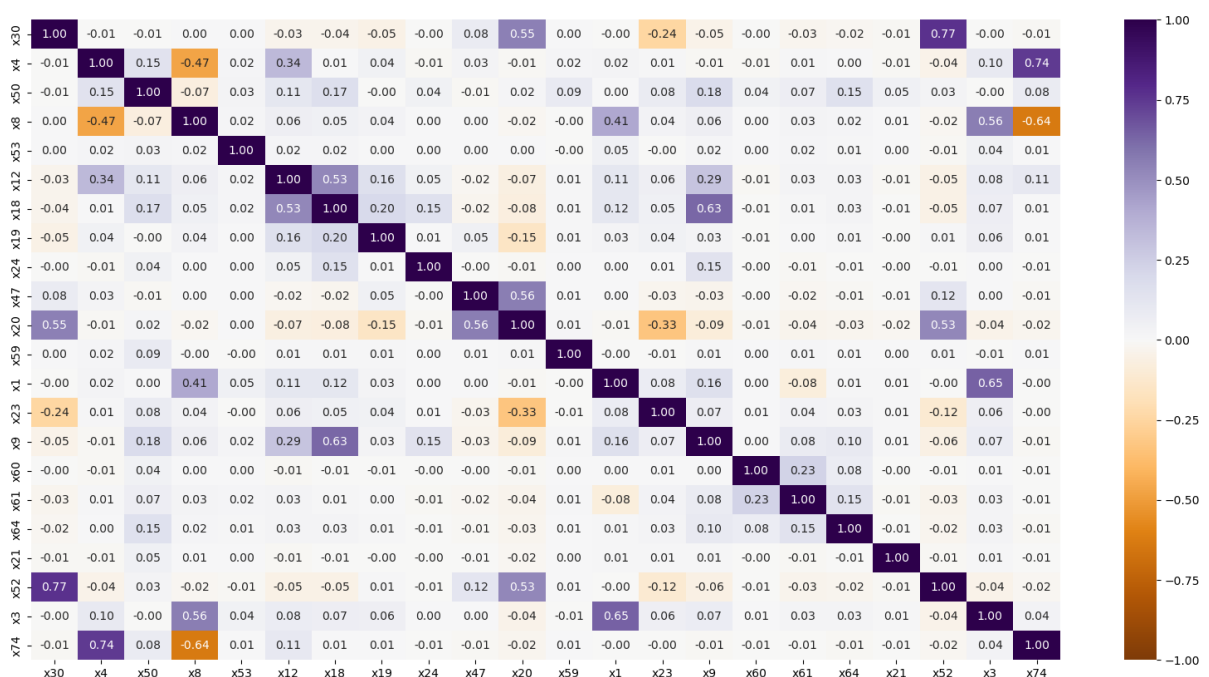


Рис. 3.1. Графік попарної кореляції фінансових змінних у сформованому наборі даних.

Джерело: складено автором.

У результаті цього етапу було сформовано скоригований набір предикторів, який забезпечує оптимальне співвідношення між точністю моделі та її економічною інтерпретованістю. Це стало підґрунтям для подальшого етапу, а саме побудови моделі інтегральної оцінки фінансової безпеки підприємства з використанням обраного множини релевантних змінних.

Таким чином, був сформований набір даних для 570 українських компаній, який включає 22 фінансові індикатори за один рік діяльності компанії в період 2014-2018 років. Важливо зазначити, що 44% компаній цієї вибірки стали банкрутами, що робить набір даних збалансованим і придатним для подальшого економіко-математичного моделювання.

Для побудови та подальшої валідації моделі прогнозування банкрутства, вся вибірка була поділена на навчальну та тестову підвибірки у співвідношенні 70% до 30% відповідно. При цьому було збережено первинне співвідношення класів – кількість компаній-банкрутів та небанкрутів у кожній із підвибірок. Такий стратифікований підхід до розподілу забезпечив репрезентативність кожної підвибірки та дозволив уникнути потенційного перекосу у розподілі цільової змінної, що, у свою чергу, є критичним для об'єктивної оцінки узагальнювальної здатності моделі.

Постановка задачі прогнозування банкрутства була реалізована як задача бінарної класифікації, де цільова змінна приймала значення «1» у випадку, якщо компанія визнана банкрутом, і «0» - якщо ні. Це в свою чергу дозволило застосувати широкий спектр сучасних алгоритмів машинного навчання, зокрема як лінійних моделей так і більш складних ансамблевих методів. Крім того, постановка у вигляді задачі класифікації спрощує інтерпретацію результатів моделі для подальшого практичного застосування в управлінні ризиками та прийнятті рішень на підприємствах.

У зв'язку з тим, що завдання прогнозування ймовірності банкрутства підприємства зводиться до задачі бінарної класифікації, існує широкий спектр методів машинного навчання, які можуть бути застосовані для вирішення цієї проблеми. Метою даного етапу дослідження стало не лише побудова коректної прогностичної моделі, а й порівняння ефективності різних алгоритмів для вибору оптимального підходу з точки зору точності, стійкості та практичної інтерпретованості. Для досягнення цієї мети було відібрано п'ять алгоритмів, які охоплюють як класичні, так і сучасні підходи до класифікації, які детально описано у п. 2.2, зокрема було використано наступні моделі: логістична

регресія, Random Forest, XGBoost, Support Vector Machines (SVM) та штучні нейронні мережі (ANN)

Оцінювання ефективності моделей здійснювалося за допомогою кількох метрик, кожна з яких дозволяє охопити різні аспекти якості класифікації. Особлива увага була приділена метрикам, чутливим до класового дисбалансу та ваги помилок. Враховуючи, що в задачі прогнозування банкрутства помилково негативний результат може призвести до серйозних втрат (тобто компанія, що є банкрутом, неправильно класифікується як здорова), модель має максимально зменшувати ймовірність таких помилок. Відповідно, основна увага приділялась Recall та метрикам, що її підсилюють [140].

З цією метою були обрані наступні ключові метрики: Accuracy, F-beta 2, ROC AUC. Найбільш важливою є метрика F-beta 2, яка є модифікація F-міри, яка надає вдвічі більшу вагу Recall у порівнянні з Precision. Це дозволяє оцінити здатність моделі виявляти максимум потенційних банкрутів, навіть за рахунок зниження точності. Формула розрахунку цієї метрики наступна:

$$F\ score = (1 + \beta^2) \cdot \frac{P \cdot R}{(\beta^2 \cdot P) + R}$$

$$\text{де } \beta = 2, P = \frac{TP}{TP+FP}, R = \frac{TP}{TP+FN},$$

*TP (True Positives)* – правильно визначені банкрути,

*TN (True Negatives)* – правильно визначені небанкрути,

*FP (False Positives)* – хибні визначення банкрутів,

*FN (False Negatives)* – пропущені реальні банкрути.

Наступною є метрика Accuracy, яка відображає загальний рівень правильності передбачень моделі. Вона показує частку всіх правильно класифікованих випадків серед загальної кількості спостережень. Формула для розрахунку наступна:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

І третьою метрикою для оцінки якості моделей прогнозування банкруства була ROC AUC, що відображає загальну здатність моделі розрізняти два класи незалежно від вибору порогу.

Моделі навчалися на тренувальній вибірці із застосуванням 5-кратної крос-валідації [27], що дозволило мінімізувати вплив випадковості розподілу спостережень та покращити узагальнювальну здатність моделі. Остаточні результати були усереднені по фолдах та представлені в табл. 3.3.

Таблиця 3.3

Результати оцінки всіх моделей на валідаційному наборі даних

| Модель              | Accuracy | ROC AUC | F-beta 2 |
|---------------------|----------|---------|----------|
| Логістична регресія | 73,2%    | 80,5%   | 65,1%    |
| SVM                 | 69,7%    | 81,0%   | 61,0%    |
| Нейронна мережа     | 75,9%    | 81,5%   | 69,6%    |
| RandomForest        | 80,0%    | 85,8%   | 77,6%    |
| XGBoost             | 79,0%    | 85,9%   | 75,3%    |

Джерело: складено автором.

На основі проведеного порівняльного аналізу встановлено, що моделі Random Forest та XGBoost продемонстрували найкращі результати за основними метриками, зокрема високий рівень F-beta 2 та AUC. У зв'язку з цим, саме ці два алгоритми були обрані для подальшого поглибленого аналізу, зокрема для побудови інтерпретованих моделей та формування практичних рекомендацій щодо оцінювання фінансової стійкості підприємств.

З метою підвищення якості моделей та уникнення випадкового підбору гіперпараметрів, для алгоритмів Random Forest та XGBoost було застосовано процедуру Grid Search у поєднанні з 5-кратною крос-валідацією [70]. Grid Search – є методикою повного перебору фіксованого набору можливих значень гіперпараметрів моделі, що дозволяє провести систематичний аналіз їхнього впливу на якість навчання. У межах цього підходу для кожної можливої

комбінації гіперпараметрів модель навчається на тренувальних підвибірках і оцінюється за допомогою крос-валідації, що забезпечує надійність та узагальнюваність результатів. Такий підхід дозволяє систематично дослідити простір параметрів і обрати комбінацію, що забезпечує найкращі результати на тренувальних підвибірках із належною перевіркою узагальнюючої здатності. Для моделі Random Forest було проаналізовано наступні гіперпараметри:

$max\_depth \in \{3, 5, 10\}$ ,  
 $min\_samples\_split \in \{2, 5, 10\}$ ,  
 $n\_estimators \in \{2, 5, 10\}$ .

Для моделі XGBoost досліджувалися наступні комбінації параметрів:

$max\_depth \in \{3, 5, 10\}$ ,  
 $learning\_rate \in \{0.1, 0.01, 0.001\}$ ,  
 $subsample \in \{0.5, 0.7, 1\}$ .

Найкраща конфігурація, яка забезпечила максимальне значення accuracy для моделі Random Forest була при

$max\_depth = 3, min\_samples\_split = 2, n\_estimators = 10$ ,

а для моделі XGBoost при:

$learning\_rate = 0.1, max\_depth = 3, subsample = 0.5$ .

Результати оцінки моделі при оптимальних параметрах представлені у табл. 3.4.

Таблиця 3.4

Результати оцінки найкращих моделей після процедури пошуку найкращих гіперпараметрів

| Метрика  | Random forest |          | XGBoost      |          |
|----------|---------------|----------|--------------|----------|
|          | Тренувальний  | Тестовий | Тренувальний | Тестовий |
| Accuracy | 83,21%        | 80,70%   | 96,24%       | 85,96%   |
| F Beta 2 | 79,61%        | 76,61%   | 95,56%       | 81,30%   |
| ROC AUC  | 82,76%        | 80,19%   | 96,16%       | 85,31%   |

Джерело: складено автором.

Результати, наведені в табл. 3.4, демонструють, що всі показники якості моделі XGBoost на навчальній вибірці істотно перевищують відповідні показники на тестовій. Така різниця є типовим індикатором перенавчання, що свідчить про здатність моделі занадто точно запам'ятовувати навчальні дані, замість виявлення узагальнених закономірностей. Це, у свою чергу, негативно впливає на генералізацію моделі та знижує точність її прогнозів для нових компаній, які не входили до початкової вибірки.

З огляду на важливість практичного застосування моделі у широкому спектрі фінансових сценаріїв, зменшення перенавчання стало критичним завданням. Теоретично найбільш ефективним засобом подолання цієї проблеми є збільшення обсягів навчальної та тестової вибірки, однак у межах наявного дослідження така можливість була обмежена через дефіцит якісних та репрезентативних фінансових даних. У зв'язку з цим, наступним етапом дослідження стало застосування регуляризаційних методів, зокрема L1 (Lasso) та L2 (Ridge) регуляризацій, які дозволяють обмежити складність моделі, зменшити ризик перенавчання та покращити узагальнюючу здатність [54]. L1-регуляризація додає до функції втрат штраф, пропорційний абсолютному значенню коефіцієнтів моделі. Такий підхід сприяє зануленню деяких параметрів, що дозволяє автоматично здійснювати відбір найбільш значущих ознак та отримувати розріджені моделі. L2-регуляризація натомість додає штраф, пропорційний квадратам значень коефіцієнтів, що стимулює модель зменшувати ваги параметрів рівномірно. Це дозволяє уникати надмірного впливу окремих змінних і забезпечує більш стійке навчання в умовах мультиколінеарності. Для коректного налаштування регуляризаційних параметрів було використано Grid Search із 5-кратною крос-валідацією, що забезпечило надійність та об'єктивність процесу оптимізації.

Аналіз результатів засвідчив, що L2-регуляризація не забезпечила суттєвого зменшення перенавчання, оскільки навіть при максимальних значеннях параметра різниця між оцінками на тренувальних та валідаційних наборах залишалася значною (рис. 3.2).

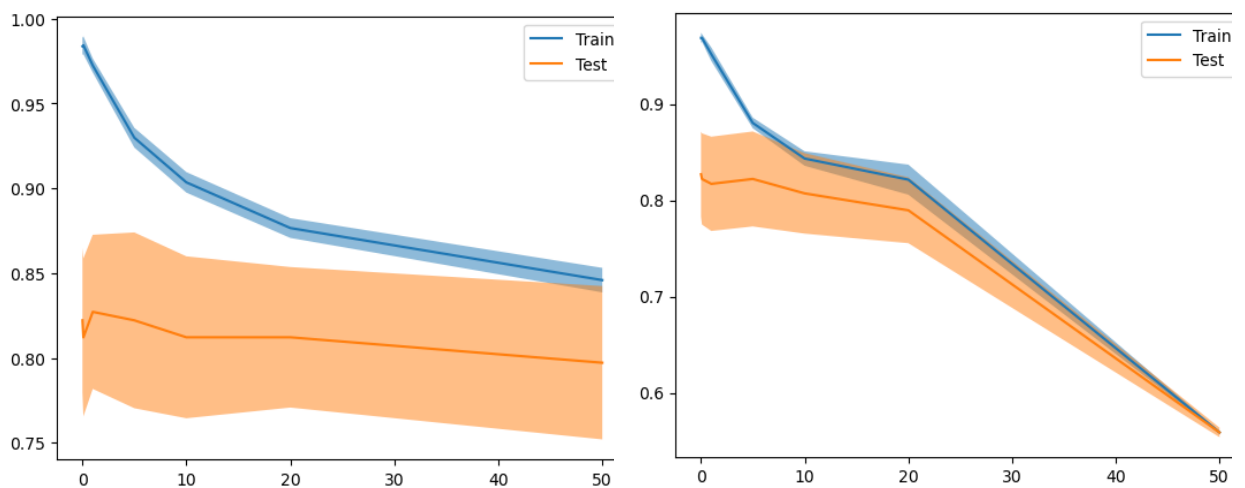


Рис. 3.2. Оцінка моделі на навчальній та валідаційній вибірках в залежності від значення параметра L2 регуляризації (ліва) та L1 регуляризації (права).

Джерело: складено автором.

Це свідчить про обмежену ефективність L2-підходу в даному випадку. Натомість, застосування L1-регуляризації з параметром  $\alpha = 10$  дозволило суттєво знизити розрив між показниками якості на навчальній та валідаційній вибірках. Більше того, середні значення Ассигасу для обох підвибірок опинилися в межах довірчих інтервалів, що вказує на досягнення бажаного балансу між точністю та узагальненням (табл. 3.5).

Таблиця 3.5

Результати оцінки найкращих моделей після процедури пошуку найкращих гіперпараметрів та регуляризації

| Метрика  | Random forest |          | XGBoost      |          |
|----------|---------------|----------|--------------|----------|
|          | Тренувальний  | Тестовий | Тренувальний | Тестовий |
| Accuracy | 83,21%        | 80,70%   | 83,96%       | 81,29%   |
| F Beta 2 | 79,61%        | 76,61%   | 81,44%       | 77,75%   |
| ROC AUC  | 82,76%        | 80,19%   | 83,67%       | 80,85%   |

Джерело: складено автором

Отже, модель XGBoost з L1-регуляризацією ( $\alpha = 10$ ) продемонструвала найкращі результати як у межах вибірки, так і при оцінці

узагальнюючої здатності, тому саме вона була обрана як фінальна модель для подальшого аналізу.

Наступним етапом розробки моделі стало врахування факторів цифровізації та оцінка їхнього потенційного впливу на фінансово-економічну безпеку підприємств. Враховуючи сучасні трансформації бізнес-середовища, пов'язані з цифровою економікою, виникла потреба у розширенні стандартних фінансових моделей додатковими змінними, що характеризують ступінь цифрового розвитку компаній. З метою кількісної оцінки цифровізації було розроблено спеціальну систему оцінювання рівня діджиталізації підприємств на основі відкритих джерел.

Методологія передбачала побудову трьох критеріальних індикаторів, кожен з яких був представлений у вигляді кількісної шкали, що дозволила сформулювати нові змінні для подальшого використання у моделі. Оцінювання проводилося відповідно до наступних критеріїв:

1. Інтернет-присутність (змінна *dg\_1\_online\_presence*):

0 балів – повна відсутність веб-сайту чи будь-яких згадок про компанію в мережі Інтернет.

1 бал – наявність згадок про компанію на сторонніх платформах без офіційного сайту.

2 бали – функціональний, але базовий веб-сайт із обмеженою інформацією.

3 бали – повнофункціональний веб-сайт із повною інформацією про діяльність, продукти, послуги, контактні дані тощо.

2. Присутність у соціальних мережах (змінна *dg\_2\_social\_media*):

0 балів – відсутність акаунтів у соціальних мережах.

1 бал – наявність акаунтів, але з низькою активністю (мала кількість публікацій, відгуків, підписників).

2 бали – активне ведення сторінок з регулярними оновленнями, комунікацією з клієнтами та ознаками залучення аудиторії.

3. Можливості електронної комерції (змінна *dg\_3\_ecommerce*):

0 балів – відсутність можливості придбати товари чи послуги онлайн.

1 бал – часткова присутність в електронній комерції (перелік товарів без можливості онлайн-оплати або присутність на сторонніх маркетплейсах).

2 бали – повноцінна реалізація e-commerce на власному сайті (кошик, особисті кабінети, кілька способів оплати, рекомендаційні алгоритми тощо).

Для збору даних було застосовано комплексний ручний аналіз, що був проведений за допомогою сервісу Wayback Machine [51], а також інші відкриті джерела в мережі Інтернет. Оцінювання проводилося з урахуванням часового зрізу, який відповідає року аналізованої фінансової звітності компанії. У межах цього процесу:

визначалась наявність веб-сайту або його копії в архіві;

здійснювалась перевірка структури сайту на відповідність переліку функціональних критеріїв;

оцінювалась активність у соціальних мережах шляхом пошуку через сайт компанії або через самі платформи соціальних медіа.

У результаті оцінювання, близько 30% компаній отримали ненульові оцінки хоча б за одним із трьох критеріїв, що свідчить про нерівномірний рівень цифровізації серед досліджуваних підприємств.

Попарний кореляційний аналіз, який представлений на рис. 3.3, показав відсутність статистично значущих кореляцій між змінними цифровізації та фінансовими індикаторами, що дозволяє використовувати їх як незалежні предиктори без ознак мультиколінеарності. Водночас було виявлено помірний рівень взаємозв'язку між змінними *dg\_1\_online\_presence* та *dg\_3\_ecommerce*, однак значення коефіцієнта кореляції не перевищило 0,8, що дозволяє залишити обидва показники в моделі.

Для подальшого використання у прогностичній моделі всі змінні цифровізації були стандартизовані за методикою, аналогічною до тієї, що застосовувалась для фінансових індикаторів. Після формування та стандартизації змінних, що характеризують рівень цифровізації підприємств, було здійснено інтеграцію цих факторів у прогностичну модель. З цією метою

використано дві найкращі моделі, які показали найвищі результати на попередньому етапі моделювання з наступними параметрами:

Random Forest:  $max\_depth = 3, min\_samples\_split = 2, n\_estimators = 10;$

XGBoost:  $max\_depth = 3, learning\_rate = 0.1, subsample = 0.5.$

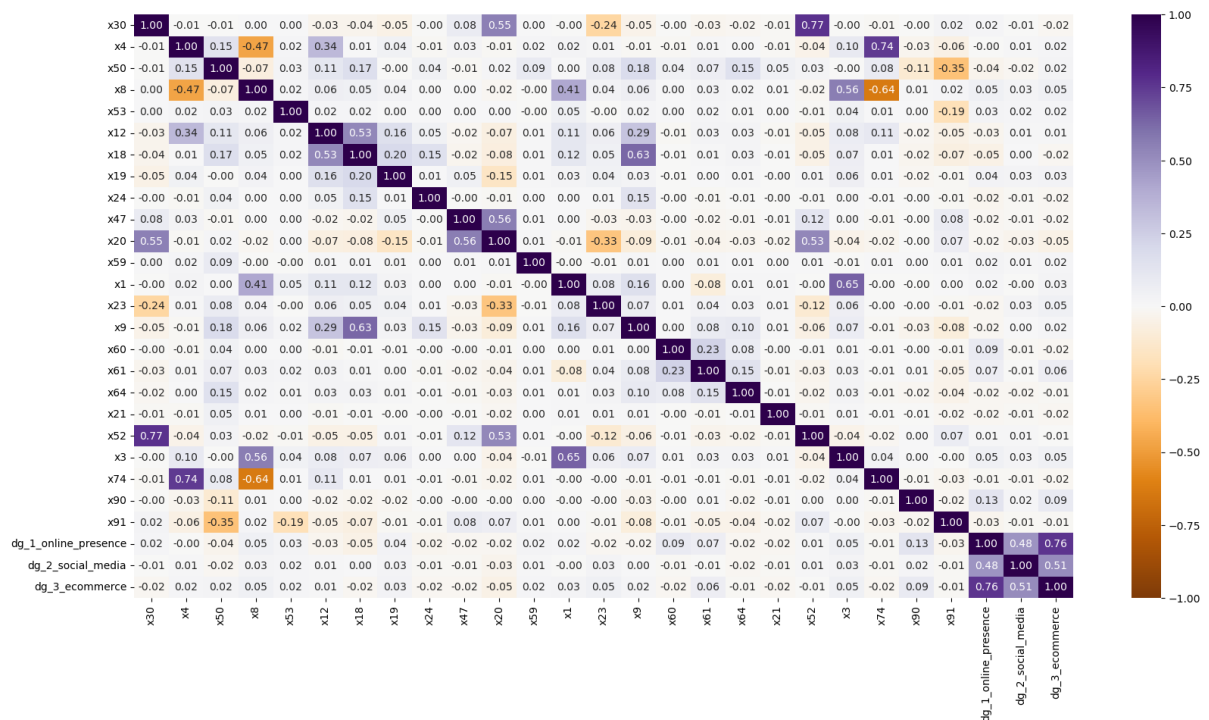


Рис. 3.3. Графік попарної кореляції фінансових змінних і змінних цифровізації у сформованому наборі даних.

Джерело: складено автором.

Оцінка результатів моделей з урахуванням змінних цифровізації наведена в табл. 3.6.

Як видно з табл. 3.6, врахування змінних цифровізації призвело до покращення результатів обох моделей на тренувальній вибірці приблизно на 1%, що свідчить про зростання обґрунтованості класифікації. Для моделі Random Forest значення на тестовій вибірці практично не змінилися, тоді як XGBoost показав покращення за всіма метриками на тестовій вибірці. До того ж, саме модель XGBoost показує результати майже на 3% кращі на тестовій

вибірці ніж Random Forest, тому саме вона було визнано найкращою для прогнозування фінансової безпеки підприємств з врахуванням факторів цифрової трансформації, і саме її було обрано для подальшого аналізу.

Таблиця 3.6

Результати оцінки найкращих моделей з використанням змінних цифровізації

| Метрика  | Random forest |          | XGBoost      |          |
|----------|---------------|----------|--------------|----------|
|          | Тренувальний  | Тестовий | Тренувальний | Тестовий |
| Accuracy | 83,71%        | 80,11%   | 84,21%       | 82,46%   |
| F Beta 2 | 80,18%        | 76,41%   | 81,53%       | 78,17%   |
| ROC AUC  | 83,27%        | 79,67%   | 83,89%       | 81,89%   |

Джерело: складено автором.

На наступному етапі дослідження проведено аналіз вагомості (значущості) входних змінних у межах побудованої моделі XGBoost. З метою візуалізації та кількісного оцінювання внеску кожного детермінанта у процес формування прогнозних значень моделлю побудовано діаграму значущості ознак (рис. 3.4) [69]. Оцінювання ієрархії значущості є критично важливим елементом аналізу, оскільки дозволяє ідентифікувати ключові фактори, які алгоритм використовує для диференціації станів фінансової безпеки та прогнозування ризику банкрутства суб'єктів господарювання.

Згідно з отриманими результатами, найбільший вплив на результуючий показник класифікації чинять такі змінні:

- $x_{12}$  – коефіцієнт відношення валового прибутку до поточних зобов'язань;
- $x_{53}$  – коефіцієнт покриття необоротних активів власним капіталом;
- $x_{18}$  – коефіцієнт валової рентабельності;
- $x_8$  – коефіцієнт фінансової незалежності;
- $dg\_3\_ecommerce$  – коефіцієнт електронної комерції.

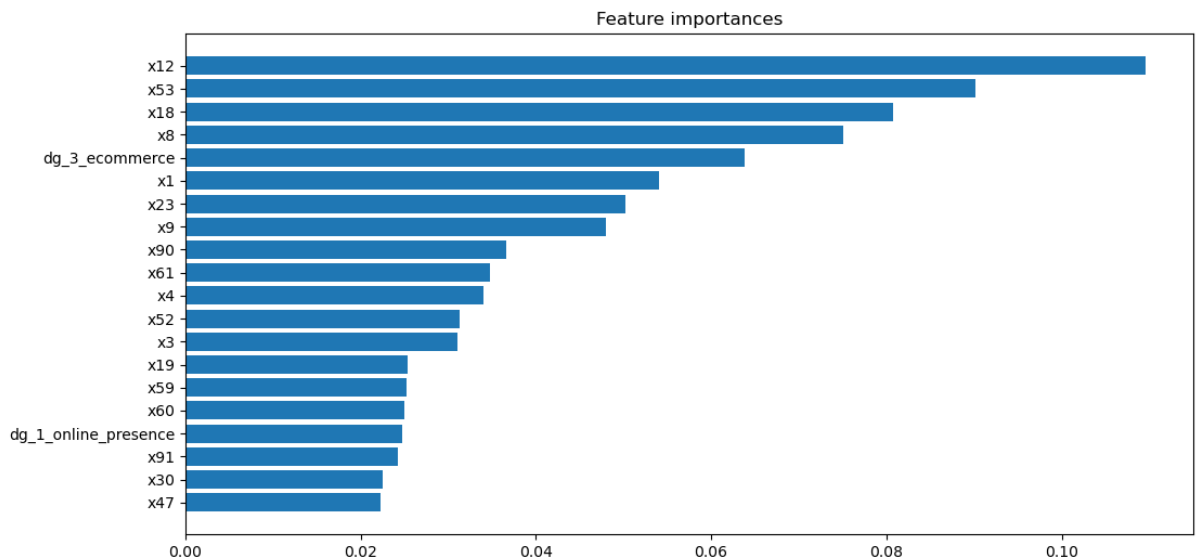


Рис. 3.4. Матриця значимості змінних у фінальній моделі XGBoost.

Джерело: складено автором.

Високий ранг змінної *dg\_3\_ecommerce* у загальній структурі моделі підтверджує наукову гіпотезу про доцільність інтеграції параметрів цифрової трансформації у систему оцінювання економічної безпеки підприємства. Поряд із цим, індикатор інтернет-присутності (*dg\_1\_online\_presence*) також демонструє помірну прогностичну потужність. Водночас встановлено, що показник активності у соціальних мережах (*dg\_2\_social\_media*) не виявляє суттєвого впливу на результати моделювання. Це пояснюється низьким рівнем діджиталізації маркетингових комунікацій на підприємствах переробної промисловості у досліджуваному періоді. Зокрема, репрезентативність даної ознаки обмежена тим, що менше 10 % компаній із вибірки мали офіційні представництва на соціальних платформах, що унеможливило формування стійких статистичних взаємозв'язків у межах даного набору даних.

Водночас слід акцентувати увагу на наявних методичних обмеженнях аналізу значущості ознак: встановлення «ваги» змінної дозволяє визначити її відносну важливість для моделі, проте не надає інформації щодо вектора впливу (позитивного чи негативного) та не дозволяє ідентифікувати критичні порогові зони, у межах яких ризик банкрутства зазнає найбільш істотних змін. З огляду на необхідність досягнення управлінських цілей дослідження, саме ці

аспекти є визначальними для розробки превентивних заходів. Відповідно, наступний етап аналізу спрямовано на ідентифікацію форми та характеру виявлених залежностей.

Завершальною стадією моделювання стало визначення напрямку та інтенсивності впливу кожної змінної на ймовірність втрати фінансової безпеки підприємства. Враховуючи високу нелінійність та складність внутрішньої структури алгоритму XGBoost, що ускладнює безпосередню інтерпретацію параметрів, для розкриття логіки функціонування моделі застосовано метод графіків часткової залежності (PDP). Використання PDP надає можливість оцінювання маржинального ефекту окремої змінної або групи змінних на прогностичні значення цільової змінної шляхом статистичного усереднення впливу всіх інших факторів [71].

Зазначений підхід дозволяє візуалізувати архітектуру взаємозв'язків між вхідними параметрами та результатами моделювання, ідентифікуючи лінійні, монотонні або складні нелінійні тренди. Це є критично важливим для моделей машинного навчання, де взаємодія між змінними має латентний характер. У межах даного дослідження застосування графіків часткової залежності дозволило оцінити динаміку зміни ймовірності банкрутства суб'єкта господарювання залежно від варіації конкретного фінансового чи цифрового показника за умови фіксації значень інших детермінантів на незмінному рівні.

Аналіз результатів побудови графіків часткової залежності (рис. 3.5) підтверджує теоретичну адекватність ідентифікованих взаємозв'язків. У межах даного дослідження найвищу інформативність демонструють змінні, для яких характерні виражені дискретні зміни (скачки) прогностичних значень. Такі показники мають чітку економічну інтерпретацію та можуть розглядатися як дієві управлінські важелі забезпечення фінансової безпеки суб'єкта господарювання.

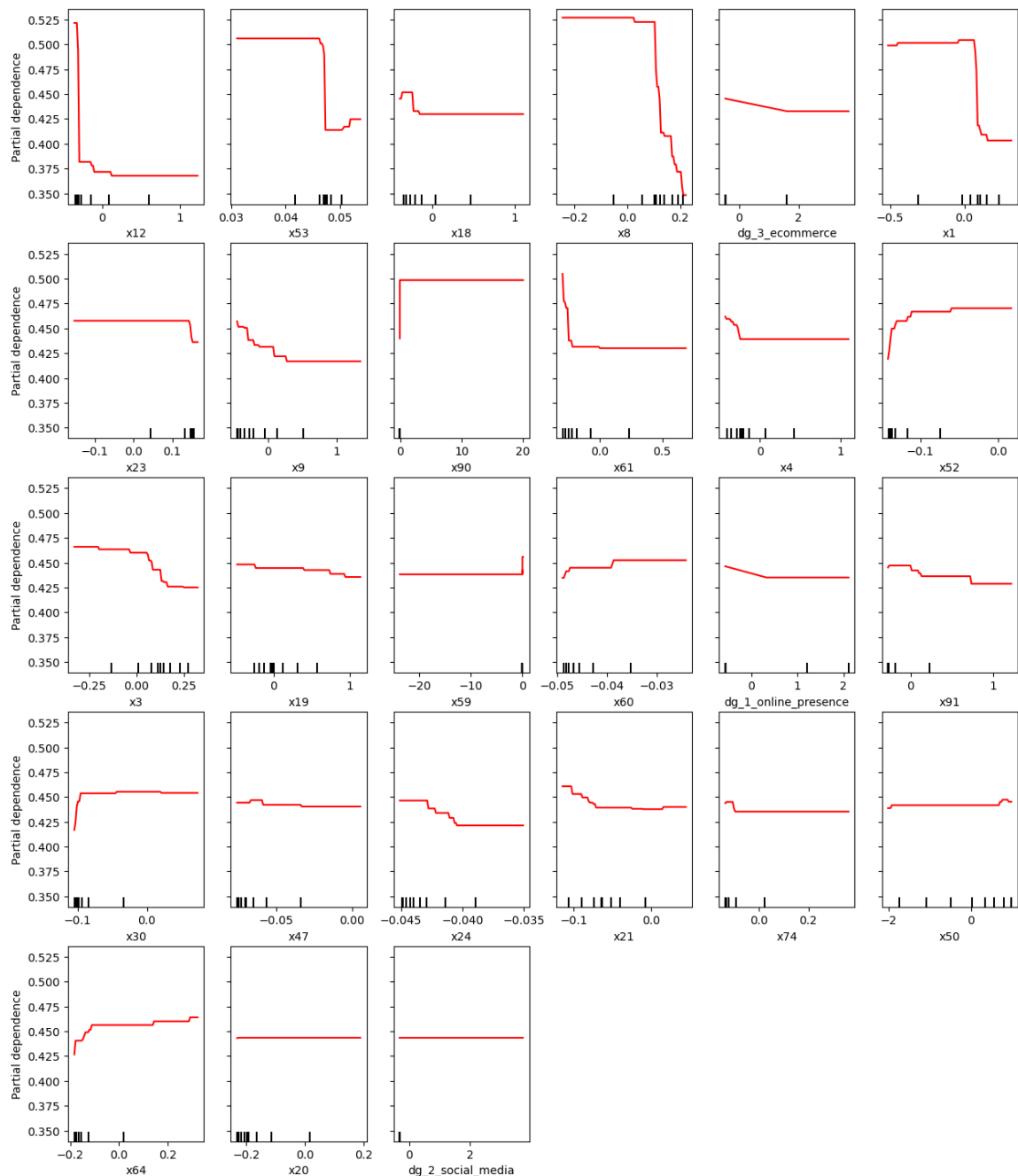


Рис. 3.5. PDP-графіки для змінних фінальної моделі XGBoost.

Джерело: складено автором.

По-перше, для змінної  $x_8$  (відношення власного капіталу до загальних пасивів), що характеризує фінансову автономію, встановлено виражений нелінійний ефект. На PDP-кривій ідентифіковано критичний коридор значень, у межах якого мінімальне зростання капіталізації забезпечує максимальний граничний ефект у зниженні ризику банкрутства, що обґрунтовує

пріоритетність рішень щодо докапіталізації та оптимізації структури пасивів для підприємств із низьким рівнем власного капіталу.

По-друге, показник  $x_{12}$  (відношення валового прибутку до поточних зобов'язань) відображає здатність до обслуговування короткострокового боргу за рахунок операційної діяльності. Виявлено пороговий характер залежності: прогнозований ризик експоненціально знижується при виході показника з критичної зони низького покриття. Управлінський акцент має бути спрямований на контроль собівартості та реструктуризацію короткострокової заборгованості для переходу у стабільну зону функціонування.

По-третє, змінна  $x_{53}$  (відношення власного капіталу до основних засобів) визначає рівень самофінансування необоротних активів. PDP-аналіз фіксує стрибкоподібне підвищення фінансової стійкості при досягненні цільового рівня показника. Іншими словами, низьке значення  $x_{53}$  свідчить про розбалансованість інвестиційної та фінансової політик, що потребує перегляду інвестиційних програм або реалізації малоефективних активів для збалансування джерел фінансування.

По-четверте, фактори цифровізації демонструють стійкий обернений зв'язок із ймовірністю дестабілізації підприємства. Зокрема:

*dg\_3\_ecommerce*: перехід від відсутності онлайн-продажів до повноцінного функціоналу електронної комерції (2 бали) знижує ймовірність банкрутства в середньому на 3%.

*dg\_1\_online\_presence*: наявність функціонального веб-сайту (3 бали) асоціюється зі зниженням ризику на 2,6% порівняно з непередставленими в мережі підприємствами.

Отримані результати підтверджують гіпотезу про суттєву роль цифрової трансформації у зміцненні економічної стійкості суб'єктів господарювання. Використання PDP-графіків дозволило не лише підтвердити значущість обраних змінних, а й отримати їх кількісні оцінки, що є підґрунтям для формування прикладних рекомендацій у системі управління фінансовою безпекою.

### **3.2. Формування моделі управління кадровою безпекою підприємства**

Як було зазначено в попередніх розділах, однією з ключових загроз для кадрової безпеки підприємства в умовах цифрової трансформації є інсайдерські ризики, а також пов'язані з ними ризики витоку конфіденційної інформації. Ці загрози набувають дедалі більшої актуальності у зв'язку з активним використанням цифрових технологій у внутрішньому управлінні, автоматизацією бізнес-процесів та підвищенням обсягів оброблюваної чутливої інформації.

Особливу небезпеку становлять працівники, які з різних причин (свідомо чи несвідомо) можуть порушити політику інформаційної безпеки підприємства. Це можуть бути як незадоволені співробітники, що діють навмисно, так і особи, які через неуважність чи відсутність відповідної цифрової грамотності мимоволі створюють передумови до інцидентів витоку даних. Саме тому виявлення потенційно небезпечної поведінки на ранніх етапах є важливою передумовою забезпечення кадрової безпеки підприємства.

З огляду на вищезазначене, у цьому розділі пропонується модель виявлення працівників, що можуть становити загрозу для інформаційної безпеки підприємства. Така модель ґрунтується на аналізі дій працівника у внутрішній корпоративній цифровій інфраструктурі зокрема, аналізу логів доступу, активності у внутрішній мережі, манери користування інформаційними системами, динаміки зміни поведінкових патернів тощо.

У зв'язку з обмеженою доступністю до фактичних корпоративних даних, що пов'язані з поведінкою співробітників у цифровому середовищі, для цілей цього дослідження було обрано відкритий набір даних CERT Insider Threat Tools [66]. Слід зауважити, що дані цього набору не є результатом реального виробничого процесу, а створені штучно в умовах симульованого середовища. Тим не менш, CERT R4.2 моделює реалістичні сценарії поведінки працівників,

зокрема потенційно ризиковані дії, що можуть призвести до порушення кадрової або інформаційної безпеки організації.

Змістове наповнення набору CERT включає журнали активності користувачів в корпоративній IT-інфраструктурі, що дозволяє відтворити умови, подібні до тих, у яких працюють реальні підприємства. Дані містять відомості про індивідуальні дії співробітників (зокрема, тип дії, її час, ідентифікатор користувача), що забезпечує можливість побудови повноцінних поведінкових профілів. Такий підхід є особливо цінним для тестування моделей виявлення інсайдерських загроз та аналізу ризиків у сфері кадрової безпеки.

У межах дослідження було використано версію CERT R4.2, яка вирізняється балансом між кількістю користувачів, обсягом спостережень та часткою інсайдерських інцидентів. Зокрема, ця версія включає дані про 1000 працівників, серед яких 70 осіб були помічені як потенційні джерела загроз для організаційної безпеки. Таким чином, набір даних дозволяє здійснити повноцінне порівняння поведінки звичайних користувачів та осіб, схильних до ризикованих дій, що є важливим для тренування алгоритмів виявлення аномалій.

Структура даних у наборі CERT R4.2 організована у декілька тематичних таблиць:

- таблиця авторизації (логування входів і виходів із системи);
- таблиця підключення пристроїв (підключення зовнішніх носіїв);
- таблиця використання мережі інтернет (запити до вебресурсів);
- таблиця файлової активності (операції із файлами);
- таблиця електронної пошти (надсилання та отримання листів).

Одним із ключових викликів при побудові моделей виявлення інсайдерських загроз є проблема дисбалансу класів. У реальних та симульованих корпоративних даних, як-от у наборі CERT R4.2, кількість інцидентів, пов'язаних із ризикованою поведінкою працівників, зазвичай є значно меншою порівняно з випадками нормальної активності. Зокрема, у

повному наборі даних кількість інсайдерів становить менше 10 % від загальної кількості користувачів, що унеможлиблює ефективне навчання моделей без спеціальних заходів балансування.

Без урахування проблеми дисбалансу класів, алгоритми навчання або побудовані моделі можуть ігнорувати аномальні значення, через їх значну меншість. У науковій літературі запропоновано низку підходів для розв'язання цієї проблеми. Вони класифікуються на чотири основні типи: методи на рівні алгоритму, методи на рівні даних, методи з урахуванням вартості помилки та ансамблеві підходи. Серед них, методи на рівні даних, які передбачають попередню обробку нерівномірних за розподілом вибірок, є одними з найпоширеніших [65].

З огляду на вказану проблему, на першому етапі дослідження було прийнято рішення сформулювати скорочену, але збалансованішу вибірку користувачів для глибинного аналізу. Повний набір CERT R4.2, що включає понад 1000 працівників, містить великий масив даних, який ускладнює деталізовану обробку та інтерпретацію. Тому з метою оптимізації аналітичного процесу та покращення якості моделі було здійснено відбір підмножини користувачів з урахуванням представлення обох класів.

Зокрема, до підвибірки увійшли 20 з 70 користувачів, ідентифікованих як потенційні інсайдери, а також 30 з 930 користувачів, які демонстрували нормальну поведінку. Загальний обсяг дослідницької вибірки склав 50 осіб, де частка інсайдерів становила 40%. Такий рівень часткового балансування є компромісом між збереженням реалістичності даних та потребою підвищити чутливість моделі до виявлення атипової поведінки. Результатом цього підходу стало зменшення ризику перенавчання моделі на домінантний клас та підвищення її здатності ідентифікувати критичні патерни поведінки.

Одним із ключових елементів новизни запропонованого підходу стало збагачення наявних даних шляхом інтеграції додаткової семантичної інформації, що була згенерована за допомогою великих мовних моделей (LLM). Залучення LLM дозволило суттєво підвищити інформативність ознак

у задачі аналізу поведінки працівників та покращити якість виявлення ризиків для кадрової безпеки підприємства. Великі мовні моделі – це сучасні архітектури машинного навчання, побудовані на основі нейронних мереж з великою кількістю параметрів, які навчалися на масштабних текстових корпусах. Вони здатні розуміти контекст, логіку та емоційне забарвлення тексту, що значно розширює їх застосування в різних сферах від автоматичного перекладу до аналізу настроїв, генерації текстів, відповіді на запитання тощо [210]. У роботі [1] представлено узагальнений огляд сучасних архітектур LLM та сфер їх застосування.

У цьому дослідженні було запропоновано використати потенціал LLM для автоматизованої класифікації вебресурсів, які відвідували працівники, з метою виявлення ознак ризикової поведінки. Це особливо актуально з огляду на те, що одним з основних індикаторів інсайдерських загроз є активність користувача в мережі Інтернет. У межах аналізу було визначено два ключові сценарії потенційної загрози:

- пошук працівником іншого місця роботи, що може супроводжуватись викраденням або виведенням корпоративних даних;

- поширення конфіденційної інформації на вебсайтах, орієнтованих на інсайдерські витoki або обмін корпоративними файлами.

Традиційні методи виявлення таких загроз зазвичай ґрунтуються на фіксованих списках доменів, віднесених до відповідних категорій (наприклад, сайти пошуку роботи або ресурси обміну даними). Однак основним обмеженням таких методів є низька гнучкість: якщо конкретний сайт не входить до списку, система не в змозі виявити потенційну загрозу, навіть якщо його зміст очевидно свідчить про ризикову поведінку.

З метою усунення цього обмеження було запропоновано інноваційний підхід, а саме класифікація вебсайтів на основі їх вмісту за допомогою LLM. На основі полів набору даних CERT R4.2 були сформульовані два запити до LLM, які дозволяють оцінити зміст відвіданих сторінок з точки зору ризику:

«Користувач відвідав вебсайт '{url}' із наступними ключовими словами: {content}. Чи шукає ця людина роботу на основі відвіданого сайту? Відповідайте тільки "так" або "ні".»

«Користувач відвідав вебсайт '{url}' із такими ключовими словами: {content}. Чи може така дія свідчити про несанкціоноване розповсюдження конфіденційної інформації? Відповідайте тільки "так" або "ні".»

Застосування LLM у такому форматі дозволяє не лише розширити покриття ризикових сайтів, а й адаптувати модель до динамічно змінного вебсередовища, що є важливою перевагою у порівнянні з традиційними методами. Отримані відповіді використовуються як бінарні ознаки, що вводяться до моделі виявлення інсайдерської активності у подальших етапах аналізу.

Зважаючи на великий обсяг веб-активності, зафіксований у наборі CERT R4.2, постала потреба у розробці ефективного та економного рішення для обробки запитів до великої мовної моделі. У середньому один працівник може відвідати десятки або навіть сотні вебсторінок протягом робочого дня, що в сукупності формує мільйони записів. Традиційні LLM, такі як GPT-3 або GPT-4 [79], мають високу вартість інференсу та значні обчислювальні вимоги, що робить їх використання у даному випадку малопрактичним.

З метою забезпечення швидкої генерації відповідей на сформульовані запити при збереженні достатнього рівня якості, у дослідженні було обрано легку інструкційну модель «Phi-3.5-mini-instruct» [4]. Ця модель є представником нового покоління компактних LLM, що містить менше ніж 4 мільйони параметрів, що, у поєднанні з оптимізованою архітектурою, дозволяє її розгортання на локальному персональному комп'ютері або у хмарному середовищі з обмеженими ресурсами. Попри відносно малу кількість параметрів, Phi-3.5-mini продемонструвала стабільну якість відповідей у рамках обраних запитів, що не поступалася більш ресурсомістким моделям у вузькому контексті бінарної класифікації.

Для подальшого підвищення продуктивності та масштабованості обробки було інтегровано одну з найновіших бібліотек для оптимізації генерації тексту vLLM [61], яка забезпечує асинхронну інференцію, ефективне використання пам'яті та підтримку пакетної обробки, що значно пришвидшує роботу із запитами до мовної моделі. Таким чином, навіть за умов обмежених обчислювальних потужностей, було забезпечено високу пропускну здатність системи, що є критично важливим у задачах реального часу.

У результаті застосування запропонованого підходу було згенеровано дві нові ознаки (індикативні змінні), які надалі інтегрувалися до загального простору ознак у моделі аналізу поведінки користувачів:

*llm\_jobs\_output* – бінарна змінна, яка приймає значення 1, якщо контент відвіданої сторінки свідчить про пошук користувачем нового місця роботи, та 0 у протилежному випадку;

*llm\_leak\_output* – бінарна змінна, що вказує, чи потенційно відвіданий сайт може бути джерелом несанкціонованого розповсюдження конфіденційної інформації.

Варто зазначити, що формування цих змінних стало ключовим етапом семантичного збагачення даних, що суттєво підвищило здатність моделі виявляти поведінкові патерни, які не завжди можна ідентифікувати на основі стандартних лог-файлів.

Загалом, обробку понад 1 мільйона унікальних записів про відвідані вебресурси було здійснено протягом приблизно п'яти годин із використанням графічного процесора Google Colab A100 [101]. Це підтверджує практичну придатність запропонованого рішення для використання у реальних умовах, де критичною є не лише точність, але й швидкість та економічність обчислень.

Після генерації нових ознак за допомогою великої мовної моделі наступним етапом стала трансформація вихідних даних у формат, придатний для моделювання поведінки користувачів. З огляду на те, що дії працівників фіксуються на рівні окремих подій у різні часові моменти, було прийнято рішення агрегувати дані на поденному рівні для кожного користувача. Такий

підхід дозволяє формалізувати поведінкову активність у вигляді числових характеристик, придатних для статистичного аналізу та застосування алгоритмів машинного навчання. Для прикладу, на основі таблиці авторизації (логування входів у систему) було створено ознаку, що відображає кількість входів користувача до комп'ютера протягом конкретного дня. Подібні прості, але стабільні метрики дозволяють ідентифікувати зміни у звичній поведінці, які можуть сигналізувати про потенційні загрози.

Одним із ключових кроків у процесі побудови ознак стало розділення активності користувачів за часовими періодами, а саме у межах робочого часу та поза його межами. Для цього було проведено аналіз щогодинного розподілу активності всіх користувачів, за результатами якого визначено типову часову рамку активності, яка відповідає основному робочому періоду (рис. 3.6). На основі цього поділу було сформовано окремі групи змінних, що характеризують денну та нічну активність, що дозволило виявляти аномальні шаблони поведінки, такі як підключення до системи у нетиповий час.

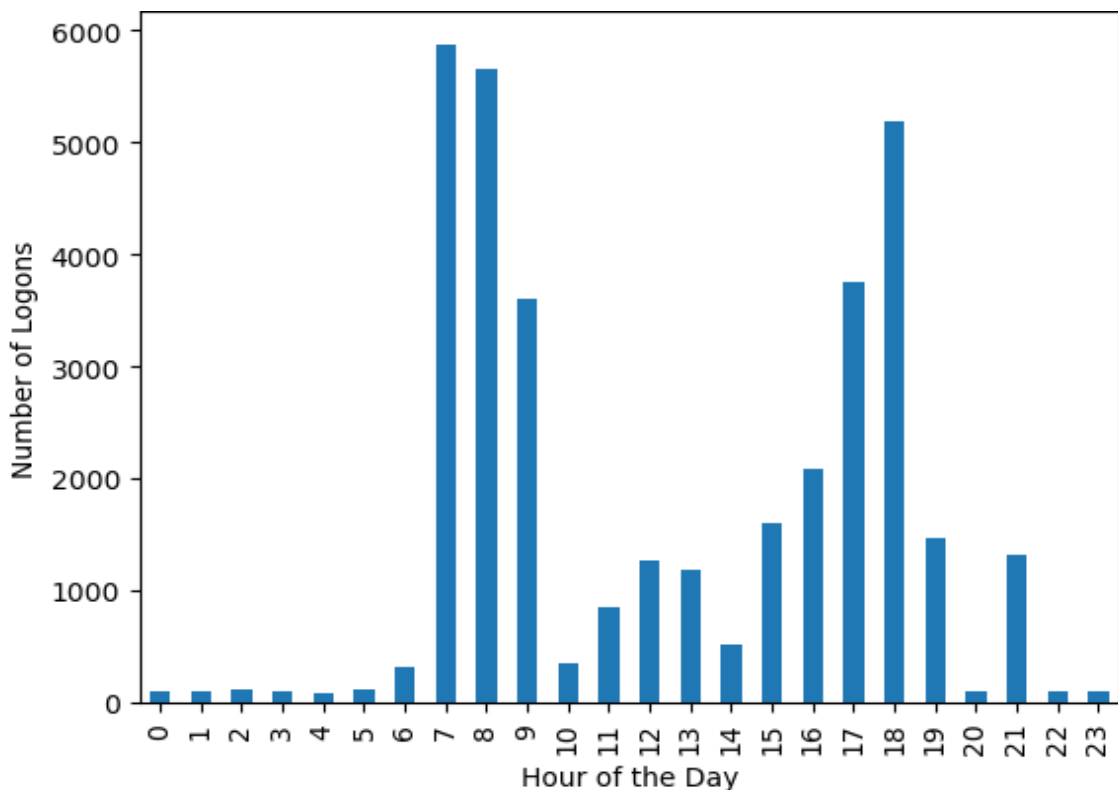


Рис. 3.6. Розподіл входу в систему всіх користувачів за годинами доби.

Джерело: складено автором.

Особливу увагу в процесі аналізу даних було приділено розробці нових змінних, що раніше не застосовувалися у дослідженнях інсайдерських загроз, але мають високий потенціал для ідентифікації складних поведінкових сценаріїв. Зокрема, було запропоновано комплексну змінну *num\_connect\_after\_job\_search*, яка враховує мультиплікативний ефект двох динамічних факторів:

1. Приріст кількості підключених зовнішніх пристроїв.
2. Зростання активності на вебсайтах, пов'язаних з пошуком роботи.

Ідея формування такої змінної базується на виявленні специфічного шаблону поведінки: на початковому етапі користувач активно цікавиться можливістю змінити місце роботи, після чого починає підключати зовнішні носії, ймовірно, з метою копіювання службової інформації. Такий тип поведінки потенційно свідчить про високий ризик витоку конфіденційних даних, і тому заслуговує на посилену увагу з боку систем управління кадровою безпекою.

Крім того, для підвищення деталізації аналізу було запропоновано ще одну ознаку, а саме ідентифікатор використання потенційно небезпечного програмного забезпечення. На основі аналізу текстових описів встановлених програм здійснювався пошук ключових слів, таких як «malware», «password», «illegal». У разі виявлення хоча б одного такого слова відповідну програму було позначено як потенційно загрозливу, а значення змінної приймало відповідне бінарне значення. Загалом, перелік відібраних змінних наведено у табл. 3.7.

Таким чином, підготовлений набір даних став надійною основою для побудови моделі виявлення загроз кадровій безпеці підприємства. У результаті проробленого аналізу:

- було сформовано 5 нових комплексних змінних, що поєднують кілька факторів ризику;

– підготовлено понад 15 000 екземплярів даних, де кожен екземпляр репрезентує поведінкову характеристику конкретного користувача протягом одного дня.

Таблиця 3.7

Ключові змінні для виявлення найбільшої потенційної загрози

| Змінна                              | Опис                                                                                                                                     |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <i>num_connect_0</i>                | Кількість підключень усіх девайсів у неробочий час                                                                                       |
| <i>num_site_leak_1</i>              | Кількість заходів на сайт з потенційною загрозою витоку інформації в робочий час                                                         |
| <i>num_site_leak_0</i>              | Кількість заходів на сайт з потенційною загрозою витоку інформації в неробочий час                                                       |
| <i>num_files_risk_1</i>             | Кількість відкриття підозрілих програм у робочий час                                                                                     |
| <i>num_connect_after_job_search</i> | Відношення між кількістю підключень у робочий час до максимального рівня приросту відвідувань сайтів з пошуку роботи за останні 40 днів. |

Джерело: складено автором

Наступним етапом став поділ всього набору даних на тренувальну та тестову вибірки відповідно до сучасних наукових рекомендацій у сфері виявлення інсайдерських загроз. У задачах виявлення аномальної поведінки інсайдерів усталеною практикою є тренування моделей лише на основі «нормальних» даних, тобто записів, що стосуються звичайних користувачів. Такий підхід дозволяє алгоритму створити еталонну модель типової поведінки. Зокрема, у дослідженні Сархан та Алтвайджрі [21] використовували One-Class SVM та Isolation Forest, тренуючи їх виключно на негативному класі (звичайні користувачі), а потім тестуючи на вибірці, що містить аномальні приклади. Аналогічні результати наведено у роботі Ле та Зінсір-Хейвуд [35], де зазначено, що надмірна кількість аномальних прикладів у тренувальних даних може негативно вплинути на якість моделі, в той час як незначна частка аномалій у тесті навпаки сприяє точнішій ідентифікації відхилень у поведінці.

Беручи це до уваги, поділ набору даних було здійснено на основі користувачів, а не окремих записів, що дозволило забезпечити незалежність

вибірок та уникнути інформаційного перетікання між тренувальною і тестовою частинами. Загалом, тестова вибірка включала 19 користувачів, з яких 68 % становили інсайдери, тоді як у тренувальну вибірку увійшли 31 користувач, з яких лише 22 % були інсайдерами. Такий підхід дозволив сконцентрувати основну кількість шкідливої активності в тестовій вибірці, зберігши при цьому реалістичність тренування моделі в умовах переважної частки «нормальних» даних. Розподіл екземплярів даних (тобто денних записів поведінки користувачів), агрегованих раніше, також зберіг пропорції, наближені до користувацького поділу: близько 65 % записів увійшли до тренувальної вибірки, решта – до тестової.

Наступним етапом дослідження стала побудова моделі для виявлення інсайдерської активності серед працівників підприємства. Оскільки основна мета моделі полягає у практичному застосуванні в реальному бізнес-середовищі, під час її розробки було сформульовано низку функціональних вимог, дотримання яких є критичним для забезпечення її ефективності й адаптивності:

- оперативність реагування: модель має виявляти потенційні ознаки інсайдерської активності у мінімально можливих строках після реальних дій користувача, щоб забезпечити своєчасне втручання;

- орієнтація на мінімізацію ризику пропуску загрози: перевага надається чутливості системи, навіть за умови підвищеного рівня хибнопозитивних спрацьовувань, адже пропущена загроза несе значно вищі ризики, ніж помилкове виявлення;

- гнучкість і масштабованість: модель має бути універсальною, з можливістю адаптації до підприємств різного розміру, галузевої специфіки та внутрішньої структури бізнес-процесів.

З урахуванням зазначених критеріїв, а також спираючись на практику вирішення аналогічних задач у сфері кадрової безпеки, було ухвалено рішення використовувати алгоритми виявлення аномалій, як універсальний та ефективний підхід до виявлення потенційно небезпечної поведінки. Як було

обґрунтовано в п. 2.2, доцільно застосовувати комбінацію алгоритмів Isolation Forest та Local Outlier Factor (LOF). Вказані методи відрізняються високою здатністю виявляти нетипові шаблони без необхідності мати великий обсяг мічених даних. Використання цих підходів дозволило реалізувати гнучку систему поведінкового моніторингу, що здатна підлаштовуватись під характерні особливості даних конкретного підприємства та відображати як загальні, так і контекстно-специфічні індикатори загроз.

Наступним логічним етапом стало визначення методів оцінки якості побудованих моделей. Для цього було обрано три основні показники, що широко використовуються у практиці машинного навчання для задач класифікації: Detection Rate (DR), Accuracy та F1 Score.

Першим та основним показником є *Detection Rate*. Він демонструє, яку частку небезпечних працівників вдалося правильно виявити серед усієї кількості реальних інсайдерів. Цей показник є надзвичайно важливим у контексті кадрової безпеки, оскільки пріоритетом є мінімізація кількості пропущених загроз. Формула для розрахунку *Detection Rate* має вигляд:

$$DR = \frac{\text{кількість виявлених інсайдерів}}{\text{загальна кількість інсайдерів}}$$

Другим показником є *Accuracy*, який відображає загальний рівень правильності передбачень моделі. Він показує частку всіх правильно класифікованих випадків (як інсайдерських, так і нормальних) серед загальної кількості спостережень. Формула для його розрахунку наступна:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

де

*TP (True Positives)* – правильно визначені інсайдери,

*TN (True Negatives)* – правильно визначені неінсайдери,

*FP (False Positives)* – хибні визначення працівників як інсайдерів,

*FN (False Negatives)* – пропущені реальні інсайдери.

Третім важливим показником виступає *F1 Score* – гармонічне середнє між точністю (*Precision*) та повнотою (*Recall*). Цей показник дозволяє краще оцінити збалансованість моделі, особливо у випадках, коли дані мають суттєвий дисбаланс між класами. Розрахунок *F1 Score* здійснюється за формулою:

$$F1 = \frac{2 \cdot P \cdot R}{P + R}$$

$$\text{де } P = \frac{TP}{TP+FP}, R = \frac{TP}{TP+FN}.$$

Таким чином, аналіз зазначених показників дозволяє комплексно оцінити ефективність запропонованої моделі як у частині своєчасного виявлення загроз, так і з точки зору загальної точності класифікації дій працівників.

Для кожної з розроблених моделей було визначено основні параметри, причому особлива увага приділялася налаштуванню параметра, що визначає частку аномальних значень у вибірці, оскільки саме він суттєво впливає на чутливість моделі до нетипових спостережень (*contamination*). З метою оптимального налаштування цього параметра було здійснено підбір значень за допомогою методу повного перебору у межах від 1 % до 5 % з кроком 1 % [27].

У результаті проведених експериментів встановлено, що найкращі результати за показниками точності є параметри 3-5 %, проте за *F1-score* найкращим є 3 %. Оскільки точність моделі не сильно відрізняється при параметрах 3-5 %, а значення *F1-score* значно краще саме при 3 %, то було прийнято рішення використовувати модель з параметром, який визначає частку аномалій саме на рівні 3 % (табл. 3.8). Це свідчить про доцільність саме такого налаштування для забезпечення збалансованості між чутливістю до аномалій та стійкістю до хибнопозитивних спрацьовувань моделі.

На основі сформованих основних змінних були побудовані моделі виявлення аномалій. Подальший аналіз передбачав обчислення відповідних значень показників як на рівні одного дня активності працівника, так і на рівні

кожного окремого користувача. На початку, було проведено оцінки на поденній основі, результати якої представлені в табл. 3.9.

Таблиця 3.8

Результати Grid Search параметру частку аномальних значень для моделі виявлення інсайдерів

| Contamination | Accuracy | F1 Score |
|---------------|----------|----------|
| 0.01          | 0.5748   | 0.1864   |
| 0.02          | 0.6121   | 0.2534   |
| 0.03          | 0.6423   | 0.2670   |
| 0.04          | 0.6433   | 0.2616   |
| 0.05          | 0.6468   | 0.2586   |

Джерело: складено автором

Як видно з табл. 3.9, результати на рівні одного дня показують невисокі значення F1-метрики для обох моделей, що свідчить про певну складність точного виявлення аномальної активності лише за денними шаблонами поведінки. Однак істотно інша картина спостерігалася при переході до аналізу поведінки на рівні окремого користувача, відповідні результати якої наведені в табл. 3.10.

Таблиця 3.9

Результати оцінки моделей виявлення аномалій на визначеному наборі даних на поденній основі

| Метрика  | Isolation Forest | LOF    |
|----------|------------------|--------|
| Accuracy | 65,74%           | 63,24% |
| F1       | 42,25%           | 33,55% |

Джерело: складено автором.

Найкращі результати у межах проведеного моделювання продемонструвала модель Isolation Forest, яка змогла ідентифікувати всіх користувачів, що становили інсайдерську загрозу, досягнувши таким чином 100 % показника виявлення. Водночас ця модель точно визначила кожного

користувача, не допустивши хибнопозитивних спрацьовувань, що свідчить про високу збалансованість між чутливістю та точністю.

Таблиця 3.10

Результати оцінки моделей виявлення аномалій на визначеному наборі даних на рівні користувача

| Метрика        | Isolation Forest | LOF     |
|----------------|------------------|---------|
| Detection rate | 100,00%          | 100,00% |
| Accuracy       | 100,00%          | 58,33%  |
| F1             | 100,00%          | 83,87%  |

Джерело: складено автором.

Попри те, що модель Local Outlier Factor (LOF) також досягла 100 % показника виявлення, її результати за збалансованою точністю (58 %) та F1-метрикою (84%) виявились суттєво нижчими порівняно з Isolation Forest. Це вказує на те, що, хоча LOF і виявила всіх інсайдерів, вона припустилась значної кількості помилкових класифікацій звичайних користувачів, що зумовило зниження точності, а отже і загальної стабільності моделі у класифікаційних задачах.

Таким чином, модель Isolation Forest може бути рекомендована як основний інструмент для реалізації автоматизованого моніторингу кадрової безпеки, особливо у випадках, коли критично важливо досягати високої чутливості без компромісів щодо точності.

Окремо варто наголосити, що у завданнях виявлення інсайдерів критично важливим є не тільки сам факт виявлення підозрілої активності, але й час реакції на загрозу. Чим швидше виявлено інсайдера, тим більше шансів своєчасно вжити заходів для запобігання витоку конфіденційної інформації або нанесення шкоди компанії.

Так, можна проаналізувати результати моделювання на прикладі одного юзера. Графік на рис. 3.7 відображає динаміку декількох ключових змінних протягом визначеного періоду для одного робітника.

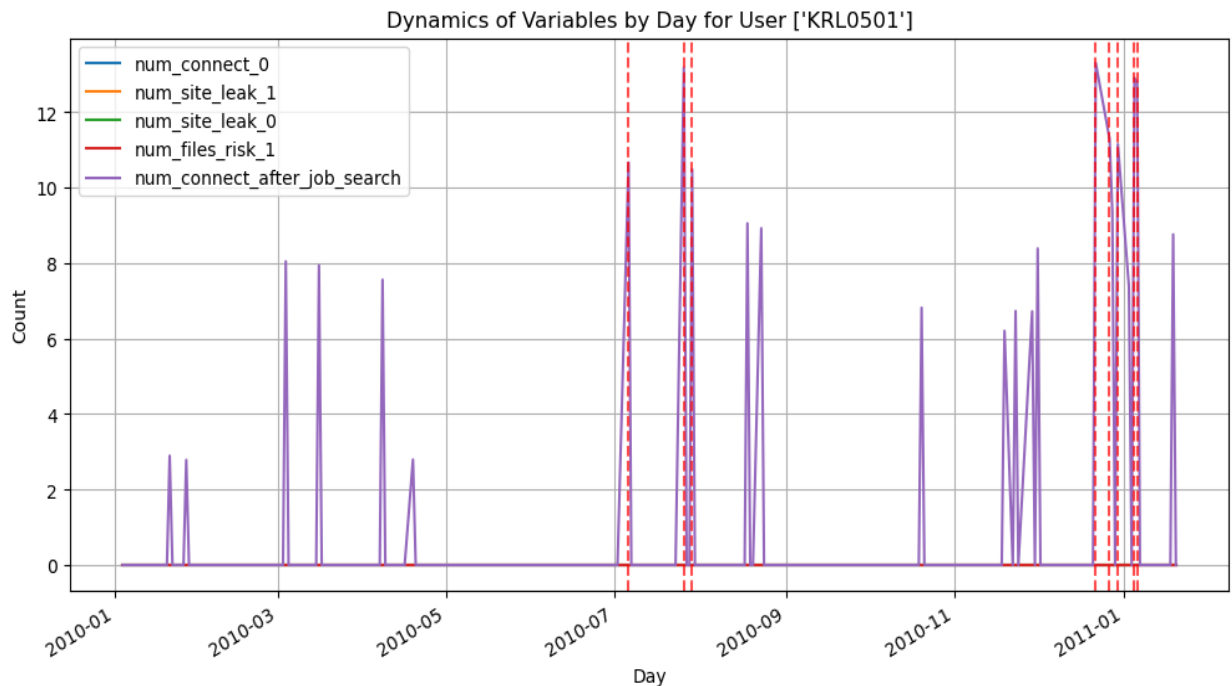


Рис. 3.7. Зміни ключових змінних моделі Isolation Forest на прикладі одного користувача.

Джерело: складено автором.

Рис. 3.7 відображає часові коливання значень основних поведінкових ознак, перелік яких подано у табл. 3.7. Червоні горизонтальні пунктирні лінії позначають дні, які модель класифікувала як аномальні, тобто ті, що потенційно відповідають ризикованим діям користувача. Особливу увагу заслуговує фіолетова крива, яка відображає значення змінної *num\_connect\_after\_job\_search*. Ця змінна інтегрує інформацію про підвищену активність на сайтах пошуку роботи у поєднанні з підключенням зовнішніх пристроїв, і її періодичні сплески можуть свідчити про реальну підготовку до несанкціонованого виведення службової інформації.

Аналіз поведінки цього користувача свідчить про нерегулярний характер активності, зокрема чергування періодів високої динаміки та практично повної

відсутності активності. Така структура поведінки є нетиповою для більшості користувачів і є показовою у контексті виявлення загроз.

Таким чином, візуалізація динаміки ознак на індивідуальному рівні дозволяє не лише підтвердити обґрунтованість класифікації з боку моделі, а й забезпечити інтерпретованість результатів для аналітиків служби безпеки підприємства, що значно підвищує довіру до моделі та створює можливості для своєчасного прийняття управлінських рішень щодо потенційно ризикованих співробітників.

Для детальнішого аналізу ефективності моделі виявлення інсайдерської активності було проведено дослідження часу, коли модель вперше зафіксувала потенційно аномальну діяльність, яка могла б свідчити про загрозу кадровій безпеці. Враховуючи важливість своєчасного виявлення інсайдерів для запобігання витoku конфіденційної інформації або інших негативних наслідків, важливим аспектом стало визначення того, наскільки швидко модель реагує на аномальні події в діяльності користувачів. Для цього був здійснений порівняльний аналіз між моментом першого виявлення аномальної активності та реальним початком інсайдерської діяльності. За результатами цього порівняння було встановлено наступні висновки:

6 інсайдерів були виявлені вже в день початку їх інсайдерської активності або навіть за кілька днів до цього, що свідчить про високий рівень чутливості моделі та її здатність виявляти загрози ще на ранніх стадіях.

4 користувачі були виявлені протягом перших 31 дня після початку інсайдерської активності, що також підтверджує ефективність моделі в умовах середньо- та короткострокового моніторингу.

Всі користувачі були виявлені до завершення періоду інсайдерської діяльності, що підкреслює надійність моделі та її здатність завершити цикл виявлення та реагування до повного здійснення загрози.

Ці результати підтверджують, що побудована модель не тільки має високу ефективність у виявленні аномальних подій, але й дозволяє оперативно реагувати на потенційні загрози. Враховуючи зазначене, можна стверджувати,

що дана модель є надійним інструментом для застосування в реальному моніторингу активності робітників на підприємствах. Вона здатна забезпечити своєчасну і якісну підтримку прийняття рішень щодо виявлення та попередження загроз кадровій безпеці, що є критично важливим у сучасних умовах цифрової трансформації та підвищеного ризику витоків конфіденційної інформації.

У результаті проведеного аналізу отримано низку важливих висновків:

1. Модель Isolation Forest продемонструвала найвищу ефективність, досягнувши 100 % показника виявлення інсайдерів та високої точності при класифікації користувачів на основі поведінкових даних.

2. Оптимізація моделі, зокрема параметра contamination, дозволила збалансувати чутливість і стійкість до хибнопозитивних спрацьовувань, що є критично важливим у задачах кадрової безпеки.

3. Часовий аналіз моменту виявлення аномалій показав, що у більшості випадків модель фіксувала загрозу ще до або на самому початку інсайдерської активності, що підтверджує її практичну цінність як інструмента для превентивного моніторингу.

4. Побудована система довела свою прикладну придатність для реального використання, забезпечуючи підтримку управлінських рішень у сфері захисту інформаційних ресурсів підприємства.

З огляду на досягнуті результати, було визначено три основні напрями практичного використання розробленої моделі в межах систем управління кадровою безпекою підприємства:

1. Інтеграція моделі в реальні системи моніторингу  
Модель Isolation Forest може бути ефективно інтегрована у системи моніторингу активності працівників, зокрема SIEM-рішення або спеціалізовані аналітичні модулі. Це дозволяє виявляти потенційні загрози у режимі, наближеному до реального часу, своєчасно попереджати витoki даних і мінімізувати наслідки внутрішніх інцидентів. Впровадження такого інструменту посилює інформаційну безпеку підприємства на всіх рівнях.

2. Підсилення внутрішнього контролю та системи управління ризиками Використання поведінкових моделей дозволяє підприємству не лише реагувати на фактичні інциденти, а й запобігати їх виникненню, виявляючи потенційно ризиковані шаблони ще до того, як буде завдано шкоди. Це зміщує акцент безпеки з реактивної до превентивної моделі, сприяючи ефективнішому управлінню кадровими ризиками.

3. Адаптація моделі до специфіки галузі чи організації Алгоритм Isolation Forest є гнучким і універсальним, що дозволяє адаптувати його до підприємств різних розмірів та секторів: від фінансових і державних установ до ІТ-компаній і промислових організацій. Наявність параметрів налаштування та можливість гнучкої інтерпретації змінних дозволяє інтегрувати модель у наявні інформаційно-аналітичні середовища з урахуванням специфіки бізнес-процесів.

Таким чином, розроблена система поведінкового моніторингу на основі алгоритму Isolation Forest може розглядатися як повноцінний елемент корпоративної інфраструктури безпеки. Її перевагами є точність, своєчасність реагування, адаптивність до конкретного середовища та можливість масштабування під потреби підприємства.

### **3.3. Реалізація прикладної інформаційної системи управління системою економічною безпекою підприємств**

Для створення прикладної інформаційної системи, яка реалізує побудовані моделі оцінки рівня економічної безпеки підприємства та забезпечує інтерактивну візуалізацію результатів, було обрано фреймворк Streamlit [2]. Streamlit – це сучасна платформа з відкритим вихідним кодом для швидкої розробки вебзастосунків на основі Python, яка спеціалізується на інтеграції моделей машинного навчання, аналітичних інструментів та інтерактивних інтерфейсів користувача.

Однією з ключових переваг Streamlit є максимальна простота інтеграції побудованих раніше моделей фінансової, кадрової та техніко-технологічної підсистем безпеки без потреби у створенні складної інфраструктури або залученні зовнішніх фахівців з веброзробки. Це дозволило зосередити зусилля на функціональній реалізації логіки прийняття рішень, не витрачаючи ресурси на інженерні аспекти інтерфейсу. Серед основних переваг вибору Streamlit варто відзначити:

- легка інтеграція моделей машинного навчання – Streamlit дозволяє безпосередньо вбудовувати попередньо навчені моделі Python у вебінтерфейс, що забезпечує оперативне прогнозування рівня ризику в реальному часі;
- гнучка система візуалізації – можливість створення динамічних графіків, таблиць, теплових карт та інших аналітичних елементів, що робить інтерфейс не лише функціональним, а й зручним для інтерпретації результатів;
- простота розгортання та підтримки – система не потребує складного налаштування серверної частини, може бути запущена локально або в хмарному середовищі, що значно знижує вартість володіння;
- можливість кастомізації – Streamlit підтримує налаштування зовнішнього вигляду, інтерактивних елементів, завантаження даних у різних форматах, фільтрацію та адаптацію системи до потреб конкретного підприємства;
- відкритий код і спільнота підтримки – наявність великої кількості прикладів, бібліотек розширень та активної спільноти розробників спрощує реалізацію нових функціональностей і пришвидшує процес удосконалення системи.

Загалом, вибір Streamlit як платформи розробки інформаційної системи дозволив реалізувати інтерактивне середовище для оцінки економічної безпеки підприємства, яке є гнучким, масштабованим і орієнтованим на прикладне використання. Система може бути легко впроваджена на підприємстві, доповнена іншими підсистемами безпеки, інтегрована в існуючу корпоративну IT-архітектуру або функціонувати як автономний застосунок.

Розроблена інформаційна система управління економічною безпекою підприємства складається з чотирьох функціонально взаємопов'язаних модулів, кожен з яких виконує специфічні аналітичні та управлінські завдання в межах відповідної підсистеми:

Фінансовий модуль здійснює автоматизовану обробку даних з основних бухгалтерських форм (зокрема, Форма №1 «Баланс» та Форма №2 «Звіт про фінансові результати»), обчислення ключових індикаторів фінансової безпеки (ліквідність, платоспроможність, рентабельність, фінансова стабільність тощо), а також прогнозування ймовірності банкрутства з використанням моделей машинного навчання.

Кадровий модуль відповідає за моніторинг та аналіз цифрової активності працівників на основі логів систем доступу (автентифікації), даних електронної пошти, звернень до файлових систем, HTTP-запитів тощо. Його функціональність включає виявлення поведінкових аномалій, оцінку ризику внутрішніх загроз та генерацію сигналів для служби безпеки підприємства.

Техніко-технологічний модуль забезпечує оцінку технічного та цифрового стану підприємства на основі п'яти критеріальних блоків. Вхідні значення нормалізуються та агрегуються в інтегральний індекс техніко-технологічної безпеки, що відображає загальний рівень технологічної вразливості підприємства.

Модуль інтеграції виконує об'єднання результатів, отриманих із трьох функціональних модулів, з метою обчислення інтегрального показника економічної безпеки підприємства. На основі узагальнених даних система визначає загальний рівень ризику та рівні ризику окремих підсистем. Окрім цього, модуль формує рекомендаційний блок, що генерує адаптивні управлінські рішення для зниження ризиків – від превентивних до антикризових заходів.

Загальна архітектура системи побудована за модульним принципом, що забезпечує її масштабованість, інтеграцію з внутрішніми інформаційними

системами підприємства та гнучкість адаптації до змін у зовнішньому середовищі або внутрішніх процесах.

Створена система реалізує наступну логіку та архітектуру роботи:

1. Завантаження фінансових даних (Форми №1 та №2), яке може здійснюватися двома способами:

шляхом підключення до корпоративної бази даних;

завантаженням відповідних файлів у спеціально передбачену директорію програми.

2. Завантаження даних про використання працівниками корпоративної мережі, зокрема логінів, HTTP-запитів, доступу до файлів, електронної пошти тощо. Аналогічно, дані можуть бути отримані з бази або завантажені вручну у форматі файлів.

3. Введення користувачем рівня цифровізації підприємства, що включає:

рівень онлайн-присутності,

активність у соціальних мережах,

рівень розвитку електронної комерції.

4. Вибір періоду прогнозування (рік та місяць), на який проводиться оцінка рівня економічної безпеки.

5. Введення користувачем рівня цифрового розвитку техніко-технологічної системи на основі визначення вибору відповідного рівня для кожного з 5 визначених критеріїв.

6. Обробка фінансових даних, включно з розрахунком фінансових індикаторів, які надалі використовуються в моделі фінансової безпеки.

7. Обробка та трансформація поведінкових даних, зокрема побудова змінних, що характеризують цифрову активність працівників для оцінки кадрової безпеки.

8. Прогнозування ймовірності банкрутства з використанням попередньо натренованої моделі XGBoost.

9. Виявлення аномальної поведінки працівників за допомогою моделі Isolation Forest, яка забезпечує виявлення ризиків у сфері кадрової безпеки.

10. Обчислення загального показника стану техніко-технологічної безпеки.

11. Трансформація результатів моделей у рівні ризику (низький, середній, високий) для кожної з підсистем економічної безпеки.

12. Обчислення інтегрального показника економічної безпеки підприємства.

13. Автоматичне формування рекомендацій щодо зниження виявлених ризиків.

14. Перегляд розрахованих фінансових індикаторів, що дозволяє користувачу детально аналізувати фінансовий стан підприємства.

15. Перегляд ключових показників цифрової активності працівників, включаючи детальні дані по кожному працівнику окремо.

В межах розробки моделі оцінювання економічної безпеки підприємства в умовах цифрової трансформації було реалізовано інтерактивний інтерфейс аналітичної системи, який забезпечує комплексний підхід до аналізу фінансової, кадрової та техніко-технологічної складових економічної безпеки. Інтерфейс побудовано з використанням принципів гнучкого інформаційно-аналітичного моделювання та адаптивної візуалізації ризиків, що дозволяє підприємству оперативно приймати обґрунтовані стратегічні та тактичні рішення в умовах зростаючих цифрових загроз.

Інтерфейс системи реалізований у вигляді односторінкового додатку, що містить дві логічно пов'язані панелі: панель управління параметрами аналізу та аналітично-візуалізаційний блок. З метою забезпечення інтуїтивної взаємодії користувача з інформаційною системою, у її структурі реалізована панель керування, яка виконує функцію основного інструменту введення вхідних параметрів для оцінювання економічної безпеки підприємства. Панель згрупована за функціональними блоками відповідно до підсистем: фінансової, кадрової та техніко-технологічної. Такий підхід забезпечує логічну послідовність, структурованість та зручність введення даних.

1. Блок оцінки цифрової присутності підприємства. У цьому блоці користувач послідовно задає параметри цифровізації підприємства, які впливають на рівень його фінансової безпеки в умовах цифрової економіки:

- рівень онлайн-присутності;
- рівень активності в соціальних мережах;
- розвиненість електронної комерції.

2. Блок прогнозування кадрової безпеки. Користувач обирає період аналізу, для якого буде проводитися прогнозування кадрової безпеки. Це дозволяє реалізувати динамічний підхід до оцінювання та враховувати часові коливання ризиків, пов'язаних із поведінкою персоналу, сезонними навантаженнями, змінами у внутрішній цифровій активності тощо.

3. Блок оцінки техніко-технологічного розвитку підприємства. Цей блок забезпечує введення параметрів, які впливають на рівень техніко-технологічної безпеки підприємства в цифровому середовищі. Передбачено п'ять ключових критеріїв:

- рівень автоматизації виробництва
- рівень захищеності IT-інфраструктури
- частка цифрових технологій у технологічних процесах
- стан технічного обладнання та інноваційна готовність
- рівень цифрової компетентності персоналу

Зібрані дані обробляються модулями системи, що дозволяє формувати індекси безпеки окремих підсистем та інтегральний показник економічної безпеки підприємства загалом (рис. 3.8).

Центральний блок інтерфейсу інформаційної системи призначений для інтегрованого представлення результатів оцінки рівнів економічної безпеки підприємства та формування відповідних управлінських рекомендацій. Цей блок є основною інформаційною панеллю для візуалізації ключових індикаторів безпеки в режимі реального часу.

**Виберіть рівень цифровізації підприємства**

Оберіть рівень онлайн присутності

Відсутні сайт і будь-яка присутність ▼

Оберіть рівень присутності в соціальних мережах

Немає присутності на платформах соціальних мереж. ▼

Оберіть рівень розвитку електронної комерції

Відсутність можливості онлайн-покупок або транзакцій ▼

**Виберіть потрібний період**

Оберіть місяць для прогнозування кадрової безпеки

2023 ▼

Оберіть місяць для прогнозування кадрової безпеки

1 ▼

**Виберіть рівень цифрового технологічного розвитку підприємства**

Оберіть рівень автоматизації виробництва

Автоматизація практично відсутня (<10% операцій) ▼

Оберіть рівень захищеності IT-інфраструктури

Відсутність захисту, відсутні політики, не зафіксовані інциде... ▼

Оберіть частку цифрових технологій у технологічних процесах

Використання майже відсутнє ▼

Інтегральний показник економічної безпеки: 0.49

● Середній ризик

Фінансова складова    Кадрова складова    Техніко-технологічна складова

● Низький ризик

● Середній ризик

● Високий ризик

**Рекомендації щодо тактичних і стратегічних дій**

● Активація цільових заходів у необхідних підсистемах безпеки

Рекомендації для фінансової підсистеми:

- Проведення планових фінансових аудитів.
- Оновлення фінансових прогнозів із використанням наявних даних.
- Перевірка актуальності фінансових резервів.
- Підтримання чинної системи управління ліквідністю.

Рекомендації для кадрової підсистеми:

- Впровадження системи контролю доступу до інформаційних ресурсів;

Рис. 3.8. Вигляд інформаційної системи економічної безпеки:  
панель керування (зліва), ключові рівні ризику та рекомендації (справа).

Джерело: складено автором

1. Відображення інтегрального показника економічної безпеки. У верхній частині центрального блоку розміщується значення інтегрального показника економічної безпеки підприємства, яке формується на основі агрегованих даних фінансової, кадрової та техніко-технологічної підсистем. Значення відображається з точністю до сотих частин. Візуальна інтерпретація результатів реалізується за допомогою кольорової індикації рівнів ризику (низький – зелений, середній – жовтий, високий – червоний), що дозволяє швидко ідентифікувати найбільш критичні компоненти економічної безпеки

2. Оцінка підсистем безпеки. Інтерфейс структуровано за допомогою трьох колонок, кожна з яких присвячена відповідній підсистемі:

фінансова підсистема – візуалізує рівень фінансового ризику підприємства;

кадрова підсистема – подає оцінку ризику, пов'язаного з поведінковими аномаліями персоналу;

техніко-технологічна підсистема – відображає технологічний рівень безпеки з урахуванням цифрових активів та інфраструктури.

Кожна підсистема супроводжується індивідуальним маркером рівня ризику за відповідним кольором і текстовим повідомленням.

3. Блок управлінських рекомендацій. Після оцінки ризиків система автоматично генерує рекомендації щодо тактичних і стратегічних дій, які залежать від загального рівня ризику:

для низького ризику – підтримка стандартного режиму безпеки;

для середнього ризику – активізація цільових заходів в окремих підсистемах;

для високого ризику – антикризове реагування та аудит.

Окрім узагальнених рекомендацій, система формує окремі текстові інструкції для кожної з трьох підсистем відповідно до їхнього індивідуального рівня ризику. Інформація виводиться у зручному форматі з бази знань, зчитаної з попередньо підготовлених таблиць.

4. Аналітичні таблиці та графічна візуалізація. Центральний блок також містить деталізовані підрозділи з аналітичною інформацією (рис. 3.9):

Фінансова складова – виводиться таблиця ключових фінансових показників, що були розраховані системою. Кожен індикатор супроводжується формулою та значенням.

Кадрова складова – забезпечує інтерактивний вибір працівника з подальшою побудовою графіка його цифрової активності. Система візуалізує періоди аномальної поведінки, що мають високу ймовірність ризику, з використанням аналітичної моделі виявлення інцидентів.

Такий підхід дозволяє керівництву підприємства не лише оперативно отримувати узагальнені оцінки безпеки, але й глибоко аналізувати конкретні складові ризику, що забезпечує проактивне управління системою економічної безпеки.

З метою перевірки ефективності запропонованої системи оцінювання економічної безпеки підприємства, яка враховує сукупний вплив фінансової, кадрової, операційної складових із включенням цифрових ризиків як внутрішнього аспекту кожної підсистеми, було проведено апробацію на промислових підприємствах різного профілю:

ПрАТ «Інститут керамічного машинобудування «Кераммаш»

ПрАТ «Дружківський завод металевих виробів»

ТОВ «Видавництво Фоліо»

ПрАТ «ВО «КОНТИ»

ТОВ «Софтсерв Технології»

ДП «Львіввугілля»

ПрАТ «Кераммаш» - це спеціалізоване науково-технічне підприємство, що займається проектуванням та виготовленням складного промислового термічного обладнання, зокрема енергозберігаючих печей для металургії та керамічної галузі. Компанія поєднує в собі функції машинобудівного заводу та проектного інституту, розробляючи автоматизовані системи управління нагрівом, які самі по собі є інструментом автоматизації для замовників.

## Показники Фінансової складової безпеки

|    | formula                                                                                | number |
|----|----------------------------------------------------------------------------------------|--------|
| 0  | Чистий прибуток / Загальна вартість активів                                            | 0.0850 |
| 1  | Валовий прибуток / Загальні поточні зобов'язання                                       | 0.9090 |
| 2  | Валовий прибуток / Загальна вартість активів                                           | 0.4880 |
| 3  | Валовий прибуток / Загальний виторг                                                    | 0.1250 |
| 4  | Запаси / Загальний виторг                                                              | 0.1060 |
| 6  | Чистий прибуток / Загальний виторг                                                     | 0.0220 |
| 7  | Валовий прибуток за 3 роки / Загальний виторг                                          | 0.4880 |
| 8  | (Загальні оборотні активи - Загальні поточні зобов'язання) / Загальна вартість активів | 0.3170 |
| 9  | (Загальні пасиви - Гроші та їх еквіваленти) / Загальний виторг                         | 0.2350 |
| 10 | Загальні оборотні активи / Загальні поточні зобов'язання                               | 1.5910 |
| 11 | Запаси / Собівартість реалізованої продукції                                           | 0.1210 |
| 12 | Загальні оборотні активи / Загальні зобов'язання                                       | 0.8540 |
| 13 | Загальні поточні зобов'язання / Собівартість реалізованої продукції                    | 0.1570 |

## Показники Кадрової складової безпеки

Оберіть робітника

Робітник 7

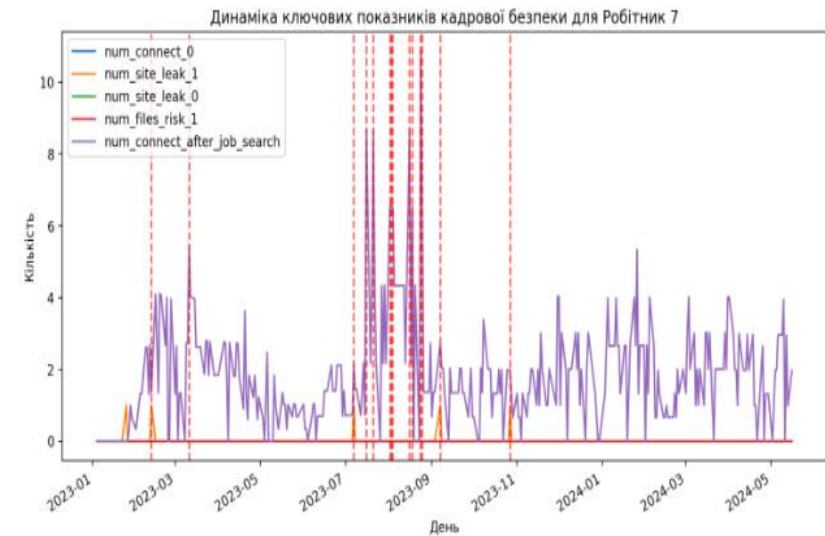


Рис. 3.9. Вигляд інформаційної системи економічної безпеки: показники фінансової та кадрової підсистем.

Джерело: складено автором

Застосування моделей прогнозування банкрутства дозволило встановити середній рівень ризику фінансової підсистеми економічної безпеки, що свідчить про наявність певних вразливостей, які можуть мати вплив на фінансову стабільність підприємства у разі негативних зовнішніх чи внутрішніх змін. Показник аномальних дій персоналу вказує на наявність поодиноких відхилень від стандартних операційних процедур, що може бути пов'язано з адаптацією колективу до роботи в кризових умовах та зміною чисельності штату. Індекс техніко-технологічної безпеки підтверджує високий рівень автоматизації. Використання багаторівневої системи АСУТП, інтеграція датчиків та наявність автоматизованих робочих місць для аналітиків відділу якості дозволяють ефективно мінімізувати технологічні ризики. Високий технологічний потенціал та науковість продукції компенсують середні фінансові ризики, формуючи стійку модель розвитку навіть за умов зовнішньої нестабільності.

ПрАТ «Дружківський завод металевих виробів» є найбільшим в Україні виробником кріплення загального призначення, забезпечуючи потреби машинобудування та залізничного транспорту широким спектром болтів, гайок та шайб високої міцності. Це потужне індустріальне підприємство повного циклу, що займає стратегічно важливу нішу в металургійному секторі країни.

Моделювання ймовірності банкрутства зафіксувало показник 0,53, що є критичним для даного сектору та пояснюється значною волатильністю доходів і періодами чистих збитків у ретроспективі. Це свідчить про високу чутливість фінансової підсистеми до макроекономічних шоків та обмежену здатність до самофінансування модернізації в умовах ринкової нестабільності. Показник аномальних дій персоналу є найвищим серед досліджуваних об'єктів, що вказує на ризики витоку конфіденційних даних, зумовлених недостатньою цифровізацією контрольних функцій та застарілими методами управління кадрами. Низький індекс техніко-технологічної безпеки обумовлений

експлуатацією значної частки морально зношеного обладнання, що потребує негайного оновлення для збереження конкурентоспроможності.

ТОВ «Видавництво Фоліо» - один із провідних приватних видавничих домів України, що спеціалізується на випуску широкого спектра художньої та наукової літератури й активно впроваджує сучасні цифрові моделі виробництва. Компанія функціонує як адаптивне підприємство, що трансформувало традиційну галузь через інтеграцію технологій «друк на вимогу» та цифрових каналів дистрибуції.

Застосування моделей прогнозування виявило найнижчий рівень ймовірності банкрутства, що підтверджує високу стійкість фінансової моделі видавництва до ринкових коливань та ефективність обраної стратегії розвитку. Відсутність аномальних дій персоналу свідчить про стабільність внутрішнього середовища, прозорість HR-процесів та високу кваліфікацію співробітників, які працюють із сучасним цифровим обладнанням. Індекс техніко-технологічної безпеки відображає успішну реалізацію стратегії цифровізації, використання сучасних друкарських комплексів та ефективний захист інтелектуальної власності від системного піратства.

ТОВ «Софтсерв Технології» є частиною глобальної IT-консалтингової компанії SoftServe, що спеціалізується на розробці програмного забезпечення та цифровій трансформації для клієнтів у сферах охорони здоров'я, фінансів та ритейлу. Компанія є одним із лідерів українського IT-ринку за рівнем доходу та інноваційності.

Низька ймовірність банкрутства за прогнозною моделлю свідчить про те, що фінансова підсистема безпеки перебуває у зоні комфорту, де поточні доходи значно перевищують будь-які операційні зобов'язання. Індекс техніко-технологічної безпеки на рівні 0,86 є найвищим у вибірці. Така оцінка обумовлена не лише використанням передових засобів розробки, а й глибокою інтеграцією міжнародних стандартів у повсякденну діяльність. Відсутність аномальних дій персоналу вказує на виняткову ефективність HR-процесів та внутрішнього контролю. Компанія використовує власну систему сертифікації

SSA, яка передбачає суворі технічні іспити, перевірку рівня англійської мови та психологічне тестування. Це створює середовище високої професійної відповідальності, де ризик навмисних або ненавмисних порушень зводиться до мінімуму.

ПрАТ «ВО «КОНТИ» - великий виробник кондитерської продукції, відомий широким асортиментом солодоців та значними виробничими потужностями в Донецькій області. Підприємство тривалий час займало лідируючі позиції в харчовій промисловості України, проте зараз перебуває у стані глибокої трансформації через втрату активів та ринків збуту.

Ймовірність банкрутства на рівні 0,79 свідчить про критичний стан фінансової безпеки, що зумовлено колосальним борговим навантаженням та збитковістю діяльності протягом останніх років. Показник аномальних дій вказує на намагання менеджменту зберегти контроль над залишками інфраструктури в умовах радикального скорочення персоналу. Індекс техніко-технологічної безпеки (0,55) відображає наявність сучасного обладнання, яке, проте, не може бути ефективно використане через операційну зупинку основних ліній у 2025 році. Економічна безпека компанії повністю залежить від зовнішнього фінансування та стратегії виживання

Державне підприємство «Львіввугілля» є стратегічно важливим об'єктом енергетичного сектору України, що об'єднує кілька вуглевидобувних шахт у Львівській області. Діяльність підприємства спрямована на забезпечення паливної незалежності держави, проте наразі воно перебуває в епіцентрі системної кризи.

Ймовірність банкрутства є критичною, що підкріплюється накопиченням податкового боргу та значними загальними зобов'язаннями. Кількість аномальних дій персоналу вказує на розвал управлінської вертикалі, що супроводжується високими ризиками втрати даних. Індекс техніко-технологічної безпеки відображає катастрофічний стан шахтного обладнання, що призводить до аварій, затоплень та неможливості виконання виробничих планів.

На основі розрахованих індикаторів сформовано зведену оцінку стану безпеки досліджуваних суб'єктів господарювання (рис. 3.10, табл. 3.11). Аналіз свідчить про пряму залежність між рівнем технологічного оновлення та загальною економічною стійкістю: підприємства, що активніше інтегрують цифрові технології, демонструють кращі показники безпеки порівняно з суб'єктами, що функціонують у традиційній індустріальній парадигмі.

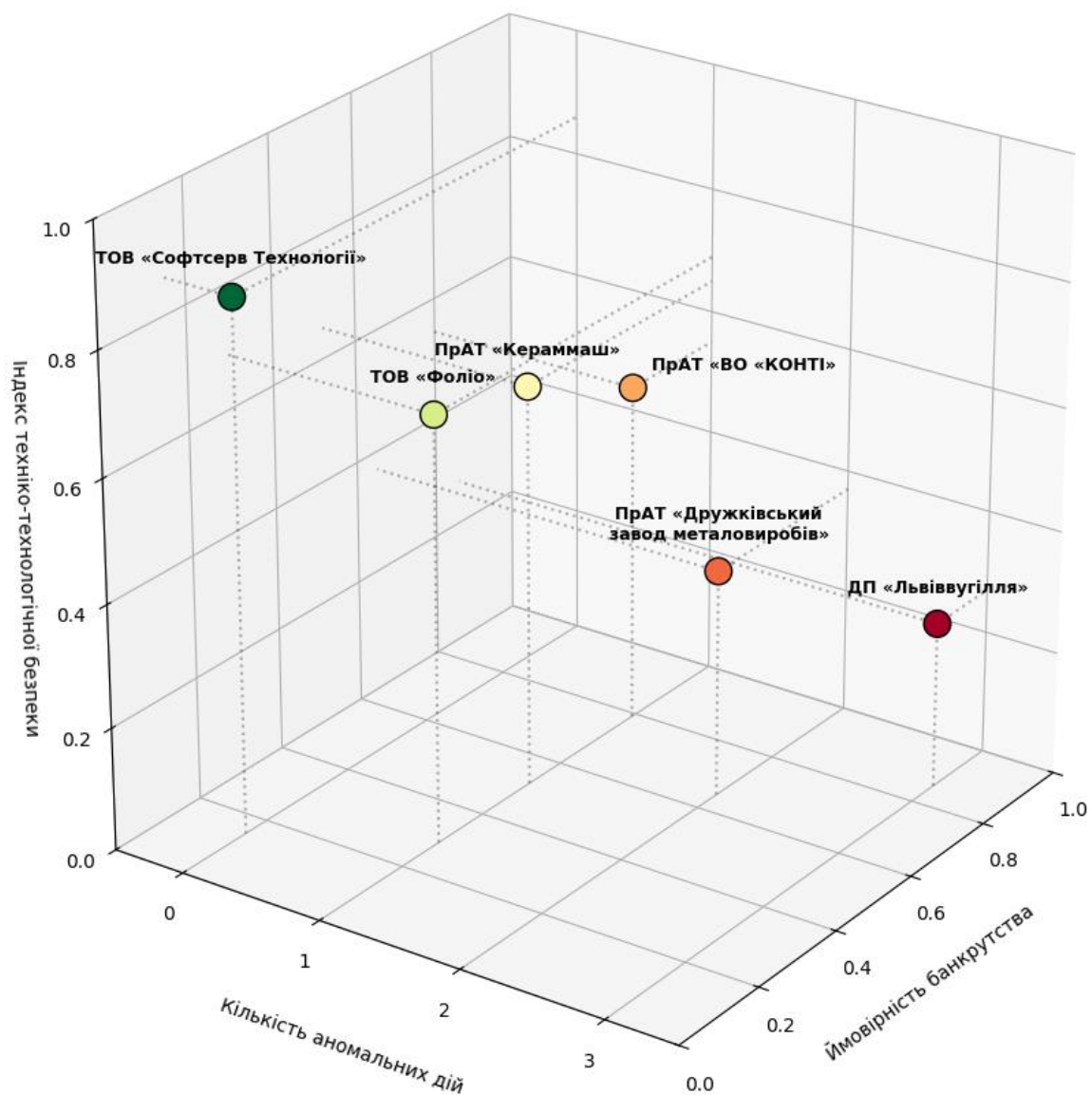


Рис. 3.10. Загальні результати апробації оцінки системи економічної безпеки в умовах цифрової трансформації на кількох українських підприємствах.

Джерело: складено автором

Таблиця 3.11

Загальні результати апробації оцінки системи економічної безпеки в умовах цифрової трансформації на кількох українських підприємствах

| Назва підприємства                          | Ймовірність банкрутства | Кількість аномальних дій працівників | Індекс техніко-технологічної безпеки |
|---------------------------------------------|-------------------------|--------------------------------------|--------------------------------------|
| ПрАТ «Кераммаш»                             | 0,52                    | 1                                    | 0,65                                 |
| ПрАТ «Дружківський завод металевих виробів» | 0,65                    | 2                                    | 0,37                                 |
| ТОВ «Фоліо»                                 | 0,30                    | 1                                    | 0,69                                 |
| ПрАТ «ВО «КОНТИ»                            | 0,79                    | 1                                    | 0,55                                 |
| ТОВ «Софтсерв Технології»                   | 0,15                    | 0                                    | 0,86                                 |
| ДП «Львіввугілля»                           | 0,86                    | 3                                    | 0,27                                 |

Джерело: складено автором

На основі розрахованих індикаторів та виявлених зон ризику для кожного підприємства, сформовано узагальнену таблицю стратегічних рекомендацій (табл. 3.12). Заходи спрямовані на нівелювання критичних загроз та зміцнення підсистем економічної безпеки.

Таблиця 3.12

Рекомендації щодо зміцнення економічної безпеки на проаналізованих українських підприємствах

| Компанія        | Ключові зони ризику                                            | Рекомендовані управлінські заходи                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ПрАТ «Кераммаш» | Фінансова нестабільність                                       | <ul style="list-style-type: none"> <li>Розробити та протестувати протоколи аварійного відновлення даних та перенесення критичних серверів у хмарні сховища для захисту від фізичних загроз.</li> <li>Формалізувати посадові інструкції та впровадити систему КРІ для мінімізації поодиноких аномальних дій персоналу.</li> </ul>                                                  |
| ПрАТ «ДЗМВ»     | Застаріле обладнання та високі ризики інсайдерської активності | <ul style="list-style-type: none"> <li>Провести термінову реструктуризацію заборгованості та оптимізацію структури витрат</li> <li>Впровадити систему SIEM для моніторингу дій персоналу та запобігання несанкціонованому доступу до активів підприємства.</li> <li>Розпочати поетапну модернізацію парку обладнання, залучаючи кредитні кошти під інноваційні проекти</li> </ul> |

|                           |                                                    |                                                                                                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ТОВ «Фоліо»               | Масштабування ІТ-інфраструктури                    | <ul style="list-style-type: none"> <li>Провести комплексний аудит ІТ-інфраструктури на предмет вразливостей перед подальшим розширенням каналів цифрової дистрибуції.</li> <li>Активізувати використання інструментів електронної комерції для підтримки високих темпів зростання доходу.</li> </ul> |
| ТОВ «Софтсерв Технології» | Стрімке масштабування                              | <ul style="list-style-type: none"> <li>Впровадити системи моніторингу безпеки ШІ-агентів для запобігання витоків конфіденційних даних клієнтів.</li> <li>Продовжити автоматизацію комплаєнсу за стандартами для скорочення витрат на інфраструктуру.</li> </ul>                                      |
| ПрАТ «ВО «КОНТІ»          | Критична фінансова ситуація                        | <ul style="list-style-type: none"> <li>Оптимізувати витрати на утримання залишків інфраструктури та персоналу</li> <li>Розпочати переговори з кредиторами щодо реструктуризації боргу</li> </ul>                                                                                                     |
| ДП «Львіввугілля»         | Суттєві кадрові ризики та технологічна відсталість | <ul style="list-style-type: none"> <li>Провести повний незалежний аудит та заміну менеджменту</li> <li>Впровадити найкращі стандарти управління процесами</li> <li>Забезпечити цільове використання бюджетних коштів для запобігання аваріям та оновлення основного фонду</li> </ul>                 |

Джерело: складено автором

Враховуючи середній рівень фінансового ризику ПрАТ «Інститут керамічного машинобудування «Кераммаш» та специфіку його діяльності як науково-виробничого центру, рекомендовано для цього підприємства розробити та протестувати протоколи аварійного відновлення даних із перенесенням критичних серверних потужностей у хмарні сховища для мінімізації впливу фізичних загроз у прифронтовій зоні. Крім того, управлінські заходи мають передбачати формалізацію посадових інструкцій та впровадження системи КРІ, що дозволить нівелювати поодинокі аномальні дії персоналу та підвищити продуктивність праці в умовах обмеженого штату.

З огляду на стан застарілого обладнання та високі ризики інсайдерської активності ПрАТ «Дружківський завод металевих виробів», рекомендовано для цього підприємства провести термінову реструктуризацію заборгованості та оптимізацію структури витрат для підвищення коефіцієнта поточної ліквідності. Додатково пропонується впровадити систему SIEM для моніторингу дій персоналу з метою запобігання несанкціонованому доступу

до активів, а також розпочати поетапну модернізацію парку обладнання через залучення кредитних коштів під інноваційні.

В межах стратегії масштабування ІТ-інфраструктури ТОВ «Видавництво Фоліо», рекомендовано для цього підприємства провести комплексний аудит систем на предмет виявлення вразливостей перед подальшим розширенням каналів цифрової дистрибуції. Важливим напрямом зміцнення безпеки є активізація використання інструментів електронної комерції для підтримки високих темпів зростання доходу.

Для управління ризиками стрімкого масштабування ТОВ «Софтсерв Технології» при мінімальній ймовірності банкрутства, рекомендовано для цього підприємства впровадити спеціалізовані системи моніторингу безпеки ІІІ-агентів для запобігання витоку конфіденційних даних клієнтів. Також доцільним є продовження повної автоматизації процесів комплаєнсу за міжнародними стандартами, що дозволить оптимізувати витрати на цифрову інфраструктуру при подальшому зростанні обсягів розробки.

Зважаючи на критичну фінансову ситуацію ПрАТ «ВО «КОНТІ», рекомендовано для цього підприємства максимально оптимізувати витрати на утримання залишків промислової інфраструктури та обмеженого персоналу. Пріоритетним кроком має стати початок переговорів з кредиторами щодо глибокої реструктуризації боргу.

Оцінюючи суттєві кадрові ризики та технологічну відсталість ДП «Львіввугілля», рекомендовано для цього підприємства провести повний незалежний аудит та радикальну заміну менеджменту. Стратегія відновлення повинна базуватися на впровадженні найкращих світових стандартів управління процесами та забезпеченні жорсткого цільового використання бюджетних коштів для оновлення основного фонду, що є критичним для запобігання техногенним аваріям на шахтах.

Узагальнюючи результати проведеного дослідження шести репрезентативних підприємств, встановлено пряму залежність між рівнем економічної безпеки в умовах цифровізації та загальною стійкістю кожної

підсистеми суб'єктів господарювання. Аналіз підтверджує, що для високотехнологічних компаній, таких як ТОВ «Софтсерв Технології» та ТОВ «Видавництво Фоліо», цифрова трансформація та впровадження систем міжнародної сертифікації виступають ключовими буферами проти макроекономічних ризиків, забезпечуючи мінімальну ймовірність банкрутства. Натомість для підприємств традиційного індустріального сектору та державної форми власності, зокрема ДП «Львіввугілля» та ПрАТ «ВО «КОНТІ», критично низькі індекси технологічної безпеки у поєднанні з високим рівнем аномальних дій персоналу стають каталізаторами фінансової деградації та накопичення зобов'язань. Таким чином, запропоновані управлінські заходи, що інтегрують інструменти технічного моніторингу з механізмами фінансової реструктуризації, є необхідною умовою для забезпечення адаптивності та виходу підприємств із зони критичного ризику в умовах цифрової економіки.

### **Висновки до третього розділу**

У третьому розділі проведено економіко-математичне моделювання та розроблено прикладний інструментарій забезпечення економічної безпеки українських підприємств в умовах цифровізації. Отримані результати дозволяють сформулювати такі висновки:

1. Удосконалено методичний підхід до оцінки фінансово-економічної стійкості шляхом застосування алгоритмів машинного навчання на масиві даних 570 підприємств за період 2014–2020 рр. Встановлено, що модель XGBoost з L1-регуляризацією забезпечує найвищу прогностичну точність порівняно з традиційними економетричними методами.

2. Доведено, що впровадження інструментів електронної комерції та розвиток інтернет-присутності є статистично значущими факторами, які знижують ймовірність дефолту підприємства на 2,6–3,0%.

3. Запропоновано модель управління кадровою безпекою, засновану на інтелектуальному аналізі цифрової поведінки персоналу. Застосування алгоритму Isolation Forest дозволило ідентифікувати латентні загрози на ранніх стадіях. Використання великих мовних моделей для семантичного аналізу мережевої активності забезпечило високу якість класифікації контекстуальних ризиків, що є недоступним для стандартних систем фільтрації трафіку.

4. Розроблено комплексну модель інтегральної оцінки стану економічної безпеки, реалізовану у формі прикладної інформаційної системи на базі фреймворку Streamlit. Система базується на уніфікованій трирівневій шкалі ризиків, що синтезує фінансові показники, індикатори аномальної поведінки персоналу та рівень технологічної зрілості суб'єкта господарювання.

5. Встановлено, що високий рівень кадрових ризиків здатний нівелювати позитивний вплив фінансової стабільності, що обґрунтовує необхідність комплексного, а не ізольованого управління функціональними компонентами безпеки.

6. Обґрунтовано стратегічну роль цифрової трансформації як детермінуючого фактора забезпечення життєздатності підприємства. Результати моделювання підтверджують, що цифровізація бізнес-процесів не лише підвищує операційну ефективність, а й виступає превентивним механізмом нейтралізації зовнішніх та внутрішніх загроз в умовах волатильності економічного середовища.

Наукові результати дослідження висвітлено у роботах [20, 113, 116, 117].

## ВИСНОВКИ

1. Дослідження теоретичних підходів до визначення сутності та структури економічної безпеки підприємства підтвердило її багатоаспектний і міждисциплінарний характер. Систематизація наукових концепцій дозволила інтерпретувати економічну безпеку як динамічний стан суб'єкта господарювання, що характеризується сукупністю кількісних та якісних індикаторів здатності системи забезпечувати захищеність економічних інтересів, стійкий розвиток та адаптивність до деструктивних впливів середовища. Обґрунтовано, що в умовах цифровізації традиційна архітектура безпеки зазнає суттєвої трансформації: фінансова, кадрова, техніко-технологічна та інформаційна підсистеми набувають ознак пріоритетності, оскільки саме вони формують базис цифрової резистентності підприємства, а їхня злагоджена взаємодія визначає загальний рівень стійкості суб'єкта господарювання.

2. Встановлено, що цифрова трансформація є стратегічним збуренням, яке змінює операційну модель підприємства та зумовлює виникнення якісно нових класів загроз, що не охоплюються класичним інструментарієм безпеки. Доведено дуальність її впливу: поряд із підвищенням операційної ефективності та клієнтоорієнтованості, цифрові технології генерують специфічні кіберризики, зростання капіталомісткості бізнесу та підвищену вразливість до інсайдерських загроз. Систематизація інструментарію цифрової трансформації крізь призму цього подвійного впливу дозволила обґрунтувати необхідність переосмислення функціональних складових системи безпеки та конкретизувати вразливості, що виникають унаслідок цифровізації фінансових, кадрових і техніко-технологічних процесів.

3. Розроблено та обґрунтовано концептуальну модель формування інтегрованої системи економічної безпеки підприємства в умовах цифрової трансформації, специфічною особливістю якої є виокремлення цифрової безпеки як наскрізного компонента, що інтегрується в усі функціональні підсистеми та виступає головною сполучною ланкою, яка забезпечує цілісність захисту й

запобігає поширенню ризиків у цифровому середовищі. Запропонована модель інтегрує фінансову, кадрову та техніко-технологічну підсистеми в єдину структуру, де базисом для формування стратегічного орієнтиру розвитку слугує інтегральна оцінка рівня безпеки, що формалізує стан захищеності через сукупність кількісних та якісних показників. Таким чином, закладено теоретичний фундамент для розуміння сутності економічної безпеки в умовах цифрової економіки, що є базою для подальших наукових досліджень та формування практичних рекомендацій.

4. Узагальнено еволюцію методичних підходів до оцінювання економічної безпеки підприємства та обґрунтовано виокремлення сучасного етапу, що характеризується інтеграцією інструментів штучного інтелекту, машинного навчання та адаптивного моніторингу в систему підтримки управлінських рішень. Встановлено, що традиційні статичні моделі, орієнтовані на ретроспективну фінансову звітність, втрачають ефективність у цифровому середовищі через неможливість урахування специфічних ІТ-ризиків та відсутність інструментарію для обробки великих масивів даних у режимі реального часу. Доведено доцільність трансформації математичного апарату моделювання складових безпеки: інтеграцію класичних статистичних методів з алгоритмами машинного навчання, впровадження моделей виявлення аномалій та застосування ієрархічних моделей та апарату нечіткої логіки.

5. Удосконалено методичний підхід до оцінювання фінансової складової економічної безпеки підприємства шляхом інтеграції традиційних фінансових індикаторів із показниками цифрової активності. Апробація розробленого підходу засвідчила, що модель XGBoost з L1-регуляризацією забезпечує найвищу прогностичну точність порівняно з традиційними економетричними методами. Застосування методів пояснюваного штучного дозволило не лише констатувати рівень фінансового ризику, а й ідентифікувати нелінійні порогові значення чинників впливу для прийняття превентивних управлінських рішень. Встановлено, що впровадження інструментів електронної комерції та розвиток інтернет-присутності є статистично значущими факторами, що знижують імовірність дефолту підприємства на 2,6-3,0%, що підтверджує визначальну роль

цифровізації як превентивного механізму нейтралізації фінансових загроз.

6. Розроблено модель управління кадровою складовою економічної безпеки на основі інтелектуального аналізу цифрової поведінки персоналу. На відміну від традиційних підходів, що потребують заздалегідь розміченої навчальної вибірки, запропонований підхід базується на алгоритмі Isolation Forest, що навчається виключно на нормальних поведінкових шаблонах і забезпечує раннє виявлення інсайдерських загроз ще до вчинення деструктивних дій. Семантичне збагачення даних корпоративного моніторингу за допомогою великих мовних моделей забезпечило високу якість класифікації контекстуальних ризиків мережевої активності, що є недоступним для стандартних систем фільтрації трафіку.

7. Удосконалено методичний підхід до оцінювання техніко-технологічної складової економічної безпеки на основі ієрархічної моделі із застосуванням апарату нечіткої логіки, що забезпечує можливість формалізації якісних експертних оцінок щодо цифрової зрілості підприємства та їх переведення в кількісний інтегральний індекс, що є критично важливим за умов високої невизначеності технологічного середовища.

8. Розроблено блочно-модульну інформаційну модель управління системою економічної безпеки, що інтегрує фінансовий, кадровий і техніко-технологічний модулі в єдиний аналітичний простір та забезпечує її високу адаптивність з існуючими системами підприємства. Обґрунтовано доцільність використання нелінійного інтегрального показника економічної безпеки, що враховує синергетичний ефект цифрових ризиків, якого неможливо досягти за допомогою традиційних адитивних методів згортання показників, а також розроблено тривимірну візуалізацію (“гіперпростір”) інтегрального індексу для ідентифікації зон стратегічного ризику та оцінки чутливості загального рівня безпеки до варіацій параметрів ключових підсистем.

9. Реалізовано прикладну інформаційну систему комплексної оцінки та моніторингу стану економічної безпеки підприємства на базі фреймворку Streamlit, яка забезпечує замкнений цикл управління: від автоматизованого збору та очищення даних до розрахунку уніфікованого інтегрального індексу за

трирівневою шкалою ризиків і генерації адаптивних управлінських рекомендацій у режимі наближеного до реального часу. Апробація системи на даних вітчизняних підприємств підтвердила її практичну ефективність та можливість реального впровадження в корпоративні системи управління.

Таким чином, результати дисертаційного дослідження поглиблюють наукові засади розуміння економічної безпеки в системі цифрової трансформації та пропонують ефективний інструментарій її забезпечення. Розроблені теоретичні положення, методичні підходи й практичні інструменти можуть бути використані для підвищення стійкості функціонування підприємств, зміцнення їх здатності протистояти фінансовим, кадровим та технологічним загрозам в умовах цифрової економіки, а також для удосконалення системи стратегічного управління на рівні окремого суб'єкта господарювання.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 157 Cybersecurity Statistics and Trends [updated 2025]. *Varonis*. URL: <https://www.varonis.com/blog/cybersecurity-statistics#:~:text=7,cyberattacks%20in%202020%2C%20more%20than>
2. A faster way to build and share data apps. URL: <https://streamlit.io/>
3. Abbing J., Linssen O. Requirements for a Decision Support System for Managing Complexity of Multidimensional IT Project Assessments in the Context of IT Portfolio Management. *PVM (Projektmanagement und Vorgehensmodelle)* 2023. Nachhaltige IT-Projekte At: Hagen, Germany. URL: [https://www.researchgate.net/publication/375824930\\_Requirements\\_for\\_a\\_Decision\\_Support\\_System\\_for\\_Managing\\_Complexity\\_of\\_Multidimensional\\_IT\\_Project\\_Assessments\\_in\\_the\\_Context\\_of\\_IT\\_Portfolio\\_Management](https://www.researchgate.net/publication/375824930_Requirements_for_a_Decision_Support_System_for_Managing_Complexity_of_Multidimensional_IT_Project_Assessments_in_the_Context_of_IT_Portfolio_Management)
4. Abdin M., Aneja J., Awadalla H., Awadallah A. et al. Phi-3 Technical Report: A Highly Capable Language Model Locally on Your Phone. 2024. DOI: <https://doi.org/10.48550/arXiv.2404.14219>
5. Ahn H., Kim K. Bankruptcy prediction modeling with hybrid case-based reasoning and genetic algorithms approach. *Applied Soft Computing*, 2009, 9, 599–607. DOI: <http://dx.doi.org/10.1016/j.asoc.2008.08.002>
6. Aker Y., Karavardar A. Using machine learning methods in financial distress prediction: sample of small and medium sized enterprises operating in Turkey. *Ege Academic Review*. 2023, 23(2), 145-162. DOI: <https://doi.org/10.21121/eab.1027084>
7. Alcacer J., Cantwell L. Piscitello J. Internationalization in the information age: A new era for places, firms, and international business networks? *Journal of International Business Studies*. 2016, 5, 499–512. URL: <https://link.springer.com/article/10.1057/jibs.2016.22>
8. Al-Shehari T., Rosaci D., Al-Razgan M., Alfaqih T., Kadri M., Afzal H., Nawaz R. Enhancing Insider Threat Detection in Imbalanced Cybersecurity Settings

Using the Density-Based Local Outlier Factor Algorithm. *IEEE Access*. 2024. 99 (1-1). DOI: <https://doi.org/10.1109/ACCESS.2024.3373694>

9. Altman E. Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *Journal of Finance*. 1968. URL: <https://www.jstor.org/stable/2978933>

10. Angelova R., Stoyancheva D. Digitalization, financial insolvency and bankruptcy risk forecasting of Bulgarian agricultural enterprises. *Scientific Papers Series Management, Economic Engineering in Agriculture and Rural Development*. 2023, 23 (2), 29-36. URL: [https://managementjournal.usamv.ro/pdf/vol.23\\_2/Art3.pdf](https://managementjournal.usamv.ro/pdf/vol.23_2/Art3.pdf)

11. API by YouControl for Automated Compliance and Counterparty Data Solution. *YouScore*. URL: <https://youscore.com.ua/en/>

12. Babbar A., Janardhanan R., Paternoster R., Soller H. Why most digital banking transformations fail – and how to flip the odds. *McKinsey&Company*. URL: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/why-most-digital-banking-transformations-fail-and-how-to-flip-the-odds>

13. Bankruptcy Score: Are You at Risk for Filing Bankruptcy? *Galler Law*, 2018. URL: <https://gallerlaw.com/bankruptcy-score-are-you-at-risk-for-filing-bankruptcy/>

14. Ben Jabeur, S. & Serret, V. Bankruptcy prediction using fuzzy convolutional neural networks. *Research in International Business and Finance, Elsevier*, 2023, 64(C). DOI: 10.1016/j.ribaf.2022.101844

15. Berman S. Digital transformation: opportunities to create new business models. *Strategy & Leadership*. 2012, 40 (2), 16-24. DOI: <https://doi.org/10.1108/10878571211209314>

16. Bilychenko M. Information model for managing enterprise economic security under digital transformation. *Innovations and New Directions in Scientific Research: proceedings of the 2nd International Scientific Conference* (Manchester, United Kingdom, 20 Sept. 2025). 2025. P.21-24. DOI: 10.64076/iedc250920.07.

17. Bilychenko M. Modeling of risks and threats in the management of personnel security of the enterprise. *Proceedings of the 6th International Conference*

on Strategies, Models and Technologies of Economic Systems Management (SMTESM 2019). 2019. DOI: [10.2991/smtesm-19.2019.92](https://doi.org/10.2991/smtesm-19.2019.92)

18. Bilychenko M. Modeling of the technical-technological component of economic security in the context of enterprise digitalization. *Economic Innovations*, 2025, 27(4(97)), 13-22. DOI [https://doi.org/10.31520/ei.2025.27.4\(97\).13-22](https://doi.org/10.31520/ei.2025.27.4(97).13-22)

19. Bilychenko M. Modern approaches to evaluate company's financial security. *X International scientific and practical conference «Modern Trends in the Development of Scientific Space»* (February 14-16, 2024) Dresden, Germany, International Scientific Unity. 2024. 286 p.

20. Bilychenko M., Kasianova N., Smerichevskyi S., Lavrynenko O., Kryvovyazyuk I. Development of a smart personnel security system using machine learning. *Cyber Security and Data Protection 2025 (CSDP 2025): proceedings* (Lviv, Ukraine, 31 Jul. 2025). 2025. P 203-215.

21. Bushra B. S., Najwa A. Insider Threat Detection Using Machine Learning Approach. *Applied Sciences*, 2023, 13(1), 259. DOI: <https://doi.org/10.3390/app13010259>

22. Cao Y., Shao Y., Zhang H. Study on early warning of E-commerce enterprise financial risk based on deep learning algorithm. *Electronic Commerce Research*. 2021, 22, 21–36. DOI: <https://doi.org/10.1007/s10660-020-09454-9>

23. Chen W., Srinivasan S. Going Digital: Implications for Firm Value and Performance. *SSRN Electronic Journal*. 2023. DOI: <https://dx.doi.org/10.2139/ssrn.4177947> .

24. Chouksey V. Automatic Selection of Outlier Detection Techniques. 2018. URL: [https://pure.tue.nl/ws/portalfiles/portal/109406381/CSE663\\_Vishal\\_Chouksey\\_31\\_aug.pdf](https://pure.tue.nl/ws/portalfiles/portal/109406381/CSE663_Vishal_Chouksey_31_aug.pdf)

25. Christian M., Thomas H., Benlian A. Digital Transformation Strategies. *Business & Information Systems Engineering*. 2015, 57 (5), 339-343. URL: <https://aisel.aisnet.org/bise/vol57/iss5/5>

26. Cost of a Data Breach: A Million-Dollar Race to Detect and Respond, *IBM Security*, 2025. URL: <https://www.ibm.com/reports/data-breach>
27. Cross-validation: evaluating estimator performance. URL: [https://scikit-learn.org/stable/modules/cross\\_validation.html](https://scikit-learn.org/stable/modules/cross_validation.html)
28. Cusolito A., Lederman D., Pena J. The Effects of Digital-Technology Adoption on Productivity and Factor Demand: Firm-Level Evidence from Developing Countries. *Policy Research Working Paper*. 2020. № 9333. URL: <https://documents1.worldbank.org/curated/en/829161595512126439/pdf/The-Effects-of-Digital-Technology-Adoption-on-Productivity-and-Factor-Demand-Firm-level-Evidence-from-Developing-Countries.pdf>
29. Data Services. 2025. URL: <https://www.accenture.com/gb-en/services/data-ai/cloud-data-ai>
30. Decision Support Systems (DSS). *The Global Centre for Risk and Innovation (GCRI)* 2025. URL: <https://therisk.global/guide/decision-support-systems-dss/?srsltid=AfmBOorzlmpEXVHjmx7Zh7ruL1Y1YWzPEncSbd9MycBW32NgGeBI8WSD#:~:text=Data%20Collection%3A%20Efficient%20data%20management,and%20reliably%2C%20minimizing%20manual%20intervention>
31. Digital transformation and cyber security. *KPMG*. 2019. URL: <https://assets.kpmg.com/content/dam/kpmg/in/pdf/2019/03/digital-transformation-cyber-security.pdf>.
32. Digital transformation definition. *Hewlett Packard Enterprise*. URL: <https://www.hpe.com/us/en/what-is/digital-transformation.html>
33. Digital transformation market size. *Fortune business insights*, 2026. URL: <https://www.fortunebusinessinsights.com/digital-transformation-market-104878>
34. Dokiienko L. Financial security of the enterprise: an alternative approach to evaluation and management. *Business, Management and Economics Engineering*, 2021, 19(2), 303-336. DOI: <https://doi.org/10.3846/bmee.2021.14255>

35. Duc C. Le, Nur Zincir-Heywood. Anomaly Detection for Insider Threats Using Unsupervised Ensembles. *IEEE TNSM*, 2021. URL: <https://web.cs.dal.ca/~lcd/pubs/TNSM2021.pdf>
36. e-Government Knowledgebase 2024. URL: <https://publicadministration.un.org/egovkb/en-us/Data-Center>
37. Europe's Digital Decade: digital targets for 2030. URL: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)
38. Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. Embracing Digital Technology: A New Strategic Imperative. *MIT Sloan Management Review*, 2014, 55, 1-12. URL: <https://www.scirp.org/reference/referencespapers?referenceid=3884971>
39. Forth P., Reichert T., Laubier R., Chakraborty S. Flipping the Odds of Digital Transformation Success. *BCG*, 2020. URL: <https://www.bcg.com/publications/2020/increasing-odds-of-success-in-digital-transformation>
40. Fujishima K. Knowledge-driven automated service composition as a method for developing decision support systems. *International Journal for Applied Information Management*, 2021, 2(1), 44-49. <https://doi.org/10.47738/ijaim.v2i1.26>
41. Gavai G., Sricharan K., Gunning D. Supervised and unsupervised methods to detect insider threat from enterprise social and online activity data. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2015, 6 (4), 47-63 URL: <https://isyou.info/jowua/papers/jowua-v6n4-2.pdf>
42. Gökalp E., Martinez V. Digital transformation capability maturity model enabling the assessment of industrial manufacturers. *Computers in Industry*. 2021, 132. DOI: <https://doi.org/10.1016/j.compind.2021.103522>
43. Hamdi, M., Sami M., Adnène A. Artificial Intelligence Techniques for Bankruptcy Prediction of Tunisian Companies: An Application of Machine Learning

and Deep Learning-Based Models. *Journal of Risk and Financial Management*, 2024, 17 (4), 132. DOI: <https://doi.org/10.3390/jrfm17040132>

44. Harahulia A., Suslov V., Horovoy O. Management of economic security of enterprises in the context of digital transformation. *Baltic Journal of Economic Studies*, 2023, 9 (5), 87–93. DOI: <https://doi.org/10.30525/2256-0742/2023-9-5-87-93>

45. Hastie, T., Tibshirani, R., & Friedman, J. The Element of Statistical Learning. California: Springer. 2017. URL: <https://esl.hohoweiya.xyz/book/The%20Elements%20of%20Statistical%20Learning.pdf>

46. Holsapple C.W., Whinston A.B. Decision Support Systems (A Knowledge Based Approach). New York: West Publishing Company, 2003. 860 p.

47. How digitalised have the EU's enterprises become? *Eurostat*, 2024. URL: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240829-1#:~:text=In%202023%2C%2059%25%20of%20EU,for%20large%20enterprises%20was%2091%25.>

48. Huang K., Wang X., Wei W., Madnick S. The Devastating Business Impacts of a Cyber Breach. *HBR*, 2023 URL: <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach#:~:text=Managing%20Cyber%20Risk&text=On%20average%2C%20compnies%20experiencing%20a,and%20cost%20to%20secure%20financing>

49. Ianioglo A., Polajeva T. Origin and definition of the category of economic security of enterprise. *9th Int. Conf. "Business and Management 2016"*, Vilnius, Lithuania. DOI: <http://dx.doi.org/10.3846/bm.2016.46>

50. IDC FutureScape: Worldwide Digital Transformation 2022 Predictions URL: <https://my.idc.com/getdoc.jsp?containerId=US47115521>

51. Internet Archive: Wayback Machine. URL: <https://archive.org/web/>

52. ISO 31000 Blog Series – Risk identification. *Wolters Kluwer*, 2022. URL: <https://www.wolterskluwer.com/en/expert-insights/iso-31000-blog-series-risk-identification#:~:text=In%20the%20risk%20matrix%2C%20we,can%20have%20a%20different%20threshold>

53. Iturriaga F.L., Sanz I.P. Bankruptcy visualization and prediction using neural networks: A study of U.S. commercial banks. *Expert Systems with Applications*, 2015, 42 (6), 2857–2869. <https://doi.org/10.1016/j.eswa.2014.11.025>
54. Jingru G. AI Notes: Regularizing neural networks. *Deeplearning*, 2024. URL: <https://deeplearning.ai/ai-notes/regularization/>
55. Joel L., Doorsamy W. A Review of Missing Data Handling Techniques for Machine Learning. *International Journal of Innovative Technology and Interdisciplinary Sciences*, 2022, 5 (3), 971-1005. DOI: <https://doi.org/10.15157/IJITIS.2022.5.3.971-1005>
56. Kharchuk T. V., Kredisov V. A., Melnik V. V., Purdenko O. A. Improved methods of evaluation of financial security for companies in Ukraine. *Financial and credit activity: problems of theory and practice*, 2020, 1 (32), 213–222. DOI: <https://doi.org/10.18371/fcaptp.v1i32.200300>
57. Kitowski J, Kowal-Pawul A, Lichota W. Identifying Symptoms of Bankruptcy Risk Based on Bankruptcy Prediction Models – A Case Study of Poland. *Sustainability*, 2022, 14(3), 1416. DOI: <https://doi.org/10.3390/su14031416>
58. Kolomiyets G, Rodchenko V, Melentsova O, Korol V, Moskalenko M. The Impact of Digitalization on the Formation of new Business models in Electronic Commerce: Analysis and Trends. *Salud, Ciencia y Tecnología - Serie de Conferencias*, 2024, 3, 652. DOI: <https://doi.org/10.56294/sctconf2024.652>
59. Korol T. Dynamic Bankruptcy Prediction Models for European Enterprises. *Journal of Risk and Financial Management*, 2019, 12 (4), 185. DOI: <https://doi.org/10.3390/jrfm12040185>
60. Kostyunik O., Andriienko M., Voinalovych I., Bosa I., Bilychenko M. Organizational support for the formation of the economic security system of enterprises in the conditions of intellectual and innovative development of society. *Management Theory and Studies for Rural Business and Infrastructure Development*, 2023, 45(4), 399–405. DOI: <https://doi.org/10.15544/mts.2023.39>
61. Kwon W., Li Z., Zhuang S., Sheng Y., Zheng L., Yu C. H., Gonzalez J., Zhang H., Stoica I. Efficient memory management for large language model serving

with pagedattention. *Proceedings of the 29th Symposium on Operating Systems Principles*, 2023, 611–626. DOI: <https://doi.org/10.48550/arXiv.2309.06180>

62. Le D. C., Zincir-Heywood N. Anomaly Detection for Insider Threats Using Unsupervised Ensembles. *IEEE Transactions on Network and Service Management*, 2021, 18 (2), 1152-1164. URL: <https://web.cs.dal.ca/~lcd/pubs/TNSM2021.pdf>

63. Lelyk L., Olikhovskiy V., Mahas N., Olikhovska M. An integrated analysis of enterprise economy security. *Decision Science Letters*. 2022, 11, 299-310. DOI: 10.5267/j.dsl.2022.2.003.

64. Letkovsky S., Jenčová S., Vašaničová P. Is Artificial Intelligence Really More Accurate in Predicting Bankruptcy? *International Journal of Financial Studies*, 2024, 12 (1), 8. DOI: <https://doi.org/10.3390/ijfs12010008>

65. Lin Wei-Chao, Tsai Chih-Fong, Hu Ya-Han, Jhang Jing-Shang. Clustering-based undersampling in class-imbalanced data, *Information Sciences*, 2017, 409–410, 17-26. DOI: <https://doi.org/10.1016/j.ins.2017.05.008>

66. Lindauer B. Insider Threat Test Dataset, 2020. DOI: <https://doi.org/10.1184/R1/12841247>

67. Liu D.-Y., Chen S.-W., Chou T.-C. Resource fit in digital transformation: Lessons learned from the CBC Bank global e-banking project. *Management Decision*, 2011, 49, 1728-1742. DOI: <https://doi.org/10.1108/00251741111183852>

68. Managing risk in digital transformation. *Deloitte*, 2018. URL: [https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za\\_managing\\_risk\\_in\\_digital\\_transformation\\_112018.pdf](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf)

69. Michelucci U. Feature Importance and Selection. In: *Fundamental Mathematical Concepts for Machine Learning in Science*, 2024, 229–242. DOI: [https://doi.org/10.1007/978-3-031-56431-4\\_10](https://doi.org/10.1007/978-3-031-56431-4_10)

70. Min J.H., Lee Y.-C. Bankruptcy prediction using support vector machine with optimal choice of kernel function parameters. *Expert Systems with Applications*, 2005, 28 (4), 603-614. DOI: <https://doi.org/10.1016/j.eswa.2004.12.008>

71. Molnar C. Interpretable Machine Learning: A Guide for Making Black Box Models Explainable, Self-Published. 2022. URL: <https://christophm.github.io/interpretable-ml-book/>
72. Mosiashvili N., Pareliussen J. Digital technology adoption, productivity gains in adopting firms and sectoral spill-overs: Firm-level evidence from Estonia. *OECD Economics Department Working Papers*, 2020, 1638. DOI: 10.1787/ba9d00be-en
73. Naveeda H., Khanb A.U., Qiuc S., Saqibd M., Anwarf S., Usmanf M., Akhtarh N., Barnesi N., Mian A. A Comprehensive Overview of Large Language Models. *ACM Transactions on Intelligent Systems and Technology*, 2023, 16 (5), p. 1-72. DOI: <https://doi.org/10.1145/3744746>.
74. Nguyen T., Newby M., Macaulay M. Information technology adoption in small business: Confirmation of a proposed framework. *Journal of Small Business Management*, 2015, 53 (1), 207–227. DOI: <https://doi.org/10.1111/jsbm.12058>
75. Noviantoro T., Huang J. P. Comparing machine learning algorithms to investigate company financial distress. *Review of Business, Accounting & Finance* 2021, 1, 454–79
76. O'Brien K., Downie A., Scapicchio M. What is digital transformation? *IBM*. URL: <https://www.ibm.com/think/topics/digital-transformation#:~:text=Digital%20transformation%20is%20a%20business,rapid%2C%20customer%2Ddriven%20innovation>
77. Peng Y., Wang G., Kou G., Shi Y. An empirical study of classification algorithm evaluation for financial risk prediction. *Applied Soft Computing*. 2011, 11 (2), 2906–2915. DOI: <https://doi.org/10.1016/j.asoc.2010.11.028>
78. Polupanova K., Khadzhynova O., Simanavičienė Ž. Influence of digital transformation on economic security of enterprises. *Public Security and Public Order*, 2022, 31. DOI: <https://doi.org/10.13165/PSPO-22-31-17>
79. Pricing. *OpenAI: API Platform*. URL: <https://openai.com/api/pricing/>

80. Raissi-Dehkordi M., Carr D. A multi-perspective approach to insider threat detection. *IEEE Military Communications Conference*, 2011. DOI: 10.1109/MILCOM.2011.6127457.
81. Rani, P., Mishra, A.R., Alrasheedi, A.F. et al. Digital transformation project risks assessment using hybrid picture fuzzy distance measure-based additive ratio assessment method. *Scientific Reports*, 2025, 15, 3286 DOI: <https://doi.org/10.1038/s41598-025-86598-4>
82. Rashid T. Agrafiotis I., Nurse J. A New Take on Detecting Insider Threats: Exploring the Use of Hidden Markov Models. *8th ACM CCS International Workshop on Managing Insider Security Threats*, 2016. URL: <https://www.cs.ox.ac.uk/files/8364/MIST2016-RAN-AuthorFinal.pdf>
83. Saaty T. L. The Analytic Hierarchy Process. McGraw-Hill, New York, 1980.
84. Samoilenko Y., Britchenko I., Levchenko I., Lošonczi P., Bilichenko O., Bodnar O. Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Economic Affairs*, 2022, 67 (4), 619–629. DOI: 10.46852/0424-2513.4.2022.28
85. Shekar S., Musa M., Brédart X. Bankruptcy Prediction Using Machine Learning Techniques. *Journal of Risk and Financial Management*, 2022, 15 (1), 35. DOI: <https://doi.org/10.3390/jrfm15010035>
86. Shumeiko D., Rozora I. Handling Missing Values in Machine Learning Regression Problems. *II International Scientific Symposium «Intelligent Solutions» IntSol-2021*, 2021, 28–30. URL: [https://ceur-ws.org/Vol-3106/Short\\_5.pdf](https://ceur-ws.org/Vol-3106/Short_5.pdf)
87. Shynkar S., Gontar Z., Dubyna M., Nasypaiko, D., Fleychuk M. Assessment of economic security of enterprises: Theoretical and methodological aspects. *Business: Theory and Practice*, 2020, 21(1), 261–271. DOI: <https://doi.org/10.3846/btp.2020.11573>
88. Smaje K., LaBerge L., Zimmel R. Three new mandates for capturing a digital transformation's full value. *McKinsey&Company*. URL:

<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-new-mandates-for-capturing-a-digital-transformations-full-value>

89. SME digital transformation analysis report. *China Electronics Standardization Institute*, 2021. URL:

<http://www.chuangze.cn/attached/file/20220507/20220507211176827682.pdf>.

90. Song C., Ma L., Zheng J., Liao J., Kuang H., Yang L. Audit-LLM: Multi-Agent Collaboration for Log-based Insider Threat Detection. *Computer Science*, 2024. DOI: <https://doi.org/10.48550/arXiv.2408.08902>

91. Song Y., Salem M., Hershkop S. System Level User Behavior Biometrics using Fisher Features and Gaussian Mixture Models. *IEEE Security and Privacy Workshops*, 2013. DOI: 10.1109/SPW.2013.33.

92. Subin S. Tech megacaps plan to spend more than \$300 billion in 2025 as AI race intensifies. *CNBC*, 2025. URL: <https://www.cnbc.com/2025/02/08/tech-megacaps-to-spend-more-than-300-billion-in-2025-to-win-in-ai.html#:~:text=Meta%2C%20Amazon%2C%20Alphabet%20and%20Microsoft,y ear%20into%20artificial%20intelligence%20technologies>

93. Thales Data Threat Report: Global Edition, 2025. *Thales Group*. URL: <https://cpl.thalesgroup.com/2025/data-threat-report#form-download>

94. The Future of Job Report 2020. *World Economic Forum*. URL: [https://www3.weforum.org/docs/WEF\\_Future\\_of\\_Jobs\\_2020.pdf](https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf)

95. The Global Risks Report 2023. *World Economic Forum*. URL: [https://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2023.pdf](https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf)

96. The state of AI in 2023: Generative AI's breakout year. *McKinsey Global Institute*. URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year>

97. UA-REGION. URL: <https://www.ua-region.com.ua/>

98. Veganzones D., Séverin E. Corporate failure prediction models in the twenty-first century: a review. *European Business Review*, 2021, 33 (2), 204–226. DOI: <https://doi.org/10.1108/EBR-12-2018-0209>.

99. Vial G. Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 2019, 28, 118-144. DOI: <https://doi.org/10.1016/j.jsis.2019.01.003>
100. What Is Digital Transformation? *Salesforce*. URL: <https://www.salesforce.com/digital-transformation/>
101. Your AI-driven, all-purpose coding partner, seamlessly embedded in the notebook you already use. *Colab*, 2025. URL: <https://colab.google/>.
102. Yvanovich R. Navigating Challenges: the Worrying State of Digital Transformation for SMEs. 2023. URL: <https://blog.trginternational.com/digital-transformation-sme-small-medium-sized-enterprises>.
103. Zhan X. An empirical study on the relationship between the investment value and performance of enterprise informatization. *Statistics&Decisions*, 2019, 6, 185–188.
104. Алькема В.Г., Копитко М.І. Інтегральна оцінка рівня економічної безпеки автомобілебудівних підприємств. *Вчені записки університету "КРОК". Серія: Економіка*, 2015, 39, С. 75-88. URL: [https://library.krok.edu.ua/media/library/category/statti/kopytko\\_0003.pdf](https://library.krok.edu.ua/media/library/category/statti/kopytko_0003.pdf)
105. Андрющенко Т. Ю. Архітектура та основні архітектурні рішення спр в управлінні партнерськими відносинами видавничо-поліграфічних підприємств. *Таврійський науковий вісник. Серія: Технічні науки*, 2023, 4, 3-10. DOI: <https://doi.org/10.32782/tnv-tech.2023.4.1>
106. Ареф'єва О.В., Кузенко Т.Б. Планування економічної безпеки підприємств. К.: Вид-во Європ. ун-ту, 2004. 170 с.
107. Бідюк П. І., Тимошук О. Л., Коваленко А. Є., Коршевніук Л. О. Системи і методи підтримки прийняття рішень: підручник. Київ : КПІ ім. Ігоря Сікорського, 2022. 610 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/73de1d73-bd75-41b3-b775-a5bcfa95a454/content>
108. Бідюк П.І., Кузнєцова Н.В., Терент'єв О.М., Коршевніук Л.О. Системи і методи підтримки прийняття рішень. К.: КПІ ім. Ігоря Сікорського

2022. 259 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/73de1d73-bd75-41b3-b775-a5bcfa95a454/content>

109. Біличенко М. М. Вплив цифрової трансформації на операційні та фінансові показники діяльності підприємств. *Матеріали IV міжнародної науково-практичної конференції «Бізнес-аналітика: моделі, інструменти та технології»*. К.: НАУ, 2023. С. 404-409.

110. Біличенко М. М. Еволюція методів прогнозування фінансово-економічної безпеки підприємства. *Матеріали XIV міжнародної науково-практичної конференції «Сучасні проблеми моделювання соціально-економічних систем»*. 6-7 Квітня 2023. Братислава Харків, ВШЕМ – ХНЕУ ім. С. Кузнеця, 2023. URL: <https://mpsesm.hneu.edu.ua/index.php/mpsesm/mpsesm-xiv/paper/view/1074>

111. Біличенко М. М. Концептуальна модель оцінки економічної безпеки підприємства в умовах цифрової трансформації. *Здобутки економіки: перспективи та інновації*, 2025, 18. DOI: <https://doi.org/10.5281/zenodo.15540326>

112. Біличенко М. М. Особливості оцінки економічної безпеки підприємства в умовах цифрової трансформації. *Міжнародної науково-практичної конференції «Розвиток економіки та бізнес-адміністрування: наукові течії та рішення»* 16 листопада 2023 року. К.: НАУ, 2023. С. 41-42.

113. Біличенко М. М. Оцінка фінансової безпеки підприємства методами машинного навчання. *Цифрова економіка та економічна безпека*, 2024, 4 (13), 101-107. DOI: <https://doi.org/10.32782/dees.13-15>

114. Біличенко М. М., Касьянова Н. В. Вплив цифрової трансформації на формування системи економічної безпеки підприємства. *Бізнес Інформ*, 2023, 7, 83–91. DOI: <https://doi.org/10.32983/2222-4459-2023-7-83-91>

115. Біличенко М. М., Касьянова Н. В. Економічна безпека підприємства в умовах цифрової економіки. *Матеріали XII міжнародної науково-практичної конференції «Сучасні проблеми економіки та бізнесу»*. К.: НАУ, 2022. С. 85-88.

116. Біличенко М.М. Прогнозування банкрутства підприємства методами інтелектуального аналізу даних. *Матеріали V Міжнародної науково-практичної конференції «Розвиток економіки та бізнес-адміністрування: наукові течії та рішення»*. 11 листопада 2024 р. - К., ДУ «КАІ», 2024. С. 24-27
117. Біличенко М.М., Смерічевський С.Ф. Застосування штучного інтелекту для аналізу фінансової безпеки підприємства. *Підприємництво та інновації*. 2026, 39, 69-75. DOI: <https://doi.org/10.32782/2415-3583/39.10>
118. Бровкіна Ю. О. Підходи до вивчення поняття економічної безпеки підприємства. *Економіка: реалії часу*, 2015,1(17), 122–128. URL: <https://economics.net.ua/files/archive/2015/No1/122-128.pdf>
119. Варналій З. С., Буркальцева Д. Д., Саєнко С. О. Економічна безпека України: проблеми та пріоритети зміцнення: Монографія. К.: Знання України, 2011. 299 с.
120. Васильєв О. В., Мейта В. І. Формування системи управління економічною безпекою промислових підприємств. *Економічний аналіз*, 2013, 14 (2), 138-145. URL: <https://www.econa.org.ua/index.php/econa/article/view/193/93>
121. Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення: монографія. Львів: Арал, 2012. 386 с.
122. Вахлакова В. В. Оцінювання фінансової та ринкової складових економічної безпеки підприємства. *Бізнес Інформ*, 2017, 8, 212-218. URL: [https://www.business-inform.net/export\\_pdf/business-inform-2017-8\\_0-pages-212\\_218.pdf](https://www.business-inform.net/export_pdf/business-inform-2017-8_0-pages-212_218.pdf)
123. Верхоглядова Н. І., Герасимова О. Л., Щеглова О. Ю., Левчинський Д. Л. Економічна діагностика. Дніпропетровськ : Свідлер, 2011. 332 с
124. Використання інформаційно-комунікаційних технологій на підприємствах. *Держстат*. URL: [https://stat.gov.ua/uk/explorer?urn=SSSU%3ADF\\_INFORM\\_COMMUN\\_TECH\\_ENTRP%287.0.0%29&filter=NMBR\\_ENTRP\\_INTERNET\\_SH.%2A.%2A.%2A.%2A.%2A.%2A](https://stat.gov.ua/uk/explorer?urn=SSSU%3ADF_INFORM_COMMUN_TECH_ENTRP%287.0.0%29&filter=NMBR_ENTRP_INTERNET_SH.%2A.%2A.%2A.%2A.%2A.%2A)

125. Вовк О. Оцінювання ефективності системи економічної безпеки підприємствах на авіамашинобудування. *Підприємництво та інновації*, 2018, 5, 119-125. URL: <http://ei-journal.in.ua/index.php/journal/article/view/77>
126. Волощук Р. В. Порівняльний аналіз підходів до визначення вагових коефіцієнтів інтегральних індексів стану складних систем. *Індуктивне моделювання складних систем*, 2013, 5, 151-165. URL: [http://nbuv.gov.ua/UJRN/Imss\\_2013\\_5\\_29](http://nbuv.gov.ua/UJRN/Imss_2013_5_29)
127. Воржакова Ю.П., Хлебінська О.І. Сутність цифрової трансформації з різних позицій підприємців та науковців. *Економіка та держава*, 2021, 9, 107–111. DOI: <https://doi.org/10.32702/2306-6806.2021.9.107>
128. Гавловська Н., Матюх С., Любохинець Л. Оцінювання стану економічної безпеки промислового підприємства. *Development Service Industry Management*, 2023, (1), 6–12. DOI: [https://doi.org/10.31891/dsim-2023-1\(1\)](https://doi.org/10.31891/dsim-2023-1(1))
129. Герасименко Ю.С. Економічна безпека діяльності підприємства: навчально-методичний посібник. Біла Церква: БІНПО ДЗВО «УМО» НАПН України, 2024. 212 с
130. Демиденко М.А. Системи підтримки прийняття рішень : навч. посіб. Нац. гірн. ун-т., 2016. 104 с.
131. Донець Л. І., Ващенко Н. В. Економічна безпека підприємства: навч. пос. К.: Центр учбової літератури, 2008. 240 с.
132. Дуб Б. С. Система економічної безпеки підприємства: поняття та структура. *Управління проектами та розвиток виробництва*, 2016, 4, 5-18. URL: [https://mpira.ub.uni-muenchen.de/88311/1/MPRA\\_paper\\_88311.pdf](https://mpira.ub.uni-muenchen.de/88311/1/MPRA_paper_88311.pdf)
133. Дубецька С. П. Економічна безпека підприємства України *Недержавна система безпеки підприємства як суб'єкт національної безпеки України: зб. мат. наук.-практ. конф.* К.: Видавництво Європейського університету фінансів, інформаційних систем, менеджменту і бізнесу, 2002. С. 146-172.
134. Економіка підприємства: підручник / За заг. ред. С.Ф. Покропивного. Вид. 2-ге., перероб. та доп. К.: КНЕУ. 2000. 528 с.

135. Економічна безпека підприємства : навч. посіб. / Г. В. Блакита, Г. В. Ситник, Т. Л. Зубко та ін. Київ : Київ. нац. торг.-екон. ун-т, 2021. 304 с. DOI: 10.31617/np.knute.2021-113

136. Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення. К. : КНТЕУ, 2001. 309 с

137. Жаворонкова Г., Жмуденко В. Методичні підходи до визначення інтегрального показника економічної безпеки аграрної сфери на регіональному рівні. *Економічний аналіз*, 2010, 7, 42-44. URL: <https://lib.udau.edu.ua/server/api/core/bitstreams/4774c936-cec0-4ecb-8b3d-ffe1394a01cc/content>

138. Журавель М.Ю., Полозова Т.В., Стороженко О.В. Ключові задачі економічної безпеки підприємства. *Вісник Харківського національного аграрного університету ім. В. В. Докучаєва. Сер.: Економічні науки*, 2014, 7, 105-112.

139. Зуб П., Калач Г. Цифровізація бізнес-процесів промислових підприємств. *Економіка та суспільство*, 2021, 26. DOI: <https://doi.org/10.32782/2524-0072/2021-26-52>

140. Іванчук Я.В., Месюра В.І., Яровий А.А., Манжілевський О.Д. Інтелектуальний аналіз даних та машинне навчання. Частина 1. Базові методи та засоби аналізу даних. Вінниця : ВНТУ, 2021. 69 с.

141. Іванюта Т.М., Заїчковський А.О. Економічна безпека підприємства. К.: Центр учбової літератури. 2009. 256 с.

142. Ілляшенко С.М. Складові економічної безпеки підприємства і підходи до їх оцінки. *Актуальні проблеми економіки*, 2003, 3(21), 12-19.

143. Карпунь І.Н. Управління фінансовою санацією підприємства: навч. посіб. Львів: Магнолія-2006, 2009. 418 с

144. Касьянова Н. В., Біличенко М. М., Севериненко А. О. Моделювання цифрової безпеки підприємства. *Modern Economics*, 2023, 39, 54-61. DOI: [https://doi.org/10.31521/modecon.V39\(2023\)-08](https://doi.org/10.31521/modecon.V39(2023)-08).

145. Касьянова Н. В., Кравчук Н. М., Коваль Ю. Л. Безпека підприємства в умовах цифрової трансформації економіки. *Modern Economics*, 2020, 20, 124–129. DOI: [https://doi.org/10.31521/modecon.V20\(2020\)-20](https://doi.org/10.31521/modecon.V20(2020)-20)
146. Ковальов Д., Плєтнікова І. Кількісна оцінка рівня економічної безпеки підприємства. *Економіка України*, 2001, 4, 35–40
147. Козаченко Г. В. Економічна безпека підприємства: сутність та механізм забезпечення : монографія. К.: Лібра, 2003. 280 с.
148. Козаченко Г. В., Погорєлов Ю. С. Оцінювання економічної безпеки підприємства: аналіз основних підходів. Менеджмент безпеки держави, регіону, підприємства: проблеми і виклики сьогодення: колективна монографія / за заг. ред. З.Б. Живко, І.Г. Бабець. Львів : Ліга-Прес, 2015. С. 238–251
149. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення: Монографія. К.: Лібра, 2003. 280 с
150. Коцюбівська К. І. Визначення вагових коефіцієнтів інтегральних індексів економічної безпеки. *Статистичне та експертно-аналітичне забезпечення управління сталим розвитком економіки і соціальної сфери : зб. матеріалів III Міжнарод. наук.-практ. конф. (м. Чернігів, 5 грудня 2017 р.)*. Чернігів : ЧНТУ, 2017. С. 92-95.
151. Кочетков О. В., Гаур Т. О., Машін В. М. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. *Наукові праці ОНАЗ ім. О.С. Попова*. 2019, 1, 97-104. URL: [http://nbuv.gov.ua/UJRN/Nponaz\\_2019\\_1\\_14](http://nbuv.gov.ua/UJRN/Nponaz_2019_1_14)
152. Кравчук А. Ю., Кліменко Т. Л. Система управління методичним забезпеченням економічної безпеки на підприємстві. *Ефективна економіка*, 2010, 9. URL: <http://www.economy.nayka.com.ua/?op=1&z=331>
153. Крисоватий А.І., Десятнюк О.М., Птащенко О.В. Цифрова економіка: підручник. Тернопіль : ЗУНУ, 2024. 520 с.
154. Кузенко Т. Б. Планування економічної безпеки підприємств в умовах ринкової економіки : автореф. дис. на здобуття наук. ступеня канд. екон.

наук: спец. 08.06.01. Європейський ун-т фінансів, інформаційних систем, менеджменту і бізнесу. К., 2004. 18 с.

155. Кучмей О. В. Моделювання ймовірності банкрутства підприємства (на прикладі ПАТ «Будівельна корпорація «Укрбуд») *Ефективна економіка*, 2017, 11. URL: <http://www.economy.nayka.com.ua/?op=1&z=6037>

156. Мазаракі А., Федулова І., Дроздова Ю., Бай С. Нечітко-множинний підхід до оцінки ризику в умовах цифровізації управлінської діяльності підприємства. *Проблеми фінансово-кредитної діяльності теорії та практики*, 2021, 5 (40), 263–275. DOI: <https://doi.org/10.18371/fcaptp.v5i40.245099>

157. Маслак О. І., Коробкова І. В. Інформаційне забезпечення процесу управління стратегічною стійкістю підприємства. *Інвестиції: практика та досвід*, 2015, 4, 23–25. URL: [http://www.investplan.com.ua/pdf/4\\_2015/6.pdf](http://www.investplan.com.ua/pdf/4_2015/6.pdf)

158. Матвійчук Л. О. Теоретичні підходи до визначення сутності поняття «економічна безпека підприємства» *Науковий вісник Волинського національного університету ім. Лесі України*, 2012, 5 (230), 50-54.

159. Мацеха Д. С. Функціональні складові економічної безпеки та показники їхньої оцінки для підприємств легкої промисловості. *Вісник соціально-економічних досліджень*, 2013, 1, 128-133. URL: <https://elar.khmnu.edu.ua/server/api/core/bitstreams/178a6017-a3c4-45f2-a544-40be77a283b3/content>

160. Мельниченко О. В. оцінка фінансової безпеки підприємств на засадах поведінкової економіки. *Вісник ЧНУ ім. Б. Хмельницького. Серія «Економічні науки»*, 2020, 3, 44-59. DOI: <https://doi.org/10.31651/2076-5843-2020-3-44-59> .

161. Менеджмент безпеки держави, регіону, підприємства: проблеми і виклики сьогодення: монографія / В.Г. Алькема, І.Г. Бабець, З.Б. Живко, Г.В. Козаченко, М.І. Копитко; За заг. ред. З.Б. Живко, І.Г. Бабець. Львів : Ліга-Прес, 2015. 345 с.

162. Мішин О. Ю., Мішина С. В. Сутність поняття «економічна безпека підприємства». *Вісник економіки транспорту і промисловості*, 2012, 38, 86–92. URL: <https://surl.luh.gov.ua/ytcusw>

163. Назарова Г. В., Лобазов С. М. Удосконалення методики розрахунку інтегрального індексу кадрової безпеки підприємства. *Економіка: реалії часу*, 2015, 1 (17), 134-139. URL: [http://nbuv.gov.ua/UJRN/econrch\\_2015\\_1\\_24](http://nbuv.gov.ua/UJRN/econrch_2015_1_24)

164. Небава М. І., Міронова Ю. В. Економічна безпека підприємства : навчальний посібник. Вінниця : ВНТУ, 2017. 73 с.

165. Нікітін Ю. О., Кульчицький О. І. Цифрова парадигма як основа визначень: цифровий бізнес, цифрове підприємство, цифрова трансформація. *Маркетинг і цифрові технології*, 2019, 3 (4), 77-87. DOI: 10.15276/mdt.3.4.2019.7

166. Оголошення та повідомлення про банкрутство. Верховний Суд : Офіційний вебпортал судової влади України. URL: [https://supreme.court.gov.ua/supreme/pro\\_sud/og\\_pov/](https://supreme.court.gov.ua/supreme/pro_sud/og_pov/)

167. Останкова Л. А., Шевченко Н. Ю. Моделювання показників економічної безпеки підприємства на основі нечіткої логіки. *Економіка промисловості*, 2010, 2, 106-110. URL: <http://jnas.nbuv.gov.ua/article/UJRN-0000070439>

168. Отенко І. П., Іващенко Г. А., Воронков Д. К. Економічна безпека підприємства: навчальний посібник. Х. : Вид. ХНЕУ, 2012. 256 с.

169. Отенко І. П., Яртим І. А. Оцінювання економічної безпеки в процесах розвитку підприємства. *Бізнес Інформ*, 2013, 11, 255–261. URL: [https://www.business-inform.net/export\\_pdf/business-inform-2013-11\\_0-pages-255\\_261.pdf](https://www.business-inform.net/export_pdf/business-inform-2013-11_0-pages-255_261.pdf)

170. П'янкова О., Рула О. Вплив цифрових трансформацій на ефективність антикризового управління в міжнародних компаніях. *Економіка та суспільство*, 2025, 72. DOI: <https://doi.org/10.32782/2524-0072/2025-72-155>

171. Павліщенко С. С., Капустян В.О. Економіко-математичне моделювання економічної безпеки малого підприємства в умовах

невизначеності. *Актуальні проблеми економіки та управління : збірник наукових праць молодих вчених*, 2020, 14. URL: <https://ela.kpi.ua/server/api/core/bitstreams/bcad516e-d4ad-4587-bc42-38bd027df80f/content>

172. Пархоменко Н. О. Особливості управління економічною безпекою будівельного підприємства. *Ефективна економіка*, 2020, 5. DOI: <https://doi.org/10.32702/2307-2105-2020.5.61>

173. Петрович Й. М., Кіт А. Ф., Семенів О. М. та ін. Економіка підприємства: Підручник. Львів, «Новий Світ 2000», 2004. 680 с.

174. Пілецька С. Т., Арєф'єв С. О., Петровська С. В., Колесников С. О. Стратегічне забезпечення економічної безпеки підприємств в контексті цифровізації економіки України. *Проблеми економіки*, 2024, 2 (60), 181–190. DOI: <https://doi.org/10.32983/2222-0712-2024-2-181-190>

175. Пілецька С. Т., Коритько Т. Ю., Ткаченко Є. В. Модель інтегральної оцінки економічної безпеки підприємства. *Економічний вісник Донбасу*, 2021, 3, 56-65. URL: [http://nbuv.gov.ua/UJRN/ecvd\\_2021\\_3\\_6](http://nbuv.gov.ua/UJRN/ecvd_2021_3_6)

176. Побережна З. М. Адаптивне управління на основі інформаційно-комунікаційних технологій в бізнес-процесах при формуванні економічної безпеки підприємства до неотехнологічних умов. *Економічний аналіз*, 2024, 34 (4), 484-491. DOI: <https://doi.org/10.35774/econa2024.04.484>

177. Покропивний С. Ф. Економіка підприємства. К. : КНЕУ. 2000. 528 с.

178. Потужна М. Цифрова трансформація: визначення, ключові аспекти, технології та етапи реалізації. *Netwave*, 2024 URL: <https://netwave.ua/blog/tsifrova-transformatsiya-viznachennya-klyuchovi-aspekti-tehnologi-ta-etapi/>

179. Приходько В. П. Управління економічною безпекою підприємства. *Економіка та держава*, 2013, 10, 10-12. URL: [http://nbuv.gov.ua/UJRN/ecde\\_2013\\_10\\_4](http://nbuv.gov.ua/UJRN/ecde_2013_10_4)

180. Реверчук Н.Й. Управління економічною безпекою підприємницьких структур: монографія. Львів: ЛБІ НБУ, 2004. 195 с.

181. Роженко О.В. Стратегії економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*, 2015, 51, 51-55. URL: [http://nbuv.gov.ua/UJRN/Vetp\\_2015\\_51\\_11](http://nbuv.gov.ua/UJRN/Vetp_2015_51_11)
182. Руська Р. В. Економетрика: навчальний посібник. Тернопіль : Тайп, 2012. 224с
183. Сак Т. В. Стратегічні підходи в управлінні економічною безпекою підприємства. *Збірник наукових праць Хмельницького кооперативного торговельно-економічного інституту*, 2013, 5, 276–285. URL: <https://evnuir.vnu.edu.ua/bitstream/123456789/4779/3/Sak.pdf>
184. Салоїд С. В. Механізм управління економічною безпекою підприємства: теоретичний аспект. *Економічний вісник НТУУ «КПІ»*, 2017, 14, 250-254. DOI: 10.20535/2307-5651.14.2017.108778
185. Сисоліна Н. П. Економічна безпека підприємства: навч. посіб. Кіровоград: КНТУ, 2014. 226 с. URL: <https://dspace.kntu.kr.ua/server/api/core/bitstreams/5be8e910-6806-43a5-9428-17e72c8a6f0e/content>
186. Системи підтримки прийняття рішень: навчальний посібник для самостійного вивчення дисципліни / уклад.: С. М. Братушка, С. М. Новак, С.О. Хайлук; Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми : ДВНЗ “УАБС НБУ”, 2010. 265 с.
187. Ситник В.Ф. Системи підтримки прийняття рішень. К.: КНЕУ, 2004. 614 с.
188. Сімкова Т., Копча Ю. Стратегічні імперативи забезпечення економічної безпеки підприємства в умовах інноваційного розвитку під впливом невизначеності і ризиків. *Економічний аналіз*, 2025, 35 (1), 167-177. DOI: <https://doi.org/10.35774/econa2025.01.167>
189. Смерічевський С.Ф. Стратегічні аспекти адаптивного управління економічною безпекою підприємств. *Український журнал прикладної*

економіки та техніки, 2023, 2, 37-44. DOI: <https://doi.org/10.36887/2415-8453-2023-2-5>

190. Смірнова Т., Константинова Л., Коноплицька-Слободенюк О., Козлов Я., Кравчук О., Козірова Н., Смірнов О. Дослідження сучасного стану сіем-систем. *Кібербезпека: освіта, наука, техніка*, 2024, 1(25), 6–18. DOI: <https://doi.org/10.28925/2663-4023.2024.25.618>

191. Смоляр Л.Г., Чоні І.В. Цифрова трансформація як складова підвищення конкурентоспроможності. *II Міжнародна науково-практична конференція «Бізнес, інновації, менеджмент: проблеми та перспективи»*. 2021. Київ: КПІ ім. І. Сікорсько-го. С. 238–239. URL: <https://confmanagement-proc.kpi.ua/article/view/23181>

192. Смоляр Л.Г., Чоні І.В. Цифрова трансформація як складова підвищення конкурентоспроможності. *II Міжнародна науково-практична конференція «Бізнес, інновації, менеджмент: проблеми та перспективи»*. 2021. Київ: КПІ ім. І. Сікорського. С. 238–239.

193. Сосновська О.О. Система економічної безпеки підприємств зв'язку: монографія. К.: «Центр учбової літератури», 2019. 440 с.

194. Тигач Г. Г. Забезпечення економічної безпеки підприємства в умовах цифрової трансформації. *Ефективна економіка*, 2025, 5. DOI: <http://doi.org/10.32702/2307-2105.2025.5.118>

195. Хамініч С. Управління конкурентоспроможністю підприємства на засадах впровадження цифрових рішень. *Цифрова економіка та економічна безпека*, 2025, 3 (18), 196-202. DOI: <https://doi.org/10.32782/dees.18-30>

196. Хамініч С.Ю. Економічна безпека підприємства у контексті розвитку цифрової інфраструктури. *Вісник ДНДІСЕ Міністерства юстиції України. Економічні науки*, 2025, 2 (12), 41-50. DOI: <https://doi.org/10.32782/2708-1834/2025-12.5>

197. Хвальчик І. Л., Волощук Л. О. Сутність інформаційно-аналітичного забезпечення управління підприємством. *Economics: time realities*, 2020, 1(47), 84–90. DOI: 10.15276/ETR.01.2020.10

198. Хоменко О. І. Види стратегій та інструментарій формування стратегії розвитку підприємства. *Управління розвитком*, 2015, 14(3), 131-137. URL: <https://devma.com.ua/uk/journals/t-13-3-2015>
199. Худолій Л. М. Складові економічної безпеки суб'єктів господарської діяльності. *Ефективна економіка*, 2011, 1. URL: <http://www.economy.nayka.com.ua/?op=1&z=455>
200. Чернега О. М. Критерії та показники фінансово-економічної безпеки підприємства / Науково-методичні аспекти забезпечення економічної безпеки: монографія. Одеса: Атлант. 2013. С. 56-61.
201. Шемаєва Л. Г. Економічна безпека підприємств у стратегічній взаємодії з суб'єктами зовнішнього середовища: автореф. дис. ... д-ра екон. наук: 21.04.02; Університет економіки та права «Крок». Київ, 2010. 40 с.
202. Шило Ж. Методика комплексної оцінки рівня економічної безпеки підприємства. *International Science Journal of Management, Economics & Finance*, 2022, 1 (4), 17–25. DOI: <https://doi.org/10.46299/j.isjmef.20220104.03>
203. Шира Т. Б. Теоретичні аспекти забезпечення економічної безпеки підприємства. *Науковий вісник Національного лісотехнічного університету України*, 2014, 24 (2), 361–366
204. Шлемко В. Т., Бінько І. Ф. Економічна безпека України: сутність і напрямки забезпечення: Монографія. К. : НІСД, 1997. 144 с
205. Шопіна І. М. Принципи цифрової трансформації України крізь призму досвіду Європейського Союзу. *Південноукраїнський правничий часопис*, 2022, 4 (3), 29–34. DOI: <https://doi.org/10.32850/sulj.2022.4.3.6>
206. Штангрет А. М., Караїм М. М. Управління економічною безпекою підприємства за часовими горизонтами. Наукові записки Української академії друкарства, 2016, 1, 201–206. URL: [http://nbuv.gov.ua/UJRN/Nz\\_2016\\_1\\_26](http://nbuv.gov.ua/UJRN/Nz_2016_1_26)
207. Штангрет А. М., Підгородецький І. М. Генезис та сучасне сприйняття економічної безпеки підприємства. *Актуальні проблеми сталого розвитку*, 2026, 3(1), 14-19. DOI: [https://doi.org/10.60022/3\(1\)-2S](https://doi.org/10.60022/3(1)-2S)

208. Штангрет А. М., Шира Т. Б., Чорненька О. Б. Цифрова трансформація підприємства: об'єктивна необхідність в поточних умовах з позиції забезпечення економічної безпеки. *Східна Європа: економіка, бізнес та управління*, 2024, 1 (42), 97-103. DOI: <https://doi.org/10.32782/easterneurope.42-14>

209. Що таке цифрова трансформація? *SAP*, 2023. URL: <https://www.sap.com/ukraine/resources/what-is-digital-transformation>

210. Юрчак І. Ю., Хіч А., Оксенюк В. Розуміння великих мовних моделей: майбутнє штучного інтелекту. *CDS*, 2024, 6 (2), 51-60. DOI: <https://doi.org/10.23939/cds2024.02.051>

211. Яременко О. Ф. Механізм управління економічною безпекою машинобудівного підприємства : автореф. дис. на здобуття наук. ступеня канд. екон. наук : спец. 08.00.04; Хмельниц.нац. ун-т. Хмельницький, 2009. 20 с.

212. Яременко О. Ф. Середовище підприємства як чинник небезпеки діяльності суб'єкта господарювання. *Вісник ХНУ*, 2006, 5 (2), 144-150.

213. Ярова Ю.О., Артеменко Л.П. Структура економічної безпеки підприємства в умовах кризи. *Економічний вісник Національного технічного університету України «КПІ»*, 2016, 13, 257-263. URL: [http://nbuv.gov.ua/UJRN/evntukpi\\_2016\\_13\\_39](http://nbuv.gov.ua/UJRN/evntukpi_2016_13_39)

## **ДОДАТКИ**

Розшифровки рівнів кожного критерію оцінки техніко-технологічної  
складової системи економічної безпеки

1. Рівень автоматизації виробництва

| Рівень             | Опис                                                                               |
|--------------------|------------------------------------------------------------------------------------|
| Дуже низький (0.1) | Автоматизація практично відсутня (<10% операцій)                                   |
| Низький (0.3)      | Часткова автоматизація (10–30%)                                                    |
| Середній (0.5)     | Автоматизовано до половини ключових процесів (31–60%)                              |
| Високий (0.7)      | Основні процеси автоматизовані (61–80%)                                            |
| Дуже високий (0.9) | Повна або майже повна автоматизація (>80%), інтегровані цифрові системи управління |

2. Захищеність IT-інфраструктури

| Рівень            | Опис                                                             |
|-------------------|------------------------------------------------------------------|
| Дуже низька (0.1) | Відсутність захисту, відсутні політики, не зафіксовані інциденти |
| Низька (0.3)      | Базовий рівень (антивіруси, мінімальний контроль доступу)        |
| Середня (0.5)     | Є firewall, періодичне оновлення, мінімальні інциденти           |
| Висока (0.7)      | Системи SIEM, регулярні аудитори, політика доступу, ISO 27001    |
| Дуже висока (0.9) | IEC 62443, Zero Trust, постійний моніторинг, Pen Testing         |

3. Частка цифрових технологій у технологічних процесах

| Рівень          | Опис                                                          |
|-----------------|---------------------------------------------------------------|
| Менше 10% (0.1) | Використання майже відсутнє                                   |
| 10–30% (0.3)    | Використовуються окремі цифрові елементи                      |
| 31–60% (0.5)    | Часткова цифровізація ключових етапів                         |
| 61–80% (0.7)    | Переважає частина виробництва використовує цифрові технології |
| Понад 80% (0.9) | Майже повна цифровізація, синхронізація з ERP, MES, IoT тощо  |

4. Стан технічного обладнання та інноваційна готовність

| Рівень                   | Опис                                                                          |
|--------------------------|-------------------------------------------------------------------------------|
| Застаріле (0.1)          | Обладнання старше 15 років, не підтримує підключення до цифрових мереж        |
| Частково застаріле (0.3) | Частина обладнання оновлена, але загалом технічно відстале                    |
| Задовільне (0.5)         | Середній стан, частково придатне до модернізації                              |
| Сучасне (0.7)            | Нове обладнання, підтримує цифровий моніторинг, часткова інтеграція           |
| Інноваційне (0.9)        | Високотехнологічне, сумісне з Industry 4.0, інтеграція з хмарними платформами |

## 5. Цифрова компетентність персоналу

| Рівень            | Опис                                                                              |
|-------------------|-----------------------------------------------------------------------------------|
| Дуже низька (0.1) | Працівники не мають цифрових навичок, відсутнє навчання                           |
| Низька (0.3)      | Лише обмежене коло персоналу проходило навчання                                   |
| Середня (0.5)     | Близько половини персоналу мають базові цифрові навички                           |
| Висока (0.7)      | Більшість персоналу підготовлена, діють цифрові ініціативи                        |
| Дуже висока (0.9) | Системна цифрова культура, регулярне навчання, лідерство у цифровій трансформації |

## Відповідність фінансових показників та коду фінансової звітності

| Назва фінансового показника   | Назва показника у звітності                                      | Код фінансової звітності |
|-------------------------------|------------------------------------------------------------------|--------------------------|
| <i>cash</i>                   | Гроші та їх еквіваленти                                          | 1165                     |
| <i>constant capital</i>       | Загальні Необоротні активи                                       | 1095                     |
| <i>costs</i>                  | Собівартість реалізованої продукції (товарів, робіт, послуг)     | 2050                     |
| <i>current assets</i>         | Загальні Оборотні активи                                         | 1195                     |
| <i>equity</i>                 | Загальний Власний капітал                                        | 1495                     |
| <i>fixed assets</i>           | Основні засоби                                                   | 1010                     |
| <i>gross profit</i>           | Валовий прибуток                                                 | 2090                     |
| <i>inventory</i>              | Запаси                                                           | 1100                     |
| <i>long-term liabilities</i>  | Загальні Довгострокові зобов'язання і забезпечення               | 1595                     |
| <i>net profit</i>             | Чистий фінансовий результат:                                     | 2350 / 2355              |
| <i>receivables</i>            | Дебіторська заборгованість за продукцію, товари, роботи, послуги | 1125                     |
| <i>retained earnings</i>      | Нерозподілений прибуток (непокритий збиток)                      | 1420                     |
| <i>sales</i>                  | Чистий дохід від реалізації продукції (товарів, робіт, послуг)   | 2000                     |
| <i>share capital</i>          | Зареєстрований (пайовий) капітал                                 | 1400                     |
| <i>short-term liabilities</i> | Загальні Поточні зобов'язання і забезпечення                     | 1695                     |
| <i>total assets</i>           | Загальні активи                                                  | 1300                     |
| <i>total liabilities</i>      | Загальні пасиви                                                  | 1900                     |

## Рекомендації щодо управління економічною безпекою при відповідному рівні ризику

| Рівень ризику | Фінансова безпека                                                                                                                                                                                                                                                                                                                                                                                                        | Кадрова безпека                                                                                                                                                                                                                                                                                                                                                                                       | Техніко-технологічна безпека                                                                                                                                                                                                                                                                                                                                 |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Низький       | <ul style="list-style-type: none"> <li>• Проведення планових фінансових аудитів.</li> <li>• Оновлення фінансових прогнозів із використанням наявних даних.</li> <li>• Перевірка актуальності фінансових резервів.</li> <li>• Підтримання чинної системи управління ліквідністю.</li> </ul>                                                                                                                               | <ul style="list-style-type: none"> <li>• Проведення онлайн-курсів з основ кібергігієни для всіх нових працівників.</li> <li>• Оцінка задоволеності працівників.</li> <li>• Ротація персоналу з доступом до конфіденційних цифрових даних.</li> <li>• Регулярний перегляд політик цифрової поведінки.</li> </ul>                                                                                       | <ul style="list-style-type: none"> <li>• Регулярне оновлення програмного забезпечення.</li> <li>• Використання VPN для технічного персоналу при віддаленому доступі.</li> <li>• Планова діагностика обладнання.</li> </ul>                                                                                                                                   |
| Середній      | <ul style="list-style-type: none"> <li>• Аналіз структури витрат і скорочення неперіоритетних видатків;</li> <li>• Впровадження програм фінансового планування й бюджетного контролю;</li> <li>• Прискорення цифрової трансформації підприємства</li> <li>• Диверсифікація джерел доходу за рахунок діджиталізації каналів збуту;</li> <li>• Тимчасове призупинення проєктів з високим рівнем невизначеності.</li> </ul> | <ul style="list-style-type: none"> <li>• Впровадження системи контролю доступу до інформаційних ресурсів;</li> <li>• Розгорнення програми навчання працівників з питань цифрової гігієни;</li> <li>• Аудит дій працівника з аномальною поведінкою;</li> <li>• Встановлення системи багатофакторної аутентифікації;</li> <li>• Посилення моніторингу вразливих сегментів IT-інфраструктури.</li> </ul> | <ul style="list-style-type: none"> <li>• Проведення аудитів IT-інфраструктури на предмет вразливостей.</li> <li>• Впровадження SIEM-систем для моніторингу IT-інцидентів у реальному часі.</li> <li>• Оновлення або часткова модернізація застарілого обладнання.</li> <li>• Резервування критичних даних та впровадження протоколів відновлення.</li> </ul> |

|         |                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Високий | <ul style="list-style-type: none"> <li>• Ініціювання процедури фінансового оздоровлення;</li> <li>• Розробка політики цифрової трансформації з найменшим витратами;</li> <li>• Призначення антикризового менеджера або консультанта.</li> <li>• Впровадження політики короткострокової ліквідності;</li> </ul> | <ul style="list-style-type: none"> <li>• Тимчасове блокування доступу працівників із високим рівнем аномалій;</li> <li>• Ініціювання службового розслідування щодо потенційного витоку інформації;</li> <li>• Перегляд кадрового резерву, зниження концентрації доступів до критичних систем;</li> <li>• Запровадження внутрішнього індикатора довіри для персоналу.</li> </ul> | <ul style="list-style-type: none"> <li>• Повна ревізія технічного парку з пріоритетною заміною критично зношених елементів.</li> <li>• Аутсорсинг або залучення зовнішніх експертів для швидкого посилення технологічної безпеки.</li> <li>• Обов'язкове навчання та сертифікація технічного персоналу.</li> </ul> |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Джерело: складено автором

## Програмний код розробленої інформаційної системи

```
## import
import streamlit as st
import joblib

import pandas as pd
import numpy as np

import pickle as pkl
from sklearn.impute import SimpleImputer
from sklearn.pipeline import Pipeline
from sklearn.preprocessing import StandardScaler
from sklearn.compose import ColumnTransformer
import xgboost as xgb

#finance prediction
from moduls.finance.processing import calculate_fin_indicators, get_all_fin_indicators,
create_variables, prepare_dataset
from moduls.finance.prediction import data_cleaning, predict_banruptcy
#staff prediction
from moduls.staff.processing import prepare_dataset_staff
from moduls.staff.prediction import prediction_staff, plot_user_stat

#finance prediction
PATH_FINANCE = 'data/finance'
FINANCE_RAW_FILE = PATH_FINANCE + '/raw/company_fin_data.csv'
FINANCE_DICT = PATH_FINANCE + '/variables_dict.csv'
#staff prediction
PATH_STAFF_DATA = 'data/staff'
#tech prediction
W_TECH_1 = 0.3
W_TECH_2 = 0.2
W_TECH_3 = 0.2
W_TECH_4 = 0.15
W_TECH_5 = 0.15
```

```

#Integral index
W_T_1 = 0.4
W_T_2 = 0.3
W_T_3 = 0.3
RECOMMENDATIONS_FILE = 'data/recommendations/by_systems.csv'

#Load models and transformers
with open('models/finance/transformers/train_v5_fit_transformer.pkl','rb') as f:
    transformer_sc = pickle.load(f)
with open('models/finance/models/best_model_xgb.pkl','rb') as f:
    finance_model_xgb = pickle.load(f)
with open('models/staff/models/model_isoforest.pkl','rb') as f:
    model_iso = pickle.load(f)

# Title the app
st.title('Система економічної безпеки підприємства')
##st.markdown("***** Використовуйте меню зліва щоб задавати параметри *****")

st.sidebar.markdown("## Виберіть рівень цифровізації підприємства")
# For finance
VAR_ONLINE_PRESENCE = st.sidebar.selectbox("Оберіть рівень онлайн присутності",
["Відсутні сайт і будь-яка присутність",
"Немає власного сайту але є певна інформація в Інтернеті",
"Є власний сайт з обмеженою функціональністю",
"Є повноціннофункціонуючий сайт з повною інформацією про
продукти"])
VAR_SOCIAL_MEDIA = st.sidebar.selectbox("Оберіть рівень присутності в соціальних
мережах",
["Немає присутності на платформах соціальних мереж.",
"Є аккаунти в соціальних мережах але відсутня або дуже мала
активність",
"Є аккаунти і велика активність"])
VAR_ECOMMERCE = st.sidebar.selectbox("Оберіть рівень розвитку електронної комерції",
["Відсутність можливості онлайн-покупок або транзакцій",
"Базові можливості для онлайн-покупок",
"Розширені можливості електронної комерції"])

```

```

# For Kadrova system
st.sidebar.markdown('## Виберіть потрібний період')
VAR_YEAR = st.sidebar.selectbox("Оберіть місяць для прогнозування кадрової безпеки",
                                ['2023', '2024'])
VAR_MONTH = st.sidebar.selectbox("Оберіть місяць для прогнозування кадрової безпеки",
                                range(1,13,1))

# For Tech system
st.sidebar.markdown("## Виберіть рівень цифрового технологічного розвитку підприємства")
VAR_TECH_1 = st.sidebar.selectbox("Оберіть рівень автоматизації виробництва",
    ["Автоматизація практично відсутня (<10% операцій)",
    "Часткова автоматизація (10–30%)",
    "Автоматизовано до половини ключових процесів (31–60%)",
    "Основні процеси автоматизовані (61–80%)",
    "Повна або майже повна автоматизація (>80%), інтегровані цифрові системи управління"])
VAR_TECH_2 = st.sidebar.selectbox("Оберіть рівень захищеності IT-інфраструктури",
    ["Відсутність захисту, відсутні політики, не зафіксовані інциденти",
    "Базовий рівень (антивіруси, мінімальний контроль доступу)",
    "Є firewall, періодичне оновлення, мінімальні інциденти",
    "Системи SIEM, регулярні аудитори, політика доступу, ISO 27001",
    "IEC 62443, Zero Trust, постійний моніторинг, Pen Testing"])
VAR_TECH_3 = st.sidebar.selectbox("Оберіть частку цифрових технологій у технологічних процесах",
    ["Використання майже відсутнє",
    "Використовуються окремі цифрові елементи",
    "Часткова цифровізація ключових етапів",
    "Переважає частина виробництва використовує цифрові технології",
    "Майже повна цифровізація, синхронізація з ERP, MES, IoT тощо"])
VAR_TECH_4 = st.sidebar.selectbox("Оберіть стан технічного обладнання та інноваційну готовність",
    ["Обладнання старше 15 років, не підтримує підключення до цифрових мереж",
    "Частина обладнання оновлена, але загалом технічно відстале",
    "Середній стан, частково придатне до модернізації",
    "Нове обладнання, підтримує цифровий моніторинг, часткова інтеграція",
    "Високотехнологічне, сумісне з Industry 4.0, інтеграція з хмарними платформами"])
VAR_TECH_5 = st.sidebar.selectbox("Оберіть рівень цифрової компетентності персоналу",
    ["Працівники не мають цифрових навичок, відсутнє навчання",
    "Лише обмежене коло персоналу проходило навчання",

```

"Близько половини персоналу мають базові цифрові навички",  
"Більшість персоналу підготовлена, діють цифрові ініціативи",  
"Системна цифрова культура, регулярне навчання, лідерство у цифровій трансформації"])

```
#####  
#####      FINANCE PART      #####  
#####
```

```
## Prepare finance data for prediction
```

```
df_finance_raw = pd.read_csv(f'{FINANCE_RAW_FILE}', converters = {'edrpou': str})
```

```
df_fin_data = get_all_fin_indicators(df_finance_raw,  
                                     column_value_current_year = 'min',  
                                     column_value_end_of_year = 'min')
```

```
df_temp_with_x = create_variables(df_fin_data)
```

```
dataset_fin = prepare_dataset(df_temp_with_x)
```

```
## Add digitalization data
```

```
def map_online_presence(value):
```

```
    if value == "Відсутні сайт і будь-яка присутність":
```

```
        return 0
```

```
    elif value == "Немає власного сайту але є певна інформація в Інтернеті":
```

```
        return 1
```

```
    elif value == "Є власний сайт з обмеженою функціональністю":
```

```
        return 2
```

```
    elif value == "Є повноціннофункціонуючий сайт з повною інформацією про продукти":
```

```
        return 3
```

```
def map_social_media(value):
```

```
    if value == "Немає присутності на платформах соціальних мереж.":
```

```
        return 0
```

```
    elif value == "Є аккаунти в соціальних мережах але відсутня або дуже мала активність":
```

```
        return 1
```

```
    elif value == "Є аккаунти і велика активність":
```

```
        return 2
```

```
def map_ecommerce(value):
```

```

if value == "Відсутність можливості онлайн-покупок або транзакцій":
    return 0
elif value == "Базові можливості для онлайн-покупок":
    return 1
elif value == "Розширені можливості електронної комерції":
    return 2

dataset_fin['dg_1_online_presence'] = map_online_presence(VAR_ONLINE_PRESENCE)
dataset_fin['dg_2_social_media'] = map_social_media(VAR_SOCIAL_MEDIA)
dataset_fin['dg_3_ecommerce'] = map_ecommerce(VAR_ECOMMERCE)

X = data_cleaning(dataset_fin, transformer_sc)
prediction = predict_banruptcy(finance_model_xgb, X)
finance_prediction = prediction[0]

def map_finance_risk_level(value):
    if value < 0.3:
        return 'low'
    elif value < 0.6:
        return 'medium'
    elif value >= 0.6:
        return 'high'
prediction_finance_level = map_finance_risk_level(finance_prediction)

#####
#####      STAFF PART      #####
#####

# df_logon = pd.read_csv(f'{PATH_STAFF_DATA}/logon_sample.csv')
# df_http = pd.read_csv(f'{PATH_STAFF_DATA}/http_sample.csv')
# df_email = pd.read_csv(f'{PATH_STAFF_DATA}/email_sample.csv')
# df_device = pd.read_csv(f'{PATH_STAFF_DATA}/device_sample.csv')
# df_file = pd.read_csv(f'{PATH_STAFF_DATA}/file_sample.csv')
# df_users = pd.read_csv(f'{PATH_STAFF_DATA}/users_sample.csv')

```

```

# dataset_staff = prepare_dataset_staff(df_users, df_logon, df_http, df_device, df_email, df_file)
# staff_prediction = prediction_staff(dataset_staff, model_iso)

# staff_stat_by_day = staff_prediction.groupby(['day'])['high_risk_ind'].sum().reset_index()
# staff_stat_by_month = staff_prediction.groupby(['month'])['high_risk_ind'].sum().reset_index()

# st.write("Рівень ризику кадрової підсистеми економічної безпеки*: ")
#                                     staff_prediction_selected                                     =
staff_stat_by_month.loc[staff_stat_by_month['month']==VAR_MONTH, 'high_risk_ind'].values[0]

staff_prediction_selected = 1
def map_staff_risk_level(value):
    if value == 0:
        return 'low'
    elif value > 0 & value <= 1 :
        return 'medium'
    elif value > 1:
        return 'high'
prediction_staff_level = map_staff_risk_level(staff_prediction_selected)

#####
#####      TECH PART      #####
#####

def map_tech_1(value):
    if value == "Автоматизація практично відсутня (<10% операцій)":
        return 0.1
    elif value == "Часткова автоматизація (10–30%)":
        return 0.3
    elif value == "Автоматизовано до половини ключових процесів (31–60%)":
        return 0.5
    elif value == "Основні процеси автоматизовані (61–80%)":
        return 0.7
    elif value == "Повна або майже повна автоматизація (>80%), інтегровані цифрові системи управління":
        return 0.9

```

```

def map_tech_2(value):
    if value == "Відсутність захисту, відсутні політики, не зафіксовані інциденти":
        return 0.1
    elif value == "Базовий рівень (антивіруси, мінімальний контроль доступу)":
        return 0.3
    elif value == "Є firewall, періодичне оновлення, мінімальні інциденти":
        return 0.5
    elif value == "Системи SIEM, регулярні аудитори, політика доступу, ISO 27001":
        return 0.7
    elif value == "IEC 62443, Zero Trust, постійний моніторинг, Pen Testing":
        return 0.9

def map_tech_3(value):
    if value == "Використання майже відсутнє":
        return 0.1
    elif value == "Використовуються окремі цифрові елементи":
        return 0.3
    elif value == "Часткова цифровізація ключових етапів":
        return 0.5
    elif value == "Переважна частина виробництва використовує цифрові технології":
        return 0.7
    elif value == "Майже повна цифровізація, синхронізація з ERP, MES, IoT тощо":
        return 0.9

def map_tech_4(value):
    if value == "Обладнання старше 15 років, не підтримує підключення до цифрових мереж":
        return 0.1
    elif value == "Частина обладнання оновлена, але загалом технічно відстале":
        return 0.3
    elif value == "Середній стан, частково придатне до модернізації":
        return 0.5
    elif value == "Нове обладнання, підтримує цифровий моніторинг, часткова інтеграція":
        return 0.7
    elif value == "Високотехнологічне, сумісне з Industry 4.0, інтеграція з хмарними платформами":
        return 0.9

```

```
def map_tech_5(value):
    if value == "Працівники не мають цифрових навичок, відсутнє навчання":
        return 0.1
    elif value == "Лише обмежене коло персоналу проходило навчання":
        return 0.3
    elif value == "Близько половини персоналу мають базові цифрові навички":
        return 0.5
    elif value == "Більшість персоналу підготовлена, діють цифрові ініціативи":
        return 0.7
    elif value == "Системна цифрова культура, регулярне навчання, лідерство у цифровій трансформації":
        return 0.9
```

```
tech_prediction = map_tech_1(VAR_TECH_1)*W_TECH_1 + \
    map_tech_2(VAR_TECH_2)*W_TECH_2 + \
    map_tech_3(VAR_TECH_3)*W_TECH_3 + \
    map_tech_4(VAR_TECH_4)*W_TECH_4 + \
    map_tech_5(VAR_TECH_5)*W_TECH_5
```

```
def map_tech_risk_level(value):
    if value <= 0.3:
        return 'high'
    elif (value > 0.3) & (value <= 0.7):
        return 'medium'
    elif value > 0.7:
        return 'low'
prediction_tech_level = map_tech_risk_level(tech_prediction)
```

```
#####
#####      INTEGRAL INDEX      #####
#####
```

```
Is = W_T_1*(1-finance_prediction) + \
    W_T_2*(1-staff_prediction_selected/(staff_prediction_selected+1)) + \
    W_T_3*tech_prediction
```

```
def map_total_risk_level(value):
```

```

if value <= 0.3:
    return 'high'
elif (value > 0.3) & (value <= 0.7):
    return 'medium'
elif value > 0.7:
    return 'low'
prediction_total_level = map_total_risk_level(Is)

#####
#### ____ Front end ____ ####
#####

st.divider() # Draws a horizontal rule
st.divider() # Draws a horizontal rule

def display_risk_level(prediction_level, size = 24):
    if prediction_level == "low":
        st.markdown(f'<p style="color:green; text-align: center; font-size:{size}px;">● Низький
ризик</p>', unsafe_allow_html=True)
    elif prediction_level == "medium":
        st.markdown(f'<p style="color:orange; text-align: center; font-size:{size}px;">● Середній
ризик</p>', unsafe_allow_html=True)
    elif prediction_level == "high":
        st.markdown(f'<p style="color:red; text-align: center; font-size:{size}px;">● Високий
ризик</p>', unsafe_allow_html=True)

st.markdown(f'""<div style="padding-top: 30px;"><h3 style="text-align: center;">
Інтегральний показник економічної безпеки: {round(Is,2)}</h3></div>""',
unsafe_allow_html=True)
display_risk_level(prediction_total_level, 32)

st.divider() # Draws a horizontal rule

col1_main, col2_main, col3_main = st.columns(3)
with col1_main:
    st.markdown("<div style='padding-bottom: 48px ;text-align: center; font-size:24px;'>Фінансова
складова</div>", unsafe_allow_html=True)

```

```

#st.markdown("Рівень ризику фінансової підсистеми економічної безпеки*: ")
display_risk_level(prediction_finance_level, 20)
with col2_main:
    st.markdown("<div style='padding-bottom: 48px ;text-align: center; font-size:24px;'> Кадрова складова</h3></div>", unsafe_allow_html=True)
    #t.write("Рівень ризику кадрової підсистеми економічної безпеки*: ")
    display_risk_level(prediction_staff_level, 20)
with col3_main:
    st.markdown("<div style='padding-bottom: 10px ;text-align: center; font-size:24px;'>Техніко-технологічна складова</h3></div>", unsafe_allow_html=True)
    #st.markdown("Рівень ризику фінансової підсистеми економічної безпеки*: ")
    display_risk_level(prediction_tech_level, 20)

st.divider() # Draws a horizontal rule
st.divider() # Draws a horizontal rule

st.subheader('Рекомендації щодо тактичних і стратегічних дій')

def general_recommendation(prediction_level, size = 24):
    if prediction_level == "low":
        st.markdown(f'<p style="color:green; text-align: center; font-size:{size}px;">🟢 Моніторинг та підтримка стандартного режиму безпеки</p>', unsafe_allow_html=True)
    elif prediction_level == "medium":
        st.markdown(f'<p style="color:orange; text-align: center; font-size:{size}px;">🟡 Активація цільових заходів у необхідних підсистемах безпеки</p>', unsafe_allow_html=True)
    elif prediction_level == "high":
        st.markdown(f'<p style="color:red; text-align: center; font-size:{size}px;">🔴 Активне антикризове реагування</p>', unsafe_allow_html=True)

df_recom = pd.read_csv(RECOMMENDATIONS_FILE, sep=';')

general_recommendation(prediction_total_level, size = 24)
#Recommendations for finance system
st.markdown("<div style='padding-bottom: 8px; font-size:24px;'>Рекомендації для фінансової підсистеми:</div>", unsafe_allow_html=True)
st.markdown(df_recom[(df_recom['risk_level'] == prediction_finance_level) & (df_recom['system']=='finance')]['recommendations'].values[0], unsafe_allow_html=True)

```

```

#Recomendations for staff system
st.markdown("<div style='padding-bottom: 8px; font-size:24px;'>Рекомендації для кадрової
підсистеми:</div>", unsafe_allow_html=True)
st.markdown(df_recom[(df_recom['risk_level'] == prediction_staff_level) &
(df_recom['system']=='staff')]['recommendations'].values[0], unsafe_allow_html=True)
#Recomendations for tech system
st.markdown("<div style='padding-bottom: 8px; font-size:24px;'>Рекомендації для техніко-
технологічної підсистеми:</div>", unsafe_allow_html=True)
st.markdown(df_recom[(df_recom['risk_level'] == prediction_tech_level) &
(df_recom['system']=='tech')]['recommendations'].values[0], unsafe_allow_html=True)


st.divider() # Draws a horizontal rule
st.divider() # Draws a horizontal rule


st.subheader('Показники Фінансової складової безпеки')
def prepare_fin_table(dataset):
    fin_vars = dataset.transpose().reset_index()
    fin_vars.columns = ['variable', 'number']

    finance_var_dict = pd.read_csv(FINANCE_DICT, sep = ';')
    finance_var_dict['variable'] = finance_var_dict['variable'].str.lower()
    finance_results = finance_var_dict.merge(fin_vars, how = 'left', on = 'variable')
    finance_results = finance_results[~finance_results['number'].isna()]
    finance_results['number'] = round(finance_results['number'].astype(float), 3)
    return finance_results[['formula', 'number']]

finance_results_table = prepare_fin_table(dataset_fin)
st.table(finance_results_table)


st.divider() # Draws a horizontal rule


st.subheader('Показники Кадрової складової безпеки')

VAR_EMPLOYEE = st.selectbox("Оберіть робітника",
                             ['Робітник ' + str(i) for i in range(1,13,1)])

```

```
dataset_staff = pd.read_csv(f'{PATH_STAFF_DATA}/dataset_v1_small.csv')
dataset_staff['day'] = pd.to_datetime(dataset_staff['day'])
staff_prediction = prediction_staff(dataset_staff, model_iso)

fig_user_activity = plot_user_stat(staff_prediction, VAR_EMPLOYEE, anomaly_col =
'high_risk_ind')
st.pyplot(fig_user_activity)
```

Приватне акціонерне товариство  
«Дружківський завод металевих виробів»  
(ПрАТ «ДРЗМВ»)  
вул. Симферопольська, 17, м. Дніпро,  
Дніпропетровської обл., Україна, 49005  
web: www.dmf.com.ua  
IBAN UA963348510000000002600224241  
у банку АТ «ПУМБ»  
ІПН 001910505109  
код ЄДРПОУ 00191052



ДСТУ  
ISO 9001-2015

Private joint-stock company  
«Druzhkivka hardware plant»  
(PJSC «DRHP»)  
Simferopolska street, 17, Dnipro  
Dnipropetrovsk region, Ukraine, 49005  
web: www.dmf.com.ua  
IBAN UA963348510000000002600224241  
at the bank JSC «PUF»  
INT 001910505109  
USREOU code 00191052

## АКТ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ НАУКОВОЇ РОБОТИ

м. Дружківка  
18 11 2024 року

Цей акт складено для підтвердження впровадження результатів наукової роботи Біличенка Максима Миколайовича у діяльність Приватного акціонерного товариства «Дружківський завод металевих виробів».

**Мета впровадження.** Зміцнення системи управління персоналом підприємства з акцентом на цифрову безпеку, аналіз і мінімізацію ризиків, пов'язаних із сучасними викликами цифровізації та людським фактором.

### Основні положення впровадженої роботи

1. Механізм управління цифровою безпекою персоналу Розроблений механізм забезпечує комплексний підхід до ідентифікації та аналізу ризиків у сфері управління персоналом, зокрема ризиків, пов'язаних із витокі конфіденційної інформації, недобросовісною поведінкою працівників та несанкціонованим доступом до даних підприємства.

2. Інтеграція цифрових інструментів в управління персоналом Впроваджено інформаційну систему моніторингу, яка дозволяє в режимі реального часу відстежувати дії працівників, що можуть мати потенційні ризики для цифрової безпеки. Система включає аналіз поведінкових показників персоналу, а також попередження про можливі загрози.

3. Підвищення кваліфікації працівників у сфері цифрової безпеки Запроваджено програму навчання персоналу з питань кібергігієни та управління ризиками, що дозволяє мінімізувати вплив людського фактору на безпеку підприємства.

4. Модель кадрової безпеки в умовах цифровізації Впроваджено модель оцінки кадрової безпеки, яка дозволяє аналізувати вплив цифрових технологій на стабільність кадрового потенціалу, зокрема оцінювати ризики втрати ключових співробітників та недобросовісної поведінки.

### Очікувані результати

1. Зниження ризиків витокі конфіденційної інформації.
2. Покращення управління персоналом через прозорі процеси моніторингу та оцінки дій працівників.
3. Підвищення обізнаності персоналу щодо питань цифрової безпеки.
4. Забезпечення стабільності кадрового потенціалу підприємства в умовах цифрових викликів.

### Підписи сторін:

Від ПрАТ «Дружківський завод металевих виробів»:  
Генеральний директор

С.С. Зімбровський

Від виконавця:

Біличенко М.М.

Документ підтверджує завершення процесу впровадження наукових розробок та їхнє використання в діяльності підприємства.

## ДОВІДКА

про впровадження результатів дисертаційного дослідження  
Біличенка Максима Миколайовича на здобуття наукового ступеня  
доктора філософії за спеціальністю 051 Економіка  
на тему «Система економічної безпеки підприємства в умовах цифрової  
трансформації»

Ознайомившись з результатами дисертаційної Біличенка Максима Миколайовича на тему «Система економічної безпеки підприємства в умовах цифрової трансформації» ПрАТ «Інститут керамічного машинобудування «КЕРАММАШ» повідомляє про теоретичну і практичну цінність даних напрацювань.

Сьогодні економічна безпека підприємства виходить на перший у низці питань щодо виживання економіки України. Дослідження мають прикладний характер і орієнтовані на створення інструментів для аналізу, оцінки та мінімізації ризиків у фінансово-економічній сфері.

В межах наукового дослідження:

1. Розроблено економіко-математичну модель для визначення та раннього попередження ризиків банкрутства, яка дозволяє оперативно оцінювати стан фінансової безпеки підприємства та своєчасно впроваджувати коригувальні заходи.

2. Створено механізм аналізу впливу цифрових технологій на економічну безпеку підприємства. Завдяки цьому підходу було вдосконалено процес прийняття управлінських рішень з урахуванням сучасних викликів цифровізації.

3. Створено інтегровану інформаційну модель, яка дозволяє підвищити ефективність управління економічною безпекою шляхом оптимізації процесу прийняття як оперативних, так і стратегічних рішень.

Результати наукової роботи Біличенка М.М. були впроваджені в систему управління підприємством, що дозволило підвищити ефективність управлінських процесів та знизити рівень економічних ризиків і забезпечити стабільний розвиток підприємства.

Голова Правління  
ПрАТ «Інститут керамічного  
машинобудування «Керамаш»

Р.О. Згоденко

**ДОВІДКА**  
**про впровадження результатів дисертаційного дослідження**  
**Біличенка Максима Миколайовича**  
**на тему: «Система економічної безпеки підприємства в умовах цифрової**  
**трансформації», яку подано на здобуття ступеня доктора філософії за**  
**спеціальністю 051 «Економіка»**

У систему управління підприємством інтегровано розроблену Біличенком М. М. прикладну модель фінансової безпеки. В умовах активної цифровізації бізнес-процесів використання цієї моделі дозволило удосконалити механізм моніторингу платоспроможності потенційних клієнтів, автоматизувати оцінку фінансових ризиків при проведенні електронних розрахунків та підвищити рівень захищеності фінансових ресурсів підприємства від зовнішніх загроз.

Розроблена система управління фінансовою безпекою базується на використанні сучасних цифрових інструментів інтелектуального аналізу даних щодо фінансових операцій підприємства, що забезпечує глибоке дослідження та оперативну обробку великих обсягів інформації. Завдяки цьому технологічному механізму стало можливим проводити моніторинг зовнішніх та внутрішніх загроз фінансовим ресурсам у режимі реального часу, прогнозувати їхній вплив на платоспроможність підприємства та оперативно впроваджувати відповідні антикризові заходи.

Використання зазначених науково-методичних розробок сприяло суттєвому підвищенню рівня фінансової стійкості ТОВ «Видавництво Фоліо». Підприємство отримало можливість приймати більш обґрунтовані управлінські рішення щодо розподілу капіталу, підвищити рівень захищеності своїх фінансових ресурсів та створити умови для стійкого розвитку в умовах високої конкуренції на цифровому ринку.

Генеральний директор  
ТОВ «ВИДАВНИЦТВО ФОЛІО»



Красовицький О. В.



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО  
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»  
(КАІ)

Проспект Гузара Любомира, 1, м. Київ, 03058, тел. (044) 497 51 51, факс: (044) 408 30 27  
E-mail: post@kai.edu.ua, http://www.kai.edu.ua, код ЄДРПОУ 45853942  
Система менеджменту якості університету сертифікована за ISO 9001:2015

28.05.2025 № 1355/60

На № \_\_\_\_\_ від \_\_\_\_\_

**ДОВІДКА**

**про впровадження в навчальний процес наукових результатів  
дисертаційної роботи Біличенка М.М. на тему:  
«Система економічної безпеки підприємства в умовах цифрової  
трансформації», яка подана на здобуття ступеня доктора філософії  
з галузі знань 05 «Соціальні та поведінкові науки»  
за спеціальністю 051 «Економіка»**

Запропоновані автором наукові положення та практичні рекомендації стосовно теми: «Система економічної безпеки підприємства в умовах цифрової трансформації» дозволили ДНП «Державний університет «Київський авіаційний інститут» використати окремі положення результатів дослідження в навчальному процесі кафедри економіки при підготовці фахівців:

зі спеціальності 051 «Економіка» за освітньо-професійною програмою «Економіка підприємства» при викладанні на першому (бакалаврському) рівні вищої освіти дисципліни – «Інструменти Big Data для бізнесу»; на другому (магістерському) рівні вищої освіти дисципліни – «Моделювання та управління розвитком економічних систем», «Міжнародна економічна безпека»

Результати дослідження впроваджено без фінансових зобов'язань перед автором.

Проректор з наукових досліджень та  
трансферу технологій, д.т.н., проф.



Сергій ГНАТЮК

В.о. декана факультету економіки та бізнес-  
адміністрування, д.е.н., проф.

Сергій СМЕРІЧЕВСЬКИЙ

Комісія кафедри економіки:

в.о. завідувача кафедри економіки,  
д.е.н., проф.

Олена АРЕФ'ЄВА

доцент кафедри економіки,  
к.е.н., доц.

Тетяна СІМКОВА

доцент кафедри економіки,  
к.е.н., доц.

Марія АНДРІЄНКО



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО  
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»  
(КАІ)**

Проспект Гузара Любомира, 1, м. Київ, 03058, тел. (044) 497 51 51, факс: (044) 408 30 27  
E-mail: post@kai.edu.ua, http://www.kai.edu.ua, код ЄДРПОУ 45853942  
Система менеджменту якості університету сертифікована за ISO 9001:2015

28.05.2025 № 1354/50

На № \_\_\_\_\_ від \_\_\_\_\_

**ДОВІДКА**

про використання результатів та окремих пропозицій  
Біличенка Максима Миколайовича, поданих в дисертації на здобуття наукового  
ступеня доктора філософії на тему  
«Система економічної безпеки підприємства в умовах цифрової трансформації»

В процесі наукових досліджень, проведених Біличенком М.М. на факультеті економіки та бізнес-адміністрування Державного університету «Київський авіаційний інститут», отримані результати, які впроваджені в науково-дослідницьких темах:

«Моделювання складних систем в контексті цифрової трансформації економічних процесів» (номер державної реєстрації 0120U103263, 2020-2022 рр.);

«Розвиток соціально-економічних систем в умовах турбулентності світової економіки» (номер державної реєстрації 0123U100645, 2023-2025 рр.);

Безпосередньо використана концептуальна модель управління економічною безпекою підприємства в умовах цифрової трансформації, яка враховує особливості впливу цифрових ризиків на ключові підсистеми функціонування підприємств; методичний підхід до моделювання цифрової безпеки підприємства, що дозволяє оцінити можливості підприємства протистояти цифровим ризикам та мінімізувати ймовірні збитки шляхом формування багаторівневої безпекової системи.

Очікуваний соціально-економічний ефект від впровадження розробок Біличенко М.М. має бути досягнуто за рахунок підвищення якості інтегрованих управлінських рішень.

Проректор з наукових досліджень та  
трансферу технологій



*[Signature]* Сергій ГНАТЮК

В.о. декана факультету економіки та бізнес-  
адміністрування, д.е.н., проф.

*[Signature]* Сергій СМЕРІЧЕВСЬКИЙ

001287