Черкаський національний університет імені Богдана Хмельницького
Міністерство освіти і науки України

Черкаський національний університет імені Богдана Хмельницького
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ПАВЛЮК ЄВГЕНІЙ СТАНІСЛАВОВИЧ

УДК 005.21:005.334:330.341.1

ДИСЕРТАЦІЯ

АДАПТАЦІЯ СТРАТЕГІЧНОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ ДЛЯ ПРОТИДІЇ ЦИФРОВИМ РИЗИКАМ ЕКОНОМІЧНІЙ БЕЗПЕЦІ

073 Менеджмент

07 Управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник:
Назаренко Сергій Анатолійович, доктор економічних наук, професор

Черкаси – 2026

АНОТАЦІЯ

Павлюк Є.С. Адаптація стратегічного управління підприємством для протидії цифровим ризикам економічній безпеці. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 073 Менеджмент. – Черкаський національний університет імені Богдана Хмельницького. Черкаси, 2026.

Дисертацію присвячено вирішенню важливого наукового завдання, що полягає в доповненні, розширенні та оновленні науково-методичних засад і практичних підходів до адаптивної модифікації системи стратегічного управління підприємством у напрямі спрямування її ресурсів і потенціалу на забезпечення його економічної безпеки в умовах інтенсифікації цифрових ризиків зовнішнього та внутрішнього середовищ.

У першому розділі «Теоретичні засади безпеко орієнтованого стратегічного управління підприємствами під впливом цифрових ризиків» проведено логічний аналіз теоретичних основ стратегічного управління у теорії менеджменту діяльності підприємств, простежено зміни парадигм стратегічного управління підприємствами під впливом пермакризи та ризиків світу BANI та окреслено сучасний стан розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації.

Узагальнено та охарактеризовано змістові трансформації класичних суджень щодо елементів парадигмальних засад стратегічного менеджменту у сучасній науці управління. Встановлено, що у теорії стратегічного управління на заміну категорії стратегічних цілей прийшло поняття стратегічних орієнтирів функціонування та розвитку бізнесу; стійкі конкурентні переваги змінилися на динамічні спроможності та можливості підприємства виживати в мінливих умовах; стратегічне планування поступово заміщується сценарним плануванням управлінських дій; управління стратегічними ризиками набуває формату забезпечення стратегічної економічної безпеки компанії; під стратегічними активами бізнесу науковці починають розуміти його стратегічні

можливості і спроможності; замість категорії прогнозування набуло поширення поняття форсайту; інтереси власників бізнесу стають другорядними порівняно з інтересами решти категорій стейкхолдерів; стратегічний горизонт планування управлінських скоротився до трьох-п’яти років, а контроль і нагляд замінюється процесами оцінювання і адаптації стратегічних управлінських рішень.

Ідентифіковано потребу у перегляді та оновленні парадигмальних засад стратегічного управління підприємством у світі BANI та запропоновано конкретні напрямки їх змін, такі як запровадження принципів гнучкого та сценарного управління, застосування адаптивного менеджменту та антикризових стратегій, запровадження практик критичного мислення та сценарного аналізу, використання цифрових технологій, інформації з різних джерел та штучного інтелекту як корпоративних ресурсів; перехід до децентралізації влади та гнучких управлінських структур; розвиток цифрового управління бізнес-процесами; розвиток екосистем і стратегічних альянсів; масштабування практик людиноцентричного управління підприємствами та використання прогностичної аналітики та технік форсайту для прийняття та реалізації управлінських рішень.

Дістали подальшого розвитку класичні судження термінополя стратегічного менеджменту та їх змістові трансформації у сучасній науці управління. Економічну безпеку підприємства визначено як динамічний стан захищеності його корпоративних ресурсів від традиційних і інноваційних (цифрових і кібернетичних) загроз і ризиків, що забезпечує стійкість і сталість бізнес-процесів в умовах цифрової трансформації та дозволяє оперативно реагувати та використовувати можливості зовнішнього та внутрішнього середовищ. Стратегічне управління підприємством ідентифіковано як безперервний процес адаптації його стратегічних орієнтирів і прийняття довгострокових управлінських рішень на основі аналізу цифрових даних із використанням цифрових технологій, спрямованих на забезпечення стійкості та конкурентоспроможності бізнесу. Формалізовано чотири етапи розвитку

наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації. Сучасний етап розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації ознаменувався переосмисленням стратегічного управління економічною безпекою в умовах крихкості, тривожності, нелінійності та незрозумілості, тобто у реаліях світу BANI, що призвело до формування принципів стратегічного менеджменту в умовах пермакризи, адаптації підходів стратегічного управління до реалій воєнного часу, у результаті чого відбулося концептуальне поєднання теорій антикризового, стратегічного, ризик-менеджменту з принципами гнучкого управління та адаптивності.

У другому розділі «Діагностика стану стратегічного управління підприємствами та досягнутого ними рівня економічної безпеки» надано характеристику методичних підходів до розробки стратегій для сучасних підприємств з позиції вітчизняного та зарубіжного досвіду, піддано аналізу вплив цифрових ризиків на стан економічної безпеки підприємства як елементу обґрунтування досяжності його стратегічних цілей та надано оцінку ефективності безпеко орієнтованих стратегій українських підприємств.

Аналіз особливостей стратегій «кольорових океанів» дозволив розкрити можливості їх використання в Україні у різних галузях економіки. У воєнний час найбільш актуальними та доцільними для запровадження запропоновано вважати такі стратегії, як стратегія Червоного океану та стратегія Рожевого океану. Запропоновано авторський методичний підхід до розробки стратегій для сучасних підприємств в умовах невизначеності та ризиків, перевагою якого є комплексність і всеосяжність, що проявляється у охопленні трьох рівнів менеджменту організації – стратегічного, тактичного та оперативного. На відміну від класичних методичних підходів до розробки та реалізації стратегії, де контроль є завершальним етапом, цей метод адаптований до умов невизначеності та ризиків завдяки інтеграції контролю і моніторингу у кожен стратегічний етап діяльності підприємства, що є критично важливим кроком

для економічної стійкості підприємства в умовах воєнних ризиків, непередбачуваності та нелінійності світу BANI.

Доведено, що планування стратегічних орієнтирів суб'єктів господарювання, які використовують цифрові технології у межах своєї діяльності, має супроводжуватись оцінюванням як традиційних, так і цифрових ризиків. У тому випадку, коли їх потенційний вплив на досяжність довгострокових цілей підприємства характеризується як надмірно високий, менеджменту варто переглянути сценарії стратегії та адаптувати її окреслених реалій і перспектив. Виявлено, що для сучасних підприємств характерними є такі цифрові ризики: кібернетичні та технологічні ризики використання цифрових і інформаційних технологій, таргетовані атаки на цифрові екосистеми суб'єктів господарювання, кібершпигунтство, втрата цифрових даних і доступу до них, деградація хмарних сервісів, цифрова міграція, фішинг, цифрове інсайдерство, низький рівень цифрової грамотності та цифрових компетенцій. Аналіз кейсів вітчизняних і зарубіжних компаній щодо протидії цифровим ризикам дозволив встановити їх деструктивний вплив на стан переважної більшості функціональних складових системи економічної безпеки: фінансової, інтелектуально-кадрової, техніко-технологічної, інформаційно-аналітичної, виробничої, матеріальної, правої.

На підставі аналізу даних з відкритих джерел та думок експертів, було оцінено рівень економічної безпеки десяти підприємств, що входять до складу критичної інфраструктури України. Наявність серед об'єктів критичної інфраструктури компаній з низьким рівнем економічної безпеки засвідчило потребу перегляду та адаптації їх стратегій або ж модернізації механізмів і алгоритмів їх реалізації.

У третьому розділі «Напрями адаптивної модифікації стратегічного управління підприємством для протидії цифровим ризикам його економічної безпеки» узагальнено та уточнено концептуальні засади адаптації стратегічного управління підприємствами під впливом цифровізації, запропоновано напрями оновлення механізму стратегічного управління економічною безпекою

підприємства із дотриманням балансу інтересів стейкхолдерів та досліджено можливості інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку підприємств в Україні.

Запропоновано авторські дефініції таких категорій, як «адаптація стратегії», «стратегія адаптації» та «адаптована стратегія». Сформовано матрицю найбільш поширених інтересів традиційних груп стейкхолдерів сучасних українських підприємств. У ній узагальнено стратегічні інтереси пов'язаних сторін, конкретизовано вектори їх зацікавленості у площині управлінні цифровими ризиками і економічною безпекою. Особливістю цієї матриці як інструменту інформаційного забезпечення адаптивного менеджменту у системі стратегічного управління суб'єктів господарювання є ідентифіковані ризики для конкурентних перспектив підприємства у випадках, якщо інтереси різних груп стейкхолдерів не будуть досягнуті. Саме останній аспект став аргументом на користь потреби балансування таких інтересів як інструменту досягнення базового рівня довгострокової економічної безпеки підприємств в умовах невизначеності, реалій воєнного часу та світу BANI.

Набули подальшого розвитку практики інформаційного забезпечення прийняття безпеко орієнтованих управлінських рішень завдяки використанню результатів SWOT і STEEPLE-аналізів для діагностики стану традиційних механізмів стратегічного управління економічною безпекою підприємств, що дозволили сформувати чотири сценарії адаптації безпеко орієнтованого менеджменту до соціальних, технологічних, економічних, екологічних, політичних, юридичних і етичних чинників функціонування сучасного бізнесу, такі як: адаптація сильних сторін до можливостей (SO-адаптована стратегія), адаптація сильних сторін до загроз (ST-адаптована стратегія), адаптація слабких сторін до можливостей (WO-адаптована стратегія), адаптація слабких сторін до загроз (WT-адаптована стратегія), та конкретизувати їх цільові орієнтири для сталого розвитку суб'єктів господарювання в умовах невизначеності та ризиків.

Запропоновано авторський підхід до інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств полягає у реалізації чотирьох етапів управлінських дій: аналізі зовнішнього середовища; формуванні та використанні організаційно-управлінського механізму, що інтегрує принципи превентивності, адаптивності, прийняття рішень на основі актуальних даних, балансування інтересів стейкхолдерів, нульової довіри та резильєнтності у безпеко орієнтовану стратегію, що реалізується на наступному етапі та сприяє цифровому економічному розвитку бізнесу (четвертий фінальний етап). Ідеологічними стовпами стратегії підприємства при цьому є: управління ризиками, проєктне управління, управління на основі актуальних даних, стейкхолдер-менеджмент, забезпечення цифрової безпеки та антикризовий менеджмент.

Удосконалено механізм стратегічного управління економічною безпекою підприємства, що відрізняється від існуючих глибокою інтеграцією принципів цифрового ризик-менеджменту в управлінські процеси, обов’язковістю процедури діагностики стану дотримання балансу інтересів основних груп стейкхолдерів і комплексним застосуванням можливостей гнучкого менеджменту на усіх етапах його функціонування, що дозволило адаптувати стратегії безпеко орієнтованого стратегічного управління українськими компаніями до деструктивних впливів цифровізації, ризиків війни, тенденцій BANI-світу, кадрового голоду, проявів пермакризи та загальноекономічної невизначеності зовнішнього середовища.

Ключові слова: стратегія, стратегічне управління, управлінські рішення, цифровізація, економічна безпека, конкурентоспроможність, цифрова стратегія, цифрові ризики, адаптація, бізнес-процес.

ANNOTATION

Pavliuk Ye.S. Adapting strategic enterprise management to counter digital economic security risks. – Qualification scientific work in the manuscript form.

The thesis for the scientific degree of Doctor of Philosophy in specialty 073 Management. – Bohdan Khmelnytsky National University of Cherkasy. Cherkasy, 2026.

The dissertation is dedicated to solving an important scientific problem, which consists in supplementing, expanding and updating scientific and methodological principles and practical approaches to adaptive modification of the enterprise's strategic management system in the direction of directing its resources and potential to ensure its economic security in the face of intensification of digital risks in external and internal environments.

The first section, “Theoretical Principles of Security-Oriented Strategic Management of Enterprises Under the Influence of Digital Risks,” provides a logical analysis of the theoretical foundations of strategic management in the theory of enterprise management, traces changes in the paradigms of strategic management of enterprises under the influence of the perma-crisis and risks of the BANI world, and outlines the current state of development of scientific theories of strategic management of the economic security of an enterprise in the context of digitalization.

The substantive transformations of classical judgments regarding the elements of the paradigmatic principles of strategic management in modern management science are summarized and characterized. It is established that in the theory of strategic management, the category of strategic goals has been replaced by the concept of strategic guidelines for the functioning and development of a business; sustainable competitive advantages have changed to dynamic capabilities and the ability of an enterprise to survive in changing conditions; strategic planning is gradually being replaced by scenario planning of management actions; strategic risk management is taking the form of ensuring the strategic economic security of the company; scientists are beginning to understand the strategic capabilities and capabilities of a business under strategic assets; instead of the category of forecasting,

the concept of foresight has become widespread; the interests of business owners are becoming secondary compared to the interests of other categories of stakeholders; the strategic horizon of management planning has been reduced to three to five years, and control and supervision are being replaced by processes of evaluation and adaptation of strategic management decisions.

The need to review and update the paradigmatic principles of strategic enterprise management in the BANI world has been identified and specific directions for their changes have been proposed, such as the introduction of the principles of flexible and scenario management, the application of adaptive management and anti-crisis strategies, the introduction of critical thinking and scenario analysis practices, the use of digital technologies, information from various sources and artificial intelligence as corporate resources; the transition to decentralization of power and flexible management structures; the development of digital management of business processes; the development of ecosystems and strategic alliances; the scaling of human-centric enterprise management practices and the use of predictive analytics and foresight techniques for making and implementing management decisions.

The classical judgments of the strategic management terminology and their substantive transformations in modern management science have been further developed. The economic security of an enterprise is defined as a dynamic state of protection of its corporate resources from traditional and innovative (digital and cyber) threats and risks, which ensures the stability and sustainability of business processes in the context of digital transformation and allows for prompt response and use of the capabilities of external and internal environments. Strategic management of an enterprise is identified as a continuous process of adapting its strategic guidelines and making long-term management decisions based on the analysis of digital data using digital technologies aimed at ensuring the sustainability and competitiveness of the business. Four stages of development of scientific theories of strategic management of economic security of an enterprise in the context of digitalization are formalized. The current stage of development of scientific theories of strategic management of economic security of an enterprise in the context of

digitalization was marked by a rethinking of strategic management of economic security in conditions of fragility, anxiety, nonlinearity and incomprehensibility, that is, in the realities of the BANI world, which led to the formation of principles of strategic management in conditions of perma-crisis, adaptation of strategic management approaches to the realities of wartime, as a result of which there was a conceptual combination of theories of anti-crisis, strategic, risk management with the principles of flexible management and adaptability.

The second section, “Diagnostics of the State of Strategic Management of Enterprises and the Level of Economic Security Achieved by Them,” provides a description of methodological approaches to developing strategies for modern enterprises from the perspective of domestic and foreign experience, analyses the impact of digital risks on the state of economic security of an enterprise as an element of substantiating the attainability of its strategic goals, and provides an assessment of the effectiveness of security-oriented strategies of Ukrainian enterprises.

The analysis of the features of the "colored oceans" strategies allowed to reveal the possibilities of their use in Ukraine in various sectors of the economy. In wartime, it is proposed to consider such strategies as the Red Ocean strategy and the Pink Ocean strategy as the most relevant and appropriate for implementation. An author's methodological approach to developing strategies for modern enterprises in conditions of uncertainty and risks is proposed, the advantage of which is complexity and comprehensiveness, which is manifested in the coverage of three levels of organization management - strategic, tactical and operational. Unlike classical methodological approaches to developing and implementing a strategy, where control is the final stage, this method is adapted to conditions of uncertainty and risks due to the integration of control and monitoring into each strategic stage of the enterprise's activity, which is a critically important step for the economic stability of the enterprise in conditions of war risks, unpredictability and nonlinearity of the BANI world.

It has been proven that planning strategic guidelines of business entities that use digital technologies within their activities should be accompanied by an assessment

of both traditional and digital risks. In the event that their potential impact on the achievement of the long-term goals of the enterprise is characterized as excessively high, management should review the strategy scenarios and adapt it to the outlined realities and prospects. It has been found that the following digital risks are characteristic of modern enterprises: cyber and technological risks of using digital and information technologies, targeted attacks on digital ecosystems of business entities, cyber espionage, loss of digital data and access to them, degradation of cloud services, digital migration, phishing, digital insider trading, low level of digital literacy and digital competencies. Analysis of cases of domestic and foreign companies in combating digital risks allowed us to establish their destructive impact on the state of the vast majority of functional components of the economic security system: financial, intellectual and personnel, technical and technological, information and analytical, production, material, legal.

Based on the analysis of data from open sources and expert opinions, the level of economic security of ten enterprises that are part of the critical infrastructure of Ukraine was assessed. The presence of companies with a low level of economic security among the objects of critical infrastructure indicated the need to review and adapt their strategies or modernize the mechanisms and algorithms for their implementation.

The third section, “Directions for adaptive modification of strategic enterprise management to counter digital risks to its economic security,” summarizes and clarifies the conceptual principles for adapting strategic enterprise management under the influence of digitalization, proposes directions for updating the mechanism for strategic enterprise economic security management while maintaining a balance of stakeholder interests, and explores the possibilities of integrating digital risk management principles into the strategy for security-oriented economic development of enterprises in Ukraine.

Authorial definitions of such categories as “strategy adaptation”, “adaptation strategy” and “adapted strategy” are proposed. A matrix of the most common interests of traditional stakeholder groups of modern Ukrainian enterprises is formed.

It summarizes the strategic interests of related parties, specifies the vectors of their interest in the field of digital risk management and economic security. A feature of this matrix as a tool for information support of adaptive management in the strategic management system of business entities is the identified risks for the competitive prospects of the enterprise in cases where the interests of different stakeholder groups are not achieved. It is the latter aspect that became an argument in favor of the need to balance such interests as a tool for achieving the basic level of long-term economic security of enterprises in conditions of uncertainty, wartime realities and the BANI world.

The practice of information support for making security-oriented management decisions has been further developed through the use of the results of SWOT and STEEPLE analyses to diagnose the state of traditional mechanisms for strategic management of economic security of enterprises, which allowed us to form four scenarios for adapting security-oriented management to social, technological, economic, environmental, political, legal and ethical factors of the functioning of modern business, such as: adaptation of strengths to opportunities (SO-adapted strategy), adaptation of strengths to threats (ST-adapted strategy), adaptation of weaknesses to opportunities (WO-adapted strategy), adaptation of weaknesses to threats (WT-adapted strategy), and to specify their target guidelines for the sustainable development of business entities in conditions of uncertainty and risks.

The author's approach to integrating the principles of digital risk management into the strategy of security-oriented economic development of domestic enterprises is proposed, which consists in implementing four stages of management actions: analysis of the external environment; formation and use of an organizational and management mechanism that integrates the principles of prevention, adaptability, decision-making based on current data, balancing the interests of stakeholders, zero trust and resilience into a security-oriented strategy that is implemented at the next stage and contributes to the digital economic development of the business (fourth final stage). The ideological pillars of the enterprise strategy are: risk management,

project management, management based on current data, stakeholder management, ensuring digital security and anti-crisis management.

The mechanism of strategic management of the economic security of the enterprise has been improved, which differs from the existing ones by the deep integration of the principles of digital risk management into management processes, the mandatory procedure for diagnosing the state of maintaining the balance of interests of the main stakeholder groups, and the comprehensive application of flexible management capabilities at all stages of its operation, which allowed adapting the strategies of security-oriented strategic management of Ukrainian companies to the destructive effects of digitalization, risks of war, trends of the BANI world, personnel famine, manifestations of perma-crisis, and general economic uncertainty of the external environment.

Key words: strategy, strategic management, management decisions, digitalization, economic security, competitiveness, digital strategy, digital risks, adaptation, business process.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у фахових виданнях України

1. Шарий В.І., Павлюк Є. С. Логічний аналіз стратегічного управління в організації. *Економіка та суспільство*. 2024. №70. URL: https://economyandsociety.in.ua/index.php/journal/article/view/5342/5285 (дата звернення: 02.04.2026) https://doi.org/10.32782/2524-0072/2024-70-85. Категорія Б, Index Copernicus. (0,83 д.а., особистий внесок автора: обґрунтовано доцільність використання різних методів наукового дослідження для формування інформаційного підґрунтя для розробки функціональних стратегій підприємства – 0,5 д.а.).

2. Павлюк Є.С. Сучасні підходи до стратегічного управління підприємствами: зміни парадигм під впливом пермакризи та ризиків світу BANI. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут».* 2025. № 35. С.162-167. https://doi.org/10.20535/2307-5651.35.2025.352397. Категорія Б, Index Copernicus. – 0,80 д.а.

3. Павлюк Є.С. Оцінка впливу цифрових ризиків на стан економічної безпеки підприємства як елемент обґрунтування досяжності його стратегічних цілей. *Науково-виробничий журнал «Бізнес-навігатор».* 2026. Випуск 1 (84). С.9-14. https://doi.org/10.32782/business-navigator.84-2. Категорія Б, Index Copernicus. – 0,85 д.а.

4. Pavliuk E. Adaptation of strategic management of enterprises under the influence of digitalization to achieve a state of economic security. *Current Problems of Sustainable Development.* 2026. Vol. 3, № 1. P.83-90. https://doi.org/10.60022/3(1)-11S. Категорія Б, Index Copernicus. – 0,87 д.а.

Опубліковані праці апробаційного характеру

1. Pavliuk E. The place of risk management in strategies for ensuring the economic security of enterprises. *Сучасний стан та тенденції розвитку науки та освіти* : матеріали III Міжнародної науково-практичної конференції / Міжнародний гуманітарний дослідницький центр (м. Дніпро, 5 січня 2026 р.). Research Europe, 2026. С.177-181. https://doi.org/10.64076/ihrc260105. – 0,26 д.а.

2. Павлюк Є. С. Адаптація стратегії управління підприємством до ризиків економічній безпеці як засіб узгодження інтересів його стейкхолдерів. *Актуальні проблеми економіки, обліку, управління і права в сучасних умовах*: збірник тез доповідей міжнародної науково-практичної конференції (м. Рівне, 8 січня 2026 р.). Рівне: ЦФЕНД, 2026. С.95-98. – 0,21 д.а.

3. Pavliuk E. Current state of development of scientific theories of strategic management of enterprises under the influence of digitalization. *Пріоритетні напрями досліджень в науковій та освітній діяльності*: матеріали XVII Міжнародної науково-практичної конференції. м. Львів, 9-10 січня 2026 року. Львів: Львівський науковий форум, 2026. С.6-10. – 0,36 д.а.

4. Павлюк Є.С. Методичні підходи до розробки стратегій для сучасних підприємств: зарубіжний досвід для вітчизняних управлінців. *Сучасні наукові підходи до вирішення глобальних криз: роль інтеграції наук і технологій у змінах суспільства*: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 13 лютого 2026 р.). Кременчук: ЦФЕНД, 2026. С.28-31. – 0,22 д.а.

ЗМІСТ

ВСТУП

Актуальність дослідження. Нестабільність стану та непередбачуваність еволюційних змін архітектури соціально-економічних систем, у яких сучасні підприємства провадять свою фінансово-господарську діяльність, викликають у їх менеджменту все більше бажання мати принаймні орієнтовні стратегічні цілі свого функціонування та розвитку, що можуть характеризуватися як досяжні у середньостроковій і довгостроковій перспективах. Класичні теорії стратегічного управління суб'єктами господарювання не здатні виконати це завдання з огляду на те, що перспективне планування та прогнозування втрачають свою достовірність у середовищі невизначеності та ризиків. Реалії воєнного часу усе агресивніше спрямовують вітчизняні бізнес-структури у кризові тенденції, а цифровізація поглиблює їх негативні прояви для тих учасників ринків, які не були готовими адаптуватися та змінюватися у відповідності до вимог нових економічних моделей. Фрагментарні механізми управління економічною безпекою підприємств, які будувалися на ситуативному прийнятті управлінських рішень та випадкових реакціях персоналу на прояви ризиків, натепер не здатні забезпечити комплексний захист їх корпоративних ресурсів. З огляду на це, переосмислення у теоретико-методологічній площині базових постулатів стратегічного управління економічною безпеки підприємства під впливом цифрових ризиків стає актуальним науковим завданням, вартим пильної уваги як з боку фахівців-теоретиків, так і спеціалістів-практиків у царині безпеко орієнтованого менеджменту організацій.

Теоретико-методичні засади стратегічного управління суб'єктами господарювання у різних ідеологічних контекстах сформовані у публікаціях таких сучасних українських дослідників, як Ачкасов І. А., Білоус С. П., Вилєгжанін С. В., Вишневська В. А., Волос М. В., Гедз М. Й., Герасименко О. М., Гребенікова О. В., Гринько Т. В., Гуцалюк О. М., Демчишак Н., Денисова Т. В., Добровольська В. В., Зачосова Н. В.,

Іванова М. І., Квасницька Р. С., Кирилюк І.М., Клек А. Р., Климчук М. М., Климчук С. А., Коваленко А. О., Кононенко С. О., Коритько Т. Ю., Кравченко О.О., Криворучко О. М., Крілик Б. Б., Кубліцька О. В., Кульгук І. І., Куценко Д. М., Лігоненко Л. О., Левченко О. М., Логінова О., Ляховецький О. О., Назаренко С. А., Науменко С. Д., Новиков Д. М., Носань Н. С., Осадча О. О., Паламарчук О. М., Панченко В. А., Поляк О. П., Романинець О. В., Роздопченюк В. М., Сазонова С. В., Світовий О. М., Семенча І. Є., Сидорчук А. О., Скрипник Р. Є., Скоробогата Л. В., Фемяк О. А., Цісінський М. М., Шевченко А. М., Шиманович П. О., Шморгун О. А., Якубець М. Р., Якушева О.В., Яременко Л. М., Янгулов Е. П.

Фундаментальні основи стратегічного управління підприємствами у науковій площині були закладені такими відомими іноземними вченими та практиками менеджменту, як Майкл Портер (Michael Porter), Ігор Ансофф (Igor Ansoff), Пітер Друкер (Peter Drucker), Генрі Мінцберг (Henry Mintzberg). Мінливість зовнішнього середовища функціонування сучасних компаній та необхідність їх адаптації до реалій цифрових трансформацій економічного простору стали причиною для ініціювання цілого ряду досліджень закордонних науковців, у яких знайшли відображення методологічні поєднання проблем стратегічного менеджменту, цифровізації, ризиків і економічної безпеки бізнесу. Їх авторами стали Амбулі Т. В. (Ambuli T. V.), Анггрені Р. Н. (Anggraeni R. N.), Амір А. М. (Amir A. M.), Бхалла М. (Bhalla M.), Вагела К. (Vaghela K.), Вікрам Г. (Vikram G.), Гассманн О. (Gassmann O.), Гоел А. В. (Goel A. V.), Девендран А. (Devendran A.), Джадон Р. (Jadon R.), Джакелі К. (Djakeli K.), Демір Р. (Demir R.), Ел Валі А. (El Ouali A.), Ел Массауді Е. М. (El Massaoudii E. M.), Ел Хаммумі А. К. (El Hammoumi A.), Еспіна-Ромеро Л. (Espina-Romero L.), Ізагірре Ольмедо Х. С. Р. (Izaguirre Olmedo J. S. R.), Кайлай М. (Kailay M.), Коундал П. (Koundal P.), Крім Б. М. (Krim B. M.), Кумарі П. (Kumari P.), Лахденранта К. (Lahdenranta K.), Малевська К. (Malewska K.), Мікл Енсі Г. (Mickle Aancy H.), Наінгголан Ф. (Nainggolan F.), Пальмі М. (Palmié M.), Парра Д. Р. (Parra D. R.), Пашкевич Н. (Pashkevich N.),

Піч В. (Pietsch W.), Раджіндра Р. (Rajindra R.), Салман С. А. (Salman S. A.), Судхакар М. (Sudhakar M.), Турюнен Т. (Turunen T.), Феррер-Давалос Р. М. (Ferrer-Dávalos R. M.), Фітріянті С. Д. (Fitriyanti S. D.), Ху Б. (Hu B.), Цолак М. (Çolak M.), Чвілковська-Кубала А. (Chwiłkowska-Kubala A.), Червінка Т. (Červinka T.), Шилдт Г. (Schildt H.), Шимовський В. (Szumowski W.), Ювоно В. (Yuwono W.), Янг В. (Yang W.), Ян С. (Yan S.).

Водночас, не зважаючи на сформоване міцне теоретико-методичне підґрунтя стратегічного управління суб'єктами господарювання та його постійне оновлення у публікаціях наших сучасників, залишаються наріжними проблеми адаптації класичних постулатів стратеготворення до особливостей функціонування та розвитку підприємств, що перебувають під постійним впливом загроз і ризиків, породжених середовищем невизначеності перспективних економічних тенденцій. Непередбачуваність фінального результату цифрових трансформацій соціально-економічних систем вимагає постійної адаптивної модифікації механізмів стратегічного управління корпоративними ресурсами компаній для того, аби спрямувати їх на протидію цифровим ризикам для стану економічної безпеки бізнес-структур.

Наукове завдання дослідження полягає в доповненні, розширенні та оновленні науково-методичних засад і практичних підходів до адаптивної модифікації системи стратегічного управління підприємством у напрямі спрямування її ресурсів і потенціалу на забезпечення його економічної безпеки в умовах інтенсифікації цифрових ризиків зовнішнього та внутрішнього економічних середовищ.

Зв'язок роботи з науковими темами. Роботу виконано відповідно до плану НДР Черкаського національного університету імені Богдана Хмельницького. У межах теми «Парадигми управління системами і процесами для забезпечення фінансово-економічної безпеки на мікро- та макрорівнях» (номер державної реєстрації 0120U100615) було обґрунтовано елементи механізму адаптації стратегічного управління підприємствам для протидії цифровим ризикам його економічної безпеки, що поєднує моніторинг загроз у

режимі реального часу, оптимізацію корпоративних ресурсів і розвиток цифрових і соціальних компетенцій персоналу. Внеском у розробку наукової теми «Проблеми управління організаціями на шляху сталого розвитку» (номер державної реєстрації 0125U000127) стали сформовані концептуальні засади адаптивного стратегічного управління підприємствами, що базуються на принципах «цифрового імунітету», «нульової довіри» та цифрової грамотності та передбачають інтеграцію засобів протидії цифровим кадровим ризикам в стратегію сталого розвитку суб'єкта господарювання.

Мета і задачі дослідження. Метою дисертаційної роботи є теоретичне обґрунтування та розроблення методичних засад і практичних рекомендацій щодо адаптації класичної структури та функціоналу системи стратегічного управління підприємством з метою протидії цифровим ризикам динамічного середовища та їх наслідкам для стану економічної безпеки бізнесу.

Для реалізації поставленої мети необхідно комплексно вирішити сукупність таких завдань:

- провести логічний аналіз парадигмальних підвалин стратегічного управління у теорії менеджменту підприємств;
- простежити зміни парадигм стратегічного управління підприємствами під впливом пермакризи та ризиків світу BANI;
- описати сучасний стан розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації;
- надати характеристику методичних підходів до розробки стратегій для сучасних підприємств з позиції вітчизняного та зарубіжного досвіду;
- надати оцінку впливу цифрових ризиків на стан економічної безпеки підприємства;
- провести діагностику ефективності безпеко орієнтованих стратегій українських підприємств;
- модифікувати та доповнити концептуальні засади адаптації стратегічного управління підприємствами під впливом цифровізації;

- запропонувати шляхи оновлення механізму стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів;

- встановити можливості та перспективи інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку підприємств в Україні.

Об'єктом дослідження виступає процес стратегічного управління діяльністю підприємства та забезпечення його економічної безпеки в умовах інтенсивної цифровізації економічного простору.

Предметом дослідження є теоретико-методичні засади, прикладні інструменти та механізми адаптації стратегічного управління, спрямовані на виявлення, оцінювання та нейтралізацію цифрових ризиків економічної безпеки підприємства.

Методи дослідження. Для отримання релевантних висновків і розробки рекомендацій, що мають високий рівень достовірності, у процесі дослідження було використано такі методи наукового пізнання: логічний, генетичний та контент-аналізи – для критичного огляду парадигмальних підвалин стратегічного управління підприємствами та задля предметного розгляду етапів виникнення та популяризації концепцій стратегічного менеджменту (п. 1.1); метод теоретичного узагальнення, що дав змогу узагальнити існуючі підходи до стратегічного управління у єдину логічну структуру, що є об'єктом досліджень у науці управління (п.1.1-1.3); компаративний аналіз – для порівняння та модернізації класичних стратегій стратегічного управління підприємствами з адаптивними стратегіями, які виникають в реаліях світу BANI та під впливом економіки воєнного часу (п.1.2); абстрактно-логічний метод – для формування висновків і узагальнень про те, як мінливість зовнішніх умов ведення бізнесу змушують менеджмент суб'єктів господарювання відмовлятися від довгострокового прогнозування фінансово-економічних показників на користь обрання сценаріїв швидкого реагування на прояви ризиків і загроз (п.1.2-1.3); бібліометричний аналіз – для встановлення зв'язків та змістових співпадінь у

термінополях категорій «стратегічне управління» та «економічна безпека» (п.1.3); порівняльний метод – для зіставлення зарубіжних моделей стратегічного управління та підходів до розроблення стратегій з українськими практиками, які сформувались у реаліях воєнного стану та дефіциту корпоративних ресурсів (п.2.1); методи систематизації, класифікації та експертного оцінювання – для ідентифікації цифрових ризиків за рівнем їх впливу на стан економічної безпеки сучасних підприємств і на досяжність їх стратегічних орієнтирів (п.2.2); фінансово-економічний та коефіцієнтний аналізи, за допомогою яких було здійснено розрахунки значень індикаторів рівня економічної безпеки українських підприємств і окреслено сильні і слабкі сторони, можливості і загрози їх стратегічного розвитку (п.2.3); методи наукової індукції та дедукції – для пропозиції шляхів переходу від поодиноких кейсів конкретних компаній щодо успішної адаптації механізмів їх стратегічного управління до цифрових ризиків до розробки адаптованих до цифрових трансформацій бізнес-процесів систем економічної безпеки підприємств і стратегій управління ними (п.3.1); матричний метод стейкхолдер-аналізу – для пошуку балансу між інтересами та потребами різних груп зацікавлених осіб щодо стратегічних орієнтирів діяльності підприємств під впливом цифрових ризиків (п.3.2); системний підхід, що допоміг сформувати механізм цифрового ризик-менеджменту у системі стратегічного управління економічною безпекою як сукупність взаємопов’язаних елементів (ресурсів, інструментів, методів, тощо), націлених на збільшення можливостей резильєтності бізнесу та забезпечення його довгострокової стійкості у кризових умовах воєнного часу (п.3.3).

Інформаційну базу дисертаційного дослідження сформували такі ресурси відкритого доступу, як законодавство України, стратегічні документи загальнонаціонального рівня, міжнародні стандарти та фреймоворки у царині управління ризиками, наукові праці фундаторів і класиків стратегічного менеджменту організацій, теорії та концепції довгострокового планування та прогнозування діяльності підприємств, публікації сучасних українських і

зарубіжних вчених, які спеціалізуються на економічній безпеці та цифрових трансформаціях економічних відносин, матеріали науково-практичних конференцій і фахових періодичних видань, а також статистичні відомості з таких джерел, як звіти Державної служби статистики України, звіти міжнародних організацій та аналітичних агентств, звітність вітчизняних підприємств та інформаційні матеріали, розміщені на їх офіційних сайтах, а також результати власних досліджень автора.

Наукова новизна отриманих результатів полягає у модифікації теоретико-методичних засад і практичних інструментів адаптації системи стратегічного управління підприємством, що ґрунтується на інтеграції механізмів превентивної протидії цифровим ризикам у загальну стратегію його безпеко орієнтованого сталого розвитку, забезпечуючи динамічну стійкість економічної безпеки бізнесу в умовах трансформаційних викликів цифровізації економічного простору. Основні результати, що мають ознаки наукової новизни, є такими:

удосконалено:

- основи тезаурусу адаптивного управління підприємствами завдяки комбінації сутнісних ознак адаптивного менеджменту, стратегічного та безпеко орієнтованого векторів управління, що характеризується авторськими визначеннями понять «адаптація стратегії», «стратегія адаптації» та «адаптована стратегія», що стали теоретико-методичним базисом для концептуалізації адаптації стратегічного управління підприємством під впливом цифровізації, унікальність якого полягає у розробленні алгоритму адаптації стратегії на різних рівнях менеджменту суб’єкта господарювання та із врахуванням непостійності інтересів стейкхолдерів, які змінюються під впливом цифрових трансформацій бізнес-процесів, дотриманні інформаційної прозорості процесу стратегування, який реалізуватиметься із урахуванням принципів цифрового менеджменту, цифрового маркетингу та цифрового ризик-менеджменту, і у результаті якого створюватиметься адаптована стратегія, спрямована на економічну безпеку підприємства у цифровому

економічному просторі та орієнтована на збереження його конкурентного впливу на ринках товарів і послуг;

- методичний інструментарій адаптивної модифікації системи стратегічного управління підприємством шляхом фокусування його на досягненні стану економічної безпеки та протидії цифровим ризикам завдяки використанню матриці інтересів груп стейкхолдерів, яка, на відміну від традиційних матричних структур, ідентифікує ризики для конкурентних перспектив підприємства у випадках, якщо інтереси різних груп стейкхолдерів не будуть досягнуті та збалансовані через використання інструментів гнучкого управління та стейкхолдер-менеджменту;

- практичні інструменти інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств завдяки авторському підходу, що, на відміну від існуючих, передбачає чотири етапи управлінських дій: аналіз зовнішнього середовища; формування та використанні організаційно-управлінського механізму, що інтегрує принципи превентивності, адаптивності, прийняття рішень на основі актуальних даних, балансування інтересів стейкхолдерів, нульової довіри та резильєнтності у безпеко орієнтовану стратегію; реалізація безпеко орієнтованої стратегії підприємства на засадах управління ризиками, проєктного управління, управління на основі актуальних даних, стейкхолдер-менеджменту, забезпечення цифрової безпеки та антикризового менеджменту та досягнення стану цифрового економічного розвитку бізнесу;

- механізм стратегічного управління економічною безпекою підприємства, що відрізняється від існуючих глибокою інтеграцією принципів цифрового ризик-менеджменту в управлінські процеси, обов’язковістю процедури діагностики стану дотримання балансу інтересів основних груп стейкхолдерів і комплексним застосуванням можливостей гнучкого менеджменту на усіх етапах його функціонування, що дозволило адаптувати стратегії безпеко орієнтованого стратегічного управління українськими компаніями до деструктивних впливів цифровізації, ризиків війни, тенденцій BANI-світу,

кадрового голоду, проявів пермакризи та загальноекономічної невизначеності зовнішнього середовища;

дістали подальшого розвитку:

- класичні судження термінополя стратегічного менеджменту та їх змістові трансформації у сучасній науці управління шляхом авторських дефініцій таких понять, як економічна безпека підприємства, стратегічне управління, управління ризиками, стратегія, безпекова стратегія, інформаційна безпека, бізнес-процеси, що, на відміну від класичних термінів, містять сутнісні трактування, адаптовані під впливом цифровізації та цифрових ризиків на теоретико-методичні засади менеджменту організацій, і завдяки використанню яких у процесах розробки стратегій функціонування та розвитку бізнесу, їх орієнтири стають релевантними та зрозумілими для більшості стейкхолдерів;

- методичні підходи до розробки безпеко орієнтованих і цифрових стратегій для вітчизняних підприємств, особливістю яких стало використання зарубіжного досвіду застосування стратегій «кольорових океанів», поєднання модифікацій методів стратегічного аналізу з методами BSC та Hoshin Kanri та застосування інструментів стейкхолдер-менеджменту, таких як матриця інтересів стейкхолдерів, матриця Менделоу, інтегральний індекс впливу стейкхолдерів на стратегічні орієнтири бізнесу;

- академічні парадигми та концептуальні засади стратегічного менеджменту організацій завдяки теоретико-методичній їх перебудові за принципами адаптивності та гнучкості, що на відміну від класичних концептуальних засад стратеготворення, дозволяє підприємству оперативно реагувати на цифрові ризики та змінювати стратегічні орієнтири для того, аби демонструвати власну резильєнтність під тиском пермакризи у реаліях світу BANI, у тому числі завдяки відмови від практики контролю реалізації стратегії на завершальному етапі її використання, та інтеграції процесів контролю і моніторингу у кожен стратегічний етап діяльності підприємства;

- основи розроблення цифрових безпеко орієнтованих стратегій українських підприємств завдяки націленню їх на попередження та протидію

негативному впливу на стан економічної безпеки суб'єкта господарювання таких цифрових ризиків, як кібернетичні та технологічні ризики використання цифрових і інформаційних технологій, таргетовані атаки на цифрові екосистеми суб'єктів господарювання, кібершпигунтство, втрата цифрових даних і доступу до них, деградація хмарних сервісів, цифрова міграція, фішинг, цифрове інсайдерство, низький рівень цифрової грамотності та цифрових компетенцій; та використанню Win-Win стратегій, таких як «Цифровий капітал і потенціал працівника», «Гейміфікація цифрової безпеки», «Технологічний апгрейд бізнес-процесів», «Гнучке управління через довіру і людиноцентризм» «Цифрова ергономіка та безпека праці» для заохочення працівників до цифрового професійного розвитку та безпеко орієнтованої поведінки;

- практики інформаційного забезпечення прийняття безпеко орієнтованих управлінських рішень завдяки використанню результатів SWOT і STEEPLE-аналізів для діагностики стану традиційних механізмів стратегічного управління економічною безпекою підприємств, що дозволили сформувати чотири сценарії адаптації безпеко орієнтованого менеджменту до соціальних, технологічних, економічних, екологічних, політичних, юридичних і етичних чинників функціонування сучасного бізнесу, такі як: адаптація сильних сторін до можливостей (SO-адаптована стратегія), адаптація сильних сторін до загроз (ST-адаптована стратегія), адаптація слабких сторін до можливостей (WO-адаптована стратегія), адаптація слабких сторін до загроз (WT-адаптована стратегія), та конкретизувати їх цільові орієнтири для сталого розвитку суб'єктів господарювання в умовах невизначеності та ризиків.

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій, що виносяться на захист. Обґрунтованість отриманих результатів і репрезентативність висновків базуються на фундаментальному аналізі актуальної нормативно-правової бази, вітчизняного й закордонного наукового доробку, а також масивів статистичних даних. Реалізація мети дисертації підтверджується високим рівнем апробації результатів, представлених у фахових виданнях та під час дискусій на наукових заходах.

Застосування комплексного методологічного інструментарію дозволило забезпечити високу практичну значущість і достовірність сформованих у роботі положень.

Практичне значення отриманих результатів полягає у можливості імплементації розроблених методичних підходів та прикладних рекомендацій у діяльність вітчизняних підприємств для побудови адаптивних стратегій їх безпеко орієнтованого розвитку, здатних ефективно нівелювати вплив цифрових ризиків на стан їх економічної безпеки. Сформульовані в роботі висновки можуть бути використані менеджментом українських суб'єктів господарювання для модернізації систем стратегічного контролю, оптимізації власних бізнес-моделей в умовах цифрової трансформації та підвищення загальної стійкості до негативних впливів цифрових загроз на сталість корпоративних ресурсів. Зокрема, ПП «Мак Тревел» успішно використано можливості командної роботи персоналу під час встановлення стратегічних орієнтирів для масштабування впливу підприємства на ринку, а також внесено зміни до алгоритмів безпеки орієнтованої поведінки працівників, у тому числі у цифровому просторі. Керівництвом компанії підкреслено інформаційну цінність проведеного дослідження у контексті розроблення win-win стратегій для підприємства у площинах взаємодії з постачальниками, клієнтами контрагентами та органами державної влади (Довідка № 1054 від 02.04.2026 р.). Пропозиції автора щодо картографування актуальних ризиків, встановлення стратегічних цілей із використанням технології Smart дозволили суттєво підвищити якість процесу стратегічного планування фінансово-господарської діяльності ТОВ «Техвантаж-Сервіс». Особливо цінними на прикладному рівні виявилися пропозиції щодо підвищення рівня економічної безпеки підприємства за допомогою мультисценарного планування ключових індикаторів його розвитку (Довідка №52 від 27.03.2026 р.). Менеджментом ТОВ «Авіа-Сервіс» було ініційовано заходи щодо оцінювання та підвищення рівня цифрової грамотності управлінського персоналу, а також проведено інформаційну роботу у напрямку важливості започаткування резильєнтних

сценаріїв реагування топ-менеджменту підприємства на форс-мажорні виклики для стану його економічної безпеки (Довідка № 287 від 03.04.2026 р.).

Наукові та методичні результати проведеного дослідження було використано у освітньому процесі Черкаського національного університету імені Богдана Хмельницького під час розробки інформаційних пакетів дисциплін «Стратегічний менеджмент», «Стратегічне та інноваційне управління розвитком організації», «Проєктний менеджмент» для студентів спеціальності 073 (D3) «Менеджмент» освітніх ступенів бакалавра та магістра та у процесі їх викладання (Довідка № 79/04 від 25.03.2026 р.).

Особистий внесок здобувача. Дисертаційне дослідження є самостійною науковою розробкою, у якій оновлено та доповнено теоретико-методичні засади і надано практичні рекомендації для адаптації системи стратегічного управління підприємствами шляхом інтеграції механізмів протидії цифровим ризикам у загальну стратегію його розвитку. Усі наукові результати, висновки та практичні рекомендації, що представлені у роботі, сформульовані автором одноосібно. У наукових працях, опублікованих у співавторстві, особистий внесок здобувача деталізовано та наведено у переліку публікацій, що міститься у матеріалах дисертації.

Апробація матеріалів дисертації. Авторські ідеї, висновки та рекомендації теоретичного та прикладного характеру були презентовані та апробовані у наукових дискусіях на міжнародних та всеукраїнських науково-практичних конференціях: III Міжнародній науково-практичній конференції «Сучасний стан та тенденції розвитку науки та освіти» (м. Дніпро, 5 січня 2026 р.)., Міжнародній науково-практичній конференції «Актуальні проблеми економіки, обліку, управління і права в сучасних умовах»: збірник тез доповідей (м. Рівне, 8 січня 2026 р.), XVII Міжнародній науково-практичній конференції «Пріоритетні напрями досліджень в науковій та освітній діяльності» (м. Львів, 9-10 січня 2026 року), Міжнародній науково-практичній конференції «Сучасні наукові підходи до вирішення глобальних криз: роль

інтеграції наук і технологій у змінах суспільства» (м. Кременчук, 13 лютого 2026 р.).

Публікації. Основні положення та результати дисертаційного дослідження опубліковані у 8 наукових працях загальним обсягом 4,4 др. арк., з них: 4 статті у фахових виданнях України категорії Б (3,35 др. арк., у т.ч. 3,02 др. арк. належать особисто автору) та 4 матеріалах і тезах доповідей на міжнародних науково-практичних конференціях (1,05 др. арк.).

Структура та обсяг дисертації. Дисертація складається з вступу, трьох розділів, дев’яти підрозділів, висновків, списку використаних джерел і додатків. Дисертаційна робота викладена на 254 сторінках. Обсяг основного тексту становить 207 сторінок, 6 додатків займають 13 сторінок, список використаних джерел налічує 300 найменувань. Матеріали дисертації містять 16 таблиць і 25 рисунків, з яких 16 – займають усю площу сторінки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ БЕЗПЕКО ОРІЄНТОВАНОГО СТРАТЕГІЧНОГО УПРАВЛІННЯ ПІДПРИЄМСТВАМИ ПІД ВПЛИВОМ ЦИФРОВИХ РИЗИКІВ

1.1. Логічний аналіз теоретичних основ стратегічного управління у теорії менеджменту діяльності підприємств

У системі менеджменту організації стратегічне управління займає найвищий рівень її архітектури. Саме в його площині формуються візії майбутнього розвитку бізнесу, його цільові орієнтири, формалізується місія його існування та функціонування, а також приймаються управлінські рішення, спрямовані на використання наявних корпоративних ресурсів задля досягнення бажаного економічного, фінансового, соціального стану підприємницької структури у майбутньому. З огляду на це, у ієрархічному контексті стратегічний менеджмент та виконання його фундаментальних завдань на прикладному рівні є прерогативою вищого керівництва організації.

У класичних парадигмах менеджменту стратегічне управління здійснювалося на основі планів фінансово-господарської діяльності суб’єкта господарювання на 5-10 років. Однак, реалії сьогодення змінили це, що викликало необхідність адаптації культури стратегічного менеджменту до нових реалій.

Стратегія організації зазвичай охоплює усі вектори її функціональних сфер, ґрунтується на наявних ресурсах та враховує ризики, які на неї впливають у конкретний момент часу та прогнозується в майбутньому. Взаємозв’язок між стратегічним управлінням і функціональними підсистемами менеджменту організації можна сформулювати таким чином: маркетингова діяльність у межах стратегічного управління визначає, на яких ринках у майбутньому підприємство реалізовуватиме свою продукцію, купуватиме сировину та замовлятиме матеріали; фінансовий менеджмент націлений на розподіл

ресурсів для досягнення стратегічних пріоритетів розвитку бізнесу; HR-менеджмент створює кадровий потенціал та інтелектуальний капітал, необхідні для реалізації стратегії діяльності суб'єкта господарювання, тощо. У межах підсистеми інноваційного менеджменту відбувається запровадження нових технологій для набуття стратегічних конкурентних переваг, проводяться розробки інноваційних рішень для наближення бажаного майбутнього стану підприємства або стабілізації його фінансово-господарської діяльності на середньостроковому та довгостроковому часових горизонтах. Комунікативний менеджмент транслює візію, місію та стратегію підприємства у його економічне оточення, робить її зрозумілою для широкого кола стейкхолдерів бізнесу. Окрім цього, у зовнішньому середовищі функціонування підприємницької структури, система стратегічного управління виконує функцію адаптивного фільтра, яка полягає у перманентному скануванні стану навколишнього простору суб'єкта господарювання з метою своєчасного виявлення у ньому загроз і ризиків, у відповідності до яких послідовно та поступально буде внесено зміни до стратегії його діяльності і розвитку. Таким чином, простежується взаємозв'язок стратегічного управління з ризик-менеджментом компанії.

Виконуючи завдання управління бізнес-структурою, націленою на отримання прибутку чи досягнення іншого економічного ефекту, його менеджери, зазвичай, прагнуть до раціональності, до обрання найкращого управлінського рішення (у тому числі і при встановлення стратегічних цілей). Проте, в умовах ринкової та поведінкової економіки, яка в Україні опинилась ще і у фреймовку воєнної моделі, вони мають обмежені можливості для пошуку, ідентифікації, знаходження, обробки та використання актуальної та достовірної інформації (у тому числі її правильної інтерпретації), а також для обрання найбільш раціонального управлінського рішення у тих чи інших господарських обставинах. Стратегічне управління підприємствами у формі директив і встановлення чітких критеріїв прийняття рішень може підвищити їх якість і поліпшити послідовність виконання, однак, потребує механізмів

гнучкого планування та перебудови сценаріїв у випадку прояву нових факторів зовнішнього або внутрішнього середовища [1].

Логічний аналіз взаємозв'язків стратегічного управління з іншими складовими системи менеджменту організації предметно досліджував видатний західний учений М. Е. Портер. У своїх публікаціях [2-6], які є відомими та цитованими в усьому світі, він достатньо глибоко обґрунтував моделі репрезентації та наукового розуміння стратегічного управління й формалізував аргументацію і логіку прийняття управлінських рішень. Для глибшого розуміння філософії ідейних концепцій стратегічного менеджменту корисними напрацювання вітчизняних учених Л. В. Губерського, І. Ф. Надольного, В. П. Андрущенка [7]. Українські методологи Д. М. Стеченко та О. С. Чмир здійснили вагомий внесок у вивчення логіки нелінійного дослідження [8], що є надзвичайно цінним для вироблення механізмів стратегічного менеджменту на прикладному рівні. Цінними для розуміння специфіки логічного аналізу стратегічного управління є праці вітчизняного ученого В. Я. Малиновського [9].

Особливості стратегічного менеджменту у концепції сучасного управління організаціями вивчають такі українські дослідники, як Балан В. Г. (вивчає методи нечіткого багатокритерійного аналізу у формуванні нової парадигми стратегічного управління підприємствами) [10], Бірбіренко С. С. (фокусується на методологічних аспектах формування концепції стратегічного управління економічною стійкістю суб'єктів господарювання) [11], Зачосова Н. В., Чакалов Р. К. (описують методологію досліджень проблем менеджменту у контексті стратегічного управління економічною безпекою підприємств) [12], Кащена Н. Б., Остапенко Р. М., Чміль Г. Л. (конкретизують організаційно-методичний аспект стратегічного аналізу в управлінні діяльністю підприємницьких структур) [13], Кондратенко Н. О., Новікова М. М., Волкова М. В., Швед А. Б. (формалізують теоретико-методичні аспекти управління стратегічним розвитком промислових підприємств України) [14], Оболенцева Л. В., Вороніна О. О. (узагальнюють теоретико-методичні аспекти

стратегічного управління підприємствами туристичної індустрії) [15], Польова О. Л., Бігун В. С., Савицький О. А. (доповнюють методичні підходи розробки економічної стратегії управління підприємством) [16], Самойленко В. В. (дає оцінку методів стратегічного управління бізнес-процесами підприємства в період цифровізації) [17], Сидорчук А. О. (визначає теоретико-методологічні засади стратегічного управління підприємствами залізничного транспорту в кризових умовах) [18], Янгулов Е. П. (надає теоретичне обґрунтування методологічних основ моделі стратегічного управління для малих підприємств) [19], та інші. Зауважимо, що більшість методів логічного аналізу стратегічного управління в організації представлені у публікаціях науковців вигляді схем. Вони дозволяють узагальнено ідентифікувати, класифікувати й зрозуміти принципові фактори, що мають стосунок до стратегічних управлінських рішень в організаціях. Схематична візуалізація є цінним інструментом передачі інформації щодо логіки стратегічного управління. Вони допомагають розібратися топ-менеджменту та виконавчому персоналу зі складними стратегічними управлінськими рішеннями та їх методологічним підґрунтям [1].

Проблема оптимізації управлінських рішень у організації набагато складніша від індивідуального вибору конкретного рішення менеджером, оскільки неможливо передбачити всі його наслідки у взаємозв’язку з різними функціональними цілями організації. В цій ситуації логічний аналіз стратегічного управління може сприяти спрощенню прийняття середньострокових і довгострокових рішень, обмежуючи діапазон їх альтернатив, що беруться до уваги за реалістичним, оптимістичним і песимістичним сценаріями розвитку подій. Науковий підхід до реалізації стратегічного менеджменту прискорює пошук ефективного управлінського рішення.

Вивчення можливостей логічного аналізу стратегічного управління, завдяки якому може здійснюватися професійна підготовка фактологічної дослідницької бази для спрямованого довгострокового управлінського впливу

на фінансово-господарський стан організації (компанії, підприємства), прийняття управлінських рішень з ціллю досягнення заданих властивостей, змін і станів, становить мету досліджень багатьох сучасних вчених [1]. Водночас, важко виокремити саме теоретико-методологічну складову їх наукових пошуків, оскільки усі вони спрямовані на спроби вирішити конкретну управлінську проблему, яка так і інакше пов'язана зі стратегічним менеджментом і його інструментарієм.

На теоретико-методичному рівні будь-яка проблема по своїй суті є суб'єктивною формою вираження необхідності розвитку існуючого знання, яка відображає суперечність між знанням і дійсністю або протиріччя в самому пізнанні; вона є одночасно засобом і методом пошуку нових знань [7, с. 264]. Логічна експертиза процесів стратегічного управління є одним із провідних способів діагностики проблем організації. Специфічною рисою логічного аналізу є оцінка подій з точки зору несуперечливості й логічної цілісності засобів опису, що відображають відповідні дії. Таким чином, логічний аналіз доцільно проводити щодо засобів вираження подій, фактів, текстів стратегій і стратегічних програм підприємств, проєктів і дій шляхом обґрунтування послідовності й аргументованості висновків, що формалізуються у результаті такого аналізу [1].

У окремих випадках найкорисніше, що можна зробити за допомогою аналізу, – одержати інформаційну допомогу в той момент, коли менеджери підприємства безпосередньо беруться до вирішення стратегічної проблеми. Якщо в них є алгоритм або схема структурування зібраної інформації, то вони опиняються в більш вигідному становищі, ніж менеджери, яким доводиться покладатися лише на власний досвід та інтуїцію. Аналітичні схеми та протоколи дій допомагають розвинути управлінську гнучкість у площинах стратегічного планування, організації, реалізації рішень і контролю їх виконання.

У межах методології та організації наукових досліджень, аналіз визначається як процес поділу в думці або фактично предмету на складові

частини (сторони, ознаки, властивості, відношення) з метою всебічного вивчення цих частин і предмета як цілого [7, с. 270]. Основними структурними одиницями логічного аналізу є поняття, судження, висновки [1].

На рівні «понять» закладається повнота й точність їх визначення, їх ідентичність первинно закладеному концептуальному змісту в межах усього документа (стратегії підприємства), що оцінюється, та стратегічних управлінських рішень, які приймаються. Основним завданням, що лежить у площині логічного аналізу на цьому рівні менеджменту, є досягнення оптимального співвідношення між змістом і обсягом понять, які використовуються в судженнях про фінансово-господарську діяльності підприємства та його економічне майбутнє.

На рівні «судження» здійснюється оцінка відповідності предикатів сутності поняття щодо якого вони встановлюються та властивості якого вони відображають. У ході визначення властивостей і ознак процесів, що досліджуються, доцільно дотримуватися правил, у відповідності з якими виокремлені властивості та ознаки не суперечать одна одній, диференціюються чітко за спільною підставою й відповідають сутності досліджуваного процесу [1].

Традиційні (класичні) судження щодо стратегічного управління підприємствами концептуально сформувалися переважно у другій половині XX століття в межах наукових шкіл планування, дизайну та позиціонування процесу правління організаціями. Вони ґрунтуються на уявленні про ринок як про відносно стабільне соціально-економічне середовище, де головною метою є досягнення підприємством стійкої конкурентної переваги на поточний момент часу та її масштабування у майбутньому.

Рис. 1.1 узагальнює класичні (традиційні) судження щодо стратегічного менеджменту та їх змістові трансформації у сучасній науці управління. Помітним є просування ідей стратеготворення від жорсткої формалізації та плановості до гнучкості та маневреності управлінських дій, націлених на миттєве реагування на нові загрози та ризики.

Рисунок 1.1. – Класичні судження щодо стратегічного менеджменту та їх змістові трансформації у сучасній науці управління

Джерело: складено автором

На основі знання типів співвідношення між судженнями визначається логічна структура відомостей про об'єкт (організацію), рівень спільності та сумісності між основними складовими його опису.

Зміст судження визначається кількістю ознак або дій (предикатів), властивих для суб'єкта відповідного судження, а також способом зв'язку між цими предикатами. Наприклад, в судженні «стратегія має як теоретичну спрямованість, так і практичне значення» щодо одного суб'єкта (стратегії) «прив'язано» два предикати (теоретична спрямованість і практичне значення). Змістовий зв'язок, що виражає перелік ознак об'єкта, який досліджується, – суб'єкта судження, які доповнюють одна іншу, – є кон'юнкцією [1].

Отже, стратегія є детальним і всеохоплюючим довгостроковим курсом розвитку організації, спрямованим на перспективу з метою реалізації місії (основного призначення) організації та цілей, що її конкретизують [9, с. 202].

Наприклад, на думку західного дослідника М. Портера, сутність стратегії полягає у визначенні того, чого саме не потрібно робити, в мотивованій відмові від переваги в конкурентній боротьбі [6, с. 61-78].

Якщо організація не дотримуватиметься прийнятої стратегії, то «застряне посередині», тобто не матиме конкурентної переваги, і буде приреченою на результати, що нижчі середнього рівня. Так, М. Портер наводить приклад із галузі кораблебудування, зазначаючи: «Верфі Іспанії та Британії перебувають у занепаді тому, що вони мають більші витрати, ніж Корея, у них відсутня основа для диверсифікації, властива Японії, і їм не вдалося виявити особливі сегменти ринку, де вони могли б досягнути конкурентної переваги, як Фінляндія (криголами)» [5, с. 40].

З концепцією стратегії тісно пов'язане явище синтезу, яке означає процес поєднання в єдине ціле складових частин (сторін, ознак, властивостей, відношень) предмета, роз'єднаних у процесі аналізу. Наукові методи аналізу і синтезу діалектично взаємообумовлені та часто використовуються синхронно або послідовно [7, с. 270].

Зв'язок, що виражає альтернативний (взаємовиключний) зміст ознак об'єкта, – є диз'юнкцією [1]. У контексті стратегічного управління це ідеальний інструмент для опису варіативності, сценаріїв та альтернатив під час обрання підприємством стратегічних орієнтирів для руху до бажаного стану. У тому

випадку, якщо в змісті об’єкта виявляється функціональна обумовленість однієї ознаки іншою, то має місце імплікація. У стратегічному управлінні імплікація є основою стратегічного передбачення та побудови причинно-наслідкових зв’язків. У межах цього дослідження імплікація буде використана для пояснення зв’язків між діями менеджменту під час прокладання стратегічних курсів підприємства та очікуваним станом його економічної безпеки.

Таким чином, логічна структура висновків (у нашому випадку – стратегічного рішення) відображає послідовність у виробленні нових знань, узагальнень, що одержуються на базі зібраних фактів. Логічна експертиза документу (стратегії) на стадії висновків має продемонструвати, наскільки аргументованими й достовірними вони є, виходячи з накопичених фактів (аналізу інформації), емпіричних узагальнень (експертних оцінок), а також наскільки доказовими виявляються власне правила логічного висновку, що сприяють одержанню нового знання (адаптації існуючої стратегії до нових умов).

У логіці стратегічного управління виокремлюються два види досліджень: дедуктивні та індуктивні. Логічною підставою дедуктивного методу є аксіома: «Все, що стверджується або заперечується відносно всього класу предметів, стверджується або заперечується і відносно кожного предмету цього класу». Дедуктивний підхід є концентрацією сил на узагальненій оцінці системи й розробці загальних принципів формування організаційної структури об’єкта [7, с. 271]. Індуктивний підхід зорієнтований на одержанні загальних висновків шляхом узагальнення одиничних суджень [1]. У процесі наукових досліджень індуктивний підхід передбачає деталізований опис об’єкта дослідження, інформаційних зв’язків і організаційних відносин, результатом якого має стати відповідний висновок, що необхідно покласти в основу стратегічної цілі перспективної діяльності підприємства, його подальшого розвитку. Індуктивний підхід притаманний спостереженням із не досить відомими об’єктами, з недостатньо дослідженою структурою, зі зв’язками й відносинами, що не устаткувалися [1]. Тому саме його пропонується використовувати в

умовах невизначеності, коли заздалегідь передбачити усі прояви ризиків неможливо. Дедуктивний підхід, у свою чергу, передбачає доведення (доказ), що ґрунтується на наявній інформації, яке базується на дотриманні правил умовиводу відповідного виду та використовується при визначенні стратегічної доцільності розвитку підприємства за більш-менш стабільних умов – наприклад, на традиційних ринках і передбачуваним попитом і обмеженою кількістю конкурентів.

Пошук надійних управлінських рішень супроводжує етап формування умовиводів, що становлять набір посилань, при узагальненні яких здійснюється вибір логічно вивіреного рішення. Дедуктивний та індуктивний варіанти цього вибору виражають два найбільш поширені стилі в проведенні наукового дослідження: стратегії послідовного та поступового пошуку заздалегідь невідомого результату, а також стратегії використання готової методологічної схеми (алгоритму) для пояснення або визначення шляхів, що ведуть до заздалегідь сформульованого результату. Відмінність між цими стратегіями наукового пошуку лежить в основі поділу функції прогнозу на пошуковий та нормативний [1].

Таким чином, володіння менеджментом сучасних компаній основними методами логічного розкладення об’єкта дослідження на окремі частини дає можливість обрати найкращий управлінський сценарій для вирішення ідентифікованої або прогнозованої проблеми у їх діяльності. Гарантією правильності управлінського рішення є цілісність і несуперечливість системи понять, що становлять об’єкт дослідження, баланс між нормативними та ціннісними судженнями в описі об’єкту, а також логічна обґрунтованість прийнятих рішень, яка наближається за власною достовірністю до суворих правил логічного висновку в класичних умовиводах. Методи встановлення причинних зв’язків дозволяють посилити рівень обґрунтованості в умовах ситуаційної невизначеності або раптової зміни умов зовнішнього чи внутрішнього середовища об’єкту.

Рівень успішності стратегії у підприємницькій діяльності вимірюється прибутковістю бізнесу. Застосування інструментів стратегічного управління здатне забезпечити одержання підприємством прибутку у довгостроковій перспективі. Проте, прибуток не може бути ціллю існування стратегії. Цільові орієнтири стратегічного розвитку сучасного бізнесу повинні містити соціальну значущість. Нехтування цим правилом здатне призвести до втрати прибутковості та ділової репутації суб'єкта господарювання [1].

Малиновський В. Я. визначає стратегічне управління як управлінську діяльність, що пов'язана з постановкою цілей і завдань організації та з підтримкою взаємовідносин між нею та навколишнім середовищем, що надає їй можливість оптимально здійснювати поставлені функції, досягати організаційних цілей, відповідає її внутрішнім ресурсним можливостям та дає змогу залишатися сприйнятливою до потреб об'єктів організації й зовнішніх викликів [9, с. 201].

У логічному аналізі традиційних і інноваційних парадигм стратегічного управління немає й не може бути універсального підходу. Щоб досягнути успіху у реалізації стратегії, менеджерам підприємств необхідно постійно вивчати вдалий і провальний досвід у бізнесі, кейси існуючих компаній, що накопичуються в усьому світі. Важливим позитивним результатом використання наукових підходів для оптимізації моделей стратегічного управління суб'єктами господарювання на рівні менеджменту є критичне оцінювання власного досвіду щодо ефективних і помилкових управлінських рішень.

Історію успіху будь-якої підприємницької ініціативи обумовлює вдало розроблена та ефективно реалізована стратегія. Успіх стратегії може бути не вираженим у економічних показниках, а успішні стратегії можуть бути сформульованими не у виглядів планів або документів з чіткою структурою, проте вони завжди логічно аналітично продумані, підкріплені аргументами й послідовно реалізовані на практиці [1].

Якщо під стратегією розуміти формування зв'язків між організацією та зовнішнім середовищем, то організації необхідно мати обґрунтовані цілі та цінності; ресурси, здібності та здатності; структуру та систему, сфокусовані на тенденціях розвитку зовнішнього економічного простору. Безперечно, суб'єкти зовнішнього середовища має економічні, демографічні, соціальні, політичні, технологічні, природні та інші фактори впливу на діяльність організації. Для ініціювання багатьох стратегічних рішень важливими є відносини підприємства з клієнтами, конкурентами, постачальниками та іншими категоріями стейкхолдерів, а мінливість їх інтересів і потреб є фактором впливу на стратегію суб'єкта господарювання.

Завданням логічного аналізу стратегічного управління підприємством є постановка таких питань і пошук відповідей на них:

–яким чином організація повинна використовувати власні корпоративні ресурси в соціально-економічному середовищі, щоб досягнути своїх довгострокових цілей;

–як побудувати організаційну структуру, щоб своєчасно та результативно реалізувати обрану стратегію?

Успіх або невдачу стратегії визначає логічний аналіз її параметрів і необхідних для їх досягнення ресурсів. Найпоширенішим методом стратегічного аналізу є SWOT-аналіз, що поділяє всі фактори, які впливають на стратегію організації, на чотири категорії: сильні сторони; слабкі сторони; можливості; загрози. У процесі аналітичної роботи сильні та слабкі сторони характеризують зовнішнє середовище організації, а можливості й загрози – її внутрішній простір і функціональний стан [1].

Проте, під час логічного аналізу стратегічних потреб у менеджера можуть виникати численні процедурні проблеми, оскільки на практиці достатньо складно однозначно конкретизувати сильні та слабкі сторони бізнесу, а також його можливості й загрози, тим більше, у майбутньому. Наприклад, чи є розміщення основних потужностей компанії у Німеччині сильною стороною її діяльності? З одного боку, німецька афіліація компанії забезпечує їй надійну

репутацію, що ґрунтується на високих технічних характеристиках і стандартах якості продукції. Водночас, Німеччина є країною з високим податковим навантаженням на бізнесу. Зважаючи на це, розташування компанії в Німеччині є її як сильною, так і слабкою стороною її діяльності на довгостроковому часовому горизонті [1].

Можна провести логічний аналіз стратегічного управління підприємством іншим дослідницьким шляхом – через зв'язок між організацією та її зовнішнім середовищем, що може створити умови для стратегічної відповідності її цілей і ресурсів. Щоб стратегія стала успішною, вона повинна відповідати особливостям зовнішнього середовища організації. При цьому важливо розуміти, що в організації має бути сформована та діяти комплексна система стратегічного управління, яка містить такі взаємопов'язані складові, як: цілі та цінності; ресурси, здібності та здатності; організаційна структура та управлінський механізм; функціональні підсистеми, що використовуються для виконання різних управлінських завдань на довгостроковому часовому горизонті.

Економічні невдачі, банкрутства та ліквідації багатьох підприємств були обумовлені саме тим, що підприємницька діяльність, якою вони займалися, не була сумісною із їх внутрішнім чи зовнішнім середовищем – ідеологічно, технічно, ресурсно, тощо.

Повна логічна аналогія щодо організації та реалізації стратегічного управління на практиці не є можливою, оскільки не буває двох цілком однакових сукупностей обставин, у яких функціонує підприємство. Тому аналогією не можна користуватися, не звертаючись до інших видів доказів, наприклад судження про причинну залежність [8, с. 103]. Таким чином, не можна використати стратегію, яка довела свою ефективність для одного підприємства, на іншому, без попереднього аналізу умов, які склалися саме для нього на ринку товарів і послуг та у його внутрішньому середовищі [1].

Вплив зовнішніх умов на стан ресурсів підприємства та перспективи їх використання можна проаналізувати, використавши інструментарій PEST-

аналізу, що дозволяє розмежувати зовнішні фактори за джерелами їх походження на політичні, економічні, соціальні й технологічні фактори. Доцільно також оцінювати силу їх впливу на суб'єкт господарювання, ймовірність настання та інші параметри, що дозволить у підсумку створити їх рейтинг і розподілити ресурси, що використовуватимуться послаблення їх негативного впливу та посилення позитивного ефекту у залежності від реальної важливості для стратегічних цілей компанії.

Висновок про причину існування того чи іншого фактора є логічним міркуванням про зміну поведінки підприємства щодо управління ним. Він може формуватися наступним чином: від причини до наслідку, коли за певних обставин результатом буде відповідне управлінське рішення; від наслідку до причини, коли певний стан суб'єкта господарювання викликаний умовами його функціонування. У першому випадку, коли мова йде про висновок, що формується від причини до наслідку, причина відома заздалегідь (прогнозована, очікувана під час розроблення стратегії) і з неї випливає наслідок. Наприклад: «Нафта подорожчала, отже, підніметься ціна й на бензин». У другому випадку, коли управлінець робить висновок від наслідку до причини, відомим є лише наслідок, а про причину робиться висновок (на рівні здогадки), до прикладу: «У працівників підприємств, де заробітна плата вища, продуктивність праці також вища, ніж на підприємствах, де оплата праці менша. Отже, заробітна плата – причина різниці у продуктивності праці» [8, с. 103].

Якщо систематично й безперервно аналізувати увесь діапазон зовнішніх факторів впливу на досяжність стратегічних орієнтирів суб'єкта господарювання, то такий аналіз буде малоефективним через високі витрати, що створить інформаційне перевантаження на управлінський персонал. Тому передумовою для ефективного аналізу зовнішнього середовища є вміння менеджера-стратега відрізнити життєво важливі для економічного стану підприємства фактори від таких, чинять другорядний вплив на його показники.

Для цього механізм стратегічного аналізу доцільно побудувати на засадах таких правил:

–для того, щоб організація змогла тримати прибуток, вона має створити цінність для покупців. Відповідно, менеджери повинні розуміти інтереси та потреби своїх покупців;

–створюючи додаткову споживчу цінність, підприємство закуповує у постачальників товари й послуги, а тому йому необхідно розуміти своїх постачальників і встановлювати з ними довгострокові ділові та партнерські стосунки;

–здатність забезпечувати прибутковість шляхом створення цінності для споживачів і клієнтів залежить від інтенсивності конкуренції між підприємствами, які перебувають у стані суперництва за одні й ті ж самі ресурси та можливості. Зважаючи на це, менеджмент підприємства має розуміти своїх конкурентів.

Таким чином, основу впливу оточуючого середовища підприємства на його стратегічний успіх і результати фінансово-господарської діяльності формують його відносини з трьома групами стейкхолдерів: клієнтами (споживачами), постачальниками та конкурентами. Один зі стратегічних орієнтирів компанії, відтак – це балансування власних стратегічних рішень з інтересами стейкхолдерів та спроба збалансувати їх інтереси між собою також.

Фактори макрорівня, такі як загальні економічні тенденції, зміни в демографічній структурі, цифровізація, соціальні й політичні тенденції, мають вагоме значення для достовірності результатів логічного аналізу стратегічних позицій та потенціалу підприємства. Ці фактори можуть визначати, з якими саме загрозами та можливостями організація ймовірно зустрінеться у майбутньому. Проте, життєво важливо для бізнесу передбачити, як саме ці фактори зовнішнього середовища вплинуть на її конкурентні позиції та наявні ресурсу.

Наприклад, у світі актуалізувалася загроза глобального потепління. Для більшості галузей і господарюючих суб’єктів у цих галузях вона не становить

стратегічні проблеми. Однак, для виробників автомобілів наслідки глобального потепління у формі податків на пальне та обмеження на спалювання видобувного палива перетворюють глобальне потепління на критичну стратегічну проблему, що потребує вжиття превентивних антикризових заходів. Для того, щоб дослідити стратегічне значення глобального потепління на перспективи власного бізнесу, виробники автомобілів повинні знайти відповіді на такі запитання:

1. Що оберуть споживачі і які їх інтереси: віддати перевагу автомобілям, які економно використовують паливо, чи відмовитись від транспорту, що працює на бензині, на користь електромобілів? Яким буде вплив таких рішень на попит на їх продукцію – за рік, три, п’ять років?

2. Чи замінить громадський транспорт приватні авто й навпаки?

3. Чи з’являться нові виробники електрокарів, чи зросте конкуренція у цьому сегменті?

4. Чи зростуть витрати на дослідження та розробки, що пов’язані з адаптацією автомобілів до протистояння новій екологічній проблемі? [1].

Таким чином, аналітичний підхід до стратегічного управління підприємствами потребує такого рівня організації системи менеджменту, за якого топ-менеджери об’єктивно й раціонально оцінюють можливості суб’єкта господарювання й стан його оточуючого середовища. Їхнім обов’язком є формулювання раціональної стратегії, реалізація якої максимально підвищує шанси бізнесу на успіх, а після цього – поступового та безупинного її застосування на практиці. У великих організаціях цей послідовний аналітичний підхід до створення стратегії, здебільшого, реалізується за допомогою підсистеми стратегічного планування.

Однак, доцільно зазначити, що беззаперечних доказів того, що превентивне стратегічне планування забезпечує фінальний успіх стратегії, немає. Те, яким чином підприємства формують власну стратегію, стало цариною палких дискусій і жвавих суперечок науковців. У їх ході очевидним

виявився той факт, що головна теоретико-методична проблема розробки стратегії полягає у тому, що саме розуміти під процесом її генерації [1].

На практиці у процесах створення й реалізації стратегії поєднуються явища системного планування та випадковості на всіх рівнях управління організацією. Важливість фактора випадковості, порівняно з плануванням, постійно зростає в міру того, як оточуюче середовище стає все більш мінливим і непередбачуваним. Так, підприємства, що існують у відносно стабільному економічному середовищі, можуть планувати власні стратегії з вищим рівнем достовірності.

Суб'єкти господарювання, що функціонують у середовищі невизначеності, щодо якого немає сенсу робити жодні прогнози, можуть сформувати лише загальні стратегічні принципи та директиви, а в цілому – покладатися на те, як складуться зовнішні обставини їх діяльності.

Системи стратегічного планування більшості успішних підприємств поєднують перспективне планування та ситуативне реагування. Наприклад, топ-менеджмент організації встановлює стратегічні орієнтири у формі місії, цілей діяльності та бюджету фінансування корпоративних ресурсів. Однак, у межах встановлених стратегічних планів, керівники функціональних підрозділів мають значну свободу у прийнятті рішень, що дозволяє їм корегувати й адаптувати плани та експериментувати з ними [1].

Швидка адаптація до зміни умов зовнішнього середовища, здебільшого, досягається через хаотичні події і відповідні управлінські реакцій на них. У цих реакціях ефективність адаптації забезпечується через помірні рівні адаптивної напруженості та прості правила, що сприяють координації дій персоналу і стратегії діяльності підприємства. Управління організацією за допомогою зрозумілих директив у поєднанні з потужними мотиваційними спонуканнями до їх реалізації може бути успішним у перспективі.

Однак концепції, теорії та інструменти аналітиків не замінять досвіду, професіоналізму та креативності, притаманних менеджерам. Методична роль логічного аналізу полягає у тому, щоб задавати загальний напрям

управлінських рішень, обробці інформації й обміну думками в організації. Логічний аналіз має сприяти комунікації та досягненню консенсусу між менеджментом, власниками, працівниками та стейкхолдерами. Логічний аналіз повинен стимулювати творчий потенціал та інновації усіх, хто задіяний у стратегічному управлінні підприємством.

Отже, стратегія відіграє роль основоположного принципу діяльності підприємства, що забезпечує взаємоузгодженість управлінських рішень, які приймаються топ-менеджером. Зважаючи на це, стратегія є важливим складником його економічного успіху. Таким чином, дотримання низки логічних правил є необхідною умовою для логічного аналізу реалістичності та ефективності стратегії:

–теза (стратегічний орієнтир) повинна бути логічно визначеною, зрозумілою і точною;

–теза (стратегічний орієнтир) повинна залишатися тотожною самій собі упродовж усього процесу її доведення (досягнення);

–аргументи (управлінські рішення) повинні бути істинними й доведеними;

–аргументи (управлінські рішення) не повинні суперечити один одному;

–аргументи (управлінські рішення) повинні бути достатніми для відповідної тези (досягнення стратегічного орієнтиру).

Ідея логічного аналізу стратегічного управління полягає в тому, щоб систематично аналізувати причини успіху та провалу відповідних управлінських рішень. Отримані інформаційні результати можна використовувати для формулювання нових ділових стратегій. Доцільно удосконалювати процеси стратегічного аналізу й інструменти розроблення стратегії, а також підходи до стратегічне планування діяльності компанії.

Стратегічний аналіз без вивчення досвіду, можливостей виникнення випадковостей й здатності підприємства до самоорганізації і гнучкого реагування на загрози в сучасних умовах господарювання в Україні не є ефективним. Прийняття стратегічних управлінських рішень повинно враховувати інтуїцію менеджера, а застосування обґрунтованого стратегічного

аналізу, у свою чергу, сприяє розвитку інтуїції та креативності управлінського персоналу.

Логічний аналіз не лише спрощує прийняття управлінського рішення, а й підвищує його якість завдяки забезпеченню інформацією. По-перше, він об’єднує знання експертів і аналітиків у єдине ціле. По-друге, він полегшує застосування аналітичних інструментів. Інструменти та алгоритми логічного аналізу діяльності підприємства та оцінки ефективності бізнесу забезпечують достовірність стратегії і закладають основу для більш ефективних управлінських рішень.

Методи логічного аналізу поглиблюють розуміння фундаментальних засад досягнення організацією конкурентної переваги, проблем задоволення потреб клієнтів. Вони поглиблюють розуміння організаційних спроможностей підприємства і основ конкуренції, проте не обмежують запровадження інновацій, гнучкості управління та вміння отримувати економічну вигоду за будь-яких обставин.

Отже, метою логічного аналізу стратегічного управління підприємством є полегшення розуміння менеджментом спірних питань і проблем, які виникають у процесі реалізації стратегії бізнесу (тобто, управління стратегічними проблемами суб’єкта господарювання режимі реального часу) [1].

Таким чином, стратегічне управління підприємством – це сукупність рішень щодо його фінансово-господарської діяльності, які у комплексі мають забезпечити досягнення ним стратегічних орієнтирів і бажаного економічного стану у майбутньому. Невизначеність і ризики ускладнюють цей процес, а тому постає необхідність у його модифікації для адаптації стратегій розвитку бізнесу до реалій пермакризи та тенденцій непередбачуваного та тривожного світу.

1.2. Зміни парадигм стратегічного управління підприємствами під впливом пермакризи та ризиків світу BANI

Теорії стратегічного в менеджменту на мікро та макро рівнях мають тривалу історію фундаменталізації та використання у науково-методичній та прикладній площинах у різних періодах розвитку науки менеджменту та економічної науки в цілому. Водночас, у часи наростання кризових явищ, під час посилення впливу ризиків, формування стійкого та тривалого середовища невизначеності функціонування бізнес-структур, концепції та парадигми стратегічного менеджменту зазнають суттєвих сутнісних трансформацій, оскільки саме цей напрямок управління суб'єктами господарювання стає найбільш непередбачуваним та важко прогнозованим. На відміну від оперативного або тактичного менеджменту, успіх і результативність стратегічного управління тісно пов'язані зі здатністю менеджерів визначати форсайт зміни економічної ситуації, точно розраховувати та оцінювати наявність і можливості розвитку економічного, інтелектуального, фінансового потенціалу підприємства, моделювати різні економічні сценарії у відповідності до поетапних планів досягнення цілей, місії, стратегічних орієнтирів діяльності та масштабування бізнесу. Перманентна криза, ризики світу BANI, який характеризується невизначеністю, нелінійністю, крихкістю та тривожністю, не дають можливості для виконання точних діагностичних процедур, тому топ-менеджмент сучасних компаній не має релевантного інформаційного підґрунтя для своєї діяльності та прийняття довгострокових управлінських рішень, а відтак опиняється у так званій «сірій» зоні, де управлінські реакції мають бути динамічними, адаптивними та своєчасними. З огляду на це, актуальності набуває перегляд класичних парадигм і концептуальних засад стратегічного управління підприємствами в умовах пермакризи та ризиків світу BANI, які є характерними для сучасного етапу розвитку економіки України та світу, і поміж іншого, характеризуються перманентністю, системністю та резистентністю.

Стратегічне управління підприємствами та різними напрямами їх фінансово-господарської діяльності – повноцінна дослідницька тема, яка предметно розкрита у науковій літературі, має сформоване теоретико-методичне підґрунтя. Однак, мінливість світу, його економічних і соціальних законів, реалій, у яких суб'єкти господарювання мають шукати нові шляхи для свого довгострокового виживання та розвитку, актуалізують тематику стратегічного менеджменту у фреймворку, який деякі сучасні вчені пропонують називати світом BANI (Brittle – крихкий, Anxious – тривожний, Non-linear – нелінійний, Incomprehensible – незрозумілий). Ця концепція опису реалій оточуючого нас середовища почала набувати популярності з 2021 року, тому у публікаціях дослідників більш пізніх років огляд парадигмальних засад і концептуальних постулатів стратегічного менеджменту відбувався уже із врахуванням обставин цього світу – свідомо або підсвідомо [20, с.163].

Серед зарубіжних дослідників натепер широко обговорюються проблемні аспекти цифровізації стратегічного управління підприємствами, зокрема стратегічної інтеграції інтелектуального цифрового управління безперервністю бізнесу у систему менеджменту організацій [21], стратегічного прийняття рішень для протидії впливу факторів непередбачених обставин на практику управлінського обліку в цифрових стартапах [22], цифрової трансформації стратегічного управління малими та середніми підприємствами [23], майбутнього стратегічного управління в цифрову епоху розвитку бізнесу [24], стратегічного управління брендами на цифрових ринках [25], цифрової трансформації як стратегічного важіля для гнучкого управління організаціями та процесами [26], цифрових компетенцій, управління людськими ресурсами та культури як стратегічних рушійних сил сталої цифрової трансформації в малих і середніх підприємствах [27], стратегічного управління змінами в епоху цифрових перетворень для забезпечення організаційної адаптивності та інноваційної культури [28], зв'язку транзакційної системи пам'яті команди вищого керівництва, стратегічної гнучкості та інновацій цифрової бізнес-моделі організацій [29], підходів до стратегічного управління для екологічно стійкої

цифрової трансформації [30], аналізу емпіричних даних про роль інформаційних систем бухгалтерського обліку в діяльності зі стратегічного планування, контролю та координації [31], управління інфраструктурою цифрових технологій та стратегічного узгодження бізнесу як факторів розвитку цифрових можливостей підприємств [32], цифрово-сталих бізнес-моделей [33], балансування сталості управління цифровими продуктами з точки зору стратегічного бізнесу [34], організаційної секретності у контексті цифровізації та її негативному впливу на зосередженість керівництва компаній у питаннях стратегічного оновлення підходів до їх діяльності [35], впливу інновацій цифрового маркетингу та стратегічної орієнтації на ефективність діяльності фірми [36], тощо.

Можна виокремити кілька напрямів розвитку наукової думки у площині стратегічного управління у вітчизняній науці – це: особливості стратегічного менеджменту підприємств різних видів економічної діяльності [37], довгострокові акценти та стратегічні орієнтири для різних об’єктів управлінського впливу (до прикладу, Гребенікова О. В., Денисова Т. В. розглядають теоретичні та практичні аспекти стратегічного управління саме інвестиційним потенціалом підприємств [38]), правила та принципи стратегічного менеджменту для суб’єктів господарювання різного розміру та складності організаційної структури [39], підходи до стратгування підприємницької діяльності у кризових умовах [40] та під впливом різного роду ризиків і загроз. Остання зазначена категорія досліджень є особливо популярною останнім часом: так, Семенча І. Є., Гринько Т. В. пропонують підходи до прийняття рішень і побудови стратегій управління із врахуванням ризиків в діяльності сучасного бізнесу в Україні [41], Сазонова С. В. опікується питаннями ідентифікації ризиків стратегічного управління телекомунікаційними підприємствами в умовах цифрової економіки [42], Вербовський І. контекстно вивчає стратегічне управління в умовах ризику та невизначеності [43], Рябуха О. О. описує стратегічне управління розвитком підприємства із урахуванням конкурентних ризикових факторів [44]. Вартими

уваги у процесі цього дослідження є напрацювання Зачосової Н.В. та її співавторів, які фокусуються на стратегії і механізмі управління фінансово-економічною безпекою підприємств в реаліях війни, тенденцій Індустрії 4.0 та світу BANI [45, 46]. Однак, попри ґрунтовні напрацювання сучасних вітчизняних вчених у площині стратегічного управління підприємствами та їх ресурсами в умовах невизначеності та ризиків, розуміння того факту, що їх господарське оточення постійно змінюється, а усталені підходи та практики менеджменту потребують адаптації, породжує необхідність модернізації парадигм розроблення стратегій функціонування та розвитку бізнесу у світі BANI [20].

Таким чином, у теоретико-методичній площині потребують узагальнення, конкретизації та доповнення сучасні підходи до стратегічного управління підприємствами та оновлення парадигм класичного стратегічного менеджменту під впливом пермакризи та цифрових ризиків світу BANI.

Про особливості управління суб'єктами господарювання, трудовими ресурсами та навіть макрорівневими соціально-економічними системами у реаліях світу BANI у 2022 році почали активно писати такі сучасні вчені, як Дуднєва Ю. Е., Долгополов В. О., які предметно розглядають особливості підприємницької діяльності в контексті викликів BANI-світу [47], Захаров Є. В., що проводить порівняльний аналіз підходів до концепцій світу у контексті SPOD (Steady – стійкий/стабільний, Predictable – передбачуваний, Ordinary – простий/звичайний, Definite – визначений), VUCA (Volatility – мінливий, Uncertainty – невизначений, Complexity – складний, Ambiguity – двозначний) та BANI-суспільства [48], Цифра Т. Ю., Моголівець А. А., Вершигора Д. М., які описують цифрові навики економістів-будівельників, що будуть їм критично необхідними в епоху VUCA та BANI-світу [49]. У 2023 році їх напрацювання розвинули та доповнили Бушуєв С., Івко А., Мудра М., Мурованський Г., Пілюгіна К., які конкретизують роль адаптивності в управлінні інноваційними проєктами в середовищі BANI [50] та простежують трансформації цінностей високотехнологічних проєктів від моделі середовища

VUCA до моделі BANI [51], Буняк Н., що узагальнює особливості менеджменту в умовах BANI-світу [52], Зачосова Н. В., Козак В. В., які досліджують стратегічне управління кадровою безпекою підприємства як напрям збереження та розвитку людського капіталу в умовах BANI World та Індустрії 4.0 [53]. У 2024 році Жегус О. В. продовжує вивчати маркетингове управління в забезпеченні резильєнтності бізнесу в умовах BANI-світу [54], Ільїн О. О., Бушуєв С. Д., Гоц В. В., Лященко Т. О. фокусуються на проблемах управління ІТ-проєктами бізнес-аналітики у BANI-оточенні [55], Помаза-Пономаренко А. Л., Батир Ю. Г., Лопатченко І. М. простежують вплив BANI-світу на державне регулювання ринку праці та державну молодіжну політику [56]. У 2025 році дослідження впливу світу BANI на управлінські процеси переходять у площини адаптивності, гнучкості, невизначеності та стратегування. Так, Вареник В., Піскова Ж. проводять тематичні дослідження компаній, що використовують Scrum, акцентуючи увагу наукової громадськості на питаннях Agile-організації в еру BANI [57], Данько Я. П. звертається до проблеми трансформація особистості та VUCA/BANI середовищ в умовах екзистенційної невизначеності [58], що є цінним внеском у теорію управління персоналом під впливом кадрових ризиків, Кифяк В. описує методологію дослідження середовища розвитку бізнесу з метою встановлення стратегічних пріоритетів агробізнесу в умовах BANI-світу [59], Попова Н. В., Муха Т. А. надають пропозиції щодо адаптації SaaS-стратегій (Software as a Service – програмне забезпечення як послуга – авт.) до логістичних викликів VUCA/BANI-середовища в контексті сталого розвитку ланцюгів постачання [60], Савенко О. А. узагальнює теоретичні аспекти формування виробничого менеджменту підприємства в умовах BANI-середовища [61], Чала Т. Г., Юхименко М. С. аналізують виклики вимірювання ділових очікувань і невизначеності бізнесу в умовах трансформації до BANI-світу з позиції статистичного підходу [62]. У той же час, сучасні економісти стверджують, що у 2025 році модель світу BANI поступово почала змінюватись на концепцію TUNA (Turbulent – турбулентний, Uncertain – непевний, нестабільний,

невизначений, Novel – новий, Ambiguous – двозначний) [63, 64]. Також у джерелах відкритих даних зустрічається абревіатура RUPT, зокрема, її використовує The Center for Creative Leadership (Центр креативного лідерства) у США (Rapid – швидкий, Unpredictable – непередбачуваний, Paradoxical – парадоксальний, Tangled – заплутаний) [64]. Найбільш радикальною концепцією світоустрою може вважатись SHIVA-світ. Ця модель згадується в контексті поширення явищ глобальних катастроф і воєнних конфліктів в усьому світі, що характерно для 2025-2026 років. Ця назва має подвійне сутнісне значення – з одного боку вона означає ім'я індуїстського бога руйнування та творення Шиви (Shiva), а з іншого, як і усі описані моделі, є акронімом – Split (розколотий), Horrible (жахливий), Inconceivable (неймовірний), Vicious (зловісний, порочний), Arising (відроджуваний). Експерти стверджують, що ця модель, як і модель світу TACI (Turbulent – турбулентний, Accidental – випадковий, Chaotic – хаотичний, Inimical – ворожий) [65, 66, 67]. Однак, у межах цього дослідження увагу буде зосереджено на стратегічному управлінні підприємствами у світі BANI, оскільки ця парадигма є найбільш поширеною у сучасній науковій літературі, здобула масштабну підтримку у експертному просторі та набула характерних теоретико-методичних засад. Крім того, традиційним для вітчизняної економіки є те, що вона із запізненням реагує на загальносвітові тенденції. Цими аргументами, а також тим, що сучасні реалії, у яких перебуває Україна та підприємницькі структури, які провадять тут фінансово-господарську діяльність, мають усі ознаки BANI-фреймворку, тобто є крихкими, непостійними, непередбачуваними, нелінійними, тривожними та важкопрогнозованими, що пояснюється воєнним станом і тривалою окупацією територій, емоційним і психологічним виснаженням населення, обмеженістю ресурсів, і пояснюється вибір моделі BANI як орієнтиру для адаптації підходів до стратегічного менеджменту суб’єктів господарювання задля надання їм резильєтності, гнучкості, ефективності та життєздатності.

Табл. 1.1 демонструє, чому класичні парадигми стратегічного управління підприємствами втрачають свою ефективність у реаліях світу BANI та потребують адаптації і оновлення:

Таблиця 1.1. – Конкретизація потреби у перегляді та оновленні парадигмальних засад стратегічного управління підприємством у світі BANI

Характеристики класичного стратегічного менеджменту	**Характеристики світу BANI**	**Невідповідність стратегічного менеджменту**	**Напрями адаптації**
Довгострокове планування цільових орієнтирів (понад п’ять років)	Крихкість (Brittle): соціально-економічні системи руйнуються під впливом криз	Довгострокові стратегії стають нераціональними та неактуальними	Запровадження принципів гнучкого та сценарного управління
Передбачуваність майбутнього та стабільність розвитку і середовища функціонування	Тривожність (Anxious): стала невизначеність у зовнішньому та внутрішньому просторі	Неможливість отримати релеватні дані та достовірно спрогнозувати майбутнє	Застосування адаптивного менеджменту та антикризових стратегій
Лінійна причинно-наслідкова логіка прийняття управлінських рішень	Нелінійність (Nonlinear): тактичні рішення мають стратегічні наслідки	Класичні стратегії не враховують турбулентність і невизначеність	Запровадження практик критичного мислення та сценарного аналізу
Раціональність менеджменту, економічність і поінформованість управлінців	Незрозумілість (Incomprehensible): суперечлива інформація з різних джерел, асиметрія даних	Неможливість комплексного аналізу інформації і прийняття ефективних стратегічних рішень	Використання цифрових технологій, інформації з різних джерел та штучного інтелекту як ресурсів
Ієрархічні організаційні структури управління	Швидкі зміни та необхідність реагувати миттєво	Затримки при прийняття рішень, втрата часу	Перехід до децентралізації влади та гнучких структур
Стандартні алгоритми фінансово-господарських процесів	Постійна турбулентність економічного середовища	Регламенти та протоколи дій знижують гнучкість управління	Розвиток цифрового і адаптивного управління бізнес-процесами
Ціль - набуття конкурентних переваг	Неочікувані кризи і поява конкурентів	Ігнорування раптових можливостей	Розвиток екосистем і стратегічних альянсів
Фокус на прибутку і раціональному використанні ресурсів	Важливість соціальної орієнтації менеджменту	Нехтування людським потенціалом і капіталом	Масштабування практик людиноцент-ричного управління
Планування майбутнього на основі ретроспективних даних	Швидка зміна тенденцій, уподобань клієнтів, інтересів споживачів	Безвідносність минулих успіхів із майбутніми здобутками	Використання прогностичної аналітики та технік форсайту

Джерело: складено автором

Отже, сучасні підходи до стратегічного управління підприємствами, які використовуються менеджментом вітчизняних компаній, змушених працювати у реаліях воєнного часу, підкріплені зарубіжним досвідом розроблення стратегій, орієнтованих на вихід підприємств зі стану кризи та на досягнення цілей сталого розвитку, призводять до поступової, але невідворотної зміни парадигм стратегічного менеджменту. У найбільш загальному значенні стратегію можна визначити як сукупність прийомів та цілей щодо досягнення мети у майбутньому. Формулювання конкретних стратегії базується на аналізі поточних та прогнозі бажаних результатів діяльності суб'єкта господарювання. Однак, нині майбутнє характеризується невизначеністю, яка має бути врахована при розробці стратегії розвитку [44]. У класичному розумінні стратегічний менеджмент націлений на досягнення підприємством його бажаного стану у майбутньому. Цей стан може охоплювати, але не обмежуватись, такими параметрами і показниками, як економічний потенціал, конкурентоспроможність, рівень економічної безпеки, ефективність управління підприємством, розвиток бізнесу, ринкова перевага. В умовах пермакризи – явища, яке розуміється як довготривалий у часі період загрози, небезпеки, притаманної для існування певного об'єкту та його нормального функціонування, спровокований послідовними або паралельними (одночасними) критичними та/або катастрофічними подіями (наприклад, світова економічна криза, глобальна пандемія, війна), економічне виживання підприємства залежить від його потенціалу та здатності менеджменту передбачати події, що можуть суттєво впливати на управління розвитком, усвідомлювати та ідентифікувати стратегічні ризики та своєчасно приймати антикризові управлінські рішення [20, с.165].

Кульбицька О.В. виділяє такі підходи до стратегічного управління підприємствами: системний, ситуаційний, процесний, холістичний, функціональний, комплексний, ресурсний [37, с.135]. Оптимальним, на її думку, у контексті стратегічного управління розвитком підприємства, є поєднання системного та процесного підходів у комбінований підхід [37, с.138].

Загалом, помітною рисою сучасного етапу розвитку стратегічного менеджменту у теоретико-методичній площині є поєднання різних підходів, оскільки невизначеність оточуючого середовища вимагає гнучкого та швидкого реагування та зміни управлінських протоколів і алгоритмів у відповідності до нових умов, які виникли на тому чи іншому етапі функціонування підприємства. Тому можна стверджувати, що нині відбувається не лише зміна парадигм стратегічного управління, але і їх синтез, симбіоз і синергія, викликані необхідністю адаптації до стану невизначеності на ринках товарів і послуг та економічної системи в цілому. Варто відзначити, що і у мирний час, у періоди відносної стабільності, формування стратегії та здійснення стратегічного управління можна було вважати одним із ключових джерел адаптації підприємства та формування стійкого та сталого розвитку [37, с.141]. Нині ж, невизначеність організаційно-економічної системи є причиною виникнення безлічі альтернатив реалізації неоднозначних подій або явищ, які можуть призвести до різних (як позитивних, так і негативних) наслідків, що супроводжуються недостатністю інформації та відсутністю детермінованості розвитку [44], і це призводить до того, що стратегія, аби залишитись інструментом адаптації, повинна сама мати здатність бути адаптованою до нових моделей і практик ведення економічних відносин. Наприклад, стратегії сучасних підприємств потребують адаптації до їх функціонування під впливом цифровізації та із урахуванням постійного масштабування меж цифрових трансформацій виробничих, фінансових, управлінських і інших бізнес-процесів.

Гребенікова О. В., Денисова Т. В. вважають, що стратегічне управління доцільно проводити на основі таких принципів: системний підхід, гнучкість та адаптивність, довгострокова орієнтація, збалансованість ризиків і доходності, інноваційність, ресурсоефективність, інституційна підтримка, соціальна відповідальність [38, с.71-72]. До цього переліку варто додати привентивність – як здатність запобігати системним і стратегічним ризиками або посиленню негативних проявів світу BANI та пермакризи, цілеспрямованості та

узгодженості стратегії з місією та цілями підприємства, а також принцип комплексності, який у межах цього дослідження означає, що генеральна стратегія компанії має охоплювати усі інші її стратегії для того, аби уникнути суперечностей та забезпечити наявність стратегічного бачення подальшого розвитку суб'єкта господарювання в усіх напрямах його діяльності.

Отже, стратегій у одного підприємства може бути кілька, і така «мультистратегічність» також є класичною ознакою традиційних парадигм сучасного менеджменту організацій. Янгулов Е.П. поділяє усі види стратегій на функціональні (маркетингова стратегія, стратегія науково-дослідних і проектно-конструкторських розробок, виробнича стратегія, фінансова стратегія, стратегія управління персоналом, логістична стратегія, стратегія зовнішньоекономічної діяльності), операційні (стратегія технічного обслуговування й ремонту машин і устаткування, стратегія заміни зношених машин, механізмів, устаткування, стратегія оновлення техніко- технологічної бази, стратегія закупок матеріальних цінностей, тощо), загальні (стратегія зростання, стратегія підтримки, стратегія реструктуризації, стратегія скорочення (згортання) діяльності, стратегія санації) та загальні конкурентні (стратегія лідерства за витратами, стратегія широкої диференціації, стратегія оптимальних витрат, стратегія, сфокусована на низьких витратах, сфокусована стратегія диференціації) [39, с.131]. У пропонованій вище класифікації відсутні актуальні натепер стратегії резильєнтності, метою яких є довгострокова життєстійкість і стратегічна активність підприємства, стратегії релокації і відновлення клієнтської бази після територіального переміщення, стратегії збереження кадрового потенціалу та людського капіталу, стратегії «зайнятості без кордонів», тобто таких форматів стратегічного людиноцентрованого менеджменту, що націлений на збереження талантів і утримання ключових фахівців на посадах безвідносно до їх фактичного місця перебування, адже основне в умовах тотальної небезпеки для життя та здоров'я працівників вітчизняних підприємств, що перебувають під постійними обстрілами, – щоб їх

інтелектуальний капітал слугував меті досягнення стратегічних орієнтирів компанії, не залежно від географічних зон чи часових поясів.

Традиційна модель розробки стратегії засновується на факті, що майбутнє передбачуване [44]. Однак, у світі BANI та з огляду на реалії сьогодення – це твердження далеке від істини. Зважаючи на інтенсифікацію та поширення кризових явищ на теренах України, Сидорчук А.О. пропонує виокремлювати та розвивати антикризові стратегії управління підприємствами, які спрямовані на покращення фінансової стабільності, оперативної ефективності, а також дозволяють підвищити адаптивність компанії до мінливого стану ринку в умовах лібералізації галузі [40]. Що до управління ризиками у діяльності підприємств, то Семенча І. Є., Гринько Т. В. у залежності від коректного набору факторів пропонують обрати управлінському персоналу або стратегію уникнення ризику, або стратегію зниження/мінімізації ризику, або стратегію передачі/транферу ризику, або стратегію прийняття ризику [41, с.99]. Окремої стратегії управління потребують стратегічні ризики, які виникають на різних етапах досягнення підприємством довгострокових орієнтирів власної діяльності.

Тенденції цифрової економіки, поєднуючись із реаліями світу BANI, формують новий простір для виникнення ризиків, які мають враховуватись у оновлених стратегіях функціонування та розвитку підприємств. Цифровізація та цифрові трансформації спровокували появу таких ризиків, як ризики, пов’язані із застосуванням хмарних технологій і розподільних обчислень, розмивання відповідальності за інформаційну безпеку та зниження рівня контролю; невизначеність правового регулювання цифрових взаємовідносин; ризик кібербезпеки [42, с.9]. Відтак, на окрему увагу заслуговує практика сьогодення, пов’язана з розробкою окремих стратегій цифровізації та створення цілих цифрових екосистем функціонування бізнесу, і механізми ризико орієнтованого менеджменту цифрових підприємницьких екосистем.

Вербовський І.В. наголошує, що саме під час періоду невизначеності перспектив суб’єктів господарювання та за умови поширення кризових явищ,

набуття ними ознак пермакризи, найбільш яскраво виявляються потенційні та реальні можливості менеджменту зосереджуватися на оптимальних діях і виробітку чітких й ефективних рішень із плануванням не тільки в напрямку стратегії виживання, але й стабілізації та зростання [43]. Варто пам'ятати, що часи економічної нестабільності призводять не лише до скорочення підприємницької діяльності, соціальної напруги та зміни очікувань, але і стають джерелом і майданчиком для нових креативних ідей, стартапів, якісних трансформацій; сприяють виживанню найсильніших учасників економічних відносин, здатних якнайкраще задовольнити інтереси та потреби клієнтів. «Бачити майбутнє», попри «білий шум» численних ризиків і загроз мінливого світу – це справжнє управлінське мистецтво, талант, яким мають володіти менеджери та стратеги сучасного успішного та резильєнтного бізнесу [20, с.166].

Під час використання проєктного підходу у стратегічному менеджменті організацій, розроблення проєктів для стратегічного управління має розпочинатися із визначення цілей бізнесу, якому передують такі управлінські процеси, як вивчення внутрішнього та зовнішнього середовища діяльності підприємства, виявлення можливостей та наявних ресурсів для ведення бізнесу у поточний момент часу та у перспективі, враховуючи потенційні можливості його зростання, формування маркетингових стратегій, прогнозування майбутніх шляхів досягнення орієнтовних цілей, створення інформаційних систем і баз даних, критичне оцінювання потенціалу цифровізації бізнес-процесів і розширення клієнтської бази [43]. У реаліях світу BANI проєктний підхід є одним із оптимальних способів забезпечити гнучке реагування та оптимально швидку зміну цілей підприємства за умови виникнення нових обставин його зовнішнього та внутрішнього середовищ. Традиційні ж парадигми стратегічного менеджменту мали в основі ідеологію необхідності досягнення задовго та завчасно визначених планових показників, без можливості їх зміни, з обов'язковим поясненням з боку менеджменту

власникам бізнесу відхилень і причин недосяжності поставленої мети [20, с.166].

Серед факторів, які можуть бути суттєвими для менеджменту підприємницької діяльності в періоди невизначеності та хаосу, варто враховувати й ті, вплив яких на реалізацію заходів стратегічного управління вважається критично важливим. Це може стосуватися, зокрема, нестачі фінансових ресурсів у бізнес-середовищі, недостатньої кваліфікації працівників, суттєвого зменшення споживчого попиту населення через наявні та потенційні небезпечні умови життя та праці, зниження купівельної спроможності потенційних споживачів товарів і послуг [43]. Усі перераховані фактори є притаманними для ведення бізнесу в Україні останні 10-15 років. Однак, оптимальним періодом для розробки стратегії в умовах невизначеності та ризику може бути інтервал у 5 років, оскільки планувати орієнтири для діяльності та розвитку на період 10-20 років українські компанії можуть лише дуже наближено. Наведений факт також є характеристикою зміни парадигм стратегічного менеджменту – його основна відмінна риса – довгостроковість – стає усе більш розмитою, оскільки сучасний світ починає «жити» короткими інтервалами (у проєктному менеджменті використовується спеціальний термін – спринт – який означає певний етап роботи, який швидко закінчується, але обов'язково має певний конкретний результат, що дає змогу оцінити його результативність і ефективність витрат ресурсів). По аналогії з проєктним менеджментом, можна говорити про ймовірність розвитку спринтерних або спринтерських стратегій, націлених на короткострокові результати, які дають можливість у підсумку досягнути масштабної цілі генеральної стратегії бізнесу [20, с.167]. Отже, в умовах BANI-світу орієнтири стратегічного управління мають переглядатися частіше; управлінцями має опрацьовуватися більша кількість сценаріїв ймовірного розвитку подій, ніж класичні; вітається максимальна залученість усіх категорій працівників до процесу ідентифікації ризиків [46, с.61]. Такий командний підхід до стратегічного менеджменту

дозволяє вчасно ідентифікувати ризики, які можуть бути непомітні вищому керівництву компанії, але очевидні виконавцям на місцях.

Розвиток потенціалу, і у першу чергу, економічного потенціалу підприємства, як стратегічна мета бізнесу, позитивно позначається на можливостях управління ризиками [44], а також посилює стан його економічної безпеки, яка також має бути одним із цільових орієнтирів розвитку суб'єкта господарювання у кризовому середовищі світу BANI [45].

Тому характеристиками сучасних стратегій має неодмінно стати розділ або окремий функціональний напрям, що буде присвячений пошуку нових можливостей для бізнесу. Раніше це були окремі стратегії розвитку, і розроблялись вони лише за потреби. Нині – це стратегії трансформації, адаптації, видозміни, без яких бізнес, що не бажає масштабуватись, але прагне вижити, не зможе цього зробити, так само, як і гарантувати принаймні мінімальний рівень власної економічної безпеки, необхідної для підтримання ліквідності, платоспроможності, фінансової стійкості, здатності погашати поточні зобов'язання та звертатись за додатковим фінансуванням до різних джерел, таких як грантодавці або інвестори. Економічна безпека в умовах невизначеності – це уже ознака ефективного стратегічного та антикризового менеджменту, хоча у сучасній Україні ці два напрями управлінської діяльності усе частіше інтегруються в один. Поєднання парадигм стратегічного, антикризового, безпеко орієнтованого та ризик-менеджменту є унікальною характеристикою поточного етапу розвитку науки управління та практики менеджменту організацій [20, с.167].

Рис. 1.2 узагальнює еволюцію теорій стратегічного менеджменту та зміни парадигм стратегічного управління підприємствами під впливом пермакризи та ризиків світу BANI аж до їх сучасного стану, оновленого із врахуванням реалій воєнного часу.

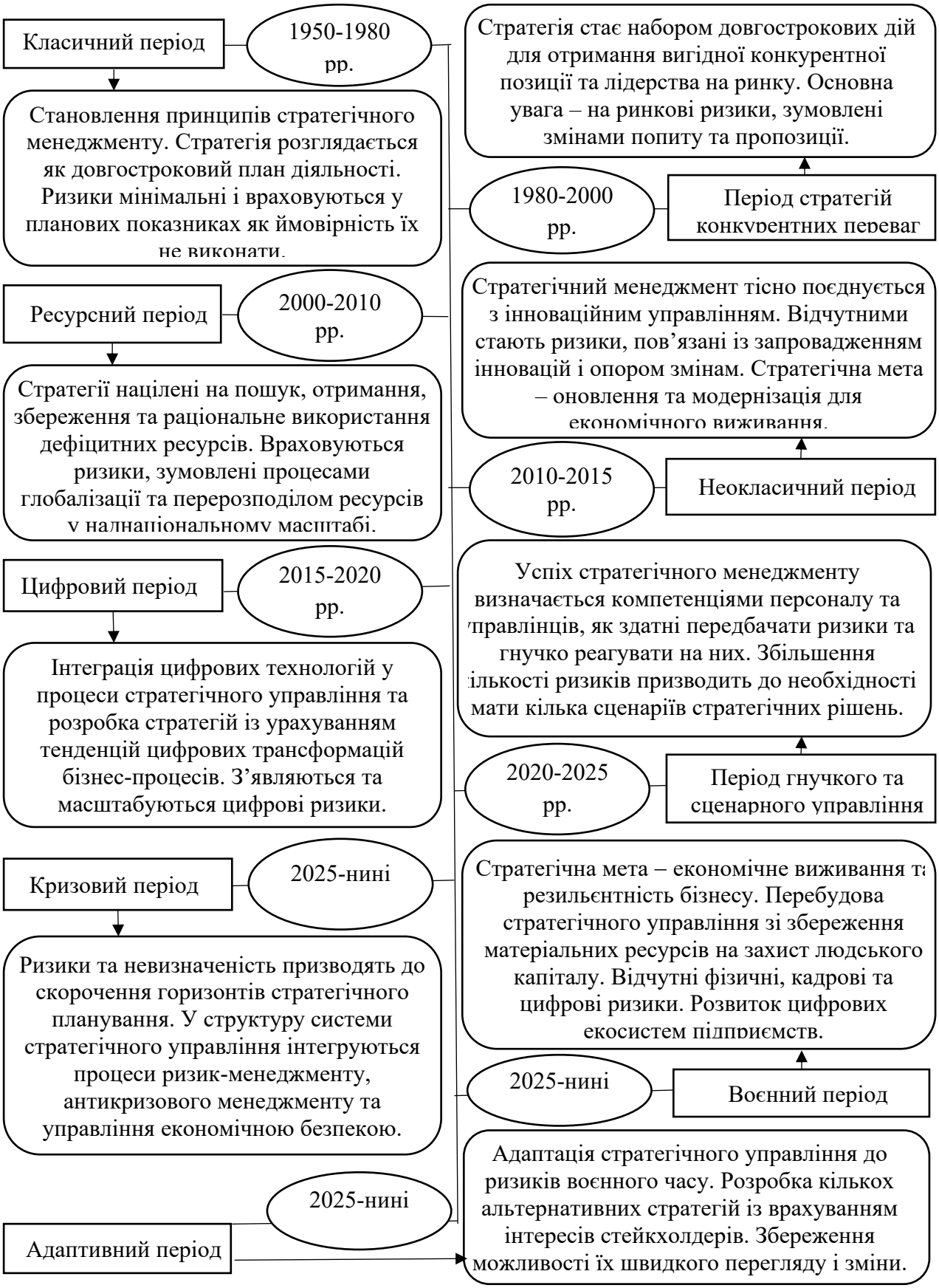


Рисунок 1.2. – Тайм-лайн еволюції парадигм стратегічного управління підприємствами під впливом ризиків

Джерело: складено автором за даними [20-67]

Таким чином, за останні 75 років концептуалізація стратегічного управління підприємствами зазнала суттєвих трансформацій, і у значній кількості випадків каталізаторами таких змін стали ризики, зумовлені тенденціями зовнішнього та внутрішнього середовища фінансово-господарської діяльності бізнесу. Частина з них мали еволюційний характер та спричинялися оновленням техніки, технологій, підходів до управління персоналом, змінами інтересів і потреб споживачів продукції та послуг, загальної соціалізації функціонування економічних систем. Водночас інші, більш критичні та непередбачувані ризики, з потенційними катастрофічними наслідками для суб'єктів підприємницької діяльності виникали по причині розгортання політичних, економічних, демографічних і соціальних криз, їх тривалого впливу на діяльність господарських структур та ефективність використання їх ресурсної бази. В Україні сучасний період зміни парадигми та концепції стратегічного менеджменту проходить із можливістю виокремити на теоретико-методичному рівні ознаки одразу трьох моделей розроблення стратегій – кризової, воєнної та адаптивної, а відтак, носить комплексний характер та створює власний, особливий, «український» стиль стратегічного управління підприємствами. Кожен із цих періодів має власні ознаки та характеристики, однак усі їх поєднує необхідність адаптації розроблених у довоєнний період стратегії до реалій воєнного часу, а також врахування цифрових ризиків, які стають усе більш відчутними у реаліях світу BANI, та кадрових ризиків, посилених міграцією населення та втратою людського капіталу. Наразі цей період ще не має конкретизованої та узагальненої науково-методичної бази для окреслення чітких принципів стратегічного управління, інструментарію, здатного забезпечити резильєнтність українського бізнесу та досягнення ним бажаних стратегічних орієнтирів, а також механізмів гнучкого ризик-менеджменту, які дозволять не лише ефективно протидіяти ризикам, уникати їх або мінімізувати наслідки їх впливу на ресурсну базу та перспективи компаній, але й використати можливості, які вони надають, для стабілізації та сталого розвитку підприємств в умовах невизначеності.

Отже, зміни парадигм стратегічного управління підприємствами під впливом пермакризи та ризиків світу BANI полягають у наступному. По-перше, сучасні підходи до стратегічного управління підприємствами характеризуються значно меншим інтервалом прогнозних показників: замість традиційних 10-25 років, стратегії розробляються на період 5-10 років. З одного боку це загрожує самій ідеї стратегічного менеджменту, який орієнтований на довгостроковий часовий період, та має на меті передбачити можливості та напрями розвитку підприємства у далекому майбутньому, однак, з іншого – є адаптивною реакцією управлінського персоналу на невизначеність і ризики, які роблять навколишнє економічне середовище суб'єкта господарювання мінливим і непередбачуваним, і які створюють фактори, на які управлінський персонал не може не відреагувати. По-друге, натепер період розвитку управлінської думки у контексті стратегічного менеджменту також характеризується взаємопроникненням, синергією та симбіозом різних типів і видів стратегії, а також поєднанням підходів і принципів антикризового, проєктного, ризик-менеджменту у механізмі стратегічного управління, узгодженістю, балансуванням їх цілей та формуванням стратегічних орієнтирів розвитку бізнесу та масштабування його економічного потенціалу з урахуванням потреб та інтересів інших функціональних напрямків менеджменту організації. По-третє, простеження зміни парадигм класичного стратегічного менеджменту під впливом пермакризи та ризиків світу BANI призводить до висновку, що усе більшої популярності набуває проектний підхід, який дозволяє розглядати стратегію як окремий проєкт, що реалізується у процесі функціонування та розвитку підприємства. Сучасні стратегії неодмінно враховують можливості цифровізації бізнесу, а також повинні мати можливості бути зміненими у випадку необхідності релокація бізнесу чи суттєвого оновлення виробництва або реалізації продукції з огляду на ті реалії, у яких опинилась Україна у воєнний період своєї історії. Пермакриза, викликана ланцюгом подій – світова економічна криза – глобальна пандемія – війна – створила таке середовище для ведення бізнесу, що не мало аналогів у світі, а відтак, український досвід

стратегічного менеджменту нині є унікальним. Його переваги – це середньострокові орієнтири, гнучкі зміни планових показників і шляхів їх досягнення, наявність кількох сценаріїв зміни оточення підприємства та параметрів його функціонування, наявність антикризової стратегії, управління стратегічними ризиками та економічним потенціалом як резервом економічного виживання та розвитку бізнесу у перспективі. Водночас, можна стверджувати про доцільність поєднання вітчизняних практик з зарубіжним досвідом стратегічного менеджменту, зокрема, щодо успішної розробки стратегій цифровізації бізнесу, а також подолання ризиків Індустрії 4.0 та формування візії переходу бізнесу до ідей та ідеалів Індустрії 5.0. Адже повоєнне відновлення економіки України потребуватиме стратегій для підприємств, що будуть здатні забезпечити їх конкурентоспроможність у порівнянні з компаніями, які перебували у мирних умовах, не мали необхідності запроваджувати антикризові заходи, намагатися зберегти людський капітал, та могли інвестувати у власний розвиток і зростання [20, с.167].

Перспективи подальших досліджень полягають у конкретизації сучасного стану розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації для того, аби встановити, до яких саме ризиків і загроз сучасного світу вітчизняним підприємствам потрібно адаптувати свої стратегії та системи стратегічного менеджменту загалом. Очевидно, що класичні парадигми стратегічного менеджменту здатні сформувати орієнтири для стратегічні функціонування та розвитку українських підприємств, однак, не мають належного інструментарію для підвищення рівня їх придатності до мінливих умов зовнішнього та внутрішнього середовищ існування бізнесу. Стратегії, які розроблялись підприємствами на період 2020-2030 років, наприклад, не враховували, і навіть потенційно не передбачали можливість розгортання активних бойових дій, окупацію територій, руйнування логістичної та критичної інфраструктури. Однак, це сталося, і для економічного виживання суб’єктів господарювання виникла гостра потреба у перегляді і переформатуванні своїх цілей у відповідності до реалій сьогодення.

1.3. Сучасний стан розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації

Сучасний стан розвитку науки управління характеризується фундаментальною зміною парадигм, що пов’язані із тривалою нестабільністю функціонування господарських структур, мінливістю стану та архітектонік економічних і соціальних систем, оновленням ринкових тенденцій та настроїв споживачів товарів і послуг, тощо. За останні двадцять років світ пережив кілька глобальних викликів, до яких мали адаптуватися суб’єкти господарської діяльності. Серед них: світова фінансова криза, інтенсифікація військових конфліктів у різних точках світу, глобальна пандемія, цифровізація економічного простору. Під впливом таких нетривіальних явищ і подій відбулося переосмислення теорій стратегічного менеджменту, розпочалися стійка трансформація концептуальних засад і рефокусування стратегічних орієнтирів господарської діяльності суб’єктів господарювання. Відтак, сучасний етап стратегічного менеджменту характеризується переходом від статичних моделей досягнення стратегічних конкурентних переваг та збереження впливу на ринках до комплексних екосистемних динамічних і гнучких концепцій довгострокового розвитку, частина з яких є безпеко орієнтованими, а інша – фокусується на активному використанні можливостей цифровізації. Вивчення зарубіжного досвіду цифрових трансформацій бізнесу призводить до висновку, що цифровізація є не лише тимчасовим явищем і технологічним чинником прогресу підприємництва, але і фактором впливу на світобачення довгострокових цілей функціонування бізнесу, який вимагає адаптивної модифікації постулатів класичних шкіл стратегічного управління до реалій ведення підприємницької діяльності в умовах масштабування цифрової економіки [68].

У теоретичній площині управлінської науки стратегія розуміється дослідниками як система, що відображає принципи внутрішньої організації або функціонування, певні ознаки та характеристики об’єкта дослідження [69,

с.273]. Необхідно додати, що характерною ознакою такої системи є зосередження її ресурсів на довгострокових цілях функціонування підприємства.

М. Й. Гедз, В. А. Вишневська, С. Д. Науменко вважають, що на сучасному етапі розвитку старатегічного менеджменту актуальним управлінським викликом є розробка науково-методичного підходу, який формує комплексну стратегію управління диверсифікаційно-інтеграційним розвитком корпоративних підприємств з урахуванням неотехнологічних умов відтворення [70, с.132]. Перевагами такого підходу можна вважати використання детерміновано-результативної технології, яка дозволяє ефективно вибудувати стратегічну піраміду та забезпечити вибір оптимально-результативного синергетичного стратегічного набору для максимальної реалізації поставлених цілей. Авторський підхід також враховує циклічність процесу диверсифікаційно-інтеграційного розвитку підприємства в умовах неотехнологічного відтворення [70, с.136] і цілком може використовуватись задля максимізації позитивного впливу цифровізації бізнес-процесів на фінансові результати підприємства та стан його економічної безпеки.

В умовах підвищення рівня невизначеності та турбулентності зовнішнього середовища ускладнюється процес розробки та реалізації стратегій, що потребує вдосконалення системи стратегічного контролю, який забезпечуватиме адаптивність стратегічного розвитку підприємства [71, с.356]. Таким чином, характерною рисою сучасного етапу теоретизації стратегічного менеджменту є привернення уваги керівництва компаній до необхідності запровадження стратегічного моніторингу, нагляду, контролінгу та інших форм і форматів спостереження за досяжністю стратегічних орієнтирів і оцінювання ефективності обраної стратегії задля гарантування можливості своєчасної її адаптації або оновлення у відповідь на виклики, загрози та ризики.

Якісними наслідками поширення цифрових технологій у економічному середовищі функціонування бізнесу є цивілізаційний розвиток, конвергенція та синергія векторів підприємницької діяльності у традиційній і цифровій

площинах, що надають переваги всім учасникам процесу цифровізації бізнесу – керівникам підприємства, інвесторам, споживачам. Ось чому в теоретичному аспекті цифровізація може стати імперативом стратегії розвитку цифрових трансформацій на підприємстві [69, с.273]. Сучасні інформаційні технології, що застосовуються в менеджменті, а також стрімкий розвиток процесів диджиталізації всіх сфер суспільного та економічного буття створюють передумови для систематизації інформаційних потоків, їх аналізу та розробки найбільш оптимальних моделей стратегічних рішень [71, с.356]. Тому на сучасному етапі стратеготворення управлінський персонал підприємств, які прагнуть бути сучасними та розвиватись у довгостроковій перспективі, усе частіше визнає важливість розроблення цифрових стратегій або стратегій цифрового розвитку бізнесу. В. В. Дергачова, Я. О. Колешня, В. Я. Голюк стверджують, що цифрова стратегія – це напрям розвитку підприємства у цифровому вимірі або ж напрям цифровізації його фінансово-господарської діяльності. Вона передбачає використання певних технологій у процесі трансформації бізнес-процесів та бізнес-моделі. Стратегія вказує на цілі, в той же час всередині стратегії існує необхідність вибору засобів, способів досягнення цих цілей – підбір відповідних технологій, їх оцінка, адаптація [72, с.115]. Важливо також зробити акцент на цифрових ризиках, які супроводжують діяльність підприємства в цілому, та є особливо непередбачуваними на довгострокових часових горизонтах, але за умови розроблення окремої стратегії для закладення підвалин цифровізації бізнесу – стають особливо відчутними, з наслідками, які можуть значно знизити рівень економічної безпеки компанії у перспективі. Відповідно до конкретного етапу розвитку підприємства – від новачка до «digitari» (термін, який означає, що діяльність і бізнес-процеси компанії повністю інтегровані в цифрові технології – авт.) прослідковуватиметься розмежування стратегій, що будуть використовуватися: відбуватиметься перехід бізнесу від стратегії цифровізації – до стратегії цифрової трансформації – і врешті до цифрової стратегії, яка є найвищим рівнем організації та формалізації стратегічного управління

підприємством у цифрову еру. Однак, середньостатистична українська компанія не обов'язково проходитиме всі три стратегії [72, с.116] під час еволюції підходів до організації власного менеджменту. Ймовірно, усе більш популярними будуть окремі функціональні стратегії підприємства, у яких певний напрям менеджменту набуде розвитку під впливом цифрових змін: наприклад, стратегія цифрового маркетингу, цифрового ризик-менеджменту, стратегія цифровізації комунікаційної політики, тощо. Науковці вважають актуальними в умовах цифрової трансформації бізнес-процесів такі стратегії менеджменту, як: стратегія цифрового партнерства, стратегія перетворення бізнес-моделі, стратегія забезпечення кібербезпеки, стратегія аналізу даних [73, с.49]. За умови використання комплексного підходу до реалізації принципів стратегічного управління підприємством, основні елементи стратегії менеджменту в цифровій трансформації бізнесу повинні містити: цифрову візію та цілі, аналіз конкурентного оточення, цифрові ресурси та інфраструктуру, інновації та експерименти, зміну організаційної структури та навичок [73, с.52].

Отже, сучасний стан розвитку наукових теорій стратегічного управління підприємствами під впливом цифровізації можна описати за допомогою таких характеристик. По-перше, це ідеологічний перехід від класичної теорії, яка ґрунтується на ефективному використанні наявних у підприємства ресурсів, до концепції динамічних спроможностей, що означає переміщення фокусу важливості від володіння корпоративними ресурсами до здатності швидко їх набути інтегрувати, масштабувати, трансформувати у такі формати, що дадуть підприємству змогу відповісти на актуальні виклики зовнішнього та внутрішнього середовищ. Особливого значення для забезпечення конкурентоспроможності бізнесу на стратегічному часовому горизонті має людський потенціал та здатність персоналу компаній набувати компетенції, які дадуть змогу адаптувати їх вчинки, рішення, підходи до виконання поставлених завдань до нетрадиційних ризиків і загроз мінливого економічного світу. У відповідності до такого підходу, стратегічне управління підприємством зосереджується на розвитку у персоналу інформаційної грамотності, а на рівні

бізнесу – «цифрової спритності», яка відображається у здатності суб'єкта господарювання швидко приймати цифрові рішення та використовувати цифрові можливості для отримання додаткових переваг і високих економічних результатів.

Другою характерною рисою сучасного стратегічного менеджменту є те, що під стратегічним управлінням науковці починають розуміти мистецтво започаткування розвитку та координації партнерств, платформ та клієнтських спільнот, значна частина яких перебуває у цифровому просторі. Конкуренція між компаніями замінюється конкуренцію між екосистемами ведення бізнесу, набуває нових характеристик параметрів, які не можна виміряти лише кількісними показниками, наприклад, такими, як обсяг реалізованої продукції наданих послуг або дохід, отриманий за результатами підприємницької діяльності. З огляду на це, стратегічні орієнтири розвитку бізнесу переміщуються від цілі збільшення обсягу прибутку «будь-якою ціною» до зростання ринкової вартості та соціальної цінності усієї мережі партнерських і економічних відносин.

Наступною помітною рисою трансформацій стратегічного управління є набуття популярності використання інструментів проєктного менеджменту для досягнення стратегічних цілей бізнесу. Такі якісні ознаки та принципи управління проєктами, як гнучкість, обмеженість у часі, конкретні економічні результати та можливість зміни цільових показників безпосередньо у процесі досягнення поставленої мети добре відповідають тенденціям нестабільності економічного світу та явищу непередбачуваності цифрових трансформації бізнесу. Тому натепер стають усе більш популярними процеси розробки функціональних стратегій підприємств як проєктів, де стратегічним орієнтиром є виробництво інноваційного продукту, охоплення нової ринкової ніші або розвиток одного з напрямів підприємницької діяльності.

Окремим вектором еволюції теорії стратегічного менеджменту дослідники вважають концептуалізацію використання штучного інтелекту в управлінні організаціями. Зокрема, приділяється значна увага напрацюванню припущень

та прогнозам щодо того, яку частину функцій стратегічного управління буде розподілено у майбутньому між людиною та штучним інтелектом. У цьому контексті варто згадати теорію «доповненого інтелекту», змістова сутність якої полягає у тому, що стратегічні рішення у процесі функціонування підприємства приймаються на основі симбіозу інтуїції, досвіду, навиків і компетенції топ-менеджменту компанії та результатів продуктивної аналітики від використання алгоритмів, які побудовані на принципах функціонування штучного інтелекту.

Таким чином, сучасний стан розвитку теорії стратегічного управління можна охарактеризувати як інтеграцію цифрових інструментів у процеси прийняття стратегічних управлінських рішень, а також як трансформацію стратегії від документу, що містить жорсткий план дій для досягнення поставленої мети на довгостроковому часовому горизонті до гнучкої адаптивної архітектури прийняття управлінських рішень, яка здатна до видозміни та вдосконалення під впливом сили нових параметрів зовнішнього та внутрішнього середовища ведення бізнесу, та до прояву швидких адаптивних реакцій на виклики цифровізації та турбулентності поведінкової ринкової економіки [68].

Під час проведеного у попередньому розділі роботи дослідження сучасного етапу розвитку теорій стратегічного управління, було ідентифіковано таку його особливість, як інтеграція управління економічною безпекою до переліку стратегічних цілей функціонування українських підприємств. В усьому світі інтерес до питання забезпечення економічної безпеки бізнесу поступово зростає, що зумовлюється нестабільністю підприємницького середовища та значною кількістю ризиків для сталого розвитку компаній у довгостроковій перспективі. Економічна безпека досліджується у різних контекстах, про що свідчать дані рис.1.3, які демонструють результати контент-аналізу джерел із наукометричної бази Scopus, починаючи з таких публікацій, що датуються 1910 роком, і завершуючи актуальними дослідженнями початку 2026 року. Зауважимо, що лідерами за кількістю наукових праць, які

стосуються проблемних питань забезпечення економічної безпеки, є науковці з США, України, Китаю, Великобританії, Індії, Австралії, Польщі та Німеччини.

Рисунок 1.3. – Галузі знань, у межах яких відбуваються дослідження проблеми забезпечення економічної безпеки

Джерело: [74]

Активні спроби теоретизацій поєднань контекстів економічної безпеки та стратегічного управління підприємствами прослідковуються у публікаціях вітчизняних вчених як довоєнного, так і воєнного періоду. Зокрема, Адлер О.О., Кавецький В. В. вважають, що стратегічне управління бізнес-процесами підприємства має будуватися на основі рівня його економічної безпеки [75]. Живко З. Б., Овечкіна О. А., Родченко С. С., Сакун Л. М. висловлюють переконання щодо необхідності розробки інноваційної моделі стратегічного розвитку в управлінні безпековою економікою в умовах посилення зовнішньоекономічних зв'язків та діджиталізації [76], Писаренко В. В., Савенко О. А., Шпортюк Н. Л. концентруються на аспектах

моделювання системи безпекового стратегічного управління інноваційно орієнтованими підприємствами в глобалізаційних умовах економіки знань [77], Зачосова Н. В. та її співавтори досліджують активні та пасивні стратегії управління економічною безпекою суб'єктів господарювання в умовах традиційних та інноваційних загроз [78], описують актуальні методологічні підходи до досліджень проблем менеджменту у контексті стратегічного управління економічною безпекою підприємств [79] та аргументують необхідність розвитку персоналу та кадрового потенціалу у системі стратегічного управління фінансово-економічною безпекою суб'єкта господарювання [80], Копча Ю. Ю. пропонує науковий підхід до формування стратегічних орієнтирів управління потенціалом економічної безпеки підприємств [81], Корчевська Л. О. розглядає адаптаційні та біфуркаційні стратегії управління економічною безпекою підприємства [82], Латишева О. В., Касьянюк С. В., Мілявський М. Ю. фокусуються на визначенні особливостей управління витратами в системі формування стратегії економічної безпеки та сталого розвитку вітчизняних підприємств [83], Лізут Р. А. формалізує загальні та деталізовані стратегії управління організаційно-економічною безпекою підприємств [84], Олійник А., Іщейкін Т., Карташов Р., Невкритий М. розкривають особливості стратегічного управління економічною безпекою аграрного підприємства у бізнес-середовищі [85], Онищенко О. В., Яценко Н. М., Гончаренко Н. О. конкретизують роль економічної безпеки у стратегічному управлінні промисловим підприємством [86], Приймак Н. С., Дев'яткова О. В. чинять спроби узагальнення теоретичних основ та інструментарію стратегічного управління економічною безпекою підприємства [87], Сидорчук І. опікується питаннями систематизації теоретико-методологічних підходів до формування, реалізації та моделювання стратегій управління інноваційним розвитком та фінансово-економічною безпекою підприємницьких структур [88], Сімкова Т. О. простежує причинно-наслідкові зв'язки між управління розвитком автотранспортних підприємств та станом складових механізму формування стратегічних напрямків в умовах

гарантування економічної безпеки [89], Толпежніков Р. О., Толпежнікова Т. Г., Балашов М. І. систематизують методологічні підходи до управління змінами в стратегії забезпечення потенціалу економічної безпеки промислових підприємств [90], Топоркова О. В., Акімова Н. С., Наумова Т. А. аналізують та уточнюють стратегічні аспекти управління ризиками для забезпечення економічної безпеки підприємства [91], Турило А. М., Турило А. А., Короленко Р. В., Короленко С. М. оцінюють взаємовпливи та причинно-наслідкові зв'язки між стратегією розвитку, корпоративним управлінням і людським капіталом відносно економічної стратагеми, економічної девіації і фінансово-економічної безпеки в діяльності підприємства [92], Яремко І. І. пропонує використання сучасних інструментів стратегічного управління як засобу підвищення рівня економічної безпеки суб'єкта господарювання [93].

Отже, сучасний етап досліджень проблематики стратегічного управління економічною безпекою підприємства можна описати кількома важливими характеристиками:

– по-перше, потребують адаптації класичні види стратегій, як то активна, пасивна, тощо, для того, аби їх можна було ефективно використовувати для управління економічною безпекою на стратегічному рівні менеджменту організацій;

– по-друге, стратегічне управління економічною безпекою має власні управлінські особливості, інструменти та цілі залежно від того, для якого виду економічної діяльності підприємства воно застосовується;

– по-третє, існує переважно авторський інструментарій стратегічного управління економічною безпекою та відсутньою на разі є комплексна концепція такого напряму менеджменту організацій, а також у теоретико-методичній площині бракує методичних підходів до оцінювання рівня ефективності стратегічного управління економічною безпекою суб'єктів господарювання.

Рис. 1.4. узагальнює сучасні контексти дослідження стратегічного управління економічною безпекою, які вдалося виокремити у результаті монографічного аналізу змісту публікацій [75-91].

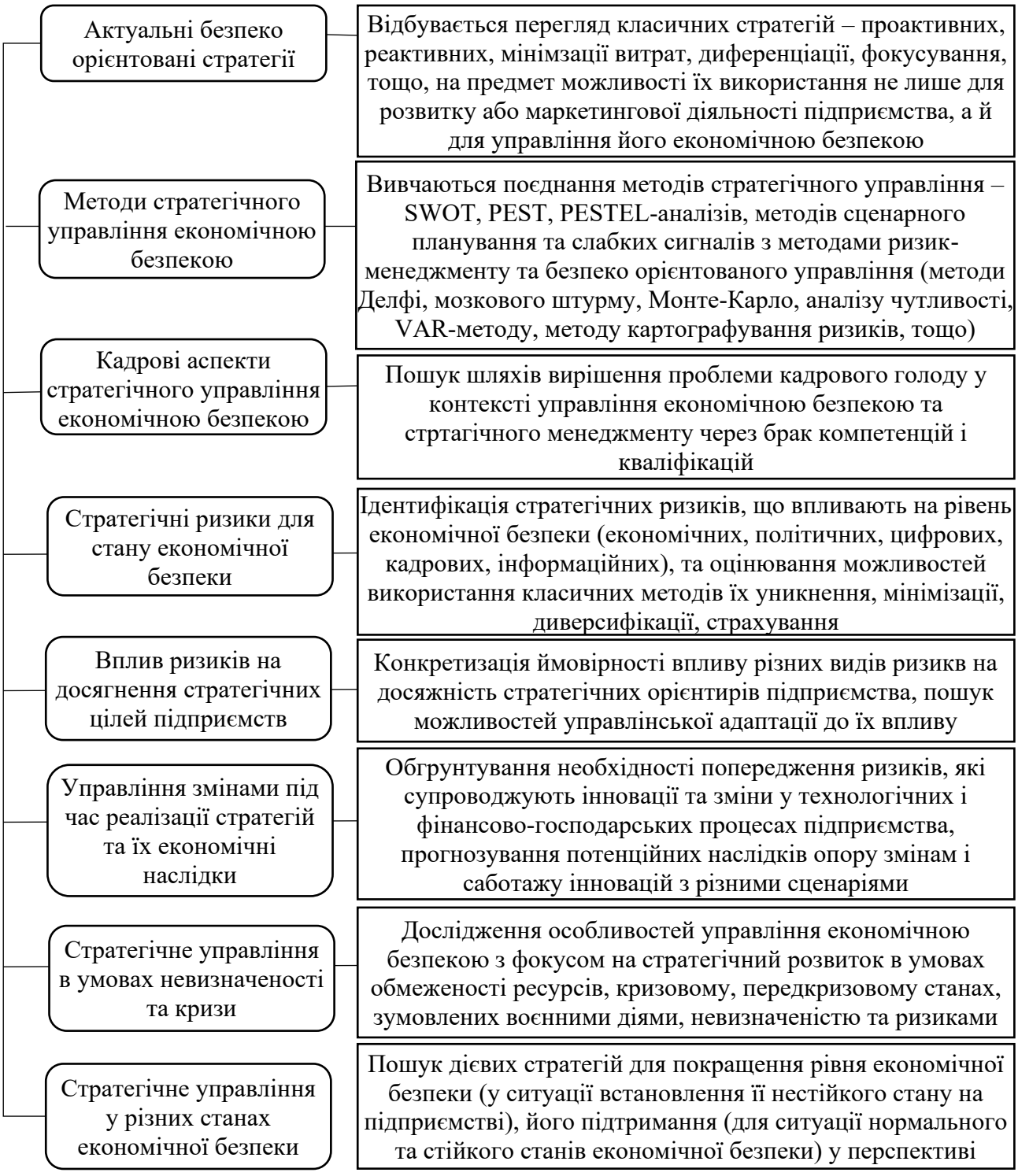


Рисунок 1.4. – Сучасні контексти дослідження стратегічного управління економічною безпекою

Джерело: складено автором на основі [75-91]

На рис. 1.5 простежується зростання інтересу до питання забезпечення економічної безпеки як на макро, так і на мікрорівні, і в Україні, і в світі загалом, за останні п’ять років. Це зумовлено посиленням нестабільності функціонування глобальних і локальних соціально-економічних систем, тривалими світовими кризами і напругою у суспільстві.

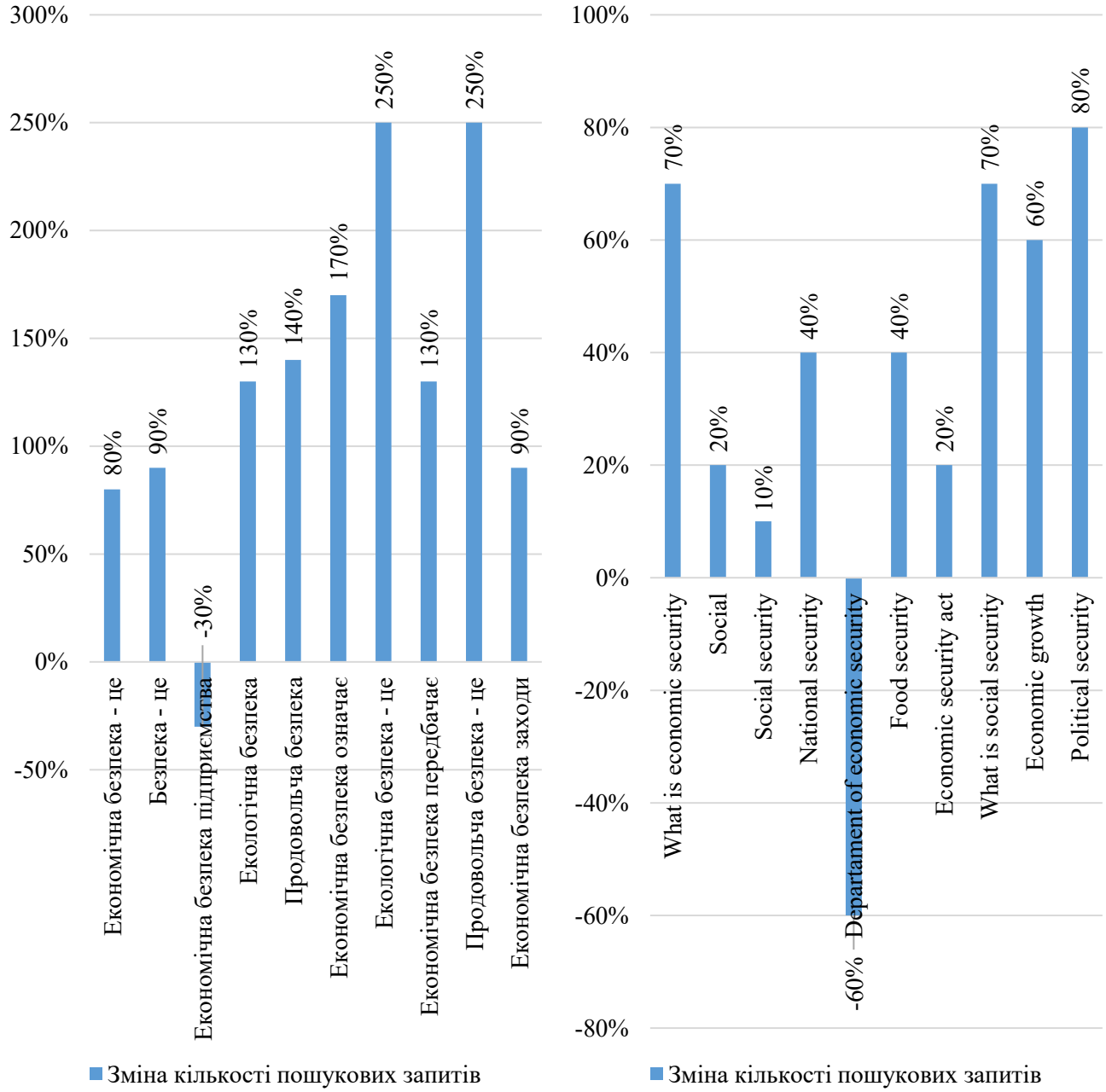


Рисунок 1.5. – Зростання інтересу до проблем управління економічною безпекою та її складовими в Україні та в світі

Джерело: складено автором на основі аналізу Google Trends [94]

Стратегічне управління економічною безпекою підприємств тісно пов'язане з ризик-менеджментом, а категорія економічної безпеки перебуває у нерозривному сутнісному зв'язку з дефініцією ризику, а також загрози, небезпеки та виклику. Зокрема, це переконливо доводять у своїх дослідженнях такі вчені, як Костюк Ж. С., що вважає поняття ризику, небезпеки та загрози базовими категоріями розкриття сутності економічної безпеки підприємства [95], Цікановська Н. А., що пропонує власну інтерпретацію понять «виклик», «небезпека», «загроза» та «ризик» у теорії фінансової безпеки [96], Новіков А. О., Рудніченко Є. М., Лубенець І. О., Данкевич А. Є., Ткачук Г. Ю., Нікітіна А. В., Колісніченко П. Т., Мельник С. І., які встановлює взаємозв'язок понять ризику, небезпеки і загрози у контексті забезпечення фінансово-економічної безпеки [97-103], Зачосова Н. В., яка конкретизує поняття фінансової безпеки як наукової та управлінської категорії у взаємозв'язку з дефініціями виклику, небезпеки, загрози і ризику [104], а також Корнієнко Т. О., що вивчає вплив загроз та ризиків на формування системи економічної безпеки підприємства [105] та Капелюшна Т. В., яка визначає особливості та специфіку формування площини безпеки підприємства під дією ризиків і загроз [106].

Ризик – це сутнісна ймовірність того, що явище, яка може трапитися у майбутньому, матиме неочікувані наслідки для стану підприємства. Категорія «майбутнє», яка вжита у цій дефініції, доводить зв'язок ризиків зі стратегічним менеджментом суб'єкта господарювання, який націлений на трансформації його поточного стану – активів, ресурсів, підприємницьких можливостей – у бажаний стан у середньо або довгостроковій перспективі. Ризик демонструє міру невизначеності майбутніх результатів діяльності суб'єкта господарювання у кількісних і якісних показниках, що може спровокувати непередбачувані втрати або інші негативні для наслідки для стану економічної безпеки бізнесу. Ризики є невід'ємною частиною будь-якої фінансово-господарської діяльності, оскільки жодна компанія або організація не може бути повністю застрахованою або захищеною від зовнішніх і внутрішніх загроз для свого існування [107].

Така гіпотеза зайвий раз доводить нерозривне поєднання ризиків і рівня економічної безпеки підприємств.

Особливістю феномену ризику є те, що його наслідки можуть бути для компанії позитивними. Ризикнувши, підприємство може отримати неочікувані позитивні можливості для свого стратегічного розвитку, наприклад, на нових ринках товарів і послуг. Проте, впевненості у цьому факті менеджери компаній не можуть мати, особливо при довгостроковому стратегічному плануванні. На прикладному рівні функціонування бізнесу вважається, що якщо в менеджмент компанії не ризикує, обираючи ти той чи інший вектор свого розвитку, він може втратити суттєві переваги та конкурентні позиції, не досягнути або не повністю досягнути стратегічних орієнтирів та мети свого створення. Відтак, ризик не можна охарактеризувати як суто негативне явище в економічній системі. Отже, у практичній площині ризик – це економічна можливість для підприємства здобути вищі економічні результати, ніж було заплановано під час розробки його стратегії.

Управління ризиками об’єднує у собі процеси ідентифікації, аналізу, оцінювання та мінімізації виявлених ризиків і їх негативних наслідків шляхом розробки стратегій і прийняття обґрунтованих управлінських рішень, що дозволяють зменшити шкоду від настання ризику або дають змогу скористатися новою підприємницькою можливістю. Розглядаючи управління ризиками з метою забезпечення фінансово-економічної безпеки підприємств, українські дослідники знаходять усе нові можливості та інструменти інтеграції ризик-менеджменту у стратегії досягнення цілей сталого розвитку та масштабування конкурентних переваг суб’єктами господарської діяльності [108-111]. У теоретико-методичній площині сучасної науки менеджменту виокремився самостійний напрям ризик-орієнтованого управління економічною безпекою підприємницьких структур, прихильниками та ідеологами якого можна вважати таких вчених, як Герасименко О. М., Пасєка С. Р., що запропонували концептуальні основи ризик-орієнтованого підходу до управління у процесі забезпечення системи економічної безпеки підприємств

різних галузей народного господарства [112], Данілова Е. І., яка концепуалізувала методологію ризик-орієнтованого підходу до управління економічною безпекою підприємства [113], Гриценко Л. Л., Кожушко І. О., Чепурко В. О., Перепеліцин Г. Б., якими запропоновано шляхи інтеграції ризик-орієнтованого управління в систему економічної безпеки корпоративного підприємства [114], Лоскутова Г. А., що описала доцільність ризик-орієнтованого управління у транспортних технологіях на шляху до економічної безпеки [115]. У контексті цього дослідження особливо цінними є здобутки таких науковців, як Потюк В. М., Василішин С., що вивчають управління ризиками та інтеграцію цифрових інструментів у бізнес-процеси підприємств для забезпечення їх економічної безпеки в умовах трансформації національної економіки [116] та удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи [117], оскільки у їх роботах простежується визнання та привернення уваги наукової спільноти до проблеми впливу цифрових ризиків на стан економічної безпеки суб'єктів господарювання.

Рис. 1.6 демонструє підходи конкретизації змістової сутності поняття ризику у сучасній науці управління.

Отже, ризики, у тому числі цифрові, є невід'ємною частиною фінансово-господарської діяльності кожного підприємства, одним із об'єктів управлінського впливу у комплексній системі його економічної безпеки та чинником впливу на результативність його стратегії. Управлінцям важливо розуміти природу виникнення та існування ризику, та передбачати його потенційний вплив на організацію та її економічну безпеку, щоб розробити ефективні стратегії для його мінімізації. Оскільки зовнішнє і внутрішнє середовище діяльності українського бізнесу постійно змінюються, трансформуються та оновлюються, особливо у цифровому економічному просторі, ефективне управління ризиками вимагає не тільки оновлення підходів до використання традиційних методів і практик ризик-менеджменту, а й впровадження сучасних цифрових інструментів для моніторингу та оцінювання

ризиків і прогнозування їх наслідків для стану економічної безпеки суб'єктів господарювання на різних часових горизонтах реалізації їх стратегій.

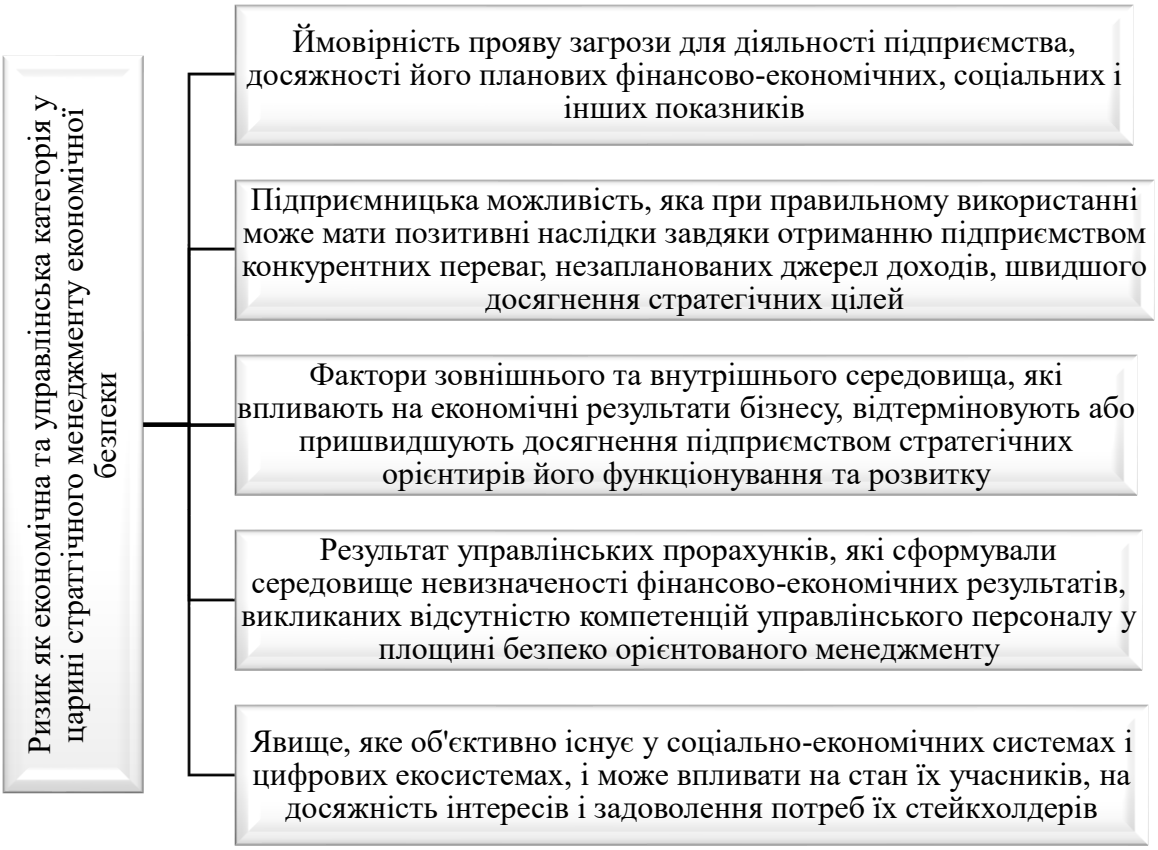


Рисунок 1.6. – Наукові підходи до розуміння поняття ризику в науці управління

Джерело: складено автором за даними [107, 118-136]

Питання методології досліджень проблематики управління ризиками у практиці роботи українських підприємств, установ, організацій уже тривалий час розглядаються багатьма вченими, що було переконливо доведено у межах цього підрозділу. Черговий етап активізації наукових досліджень у цій площині розпочався з моменту старту повномасштабної війни у 2022 році. Управління ризиками в умовах воєнного часу – це нова сторінка історії українського безпекознавства, оскільки ще ніколи ризики для функціонування бізнесу не були такими суттєвими, а наслідки їх прояву – настільки реальними, критичними та руйнівними для їх стратегічного розвитку.

Зміни, що відбуваються в глобальній економіці, технологічному середовищі та внутрішніх процесах підприємств, ставлять перед управлінцями нові виклики, які потребують своєчасної адаптивної реакції у площині стратегічного управління бізнесом. На рис. 1.7 узагальнено функціональні напрями управління ризиками, які мають існувати на сучасних підприємствах, метою яких є комплексне управління ризиками для економічної безпеки у довгостроковій перспективі під впливом цифровізації.

Рисунок 1.7. – Функціональні напрями стратегічного управління ризиками на сучасних підприємствах в умовах цифровізації

Джерело: складено автором за даними [118-136]

Під час стратегічного ризик-менеджменту управлінський персонал встановлює довгострокові орієнтири для управління ризиками, планує показники діяльності підприємства за різними сценаріями: на випадок інтенсивного прояву ризику, у ситуації помірного його впливу на результати фінансово-господарської діяльності та в умовах відсутності ризику або в умовах, коли його негативні наслідки для підприємства не проявились.

Стратегічний ризик-менеджмент має важливе значення для визначення довгострокових цілей генеральної стратегії діяльності та розвитку суб'єкта господарювання, оскільки дає змогу оцінити рівень її досяжності, а відтак сформувати реалістичні шляхи поступового руху до встановлених цілей.

Рис. 1.8 узагальнює та унаочнює циклічний підхід до розробки та запровадження моделі управління ризиками для сучасних українських компаній із використанням цифрових інструментів.

Рисунок 1.8. – Циклічний підхід до розробки та запровадження моделі стратегічного управління ризиками у системі забезпечення економічної безпеки підприємства з використанням цифрових інструментів

Джерело: складно автором

Для досягнення стратегічної мети ризик-менеджменту у системі управління економічною безпекою на підприємстві можна використати:

– стратегію уникнення ризиків, яка полягає у прийнятті управлінських рішень, які дозволяють уникнути певного виду ризику, існування якого для підприємства було визначено та доведено на попередніх етапах досліджень;

– стратегію хеджування – як засіб застосування фінансових інструментів чи контрактів для мінімізації можливих втрат (переважно використовується для зменшення та уникнення фінансових ризиків, або фінансових наслідків від впливу інших видів ризику на діяльність суб'єкта господарювання та його економічну безпеку);

– стратегію диверсифікації, який означає розподіл активів або інвестицій підприємства з метою зменшення впливу одного виду ризику на всю його ресурсну систему та результативність бізнес-процесів.

Отже, цифровізація стимулює оновлення підходів до управління ризиками, надаючи менеджерам сучасних компаній інструменти для швидкого та ефективного реагування на зміни в бізнес-середовищі. Інноваційні технології, такі як ІТ-системи, великі дані, штучний інтелект та блокчейн, дозволяють проводити глибокий аналіз ризиків, причин їх виникнення та розвитку, покращувати процеси прийняття стратегічних управлінських рішень і значно знижувати ймовірність негативних наслідків від впливу ризиків для фінансово-господарських результатів та стану економічної безпеки підприємства. Нині, у 2026 році, цифровізація стає основним фактором, що підвищує стійкість компаній до впливу різноманітних ризиків на її економічні показники та джерелом можливостей для удосконалення підходів і практик до ефективної організації системи ризик-менеджменту на сучасних підприємствах в Україні та в світі. Водночас, вона є і інноваційним джерелом для виникнення та поширення цифрових ризиків. Тому без належної підготовки на стратегічному рівні менеджменту, активне запровадження цифрових трансформацій може стати критичним фактором для стану економічної безпеки компанії та її фізичного виживання на ринку.

Цифровізація впливає на сутнісні ознаки та властивості термінополя стратегічного управління економічною безпекою підприємства. З'являються нові категорії та поняття, які набувають широкого вжитку під час управління ризиками та у процесі розроблення стратегій безпеко орієнтованого розвитку бізнесу, а класичні терміни отримують нові сенси, які потрібно розуміти та враховувати і на теоретико-методичному, і на прикладному рівні.

У табл. 1.2 узагальнено оновлені поняття термінополя стратегічного управління економічною безпекою підприємства, що трансформувались під впливом цифровізації та цифрових ризиків.

Таблиця 1.2. – Оновлення термінополя стратегічного управління економічною безпекою підприємства під впливом цифровізації та цифрових ризиків

Поняття з термінополя	**Традиційна(класична) дефініція**	**Зміна розуміння суті поняття з урахуванням цифровізації і цифрових ризиків**
1	2	3
Економічна безпека підприємства	Стан захищеності корпоративних ресурсів підприємства від внутрішніх і зовнішніх загроз, та ефективне їх використання з мінімальними ризиками, що забезпечує стабільний економічний стан і перспективи розвитку	Динамічний стан захищеності корпоративних ресурсів підприємства від традиційних і інноваційних (цифрових і кібернетичних) загроз і ризиків, що забезпечує стійкість і сталість його бізнес-процесів в умовах цифрової трансформації та дозволяє оперативно реагувати та використовувати можливості зовнішнього та внутрішнього середовищ.
Стратегічне управління	Процес розробки і реалізації довгострокових орієнтирів діяльності і розвитку потенціалу підприємства з урахуванням змін тенденцій зовнішнього середовища	Безперервний процес адаптації стратегічних орієнтирів підприємства і прийняття довгострокових управлінських рішень на основі аналізу цифрових даних із використанням цифрових технологій, спрямованих на забезпечення стійкості та конкурентоспроможності бізнесу.
Загроза	Потенційна або реальна небезпека, що може завдати збитків підприємству та порушити стан його безпеки.	Потенційний або наявний негативний чинник, що виникає у екосистемі бізнесу або його цифровому середовищі, і деструктивно впливає на його економічну стабільність
Ризик	Ймовірність виникнення негативних тенденцій у економічному стані підприємства, що загрожує збитками.	Ймовірність втрати стійкості, спричинена цифровими збоями, кіберінцидентами, алгоритмічними помилками та асиметрією дпних.

Продовження табл. 1.2

1	2	3
Стійкість (резильєнтність)	Здатність соціально-економічної системи протистояти негативним факторам і відновлюватися після впливу криз.	Здатність соціально-економічної системи адаптуватися до криз, цифрових збоїв, кіберзагроз і зміни трендів, використовуючи цифрові технології та гнучкі моделі управління ресурсами.
Управління ризиками	Ідентифікація, оцінювання та мінімізація впливу ризиків на економічний стан підприємства.	Протидія ризикам і їх наслідкам на основі аналізу аналогових і цифрових даних та використання ШІ для розробки рішень щодо ризик-менеджменту.
Стратегія	Довгостроковий план досягнення основних функціональних цілей підприємства.	Гнучкий алгоритм дій, що базується на даних, інноваціях і управлінні ризиками, спрямований на досягнення стратегічних орієнтирів розвитку бізнесу.
Безпекова стратегія	Довгостроковий план забезпечення економічної безпеки підприємства.	Комплексна безпеко орієнтована стратегія ведення бізнесу, що поєднує стратегічний, антикризовий і ризик-менеджмент.
Інформаційна безпека	Захист відомостей підприємства від несанкціонованого доступу та використання.	Комплекс заходів щодо захисту інформації, цифрових платформ, хмарних сервісів і мереж від цифрових ризиків.
Бізнес-процеси	Комплекс взаємопов'язаних господарських операцій, спрямованих на створення продукту чи послуги.	Цифровізовані та автоматизовані господарські процеси, інтегровані в екосистему бізнесу, що забезпечують його функціонування.

Джерело: складно автором

За даними, згрупованими у табл.1.2, можна простежити, як у теоретико-методичній площині цифровізація поступово трансформує концептуальний зміст ключових понять, що використовуються у процесі управління економічною безпекою підприємства, зміщуючи акцент від статичної захищеності активів і ресурсів суб'єкта господарювання під час їх використання від ризиків зовнішнього та внутрішнього середовища до динамічної стійкості системи економічної безпеки, яка змінюється разом із новими формами ризиків і загроз для ефективної протидії їм; від надання пріоритету управлінню традиційними економічними ризиками, що є найбільш впливовими для матеріальних активів підприємств до кібернетичних і цифрових загроз, здатних впливати на стан нематеріальних ресурсів, інтелектуального капіталу та кадрового потенціалу бізнесу; від лінійного менеджменту до управління на основі аналізу даних (переважно цифрових) та адаптивного управління стратегіями, ризиками, безпековими факторами, тощо.

Рис. 1.9 демонструє перехід у теоретико-методичному просторі до сучасного стан розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації.

Рисунок 1.9. – Сучасний стан розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації

Джерело: складно автором

Отже, на сучасному етапі розвитку науки менеджменту відбувається еволюція підходів до управління економічної безпеки підприємства із використанням принципів стратегічного менеджменту. Водночас, оскільки управління економічною безпекою та ризик-менеджмент є досить динамічними напрямами управління бізнес-процесами суб'єктів господарювання, вони першими трансформуються від впливу новітніх тенденцій розвитку соціально-економічного середовища ведення бізнесу, як цифровізація. З огляду на це, натепер сформувалися основоположні концептуальні засади безпеко орієнтованого стратегічного менеджменту, шо на відміну від традиційних парадигм, враховують цифрові ризики, і дозволяють управлінцям розширені можливостей використання цифрових інструментів для аналізу даних щодо ризиків, формування актуальної аналітики із відкритих джерел інформації на основі застосування ШІ, протидії кіберзагрозам, тощо, у поєднанні їх з класичними постулатами антикризового та ризик-менеджменту, що спрямовують управлінські зусилля на мінімізацію загроз для діяльності бізнесу та досягнення ним стратегічних орієнтирів свого функціонування та розвитку.

Простеження еволюції стратегічного управління економічною безпекою підприємств дозволяє дійти висновку, що на сучасному етапі управлінські дії персоналу, спрямовані на підтримання її високого рівня, характеризуються багаторівневістю та нелінійністю, що в цілому відповідає концепції світу BANI та робить захисні управлінські рішення адаптивними та придатними для застосування у форматі реакції на різкі та непередбачувані прояви загроз і ризиків в оточенні підприємства. Крім того, помітним є ідеологічний перехід від реактивного захисту корпоративних ресурсів компаній до проективного управління ризиками та інтеграції механізмів ризик-менеджменту до цифрової екосистеми ведення бізнесу. Водночас, негативною характеристикою цього етапу є залежність системи економічної безпеки підприємства та його стратегії від технологічних змін та опору їм з боку персоналу, а також від негативного впливу глобальних криз та тенденцій воєнного стану на підприємницьке середовище та вітчизняні ринки товарів і послуг.

Висновки до розділу 1

1. Узагальнено та охарактеризовано змістові трансформації класичних суджень щодо елементів парадигмальних засад стратегічного менеджменту у сучасній науці управління. Причинами та чинниками ідентифікованих змін запропоновано вважати: мінливість умов зовнішнього та внутрішнього середовищ, що зміщує фокус управлінських рішень із конкретики на варіативність; непостійність конкуренції по причині оновлення інтересів і потреб споживачів; необхідність врахування різних сценаріїв майбутнього; заміщення роботи з окремими ризиками на комплексний захист корпоративних ресурсів; визнання важливості нематеріальних активів і інтелектуальних цінностей для стану економічного потенціалу підприємства; практику проєктування сценаріїв майбутнього замість здогадок і припущень; реалії світу BANI; перехід до гнучких форматів взаємодії зі стйкхолдерами та зміщення фокусу з пріоритету отримання підприємством прибутку за будь-яку ціну. Ці та інші фактори призвели до того, що у теорії стратегічного управління на заміну категорії стратегічних цілей прийшло поняття стратегічних орієнтирів функціонування та розвитку бізнесу; стійкі конкурентні переваги змінилися на динамічні спроможності та можливості підприємства виживати в мінливих умовах; стратегічне планування поступово заміщується сценарним плануванням управлінських дій; управління стратегічними ризиками набуває формату забезпечення стратегічної економічної безпеки компанії; під стратегічними активами бізнесу науковці починають розуміти його стратегічні можливості і спроможності; замість категорії прогнозування набуло поширення поняття форсайту; інтереси власників бізнесу стають другорядними порівняно з інтересами решти категорій стейкхолдерів; стратегічний горизонт планування управлінських скоротився до трьох-п’яти років, а контроль і нагляд замінюється процесами оцінювання і адаптації стратегічних управлінських рішень.

2. Встановлено потребу у перегляді та оновленні парадигмальних засад стратегічного управління підприємством у світі BANI та запропоновано конкретні напрямки їх змін, такі як запровадження принципів гнучкого та сценарного управління, застосування адаптивного менеджменту та антикризових стратегій, запровадження практик критичного мислення та сценарного аналізу, використання цифрових технологій, інформації з різних джерел та штучного інтелекту як корпоративних ресурсів; перехід до децентралізації влади та гнучких управлінських структур; розвиток цифрового управління бізнес-процесами; розвиток екосистем і стратегічних альянсів; масштабування практик людиноцентричного управління підприємствами та використання прогностичної аналітики та технік форсайту для прийняття та реалізації управлінських рішень. Ці трансформації стануть гідними відповідями на такі виклики, як нераціональність і втрата актуальності довгостроковими стратегіями, неможливість отримати релевантні дані та достовірно спрогнозувати майбутнє підприємства; потреба у врахуванні у стратегіях явищ турбулентності і невизначеності економічного простору, ігнорування менеджментом випадкових можливостей розвитку бізнесу, нехтування людським потенціалом і капіталом.

3. Оновлено термінополе стратегічного управління економічною безпекою підприємства. Запропоновано адаптовані під впливом цифровізації та цифрових ризиків сутнісні трактування таких класичних понять, як економічна безпека підприємства, стратегічне управління, загроза, ризик, стійкість, управління ризиками, стратегія, безпекова стратегія, інформаційна безпека, бізнес-процеси. Економічну безпеку підприємства визначено як динамічний стан захищеності його корпоративних ресурсів від традиційних і інноваційних (цифрових і кібернетичних) загроз і ризиків, що забезпечує стійкість і сталість бізнес-процесів в умовах цифрової трансформації та дозволяє оперативно реагувати та використовувати можливості зовнішнього та внутрішнього середовищ. Стратегічне управління підприємством ідентифіковано як безперервний процес адаптації його стратегічних орієнтирів і прийняття довгострокових

управлінських рішень на основі аналізу цифрових даних із використанням цифрових технологій, спрямованих на забезпечення стійкості та конкурентоспроможності бізнесу.

4. Виокремлено та формалізовано чотири етапи розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації. На першому етапі теоретико-методичним основам стратегічного безпеко орієнтованого менеджменту були притаманні такі процеси, як формування науково-теоретичного базису стратегічного управління економічною безпекою підприємства, ототожнення стану економічної безпеки з ефективним використання ресурсів підприємства та отримання ним прибутку та інтеграція безпеки у стратегічний менеджмент. На другому етапі відбулося усвідомлення ризиків як важливої складової системи управління економічною безпекою та інтеграція елементів ризик-менеджменту у стратегії підприємств. На третьому етапі відбувся початок використання елементів адаптації та гнучкого управління (проєктного підходу) для оптимізації стратегічного управління економічною безпекою підприємств, а також виокремлення цифрової і кібербезпеки у окремі функціональні підсистеми управління економічною безпекою підприємства. Сучасний етап розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації ознаменувався переосмисленням стратегічного управління економічною безпекою в умовах крихкості, тривожності, нелінійності та незрозумілості, тобто у реаліях світу BANI, що призвело до формування принципів стратегічного менеджменту в умовах пермакризи, адаптації підходів стратегічного управління до реалій воєнного часу, у результаті чого відбулося концептуальне поєднання теорій антикризового, стратегічного, ризик-менеджменту з принципами гнучкого управління та адаптивності.

Отримані у межах розділу наукові результати опубліковані у працях здобувача [1], [20], [68], що наведені у списку використаних джерел.

РОЗДІЛ 2
ДІАГНОСТИКА СТАНУ СТРАТЕГІЧНОГО УПРАВЛІННЯ ПІДПРИЄМСТВАМИ ТА ДОСЯГНУТОГО НИМИ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ

2.1. Характеристика методичних підходів до розробки стратегій для сучасних підприємств: вітчизняний та зарубіжний досвід

Розробка стратегії для підприємства – це складний процес, який реалізується у межах управління ним та потребує значного масиву релевантної, достовірної та повної інформації, яка ґрунтується на ретроспективному аналізі його діяльності та на планових показниках, які менеджменту хотілося б досягти у майбутньому. У сучасній Україні процедура стратеготворення суттєво ускладнюється високим рівнем невизначеності та ризиків, які не дають можливості коректно прогнозувати фактори зовнішнього та внутрішнього середовища, що чинять вплив на фінансово-господарський стан підприємства.

В залежності від того, який вид стратегії розробляється, її творцям необхідно обрати методи та інструменти, якими варто послуговуватись у цьому процесі [137]. Вітчизняними дослідниками пропонується чималий арсенал методологічних прийомів, що можуть стати в нагоді фахівцям, задіяним у механізмі стратегічного менеджменту суб'єкта господарювання. До прикладу, Степанова О. В., Степанова Н. С. пропонують універсальний методичний підхід до формування та оцінки стратегії підприємства [138], Чуприна Х., Ніколайко Д., Гуляєв Д., Якимчук Т. визначають наукові підходи та методологічні засади розробки стратегій модернізації підприємств [139], Балюк Ю. С. опікується питанням методичного забезпечення формування стратегії розвитку експортно-імпортної діяльності підприємств [140], Петченко М. В. систематизує методологічні підходи до стратегізації розвитку інноваційних екосистем авіатранспортних підприємств [141], Олешко О. В., Дзюба О. М. узагальнюють методичні аспекти удосконалення формування

інноваційної стратегії підприємств [142], а Терещенко С. І., В'юненко О. Б. фокусуються на методологічних засадах впровадження хмарних технологій у процес розробки та реалізації антикризової стратегії підприємства під час воєнного стану [143].

Керуючись результатами аналізу спеціалізованої економічної літератури, можна дійти висновку, що у сучасній науковій думці простежується кілька традиційних підходів, у межах яких використовується певний набір методів для розробки стратегій. Це ресурсний підхід, при обранні якого стратегія підприємства будується на основі його унікальних внутрішніх перевагах і особливостях, що вирізняють його на ринку; ринковий (або позиційний) підхід, який передбачає побудову стратегії, сфокусованої на пошуку вигідної ніші на ринку на підставі результатів аналізу зовнішнього середовища підприємства; ціннісний (антропоцентричний) підхід, за якого у фокусі стратегії перебуває потенціал створення підприємством цінності для споживача та суспільства (у формі продукту або послуги, що матимуть набір споживчих цінностей); адаптивний (гнучкий) підхід, який характеризується побудовою стратегії підприємства на підвалинах використання гнучкого проєктного управління та сценарного планування в умовах високої невизначеності (стратегія – як проєкт функціонування, розвитку, диверсифікації, цифровізації або іншого напряму підприємницької діяльності).

У розвинутих країнах світу полярності набувають інноваційні методи розроблення стратегій. Наприклад, існує класифікація підходів до стратегування, у якій підприємство порівнюється з кораблем, що виходить в океан (аналогія до зовнішнього середовища ведення бізнесу, ринку, на який входить суб'єкт господарювання). У залежності від стану та тенденцій бажаної ринкової ніші, менеджмент компанії може обрати: стратегію Блакитного океану – тобто інноваційну діяльність, яка передбачає створення нових ринків для реалізації власних товарів або послуг, де немає конкуренції; стратегію Червоного океану, продовжуючи працювати на традиційних ринках з високим рівнем конкуренції, намагаючись здобути нові конкурентні переваги за рахунок

цінової переваги та вирізнити свій товар серед наявних аналогів параметрами якості або споживчими властивостями; стратегію Фіолетового океану, яка поєднує елементи червоного та блакитного океанів, і суть якої криється у запровадженні інноваційних підходів для оновлення характеристик товарів або сервісів (елементи блакитного океану), що дозволить обійти конкурентів у гонитві за клієнтами та перемогти їх у традиційних сегментах ринку (елементи червоного океану); стратегію Чорного океану, що характеризується найвищим поміж існуючих стратегій рівнем ризику для підприємства, та націлена на його економічне виживання в умовах екстремальної кризи, тотальної корупції, тощо, і допускає використання неетичних методів конкурентної боротьби (рейдерство, монополізація через непотизм), тощо. Позитивною рисою цієї стратегії є її антикризові інструменти, що робить доцільним розгляд можливостей її використання у видозміненому форматі для вітчизняних компаній, зважаючи на реалії воєнного часу. Також усе більшої популярності у світі набуває стратегія Зеленого океану, що орієнтує діяльність підприємства на екологічність та слідування цілям сталого розвитку, та має на меті здобуття ним стратегічних конкурентних переваг завдяки турботі про екологічність продукції та її відповідності високим стандартам якості. Ця стратегія має ряд спільних рис зі стратегією Білого океану, у якій місія підприємства нерозривно пов’язана з питаннями моралі, духовності та орієнтації на суспільне благо, а метою ведення бізнесу є покращення світу у тій чи іншій формі, для чого і використовується прибуток, який отримує компанія від своєї діяльності. Важливим елементом успіху під час обрання такої стратегії є створення підприємством соціально орієнтованого іміджу та бренду, який має високий рівень довіри, популярність та безумовну підтримку суспільства.

Підприємства, що прагнуть сформувати або підвищити попит на свою продукцію завдяки емпатії споживачів, чи планують розвиватись у специфічних сегментах ринку, орієнтованих на турботу про людей, тварин, оточення, тощо, можуть обрати для себе стратегію Рожевого океану, метою якої є побудова глибокого емоційного зв’язку з клієнтами та партнерами. Ця

стратегія базується на методології «економіки співчуття» та емоційного маркетингу [137].

У табл. 2.1 узагальнено особливості «океанічних» стратегій та можливості їх використання в Україні.

У традиційних галузях найбільш поширеними в Україні є стратегії Червоного океану. Саме вони характеризуються мінімальними ризиками, що приваблює менеджерів, і є оптимальними для підтримання достатнього рівня економічної безпеки за умови наявності ресурсів для агресивної боротьби з конкурентами за уподобання клієнтів і за партнерів, готових запропонувати кращі умови співпраці. Однак, для сталого розвитку вітчизняних підприємств із перерахованих стратегій найбільш актуальними та доцільними для запровадження такі, як стратегія Червоного океану (з огляду на кількість учасників у більшості сегментів традиційних ринків і їх постійне збільшення за рахунок представництва суб'єктів господарювання із країн ЄС) та стратегія Рожевого океану, що може виявитись дієвою у реаліях воєнного часу, які спонукають людей до співпраці, єднання, емпатичного ставлення до ближніх і взаємодопомоги. Загалом на практиці варто поєднувати окремі елементи кількох стратегій для створення саме такої моделі, що якнайкраще відповідатиме інтересам підприємства та поточному стану ринку, на якому воно знаходиться. Вітчизняним суб'єктам господарської діяльності, які прагнуть подолати кризові тенденції та розширити свій вплив на внутрішньому та зовнішньому ринках, актуальною може стати комбінація методів стратегії Фіолетового океану (у частині запровадження інновацій на існуючих ринках і здобуття уваги клієнтів за допомогою нестандартних сервісних практик) і методів стратегії Зеленого океану (у частині забезпечення відповідності продукції стандартам ЄС, що дозволить розширити вплив на зарубіжних ринках). Такий підхід дозволить поступово відновлювати та зміцнювати конкурентоспроможність підприємства, без тривалого та ресурсно затратного очікування його менеджментом ідеальних умов для розроблення «чистої» моделі стратегії Блакитного океану [137].

Таблиця 2.1. – Стратегії «кольорових океанів» та можливості їх використання вітчизняними підприємствами

Назва стратегії	Характерні особливості стартегії	Приклади використання	Можливості використання в Україні
«Синій океан»	Створення власного нового ринку без конкуренції для інноваційного продукту; прагнення монополії	Cirque du Soleil – поєднання циркового та театрального шоу; Apple – створення нових продуктів	Актуальна для ІТ-компаній, компаній-єдинорогів, підприємств із креативних індустрій, стартапів; дає можливість виходу на наднаціональні ринки
«Червоний океан»	Жорстка конкурентна боротьба на традиційному ринку існуючий попит; цінова конкуренція	Боротьба компаній Coca-Cola та PepsiCo, Airbus та Boeing, Apple та Samsung, Nike та Adidas, McDonald's та Burger King	Ця стратегія уже активно використовується для традиційних галузей України (Нова Пошта і Укрпошта, Rozetka і Epicentr, АТБ і Сільпо, Київстар і Vodafone Україна)
«Білий океан»	Використання нових підходів до ведення бізнесу завдяки партнерствам і кооперації; ефект від синергії підприємницьких зусиль	Tesla (стратегія використана для відкриття патентів для розвитку екосистеми електромобілів)	Використання стратегії є перспективним для технопарків, кластерів, суб'єктів державно-приватного партнерства, критичної інфраструктури і може суттєво пришвидшити відбудову економіки
«Блакитний океан»	Активне використання цифрових інновації; створення діджитал-платформ і екосистем	Amazon, Google, Marvel, Airbnb, Nintendo Wii	Доцільна для використання у сенментах ІТ, цифрових сервісів, для просування послуг цифрового уряду та фінансового обслуговування)
«Зелений океан»	Орієнтація на екологічність і сталий розвиток (ESG-стратегія)	IKEA, Tesla (екологічність, соціальна орієнтація)	Актуальна для енергетичних компаній, підприємств аграрного сектору
«Чорний океан»	Націлена на діяльність у кризових умовах або у періоди ризиків для виживання бізнесу	Активне використання під час пандемії COVID-19 та воєнних дій (релокація бізнесу)	Рекомендована для українських підприємств у воєнний час з метою економічного виживання та адаптації до ризиків
«Сірий океан»	Придатна для нових ринків без жорсткої конкурентної боротьби і для традиційних ринків за умови модернізації	IBM, Miele, Toyota,	Частково використовується в Україні (ПрАТ «МХП»), однак, вимагає від менеджменту переходу до інноваційних стратегій і адаптації
«Фіолетовий океан»	Поєднання конкуренції та співпраці у окремих напрямах діяльності	Samsung і Apple (співпраця для виробництва компонентів продукції)	Перспективна для кластерних моделей, ІТ-компаній та суб'єктів промислових екосистем і технопарків
«Золотий океан»	Орієнтація на високі доходи та інновації	LVMH – люксовий сегмент брендів	Актуальна для нішевих і крафтових українських брендів

Джерело: складено автором за даними [144-148]

Одним із найбільш перспективних напрямів Кравченко А.О., Кузнецова С.О. вважають адаптивне стратегічне управління, що поєднує переваги ситуативного менеджменту, сценарного прогнозування та принципів децентралізації прийняття рішень [149, с.198]. Дослідниці розвивають авторський підхід до реалізації адаптивного стратегічного управління інвестиційною діяльністю підприємства, який, на нашу думку, може бути використаним і для управління цифровими ризиками економічної безпеки. Пропонований алгоритм об'єднує три плошини управлінських дій: діагностику середовища та передумов для інвестицій (моніторинг зовнішнього середовища та генерацію альтернативних стратегій), розробку та вибір адаптивної інвестиційної стратегії (моніторинг реалізації та зворотний зв'язок, реалізацію стратегії, оцінку ефективності та стійкості та формування сценаріїв) та реалізацію та коригування стратегії (вибір адаптивної стратегії, оцінку турбулентності) [149, с.201].

Коваленко О. С. зазначає, що прийняття рішення – у тому числі щодо того, яку стратегію обрати – являє собою свідомий вибір серед варіантів, що існують, або альтернатив напряму дій, що скорочують розрив між теперішнім часом і майбутнім бажаним станом організації [150, с.97]. Саме з рішення розробити, оновити, змінити стратегію діяльності підприємства розпочинається новий цикл стратегічного менеджменту компанії. Чичун В. А., конкретизуючи методологічні аспекти розробки корпоративних стратегій, пропонує таку послідовність розробки та реалізації корпоративної стратегії підприємства (тобто такої стратегії, що визначає основні напрямки діяльності, такі комбінації стратегічних одиниць бізнесу підприємства, в яких воно буде намагатися досягти своїх цілей):

– обрання конкретної стратегії та стратегічних орієнтирів для набуття підприємством конкурентних переваг у довгостроковій перспективі;

– розроблення стратегії підтримання та забезпечення конкурентоспроможності підприємства, в якій будуть поєднані довгострокові плани та програми управлінських дій за усіма функціональними напрямками

діяльності підприємства; реалізація таких програм має забезпечувати формування стійких і довгострокових конкурентних переваг бізнесу попри можливі прояви ризиків і загроз;

– використання «підстратегій» для фокусування конкурентної поведінки у залежності від ситуації на ринках та із врахуванням визначених на попередніх етапах стратегії особливостей забезпечення та утримання конкурентних позицій підприємства;

– реалізація обраної стратегії, яка має супроводжуватися періодичним оцінюванням і комплексним аналізом досягнутих результатів, конкретизацією та ідентифікацію відхилень від стратегічних орієнтирів і запланованих показників, і швидкою управлінської реакцією на непрогнозовані ризики та зміни зовнішніх і внутрішніх умов функціонування бізнесу [151, с.220].

Обранню стратегії підприємства у методичній площині має передувати етап стратегічного аналізу середовища, у якому воно опинилося у конкретний момент часу та оцінка чинників, які ініціюватимуть його зміни у майбутньому. Науменко М. О. та Луханіна К. Д. пропонують таку поетапну процедуру стратегічного аналізу стійкості економічного становища підприємства:

1) виявлення негативних факторів зовнішнього середовища;

2) визначення можливих негативних подій;

3) визначення ймовірності виникнення кожної негативної події;

4) оцінка можливих наслідків реалізації негативних подій [152, с.190].

Дослідниці відзначають, що при аналізі впливу факторів зовнішнього середовища на стійкість підприємства в координатах «вірогідність події/інтенсивність впливу» можна виділити чотири можливі стани підприємства, у відповідності до яких варто обирати конкретну стратегію його подальшого розвитку: стабільний стан, відносно стабільний стан, нестабільний стан, відносно нестабільний стан. Описані стани ідентифікуються та опрацьовуються за методикою картографування, формуючи чотири квадранти. При аналізі негативних подій середовища, що мають серйозні наслідки для підприємства, доцільно використати методи класифікації можливих ризиків, їх

ранжування, і визначити найважливіші напрямки ризик-менеджменту для забезпечення сталого розвитку підприємства [152, с.190].

Анісімова О. М., Шикова Л. В. пропонуть SWOT-аналіз підприємства як метод забезпечення розробки ефективної стратегії управління [153]. Виходячи з загального SWOT-аналізу, тобто після ідентифікації сильних і слабких сторін діяльності суб'єкта господарювання (S – Strengths, W – Weaknesses), його можливостей і загроз для їх реалізації (O – Opportunities, T – Threats), топ-менеджери, відповідальні за розробку та реалізацію стратегії підприємства, здатні сформувати матрицю, яка дозволить формалізувати та обрати конкретні стратегії для розвитку або стабілізації стану бізнесу, що дозволять втілити існуючі можливості за рахунок сильних сторін, та уникнути можливих загроз за рахунок подолання слабких сторін [153, с.28].

У методичній площині використання матриці SWOT-аналізу для стратеготворення у вітчизняній практиці стратегічного менеджменту доцільне у наступному форматі. При розробці матриці експерти отримують чотири поля (квадранти): «СІМ» (сила і можливість – SO); СІЗ (сила і загрози – ST); «СЛМ» (слабкість і можливість – WO); «СЛЗ» (слабкість і загрози – WT).

Для квадранту «СІМ» необхідно розробляти стратегію по використанню сильних сторін підприємства, для того щоб отримати віддачу від можливостей які виникають у зовнішньому середовищі. Для квадранту «СЛМ» стратегія повинна бути спрямована на подолання слабких сторін підприємства за рахунок існуючих можливостей. У квадранті «СІЗ» стратегія повинна бути спрямована на використання сильних сторін підприємства для уникнення У квадранті «СЛЗ» підприємство повинно використовувати стратегію подолання слабких сторін та уникнення можливих загроз [153, с.28-29].

Для визначення та ідентифікації загроз, джерелом яких є зовнішнє середовище, Палига Є.М., Бурда І.Я. пропонують скористатися таким методичним інструментом, як PEST-аналіз (P (Political) – політичні чинники, E (Economic) – економічні чинники, S (Social) – соціальні (соціокультурні) чинники, T (Technological) – технологічні чинники) [154, с.294]. У зарубіжній

практиці цей метод стратегічного аналізу отримав багато доповнень і еволюціонував у різні формати. Зокрема, активно використовуються такі його варіанти, як PESTEL/PESTLE-аналіз, де додатково визначаються L (Legal) – правові чинники та E (Environmental/Ecological) – екологічні чинники; STEEPLE: до вищезгаданих додаються ще й E (Ethical) – етичні чинники; SLEPT: варіант аналізу, що поєднує соціальні, правові, економічні, політичні та технологічні чинники; DESTEP: додається D (Demographic) – домографічні чинники (актуально для сучасної України) та PESTLIED: найбільш розширений варіант, що поєднує політичні, економічні, соціальні, технологічні, правові, міжнародні, екологічні та демографічні чинники.

Для вибору стратегії розвитку підприємств Цимбал С.В. пропонує використовувати метод імітаційного моделювання, що проводиться шляхом відтворення подій, які відбуваються одночасно або послідовно в модельному часі. Основне завдання при розробці імітаційної моделі вибору оптимальної стратегії розвитку підприємств зводиться до визначення максимального прибутку, який слід очікувати від її реалізації при обмежених інвестиціях [155, с.199].

У контексті цього дослідження пропонується розглянути ще три методичні підходи, які оформились у діяльності зарубіжних компаній, і використовуються для потреб їх стратегічного менеджменту. Це: збалансована система показників (Balanced Scorecard, BSC), яка дозволяє «розкласти» корпоративну стратегію підприємства на конкретні KPI, за досягненням яких можна визначити її успіх або невдачу та своєчасно внести необхідні корективи; Hoshin Kanri – японський метод стратегічного менеджменту, що у перекладі означає «управління вектором» або «компас менеджменту» і являє собою стратегічну методологію, яка забезпечує повну узгодженість цілей підприємства, закладених у його стратегії із щоденними завданнями та діями кожного працівника (тактичним рівнем менеджменту) та цифрові стратегії, які базуються на використанні методів аналізу великих масивів даних для ефективного планування стратегічних орієнтирів підприємства.

BSC – це система стратегічного менеджменту, авторами якої є Роберт Каплан та Девід Нортон. Вона використовується для того, аби трансформувати місію підприємства та його стратегію функціонування і розвитку у набір конкретних показників, бажані значення яких можна досягнути у процесі стратегічного менеджменту організації. BSC є сучасним управлінським інструментом, який здатен пов'язати абстрактні стратегічні орієнтири діяльності компаній, їх глобальні цілі, із щоденними завданнями та результатами бізнес-процесів, з продуктивністю праці управлінського персоналу та працівників, які виконують прийняті ними рішення. Використання цього методу на прикладному рівні дозволяє покращити систему моніторингу та контролю за перебігом етапів реалізації стратегії, своєчасно ідентифікувати стратегічні ризики та оперативно відреагувати на них. Досяжність або недосяжність запланованих показників, відставання від графіку або його випередження є індикаторами (червоними прапорами) для адаптації стратегії до мінливих економічних обставин.

Класична модель BSC будується на ідентифікації та візуалізації для виконавців стратегічних цілей бізнесу з чотирьох взаємопов'язаних кутів зору: фінансовому, клієнтському, внутрішньому баченні та навчанні і розвитку бізнесу.

Фінансова складова покликана ідентифікувати, як підприємство та його діяльність сприймаються акціонерами та стейкхолдерами. Цей аспект потребує планування та розрахунку фінансових індикаторів стану суб'єкта господарювання. Змістовно та суттєво цей компонент найбільш пов'язаний зі станом економічної безпеки підприємства, що робить метод BSC придатним для застосування з метою реалізації стратегічного безпеко орієнтованого менеджменту компанії.

Клієнтська складова методу BSC націлена на справлення якнайкращого враження від діяльності суб'єкта господарювання на його клієнтів. Вимірниками успіху реалізації стратегії у межах цієї складової можуть бути:

частка ринку, яку вдалося зайняти підприємству, рівень задоволеності клієнтів продукцією та сервісами та рівень їх лояльності.

Внутрішні бізнес-процеси підприємства оцінюється для того, аби творці та реалізатори стратегії змогли усвідомити, наскільки раціональним та ефективним є управління компанією, які саме вміння та навики роблять її менеджмент унікальним та дозволяють їй досягти нових конкурентних переваг. Індикаторами оцінювання цього сегменту можна обрати якість управлінських рішень, тривалість циклу прийняття рішення, тривалість виробничого циклу та рівень запровадження інновацій, які позитивно впливають на якість товарів і послуг.

Четвертий названий компонент – навчання та розвиток – сфокусований на можливостях підприємства еволюціонувати, вдосконалюватися та покращувати результати своєї діяльності. Його можна оцінити за станом наявного у суб'єкта господарювання інтелектуального капіталу, досягнутим рівнем корпоративної культури та функціональною здатністю ІТ-системи, а також рівнем захисту корпоративних ресурсів від цифрових загроз і зовнішніх кібернетичних втручань.

Основою досліджуваного методу є процес каскадування, тобто розбиття масштабних стратегічних цілей найвищого управлінського рівня на конкретні функціональні завдання для підрозділів та окремих працівників. Саме елемент каскадування визначає особливість цього методу стратегічного управління. Так, на першому рівні каскадування формується корпоративна стратегічна карта підприємства, до якої входять стратегічні цілі розвитку бізнесу. На другому рівні містяться стратегічні карти функціональних підрозділів та департаментів. Кожен структурний підрозділ у організаційній структурі суб'єкта господарювання має зробити свій внесок у фінальний результат реалізації стратегії. На третьому рівні встановлюється командні та індивідуальні KPI. Саме на цьому рівні найкраще простежується, як стратегічні цілі підприємства перетворюються на вимірювані показники, які можна розрахувати та проаналізувати. Перевагою цього методу є конкретика, а також чіткий розподіл

відповідальності між виконавцями на різних рівнях управлінських системи. Метод BSC у стратегічному управлінні сучасними підприємствами дозволяє подолати крихкість світу BANI, оскільки не дає менеджменту компанії сфокусуватися лише на отриманні прибутку та фінансових показниках, а демонструє потребу комплексної взаємодії людського та матеріального капіталів.

Hoshin Kanri – основна відмінність цього методу від класичного директивного стратегічного управління підприємством – це процес, який отримав назву «гра в м'яч» (catchball). Його суть полягає у тому, що стратегічні цілі, яких компанія прагне досягти, не просто «спускаються» до виконавців з верхніх рівнів менеджменту, а відбувається «пас цілі» – керівництво «кидає м'яч» (стратегічну ціль) підлеглим, які піддають її аналізу, пропонують власні тактичні рішення, спираючись на досвід, наявні можливості, тощо, та «кидають м'яч» назад із зробленими уточненнями та оформленими пропозиціями. Такий підхід створює двосторонній зв'язок, сприяє оперативній комунікації, прозорості стратегічного управління і забезпечує реалістичність стратегічних планів.

Реалізація методу Hoshin Kanri на практиці передбачає п'ять етапів. На першому етапі розробляється візія діяльності компанії на перспективу та визначається довгостроковий курс руху її подальшого розвитку для досягнення бажаного стану у майбутньому не залежно від того, як тенденції світу BANI можуть вплинути на цей процес. На другому етапі відбувається розробка конкретних проривних цілей діяльності підприємства. Наприклад, це можуть бути дві-три стратегічно важливі цілі на рік, досяжність яких оцінюється конкретними цифровими показниками. На третьому етапі відбуваються конкретизація та уточнення встановлених цілей із використанням спеціальної Х-матриці. Цей аналітичний інструмент використовується для того, аби візуалізувати причинно-наслідкові зв'язки між стратегією, тактикою та результатами діяльності підприємства. На четвертому етапі відбувається реалізація стратегії у різних відділах та підрозділах підприємства. П'ятий етап

передбачає проведення щомісячного та щорічного моніторингу досяжності поставлених цілей та контроль за відхиленнями.

Метод побудови Х-матриці полягає у наступному (Додаток В) [156]. Формується карта, на якій відмічаються чотири сторони світу. В результаті, у компактному форматі, на одному аркуші паперу об'єднуються довгострокові цілі та орієнтири діяльності підприємства, які позначають південь, річні цілі, які асоціюються із заходом, пріоритетні проєкти та тактики, що розуміються як північ на карті, та показники ефективності реалізації стратегії у формі KPI відповідальних осіб, які відображають схід.

Порівняно з методом встановлення OKR (Objectives and Key Results) для оцінки стратегічних цілей підприємства, метод Hoshin Kanri виглядає більш системним і довгостроковим. OKR частіше фокусується квартальних цілях бізнесу, а Hoshin – на цілісності усієї системи стратегічного управління у взаємозв'язку та взаємозалежності з іншими напрямами менеджменту організацій.

У порівнянні з описаним вище методом BSC, Hoshin Kanri є інструментом виконання стратегії і досяжності стратегічних цілей, у той час, як BSC використовується як засіб вимірювання успіху стратегії. Використання цих двох методів у комплексі здатне забезпечити синергетичний ефект для стратегічного менеджменту підприємства.

Переваги використання методу Hoshin Kanri у реаліях світу BANI криються у здатності знизити рівень незрозумілості для виконавців стратегічних рішень, адже завдяки використанню прийому каскадування складні глобальні виклики перетворюються на зрозумілі поетапні завдання для кожного відділу. Х-матриця є зручним засобом візуалізації логіки реалізації стратегії, і тим інструментом, що може передаватись каналами цифрової комунікації від менеджменту до виконавців. З позиції забезпечення економічної безпеки підприємства, метод Hoshin Kanri мінімізує ризик «розсинхронізації» управлінських і виконавчих дій, що є критично важливим для стійкості підприємства в умовах пермакризи та ризиків воєнного часу.

Методика розробки цифрових стратегій у зарубіжній практиці стратегічного менеджменту демонструє поступовий перехід від «планування результату» до «проєктування спроможності» його досягнути. Тобто, зазвичай стратегами розробляється не конкретний план управлінських дій, а система (алгоритми, дані, ресурси), яка зможе згенерувати правильну реакцію на будь-який непередбачуваний виклик світу BANI.

Розробка цифрової стратегії із використанням моделей Gartner, McKinsey в цілому базується на методі оцінки цифрової зрілості компанії (Digital Maturity Assessment). На першому етапі розроблення такої стратегії відбувається конкретизація цифрового вектора діяльності підприємства. Зокрема, важливим елементом цього процесу є аудит цифрового розриву, тобто визначення різниці між поточним станом цифрової інфраструктури компанії та цільовими орієнтирами її інтеграції у цифровий економічний простір. Визначення стратегічних орієнтирів у межах цифрових стратегії розвитку підприємства передбачає відсутність фіксованих планів, наприклад, на період 10 і більше років, їх заміщення цифровим показником, який можна виміряти, що характеризує рівень цифрового розвитку бізнесу (наприклад, частка автоматизованих бізнес-процесів за 1, 2, 3 рік і так далі). Характерними елементом цифрової стратегії є моделювання різних сценаріїв розвитку підприємства. Для забезпечення достовірності важливим є використання логічного аналізу, який досліджувався у першому розділі цієї роботи. Завершується описаний етап обранням конкретної архітектури для прийняття управлінських рішень щодо цифровізації бізнес-процесів.

Другий етап – реалізація цифрової стратегії являє собою ітераційний управлінський процес, який у зарубіжних компаніях часто виконується із застосуванням методики гнучкого стратегічного планування. Під час реалізації цифрової стратегії відбувається створення Data-платформи, яка дозволяє організувати збір, аналіз і збереження розрізнених даних (фінансових, кадрових, виробничих). Не менш важливим є і запровадження алгоритмів підтримки рішень (DSS) через використання засобів прогнозної аналітики.

Використання штучного інтелекту дозволить менеджеру отримати сигнал про критичне зниження фінансової безпеки (або будь-який інший ризик) до того, як це відобразиться у офіційних звітах компанії.

Цифрові стратегії будуються із використанням методичних підходів, притаманних і для інших варіантів стратеготворення. Зокрема, каскадування через застосування OKR дозволяє відійти від жорсткого планування KPI. В цілому, цифрові стратегії реалізуються через гнучкі цілі, які переглядаються щокварталу або частіше за потреби.

Цифрова стратегія не забезпечить бажаного ефекту для підприємства, якщо культура організації залишиться незмінною. Управління змінами та подолання опору їм з боку працівників має відбуватися через розвиток інтелектуального капіталу компанії, через навчання персоналу роботі з новими інструментами, підвищення рівня їх професійної цифрової грамотності.

У реаліях світу BANI вітчизняним підприємствам буде складно розробити ідеальну цифрову стратегію відразу. З огляду на це, стратегія MVP (Minimum Viable Strategy), яка передбачає запуск невеликих цифрових проєктів (пілотів), їх тестування та подальше масштабування для охоплення усіх бізнес-процесів може бути ефективним варіантом цифровізації стратегічного менеджменту українського бізнесу. У площині управління економічною безпекою, реалізація цифрових стратегій обов’язково повинна передбачати напрям забезпечення кібербезпеки. Безпека інформації та особистих даних має бути невід’ємною складовою загальної стратегії економічної безпеки підприємства в умовах невизначеності та диверсифікації цифрових ризиків.

Специфіка вітчизняного досвіду щодо розвитку методик стратегічного управління підприємствами розкривається у публікаціях таких сучасних вчених, як Балан В. Г., що пропонує методи нечіткого багатокритерійного аналізу у формуванні нової парадигми стратегічного управління підприємствами [157] та дає рекомендації щодо оцінювання стратегічних наборів підприємства з використанням Fuzzy CODAS-методу [158], Грищенко С. І., що вивчає методичні положення формування фінансової

стратегії сталого розвитку підприємства [159], Дем'яненко Т. І., Яковенко І. С., які пропонують використовувати реінжиніринг бізнес-процесів як сучасний метод управління стратегічними змінами на підприємстві [160], Дикань В. Л., Кузнецов Є. М., що узагальнюють методичне забезпечення формування стратегії сталого розвитку суб'єктів господарювання [161], Овсієнко Н. В., Котвицька Н. М., Овсієнко В. В., які доповнюють методичні підходи до створення стратегії управління ризиками сучасних підприємств [162], Олійник Т. І., Сапожніков Н. М., що формалізують методологічні основи у формуванні адаптивної стратегії підприємницького середовища [163], Польова О. Л., Бігун В. С., Савицький О. А., що критично переглядають методичні підходи розробки економічної стратегії управління підприємством [164], Турило А. М., Турило А. А., Короленко Р. В., які описують методологію наукових досліджень в аспекті загальної і фінансової стратегії підприємства [165], Філіна С. В., Дрига О. В., Кужель О. В., що коцептуалізують теоретичні та методичні аспекти стратегії розвитку сучасних бізнес-структур [166], Янгулов Е. П., який надає теоретичне обґрунтування методологічних основ моделі стратегічного управління для малих підприємств [167]. На особливу увагу у контексті цього дослідження заслуговують публікації таких дослідників, Самойленко В. В., у яких дається авторська оцінка методів стратегічного управління бізнес-процесами підприємства в період цифровізації [168] та Сироїд Т. І., що пропонує методологічні підходи до формування та реалізації інвестиційно-інноваційної стратегії підприємства в умовах діджиталізації [169]. Загалом, праці В. Г. Балана [157, 158] засвідчують можливість використання нечітких множин для математичної формалізації «незрозумілості», якою сповнений світ BANI. Такий методичний підхід дозволяє перетворити суб’єктивні судження експертів, які часто використовуються як під час розроблення стратегій, так і для оцінювання рівня їх ефективності, у об’єктивні дані, придатні для прийняття стратегічних управлінських рішень. Також роботи сучасних українських вчених [160, 162] розкривають механізми реінжинірингу та формування адаптивних стратегій, що

підкріплює авторську ідею про стратегічне управління як «адаптивний фільтр» змін в організації на довгостроковому часовому горизонті. У свою чергу, дослідження [168, 169] дають аргументи на користь тісного зв'язку сучасних методів стратегічного управління з технологічними трансформаціями діяльності підприємницьких структур.

Контент-аналіз цих і інших дослідницьких матеріалів, дає змогу виокремити кілька фундаментальних напрямів, за якими відбувається розвиток методичних підвалин стратегічного управління сучасними вітчизняними підприємствами в умовах невизначеності та ризиків:

– спроби адаптації теорії стратегічного менеджменту до турбулентних реалій економічного простору, світу BANI та пермакризи;

– фокусування орієнтирів функціонування бізнесу на стратегіях економічного виживання та релокації в умовах війни для пошуку оптимальних умов для сталого перспективного розвитку;

– врахування ролі GR (взаємодії бізнесу з органами влади) для врахування воєнно-політичних ризиків у економічних стратегіях і для отримання інформаційної та матеріальної підтримки підприємницьких ініціатив;

– запровадження у практиці стратегічного менеджменту інтуїтивне стратегування, тобто методики, за якої серед управлінських рішень спостергається висока частка таких рішень, що приймаються власниками та топ-менеджментом на основі власного експертного досвіду, а не детальних розрахунків і інструментів економіко-математичного моделювання (через відсутність релевантних даних, особливо у воєнний час).

– слідування тенденціям процесу євроінтеграції вітчизняного бізнесу у зовнішні ринки та конвергенції цілей існування українських підприємств з європейськими цінностями, що формує сталу та нагальну вимогу підлаштовувати підприємницькі стратегії під стандарти якості та сертифікаційні вимоги країн ЄС.

У табл. 2.2 узагальнено методики розробки стратегій для підприємств, що набули популярності в Україні та в світі.

Таблиця 2.2. – Методики розробки стратегій для підприємств, що набули популярності в Україні та в світі

Метод	Сутність підходу	Вітчизняний досвід	Зарубіжний досвід
Класичний метод стратегічного планування	Конкретизація перспективних цілей і розроблення довгострокових планів розвитку підприємства з конкретними показниками	Широко застосовується підприємствами; які орієнтовані на стабільні ринкові позиції у традиційних сегментах	Застосовується у традиційних галузях, але дедалі частіше трансформовується у гнучкі моделі стратегічного управління
Конкурентний метод	Передбачає досягнення конкурентних переваг завдяки аналізу поведінки клієнтів і переваг конкурентів, а також власних сильних і слабких сторін, загроз і можливостей.	Використовується переважно великими компаніями, які є флагманами на ринку та можуть вести конкурентну боротьбу тривалий час, витрачаючи ресурси	Активно застосовується (модель Портера, п'ять сил); передбачає глибокий галузевий аналіз для встановлення ніш для конкурентних переваг
Ресурсний метод	Активне використання та розвиток внутрішніх ресурсів і компетенцій людського капіталу як джерел стратегічних переваг для бізнесу	Частково використовується, однак, характеризується недостатньою увагою менеджменту до нематеріальних активів	Широко застосовується у бізнесі; фокус робиться на знаннях, інноваціях, інтелектуальному потенціалі і їх розвитку
Сценарний метод	Розробка кількох альтернативних сценаріїв розвитку довгострокового розвитку підприємства	Використовується обмежено через витрати ресурсів; часто носить формальний характер	Активно використовується для управління в умовах ризиків
Ризик-орієнтований метод	Інтеграція методів ризик-менеджменту у стратегію бізнесу	Популяризується з огляду на реалії воєнного часу	Системно інтегрований в управлінські механізми
Адаптивний (гнучкий) метод	Гнучке стратегічне управління з можливістю швидких змін рішень	Обмежене використання, переважно в ІТ-секторі	Широко використовується як іструмент постійної адаптації
Цифровий метод	Використання цифрових технологій і масивів даних для стратегічних рішень	Використовується, але вимагає ресурсів і підготовки персоналу	Домінуючий сучасний метод, широке використання ШІ
Інноваційний метод (блакитний океан)	Створення інноваційних продуктів і послуг та ринків для їх реалізації або нових ринкових ніш	Починає використовуватись, але застосування обмежене через відсутність необхідних ресурсів	Широко застосовується у інноваційному бізнесі, креативних галузях, ІТ-компаніях
Екосистемний метод	Формування довгострокових бізнес-партнерств	Тільки починає з'являтись у вітчизняному бізнесі	Активна співпраця цифрових платформ і екосистем для бізнесу
Резильєнтний метод	Встановлення мети економічного виживання та відновлювлення	Набуває популярності через зростання воєнних ризиків	Обмежено застосовується у кризові періоди

Джерело: складено автором за даними [137-167]

Рис. 2.1 демонструє комплексний методичний підхід до розробки стратегій для сучасних підприємств в умовах невизначеності та ризиків.

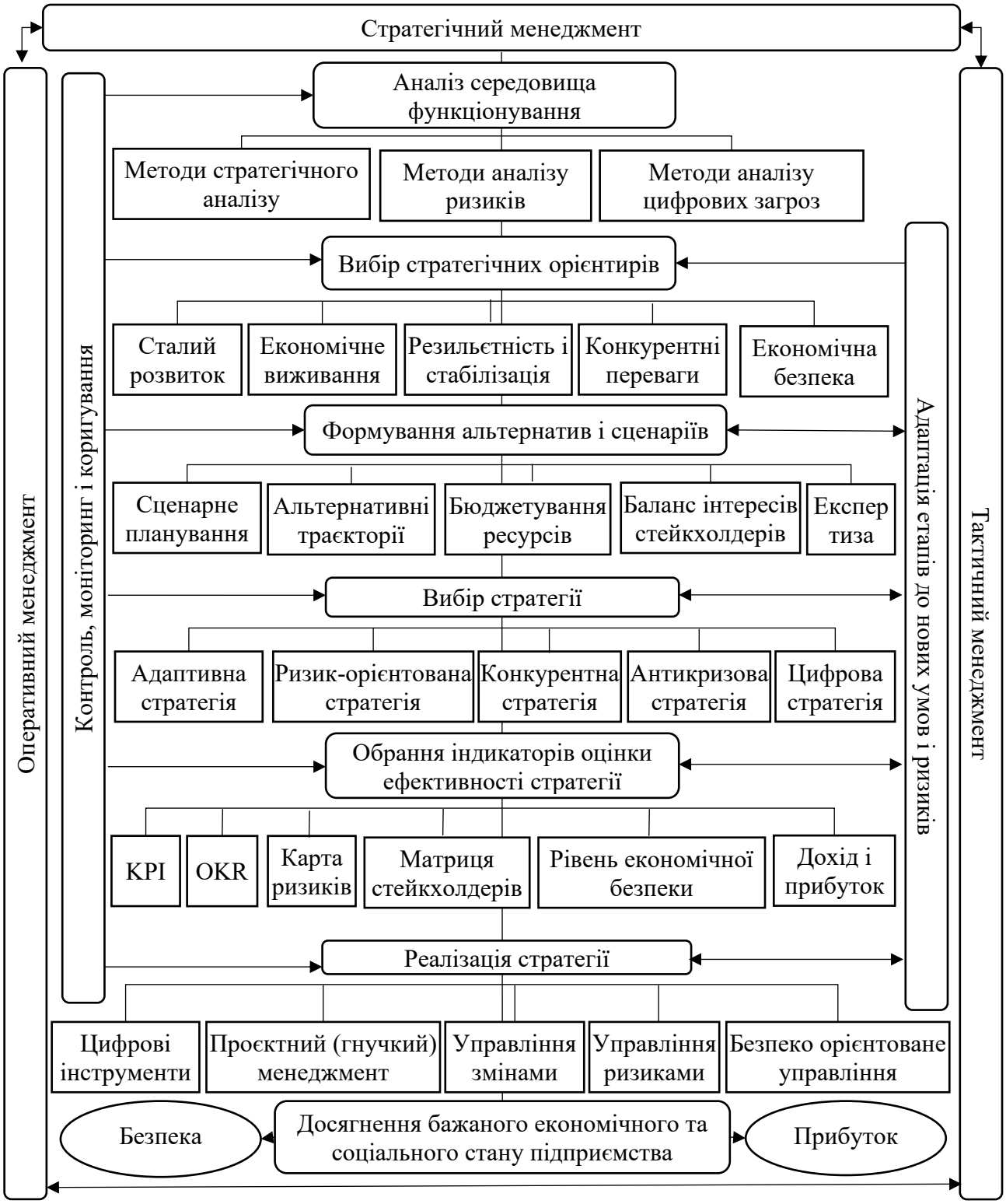


Рисунок 2.1. - Методичний підхід до розробки стратегій для сучасних підприємств в умовах невизначеності та ризиків

Джерело: складено автором

Перевагою запропонованої моделі є її комплексність і всеосяжність, що проявляється у охопленні нею усіх трьох рівнів менеджменту організації – стратегічного, тактичного та оперативного. Це дозволяє встановити взаємозв'язки та відповідальність за реалізацію кожного конкретного завдання (за принципами зарубіжних моделей BSC або Hoshin Kanri). Поєднання методів стратегічного аналізу (PESTEL-аналізу, моделі 5 сил Портера для ідентифікації ризиків і загроз зовнішнього середовища, оцінки конкурентів, тощо, діагностики інтелектуального капіталу та цифрової зрілості через SNW-аналіз, SWOT-аналізу з фокусом на кореляцію між зовнішніми загрозами та внутрішніми вразливостями) у аналітичний фреймворк забезпечує якісне інформаційне охоплення різних напрямів управлінських дій та формує якісне підґрунтя для прийняття управлінських рішень. Розробка мінімум трьох сценаріїв: оптимістичного, песимістичного та реалістичного залишає можливість стратегічного вибору з огляду на мінливість оточення.

На відміну від класичних методичних підходів до розробки та реалізації стратегії, де контроль є завершальним етапом, авторська модель адаптована до умов невизначеності та ризиків завдяки інтеграції контролю і моніторингу у кожен стратегічний етап діяльності підприємства через систему «адаптивних фільтрів». Такий підхід дозволяє трансформувати систему менеджменту організації з лінійної у реактивну, що є критично важливим кроком для економічної стійкості підприємства в умовах воєнних ризиків, непередбачуваності та нелінійності світу BANI.

Таким чином, запропонований метод дозволяє нівелювати «крихкість» системи економічної безпеки сучасних українських підприємств. Завдяки перманентній циклічності процесів аналізу ризиків та контролю результатів, їх стратегії перетворюються з чіткого та безапеляційного документу-плану на динамічну модель економічної поведінки, яка дає змогу суб'єкту господарювання не просто виживати в умовах диверсифікації та посилення ризиків, а й використовувати невизначеність як джерело нових можливостей та ідей для стратегічного розвитку.

2.2. Аналіз впливу цифрових ризиків на стан економічної безпеки підприємства як елемент обґрунтування досяжності його стратегічних цілей

Жодне підприємство в сучасній Україні, що перебуває в умовах воєнної агресії, політичної і соціальної нестабільності, не функціонує у безризикових і стабільних умовах. Відтак, для того, аби планувати свою майбутню фінансово-господарську діяльність, учасники ринкових відносин та їх топ-менеджмент мають орієнтуватися у багатовекторній плеяді ризиків і загроз, які впливають на стан економічної безпеки бізнесу, його конкурентоспроможність, ресурсне забезпечення та перспективи подальшого сталого або інтенсивного розвитку [170, с. 177]. Основною метою управління ризиками на підприємстві дослідники науки менеджменту традиційно вважають забезпечення максимальної ефективності його системи управління та досягнення фінансової стійкості й стабільності, враховуючи стан невизначеності та фактори, що можуть як негативно, так і позитивно вплинути на досягнення головних цілей [171, с.99]. Така мета добре корелює зі стратегічними орієнтирами економічного виживання суб’єктів господарювання в умовах невизначеності світу BANI. Усі без винятку стратегії, які починають розроблятися для впорядкування векторів діяльності підприємств на період 2026-2030 років мають містити змістовий і структурний компоненти, присвячені управління ризиками; а ті стратегічні орієнтири, які були визначені до початку повномасштабного вторгнення або ж із надією топ-менеджерів підприємств щодо швидкого закінчення воєнних дій на території України, мають бути переглянуті та адаптовані під довготривалі тенденції розвитку економіки воєнного часу, нестабільності зовнішнього середовища та дисбалансів ринків товарів і послуг.

Якщо вести мову конкретно про стратегії забезпечення економічної безпеки підприємства як окремий вид функціональних стратегій розвитку бізнесу, то управління ризиками у цьому контексті стає ключовим

управлінським завданням, покликаним гарантувати економічну життєдіяльність суб'єкта господарювання попри постійне масштабування проявів пермакризи та ймовірну появу нових інноваційних видів ризиків, зокрема, таких, що пов'язані з цифровізацією економічних відносин. Таким чином, на теоретико-методологічному рівні ризик-менеджмент може розглядатися як попереджувальна або превентивна складова управління економічною безпекою підприємства, що поєднує усі класичні функції менеджменту організацій, такі як: планування діяльності з управління ризиками, прогнозування ризиків, оцінювання рівня ймовірності їх негативного прояву та сили впливу на результати економічних рішень і бізнес-процеси у компанії; організування системи попередження та мінімізації ризиків; контроль за виконанням безпеко орієнтованих управлінських рішень. Забезпечення реалізації фінансово-економічних інтересів зацікавлених у результатах діяльності підприємства сторін в умовах інтенсивної зміни середовища потребує розробки концептуальних основ стратегічного управління фінансово-економічною безпекою суб'єкта господарювання з урахуванням здобутків сучасних теорій, наукових підходів і концепцій [172, с.243]. Таким чином, ризик-менеджмент для забезпечення економічної безпеки може слугувати ідеологічним фундаментом та інтеграційним вузлом управлінських рішень, спрямованих на те, аби рівень економічної безпеки підприємства залишався стабільно високим впродовж тривалого проміжку часу. Управлінському персоналу українських компаній необхідно визнати, що сучасний ризик-менеджмент – це не окремий управлінський процес, а засіб досягнення та підтримання стану економічної безпеки підприємства, тобто захищеності його корпоративних ресурсів і стабільності їх використання з метою реаліязації місії і цілей бізнесу.

Управління ризиками у системі розробки стратегії забезпечення економічної безпеки – це формування планів і алгоритмів використання набору динамічних засобів ідентифікації, уникнення та нейтралізації внутрішніх і зовнішніх факторів, які можуть порушити захисні бар'єри. Таким чином, концептуально – економічна безпека – це статичний стан підприємства,

позитивна характеристика його економічних показників, а управління ризиками – це динамічний процес досягнення такого стану, що ініціюється з метою адаптації управлінських механізмів до негативних впливів економічного середовища. Оскільки в основі розроблення будь-якої стратегії функціонування, відновлення або розвитку бізнесу лежать управлінські рішення, побудовані на балансі параметрів ризику і вигоди, управління ризиками, а точніше – результати оцінювання можливих збитків від їх наслідків, стають інформаційним ресурсом для обґрунтування вищому керівництву підприємства та його власникам доцільності використання того чи іншого варіанту стратегії при наявності кількох стратегічних сценаріїв та альтернатив.

Для вирішення завдання адаптивної модифікації сучасних стратегії управління підприємствами для протидії інноваційним викликам, можливості механізму ризик-менеджменту дають змогу оперативно скоригувати траєкторію ведення бізнесу, ґрунтуючись на аналізі потенційних майбутніх «точок розриву» економічних показників – планових із реальними. Такий підхід трансформує систему забезпечення економічної безпеки з реактивної, тобто такої, що покликана реагувати на інциденти у зовнішньому та внутрішньому середовищі підприємства, на проактивну, сфокусовану на попередженні таких інцидентів. Отже, можна стверджувати, що управління ризиками у системі менеджменту організацій, у функціональних підсистемах управління економічною безпекою та у стратегіях розвитку економічного потенціалу бізнесу виконує одразу три ролі: це ідентифікація загроз для стану економічної безпеки підприємства, оцінювання ймовірності впливу ризиків на його економічні показники у поточний момент часу (тактичний та оперативний менеджмент) та в майбутньому (стратегічне управління економічною безпекою), а також вибір дії та інструментів нівелювання ризиків та їх наслідків.

Управлінні ризиками складає теоретико-методологічні та практичну основу для функціонування механізму забезпечення економічної безпеки

підприємства, який об’єднує теоретичні орієнтири та категорії безпеко орієнтованого менеджменту з конкретними управлінськими рішеннями у напрямку їх досягнення. Нехтування необхідністю інтеграції принципів ризик-менеджменту у систему стратегічного управління підприємством матиме негативні наслідки для результатів його діяльності та стану економічної безпеки. Ще у довоєнний період, у 2013-2014 рр., вітчизняними дослідниками висувались гіпотези, що ефективне формування стратегії управління економічними ризиками для забезпечення економічної безпеки займає все більш значимі позиції у загальній стратегії управління вітчизняними підприємствами, оскільки на ринку існують досить жорсткі умови конкурентоспроможності, економічна та соціальна нестабільність [171, с.102]. Нині ж вибір того чи іншого методу ризик-менеджменту потребує коригування стратегії підприємства або попереднього оцінювання певних ризиків при її формуванні, адже управління ризиком впливає на стратегію розвитку підприємства та на досяжність обраних цілей [91, с.241]. Відтак, кожне стратегічне рішення щодо забезпечення фінансово-економічної безпеки суб’єкта господарювання має бути розглянуто й оцінено в контексті ризиків його реалізації, а теорію ризиків можна розглядати як наукову основу визначення стратегічних альтернатив та розроблення критеріальної бази їх оцінювання [172, с.242].

Перспективними векторами стратегічного управління ризиками для підтримки високого рівня економічної безпеки підприємницьких структур в теорії може стати розширення меж залучення зовнішніх фахівців для налагодження процесу ризик-менеджменту, формування набору сценаріїв впливу ризиків на стан економічної безпеки компанії на різних часових інтервалах і каталогу управлінських рішень щодо ідентифікації, оцінювання та мінімізації ризиків і наслідків їхнього потенційного впливу на рівень економічної безпеки суб’єкта господарювання [79, с.50]. У свою чергу, нехтування необхідністю адаптації стратегічного менеджменту до потреби забезпечення економічної безпеки бізнесу на прикладному рівні призводять до

того, що підприємство втрачає здатність гнучко пристосовуватись до повсюдних проявів невизначеності та ризиків, і його управління економічною безпекою стає формальним бюрократичним процесом, який не спроможний забезпечити реальний захист корпоративних ресурсів та протидіяти викликам його економічного оточення [170, с.178-181].

Для підприємств України стан їх економічної безпеки є базовою умовою виживання бізнесу у середньостроковій та довгостроковій перспективах. Вміння знаходити можливості та резерви для формування захисних механізмів, здатних протидіяти негативним наслідкам не лише очевидних і традиційних видів ризиків, але і їх новітнім типам, які, поміж іншого, сформовані і фактом поширення цифровізації бізнесу у різних фінансово-господарських площинах, дає компанії не лише стратегічну конкурентну перевагу, але і підґрунтя для стабілізації підприємницької діяльності після пережитих шоків і стресів воєнного часу та форс-мажорних обставин. Своєчасна ідентифікація ризиків ускладнюється тим, що з одного боку на сучасних українських підприємствах бракує фахівців, здатних організувати та реалізувати процеси ризик-менеджменту на високому професійному рівні, а з іншого – перебування суб'єктів підприємницької діяльності одразу у двох «світах» – традиційному економічному середовищі та цифровому просторі – подвоює кількість небезпек, викликів і ризиків, на які має звертати увагу управлінський персонал. Відтак, сучасні стратегії функціонування та розвитку бізнесу мають розроблятися із врахуванням необхідності активної інтеграції бізнесу у цифровий простір, що породжує потребу фахового оцінювання цифрових ризиків для стану економічної безпеки та врахування результатів проведеної аналітичної роботи під час стратеготворення [173, с.10].

На потребі врахування цифрових ризиків під час розроблення стратегій відновлення, масштабування, розвитку, стабілізації бізнесу, наголошують сучасні вітчизняні дослідники проблем менеджменту та безпекознавства у своїх публікаціях. Так, Добровольська В. В., Ляховецький О. О. ідентифікують перешкоди та ризики при впровадженні цифрових технологій у господарську

діяльність [174], Зачосова Н. В., Коваленко А. О., Куценко Д. М. фокусуються на кадрових ризиках, які виникають у процесі економічною безпекою підприємств в умовах цифрових трансформацій бізнесу, пов'язаних із розширенням меж впливу на підприємницьку діяльність тенденцій четвертої промислової революції [175], Демчишак Н. Б., Клек А. Р., Цвєткова З. М. простежують ризиків, які виникають під час інвестиційної діяльності і пов'язані з цифровізацією підприємств [176], Осадча О. О., Роздопченюк В. М. узагальнюють та пропонують назагал власний погляд на ризики економічної безпеки підприємства в умовах цифровізації [177], Світовий О. М., Вилєгжанін С. В. вивчають можливості застосування елементів штучного інтелекту в управлінні ризиками ІТ-проєктів в контексті цифрової трансформації підприємств [178], Іванова Н. В., Кононенко С. О. конкретизують ризики економічної безпеки в контексті глобальної діджиталізації аутсорсингу [179]. Таким чином, стає очевидним, що цифрові ризики або ризики, пов'язані з цифровізацією економічних відносин, є характерними для усіх напрямів господарської діяльності підприємства, та можуть негативно впливати на різні функціональні види менеджменту організацій. Суттєвим є їх вплив і на стратегічне управління та на процеси стратеготворення, яке в умовах невизначеності воєнного часу є особливо складним завданням. Тому особливо цінними є дослідження, які пов'язують цифрові ризики та стратегічні орієнтири функціонування підприємств. Наприклад, Гедз М. Й., Вишневська В. А., Науменко С. Д. розглядають маркетингові стратегії та економічні ризики цифровізації інтеграційно-диверсифікаційних процесів в корпоративному менеджменті [70], Климчук М. М., Ачкасов І. А., Климчук С. А., Поляк О. П. досліджують вплив ризик-менеджменту на формування стратегії управління бізнес-процесами підприємства в умовах цифрової економіки із використанням здобутків міжнародного досвіду у цьому питанні [69], Сазонова С. В. ідентифікує та оцінює ризики стратегічного управління телекомунікаційними підприємствами в умовах цифрової економіки [42], [180]. Внеском у теорію ризик-менеджменту

у системі управління економічною безпекою підприємств стали публікації таких сучасних вчених, як Левченко О.М. [181, 182], Панченко В.А. [183-186], Іванова М.І. [187-189], Гуцалюк О. М. [190-192], Шевченко А. М. [193-195], Носань Н. С. [196-198], Білоус С. П. [199, 200]. Попри наявні вагомі наукові напрацювання у площині впливу ризиків на процес стратегічного управління окремими напрямами розвитку суб'єктів господарської діяльності, залишається без чіткої та конкретної відповіді від науковців питання, чи можливо уникнути або ефективно мінімізувати цифрові ризики та їх вплив на стан економічної безпеки підприємства через розробку або адаптацію механізмів стратегічного управління підприємством.

Оцінювання міри впливу цифрових ризиків на стан економічної безпеки сучасних вітчизняних підприємств і визначення можливості використання отриманого аналітичного висновку управлінським персоналом суб'єкта господарювання як аргументу на користь або проти ймовірності досягнення стратегічних цілей бізнесу, є важливим сучасним науковим і прикладним завданням.

Ризики, виклики, небезпеки та загрози ведення бізнесу є саме тими факторами, які не дають можливості управлінському персоналу достовірно визначити імовірність досягнення планових показників під час розробки стратегії. Для того, аби стратегія діяльності підприємства була реалістичною та дійсно мала інформаційну цінність для його функціонування у перспективі, для налагодження його бізнес-процесів та виконання персоналом поставлених завдань на шляху до реалізації генеральної мети започаткування бізнесу його фундаторами, планування прогнозування та форсайт його майбутнього економічного стану та позиції на ринку має ґрунтуватися на релевантній інформації про тенденції зовнішнього та внутрішнього середовища суб'єкта господарювання. Перебіг процесів внутрішнього середовища у значній мірі характеризується показниками економічної безпеки компанії, і є підвладним контролю її менеджменту в більші або менші мірі, однак, зовнішнє середовище традиційно стає джерелом для появи численних ризиків, передбачити які

інколи неможливо. Тому трапляються випадки, коли стратегічне бачення цілей підприємницької структури виявляється недалекоглядним, а досягнути планових показників просто неможливо, і причиною цьому є відсутність етапу оцінювання ризиків у процесі стратеготворення, його формальний характер або нестача ресурсів.

Цифрові або у ряді джерел – ІТ-ризики – умовно поділяються на дві групи: ризики, пов'язані з розвитком інформаційних систем, і ризики, пов'язані з поточною роботою інформаційних систем. На думку вчених, існує необхідність комплексного підходу до аналізу ІТ-ризиків, пов'язаних з організаційним рівнем, на якому знання та навички користувачів, їх соціальні взаємодії при використанні комп'ютерної інформації та системи також важливі для розуміння ризику, як і ризики технічної системи [69, с.274-275]. Також науковці виділяють організаційні ризики, пов'язані з цифровізацією бізнес-процесів. До них віднесені: втрата підприємством конкурентних позицій через відсутність можливостей впровадження цифрових технологій, індивідуалізація виробництва [177, с.119].

Вивчення кейсів і аналітичних матеріалів вітчизняних і зарубіжних компаній дозволяє дійти висновку, що оцінка впливу цифрових ризиків на стан економічної безпеки підприємства є тим вищою, чим більш цифровізованою є його діяльність, і чим менш розвинутими при цьому виявляються механізми управління економічною безпекою (рис.2.2).

Запропонований рисунок слугує візуальним підтвердженням гіпотези, що чим більше підприємство прагне інтегруватися у цифровий простір та розвинути цифрові напрями свого бізнесу, або просто перевести свої базові бізнес-процеси в цифрову екосистему, тим більшим і потужнішим є вплив цифрових ризиків на його результуючі фінансові показники та на стан його економічної безпеки [173, с.11].

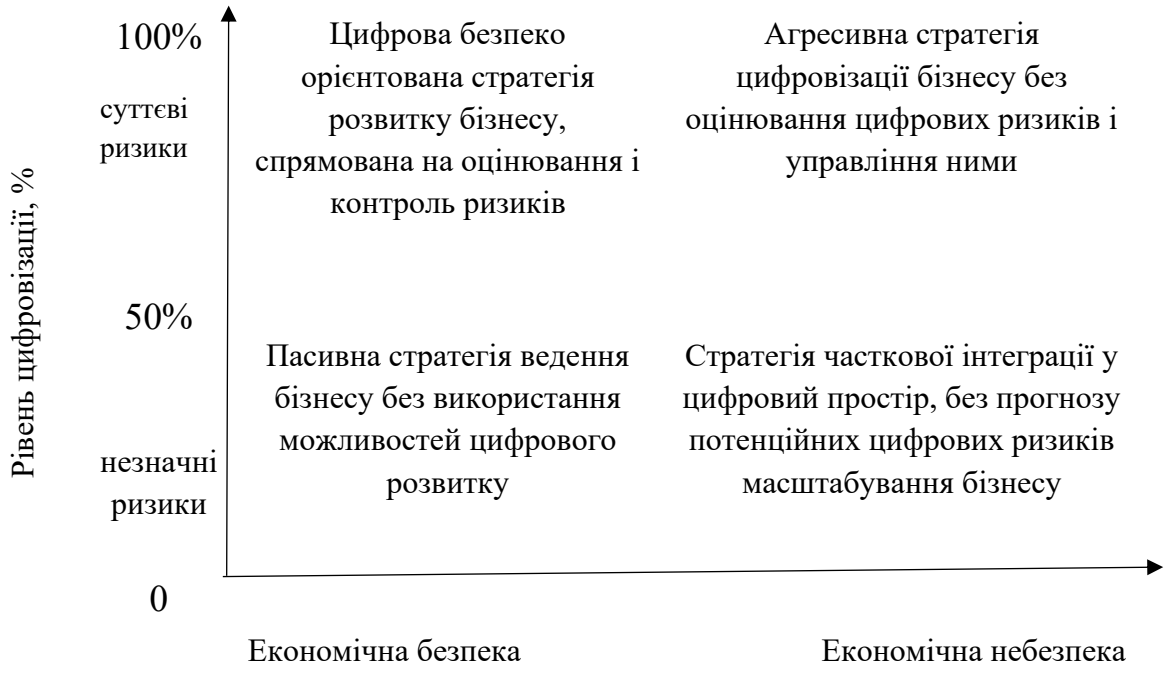


Рисунок 2.2. - Залежність стану економічної безпеки підприємства від впливу цифрових ризиків

Джерело: [173, с.11]

У звіті «Navigate: Digital Risk Index 2025», який формується на підставі аналітичних і експертних даних від авторитетних міжнародних консалтингових компаній і агентств з безпеки, згруповано основні види цифрових ризиків, притаманних для підприємств і державних структур в усьому світі (табл.2.3). Цей індекс і інформація щодо конкретних його складових можуть бути використані українськими підприємствами та їх управлінським персоналом як орієнтири для розробки стратегій адаптації та забезпечення економічної безпеки в умовах глобальної цифровізації [201, с.88]. Зокрема, впливовість цих ризиків може стати важливим параметром під час розроблення різних сценаріїв та альтернативних варіантів стратегічних планів стабілізації або розвитку бізнесу. Навіть якщо для конкретного підприємства означені ризики не є притаманними у певний момент часу, їх превентивне вивчення може дозволити попередити ймовірні збитки у майбутньому та сформувати стратегічні орієнтири, для досягнення яких не вимагатиметься значний бюджет для протидії цифровим ризикам.

Таблиця 2.3 – Цифрові ризики, що мають враховуватись під час адаптації стратегій сучасних підприємств

Ризики	Впливовість
Геополітичні	
Кібератаки, шпигунство та війна	42%
Політична спрямованість на зниження пріоритетів управління та дотримання вимог	39%
Економічна конкуренція та конфронтація, зокрема через політичні директиви, які захищають або надають перевагу певним постачальникам цифрових технологій над іншими	33%
Ризики для прав людини та/або громадянських свобод, пов'язані з політичними, політичними та регуляторними втручаннями у цифрове управління	31%
Багатополярність, ізольованість або фрагментарність норм та правил управління	31%
Соціальні ризики та ризики навколишнього середовища	
Ризик для конфіденційності та захисту даних	58%
Технології штучного інтелекту як фактори, що прискорюють або збільшують ризик несприятливих наслідків від їх використання	54%
Дезінформація (у т.ч. в Інтернеті)	37%
Проблеми з визначенням та вимірюванням потенційно шкідливого впливу технологій	34%
Ризик дискримінації, упередженості та несправедливості	30%
Організаційні ризики	
Брак бюджету та ресурсів для інвестування у фахівців, практики та інструменти управління ризиками	48%
Знецінювання бізнесом управління ризиками та дотримання вимог і стандартів ризик-менеджменту (зниження пріоритетів щодо контролю управління та дотримання вимог комплаєнсу)	36%
Відсутність або нечітка підзвітність і відповідальність за управління ризиками та прийняття ризиків	35%
Відсутність доступу до кваліфікованих фахівців і «талантів»	29%
Застаріла або недостатня архітектура та процеси управління даними	29%
Технологічні ризики	
Залежність від постачальників та ризики, пов'язані з ними	51%
Застаріла інфраструктура та інструментарій, що не відповідає цільовому призначенню	41%
Відсутність розуміння або недостатня обізнаність щодо картографування даних і систем	39%
Ризики фізичної та кібербезпеки та стійкості	34%
Темпи інновацій та технологічних змін, що призводять до технологічного старіння	29%

Джерело: [201, с.88-89, 202]

Отже, до першої десятки найбільш впливових цифрових ризиків респонденти віднесли: ризики для конфіденційності та захисту даних (58%), масштабування використання технологій штучного інтелекту без належної

безпекової підтримки цього процесу (54%), залежність від сторонніх постачальників та ризики, пов'язані їх діями або бездіяльністю (51%), нестачу ресурсів для інвестування в розвиток управлінського персоналу, фахівців з управління ризиками, практики та інструменти ризик-менеджменту (48%), кібератаки, шпигунство та війни (42%), застарілу інфраструктуру та інструменти, що не відповідають цільовому призначенню (41%), політичну спрямованість на зниження пріоритетів управління та дотримання вимог і стандартів (39%), недостатню обізнаність щодо картографування даних і систем (39%), дезінформацію (37%), зниження пріоритетів щодо контролю управління та дотримання вимог комплаєнсу (36%). Тому, засновуючись на зарубіжному досвіді, можна рекомендувати українським компаніям розпочати адаптацію власних стратегій, орієнтуючи їх на цілі досягнення економічної безпеки в цифровому середовищі, саме з заходів мінімізації перерахованих ризиків [201, с.89].

Підприємства, які успішно функціонують в умовах невизначеності та ризиків, характеризуються наявністю комплексних систем економічної безпеки, що мають фінансову, кадрову, інформаційну, правову, техніко-технологічну та інші складові. Застосування цифрових технологій має відображатись на процесах управління кожною із названих функціональних підсистем безпеко орієнтованого менеджменту. Наприклад, в управлінні правовою складовою економічної безпеки підприємства: як зазначають Добровольська В. В., Ляховецький О. О., стратегічне управління цифровими ризиками у юридичній площині має охоплювати такі основні сфери: цифрові контракти та угоди (смарт-контракти); електронна комерція; електронний документообіг; цифровізація державних послуг; інтелектуальна власність; фінансові технології (FinTech); технології штучного інтелекту та автоматизація бізнес-процесів [174, с.12]. Цифрові ризики виникають під час використання електронного цифрового підпису, при захисті інтелектуальної власності у цифровому просторі, у процесі регулювання відповідальності за діяльність автоматизованих систем і алгоритмів. Також цифровізація правових відносин

характеризується ризиками технічних збоїв та помилок в оформленні документів або своєчасності їх надходження до адресата, що відображається на якості управління фінансово-господарськими процесами [174, с.14-16].

Зачосова Н. В., Коваленко А. О., Куценко Д. М. відзначають, що у межах поширення Індустрії 4.0 на теренах вітчизняного бізнесу, цифрові ризики для підприємств усе частіше виникають у царині господарських відносин, пов'язаних із масштабуванням Інтернету речей, Інтернету даних, Інтернету послуг та Інтернету людей. Також до інтенсифікації ризиків можуть призвести незбалансоване застосування цифрових технологій, висока енергоємність бізнес-процесів, що реалізуються у цифровому просторі [175, с.146].

До переліку цифрових ризиків у інтелектуально-кадровій підсистемі економічної безпеки можна віднести відсутність у персоналу цифрових компетенцій та збільшення частки віддаленої зайнятості на ринку праці, що призводить до дефіциту кадрів і збільшення тривалості закриття вакансій. Це, у свою чергу, означає для підприємств додаткові витрати ресурсів [177, с.120], а отже, негативно впливає на стан їх економічної безпеки та стратегічні можливості розвитку бізнесу.

Сучасні науковці погоджуються у думці, що для успішного впровадження цифрових технологій підприємствам необхідно розробити комплексну стратегію, що враховує технічні, фінансові, організаційні та соціальні аспекти [174, с.17]. Демчишак Н. Б., Клек А. Р., Цвєткова З. М. вважають, що у площині стратегічного менеджменту управлінському персоналу варто зосередитись на розробці гнучких та адаптивних стратегій, які дозволяють компаніям швидко реагувати на зміни в ринкових умовах і в поведінці споживачів, а для протидії цифровим ризикам – практикувати впровадження жорстких заходів випередження кібератак та управління кібербезпекою для захисту даних і систем, та приділяти увагу розробці планів реагування на кібератаки та навчанню співробітників основам кібербезпеки, кібергігієни та кращим практикам захисту даних [176].

Для спрощення завдання врахування цифрових ризиків у стратегіях підприємств необхідно розробити їх типову класифікацію, яка слугуватиме для ризик-менеджерів орієнтиром під час ідентифікації та оцінювання впливу ризиків на різні складові комплексної системи економічної безпеки суб'єкта господарювання. Осадча О. О., Роздопченюк В. М. пропонують авторську класифікацію ризиків стійкості підприємства як елемента економічної безпеки в умовах цифровізації, поділяючи їх на групи з типом стійкості: ризики для економічної стійкості, ризики для технічної стійкості, ризики для цифрової стійкості, ризики для стійкості енергоефективності, ризики для інноваційної стійкості [177, с.122]. Раціональним буде підхід, де цифрові ризики розподілятимуться за напрямом виникнення або впливу – характерні для інтелектуально-кадрової, фінансово-інвестиційної, фізичної, правової, техніко-технологічної, ринкової, інтефейсної, тощо, складової системи економічної безпеки підприємства. Така класифікація дозволить будувати карти ризиків і визначати набір управлінських рішень, здатних оптимально спрямувати зусилля та ресурси на досягнення контролю над ними.

Сазонова С.В. вважає, що оцінювання ризиків – одна з найбільш складних проблем стратегічного управління. Метою оцінювання ризиків є визначення повного переліку ризиків, які можуть вплинути на досягнення цілей підприємства та вибір методу оцінювання певного ризику або групи ризиків [42, с.32]. Дослідниця пропонує використовувати такий набір методів, застосовуючи різні їх комбінації, у залежності від характеру та джерела походження ризику, що підлягає оцінці: методи ідентифікації ризиків – мозковий штурм, структуровані або частково структуровані інтерв'ю, метод Дельфі, контрольні листи, попередній аналіз небезпек (PHA – Preliminary Hazard Analysis), дослідження HAZOR (HAZOR – Hazard and Operability Study); методи обробки ризиків – аналіз небезпеки і критичних контрольних точок (HACCP – Hazard Analysis and Critical Control Points), аналіз першопричин (RCA – Root Cause Analysis), аналіз «дерева несправностей» (FTA), аналіз «дерева подій» (ETA), аналіз причин і наслідків, і методи оцінювання ризиків –

структурований аналіз сценаріїв методом «що, якщо?» (SWIFT – Structured what-if technique), аналіз впливу на бізнес (BIA – Business Impact Analysis), аналіз ефективності витрат (CBA – Cost / benefit analysis), аналіз першопричини відмови (RCFA – Root Cause Failure Analysis), технічне обслуговування, спрямоване на забезпечення надійності (RCM – Reliability centred maintenance) [42, с.34]. Водночас, залишається актуальним питання, чи усі ці методи та інструменти доцільні для використання під час оцінювання цифрових ризиків? Їх апробація у цьому контексті є важливим науково-практичним завданням, однак, потребує часового та кадрового ресурсів. І тут у нагоді також можуть стати засоби штучного інтелекту, який здатен протестувати пропонований інструментарій за умови коректної поставки для нього аналітичного завдання та надання доступу до баз даних конкретного підприємства, що потребує такої оцінки у процесі розроблення власної стратегії цифрової трансформації бізнесу або управління економічною безпекою.

Цифровізація підприємницької діяльності набуває розмаху, а відтак зростає і вплив цифрових ризиків на стан економічної безпеки компаній, як в Україні, так і за кордоном. Рис. 2.3 демонструє частку підприємств в Європі, що використовують будь-яке бізнес-програмне забезпечення (ERP, CRM або BI). Помітним є зростання їх кількості за два роки.

У такому контексті, перспективи подальших досліджень впливу цифрових ризиків на стан економічної безпеки підприємств сучасним науковцям варто вбачати у розробленні комплексного інструментарію для реалізації завдань автоматичної ідентифікації та адаптивного моніторингу цифрових ризиків із використанням технологій Big Data та штучного інтелекту, що дозволить своєчасно відкоригувати стратегічні цілі підприємства в ітераційному режимі, забезпечуючи високу ймовірність досягнення стратегічних орієнтирів стану його економічної безпеки та перспектив сталого розвитку в умовах поглиблення цифрових трансформацій бізнесу [173, с.11-14].

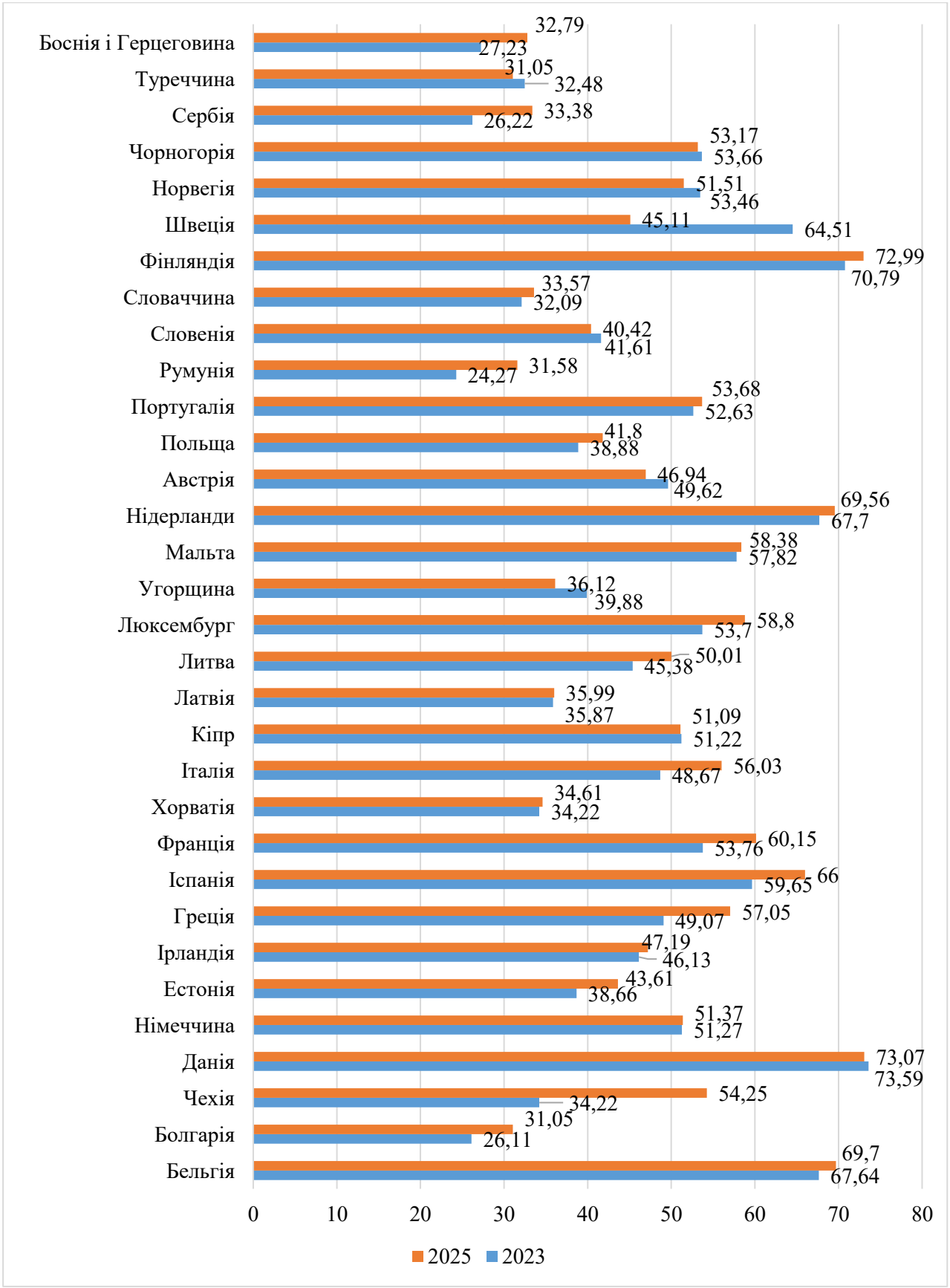


Рисунок 2.3. - Частка європейських компаній, що використовують бізнес-програмне забезпечення (ERP, CRM або BI)

Джерело: [203]

Європейська статистика не демонструє відомостей щодо України. Однак, у травні 2025 року було оприлюднено документ під назвою «Україна. Профіль країни з цифрового розвитку» [204]. Він містить дані станом на 2023 рік, проте, дає змогу отримати уявлення про ключові індикатори цифровізації економіки держави. Індекс цифрової трансформації регіонів України підкреслює значний прогрес у цифровому управлінні та послугах, незважаючи на виклики, спричинені тривалою війною. Хоча регіони з найкращими показниками (Дніпропетровський, Львівський, Полтавський, Тернопільський) встановлюють орієнтири для інновацій та ефективності, значні розбіжності залишаються, що підкреслює необхідність цільових інвестицій. Очевидною є необхідність створення дорожньої карти для масштабування цифрової трансформації соціально-економічних систем в Україні [204, с.16-17].

Під час війни спостерігається збільшення кількості кібератак, спрямованих на українські телекомунікаційні мережі, які широко використовуються для забезпечення безперервності підприємницької діяльності, що має суттєвий вплив на стан економічної безпеки вітчизняних підприємств. Ці атаки спрямовані на порушення зв’язку, ускладнюючи зусилля з підтримки надійного покриття мобільної мережі [204, с.20].

У огляді ринку кібербезпеки в Україні, у січні 2025 року пропонуються такі складові, що могли б стати елементами комплексної системи економічної безпеки сучасних підприємств: безпека додатків, хмарна безпека, безпека даних, мережева безпека, безпека кінцевих точок [205, с.4]. Також автори звіту зазначають, що найчастіше під ураження потрапляють сектори виробництва, фінансів, охорони здоров'я та цифрових послуг. Найпопулярнішими видами кібератак залишаються DDoS, Ransomware, Phishing, а країнами, на які здійснюється найбільша кількість кібератак, виступають США, Україна, Південна Корея, Китай [205, с.7]. Український ринок кібербезпеки зріс у 4 рази за останні з 2016 по 2023 роки і, за прогнозами, зросте ще на 50% до 2029 року [205, с.9]. Це є свідченням усвідомлення важливості захисту цифрової безпеки на мікро та макрорівнях.

Характерними рисами вітчизняного ринку кібербезпеки у 2025 році залишались:

– підвищення частоти та масштабу кібератак (війна збільшила кількість та складність кібератак вітчизняний бізнес, що призвело до швидкого впровадження автоматизованих рішень, як шифрування даних, автоматизоване виявлення загроз;

– необхідність негайних рішень: ризики масштабних кібератак, змусили компанії надавати перевагу готовим кіберрішенням над планомірним впровадженням персоналізованих рішень;

– нестача кадрів: обмеженість спеціалістів призвела до використання автоматизованих рішень, які потребують меншого втручання людини [205, с.11].

У 2023 році рівень користування послугами кібербезпеки серед компаній мав такі показники: 63% компаній користувалися послугами іноземних вендорів, 37% компаній працювали лише з українськими вендорами, а 61% замовників не отримували пропозицію співпраці від українських вендорів. 10-15% в середньому витрачали великі компанії зі свого річного бюджету на кібербезпеку і >20% в середньому витрачали невеликі компанії, що обслуговують багато клієнтів з критичними даними [205, с.30].

Цифрова трансформація стала вирішальним фактором прогресу в різних секторах національної економіки, впливаючи на те, як суб’єкти господарювання провадять свою діяльність, надають послуги та взаємодіють із стейкхолдерами. Однак, успіх цифрової трансформації залежить не лише від наявності передових технологій, а й від впровадження цих технологій користувачами та підприємствами. На процес впровадження впливає кілька факторів, таких як доступність, ефективність використання, а також цифрові навички персоналу та цифрова інклюзія [204, с.33].

Наприкінці 2025 року в Україні було активних 55,0 мільйонів стільникових мобільних з’єднань, що еквівалентно 140% від загальної чисельності населення. Однак, деякі з цих з’єднань можуть включати лише такі послуги, як голосовий

зв’язок та SMS, а деякі можуть не включати доступ до Інтернету. Наприкінці 2025 року в Україні було 35,3 мільйона осіб, які користувалися Інтернетом, тоді як рівень проникнення онлайн становив 89,6%. У жовтні 2025 року в Україні налічувалося 23,0 мільйони користувачів соціальних мереж, що дорівнює 58,5% від загальної чисельності населення [206]. Такий масштаб цифровізації призводить до прискорення цифрових трансформацій бізнес-процесів, а отже, означає більшу кількість ризиків для стану економічної безпеки підприємств.

Табл. 2.4 узагальнює випадки впливу цифрових ризиків на стан економічної безпеки підприємств в Україні та в світі. Дані отримані з відкритих джерел, оскільки статистика проявів цифрових загроз у фінансово-господарській діяльності компаній, особливо у воєнний час, є закритою для зовнішніх користувачів. Однак, висновки щодо взаємозв’язків між рівнем цифрових ризиків і станом економічної безпеки суб’єктів господарювання – зроблені особисто автором.

Таблиця 2.4. – Аналіз впливу цифрових ризиків на стан економічної безпеки підприємства

Підприємство /сектор	**Рік**	**Вид цифрового ризику**	**Суть негативної події**	**Наслідки**	**Підсистема економічної безпеки, що постраждала**
Kyivstar (телекому-нікації)	2023	Кібератака для знищення інформації (wiper)	Знищення IT-інфраструктури підприємства, зупинка обслуговування клієнтів	Фінансові збитки, втрата часу для відновлення	Інформаційна, техніко-технологічна, фінансова, правова
Capita (аутсорсинг)	2023	Блокування доступу до інформації (ransomware) і витік даних	Компрометація персональних даних	Штрафи, фінансові збитки, репутаційні втрати	Інформаційно-аналітична, правова, фінансова, репутаційна
MGM Resorts / Caesars	2023	Соціальна інженерія, цифрова неграмотність, хакерська атака	Доступ через персонал до інформації з обмеженим доступом, блокування роботи, вимагання коштів	Фінансові витрати для задоволення вимог, врата даних, зупинка діяльності	Інтелектуально-кадрова, інформаційно-аналітична, фінансова

Продовження табл. 2.4.

Підприємство /сектор	Рік	Вид цифрового ризику	Суть негативної події	Наслідки	Підсистема економічної безпеки, що постраждала
23andMe (біотех)	2023	Соціальна інженерія, доступ до закритих даних	Використання паролів, які користувачі вводили на інших сайтах, шахрайство	Витік даних клієнтів, втрата капіталізації та ділової репутації	Інформаційна, репутаційна, правова
British Library (бібліотечна справа)	2023	Використання програми-вимагача	Шифрування серверів, викрадення даних, блокування систем	Зупинка функціонування	Інформаційно-аналітична, організаційна, фінансова
Kido International (освіта)	2023	Витік даних	Компрометація персональних даних, доступ до платіжних даних	Зупинка онлайн-платформи, втрата клієнтів	Інформаційна, правова, репутаційна, фінансова
TOMRA (виробництво)	2023	Кібератака на IT/OT	Порушення виробничих процесів	Зниження операційної ефективності, інформаційні втрат	Техніко-технологічна, виробнича, інформаційна
MOVEit (глобальне ПЗ)	2023	Доступ до баз даних через хакерську атаку	Вразливість програмного забезпечення і масові витоки даних	Масові збитки для компаній-клієнтів і партнерів	Інформаційна, техніко-технологічна, фінансова
Synnovis (медичні послуги)	2024	Блокування, знищення і викрадення даних	Порушення працездатності IT-інтерфейсів	Втрата часу на відновлення, блокування роботи	Інформаційна, матеріальна, техніко-технологічна

Джерело: складено автором за даними [207-219]

Використання аналізу цифрових ризиків як інформаційної бази для обґрунтування стратегії підприємства, оцінки рівня досяжності стратегічних орієнтирів та ідентифікації потреби своєчасних адаптаційних трансформацій дозволяє змінити усталену наукову парадигму, яка набула широкого вжитку на прикладному рівні серед менеджменту сучасних компаній і перейти від управління успіхом до управління спроможністю його утримувати тривалий час. Такий підхід дозволяє уникнути безапеляційного погляду на досяжність стратегічної цілі, а поставити її у залежність від стану безпеки цифрових даних, цифрових транзакцій, цифрових комунікацій, надання цифрових послуг, цифрових трансформацій бізнес-процесів підприємства.

2.3. Оцінка ефективності безпеко орієнтованих стратегій українських підприємств

Залежність стану економічної безпеки підприємства від впливу цифрових ризиків на його фінансово-економічну діяльність є очевидною, і зростає відповідно до нарощення масштабів цифровізації бізнесу та вчинення спроб інтеграції до цифрових ринків товарів і послуг. Встановлено, що підприємства можуть обрати чотири базові варіанта стратегії своєї поведінки, у залежності від бажання цифровізувати підприємницьку діяльність, враховувати при цьому цифрові ризики та дбати про стан економічної безпеки. Це такі стратегії, як цифрова безпеко орієнтована стратегія розвитку бізнесу, спрямована на оцінювання і контроль ризиків (дозволяє досягти та підтримувати стан економічної безпеки попри наявність суттєвих цифрових ризиків), агресивна стратегія цифровізації бізнесу без оцінювання цифрових ризиків і управління ними (характеризується значними цифровими ризиками, що без належних управлінських зусиль призводять до погіршення стану економічної безпеки підприємства), пасивна стратегія ведення бізнесу без використання можливостей цифрового розвитку (характеризується незначним рівнем цифрових ризиків і стабільним станом економічної безпеки) та стратегія часткової інтеграції у цифровий простір, без прогнозу потенційних цифрових ризиків масштабування бізнесу (характеризується невисокими цифровими ризиками, але і станом економічної небезпеки, що виникає через вперте нехтування фактом їх існування) [173, с.11].

Водночас, цифровізація є не лише джерелом ризиків для стану економічної безпеки підприємства, але і засобом оптимізації процесу управління ними. Наприклад, застосування елементів ШІ в ризик-менеджменті трансформує підходи до управління ризиками та надає численні переваги, зокрема, щодо рутинного аналізу великих масивів даних. Представникам управлінського персоналу залишаються ролі більш стратегічного характеру та виконання завдань, які пов’язані із новими викликами, та з тими факторами, які мають не

чітку логіку прояву, або базуються на етичних або соціальних нормах, досвіді та потребах в застосуванні знань із суміжних галузей. Таким чином, синергія людського та штучного інтелекту вже зараз гарантує підвищену ефективність та адаптивність систем управління ризиками [178] – як при формуванні комплексних механізмів управління економічною безпекою, так і у процесі розробки безпеко орієнтованих стратегій розвитку бізнесу на традиційних і цифрових ринках товарів і послуг [173, с.12].

Існує кілька варіантів управлінських дій, які здатні пом'якшити негативний вплив цифрових ризиків на корпоративні ресурси та навіть дають змогу використати їх як додаткові можливості для масштабування та якісного оновлення підприємницької діяльності. Якщо топ-менеджмент компанії обирає у якості стратегічного орієнтиру низький рівень цифровізації фінансово-господарських процесів і прагне продовжувати працювати у знайомому середовищі, у традиційних сегментах ринків товарів і послуг, тоді для нього залишаються доступними та актуальними класичні стратегії розвитку бізнесу без досягнення далекоглядних перспектив, доступних за умови активного використання цифрових тенденцій модифікації бізнесу. При цьому, цифрові ризики залишаються незначними для стану економічної безпеки компанії. Якщо ж вплив цифрових ризиків посилюється, навіть попри бажання очільників підприємства, наприклад, під час взаємодії з клієнтами та партнерами, які значною мірою інтегровані у цифровий економічний простір або ж суб'єкт господарювання прагне розширити свій вплив на цифрових ринках у перспективі без приділення достатньої уваги цифровими ризиками (через незнання або відсутність необхідних ресурсів) то така стратегія може виявитися провальною, оскільки рівень економічної безпеки у цифровому просторі буде низьким, що майже неминуче означатиме збитки та погіршення ділової репутації перед стейкхолдерами. Оптимальним варіантом за умови спроб досягнення високого рівня цифровізації бізнес-процесів, а відтак, і активного перебування у зоні високих цифрових ризиків, для підприємства буде розробка цифрової безпеко орієнтованої стратегії, яка дозволить

використовувати можливості цифрових трансформацій бізнесу за результатами ґрунтовного та комплексного оцінювання цифрових ризиків та після передбачення фахівцями їх потенційного впливу на стратегічні орієнтири підприємницької діяльності [173, с.12].

Таблиця 2.5 демонструє взаємозалежність рівня цифровізації підприємства і ймовірності впливу цифрових ризиків на його систему економічної безпеки та стратегічне управління нею.

Таблиця 2.5. - Матриця цифрових ризиків підприємств залежно від рівня його цифровізації

Рівень цифровізації бізнес-процесів	**Характеристики досягнутого рівня**	**Основні цифрові ризики для підприємства**	**Ймовірність негативного впливу ризику**	**Оцінка впливовості ризику**	**Функціональні підсистеми економічної безпеки, що підпадають під вплив**
10-20% (мінімальний)	Фрагментарна цифровізація, домінування класичного документообігу	Помилки персоналу, втрата даних, відсутність захисту, його слабкість	Низька ймовірність	Низька-середня, наслідки контрольовані	Інтелектуально-кадрова, інформаційно-аналітична
30-40% (низький)	Часткова автоматизація обліку, HRM і фінансових операцій	Зовнішній доступ до даних, слабкі паролі, локальні віруси, помилки	Середня ймовірність	Середня, наслідки можна компенсувати	Інформаційно-аналітична, фінансово-інвестиційна
50-60% (середній)	Інтеграція IT-систем у менеджмент компанії (ERP, CRM)	Кібератаки, збої системних процесів, помилки користувачів	Висока ймовірність	Середня-висока, наслідки відчутні для бізнесу	Інформаційна, техніко-технологічна, фінансово-інвестиційна
70-80% (достатній)	Цифрова трансформація екосистеми бізнесу, хмарні сервіси	Викрадення і блокування даних, залежність від провайдерів	Висока ймовірність	Висока, наслідки можуть призвести до стану кризи	Інформаційно-аналітична, фінансово-інвестиційна, інтерфейсна
90-100% (високий)	Розумне цифрове підприємство, що активно використовує ШІ	Кібертероризм, APT-атаки, системні збої, соціальна інженерія	Дуже висока ймовірність	Надвисока, наслідки провокують критичний стан бізнесу	Інформаційно-аналітична, техніко-технологічна, фінансова, кадрова

Джерело: складено автором

Отже, цифровізація господарської діяльності підприємства має двосторонній характер і вплив на стан його економічної безпеки. З одного боку, вона є драйвером ефективності та забезпечує можливості використання цифрових інструментів і штучного інтелекту для захисту економічної безпеки корпоративних ресурсів компаній, а з іншого – є каталізатором і мультиплікатором ризиків, темпи зростання яких випереджають темпи адаптації менеджменту компанії для ефективного управління ними.

Опинившись у реаліях воєнного часу та відчувши у повній мірі тенденції світу BANI на власних фінансово-економічних показниках, українські підприємства усе частіше обирають безпеко орієнтовані стратегії свого функціонування та розвитку або принаймні інтегрують стратегічні орієнтири, націлені на досягнення оптимального рівня економічної безпеки у традиційні стратегії, зокрема і ті, які були розроблені ще у довоєнний період. Оцінити їх ефективність дозволяє діагностика стану економічної безпеки компанії, однак, результати монографічного аналізу фахової економічної літератури доводять відсутність універсального методичного інструментарію для реалізації цього процесу на практиці, хоча і тематика оцінювання економічної безпеки є досить популярною серед вітчизняних вчених. Наприклад, Кошельок І. П., Малікова І. П. критикують та узагальнюють існуючі методичні підходи до оцінки економічної безпеки підприємства [219], Орлова А. А., Вишневська В. А., Бурлака В. В. пропонують результати авторського аналіз методичних практик оцінювання економічної безпеки суб’єктів господарювання [220], Ткаченко Т. П., Гречко А. В. вказують на специфіку та унікальність методичних інструментів оцінювання економічної безпеки промислових підприємств [221], Богданюк І. В. пропонує використання індикаторного підходу до оцінки економічної безпеки компаній [222], Хаванов А. В. вважає доцільною розробку та впровадження комплаєнс-індикаторів для оцінювання рівня зрілості системи економічної безпеки підприємницьких структур [223], Середа О. О. фокусується на аспекті оцінювання фінансової безпеки корпоративних підприємств в умовах цифрової

економіки [224], Кукоба А. В. розглядає перспективи та доцільність нефінансового оцінювання стану виробничої складової економічної безпеки суб'єктів господарської діяльності [225], Мазіашвілі А. Р., Воловельська І. В., Кулеш В. Р. простежують унікальні риси оцінювання рівня системи економічної безпеки підприємства залізничного транспорту [226], Вівчар О. І. піднімає актуальне у контексті цього дослідження питання комплексного оцінювання стратегії зміцнення економічної безпеки підприємств мережевих структур України в умовах воєнного стану [227], Назаренко І. Л., Білоусова В. М. вивчають можливості адаптування комплексної методики визначення рівня економічної безпеки, оцінки ризиків та ймовірності банкрутства для малих підприємств [228], Богданюк І. В., Мандич С. М. наполягають на застосуванні багатофакторної моделі оцінювання ризиків та їх впливу на економічну безпеку компаній [229]; з їх думкою погоджуються і Сластяникова А., П'ятодверний М. [230], Ткаченко Т. [231], Копилюк О. І., Музичка О. М., Рутар Р. І. [232], Бабічев А. В., Самородов Б. В. [233].

Таким чином, на сучасному етапі розвитку методології оцінювання економічної безпеки підприємств її характеристиками, особливостями та унікальними рисами є:

- об'єктом оцінювання у різних методиках виступає то економічна безпека в цілому, то її рівень, то її стан; цей аспект потребує універсалізації у теоретико-методичній площині;

- велика кількість якісних і кількісних показників, знайти відомості для розрахунку яких на разі неможливо через обмеження доступу до даних про діяльність підприємств в умовах воєнного часу;

- різні підходи до розрахунку кількісних показників, а також до встановлення їх нормативних або оптимальних значень;

- значна роль експертної оцінки як під час процедури діагностики, так і у момент інтерпретації результатів і формування остаточного висновку;

- суб'єктивність оціночних моделей;

- активне використання скорингу та рейтингування для оцінювання.

Для оцінювання ефективності безпеко орієнтованих стратегій українських підприємств об’єктами було обрано десять підприємств критичної інфраструктури (п’ять – загальнонаціональних і п’ять – Черкаського регіону), які у воєнний час використовують саме такі стратегії для свого функціонування, зважаючи на мету свого існування та важливу соціальну та стратегічну функцію у суспільстві:

– АТ «Укртелеком» [234];
– АТ «Укрпошта» [235];
– АТ «Укрзалізниця» [236];
– ПрАТ «Київстар» [237];
– НЕК «Укренерго» [238];
– КПТМ «Черкаситеплокомуненерго» [239];
– АТ «Черкасиобленерго» [240];
– КП «Черкасиводоканал» [241];
– ПрАТ «Черкаське хімволокно» (ДП «Черкаська ТЕЦ») [242];
– АТ «Черкаський автобус» [243].

Відомості про індикатори стану економічної безпеки цих підприємств узагальнено у Додатку Д.

На рис. 2.4 і 2.5 продемонстровано зміну показників, за якими можна узагальнено оцінити стан кадрової безпеки досліджуваних підприємств.

Аналіз значень унаочнених показників призводить до висновку, що стан кадрової безпеки більшості підприємств критичної інфраструктури у 2025 році стабілізувався. Цьому сприяли такі тенденції, як збільшення кількості персоналу після його стрімкої втрати у 2022-2023 роках, підвищення розмірів заробітної плати до показників, середніх на ринку праці та вище. Однак, показники оплати праці є суттєво нижчими за дохід, який кадровий ресурс приносить компаніям. У більшості випадків відсутня взаємозалежність між зростанням показника доходу підприємств на одного працівника та середнім розміром заробітної плати.

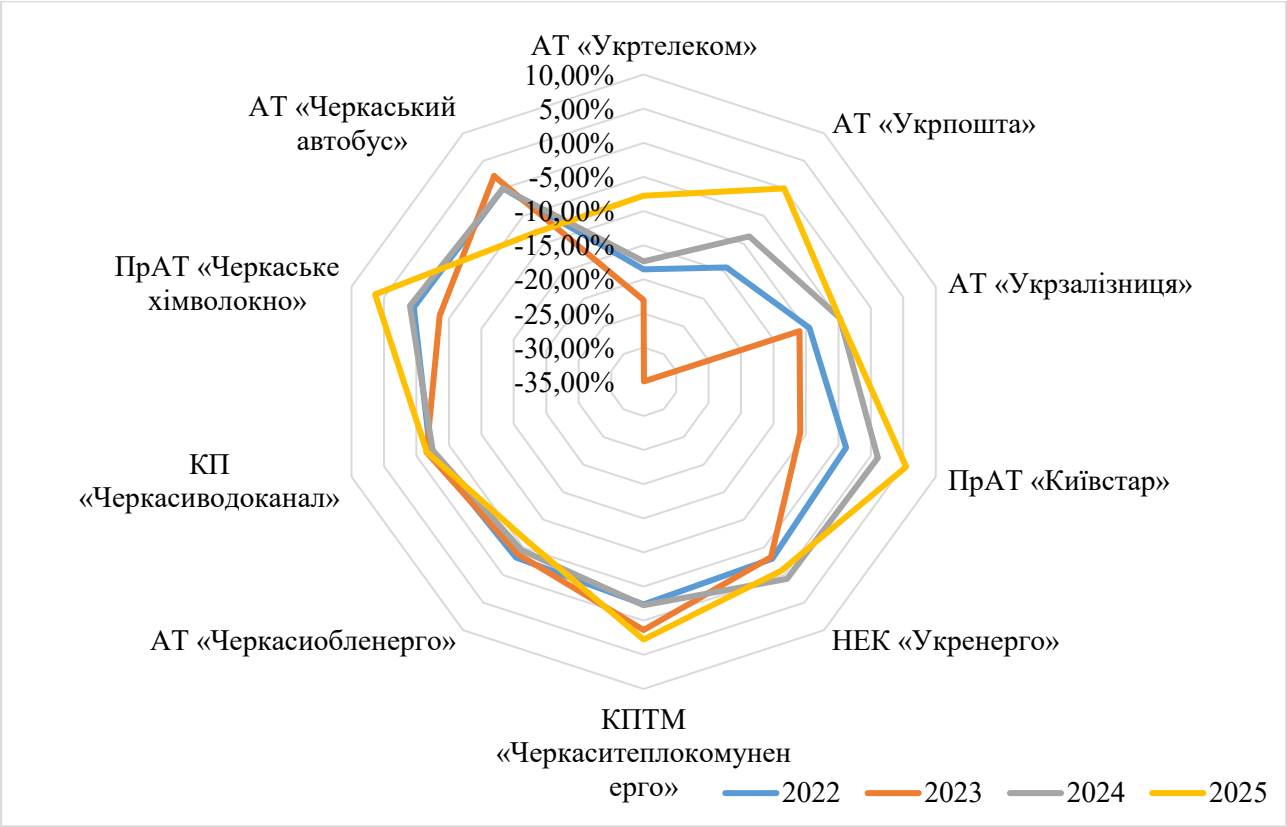


Рисунок 2.4. – Динаміка кількості персоналу підприємств

Джерело: складено автором за даними [234-243]

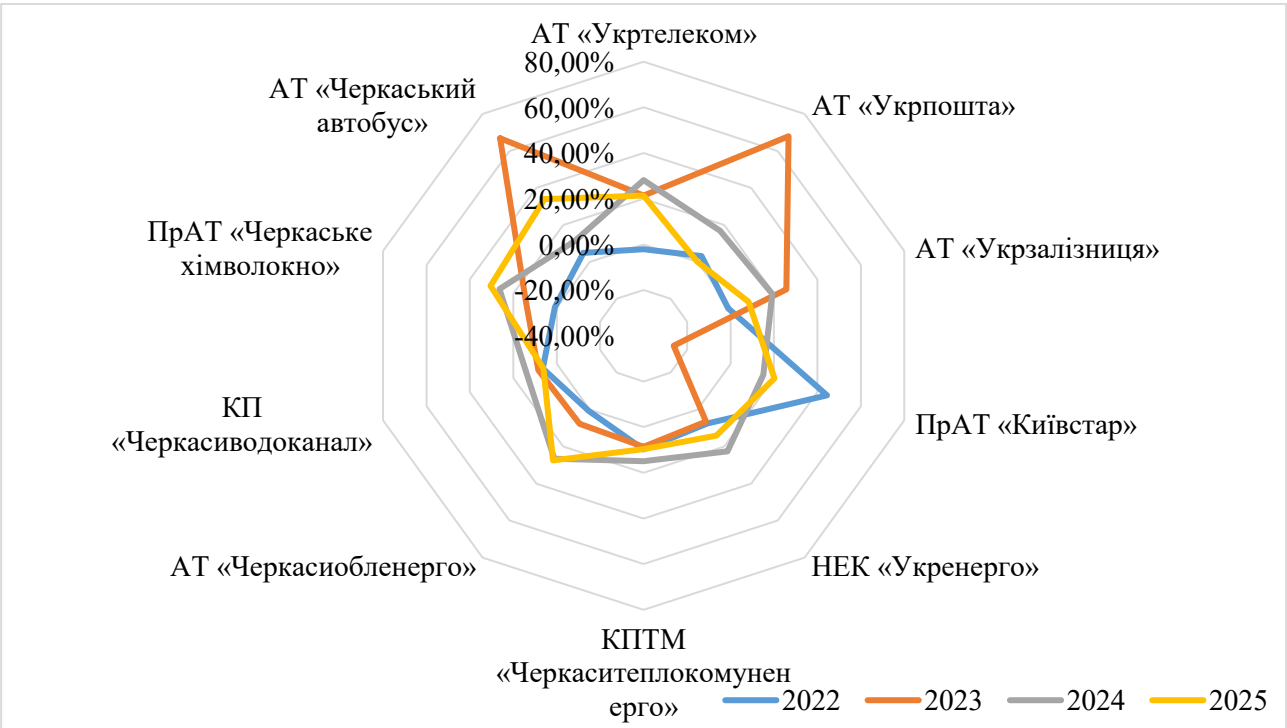


Рисунок 2.5. – Динаміка зміни розміру середньої заробітної плати персоналу підприємств

Джерело: складено автором за даними [234-243]

Рис. 2.6 характеризує динаміку зміни показника доходу підприємств на одного працівника, що дає змогу оцінити продуктивність праці, а також усвідомити взаємозв'язок між станом кадрової та економічної безпеки суб'єктів господарювання.

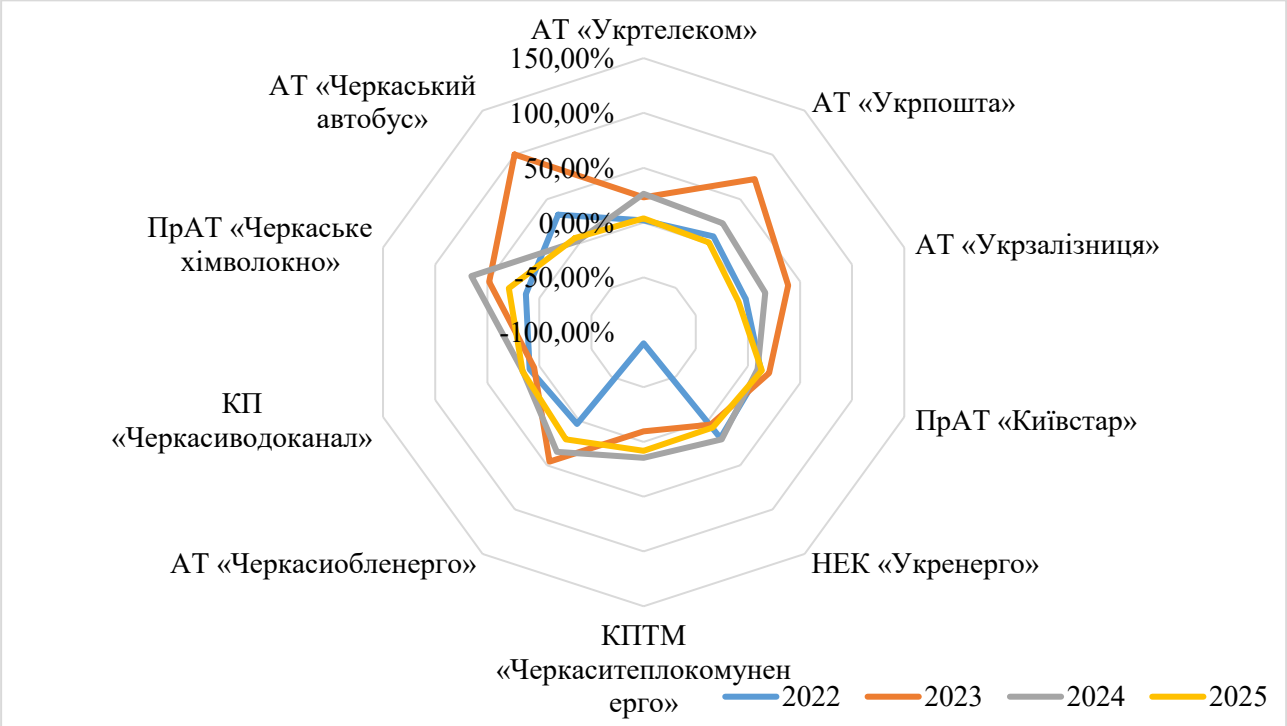


Рисунок 2.6. – Динаміка зміни показника доходу підприємств на одного працівника

Джерело: складено автором за даними [234-243]

Отже, на підставі абсолютних значень показників із Додатку Д та порівнявши їх зміни у динаміці, доходимо висновку, що оптимальний рівень кадрової безпеки мають ПрАТ «Київстар» та НЕК «Укренерго», середній (достатній) рівень демонструють АТ «Укрзалізниця», АТ «Черкасиобленерго», КП «Черкасиводоканал», АТ «Черкаський автобус», а для АТ «Укртелеком», АТ «Укрпошта», КПТМ «Черкаситеплокомуненерго» та ПрАТ «Черкаське хімволокно» характерний низький рівень кадрової безпеки з тенденцією до покращення у 2025 році порівняно з періодом 2022-2023 років.

Табл. 2.6 містить окремі показники фінансового стану підприємств, за якими можна поверхнево оцінити стан їх фінансової безпеки.

Таблиця 2.6. - Показники фінансової безпеки підприємств, 2025 рік

Показники	АТ «Укртелеком»	АТ «Укрпошта»	АТ «Укрзалізниця»	ПрАТ «Київстар»	НЕК «Укренерго»	КПТМ «Черкаситеплокомуненерго»	АТ «Черкасиобленерго»	КП «Черкасиводоканал»	ПрАТ «Черкаське хімволокно»	АТ «Черкаський автобус»
Частка основних засобів в активах підприємства, %	63,38	27,71	77,36	39,75	50,18	52,2	64,32	78,73	8,05	14,59
Коефіцієнт поточної (загальної) ліквідності	0,5	0,86	0,54	1,62	0,32	0,6	0,63	0,8	1,37	2,1
Коефіцієнт фінансової залежності	1,29	12	1,65	1,51	45,18	5,23	2,33	1,95	-5,12	2,09
Коефіцієнт співвідношення позикових та власних коштів	0,29	11	0,65	0,51	44,18	4,23	1,33	0,95	-6,12	1,09
Поточна платоспроможність, грн	-2955647 8	-7393674 8	-106108 8458	15397138	-163706385	-1 626 885 8	-4 442 056	-404 103 8	-5238 097 8	-565 052 8
Рентабельність продукції, %	29,58	12,47	5,85	128,51	11,6	3,28	н/д	н/д	6,52	26,21

Джерело: складено автором за даними [234-243]

Кольором на рисунку виділено ті показники, значення яких є «червоними прапорцями» для стану фінансової безпеки підприємств. Їх значення є або суттєво нижчими за існуючі нормативні чи орієнтовані значення, або негативно характеризують фінансовий стан компанії за відсутності загальновизнаного нормативу.

Рис.2.7, 2.8 і 2.9 демонструють динаміку основних індикаторів фінансової безпеки підприємств.

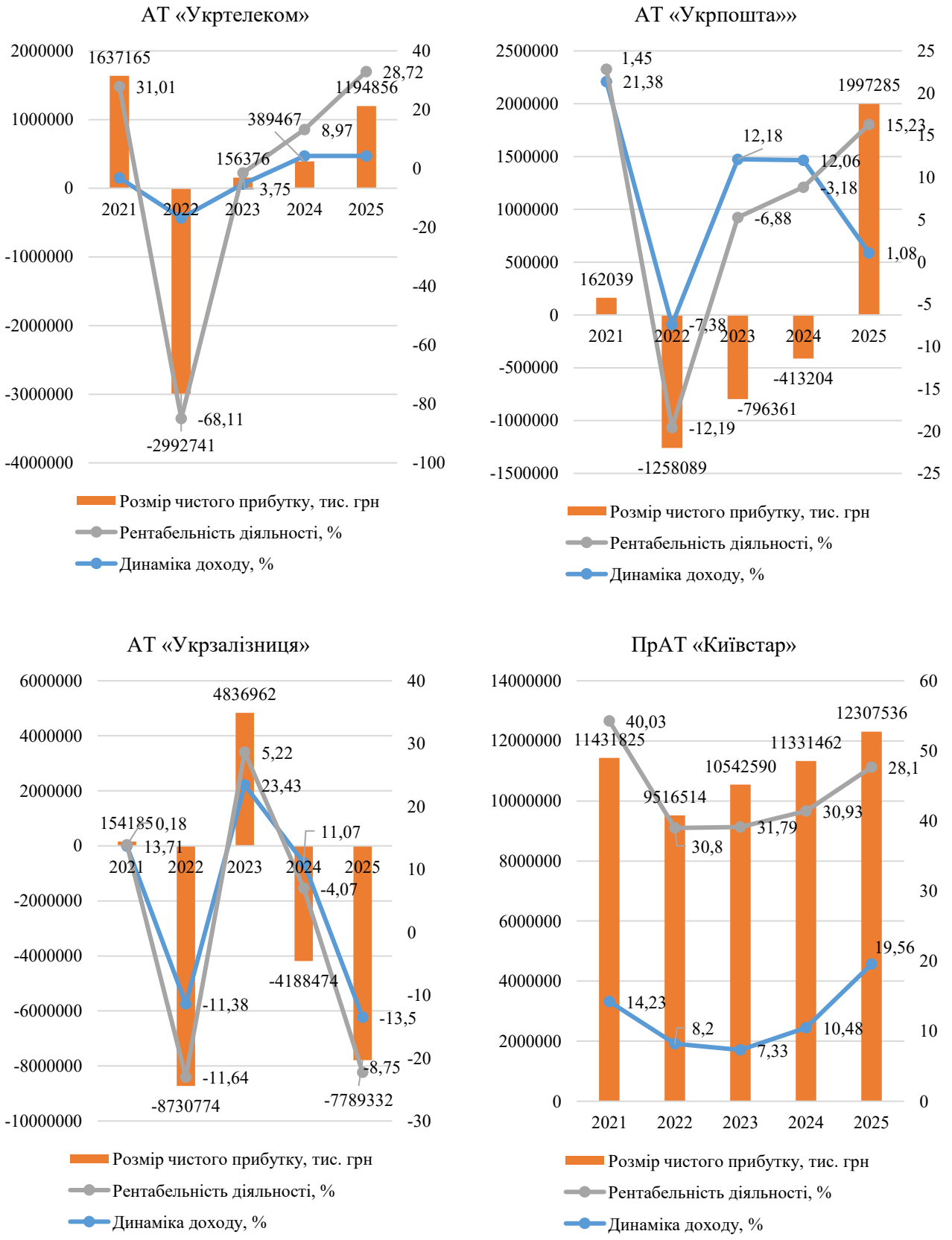


Рисунок 2.7. – Динаміка зміни показників фінансової безпеки АТ «Укртелеком», АТ «Укрпошта», АТ «Укрзалізниця», ПрАТ «Київстар»

Джерело: складено автором за даними Додатку Д

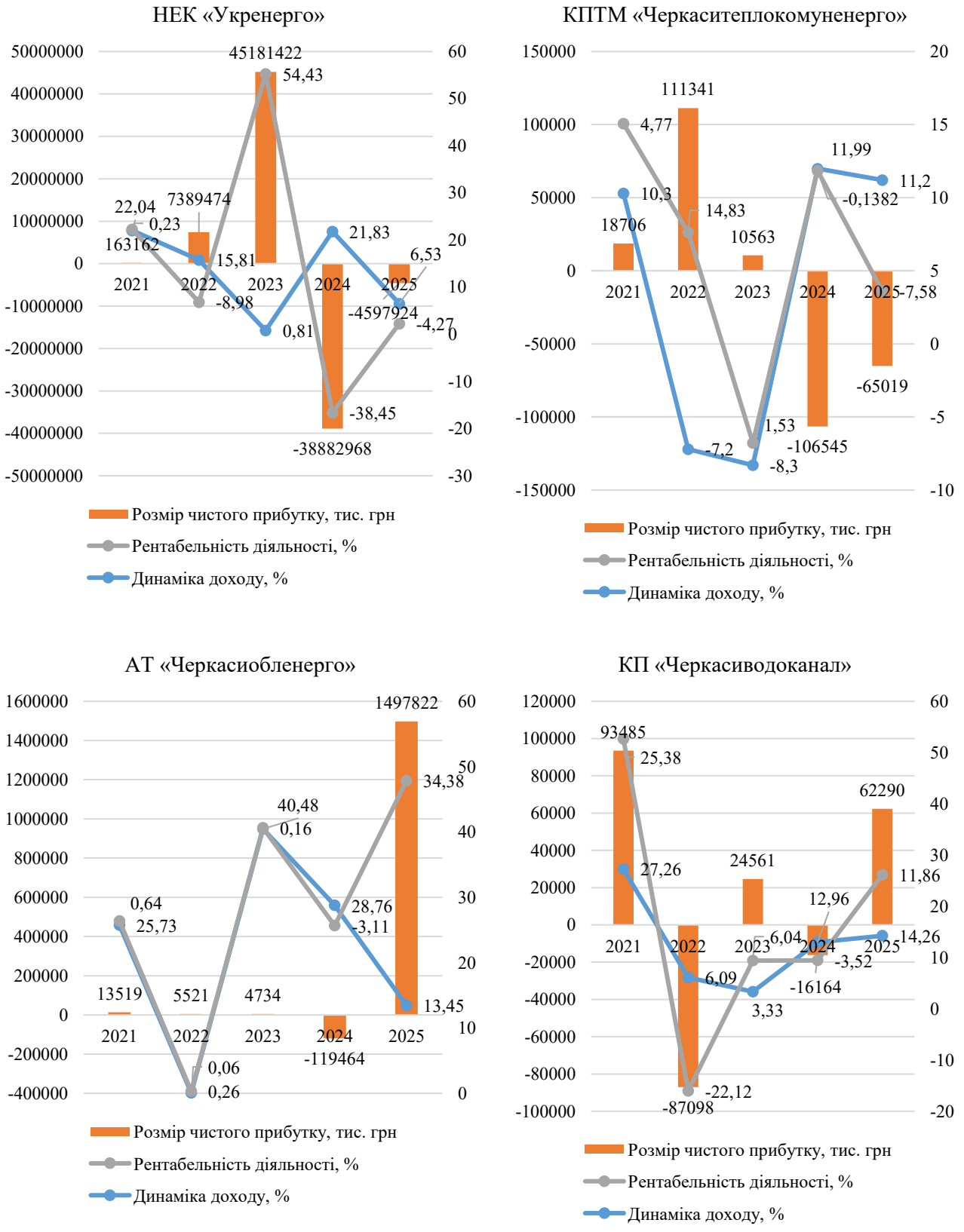


Рисунок 2.8. – Динаміка зміни показників фінансової безпеки НЕК «Укренерго», КПТМ «Черкаситеплокомуненерго», АТ «Черкасиобленерго», КП «Черкасиводоканал»

Джерело: складено автором за даними Додатку Д

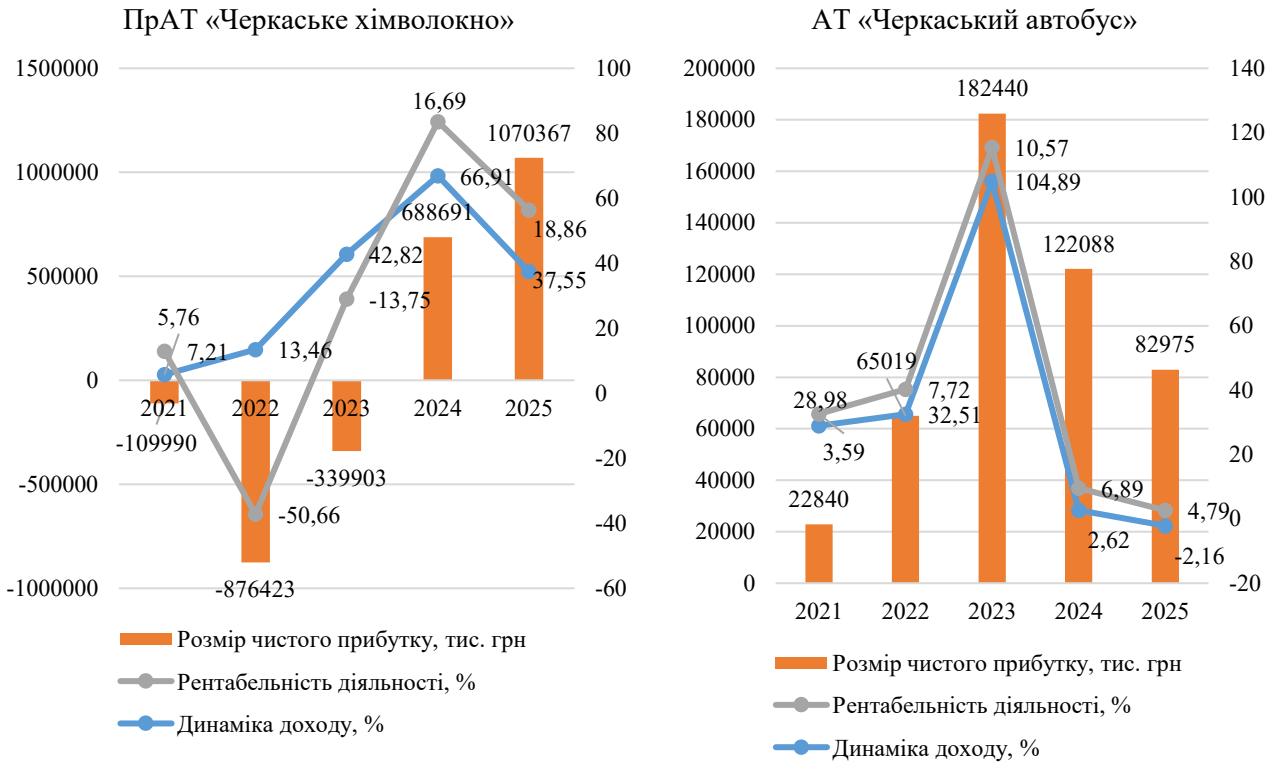


Рисунок 2.9. – Динаміка зміни показників фінансової безпеки ПрАТ «Черкаське хімволокно» та АТ «Черкаський автобус»

Джерело: складено автором за даними Додатку Д

Отже, за результатами оцінювання показників фінансового стану та фінансових результатів діяльності підприємств критичної інфраструктури, маємо зазначити, що найвищий рівень фінансової безпеки демонструє ПрАТ «Київстар», залишаючись стабільно прибутковим підприємством попри реалії світу BANI та численні цифрові ризики. З критичного стану фінансової безпеки у 2025 році вдалося вийти ПАТ «Укрпошта», а от НЕК «Укренерго» – наближається до критичного стану у цьому періоді. Низький рівень фінансової безпеки мають ПАТ «Укрзалізниця» та КП «Черкасиводоканал». Середній рівень фінансової безпеки притаманний для решти компаній – АТ «Укртелеком», КПТМ «Черкаситеплокомуненерго», ПрАТ «Черкаське хімволокно», АТ «Черкаський автобус».

Рис.2.10-2.12 демонструють значення показників майнової (матеріальної) безпеки підприємств.

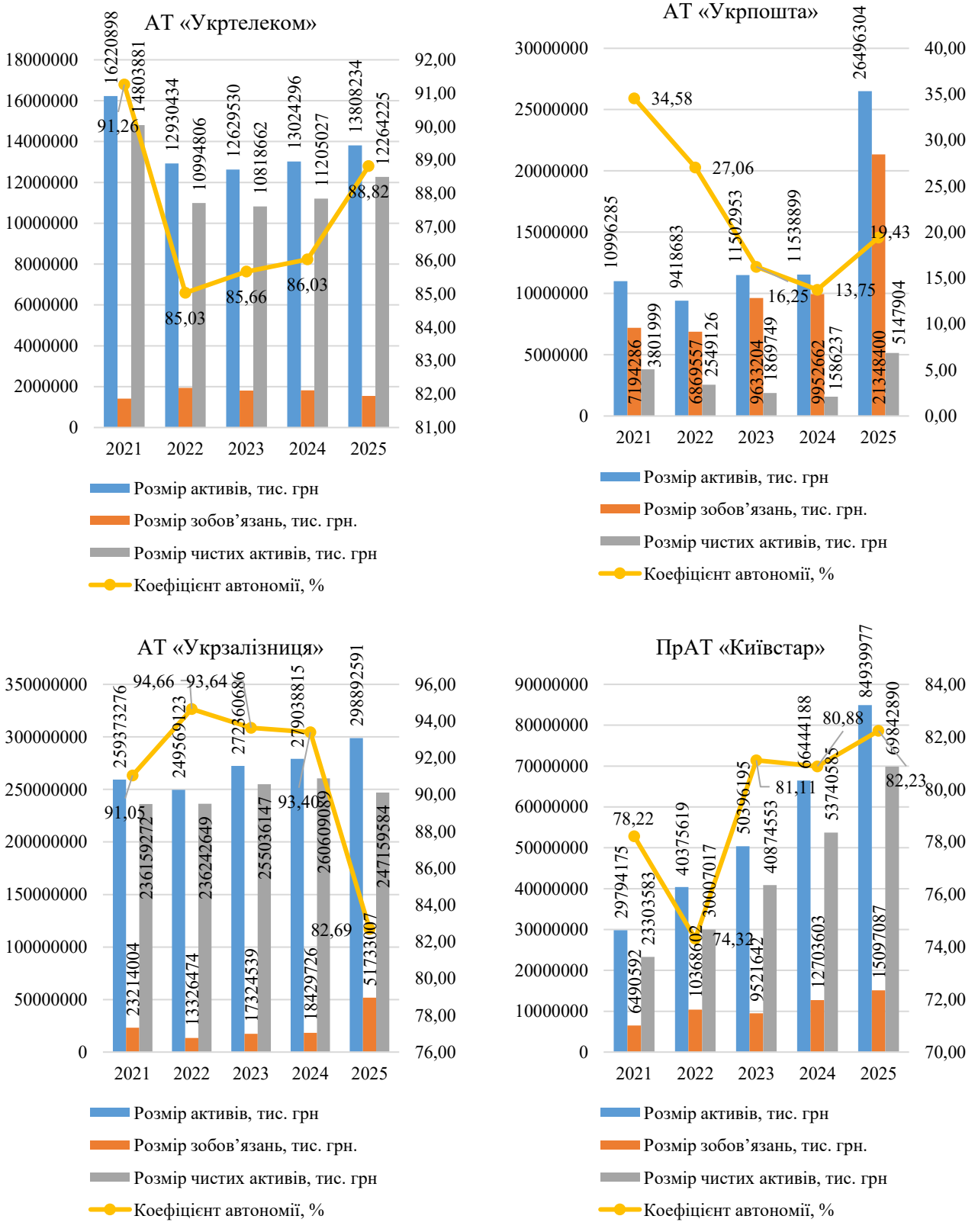


Рисунок 2.10. – Динаміка зміни показників майнової (матеріальної) безпеки АТ «Укртелеком», АТ «Укрпошта», АТ «Укрзалізниця», ПрАТ «Київстар»

Джерело: складено автором за даними Додатку Д

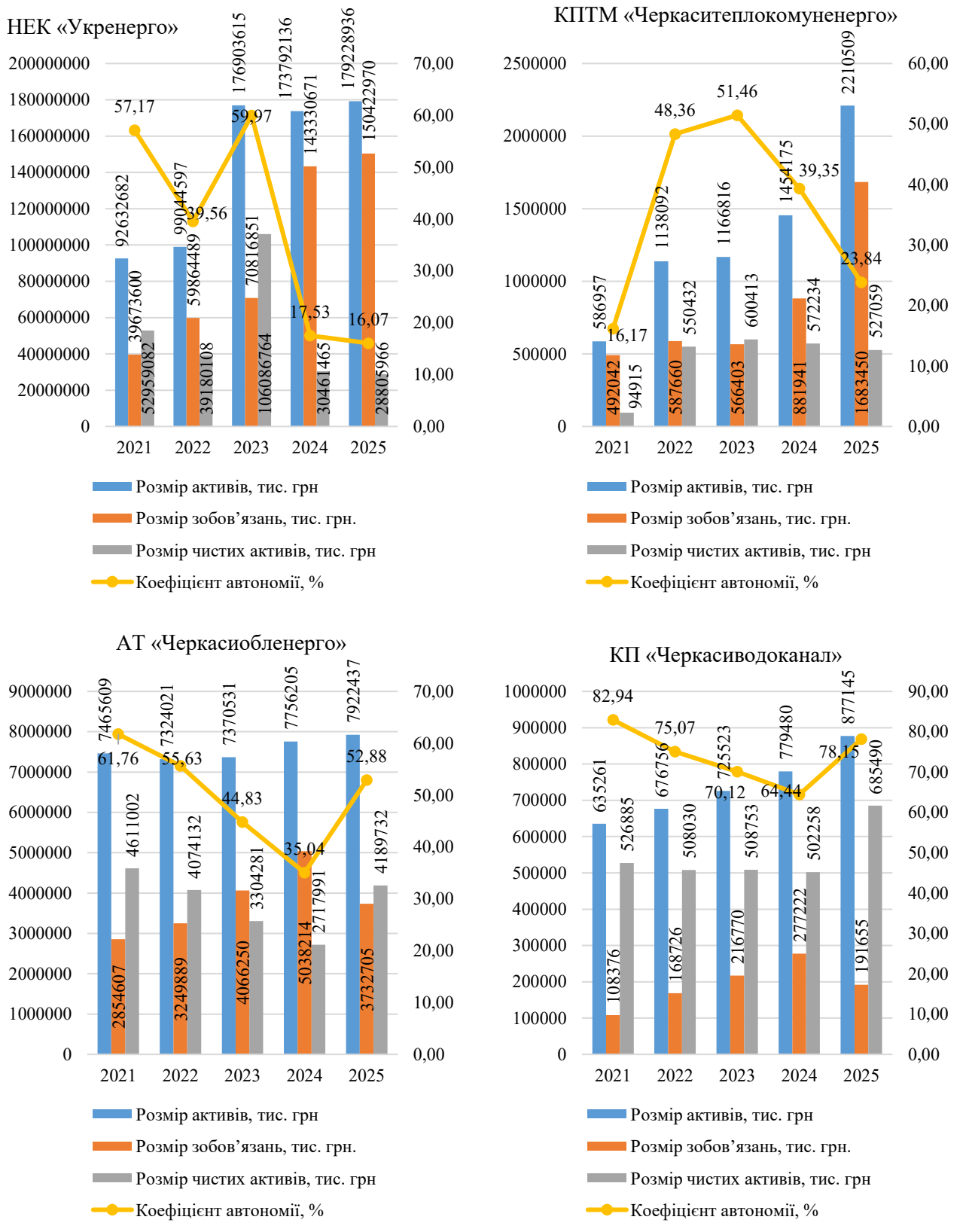


Рисунок 2.11. – Динаміка зміни показників майнової (матеріальної) безпеки НЕК «Укренерго», КПТМ «Черкаситеплокомуненерго», АТ «Черкасиобленерго», КП «Черкасиводоканал»

Джерело: складено автором за даними Додатку Д

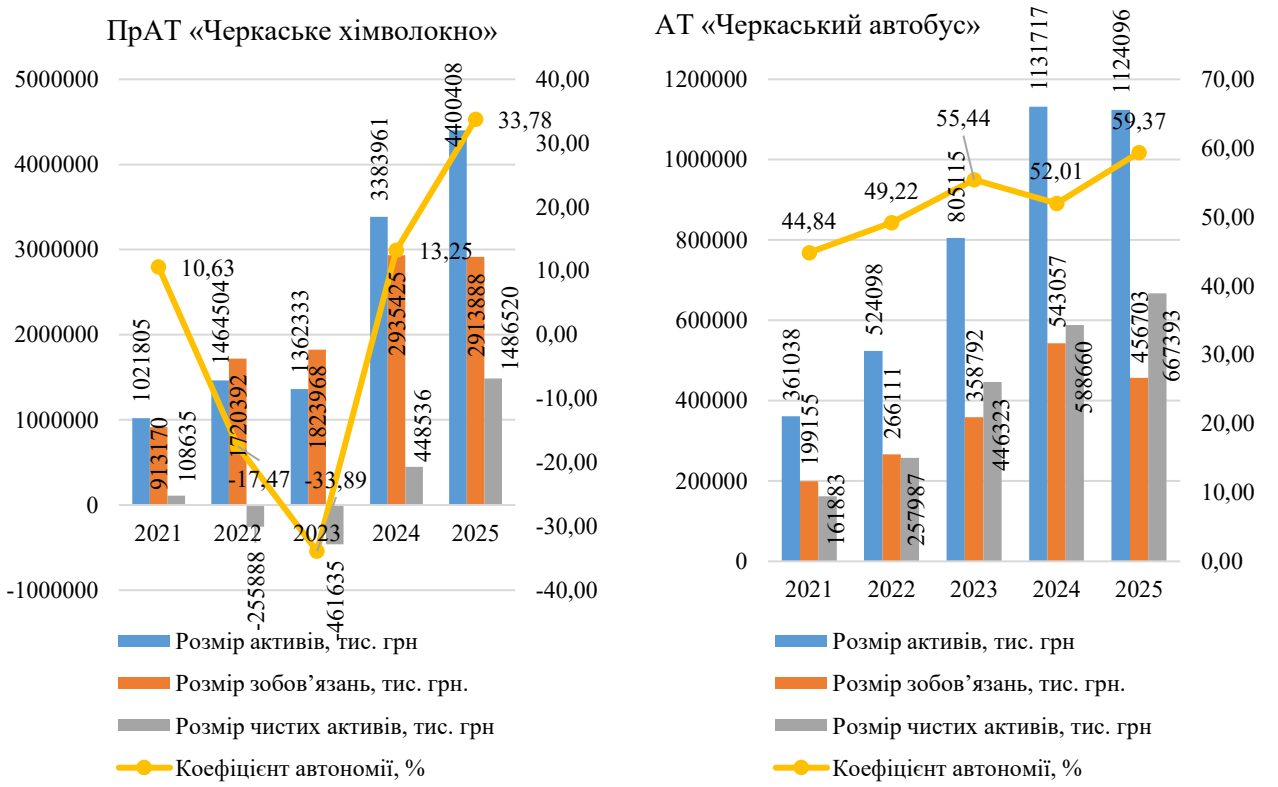


Рисунок 2.12. – Динаміка зміни показників майнової (матеріальної) безпеки ПрАТ «Черкаське хімволокно» та АТ «Черкаський автобус»

Джерело: складено автором за даними Додатку Д

Отже, за показниками майнового стану у динаміці можна зробити висновок про стан матеріальної безпеки досліджуваних підприємств. Найбільшу матеріальну базу мають АТ «Укрзалізниця» та НЕК «Укренерго», за ними слідують АТ «Укртелеком», АТ «Укрпошта» та ПрАТ «Київстар». Цілком логічно, що потужнішу базу активів мають компанії загально національного значення, які завдяки ефекту масштабу, випереджають за показниками майнової безпеки регіональні компанії. Водночас, коефіцієнт автономії демонструє залежність ряду підприємств від позикового капіталу, що свідчить про суттєві економічні ризики та можливість втрати економічної стабільності у перспективі. Загалом, усі регіональні компанії мають середній рівень майнової безпеки, а національні бізнес-структури – високий рівень.

У табл. 2.7 згруповані та оцінені із використанням експертної думки окремі індикатори інформаційної, техніко-технологічної та правової безпеки.

Таблиця 2.7. – Окремі індикатори інформаційної, техніко-технологічної та правової підприємств, 2025 рік

Показники	Характер показника (стимулятор/дестимулятор)	АТ «Укртелеком»	АТ «Укрпошта»	АТ «Укрзалізниця»	ПрАТ «Київстар»	НЕК «Укренерго»	КПТМ «Черкаситеплокомуненерго»	АТ «Черкасиобленерго»	КП «Черкасиводоканал»	ПрАТ «Черкаське хімволокно»	АТ «Черкаський автобус»
Рівень цифровізації бізнес-процесів	с	4	3	3	5	4	2	3	2	2	2
Техніко-технологічне оснащення	с	3	3	3	5	4	3	3	3	2	3
Оновлення обладнання	с	3	2	2	4	5	2	3	2	2	3
Факти і наслідки кібертак	д	3	3	2	5	2	1	1	1	1	1
Наявність механізмів захисту інформації	с	5	4	4	5	5	3	3	3	2	2
Використання інформації з обмеженим доступом	д	5	5	5	5	5	5	5	5	5	3
Рівень цифрової грамотності персоналу	с	4	3	3	4	3	2	2	2	1	2
Наявність і частота судових позовів проти підприємства	д	4	4	5	4	3	3	3	3	3	1
Рівень юридичних ризиків	д	4	4	5	5	4	5	4	5	5	4
Наявність і функціональність юридичного відділу	с	5	4	4	5	5	3	4	3	3	2

Джерело: складено автором на основі [234-243] із використанням експертного методу та методу скорингу (оцінка за 5-бальною шкалою, 1- мінімальне значення)

За усією сукупністю аналізованих показників, можемо зробити висновок про низький рівень інформаційної безпеки у більшості компаній. Кращі захисні механізми для запобіганню зовнішніх втручань у внутрішні бази даних з обмеженим доступом мають підприємства, що характеризуються вищим рівнем цифровізації бізнес-процесів, такі як АТ «Укртелеком» та ПрАТ «Київстар».

Водночас, специфіка їх діяльності та інформаційна активність у цифровому просторі збільшує потребу у комплексному захисті, і кількість відомостей, які мають обмежений доступ, тобто об'єктів системи інформаційної безпеки – у них незрівнянно більша, ніж, до прикладу, у КП «Черкасиводоканал», АТ «Черкасиобленерго» або АТ «Черкаський автобус». Середній рівень інформаційної безпеки мають НЕК «Укренерго», АТ «Укрпошта» та АТ «Укрзалізниця». Низький рівень інформаційної безпеки притаманний для КПТМ «Черкаситеплокомуненерго» та ПрАТ «Черкаське хімволокно». Для останнього з названих підприємств основним чинником, що негативно впливає на стан інформаційної безпеки, є недостатній рівень цифрової грамотності персоналу. В цілому, цей показник є проблемним у більшій чи меншій мірі для усіх досліджуваних компаній.

Стан техніко-технологічної безпеки визначається наявністю сучасного обладнання, періодичним оновленням матеріальної бази, контролем якості продукції і послуг і цифровізацією виробничих і допоміжних процесів. Найбільш технологічними серед об'єктів дослідження є ПрАТ «Київстар», АТ «Укртелеком», НЕК «Укренерго» та АТ «Укрзалізниця». Регіональні комунальні та приватні підприємства – КПТМ «Черкаситеплокомуненерго», АТ «Черкасиобленерго», КП «Черкасиводоканал», ПрАТ «Черкаське хімволокно» - є аутсайдерами у цьому сегменті системи економічної безпеки, оскільки не мають належних фінансових ресурсів для постійних реновацій. Однак, зважаючи на рівень їх соціальної значущості для суспільства, обрані ними стратегії та сприяння інвесторів і державних структур забезпечили перерахованим підприємствам середній рівень техніко-технологічної безпеки.

Оскільки усі аналізовані суб'єкти господарювання перебувають (або перебували в останні п'ять років) у процесах судових суперечок, проте, мають власних представників своїх законних інтересів, і не знаходяться під ризиком ліквідації або рейденського захоплення, стан їх правової безпеки оцінюємо як середній із можливістю до покращення у найближчому майбутньому.

За сукупністю оцінених і підданих експертизі даних із відкритих джерел, що характеризують різні аспекти стану економічної безпеки десяти вітчизняних об'єктів критичної інфраструктури за п'ятирічний часовий період, можемо сформувати рейтинг підприємств за рівнем їх захищеності від зовнішніх і внутрішніх загроз:

1) ПрАТ «Київстар» – високий рівень економічної безпеки;

2) НЕК «Укренерго» – середній рівень економічної безпеки;

3) АТ «Укртелеком» – середній рівень економічної безпеки;

4) АТ «Укрпошта» – середній рівень економічної безпеки;

5) АТ «Укрзалізниця» – середній рівень економічної безпеки;

6) АТ «Черкасиобленерго» – достатній рівень економічної безпеки;

7) КП «Черкасиводоканал» – достатній рівень економічної безпеки;

8) КПТМ «Черкаситеплокомуненерго» – низький рівень економічної безпеки;

9) АТ «Черкаський автобус» – низький рівень економічної безпеки;

10) ПрАТ «Черкаське хімволокно» – низький рівень економічної безпеки.

Отже, проаналізовані підприємства в цілому ефективно реалізують свої безпеко орієнтовані стратегії та частково досягають стратегічних цілей, пов'язаних з досягненням стану економічної безпеки. Водночас, наявність серед об'єктів критичної інфраструктури компаній з низьким рівнем безпеки свідчить про потребу перегляду та адаптації їй стратегій або ж модернізації механізмів і алгоритмів їх реалізації. Якщо підприємства, що мають державну підтримку, не здатні протидіяти ризикам і стикаються з викликами для успішного та ефективного захисту своїх корпоративних ресурсів, то можна сміливо припустити, що у приватному секторі бізнесу ситуація з рівнем економічної безпеки буде суттєво гіршою. Тому необхідно спрямувати вектор наукових пошуків у царину можливостей адаптивної модифікації стратегій вітчизняних підприємств у напрямі підвищення рівня їх придатності для протидії ризикам їх економічній безпеці – як традиційним, так і цифровим.

Висновки до розділу 2

1. Вивчення методичних підходів до розробки стратегій для сучасних підприємств з позицій вітчизняного та зарубіжного досвіду засвідчило, що іноземні компанії активно використовують цифрові стратегії, застосовують цифровий інструментарій для оцінювання ризиків і будують свої перспективні плани на основі аналізу великих масивів даних, у той час, як серед українських підприємств такі підходи тільки набувають популярності. Аналіз особливостей стратегій «кольорових океанів» дозволив розкрити можливості їх використання в Україні у різних галузях економіки. У воєнний час найбільш актуальними та доцільними для запровадження є такі стратегії, як стратегія Червоного океану та стратегія Рожевого океану. Інформаційний базис для обрання підприємством власної стратегії може бути сформовано завдяки використанню класичних прийомів аналізу стану середовища – SWOT-аналізу та PEST-аналізу, а також численних їх модифікацій: PESTEL/PESTLE, STEEPLE, SLEPT, DESTEP, PESTLIED-аналізи, а методами її реалізації рекомендовано обрати метод BSC або Hoshin Kanri.

2. Найбільш формалізованими та доцільними для використання натепер методиками розробки стратегій для підприємств в Україні та в світі було визнано класичний метод стратегічного планування, конкурентний метод, ресурсний метод, сценарний метод, ризик-орієнтований метод, адаптивний (гнучкий) метод, цифровий метод, інноваційний метод (блакитний океан), екосистемний метод і резильєнтний метод. Запропоновано авторський методичний підхід до розробки стратегій для сучасних підприємств в умовах невизначеності та ризиків, перевагою якого є комплексність і всеосяжність, що проявляється у охопленні трьох рівнів менеджменту організації - стратегічного, тактичного та оперативного. На відміну від класичних методичних підходів до розробки та реалізації стратегії, де контроль є завершальним етапом, цей метод адаптований до умов невизначеності та ризиків завдяки інтеграції контролю і моніторингу у кожен стратегічний етап діяльності підприємства, що є критично

важливим кроком для економічної стійкості підприємства в умовах воєнних ризиків, непередбачуваності та нелінійності світу BANI.

3. Виявлено, що для сучасних підприємств характерними є такі цифрові ризики: кібернетичні та технологічні ризики використання цифрових і інформаційних технологій, таргетовані атаки на цифрові екосистеми суб'єктів господарювання, кібершпигунтство, втрата цифрових даних і доступу до них, деградація хмарних сервісів, цифрова міграція (перехід від використання російського ПЗ на аналогічні продукти, які не завжди відповідають потребам вітчизняного бізнесу), фішинг, цифрове інсайдерство, низький рівень цифрової грамотності та цифрових компетенцій. Їх вплив, за умови відсутності своєчасних управлінських рішень, може призвести до недосяжності стратегічних орієнтирів функціонування та розвитку бізнесу та мати руйнівні наслідки для стану економічної безпеки компаній. Відтак, оцінювання цифрових ризиків має бути одним із перших етапів розроблення стратегій безпеко орієнтованого функціонування та відновлення економічного потенціалу українських підприємств у реаліях воєнного часу.

4. Встановлено, що сучасні підприємства мають досить високий рівень цифровізації фінансово-господарських і виробничих процесів, що співвідносне з європейським контекстом цього аспекту розвитку бізнесу. Звіти міжнародних компаній і агентств переконливо свідчать, що чим вищим є рівень цифровізації компанії, тим різноманітнішими та впливовішими є цифрові ризики. Тому планування стратегічних орієнтирів суб'єктів господарювання, які використовують цифрові технології у межах своєї діяльності, має супроводжуватись оцінюванням як традиційних, так і цифрових ризиків. У тому випадку, коли їх потенційний вплив на досяжність довгострокових цілей підприємства характеризується як надмірно високий, менеджменту варто переглянути сценарії стратегії та адаптувати її окреслених реалій і перспектив. Аналіз кейсів вітчизняних і зарубіжних компаній щодо протидії цифровим ризикам дозволив встановити їх деструктивний вплив на стан переважної більшості функціональних складових системи економічної безпеки: фінансової,

інтелектуально-кадрової, техніко-технологічної, інформаційно-аналітичної, виробничої, матеріальної, правої. Це схиляє до висновку про те, що стратегії підприємств, націлені на досягнення та підтримання ними високого рівня економічної безпеки, мають передбачати запровадження принципів цифрового ризик-менеджменту у механізмі безпеко орієнтованого стратегічного управління компанією.

5. На підставі аналізу даних з відкритих джерел та думок експертів, було оцінено рівень економічної безпеки десяти підприємств, що входять до складу критичної інфраструктури України на національному та регіональному рівнях. Саме такі підприємства зазвичай обирають безпеко орієнтовані стратегії функціонування та розвитку, адже їх банкрутство та ліквідація спричинять колосальний резонанс у суспільстві, викличуть соціальну напругу та становитимуть загрозу для життя населення – як фізичного, так і економічного. Виявлено, що ПрАТ «Київстар» має високий рівень економічної безпеки, НЕК «Укренерго», АТ «Укртелеком», АТ «Укрпошта» та АТ «Укрзалізниця» – середній рівень економічної безпеки; АТ «Черкасиобленерго» та КП «Черкасиводоканал» – достатній рівень економічної безпеки; КПТМ «Черкаситеплокомуненерго», АТ «Черкаський автобус» та ПрАТ «Черкаське хімволокно» – низький рівень економічної безпеки. На підставі цього було зроблено висновок, що вітчизняні підприємства в цілому ефективно реалізують свої безпеко орієнтовані стратегії та частково досягають стратегічних цілей, пов’язаних з досягненням стану економічної безпеки. Водночас, наявність серед об’єктів критичної інфраструктури компаній з низьким рівнем економічної безпеки свідчить про потребу перегляду та адаптації їх стратегій або ж модернізації механізмів і алгоритмів їх реалізації.

Отримані у межах розділу наукові результати опубліковані у працях здобувача [137], [170], [173], [201], що наведені у списку використаних джерел.

РОЗДІЛ 3
НАПРЯМИ АДАПТИВНОЇ МОДИФІКАЦІЇ СТРАТЕГІЧНОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ ДЛЯ ПРОТИДІЇ ЦИФРОВИМ РИЗИКАМ ЙОГО ЕКОНОМІЧНІЙ БЕЗПЕЦІ

3.1. Концептуальні засади адаптації стратегічного управління підприємствами під впливом цифровізації

Потреба у адаптивній модифікації стратегічного управління підприємствами у різних площинах і різних контекстах їх фінансово-господарської діяльності виникла не раптово, а пов’язана з глибокими сутнісними трансформаціями функціональних процесів діяльності сучасних підприємств. Окрім загально економічної нестабільності, яка пояснюється поширенням фреймворку світу BANI на теренах сучасної економіки, інтенсифікацією цифрових процесів, масштабуванням тенденцій Індустрії 4.0 та їх переходом у концепцію Індустрії 5.0, наслідками глобальної пандемії, яка послугувала каталізатором для оновлення підходів до управління персоналом, поглибленням філософії клієнтоцентризму, розширенням меж дистанційного обслуговування та переходу у цифровий підприємницький простір, в Україні стимулом для перегляду стратегій діяльності та розвитку підприємств стало повномасштабне вторгнення, яке триває вже майже чотири роки. Усі стратегії, які були прийняті українськими компаніями на періоди з 2022 року, потребували від менеджменту оптимізації та рефокусу ресурсів, калібрування стратегічних орієнтирів на нових викликах, пов’язаних з реаліями воєнного часу, що змусило управлінський персонал ставити на перше місце питання забезпечення безпеки підприємницьких структур, збереження їх людського капіталу, а також захисту активів і потенціалу. Такий підхід засвідчив важливість управління економічною безпекою в умовах невизначеності та тривалої мультикризи. Відтак, на сучасному етапі розвитку економіки України адаптація стратегічного бачення підприємства на середньострокову та

довгострокову перспективу означає намагання його власників і керівників зберегти економічну цілісність бізнесу та потенціал підприємницького виживання попри постійно зростаючу кількість ризиків і загроз, яку важливо підтримати на теоретико-методичному рівні за допомогою розробки рекомендацій та інформаційного підґрунтя для ініціювання та проведення таких стратегічних змін [201, с.84].

Адаптація стратегічного управління підприємствами під впливом цифровізації, зважаючи на стрімке поширення тенденції до цифрових трансформацій бізнес-процесів, опинилася у фокусі уваги багатьох вітчизняних дослідників, і розгляд цієї теми не обмежується лише контекстом забезпечення економічної безпеки. Цифровізація має суттєво більший вплив на різні вектори управління організаціями, що ґрунтовно доводять українські вчені. Наприклад, Криворучко О. М., Шморгун О. А. вивчають особливості розроблення стратегій управління персоналом в умовах цифровізації [244] та роблять акценти на концептуалізації стратегічного кадрового менеджменту [245], Квасницька Р. С., Скоробогата Л. В., Кульгук І. І. аналізують інноваційні стратегії управління ринковою цінністю підприємств за умов цифровізації системи адміністрування в період дії військового стану [246], Коритько Т. Ю. описує механізм управління та формування стратегії адаптації підприємств в умовах цифровізації економіки [247], Лігоненко Л. О. простежує вплив цифровізації на систему управління результативністю підприємств та формування стратегії їх діяльності [248]. Нові можливості для стратегічного управління підприємствами в умовах цифровізації вивчають Логінова О. [249], Паламарчук О. М., Яременко Л. М., Скрипник Р. Є. [250], Сазонова С. В., Новиков Д. М., Макаренко Т. [251], Шиманович П. О., Крілик Б. Б., Якубець М. Р., Волос М. В., Романинець О. В., Цісінський М. М. [252]. Суттєвий внесок у розгляд проблематики стратегічного управління підприємствами різних видів економічної діяльності у період активної цифрової трансформації їх бізнес-процесів зроблено Кирилюк І.М., яка, зокрема, узагальнює сучасні особливості стратегічного розвитку підприємств

[253], упорядковує теоретичні засади управління цифровізацією бізнес-процесів суб'єктів господарювання [254], оновлює та модернізує концептуальні підходи до формування системи управління цифровою трансформацією бізнес-процесів [255], аргументує необхідність управління цифровою трансформацією підприємства для забезпечення його конкурентоспроможності у стратегічній перспективі [256] та описує значення «data-driven» підходу в маркетинговій діяльності та визначає його потенціал в стратегії управління інноваційно орієнтованими вітчизняними підприємствами [257]. У дослідженні Зачосової Н.В. та Коваля О.В. узагальнено роль стратегічного менеджменту для успішного забезпечення економічної безпеки підприємства, що працює в умовах поширення цифрової економіки, у світі, який характеризується мінливістю, невизначеністю, складністю та неоднозначністю [258]. Однак, попри сформованість теоретичного підґрунтя для запровадження технік адаптаційного менеджменту у стратегічному управлінні підприємствами, залишаються малодослідженими аспекти модернізації стратегій сучасних українських компаній під потреби забезпечення їх економічної безпеки, яка зазнає суттєвого негативного впливу не лише від ризиків воєнного часу, але і від цифрових трансформацій бізнес-процесів, що не були належним чином сплановані та обґрунтовані на експертному рівні.

Тому для посилення наукової цінності та практичної значущості цього дослідження було прийнято рішення про необхідність ідентифікації напрямів адаптації стратегічного управління підприємствами під впливом цифровізації задля досягнення стану їх економічної безпеки [201, с.84].

Після початку повномасштабного вторгнення, значна кількість українських компаній зосередили свої стратегії на завданні забезпечення власної економічної безпеки. Водночас, лише задекларовані на папері наміри, без чітких інструментів і алгоритмів їх досягнення, викликали супротив з боку стейкхолдерів, які б воліли отримувати прибутки або задовольняти інші особисті потреби, пов'язані з діяльністю компаній, більше, ніж інвестувати ресурси у захисні механізми бізнесу, які, до того ж, залишались переважно не

конкретизованими та не зрозумілими. Для того, аби стратегії набули безпеко орієнтованого характеру, були сприйняті зацікавленими сторонами позитивно та отримали підтримку на усіх щаблях менеджменту організацій, їх довгостроковими цілями повинні стати: сталий розвиток суб'єкта господарювання, збереження ринкових позицій і клієнтської бази, формування комплексної та багатофункціональної системи економічної безпеки, запровадження та розвиток механізмів захисту корпоративних ресурсів від цифрових ризиків і в цілому під час їх використання у цифровому економічному просторі, тощо. Перехід від традиційних стратегічних орієнтирів функціонування бізнесу, таких як максимізація прибутку, клієнтоцентризм, нарощення економічного потенціалу, вихід на зовнішні ринки товарів і послуг, монопольне становище в галузі, тощо, до описаних вище, можливий за умови адаптації стратегії підприємства до викликів його економічній безпеці, що актуалізує проблему запровадження гнучкого та адаптивного стратегічного менеджменту в українських компаніях [201, с.85].

Квасницька Р. С., Скоробогата Л. В., Кульгук І. І. наголошують на тому, що здатність адаптуватися до криз і продовжувати працювати в тому ж темпі – це прояв резильєнтності системи адміністрування, яка спрямована на збереження та нарощування ринкової цінності підприємства за умов дії воєнного стану [246, с.113]. Таким чином, адаптація стратегічного менеджменту для потреби забезпечення економічної безпеки, заснована на принципі балансування економічних показників розвитку та стійкості, та спланована на засадах антикризового менеджменту та управління ризиками, здатна сфокусувати підприємство на першочергових потребах – по аналогії з пірамідою Маслоу – це потреби у безпеці та збереженні ресурсів, однак, згодом може стати платформою для відновлення або нарощення економічного потенціалу, необхідного для розвитку бізнесу у довгостроковій перспективі.

Реалії воєнного часу посилили загрозу втрати власного людського капіталу підприємствами, що не вжили заходів для адаптації своїх кадрових стратегій до нових викликів. Тому адаптація функціональних управлінських стратегій,

таких, як HRM-стратегії, має стати одним із етапів упорядкування зусиль менеджменту компаній у напрямку збереження трудових колективів та їх інтелектуальної цінності і цілісності. Однак, при формуванні адаптивних HR-стратегій на практиці натепер недостатньо враховуються як внутрішні фактори (структура персоналу, рівень цифрової компетентності, типові функціональні ролі), так і зовнішні виклики (цифровізація, запровадження міжнародних стандартів) [244, с.39-40].

Стратегічний підхід, що поєднує співпрацю та конкуренцію в цифровій сфері, має величезний потенціал для досягнення мети функціонування бізнесу, що прагне бути сучасним і резильєнтним у нестальному та кризовому економічному просторі [246, с.118]. Науковці вважають, що вибір стратегії адаптації фінансово-господарської діяльності у таких умовах, що склалися нині в Україні, слід здійснювати на основі матриці «нестабільність зовнішнього середовища – інтегральний показник адаптивності», що дозволить визначити місце підприємства в адаптаційному просторі та обґрунтувати стратегію [247, с.59]. Існує багато варіантів сучасних стратегій, які спрямовані на відновлення, підтримання, досягнення або зростання рівня економічної безпеки підприємства. Зокрема, можна виділити набір функціональних стратегій, націлених на ефективне функціонування підсистем економічної безпеки – фінансово-інвестиційної, інтелектуально-кадрової, юридичної, інформаційно-аналітичної, тощо. Це такі стратегії, як: фінансова, кадрова (HR-стратегія), техніко-технологічна стратегія (стратегія цифрової трансформації або цифрового розвитку), інформаційна стратегія.

Фінансова стратегія, орієнтована на досягнення стану фінансової безпеки підприємства, має на меті забезпечення нормативного рівня його платоспроможності, ліквідності, фінансової стійкості та на підтримання оптимальної структури капіталу із зовнішніх і внутрішніх джерел, достатньої для того, аби уникнути ризику банкрутства та ліквідації суб’єкта господарювання у перспективі.

Кадрова стратегія спрямована на організацію та реалізацію процесів, пов'язаних зі стратегічним управлінням персоналом. Під стратегічним управлінням персоналом Криворучко О. М., Фемяк О. А. пропонують розуміти комплексний динамічний інтеграційний процес щодо формування, ефективного використання та розвитку персоналу, виходячи із цілісного уявлення про мету підприємства, загальну стратегію та умови забезпечення адаптації до змін у внутрішньому і зовнішньому середовищі. Стратегічне управління розвитком персоналу, мотивацією та маркетингом слід розглядати як окремі напрямки досягнення стратегічних орієнтирів в управлінні підприємством [245, с.119]. Основна мета кадрової стратегії у контексті забезпечення економічної безпеки підприємства полягає у збереженні людського капіталу, протидії звільненню персоналу та плинності кадрів, особливо серед топових фахівців, чия професійна діяльність пов'язана з інтелектуальною працею, вимагає креативності та високого рівня розвитку цифрових навиків.

Техніко-технологічна стратегія, яка в умовах цифровізації може бути трансформована у стратегію цифрового оновлення або цифрового розвитку підприємства, в цілому передбачає запобігання фінансовому та моральному зносу основних засобів до рівня, який унеможливлює їх ефективне та конкурентне використання, та масштабування використання інновацій з метою отримання додаткових якісних переваг для продукції компанії у площині задоволення споживчого попиту та посилення її впливу на ринку завдяки інноваційним підходам в обслуговуванні клієнтів і під час надання їм післяпродажного сервісу.

Також заслуговує на увагу інформаційна стратегія, яка у цифровому інформаційному просторі націлена на підтримання високого рівня кібербезпеки підприємства, організацію збереження цілісності та захисту даних, що використовуються в процесі підприємницької діяльності, від зовнішніх втручань та від недобросовісного використання персоналом суб'єкта господарювання з корисливою метою, а також на підтримання стійкості

цифрової екосистеми компанії та сталого розвитку її функціоналу [201, с.85-86].

Окрім того, що кожна з цих стратегій має власні орієнтири, фокус і пріоритетні завдання, усі вони можуть застосовуватись комбіновано, а також адаптуватись під впливом тих загроз і ризиків, які раптово постають перед менеджментом підприємства на шляху до досягнення його функціональних цілей. Крім того, науковці доводять переваги використання окремої, цілісної стратегії адаптації бізнесу до цифрового середовища під час спроб комплексного забезпечення економічної безпеки суб'єкта господарювання.

Деякі дослідники вважають, що адаптація стратегії підприємства має розумітися на рівні менеджменту як реакція та видозміна його стратегічних векторів у відповідь на загрози, які були ідентифіковані у зовнішньому чи внутрішньому середовищі його функціонування. Сила та продуманість управлінської реакції дозволяють виокремити превентивну стратегію, реактивну або захисну стратегію та адаптивну стратегію. Підприємства, які відрізняються високим рівнем активності та гнучкості управлінського персоналу при прийнятті рішень, що стосуються раптової появи непередбачуваних факторів, проблем, ризиків, здатних призвести до збитків і порушити стан економічної безпеки, найчастіше використовують превентивну стратегію, що спрямована на нейтралізацію та випередження попередньо ідентифікованих загроз та на взаємодію з ними з метою протистояння ще до моменту початку їх негативного впливу на корпоративні ресурси суб'єкта господарювання, їх цілісність та ефективність використання. У системі ризик-менеджменту така стратегія реалізується через механізми раннього попередження та перманентний моніторинг ризиків, оцінювання їх імовірності та потенційних наслідків, ранжування, тощо.

Реактивна або захисна стратегія на практиці є більш «хаотичною», непослідовною, вимагає від керівництва підприємства та його фахівців з економічної безпеки лідерських якостей, ініціативності та здатності швидко приймати управлінські рішення, оскільки її ідеологія спрямована на вироблення

реакції на настання певної несприятливої події, унаслідок якої підприємство може отримати збитки, та націлена на відновлення стану його економічної безпеки, а не на підтримку її високого рівня впродовж тривалого проміжку часу, як це передбачено в превентивній стратегії [201, с.86].

Адаптивна стратегія здається особливо актуальною в умовах тривалої мультикризи, а також у реаліях воєнного часу, і характеризується гнучкістю щодо планування цільових показників стратегічного розвитку підприємства, шляхів їх досягнення та параметрів системи прийняття управлінських рішень, здатних оперативно оновлюватися у залежності від оцінки фахівцями стану зовнішнього середовища діяльності суб'єкта господарювання та ризиків, які є для нього характерними у певний момент часу. Зокрема, Коритько Т. Ю. вважає, що впровадження стратегії адаптації в умовах цифрової трансформації на підприємстві є ключовим фактором забезпечення довгострокового сталого розвитку та їх виживання [247, с.60]. Варто відзначити, що стратегія адаптації і адаптація стратегії – на рівні ідеології менеджменту та на прикладному рівні – різні поняття, які, однак, значна кількість дослідників використовує як синонімічні терміни. Адаптація стратегії – це динамічний та гнучкий процес ініціювання та виконання послідовних управлінських дій, спрямованих на коригування довгострокових цілей підприємства, а також шляхів, інструментів і засобів їх досягнення, що розпочинається як реакція на зміни у внутрішньому та зовнішньому середовищі, які є суттєвими для досяжності планових показників його діяльності. Отже, адаптація стратегії узагальнено – це процес її коригування. У свою чергу, стратегія адаптації – це розроблений послідовний план дій (а не процес їх виконання, що є сутнісною відмінністю між досліджуваними дефініціями), націлений на підвищення рівня резильєтності підприємства через використання гнучкого управління його реакціями на виникнення непередбачуваних ризиків і загроз у економічному просторі (у тому числі у його цифровому вимірі).

На окрему увагу заслуговує і дефініція «адаптована стратегія» – як бажаний і очікуваний з позиції стратегічного менеджменту результат

докладання управлінських зусиль і витрат ресурсів у процесі адаптації стратегії до ризиків і викликів діяльності суб'єкта господарювання, що мають тривалу дію або є характерними для неї впродовж тривалого проміжку часу [201, с.86].

Лігоненко Л. О. наголошує, що у сучасній науковій літературі недостатньо розкритим залишається питання, яким чином цифрові платформи впливають на формування та реалізацію стратегій діяльності підприємств, а також як змінюється роль керівника в цифровому середовищі [248, с.221]. Тому на рис.3.1 здійснено спробу концептуалізації процесу адаптації стратегічного управління підприємствами під впливом цифровізації.

Рисунок 3.1. - Концептуалізація процесу адаптації стратегічного управління підприємствами під впливом цифровізації

Джерело: [201, с.87]

Отже, адаптація стратегічного управління підприємством під впливом цифровізації має свої особливості у порівнянні з класичними практиками адаптивного менеджменту. Існує думка, що механізм адаптивного управління підприємством на основі цифрових платформ необхідно розглядати як сукупність засобів (форм, методів) та інструментів керуючого впливу на структуру управління та функції управління при взаємодії суб'єкту та об'єкту [247, с.59]. Однак, пропонована дефініція не містить вказівки щодо того, як мають враховуватись цифрові ризики, зокрема, стратегічні, у цьому процесі. Також сучасні цифрові інструменти трансформують управлінське середовище підприємства, забезпечуючи не лише оперативне контролювання результативності, але й формуючи підґрунтя для побудови інноваційних стратегій розвитку [248, с.222]. Крім того, цифровізація впливає на усі елементи процесу стратегічного управління підприємством, такі як формування стратегії (перехід до гнучких форматів стратегій, побудованих на великих масивах цифрових прогнозних даних), встановлення стратегічних цілей (перегляд і оновлення планових показників – без встановленої періодичності, за потреби), прийняття стратегічних рішень (мультивибір з прогнозних сценаріїв, побудованих із використанням штучного інтелекту), коригування стратегії (адаптивне планування за допомогою використання сценарного прогнозування) та забезпечення прозорості стратегічного менеджменту (стратегічний моніторинг у режимі реального часу зі спільним доступом стейкхолдерів до даних, що не містить таємницю) [248, с.223].

З метою ефективного стратегічного управління суб'єктом підприємництва в умовах цифровізації Логінова О. рекомендує реалізувати такі заходи: аналізувати технологічні тенденції, впроваджувати цифрові інструменти управління, забезпечувати кібербезпеку, розвивати цифрові компетенції персоналу, створювати цифрові стратегії маркетингу та продажу, аналізувати дані для прийняття рішень, підтримувати інноваційну культуру, адаптувати стратегії до змін [249, с.126].

Отже, цифрові технології стали важливим елементом стратегічного планування для підприємств в Україні. Вони надають можливість підвищити гнучкість, оптимізувати процеси прийняття рішень та швидко адаптуватися до змін ринкової кон'юнктури. Використання великих масивів даних, штучного інтелекту та цифрових платформ сприяє підвищенню конкурентоспроможності українських підприємств та їх адаптивності до нових викликів [250, с.95].

Рис. 3.2 демонструє перспективні напрями адаптації стратегічного управління підприємствами під впливом цифровізації задля досягнення стану економічної безпеки.

Резильєнтність системи адміністрування залежить від того, наскільки ефективно працюють системи загалом, а не лише від того, наскільки вони залишаються безпечними [246, с.115]. У свою чергу, ефективність цифрової трансформації стратегічного управління значною мірою залежить від наявності чіткої поетапної стратегії впровадження, формування цифрової культури управління, розвитку цифрових компетенцій персоналу та забезпечення цілісної інформаційної архітектури підприємства [248, с.225].

Як вважають Сазонова С. В., Новиков Д. М., Макаренко Т., сучасні підприємства в умовах цифрової економіки отримують унікальну можливість впроваджувати гучкі та адаптивні моделі стратегічного управління підприємством, а також, в деяких випадках ситуативну систему управління [251, с.119]. Механізми стратегічного управління, ефективно розроблені в руслі цифровізації, мобілізують використання науково-технологічного, інноваційного, фінансово-економічного, соціального та організаційного потенціалу [252, с.178], а також після їх запровадження – суттєво економлять час і кадровий ресурс підприємства, мінімізують кадрові ризики, пов'язані з суб'єктивністю персоналу у питаннях, що перебувають на стику інтересів кількох стейкхолдерів, і це дозволяє змінити стан економічної безпеки, навіть попри появу нових цифрових ризиків.

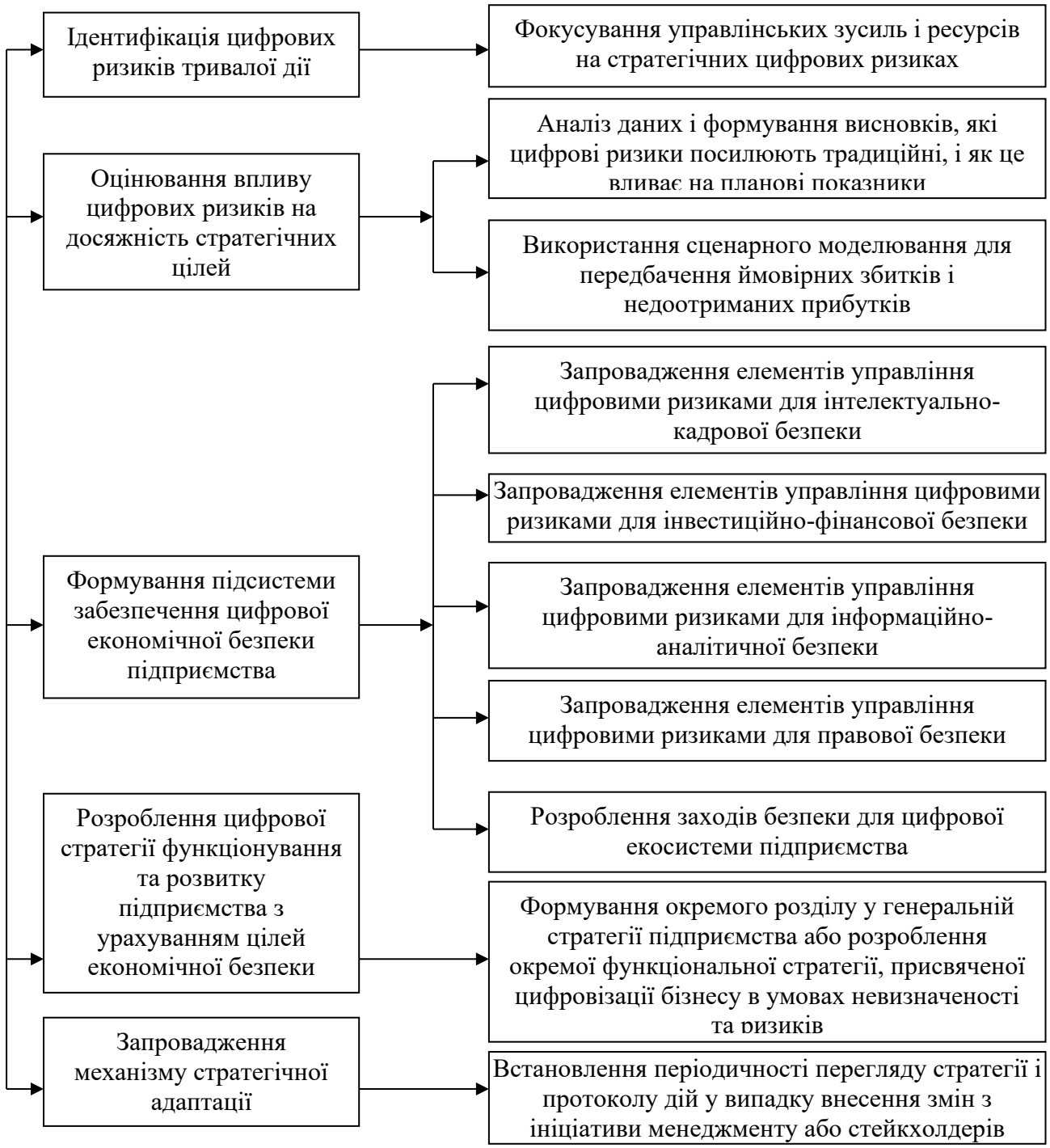


Рисунок 3.2. - Напрями адаптації стратегічного управління підприємствами під впливом цифровізації задля досягнення стану економічної безпеки

Джерело: [201, с.88]

Отже, проведене дослідження підвалин, можливостей та особливостей адаптації стратегічного управління підприємствами під впливом цифровізації задля досягнення стану економічної безпеки дало змогу зробити такі висновки.

Концептуально процес адаптації стратегічного управління підприємством під впливом цифровізації має розпочинатися з розроблення алгоритму адаптації існуючої стратегії, який охоплюватиме всі рівні менеджменту суб'єкта господарювання, але особливо буде сфокусованим на оперативному та стратегічному рівнях. Взаємо доповнення управлінських дій і цілей під впливом нових реалій господарського оточення підприємства дозволить оновити його стратегічні орієнтири та уникнути дисбалансу інтересів стейкхолдерів, які швидко змінюються з плином часу і під час виходу компанії на цифрові ринки або у їх нові сегменти. Водночас, процес адаптації має враховувати традиційні та цифрові загрози та ризики, які виникають раптово, і вимагають управлінських реакцій у цифровій екосистемі бізнесу. Розроблений менеджерами проєкт адаптованої стратегії має бути поширений цифровими каналами комунікації, які діють у компанії, для всебічного його обговорення, у результаті якого можна сподіватися на успішну оптимізацію стратегічного управління підприємством у цифровому просторі. Пріоритетними напрямками адаптації стратегічного управління підприємством під впливом цифровізації мають стати: цифровий менеджмент, цифровий маркетинг та, зважаючи на реалії функціонування українських підприємств, цифровий ризик-менеджмент. Саме ці три вектори претендують на роль ідеологічних колон для адаптованої стратегії підприємства, здатної гарантувати його економічну безпеку у цифровому економічному просторі. У свою чергу, успішна реалізація такої стратегії дозволить зберегти та масштабувати вплив компанії на ринку із використанням при цьому можливостей цифровізації.

Фокусування сучасних українських підприємств на меті досягнення стану власної економічної безпеки, що є підґрунтям для їх сталого розвитку та економічного виживання в умовах невизначеності та ризиків, викликає необхідність у конкретизації напрямів адаптації стратегічного управління підприємством під впливом цифровізації у напрямку безпеко орієнтованого менеджменту. Серед таких напрямів було обрано: ідентифікацію цифрових ризиків тривалої дії, оцінювання впливу цифрових ризиків на досяжність

стратегічних цілей бізнесу, формування підсистеми забезпечення цифрової економічної безпеки підприємства, розроблення цифрової стратегії функціонування та розвитку суб'єкта господарювання з урахуванням цілей економічної безпеки та запровадження механізму стратегічної адаптації до тих загроз і викликів, які цифровізація несе для стану економічної безпеки підприємства на довгостроковому часовому горизонті [201, с.89-90].

Наукове підґрунтя для формування концептуальних засад адаптації стратегічного управління підприємствами під впливом цифровізації має будуватися на основі таких змін у парадигмах безпеко орієнтованого стратегічного менеджменту. Традиційні стратегічні підходи, у яких конкурентні переваги підприємства забезпечуються унікальними ресурсами у класичній формі – кадровими, матеріальними, фінансовими, тощо, поступаються місцем ефективному використанню цифрових ресурсів, екосистем, адаптованих управлінських підходів до цифрових трансформації бізнес-процесів, діджиталізованих інформаційних платформ, які стають стратегічними корпоративними активами та базою для посилення конкурентних позицій підприємства. У площині управління персоналом домінуючою стала теорія поціновування компетенції працівників, їх поступового розвитку через системи навчання та самоосвіти з метою підвищення рівня цифрової грамотності задля використання інтелектуального потенціалу для досягнення стратегічних орієнтирів бізнесу, а також формування здатностей до безпеко орієнтованої поведінки для забезпечення внутрішніх механізмів управління традиційними та цифровими ризиками. Для пришвидшення інтеграції цифрових технологій у різні функціональні напрями менеджменту організацій і оновлення бізнес-процесів за допомогою аналітики великих даних необхідним на управлінському рівні є застосування системного підходу. Той факт, що кібернетичні та інші цифрові ризики набувають системного характеру для бізнесу, формує стійкі підвалини для популяризації ризик орієнтованого менеджменту стратегічного управління підприємствами, націленого на досягнення стабільного стану економічної безпеки.

3.2. Оновлення механізму стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів

Оновлення механізму стратегічного управління економічною безпекою підприємства має здійснюватися нині із фокусом на баланс інтересів стейкхолдерів. Такий підхід є критичною необхідністю у ситуації, коли вітчизняні компанії чинять спроби ефективного переходу до парадигми цифрової стійкості та протидії викликам довготривалого функціонування бізнесу у реаліях світу BANI.

У сучасних умовах функціонування підприємств найбільше шансів на досягнення стратегічних орієнтирів будуть мати підприємства, в яких загально організаційні цілі та цілі окремих учасників стратегічного процесу будуть співпадати. Головною проблемою при узгодженості всіх цілей зацікавлених сторін виступає пошук таких параметрів розвитку організації, які б дозволили досягати задоволення потреб кожного учасника стратегічного процесу [152, с.191].

Серед багатьох функціональних напрямів менеджменту організацій, управління економічної безпекою є одними з найбільш резонансних та спірних серед учасників управлінського процесу, зокрема, якщо розглядати його з позиції стратегічних інтересів стейкхолдерів бізнесу. Така проблема виникає тому, що стан економічної безпеки підприємства у значній мірі визначається тим, чи готові власники відмовитися від частини можливостей отримати дохід, які дають їм наявні ризики, та витратити ресурси на захист економічного потенціалу замість того, аби фінансувати існуючі активи у масштабування підприємницької діяльності та збільшення обсягів прибутку.

Українські підприємства рідко мають розроблену та затверджену стратегію забезпечення власної економічної безпеки. Як аргументовано у другому розділі цього дослідження, безпеко орієнтовані стратегії функціонування та розвитку використовуються переважно суб’єктами господарювання, які належать до об’єктів критичної інфраструктури. Більш

поширеною у площині вітчизняного бізнесу є практика включення розділу, що описує наявні ризики та окреслює підходи до управління ними, у існуючі стратегії суб'єктів господарювання. Тому якщо економічний ландшафт для підприємства змінюється, з'являються нові загрози та виклики для його можливостей залишатись на ринку та зберігати клієнтуру, виникає нагальна потреба адаптувати стратегічні орієнтири під зміну моделі економічної поведінки компанії, переформатувати витрати корпоративних ресурсів у напрямку протидії деструктивному впливу небезпек на фінансово-господарський стан і результати її діяльності, тощо [259, с.95].

Адаптацію в найбільш загальному варіанті доцільно розуміти як послідовну науково-організовувану програму дій, яка стосується основних складових підприємства як соціально-економічної системи, результатом реалізації якої має стати пристосування до змінених умов ведення фінансово-господарської діяльності [260, с.101]. Для того, аби використати адаптацію як інструмент узгодження інтересів стейкхолдерів у площині забезпечення економічної безпеки бізнесу, необхідно: ідентифікувати потреби та бажання зацікавлених осіб щодо діяльності підприємства в цілому та щодо стану захищеності його корпоративних ресурсів, побудувати карту стейкхолдерів, яка стане інструментом візуалізації та усвідомлення впливу кожного з них на прийняття управлінських рішень і конкретизацію стратегічних орієнтирів компанії, створити карти ризиків, які продемонструють зміну ймовірності впливу негативних наслідків ризиків на економічні результати бізнесу за умови прийняття рішення на користь задоволення того чи іншого інтересу стейкхолдера та запропонувати альтернативи – з меншим рівнем ризиків, прийняття яких, однак, може супроводжуватись потребою когось із зацікавлених сторін поступитись своїми амбіціями, прагненнями та бажаннями або відкласти їх задоволення у часі.

Те, наскільки стратегія може бути адаптованою під зміни умов господарської діяльності підприємства, які є джерелом формування більшості ризиків для стану його економічної безпеки, визначає адаптаційний потенціал

суб'єкта господарювання. Адаптаційним потенціалом, виходячи з аспектів безпекової діяльності, потрібно вважати всі наявні ресурси й можливості, які можуть бути задіяні для реалізації заходів, спрямованих на адаптацію до впливу внутрішніх і зовнішніх загроз, що виникають через зміну умов функціонування, відповідно до стратегії розвитку підприємства задля вдосконалення керуючої й керованої підсистем у межах системи управління економічною безпекою як основи підтримання стійкості та забезпечення розвитку [261, с.85-86]. Адаптаційним потенціалом можуть бути вміння та навики управлінського персоналу у царині ризик-менеджменту. Особливу цінність має здатність фахівців прогнозувати прояви ризиків у залежності від оцінки економічних, соціальних, цифрових тенденцій зовнішнього середовища. Такий метод превентивного безпеко орієнтованого менеджменту дає своєчасне інформаційне підґрунтя для оновлення стратегій підприємства, забезпечує можливість досягнення їх реалістичності та досяжності бажаних економічних результатів.

Адаптація існуючої стратегії – це перший етап трансформації менеджменту організацій у площині підвищення рівня її гнучкості у середньо та довгостроковій перспективі. Наступний етап розвитку стратегічного менеджменту для підприємств, які функціонують в умовах невизначеності та ризиків і націлені на підтримання високого рівня власної економічної безпеки – це комплексна адаптивна стратегія економічної безпеки. Василега В. вважає, що адаптивна стратегія забезпечення економічної безпеки є найважливішою ланкою комплексної системи та складного багатоетапного процесу реалізації стратегічного управління підприємством. Вона визначає об'єкти, індикатори, показники, небезпеки та загрози, основні механізми та заходи їх запобігання, ліквідації з урахуванням реальних обмежень ресурсів в умовах мінливого зовнішнього середовища [262]. Спроби узгодження інтересів стейкхолдерів можуть знайти відображення у формуванні менеджментом компанії кількох альтернативних варіантів для кожного названого елементу стратегії. Наприклад, суттєво спростити прийняття безпеко орієнтованих управлінських

рівень може ранжування загроз і ризиків. Для топових позицій ризик-рейтингу вживатимуться заходи уникнення та страхування (за можливості), а для стейкхолдерів, на досяжність інтересів яких такі ризики впливатимуть, буде проведено інформаційну компанію з роз'ясненнями потенційних втрат від прояву ризику для стратегічних цілей підприємства. Ризики, що будуть визнані найменш небезпечними, доцільно використати як можливості для масштабування бізнесу після того, як буде розроблено та схвалено механізми та бюджети компенсації їх потенційних наслідків для стану економічної безпеки суб'єкта господарювання. Для того, аби стратегія могла бути швидко адаптованою до нових умов або до впливу ризиків, вона повинна будуватися на таких принципах, як системність, багатофакторність, превентивність, варіативність, ієрархічність, інноваційність, цілісність, динамічність, комплексність, гнучкість [262].

Адаптація до змін має свою ціну – це ресурси, які необхідно витратити для своєчасної реакції на зовнішнє та внутрішнє середовище функціонування [262]. Проте, розроблення нової стратегії стане більш вартісним і часовитратним процесом, а залишення стратегічних орієнтирів незмінними у ситуації, коли кількість ризиків для стану економічної безпеки бізнесу зростає, може зробити цілі підприємства недосяжними, а збитки – суттєвими.

Адаптація стратегії управління підприємством до ризиків економічній безпеці як засіб узгодження інтересів його стейкхолдерів може бути реалізованою через запровадження механізму компромісного управління, за допомогою якого можна буде гнучко та своєчасно змінювати стратегічні пріоритети діяльності підприємства в залежності від тих інтересів його стейкхолдерів, якими ті не готові поступитися навіть попри пов'язані з ними ризики. З іншого боку, використання процесу адаптації як «комунікаційного містка» між учасниками системи менеджменту підприємства та бенефіціарами прийняття управлінських рішень сприятиме формуванню атмосфери взаємоповаги та людиноцентрованості у управлінні суб'єктом господарювання. Оскільки адаптація стратегії означає перегляд цілей функціонування та

розвитку бізнесу, інформаційне забезпечення цього процесу має бути пріоритетом ініціаторів трансформацій і лідерів перемовин. Адаптація до ризиків економічній безпеці дозволить оновити стратегічні цілі підприємства аби гарантувати їх досяжність у нових формулюваннях або форматах, що відповідає інтересам більшості стейкхолдерів, зацікавлених у збереженні компанією ресурсного потенціалу та ринкових позицій [259, с.96].

Науково-методичне підґрунтя для розробки пропозицій щодо оновлення механізму стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів базується на наукових напрацюваннях таких сучасних дослідників, як Бедрій Д. І. [263], Бєлобородова М. В., Олійник Т. І. [264], Власенко Т., Котельникова Ю., Городецька Т., Помогалова Н. [265], Давидов О. І. [266], Кавецький В. В. [267], Казіміров М. А. [268], Коваленко В., Сергєєва О., Іванова Т. [269], Петренко В. С. [270], Федичишин А. С., Ніронов Д. А. [271], Шкромида В. В., Максимів Ю. В., Гнатюк Т. М. [272]. Найбільш суттєвими напрацюваннями щодо інтеграції стейкхолдер-орієнтованого підходу в систему стратегічного управління підприємством із врахуванням ризиків цього процесу вважаємо публікації таких авторів, як Кильницька Є. В., Сергієнко Ю. І., які узагальнюють теоретико-методичні аспекти організації управління підприємством з позиції взаємодії зі стейкхолдерами [273], Роїк О. Р., що займається питанням оцінки ризиків при побудові стейкхолдерної моделі стратегічного управління туристичним бізнесом [274], Залуцька Х. Я., Гнат І. А., Стефанцов Д. В., які описують процес стратегічного управління підприємством з урахуванням особливостей його взаємодії зі стейкхолдерами [275], Портна О. В., Цвар О. О., що конкретизують стратегічні зміни в управлінні персоналом на засадах світового досвіду застосування стейкхолдерно-орієнтованих підходів [276], Нор В. В., що доводить роль інформаційної прозорості в управлінні економічною безпекою підприємств із використанням стейкхолдер-орієнтованого підходу [277]. Ці джерела створюють потужний теоретичний фундамент для пошуку аргументів на

користь оновлення механізму стратегічного управління. Наприклад, Нор В. В. підтверджує тезу про те, що цифрова інтеграція управлінської звітності у процеси стратегічного менеджменту відповідає ціннісним інтересам стейкхолдерів і виступає важливим чинником забезпечення інформаційно-аналітичної безпеки бізнесу [277]. Стейкхолдер-орієнтована модель ІТ-підприємств, запропонована Петренко В. С. дає змогу провести паралель між ІТ-сектором і виробленими у ньому цифровими стратегіями управління ризиками та будь-яким підприємством, що проходить крізь етапи цифрової трансформації бізнес-процесів і відчуває суттєві цифрові ризики для стану власної фінансово-економічної безпеки [270]. Ризик-орієнтовані підходи, запропоновані у джерелах [263, 274], дають змогу інтегрувати стейкхолдер-менеджмент безпосередньо у моделі оцінювання ризиків, що використовуються менеджерами під час розроблення стратегій управління економічною безпекою.

Ризики для інтересів стейкхолдерів, які полягають у тому, що очікувані підприємством та його зацікавленими сторонами результати та заплановані показники не будуть досягнуті вчасно або в повній мірі, трансформуються від таких, що мають локальні негативні наслідки (вплив на внутрішні корпоративні ресурси компаній) у екосистемні, які впливають на усіх учасників економічних відносин, що мають пов’язані з діяльністю підприємства, професійні або особисті цілі. Кейси сучасних компаній, які були розглянуті у другому розділі цього дослідження, довели дієвість «принципу доміно» у системі стратегічного ризик-менеджменту підприємства. Зокрема, цифровий ризик втрати інформації або блокування доступу до неї для одного зі стейкхолдерів, наприклад, для підприємства, яке є постачальником ІТ-послуг, суттєво впливає на стан економічної безпеки суб’єктів господарювання, яким ці послуги надаються, та їх клієнтам, які ними користуються безпосередньо або опосередковано. Таким чином, адаптація механізму стратегічного управління економічною безпекою має відбуватися у напрямку забезпечення масштабного охоплення цифрової та операційної стійкості не лише підприємства, яке ним послуговується, але і усіх учасників, дотичних до його бізнес-процесів або їх фінальних результатів.

Цифровізація поглиблює протиріччя між різними категоріями стейкхолдерів, як внутрішніми, так і зовнішніми, створює нові «точки напруги», викликані можливостями і ризиками цифрових трансформацій бізнесу. Як переконливо демонструє розроблена автором матриця інтересів стейкхолдерів сучасних підприємств (табл.3.1), яку пропонується використовувати топ-менеджментом у процесі оновлення стратегій розвитку як інструмент інформаційного забезпечення адаптивного менеджменту, власники та інвестори, тобто основні фінансові спонсори діяльності підприємств, прагнуть максимізації розмірів його (а відповідно, і власних) прибутків через швидку цифровізацію, тобто використати цифрові трансформації переважно з фінансовою метою. У свою чергу, персонал підприємств вбачає у цифровізації ризики для свого перебування у штаті компаній, а відтак, може чинити опір цифровим змінам як через острах звільнення, так і по причині низької цифрової грамотності, підвищення якої має стати стратегічним орієнтиром для розвитку підприємств і елементом win-win стратегій між управлінцями та виконавцями професійних завдань. Клієнти компаній, споживачі їх продукції і користувачі послуг зацікавлені у всебічному та надійному захисті своїх персональних даних, які підприємства збирають і зберігають у інформаційних базах, що підпадають під вплив цифрових ризиків і неодноразово були пошкоджені внаслідок кібернетичних і хакерських атак. Традиційний механізм стратегічного управління економічною безпекою підприємства на разі досить умовно, формально та декларативно враховує той факт, що ігнорування інтересів однієї групи стейкхолдерів (наприклад, економія на заробітній платі, навчанні основам цифрової грамотності або захисті персональних даних клієнтів) призводить до критичних втрат інтелектуального потенціалу та репутаційних втрат. Дисбаланс інтересів внутрішніх стейкхолдерів – причина конфліктів, джерело формування загроз і ризиків для інтелектуально-кадрової, фінансової, правової складових комплексної системи економічної безпеки. Дисбаланс інтересів зовнішніх стейкхолдерів – причина недофінансування, втрати конкурентних позицій на ринку та інших стратегічних ризиків.

Таблиця 3.1. – Матриця інтересів стейкхолдерів сучасних підприємств як інструмент інформаційного забезпечення адаптивного менеджменту

Категорія стейкхолдерів	Стратегічні інтереси	Інтереси щодо цифрових ризиків	Інтереси щодо стану економічної безпеки	Ризики у разі неврахування інтересів
Власники підприємства	Зростання вартості підприємства, прибутковість, рентабельність	Захист цифрових активів, персональних даних, відсутність кібератак	Стабільність прибутків, відсутність ризику банкрутства і ліквідації	Втрата інвестицій, брак джерел фінансування, фінансова дестабілізація
Топ-менеджмент	Виконання стратегічних планів, ефективність управління ресурсами	Ініціювання і моніторинг цифрових трансформацій, оцінка кіберзагроз	Стійкість і ефективність обраної бізнес-моделі, мінімізація ризиків	Кризи менеджменту організацій, стратегічні прорахунки
Персонал	Висока заробітна плата, якісні умови праці, мотивація	Захист даних, підвищення цифрової грамотності	Інтелектуальна, фізична та кадрова безпека	Зниження продуктивності праці, плинність кадрів
Клієнти, споживачі продукції і послуг	Якість продукції/сервісів, доступність, оновлення	Захист персональних даних, безпека фінансових транзакцій	Надійність і безперервність постачання товарів і послуг, доступні ціни	Втрата клієнтів, зменшення товарообігу, репутаційні збитки
Постачальники, партнери	Стабільність і надійність співпраці	Захист логістики і ланцюгів постачання	Своєчасне виконання зобов’язань	Витрати на встановлення нових партнерств
Держава та владні структури	Відповідність законодавству, фіскальна дисципліна	Кібербзахист від хакерських атак, уникнення соціальних наслідків	Економічна стабільність, збереження людського капіталу	Штрафи, санкції, судові позови, репутаційні збитки, обмеження діяльності
Інвестори, кредитори, інші фінансові донори	Повернення інвестицій, отриманні прибутку	Прозорість цифрових операцій, захист комерційних таємниць	Фінансова стійкість, платоспроможність, капіталізація, дохідність	Зростання вартості капіталу, пошук фінансових альтернатив
Об’єднані територіальні громади	Робочі місця, продуктивна зайнятість	Захист інформації, екологічні цифрові ініціативи	Зниження соціальної напруги, добробут громади	Безробіття, відсутність кадрового ресурсу, соціальні кризи
IT-провайдери, надавачі цифрових послуг	Довгострокова співпраця, повна цифровізація бізнес-процесів	Надійність і ефективність цифрової інфраструктури	Техніко-технологічна та інформаційно-аналітична безпека	Зупинка діяльності, втрата ресурсів, фінансові витрати
Конкуренти	Збереження впливу у ринковій ніші	Отримання переваг у цифровому середовищі	Добросовісна конкуренція	Втрата конкурентних переваг

Джерело: складено автором

У якості посилення інформаційної бази для побудови моделі адаптованого до інтересів стейкхолдерів механізму стратегічного управління економічною безпекою підприємства було проведено SWOT та STEEPLE-аналізи, результати яких містяться у табл. 3.2 та 3.3.

У результаті проведених аналітичних процедур вдалося виявити, що традиційні механізми стратегічного безпеко орієнтованого менеджменту підприємств критичної інфраструктури характеризуються зависокими рівнями формалізації та контрольованості. У періоди планової економіки це було б перевагою, та означало б здатність суб'єкта господарювання правильно прогнозувати та планувати майбутні показники та неухильно дотримуватися курсу їх досягнення, подекуди навіть нехтуючи можливостями, які з'являються з плином прогресу. Однак, в умовах цифровізації бізнес-процесів і BANI-середовища традиційні стратегії втрачають ефективність через низьку адаптивність, відсутність цифрового ризик-менеджменту і ігнорування інтересів стейкхолдерів. Тому пропонованим у межах цього дослідження напрямом їх трансформації та осучаснення є перехід до гнучких, ризик-орієнтованих і стейкхолдер-центрованих моделей стратегічного менеджменту.

В умовах війни та постійного зростання цифрових ризиків, економічна безпека стає тим ресурсним фундаментом, без якого економічне зростання бізнесу тривалий час, як того вимагає ідеологія стратегічного управління, неможливе. Тому оновлений механізм безпеко орієнтованого стратегічного менеджменту повинен будуватися на результатах комплексного аналізу цифрових ризиків, що має використовуватись у якості «адаптивного фільтру» для існуючих стратегій, які зараз перебувають на різних етапах реалізації, який дозволить ідентифікувати стратегічні цілі або орієнтири (за умови використання принципів гнучкого проєктного менеджменту у системі стратегічного управління), що не підкріплені реальним рівнем захисту цифрових корпоративних ресурсів або є надмірно ризиковими та примарно досяжними по причині цифрової неспроможності функціонування та розвитку бізнесу.

Таблиця 3.2. – SWOT-аналіз традиційних механізмів стратегічного управління економічною безпекою підприємств критичної інфраструктури

	Можливості (Opportunities) 1. Балансування інтересів стейкхолдерів для підвищення лояльності та залучення інвестицій. 2. Впровадження інструментів ШІ та аналізу великих даних для моніторингу загроз і ризиків. 3. Підвищення прозорості цифрової звітності та комунікації зі стейкхолдерами. 4. Залучення грантів і інших форм фінансування для цифровізації бізнес-процесів.	*Загрози (Threats)* 1. Зростання інтенсивності кібератак на екосистеми бізнесу. 2. Фізичні руйнування матеріальної бази та дефіцит ресурсів на її відновлення та модернізацію. 3. Втрата кваліфікованих кадрів (через міграцію і внутрішні переміщення). 4. Неможливість прогнозування законодавчих змін, тарифних обмежень і цін на ринках товарів і послуг.
Сильні сторони (Strengths): 1. Наявність чітких алгоритмів дій і нормативної бази діяльності. 2. Досвід фізичного захисту матеріальних об'єктів і персоналу. 3. Структурованість управління, підпорядкування та ієрархічність рішень. 4. Наявність підрозділів безпеки. 5. Бронювання цінних працівників.	*Адаптація сильних сторін до можливостей (SO-адаптована стратегія)* 1. Інтегроване звітування шляхом використання екосистеми і управління для запровадження цифрової інтеграції звітності, що задовольнить інтереси інвесторів та держави одночасно. 2. Цифрова модернізація системи економічної безпеки завдяки запровадженню системи раннього виявлення загроз засобами ШІ за підтримки фінансових донорів.	*Адаптація сильних сторін до загроз (ST-адаптована стратегія)* 1. Використання досвіду класичної фізичної охорони об’єктів для побудови архітектури «екосистемного захисту», де фізичний контроль доступу до даних поєднується з кіберзахистом і цифровою безпекою. 2. Формування кадрового резерву шляхом використання статусу об’єкта критичної інфраструктури та системи бронювання працівників для утримання топових ІТ-фахівців і кризових менеджерів.
Слабкі сторони (Weaknesses) 1. Неврахування інтересів стейкхолдерів (пріоритет державним і суспільним інтересам). 2. Орієнтація на реактивне реагування на ризики замість проактивного запобігання їм. 3. Низький рівень гнучкості управління. 4. Низька цифрова грамотність. 5. Недостатня увага до корпоративної культури і цифрової гігієни праці.	*Адаптація слабких сторін до можливостей (WO-адаптована стратегія)* 1. Запровадження стейкхолдер-менеджменту як елементу механізму управління економічною безпекою на основі комунікаційних платформ і каналів, що дозволить отримувати оперативні дані щодо їхніх інтересів та зменшити рівень соціальної напруги у колективі. 2. Ініціювати навчання персоналу для підвищення рівня цифрової грамотності персоналу та формування у працівників здатності до безпеко орієнтованої поведінки та самоменеджменту.	*Адаптація слабких сторін до загроз (WT-адаптована стратегія)* 1. Антикризова реструктуризація стратегування: трансформація «управління успіхом» в «управління спроможністю», відмова від ігнорування інтересів стейкхолдерів, запровадження принципу нульової довіри, щоб мінімізувати кадрові ризики. 2. Аутсорсинг безпеки та цифровізації бізнес-процесів шляхом передання частини цифрового моніторингу спеціалізованим зовнішнім стейкхолдерам (провайдерам кібербезпеки) для посилення рівня цифрового захисту та пришвидшення діджиталізації.

Джерело: складено автором

Таблиця 3.3. – STEEPLE-аналіз традиційних механізмів стратегічного управління економічною безпекою підприємств критичної інфраструктури

Фактор	Вплив на традиційний механізм	Наслідки для економічної безпеки
Соціальний (Social)	Орієнтація на жорстку управлінську ієрархію; нехтування потребами персоналу як стейкхолдерів діяльності компанії.	Зростання плинності кадрів, посилення опору змінам, низька цифрова гігієна і цифрова грамотність працівників (вразливість до соціальної інженерії і інших ризиків цифрових шахрайств).
Технологічний (Technological)	Використання ізольованих внутрішніх цифрових систем; акцент на матеріальній і фізичній безпеці в умовах ризиків воєнного часу та надання цифровим ризикам другорядної ролі.	Вразливість перед атаками на управлінські та інформаційні системи, неможливість швидкого відновлення бізнес-процесів після зовнішніх втручань, витрати на відновлення даних.
Економічний (Economic)	Залежність від обсягів державного фінансування та встановлених тарифів; акцент на мінімізації поточних витрат, потреба у фінансових альтернативах.	Фінансування безпекових заходів за «залишковим принципом»; високий рівень фінансових ризиків, неможливість достовірно прогнозувати витрати на відновлення безпеки.
Екологічний (Environmental)	Дотримання мінімальних нормативних вимог щодо екології, якості та енергоефективності, відсутність бюджетів для досягнення цілей сталого розвитку та захисту навколишнього середовища.	Високі штрафи, компенсаційні витрати та репутаційні збитки у разі техногенних аварій, спричинених кібератаками або фізичними пошкодженнями обладнання, споруд чи будівель або неправильної організації виробничих процесів (кадрові ризики).
Політичний (Political)	Залежність підприємств від політичних рішень, тенденцій воєнного стану, державного регулювання та фіскального навантаження.	Ризик раптової зміни стратегічних пріоритетів фінансово-господарської діяльності, затримки у прийнятті управлінських рішень або реагування на прояви ризиків через бюрократизацію бізнес-процесів.
Юридичний (Legal)	Функціонування підприємств регламентується чинним законодавством, яке часто не враховує можливостей і темпів цифрових трансформацій бізнесу.	Неготовність персоналу та екосистеми підприємства до нових стандартів захисту даних (GDPR) і складність правового захисту від цифрових втручань і кібератак.
Етичний (Ethical)	Низький рівень прозорості прийняття стратегічних управлінських рішень; відсутність етичних протоколів організації комунікації зі стейкхолдерами, збереження та використання їх цифрових даних і інтелектуального потенціалу.	Втрата довіри стейкхолдерів до підприємства; етичні дилеми менеджерів під час обрання між потребою заощаджувати обмежені ресурсу та забезпечувати безпеку персоналу або клієнтів (як у кейсах медичних компаній, дані про пацієнтів яких було розсекречено).

Джерело: складено автором

Використання STEEPLE-аналізу дозволило навести додаткові аргументи на користь авторських припущень, що традиційний механізм стратегічного управління економічною безпекою є фрагментарним і зарегульованим. Він добре працює з правовими та політичними ризиками, але майже повністю лишає поза увагою менеджменту підприємств етичні та соціальні фактори, що створює середовище для неврахування інтересів стейкхолдерів і нехтування їх потребами, а також не здатен впоратися з технологічними викликами світу BANI, у якому цифрові ризики є нелінійними та важко прогнозуються.

Кожен із семи факторів STEEPLE-аналіз містить власні «дестимулятори» для механізму стратегічного управління економічною безпекою (наприклад, моральне застаріння обладнання в T або низький рівень лояльності персоналу у S). Оновлений механізм стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів має функціонувати як «коректор», що перетворює ці ризики на можливості через балансування інтересів стейкхолдерів (наприклад, через цифрову інтеграцію звітності для задоволення інтересів L, E та S одночасно).

У реаліях світу BANI навіть невеликий функціональний збій у цифровій екосистемі підприємства може спричинити «ефект доміно» – розпочати деградацію і руйнування інформаційно-аналітичної підсистеми економічної безпеки та завершитись колапсом її фінансової і правової складових. Водночас, класичні аналітичні методи ретроспективного аналізу, які слугують інформаційним підґрунтям для планування перспективних стратегічних орієнтирів, надають історичні дані, що були релевантними для стратегічного управління на початку цього століття, однак, виявляються неактуальними у реаліях цифрової економіки, коли відомості змінюються швидко, а їх обсяг потребує використання штучного інтелекту та цифрових інструментів для ефективного їх опрацювання та узагальнення. На разі очевидною є потреба у розробці динамічного механізму стратегування, який дозволить оперативно моделювати імовірнісні сценарії зміни стану економічної безпеки підприємства за умови оновлення інтересів стейкхолдерів. Матриця Менделоу у цьому

контексті дозволяє оцінити, як інтереси груп стейкхолдерів впливають на стратегічні орієнтири підприємства (табл.3.4).

Таблиця 3.4. – Оцінювання впливу стейкхолдерів на стратегічні орієнтири підприємства згідно матриці Менделоу

Влада / Інтерес	Низький рівень інтересу до стратегічних орієнтирів	Високий рівень інтересу до стратегічних орієнтирів
Високий рівень влади (впливу)	*Сектор B:* потребує потреб і інтересів стейкхолдерів за законом (стейкхолдерами є державні регулятори, органи місцевого самоврядування. Орієнтир для стратегії: комплаєнс-менеджмент, дотримання нормативів цифрової безпеки, тарифів.	*Сектор C:* потребує максимально можливого задоволення інтересів і потреб стейкхолдерів (інвесторів, топ-менеджменту, власників бізнесу). Орієнтири для стратегії: фінансова стійкість, безперервність бізнес-процесів, комплексний захист активів.
Низький рівень влади (впливу)	*Сектор A:* потребує мінімальних зусиль з боку менеджменту для задоволення інтересів стейкхолдерів, якими є: постачальники дрібних витратних матеріалів, віддалені громади, міноритарні споживачі. Орієнтир для стратегії – це операційна ефективність, постійний моніторинг трендів ринків.	*Сектор D:* потребує інформації і комунікації до стейкхолдерів з боку менеджменту (стейкхолдери – це персонал, населення, екологічні активісти. Орієнтир для стратегії: соціальна відповідальність бізнесу, захист персональних даних, висока цифрова грамотність персоналу.

Джерело: складено автором

У Додатку Ж представлено 3D-модель матриці Менделоу, де вісь X демонструє рівень зацікавленості стейкхолдера у досягненні підприємством стратегічних орієнтирів, вісь Y – вимірює рівень впливу стейкхолдера на досяжність стратегічних цілей підприємства, а вісь Z призначена для вимірювання ступеня впливу стейкхолдерів на цифрові ризики підприємства. Рівні впливу ризиків були визначені за шкалою від 0 до 1, де 0,8-1.0 – критичний вплив на досяжність стратегічних цілей підприємства, 0,6-0,8 – високий вплив, 0,4-0,6 – середній вплив і <0,4 → низький (незначний) вплив. Рівні впливу було визначено із використанням експертної думки представників менеджменту вітчизняних підприємств критичної інфраструктури.

На рис. 3.3 запропоновано оновлений механізм стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів.

Рисунок 3.3. – Оновлений механізм стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів

Джерело: складено автором

Зображена модель механізму націлена на те, аби перетворити систему економічної безпеки сучасного суб'єкта господарювання з «витратного процесу» у інструмент узгодження інтересів учасників бізнес-процесів і ефективного розподілу ресурсів для забезпечення пріоритетних потреб існування компанії на довгостроковому часовому горизонті. Останнє стає можливим завдяки зростанню довіри інвесторів та лояльності персоналу та клієнтів завдяки принципам прозорої комунікації та нульової довіри.

Конвергенція вітчизняного бізнесу з цінностями та принципами розвитку підприємств Європейського Союзу, прагнення гідної конкуренції з європейськими компаніями на внутрішньому та зовнішньому ринках, зумовлює необхідність перебудови механізму їх стратегічного управління у відповідності до людиноцентричної моделі менеджменту та використання соціальної відповідальності як активу для досягнення та підтримання стану економічної безпеки підприємств. Кейси медичних компаній, розглянуті у другому розділі, пов'язані з отриманням несанкціонованого доступу до медичних даних громадян, довели, що нехтування інтересами споживачів послуг не лише призводить до значних фінансових і репутаційних збитків, що унеможливлює досягнення стратегічних орієнтирів у майбутньому, а й становить загрозу для життя пацієнтів (у випадку медичних компаній – основних їх стейкхолдерів). Аналогічно, втрата персональних даних працівників підприємств або їх передання третім особам з корисливою метою, може трансформуватись у втрату людського капіталу та інтелектуального ресурсу для сталого розвитку.

Отже, в моделі Суспільства 5.0 та у реаліях світу BANI, економічна безпека суб'єкта господарювання припиняє бути виключно фінансово-економічною категорією. Її рівень у значній мірі визначається соціальною довірою до бізнесу, його роллю у розбудові громади регіону та збереженні інтелектуального капіталу нації. Механізм стратегічного управління має містити алгоритм дотримання етичних і соціальних параметрів захисту інтересів стейкхолдерів, що прямо пов'язані з підприємством, та суспільними інтересами.

3.3. Інтеграція принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку підприємств в Україні

У сучасних умовах поширення меж цифровізації на теренах національних економік країн світу, забезпечення інформаційної безпеки підприємств перестає бути суто технічною функцію організації кіберзахисту їх цифрових ресурсів від сторонніх втручань, і набуває рис справжнього повноцінного стратегічного напрямку забезпечення економічного захисту бізнесу та орієнтиру його розвитку. Складність управління інформаційною безпекою на рівні мідл і топ-менеджменту компанії пояснюється тим, що з одного боку така діяльність пов'язана з протидією ризикам безпосередньо у цифровому просторі ведення бізнесу, що вимагає високого рівня знань і навиків від управлінського та виконавчого персоналу, з іншого ж боку, інформаційна безпека – це складова іміджевої політики підприємства, засіб трансляції стейкхолдерам меседжу щодо відкритості та готовності підприємства до співпраці, засобом посилення його впливу у цифровому інформаційному просторі, демонстрація вміння працювати з інформацію та захищати дані (що у свою чергу є важливою конкурентною перевагою на діджитал-ринку), інструментом маркетингової політики, спрямованим на розширення споживацької аудиторії і підвищення лояльності клієнтів та додатковим аргументом для проактивної роботи з інвесторами задля отримання вигідних проєктів для співпраці. Таким чином, управління інформаційною безпекою в умовах цифровізації стає складним комплексним механізмом, пов'язаним із комунікаціями, пошуком і використанням інформації у різних форматах, технологічними прийомами аналізу та контролю доступу до даних, здатністю приймати рішення щодо повної або часткової інформаційної відкритості ведення бізнесу, тощо.

Вітчизняними вченими питання управління інформаційною безпекою з позиції стратегічного менеджменту розглядалось у різних контекстах. Наприклад, Галахов Є. М., Барабаш О. В. досліджують стратегічні пріоритети системи інформаційної безпеки підприємства, що залучає фріланс-ресурс [278],

Нехай В. у фокусі уваги тримає інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою сільськогосподарських підприємств на основі стратегії Cyber Situation Awareness [279], Храпкін О. уточнює та узагальнює сучасні підходи та виклики стратегічного управління інформаційною безпекою підприємства [280], а Чубаєвський В. І. визначає стратегічні орієнтири формування корпоративної політики інформаційної безпеки [281]. Таким чином, у межах науки управління проблематика управління інформаційною безпекою визнається одним із актуальних і сучасних напрямів досліджень. Однак, якщо підприємство прагне інтегруватись у цифровий економічний простір, вирішувати поставлене управлінська завдання доводиться одразу у двох площинах – традиційній та цифровій, кожна з яких має власні джерела виникнення ризиків для повноти, якості та захищеності інформаційних ресурсів суб'єктів господарської діяльності.

Галахов Є. М., Барабаш О. В. виділяють три ключові блоки бізнес-процесів підприємства, що пов'язані з його інформаційною безпекою як на стратегічному, так і на тактичному та оперативному рівнях менеджменту: бізнес-процеси, які опосередковуються он-лайн каналами комунікації між учасниками економічних відносин; бізнес-процеси підприємства, які включають оф-лайн канали комунікації, бізнес-процеси підприємства, що стосуються внутрішньої діяльності [278, с.30-31]. Для існування кожного з цих блоків притаманними є цифрові ризики – спотворення цифрових даних, несанкціонований віддалений доступ до них, викрадення, використання з корисливою метою, оприлюднення на цифрових платформах і у каналах без належного дозволу, обробки, поширення неправдивої інформації про підприємство, його клієнтів, персонал, партнерів, затримки повідомлень, що мають короткочасну інформаційну цінність і є суттєвими для прийняття своєчасних управлінських рішень, тощо.

Інформація стає найважливішим стратегічним ресурсом будь-якого підприємства, її формування та споживання, стає важливою основою ефективного функціонування і розвитку різних сфер суспільної та економічної

діяльності [279, с.240]. Стратегічним орієнтири управління інформаційною безпекою підприємства під впливом цифрових ризиків має стати досягнення максимально можливого рівня якості інформації, що оцінюється її повнотою, релевантністю, зрозумілістю.

Таким чином, комплексна система інформаційної безпеки підприємства має включати в себе як тактичні аспекти інформаційного захисту (експрес-аудит інформаційних загроз підприємства), так і стратегічні пріоритети, що відображає інформаційна політика та інформаційна стратегія підприємства [278, с.35]. Тобто, інформаційна безпека трансформується від комплексу завдань, виконанням яких фахівці з ІТ у компаніях мали забезпечити захист її ресурсів від кібервтручань, до стратегічного пріоритету топ-менеджменту, причому чим більш технологічною є компанія, тим вищого порядку стає цей пріоритет.

Крім якості інформації, якою послуговується управлінський персонал для визначення стратегічного курсу розвитку підприємства та яку застосовує у якості інформаційного ресурсу для виконання поточних завдань, стратегічними орієнтирами управління інформаційною безпекою компанії має стати побудова такої системи протидії цифровим і аналоговим ризикам, яка гарантуватиме конфіденційність даних, їх цілісність та доступність [280, с.88]. Останній параметр повинен передбачати запровадження практики контролю доступу до інформації, комплексної перевірки суб'єктів, які її використовують та сигналізування про факти спроб стороннього втручання у інформаційні ресурси, особливо такі, що містять відомості категорії обмеженого доступу, наприклад, особисті дані працівників або клієнтів підприємства.

Для того, аби формалізувати правила забезпечення інформаційної безпеки, вивести їх із категорії побажань у площину стратегічних орієнтирів функціонування бізнесу, менеджментом компанії може бути затверджено документ - політику інформаційної безпеки підприємства, який стане важливим елементом корпоративного управління і ґрунтуватиметься на стратегічних вимогах, які існують щодо управління ризиками в організації. Як вважає

Чубаєвський В. І., стратегічні зміни, зумовлені впровадженням інформаційних технологій та формуванням єдиного цифрового корпоративного бізнес-простору, спричинили стійку потребу у трансформації підходів до розроблення методичних засад використання підприємствами корпоративних політик інформаційної безпеки, які б ураховували динаміку стратегічних змін напрямів їх діяльності [281, с.28]. Отже, управління інформаційною безпекою суб'єкта господарювання має бути частиною його генеральної стратегії, спрямованої на протидію інформаційним і цифровим ризикам і їх негативному впливу на цілісність і результативність використання корпоративних ресурсів.

Сучасні тенденції реалізації фінансово-господарських процесів змінюють механізми організації системи інформаційної безпеки та підходи до управління нею. Зокрема, популярності набуває принцип нульової довіри (Zero Trust), суть якого криється у припущенні, що жоден користувач корпоративної інформаційної мережі або пристрій, який перебуває у цифровій екосистемі підприємства, не може вважатися безпечним та таким, що не потребує додаткової перевірки під час доступу до даних. Тому стратегія управління інформаційною безпекою має бути спрямована на те, щоб кожна спроба доступу до інформації була верифікована та підтверджена. Іншим важливим стратегічним аспектом у площині інформаційної безпеки є здатність до швидкого відновлення інформації після її втрати та побудова систем альтернативного доступу до інформації у випадку, коли основний канал доступу до відомостей обмежений через блекаути, відсутність інтернету, руйнування мереж внаслідок ворожих атак.

Для протидії цифровим ризикам у системі забезпечення економічної безпеки підприємств менеджменту варто запровадити на усіх рівнях «принцип нульової довіри» – модель цифрової та економічної безпеки, яка передбачає сувору перевірку пристроїв і користувачів, надання мінімально необхідних прав і моніторинг поведінки при доступі до даних або послуг, що реалізується як політика в рамках цифрової інфраструктури [205, с.13].

Осадча О. О., Роздопченюк В. М. наголошують на тому, що цифровізація передбачає радикальну зміну логіки бізнес-процесів та перехід на ризик-орієнтований підхід в управлінні, в основі якого – цифрові технології [177, с.116]. Категорію ризику використовують для дефініції економічної безпеки на мікрорівні Іванова Н. В., Кононенко С. О. наполягаючи, що економічна безпека – це такий стан суб'єкта будь-якого рівня господарювання, за якого він здатний нівелювати внутрішні та зовнішні загрози і ризики свого існування у короткостроковому та довгостроковому періодах на основі принципів і методів стійкого цілеспрямованого функціонування та сталого розвитку [179, с.170]. Вважаємо, що економічна безпека підприємства під впливом цифровізації – це стан захищеності його матеріальних і нематеріальних ресурсів, які перебувають у фізичній і нефізичній формах, та використовуються у екосистемі бізнесу, у тому числі, у цифровій її частині, від негативного впливу загроз і ризиків, що мають різні джерела походження, одним із яких є цифровий простір реалізації фінансово-господарських відносин і бізнес-процесів, і можуть спричинити втрати або неефективне використання корпоративних ресурсів, що призведуть до збитків чи недоотримання прибутків [173, с.12].

Як відзначають Климчук М. М., Ачкасов І. А., Климчук С. А., Поляк О. П., для більшості вітчизняних підприємств характерною є реактивна форма розробки стратегії, коли процес прийняття управлінських рішень є реакцію на поточні проблеми виробничо-економічної системи, а визначення стратегічних пріоритетів є фрагментарним [69, с.273]. Гедз М. Й., Вишневська В. А., Науменко С. Д. пропонують розробку стратегії підприємства проводити за двома основними етапами: перший етап охоплює стратегічний аналіз, який передбачає вивчення зовнішнього та внутрішнього середовища підприємства; визначення сильних і слабких сторін, можливостей та загроз; формулювання місії та бачення підприємства; другий етап передбачає стратегічний вибір, направлений на розробку альтернативних стратегій; оцінку та вибір найкращої стратегії [70, с.131]. У межах цього дослідження пропонується перехід до проактивної форми стратеготворення, яка передбачає: ідентифікацію та

оцінювання ризиків (традиційних і цифрових), характерних для поточної діяльності підприємства та таких, що ймовірно, будуть притаманними для неї у майбутньому; проведення стратегічних сесій з фахівцями різних відділів в підрозділів щодо їх бачення подальшого розвитку бізнесу або існуючих резервів стабілізації і посилення стану його економічної безпеки, широке використання засобів фасилітації з метою заохочення креативних підходів до вирішення стратегічних проблем функціонування вітчизняного бізнесу, формалізації стратегічних альтернатив, а також обговорення проєктів стратегій за різними сценаріями та врешті колегіальне погодження фінального варіанту стратегії.

Не виникає сумнівів, що сучасна стратегія управління підприємствами повинна регламентувати напрями, ступінь та базові умови ідентифікації ризиків та передбачати процедури їх оцінювання із метою подальшої оцінки, інтерпретації та їх усунення. Аналіз кейсів і досвіду функціонування українських компаній демонструє, шо на стан економічної безпеки підприємства мають впливу такі цифрові ризики: ризик втрати цифрової інформації та доступу до даних, ризики кібератак і втручань у роботу цифрових екосистем бізнесу, ризик цифрового блеатуту, залежність від провайдерів, повільний або відсутній Інтернет, що паралізує роботу у цифровому просторі, відсутність вітчизняного програмного забезпечення, глибока інтеграція російського ПЗ у цифрові екосистеми українських компаній, низький рівень цифрових компетенцій персоналу та мотивації до його підвищення та опанування основ цифрової грамотності, зростання потреби у фахівцях з цифрової безпеки бізнесу. Вплив окреслених ризиків може бути настільки суттєвим для досягнення суб’єктом господарювання довгострокових цілей розвитку, що має враховуватись під час розробки або адаптації їх стратегії до реалій ведення бізнесу, що у Україні характеризуються тотальною невизначеністю та кризою у більшості сегментів соціально-економічної системи [173, с.12-13].

Проблемою на шляху до якісного управління цифровими ризиками для потреби забезпечення економічної безпеки сучасних підприємств залишається рівень цифрової грамотності населення і водночас рівень цифрових навиків їх персоналу. Експерти стверджують про відсутність у випускників технічних спеціальностей практичних цифрових навичок з кібербезпеки, що призводить до браку практичного досвіду та спеціальних знань, необхідних у сфері кібербезпеки. Через недостатню підготовку багато студентів, які планували пов'язати своє життя з кібербезпекою, у підсумку працюють на загальних IT-посадах, таких як фронт-енд або бек-енд розробка. Приватні компанії намагаються подолати кадровий голод: пропонують широкий спектр практичних програм та спеціалізованих курсів, практичну підготовку з кібербезпеки, з урахуванням вимог професійних стандартів та вимог індустрії [205, с.31].

Рівень цифрової грамотності працівників підприємств вважаємо одним із актуальних цифрових ризиків для стану їх економічної безпеки, оскільки він може бути як джерелом можливостей для отримання стратегічних конкурентних переваг (у випадку високого рівня), так і причиною недосяжності стратегічних орієнтирів в умовах поширення явища цифровізації у економічному просторі (у випадку низького рівня). На основі вивчення еволюції поняття цифрової грамотності у зарубіжній науковій думці, Дімітров О.Ю. пропонує розуміти це поняття як багатовимірний феномен, що охоплює не лише технічні навички, а й критичне мислення, етичну та безпечну поведінку в цифровому середовищі, здатність до творчого використання цифрових ресурсів [282, с.421]. Пропозиції щодо оцінювання рівня цифрової грамотності населення та засобів покращення її стану у перспективі можна знайти у джерелах [283-286]. Водночас, специфіка функціонування підприємств різних видів економічної діяльності, рівень автоматизації і цифровізації їх бізнес-процесів, стан ринкових сегментів і інтереси стейкхолдерів і клієнтів, які потрібно задовольняти, потребують специфічних підходів і методів до

оцінювання цифрової грамотності та вміння дотримуватись цифрової гігієни у колективі їх працівників.

Цифрова грамотність персоналу та менеджерів підприємств формує підґрунтя для запровадження цифрового ризик-менеджменту як елементу функціонування системи економічної безпеки та одного із процесів управління нею. Це поняття не разі не знайшло широкого представлення у вітчизняній науковій літературі, однак, найбільш синонімічними категоріями, які передають сутність цього процесу на методологічному та прикладному рівнях, є ризик-менеджмент цифрової трансформації [287], ризик-менеджмент в умовах цифровізації [288], менеджмент цифрових ризиків [289], менеджмент кібер-ризиків [290]. У контексті цього дослідження вагомими та вартими уваги видаються висновки таких дослідників, як Зварич Р., Дудник Ю., Гомотюк В., Боднар С., щодо того, що мінімізація можливих ризиків для стану економічної безпеки підприємств у постпандемічний період потребує уваги до перспективних технологічних напрямів, які активно розвиваються за кордоном, та інтеграцій у систему безпеко орієнтованого менеджменту вітчизняних компаній (де це можливо та доцільно) – геоінформаційних і навігаційних технологій, технологій фотоніки, хмарних обчислень, кібербіологічних систем, системи аутентифікації та ідентифікації, суперкомп’ютерних і грід-технологій. У результаті цього основними заходами ризик-менеджменту цифрової трансформації бізнес-процесів мають стати: застосування планів реагування, моніторинг заходів з пом’якшення ризиків, перевірка готовності інфраструктури до навантаження, резервне планування роботи працівників, створення механізму дистанційної комунікації [287, с.50].

У табл. 3.5 узагальнено принципи, яким стратегічним менеджерам підприємств варто слідувати під час інтеграції цифрового ризик-менеджменту у систему забезпечення економічної безпеки. Їх дотримання стимулюватиме гнучкість безпеко орієнтованого управління у цифрових екосистемах і позитивно вплине на задоволення інтересів стейкхолдерів, що відповідає висновкам і пропозиціям попереднього розділу дослідження.

Таблиця 3.5. – Зв’язки принципів цифрового ризик-менеджменту зі стратегічними цілями системи економічної безпеки підприємств

Принцип цифрового ризик-менеджменту	Зв'язок зі стратегічними цілями системи економічної безпеки	Роль цифрової грамотності працівників у цьому процесі	Сприятяння задоволенню інтересів стейкхолдерів
Превентивність заходів з безпеки і управління ризиком	Запобігання фінансовим і репутаційним збиткам і втратам до їх виникнення; підтримання безперебійності бізнес-процесів; попередження кібератак	Працівники повинні мати навики ідентифікації «попередніх сигналів» загроз (фішинг, аномалії в програмному забезпеченні).	Інтереси власників і інвесторів - захист капіталу. Інтереси клієнтів - гарантія отримання послуг.
Орієнтованість на баланс інтересів стейкхолдерів	Забезпечення стійкості та резильєнтності завдяки балансуванню інтересів стейкхолдерів; мінімізація репутаційних ризиків через постійну комунікацію у захищених цифрових каналах.	Усвідомлення персоналом відповідальності перед клієнтами за збереження конфіденційності їх особистих даних і історії користування послугами.	Інтереси партнерів - прозорість ризиків контрагентських відносин. Інтереси громади - етичне поводження з персональними даними.
Адаптивність управлінських систем	Здатність системи економічної безпеки оперативно трансформуватись і адаптуватись під впливом тенденцій середовища BANI і цифрових трансформацій бізнесу.	Безперервне навчання і самоосвіта (Life-long learning) для опанування нових інструментів цифрового захисту та підвищення рівня цифрової гігієни.	Інтереси управлінського персоналу: швидке прийняття обгрунтованих рішень. Інтереси регуляторів: дотримання вимог і стандартів.
Резильєнтність ризикам і загрозам цифрового простору	Орієнтація ресурсів системи на «управління економічною спроможністю» – здатність швидко відновлюватися після цифрових інцидентів.	Знання алгоритмів дій у критичних ситуаціях і протоколів антикризового менеджменту.	Інтереси клієнтів - мінімальний час надання послуг. Інтереси персоналу - стабільність робочих місць.
Управління на основі актуальних даних	Аргументація і прийняття стратегічних рішень на основі аналітики ветиких масивів даних (методи Монте-Карло, аналіз Big Data).	Наявність навичкок роботи з аналітичними панелями, великими масивами даних і їх інтерпретації для оцінки ризиків.	Інтереси кредиторів: впевненість у реалістичності прогнозів економічного потенціалу.
Нульова довіра	Мінімізація внутрішніх кадрових ризиків; посилення рівня інтелектуально-кадрової безпеки підприємства; людиноцентризм в HRM	Чітке дотримання протоколів доступу; відмова від використання неперевірених цифрових ресурсів.	Інтереси держави - дотримання вимог кіберзахисту і запобігання витоку даних про громадян і їх інтереси.

Джерело: складено автором

У табл. 3.6 запропоновано встановити стратегічні цілі щодо інтеграції цифрового менеджменту у процеси управління економічною безпекою сучасних українських підприємств, що були розроблені із використанням технології SMART (згідно неї, ціль має задовольняти таким параметрам: бути конкретною, вимірюваною, досяжною, релевантною і мати визначені часові межі її досягнення). Такий підхід дозволяє вибудувати систему досяжних і чітко конкретизованих у часовому просторі етапів запровадження елементів управління цифровими ризиками у межах реалізації безпеко орівєнтованих стратегій функціонування та розвитку вітчизняного бізнесу.

Таблиця 3.6. – Стратегічні цілі щодо інтеграції цифрового менеджменту у процеси управління економічною безпекою українських підприємств

Стратегічна ціль підприємства	**SMART-характеристики цілі**	**KPI**	**OKR**	**Необхідний рівень цифрової грамотності (ЦГ) персоналу**
1	**2**	**3**	**4**	**5**
1. Ідентифікація та оцінювання цифрових ризиків	Запровадити до кінця 2026 року систему автоматизованого скринінгу 100% цифрових активів на предмет вразливостей та наявності цифрових ризиків у внутішньому та зовнішньому середовищі.	Кількість виявлених ризиків; ресурс часу, потрібний для ідентифікації критичної загрози для стану цифрової безпеки підприємства.	О: створити карту цифрових ризиків. KR: оцифрувати 100% бізнес-процесів за ризик-профілем і проводити їх постійний моніторинг.	Високий рівень ЦГ, що характеризується вмінням працювати з програмним забезпеченням для ризик-менеджменту та розумінням архітектури даних і її вразливостей.
2. Планування показників цифрової трансформації бізнес-процесів	Розробити до вересня 2026 року план-графік автоматизації та оцифрування 40% рутинних операцій з попередньо визначеним лімітом бюджету фінансових, кадрових і матеріальних ресурсів.	Частка оцифрованих бізнес-процесів, прогнозне зниження операційних витрат (%) після цифрових трансформації бізнесу.	О: мінімізувати вплив людського фактору на стан безпеки. KR: сформувати перелік із 10 пріоритетних KPI для цифрового стратегічного розвитку.	Середній рівень ЦГ, що характеризується навичками стратегічного планування в цифровому середовищі та знанням основ хмарних технологій.

Продовження табл. 3.6

1	2	3	4	5
3. Розробка та реалізація стратегії цифровізації підприємства	Розробити та затвердити дорожню карту цифровізації діяльності підприємства на 3 роки, що на 15% підвищить стійкість системи економічної безпеки до BANI-чинників.	Рівень виконання дорожньої карти цифровізації (%); обсяг інвестицій у цифрову безпеку підприємства у % від розміру отриманого доходу.	О: стати лідером галузі за рівнем захищеності цифрової інформації. KR: запустити три стратегічні цифрові модулі (ERP, CRM, Cybersecurity Center).	Високий рівень ЦГ, що характеризується глибоке розумінням принципів стратегічного менеджменту, кібербезпеки та знанням стандартів ISO/IEC 27001.
4. Моніторинг і контроль показників цифрового розвитку бізнесу	Створити онлайн-дошку зі спільним доступом персоналу, що відображатиме у режимі реального часу відхилення фактичних показників від планових з похибкою <5%.	Кількість спрацювань системи раннього попередження ризиків; коефіцієнт точності прогнозів цифрових загроз.	О: забезпечити 100%-ву керованість цифровим розвитком підприємства. KR: скоротити час реакції на відхилення показників у цифровій екосистемі на 50%.	Середній рівень ЦГ, що характеризується вільним володінням цифровими інструментами візуалізації даних (Power BI, Tableau) та Excel на фаховому рівні.
5. Аналіз стану цифрової безпеки підприємства	Здійснювати щоквартальний цифровий аудит (пентести та фінансовий аудит цифрових даних) і цифровий моніторинг для оцінки економічних збитків від потенційних цифрових загроз і ризиків.	Індекс фінансової стійкості бізнесу до кібератак і цифрових втручань; кількість успішних відбиттів цифрових атак за конкретний період.	О: досягти рівня «нульової вразливості» для критичних вузлів цифрових бізнес-процесів. KR: успішно пройти зовнішній IT-аудит без критичних зауважень до стану цифрової безпеки.	Базовий рівень ЦГ, що характеризується розумінням принципів цифрової гігієни (фішинг, паролі) для всіх працівників; і високий рівень ЦГ - для аналітиків і аудиторів цифрових даних.

Джерело: складено автором

Залежність успіху щодо інтеграції цифрового ризик-менеджменту у систему стратегічного управління економічною безпекою підприємств від рівня цифрової грамотності персоналу породжує необхідність розробки рекомендацій

щодо навчання працівників підприємств у напрямі покращення стану їх цифрових компетенцій [291-300]. Однак, без належної мотивації цей процес може зустріти опір, сформувати середовище для виникнення конфліктів і створити напругу у колективі. Тому нами запропоновано кілька варіантів win-win стратегій задля заохочення працівників до підвищення рівня власної цифрової грамотності, осучаснення цифрових навиків і використання принципів безпеко орієнтованої поведінки під час виконання професійних завдань із використанням цифрових інструментів та у цифровому економічному просторі (табл.3.7).

Запропоновані стратегії можуть бути використані у якості додаткових аргументів для обґрунтувати мотиваційної частини запропонованого у попередньому розділі дослідження оновленого механізму стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів. Наприклад, замість традиційних «наказів, розпоряджень і штрафів», які були ідентифіковані як слабка сторона суб'єктів господарювання за результатми SWOT-аналізу), у розроблених Win-Win стратегіях пропонується:

– інтеграція інтересів стейкхолдерів для досягнення спільної довгострокової мети: наприклад, працівник зацікавлений у власній конкурентоспроможності на ринку праці для збереження посади та отримання підвищення заробітної плати, а підприємство – у розвитку його професійних навичок щодо захисту корпоративних ресурсів і підвищенні рівня цифрової грамотності;

– психологічна трансформація моделі поведінки персоналу (у першу чергу управлінського): безпеко-орієнтована поведінка працівників має стати частиною «професійного кодексу честі», етики ділового менеджменту та ознакою корпоративної культури, а не примусом;

– забезпечення економічних ефектів: запобігання одному серйозному кіберінциденту через пильність працівника зазвичай окупає усі витрати на його навчання цифровим компетенціям і на мотивацію його за успіхи.

Таблиця 3.7. – Win-Win стратегії заохочення до цифрового професійного розвитку та безпеко орієнтованої поведінки працівників

Стратегія	Дії підприємства, що забезпечують вигоди для бізнесу	Мотивація працівника (ідивідуальні вигоди)	Вплив стратегії на економічну безпеку підприємства
Цифровий капітал і потенціал працівника	Оплата курсів на едукативних цифрових платформах (наприклад, з кібербезпеки чи аналітики даних) і надання часу на навчання в межах робочого дня.	Отримання сертифіката, що підвищує ринкову вартість фахівця, посилює його CV та покращує його «цифрову вагу».	Зменшення ризику «людської помилки» при роботі з цифровими системами і кадрових ризиків в управлінні в цілому, формування інтелектуально-кадрового резерву підприємства.
Гейміфікація цифрової безпеки	Запровадження внутрішнього рейтингу працівників з метою мотивування за відсутність порушень і успішне проходження імітованих цифрових атак на активи.	Бонуси, похвала, додаткові дні відпустки або статус Флагмана цифрового розвитку з привілеями (нові гаджети, онлайн-робота).	Формування культури безпеко-орієнтованої поведінки персоналу на підсвідомому рівні як елементу корпоративної культури підприємства.
Технологічний апгрейд бізнес-процесів	Заміна застарілого обладнання та програмного забезпечення на сучасні захищені цифрові інструменти і гаджети (архітектура нульової довіри).	Робота з престижними, швидкими та зручними інтерфейсами, що зменшує рівень стресу працівників і рутини при виконанні щоденних завдань.	Техніко-технологічна стійкість цифрових екосистем, мінімізація вразливостей бізнес-процесів до проявів цифрових ризиків.
Гнучкість управління через довіру і людиноцентризм	Дозвіл на дистанційну чи гібридну роботу за умови використання захищених корпоративних VPN, протоколів і робочих гаджетів зі встановленими захисними системами.	Можливість досягнення і підтримання балансу між роботою та особистим життям (work-life balance); економія часу на трансфер до робочого місця.	Забезпечення безперебійності бізнес-процесів навіть у критичних умовах воєнного часу та поширення тенденцій світу BANI.
Цифрова ергономіка та безпека праці	Запровадження інструментів автоматизації звітності, що мінімізують ризикм допущення помилок у фінансових розрахунках.	Усунення страху пересоналу отримати штрафи чи покарання за випадкові помилки в документах чи порушення дедлайнів.	Підвищення якості фінансової інформації у цифровому форматі в інтересах усіх категорій стейкхолдерів.

Джерело: складено автором

У якості інструменту аналітики для визначення почерговості інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств запропоновано використовувати інтегральний індекс впливу стейкхолдерів на стратегічні орієнтири бізнесу. У той час, як класична матриця Менделоу може надати якісну оцінку впливовості та зацікавленості інвесторів, запропонований індекс поєднує можливості кількісної оцінки з цифровим виміром функціонування та розвитку бізнесу. Інтегральний індекс впливу стейкхолдерів дозволяє кількісно оцінити їх роль у формуванні стратегічних орієнтирів підприємства з урахуванням цифрових ризиків, що забезпечує підвищення обґрунтованості використання принципів цифрового ризик-менеджменту у стратегіях безпеко орієнтованого економічного розвитку вітчизняних підприємств.

Індекс враховує три такі параметри:

– ImL – рівень впливовості стейкхолдера;

– IL – рівень інтересу у результатах діяльності підприємства;

– DRI – вплив інтересу стейкхолдера на цифрові ризики підприємства.

$$I_{int}=w_1 \cdot ImL + w_2 \cdot IL + w_3 \cdot DRI \qquad (3.1)$$

де I_{int} – інтегральний індекс впливу стейкхолдера;

w_1, w_2, w_3 – вагові коефіцієнти впливу, які у сумі становлять 1.

Рекомендовані вагові значення обраних коефіцієнтів із використанням думок експертів – працівників реально діючих підприємств Черкащини, зважаючи на стан цифровізації їх бізнес-процесів було встановлено на рівнях: w_1 = 0,4, w_2, = 0,3, w_3 = 0,3, оскільки вплив стейкхолдерів є домінуючим фактором, у той час як їх інтереси і цифрові ризики є рівнозначними для результуючого показника.

Розрахунки значень індексів для трьох підприємств Черкащини – ПП «Мак Тревел», ТОВ «Техвантаж-Сервіс», ТОВ «Авіа-Сервіс»представлено у Додатку З. Інтерпретувати отримані дані дозволяє табл. 3.8.

Таблиця 3.8. - Інтерпретація значень індексу для інформаційних потреб менеджменту підприємств

Значення індексу	Рівень впливу на інтеграцію принципів цифрового ризик-менеджменту в бізнес-процеси	Управлінське рішення щодо інтеграції цифрового ризик-менеджменту
0,76-1,0	Максимальний	Пряма інтеграція у стратегічне управління економічною безпекою
0,51-0,75	Високий	Активне управління цифровими ризиками та екосистемою
0,31-0,50	Середній	Моніторинг і аналіз даних
<0,3	Мінімальний	Мінімальний контроль цифрових ризиків

Джерело: складено автором за допомогою експертного методу

Рис. 3.4 узагальнює авторське бачення процесу інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств.

Рисунок 3.4. - Інтеграція принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств

Джерело: складено автором

Інтерпретація значень інтегрального індексу впливу стейкхолдерів для інформаційних потреб менеджменту підприємств демонструє, що максимальний рівень цього показника мають власники та інвестори суб'єктів господарювання, їх управлінський персонал і виконавчий персонал, а також представники державних органів влади. Банки та фінансові донори, клієнти і споживачі зазвичай мають високий рівень впливу (інколи середній) на інтеграцію принципів цифрового ризик-менеджменту в бізнес-процеси, постачальники і контрагенти – середній (інколи високий), а громада (локальне ком'юніті) – низький (інколи середній).

Інтеграція принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств дозволить досягнути їм мети цифрового економічного розвитку з мінімальними ризиками втрати ресурсів і активів, що полягає у сукупності таких перспективних характеристик їх діяльності, як безпечна цифровізація бізнес-процесів, наявність довгострокової цифрової безпекової стратегії, стійкість досягнутих конкурентних переваг на цифровому ринку, мінімальні фінансові, інформаційні та репутаційні втрати від цифрових загроз і ризиків, оптимізація впливу ризиків при використанні інноваційних можливостей у цифровому просторі, досягнення високого рівня цифрової грамотності персоналу підприємств.

Висновки до розділу 3

1. У результаті змістового та процесного оновлення парадигмальних засад адаптивного управління підприємствами шляхом комбінації сутнісних ознак адаптивного менеджменту, стратегічного та безпеко орієнтованого векторів управління, запропоновано авторські дефініції таких категорій, як «адаптація стратегії», що розуміється як динамічний та гнучкий процес ініціювання та виконання послідовних управлінських дій, спрямованих на коригування довгострокових цілей підприємства, а також шляхів, інструментів і засобів їх

досягнення, що розпочинається як реакція на зміни у внутрішньому та зовнішньому середовищі, які є суттєвими для досяжності планових показників його діяльності; «стратегія адаптації», що сприймається як розроблений послідовний план дій (а не процес їх виконання, що є сутнісною відмінністю між досліджуваними дефініціями), націлений на підвищення рівня резильєтності підприємства через використання гнучкого управління його реакціями на виникнення непередбачуваних ризиків і загроз у економічному просторі (у тому числі у його цифровому вимірі) та «адаптована стратегія» – яку охарактеризовано як бажаний і очікуваний з позиції стратегічного менеджменту результат докладання управлінських зусиль і витрат ресурсів у процесі адаптації стратегії до ризиків і викликів діяльності суб'єкта господарювання, що мають тривалу дію або є характерними для неї впродовж тривалого проміжку часу.

2. Сформовано матрицю найбільш поширених інтересів традиційних груп стейкхолдерів сучасних українських підприємств. У ній узагальнено стратегічні інтереси пов'язаних сторін, конкретизовано вектори їх зацікавленості у площині управлінні цифровими ризиками і економічною безпекою. Особливістю цієї матриці як інструменту інформаційного забезпечення адаптивного менеджменту у системі стратегічного управління суб'єктів господарювання є ідентифіковані ризики для конкурентних перспектив підприємства у випадках, якщо інтереси різних груп стейкхолдерів не будуть досягнуті. Саме останній аспект став аргументом на користь потреби балансування таких інтересів як інструменту досягнення базового рівня довгострокової економічної безпеки підприємств в умовах невизначеності, реалій воєнного часу та світу BANI.

3. За результатами SWOT і STEEPLE-аналізів традиційних механізмів стратегічного управління економічною безпекою підприємств сформовано чотири сценарії адаптації безпеко орієнтованого менеджменту до соціальних, технологічних, економічних, екологічних, політичних, юридичних і етичних чинників функціонування бізнесу, такі як: адаптація сильних сторін до

можливостей (SO-адаптована стратегія), адаптація сильних сторін до загроз (ST-адаптована стратегія), адаптація слабких сторін до можливостей (WO-адаптована стратегія), адаптація слабких сторін до загроз (WT-адаптована стратегія). Оцінювання впливу стейкхолдерів на стратегічні орієнтири підприємства згідно матриці Менделоу дало змогу змоделювати оновлений механізм стратегічного управління економічною безпекою підприємства, що відрізняється від існуючих елементом пошуку можливостей і діагностики стану дотримання балансу інтересів його стейкхолдерів. Особливістю цього механізму є комплексне застосування можливостей гнучкого менеджменту на усіх етапах його функціонування, що дозволяє адаптувати стратегію до мінливих умов навколишнього середовища, які виявляються у реаліях світу BANI та посилюються цифровими трансформаціями екосистем.

4. Авторський підхід до інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств полягає у реалізації чотирьох етапів управлінських дій: аналізі зовнішнього середовища із фокусом на можливості цифровізації, ризики війни, тенденції BANI-світу, кадровий голод, прояви пермакриз та загальноекономічної невизначеності; формуванні та використанні організаційно-управлінського механізму, що інтегрує принципи превентивності, адаптивності, прийняття рішень на основі актуальних даних, балансування інтересів стейкхолдерів, нульової довіри та резильєнтності у безпеко орієнтовану стратегію, що реалізується на наступному етапі та сприяє цифровому економічному розвитку бізнесу (четвертий фінальний етап). Ідеологічними стовпами стратегії підприємства при цьому є: управління ризиками, проєктне управління, управління на основі актуальних даних, стейкхолдер-менеджмент, забезпечення цифрової безпеки та антикризовий менеджмент.

Отримані у межах розділу наукові результати опубліковані у працях здобувача [173], [201], [259].

ВИСНОВКИ

У дисертаційній роботі вирішено важливе наукове завдання, яке полягало в доповненні, розширенні та оновленні науково-методичних засад і практичних підходів до адаптивної модифікації системи стратегічного управління підприємством у напрямі спрямування її ресурсів і потенціалу на забезпечення його економічної безпеки в умовах інтенсифікації цифрових ризиків зовнішнього та внутрішнього середовищ.

За матеріалами дослідження отримані такі висновки.

1. Проведено логічний аналіз теоретичних основ стратегічного управління у теорії менеджменту діяльності підприємств. В умовах пермакризи та мінливості тенденцій економічного середовища, підходи до стратегічного управління підприємствами еволюціонують від жорсткої фіксації довгострокових планів до моделі адаптивного фільтра стратегічних ризиків і загроз. Одним зі стратегічних управлінських завдань стає перманентне сканування зовнішнього середовища для своєчасного коригування стратегії функціонування та розвитку підприємницької діяльності у відповідь на ідентифіковані ризики. У роботі переконливо доведена необхідність переходу від класичного розуміння заздалегідь визначених стратегічних цілей підприємства до стратегічних орієнтирів його фінансово-господарської діяльності. Це дозволяє змістити фокус із конкретних кількісних показників перспективного планування, що є важко прогнозованими у воєнний час, на варіативність і динамічні спроможності підприємства до сталого розвитку. У теоретико-методичній площині запропоновано використовувати логічні операції (кон’юнкцію, диз’юнкцію, імплікацію) для формалізації зв’язків між діями менеджменту та рівнем досягнутої підприємством економічної безпеки. Обґрунтовано раціональність скорочення стратегічного горизонту перспективних планів підприємств з традиційних 10-25 років до 3-5 років. Це обумовлено реаліями світу BANI, де довгострокове прогнозування стає недостовірним, а успіх визначається швидкістю адаптації до змін. Висловлено

припущення, що у таких умовах прибуток не може бути кінцевою метою стратегії, а успіх бізнесу прямо залежить від балансування інтересів широкого кола стейкхолдерів та соціальної значущості діяльності підприємства. Таким чином, сучасна концепція стратегічного управління полягає у переході до ризик-орієнтованого перспективного менеджменту, де логічний аналіз виступає інструментом подолання обмеженої раціональності менеджерів і засобом інтеграції інтуїції й досвіду в науково обґрунтовані алгоритми прийняття стратегічних управлінських рішень.

2. Простежено зміни парадигм стратегічного управління підприємствами під впливом пермакризи та ризиків світу BANI. Виокремлено кілька періодів еволюції парадигм стратегічного управління підприємствами під впливом ризиків середовища їх функціонування, такі як класичний період, період стратегій конкурентних переваг, ресурсний період, неокласичний період, цифровий період, період гнучкого та сценарного управління, кризовий період, воєнний період, адаптивний період. Встановлено потребу у перегляді та оновленні парадигмальних засад стратегічного управління підприємством у світі BANI та запропоновано конкретні напрямки їх змін, такі як запровадження принципів гнучкого та сценарного управління, застосування адаптивного менеджменту та антикризових стратегій, запровадження практик критичного мислення та сценарного аналізу, використання цифрових технологій, інформації з різних джерел та штучного інтелекту як корпоративних ресурсів; перехід до децентралізації влади та гнучких управлінських структур; розвиток цифрового управління бізнес-процесами; розвиток екосистем і стратегічних альянсів; масштабування практик людиноцентричного управління підприємствами та використання прогностичної аналітики та технік форсайту для прийняття та реалізації управлінських рішень. Ці трансформації стануть гідними відповідями на такі виклики, як нераціональність і втрата актуальності довгостроковими стратегіями, неможливість отримати релевантні дані та достовірно спрогнозувати майбутнє підприємства; потреба у врахуванні у стратегіях явищ турбулентності і невизначеності економічного простору,

ігнорування менеджментом випадкових можливостей розвитку бізнесу, нехтування людським потенціалом і капіталом.

3. Охарактеризовано сучасний стан розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації. Сучасний етап розвитку наукових теорій стратегічного управління економічною безпекою підприємства у контексті цифровізації ознаменувався переосмисленням стратегічного управління економічною безпекою в умовах крихкості, тривожності, нелінійності та незрозумілості, тобто у реаліях світу BANI, що призвело до формування принципів стратегічного менеджменту в умовах пермакризи, адаптації підходів стратегічного управління до реалій воєнного часу, у результаті чого відбулося концептуальне поєднання теорій антикризового, стратегічного, ризик-менеджменту з принципами гнучкого управління та адаптивності. Виявлено, що сучасні контексти дослідження стратегічного управління економічною безпекою зводяться до визначення актуальних безпеко орієнтованих стратегій діяльності підприємств, оновлення методів стратегічного управління економічною безпекою, конкретизації кадрових аспектів стратегічного управління економічною безпекою, встановлення особливостей стратегічного управління в умовах невизначеності та кризи, ідентифікації стратегічних ризиків для стану економічної безпеки суб’єктів господарювання, оцінювання впливу ризиків на досяжність стратегічних цілей підприємств, уточнення характеристик стратегічного управління у різних станах економічної безпеки бізнесу та до проблематики управління змінами під час реалізації стратегій та передбачення їх економічних наслідків.

4. Надано характеристику методичних підходів до розробки стратегій для сучасних підприємств з позиції вітчизняного та зарубіжного досвіду. Виявлено, що вітчизняний досвід стратеготворення характеризується домінуванням традиційних (планових і функціональних) підходів до розробки стратегій, поступовим переходом до ризик-орієнтованого стратегічного управління, високою актуальністю та популяризацією резильєнтних стратегій через реалії

воєнного часу та нерівномірною цифровізацією бізнес-процесів українських підприємств. Для зарубіжного досвіду притаманними є перехід від класичних моделей до адаптивних і цифрових стратегій розвитку бізнесу, масштабне використання цифрових інструментів, аналізу даних і штучного інтелекту у механізмах стратегічного менеджменту; розвиток екосистемного мислення серед персоналу компаній, інтеграція інновацій та резильєнтності у стратегіях підприємств.

5. Оцінено вплив цифрових ризиків на стан економічної безпеки вітчизняних підприємств, який перебуває у прямій залежності від рівня цифровізації бізнес-процесів: чим масштабнішою є інтеграція компанії в цифровий економічний простір, тим суттєвішим є вплив цифрових ризиків на фінансові показники її діяльності. Встановлено, що цифрові загрози мають системний характер, і здебільшого впливають одночасно на декілька функціональних підсистем комплексної системи економічної безпеки: інформаційно-аналітичну (страждає через кібератаки, витік конфіденційних даних та порушення цілісності IT-інфраструктури), інтелектуально-кадрову (потерпає від низької цифрової грамотності персоналу, наслідків соціальної інженерії, дефіциту фахівців та відсутності цифрових компетенцій і низького рівня цифрової грамотності), техніко-технологічну (цифрові ризики призводять до зупинки виробничих процесів та зниження операційної ефективності), фінансову (підприємство зазнає прямих і непрямих збитків через вимагання коштів, штрафи, витрати на відновлення бізнес-процесів), правову (судові позови через невиконання контрактів, порушення прав інтелектуальної власності). Оцінка цифрових ризиків є перспективним інструментом обґрунтування досяжності довгострокових цілей під час розробки стратегії: якщо потенційні ризики перевищують захисні можливості підприємства, така стратегія має бути адаптовано модифікованою і презентованою у новому сценарії.

6. Проведено діагностику ефективності безпеко орієнтованих стратегій українських підприємств. Об’єктами дослідження було обрано десять

підприємств критичної інфраструктури – національного та регіонального значення. На підставі аналізу даних з відкритих джерел та думок експертів, було встановлено, що ПрАТ «Київстар» має високий рівень економічної безпеки, НЕК «Укренерго», АТ «Укртелеком», АТ «Укрпошта» та АТ «Укрзалізниця» – середній рівень економічної безпеки; АТ «Черкасиобленерго» та КП «Черкасиводоканал» – достатній рівень економічної безпеки; КПТМ «Черкаситеплокомуненерго», АТ «Черкаський автобус» та ПрАТ «Черкаське хімволокно» – низький рівень економічної безпеки. На підставі цього було зроблено висновок, що вітчизняні підприємства в цілому ефективно реалізують свої безпеко орієнтовані стратегії та частково досягають стратегічних цілей, пов'язаних з досягненням стану економічної безпеки. Водночас, наявність серед об'єктів критичної інфраструктури компаній з низьким рівнем економічної безпеки свідчить про потребу перегляду та адаптації їй стратегій або ж модернізації механізмів і алгоритмів їх реалізації.

7. Модифіковано та доповнено концептуальні засади адаптації стратегічного управління підприємствами під впливом цифровізації. Запропоновано такі напрями адаптації стратегічного управління підприємством під впливом цифровізації задля досягнення стану економічної безпеки, як: ідентифікація цифрових ризиків тривалої дії, оцінювання впливу цифрових ризиків на досяжність стратегічних орієнтирів підприємства, формування підсистеми забезпечення цифрової економічної безпеки бізнесу, розроблення цифрової стратегії функціонування та розвитку підприємства з урахуванням цілей економічної безпеки та запровадження механізму стратегічної адаптації до ризиків (у тому числі і цифрових). Розроблення цифрової стратегії бізнесу потребує формування окремого розділу у генеральній стратегії суб'єкта господарювання або розроблення окремої функціональної стратегії, присвяченої конкретно питанням і проблематиці цифровізації бізнесу в умовах невизначеності цифрових трансформацій економічного простору та ризиків, які з цим пов'язані. Натомість запровадження механізму стратегічної адаптації підприємства передбачає встановлення періодичності перегляду існуючої

стратегії та наявності протоколу та алгоритмів дій у випадку нагальної потреби внесення змін до розділів стратегії або до переліку стратегічних орієнтирів з ініціативи менеджменту чи інших категорій стейкхолдерів.

8. Запропоновано шляхи оновлення механізму стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів. На основі розробленої матриці стейкхолдерів було виявлено основні групи зацікавлених сторін (власники компаній; топ-менеджмент, персонал; клієнти; споживачі продукції і послуг; постачальники, партнери; держава та владні структури, інвестори, кредитори, інші фінансові донори; об'єднані територіальні громади; IT-провайдери, надавачі цифрових послуг; конкуренти) і ідентифіковано їх пріоритетні інтереси, які слугують каталізаторами для адаптивної модифікації сучасних безпеко орієнтованих стратегій для сучасних підприємств. Практичне значення запропонованої матриці, як інструменту інформаційного забезпечення адаптивного стратегічного менеджменту, полягає у визначенні стратегічних інтересів стейкхолдерів, їх інтересів у контексті управління цифровими ризиками, інтересів щодо стану економічної безпеки підприємства, а також у прогнозі прояву додаткових ризиків, спричинених у разі неврахування цих інтересів і нездатності управлінського персоналу збалансувати їх шляхом адаптації стратегічних орієнтирів суб'єктів господарювання. Оцінювання впливу стейкхолдерів на стратегічні орієнтири підприємства згідно матриці Менделоу дало змогу змоделювати оновлений механізм стратегічного управління економічною безпекою підприємства, що відрізняється від існуючих елементом пошуку можливостей і діагностики стану дотримання балансу інтересів його стейкхолдерів. Особливістю цього механізму є комплексне застосування можливостей гнучкого менеджменту на усіх етапах його функціонування, що дозволяє адаптувати стратегію до мінливих умов навколишнього середовища, які виявляються у реаліях світу BANI та посилюються цифровими трансформаціями екосистем. На першому етапі пропонується адаптувати структурну будову класичного механізму стратегічного управління

економічною безпекою підприємства до актуальних умов сьогодення, на другому провести реалізацію стратегічних орієнтирів засобами функціонування адаптованого механізму та на третьому етапі здійснити оцінювання його ефективності та ідентифікувати потребу у нових адаптивних модифікаціях його структури або функціоналу. До особливостей та відмінних рис авторського механізму можна віднести: пропозиції щодо планування стратегічних цілей за SMART-підходом з орієнтацію на інтереси стейкхолдерів за кількома сценаріями, узгодження таймінгу та метрик проміжних і фінальних результатів, що дозволяє оперативно вносити зміни та стало рухатися до досягнення стратегічних цілей бізнесу у площині економічної безпеки; та виокремлення чотирьох важливих процесів, які мають відбуватися під час реалізації стратегічних орієнтирів, а саме: захист екосистеми підприємства, розробка win-win стратегій для партнерських відносин, людиноцентрований HR-менеджмент та убезпечення бізнес-процесів за допомогою наявних у суб'єкта господарювання корпоративних ресурсів.

9. Встановлено можливості та перспективи інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку підприємств в Україні. Простежено зв'язки принципів цифрового ризик-менеджменту (превентивність заходів з безпеки і управління ризиком, орієнтованість на баланс інтересів стейкхолдерів, адаптивність управлінських систем, резильєнтність ризикам і загрозам цифрового простору, управління на основі актуальних даних, нульова довіра) зі стратегічними цілями системи економічної безпеки підприємств. Запропоновано стратегічні цілі щодо інтеграції цифрового менеджменту у процеси управління економічною безпекою українських підприємств, формалізовані із використанням технології SMART та описані за допомогою KPI та OKR. Доведено, що їх досяжність тісно пов'язана з рівнем цифрової грамотності персоналу. Окреслено сутність Win-Win стратегій заохочення працівників до цифрового професійного розвитку та безпеко орієнтованої поведінки, такі як: «Цифровий капітал і потенціал працівника», «Гейміфікація цифрової безпеки», «Технологічний

апгрейд бізнес-процесів», «Гнучкість управління через довіру і людиноцентризм», «Цифрова ергономіка та безпека праці». У якості інструменту аналітики для визначення почерговості інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств запропоновано використовувати інтегральний індекс впливу стейкхолдерів на стратегічні орієнтири бізнесу. Інтерпретація його значень продемонструвала, що максимальний рівень цього показника мають власники та інвестори суб'єктів господарювання, їх управлінський персонал і виконавчий персонал, а також представники державних органів влади. Банки та фінансові донори, клієнти і споживачі зазвичай мають високий рівень впливу (інколи середній) на інтеграцію принципів цифрового ризик-менеджменту в бізнес-процеси, постачальники і контрагенти – середній (інколи високий), а громада (локальне ком'юніті) – низький (інколи середній). Запропоновано авторський підхід до інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку вітчизняних підприємств, що полягає у реалізації чотирьох етапів управлінських дій: аналізі зовнішнього середовища із фокусом на можливості цифровізації, ризики війни, тенденції BANI-світу, кадровий голод, прояви пермакриз та загальноекономічної невизначеності; формуванні та використанні організаційно-управлінського механізму, що використовується для створення безпеко орієнтованої стратегії, яка реалізується на наступному етапі та сприяє цифровому економічному розвитку бізнесу (четвертий фінальний етап).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шарий В.І., Павлюк Є. С. Логічний аналіз стратегічного управління в організації. *Економіка та суспільство*. 2024. №70. URL: https://economyandsociety.in.ua/index.php/journal/article/view/5342/5285 (дата звернення: 02.01.2026).

2. Porter M. E. Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York: Free Press, 1980. 422 p.

3. Porter M. E. Competitive Advantage: Creating and Sustaining Superior Performance. New York: Free Press, 1985. 557 p.

4. Porter M. E. How Competitive Forces Shape Strategy. *Harvard Business Review*. 1979. Vol. 57, № 2. P. 137-145.

5. Porter M. E. The Competitive Advantage of Nations. New York: Free Press, 1990. 855 p.

6. Porter M. E. What is Strategy? *Harvard Business Review*. 1996. Vol. 74, №. 6. P. 61-78.

7. Філософія: навч. посіб. / Л. В. Губерський, І. Ф. Надольний, В. П. Андрущенко та ін. ; за ред. І. Ф. Надольного. 3-тє вид., стер. К.: Вікар, 2002. 516 с.

8. Стеченко Д. М., Чмир О. С. Методологія наукових досліджень: підручник. 2-ге вид., переоб. і доп. К. : Знання, 2007. 317 с.

9. Малиновський В. Я. Словник термінів і понять з державного управління. К. : Атіка, 2005. 240 с.

10. Балан В. Г. Методи нечіткого багатокритерійного аналізу у формуванні нової парадигми стратегічного управління підприємствами. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2025. № 1(1). С. 132-146.

11. Бірбіренко С. С. Методологічні аспекти формування концепції стратегічного управління економічною стійкістю телекомунікаційного

підприємства. *Східна Європа: економіка, бізнес та управління*. 2022. Вип. 1. С. 55-60.

12. Зачосова Н. В., Чакалов Р. К. Методологія досліджень проблем менеджменту у контексті стратегічного управління економічною безпекою підприємств. *Східна Європа: економіка, бізнес та управління*. 2024. Вип. 2. С. 51-56.

13. Кащена Н. Б., Остапенко Р. М., Чміль Г. Л. Стратегічний аналіз в управлінні діяльністю підприємств агробізнесу: організаційно-методичний аспект. *Наукові праці Міжрегіональної академії управління персоналом. Економічні науки*. 2023. Вип. 2. С. 40-46.

14. Кондратенко Н. О., Новікова М. М., Волкова М. В., Швед А. Б. Теоретико-методичні аспекти управління стратегічним розвитком промислових підприємств України. *Проблеми економіки*. 2022. № 4. С. 163-170.

15. Оболенцева Л. В., Вороніна О. О. Теоретико-методичні аспекти стратегічного управління підприємствами туристичної індустрії. *Наукові записки Національного університету "Острозька академія". Серія : Економіка*. 2021. № 20. С. 76-81.

16. Польова О. Л., Бігун В. С., Савицький О. А. Методичні підходи розробки економічної стратегії управління підприємством. *Ефективна економіка*. 2024. № 8. URL: http://nbuv.gov.ua/UJRN/efek_2024_8_33 (дата звернення: 10.01.2026).

17. Самойленко В. В. Оцінка методів стратегічного управління бізнес-процесами підприємства в період цифровізації. *Ефективна економіка*. 2025. № 4. URL: http://nbuv.gov.ua/UJRN/efek_2025_4_70 (дата звернення: 10.01.2026).

18. Сидорчук А. О. Теоретико-методологічні засади стратегічного управління підприємствами залізничного транспорту в кризових умовах. *Ефективна економіка*. 2024. № 9. URL: http://nbuv.gov.ua/UJRN/efek_2024_9_71 (дата звернення: 10.01.2026).

19. Янгулов Е. П. Теоретичне обґрунтування методологічних основ моделі стратегічного управління для малих підприємств. *Економічний простір*. 2024. № 196. С. 128-136.

20. Павлюк Є.С. Сучасні підходи до стратегічного управління підприємствами: зміни парадигм під впливом пермакризи та ризиків світу BANI. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут»*. 2025. № 35. С.162-167.

21. Ambuli T. V., Vikram G., Devendran A., Mickle Aancy H., Sudhakar M. Strategic integration of smart digital business continuity and configuration management. *Essential Information Systems Service Management*. 2024. P. 133-162.

22. Anggraeni R. N., Amir A. M., Jurnana J., Rajindra R. Strategic decision-making as a behavioral bridge: Mediating the impact of contingency factors on management accounting practices in digital startups. *Multidisciplinary Science Journal*. 2026. URL: https://doi.org/10.31893/multiscience.2026417 (дата звернення: 17.10.2025).

23. Červinka T. Digital transformation of strategic management of SMEs in the Czech Republic. *Journal of Information and Organizational Sciences*. 2023. №47(2). P. 385-398.

24. Çolak M., Erdost Çolak H. E. Future of Strategic Management in the Digital Age. *Accounting Finance Sustainability Governance and Fraud*. 2025. Part F517. P. 233-249.

25. Djakeli K. Strategic management for digital platform brands in the phygital era. *Brand Creation and Management in the Phygital Era*. 2025. P. 499-520.

26. El Massaoudii E. M., Berdi A., Krim B. M., El Hammoumi A., El Ouali A. Digital Transformation: A Strategic Lever for Collaborative and Agile Management. *International Conference on Circuit Systems and Communication Iccsc*. 2025.

27. Espina-Romero L., Ferrer-Dávalos R. M., Parra D. R., Izaguirre Olmedo J. S. R. Digital Competencies, Human Resource Management, and Culture as Strategic Drivers of Sustainable Digital Transformation in SMEs of Lima. *Administrative*

Sciences. 2026. Vol. 16, Iss. 1. Art. 3. https://doi.org/10.46661/10.3390/admsci16010003 (дата звернення: 17.10.2025).

28. Goel A. V., Kumari P., Vaghela K., Salman S. A., Brahmane P. Strategic change management in the era of digital disruption: an interdisciplinary study on organisational adaptability and innovation culture. *Scientific Culture*. 2025. 11(4). P. 236-246.

29. Hu B., Yang W., Zhang S., Yan S., Xiang Y. Linking the top management team transactive memory system, strategic flexibility and digital business model innovation: a dynamic capabilities perspective. *Technology Analysis and Strategic Management*. 2025. №37(11). P. 1621-1633.

30. Jadon R. Exploring strategic management approaches for environmentally sustainable digital transformation: A case study analysis. *Adaptive Strategies for Green Economy and Sustainability Policies*. 2025. P. 631-648.

31. Koundal P., Bhalla M., Kailay M. Driving SME management in the digital era: an empirical evidence on the role of accounting information systems in strategic planning, controlling, and coordination activities. *International Journal of Globalisation and Small Business*. 2025. №15(2). P. 135-157.

32. Malewska K., Chwiłkowska-Kubala A., Szumowski W. Digital technology infrastructure management and business strategic alignment as enablers of digital capabilities in energy SMEs. *Economics and Environment*. 2025. №94(3). P. 1026.

33. Palmié M., Aebersold A., Oghazi P., Pashkevich N., Gassmann O. Digital-sustainable business models: Definition, systematic literature review, integrative framework and research agenda from a strategic management perspective. *International Journal of Management Reviews*. 2025. № 27(3). P. 346-374.

34. Pietsch W. Balancing the Sustainability of Digital Product Management from a Strategic Business Perspective. *Lecture Notes in Business Information Processing*. 2025. 528 LNBIP. P. 15-27.

35. Schildt H., Lahdenranta K., Demir R., Turunen T. Waking up to digital innovation: how organisational secrecy hampers top management focus on strategic renewal. *Innovation Organization and Management*. 2024. 26(4). P. 532-558.

36. Yuwono W., Fitriyanti S. D., Nainggolan F. The Impact of Digital Marketing Innovation and Strategic Orientation on Firm Performance: Mediation by Marketing Capability and Moderation by Risk Management. *Revista de Metodos Cuantitativos para la Economia y la Empresa*. 2025. URL: https://doi.org/10.46661/rev.metodoscuant.econ.empresa.10841 (дата звернення: 17.10.2025).

37. Кубліцька О. В. Теоретико-методичні основи управління стратегічним розвитком підприємств електронної комерції. *Проблеми і перспективи економіки та управління*. 2024. № 1. С. 133–145.

38. Гребенікова О. В., Денисова Т. В. Теоретичні та практичні аспекти стратегічного управління інвестиційним потенціалом підприємств. *Часопис економічних реформ*. 2025. № 1. С. 69–76.

39. Янгулов Е. П. Теоретичне обґрунтування методологічних основ моделі стратегічного управління для малих підприємств. *Економічний простір*. 2024. № 196. С. 128–136.

40. Сидорчук А. О. Теоретико-методологічні засади стратегічного управління підприємствами залізничного транспорту в кризових умовах. *Ефективна економіка*. 2024. № 9. URL: http://nbuv.gov.ua/UJRN/efek_2024_9_71 (дата звернення: 11.12.2025).

41. Семенча І. Є., Гринько Т. В. Ризики в діяльності сучасного бізнесу в Україні: підходи до прийняття рішень та побудови стратегій управління. *Економіка. Фінанси. Право*. 2025. № 7. С. 97–101.

42. Сазонова С. В. Ідентифікація ризиків стратегічного управління телекомунікаційними підприємствами в умовах цифрової економіки. *Причорноморські економічні студії*. 2021. Вип. 72(2). С. 7–12.

43. Вербовський І. Стратегічне управління в умовах ризику та невизначеності. *Економіка. Управління. Інновації. Серія : Економічні науки*. 2024. Вип. 1. URL: http://nbuv.gov.ua/UJRN/eui_2024_1_10 (дата звернення: 11.12.2025).

44. Рябуха О. О. Стратегічне управління розвитком підприємства в умовах конкурентних ризиків та невизначеності. *Ефективна економіка*. 2023. № 12. URL: http://nbuv.gov.ua/UJRN/efek_2023_12_76 (дата звернення: 11.12.2025).

45. Zachosova N., Kutsenko D., Koval O. Strategy and mechanism of enterprises financial and economic security management in the conditions of war, Industry 4.0 and BANI World. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2022. № 4. С. 223–233.

46. Зачосова Н. В., Назаренко С. А., Собко В. В. Формування системи фінансово-економічної безпеки суб'єкта господарювання та стратегічне управління нею у реаліях BANI World. *Підприємництво та інновації*. 2022. Вип. 23. С. 59–62.

47. Дуднєва Ю. Е., Долгополов В. О. Особливості підприємницької діяльності в контексті викликів BANI-світу. *Адаптивне управління: теорія і практика. Серія : Економіка*. 2022. Вип. 14. URL: http://nbuv.gov.ua/UJRN/admthp_2022_14_10 (дата звернення: 16.02.2026).

48. Захаров Є. В. Порівняльний аналіз підходів до концепцій світу: SPOD суспільство, VUCA суспільство та BANI суспільство. *Соціальна економіка*. 2022. Вип. 64. С. 149-158.

49. Цифра Т. Ю., Моголівець А. А., Вершигора Д. М. Digital-skills економістів-будівельників в епоху VUCA та BANI-світу. *Шляхи підвищення ефективності будівництва в умовах формування ринкових відносин*. 2022. Вип. 49(1). С. 192-205.

50. Bushuyev S., Ivko A., Mudra M., Murovanskiy H., Piliuhina K. Adaptability in managing innovative projects within the BANI environment. *Управління розвитком складних систем*. 2023. Вип. 54. С. 5-11.

51. Bushuyev S., Piliuhina K., Chetin E. Transformation of values of the high technology projects from a VUCA to a BANI environment model. *Сучасний стан наукових досліджень та технологій в промисловості*. 2023. № 2. С. 191-199.

52. Буняк Н. Особливості менеджменту в умовах BANI-світу. *Економічний часопис Волинського національного університету імені Лесі Українки*. 2023. № 4. С. 97-103.

53. Зачосова Н. В., Козак В. В. Стратегічне управління кадровою безпекою підприємства як напрям збереження та розвитку людського капіталу в умовах BANI World та Індустрії 4.0. *Східна Європа: економіка, бізнес та управління*. 2023. Вип. 3. С. 35-39.

54. Жегус О. В. Маркетингове управління в забезпеченні резильєнтності бізнесу в умовах BANI-світу. *Бізнес Інформ*. 2024. № 4. С. 348-359.

55. Ільїн О. О., Бушуєв С. Д., Гоц В. В., Лященко Т. О. Управління IT-проєктами бізнес-аналітики у BANI-оточенні. *Управління розвитком складних систем*. 2024. Вип. 59. С. 45-52.

56. Помаза-Пономаренко А. Л., Батир Ю. Г., Лопатченко І. М. Вплив BANI-світу на державне регулювання ринку праці та державну молодіжну політику. *Вісник Національного університету цивільного захисту України. Серія : Державне управління*. 2024. Вип. 1. С. 296-306.

57. Varenyk V., Piskova Zh. Agile organisations in the BANI era: Case studies of companies utilising Scrum. *Управління розвитком*. 2025. Т. 24, № 2. С. 8-19.

58. Данько Я. П. Навігація в умовах екзистенційної невизначеності: трансформація особистості та VUCA/BANI середовищ. *Перспективи та інновації науки (Серія "Педагогіка", Серія "Психологія", Серія "Медицина")*. 2025. № 7. С. 1234-1243.

59. Кифяк В. Методологія дослідження середовища розвитку бізнесу з метою встановлення стратегічних пріоритетів агробізнесу в умовах BANI-світу. *Economic synergy*. 2025. Вип. 3. С. 97-114.

60. Попова Н. В., Муха Т. А. Адаптація SaaS-стратегій до логістичних викликів VUCA/BANI-середовища в контексті сталого розвитку ланцюгів постачання. *Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент*. 2025. Вип. 63. С. 41-47.

61. Савенко О. А. Теоретичні аспекти формування виробничого менеджменту підприємства в умовах BANI-середовища. *Інвестиції: практика та досвід*. 2025. № 2. С. 121-127.

62. Чала Т. Г., Юхименко М. С. Виклики вимірювання ділових очікувань і невизначеності бізнесу в умовах трансформації до BANI-світу: статистичний підхід. *Проблеми економіки*. 2025. № 1. С. 357-366.

63. Jørgensen M. Welcome to the TUNA world! *LinkedIn*. 2024. URL: https://www.linkedin.com/pulse/welcome-tuna-world-mads-j%C3%B8rgensen-75aze/ (дата звернення: 16.03.2026).

64. VUCA-World. VUCA, BANI, RUPT & TUNA. VUCA-World: Management in a world of complexity. URL: https://www.vuca-world.org/vuca-bani-rupt-tuna/ (дата звернення: 16.03.2026).

65. Невизначеність, брак талантів та майбутнє: якою є реальність для України та що відбувається у світі. *Budni: платформа про роботу від robota.ua*. URL: https://budni.robota.ua/hr/neviznachenist-brak-talantiv-ta-maybutnye-yakoyu-ye-realnist-dlya-ukrayini-ta-shho-vidbuvayetsya-u-sviti (дата звернення: 16.03.2026).

66. Що таке BANI-світ і як у ньому вижити? *Портал ГУРТ*. 2023. URL: https://gurt.org.ua/news/informator/94406/ (дата звернення: 16.03.2026).

67. Шаленна О. Як жити в нестабільному світі: VUCA, BANI, TUNA. *Shalenna.pro: Психологія та саморозвиток*. 2024. URL: https://shalenna.pro/yak-zhyty-v-nestabilnomu-sviti/ (дата звернення: 16.03.2026).

68. Pavliuk E. Current state of development of scientific theories of strategic management of enterprises under the influence of digitalization. *Пріоритетні напрями досліджень в науковій та освітній діяльності*: матеріали XVII Міжнародної науково-практичної конференції. м. Львів, 9-10 січня 2026 року. Львів: Львівський науковий форум, 2026. С.6-10.

69. Климчук М. М., Ачкасов І. А., Климчук С. А., Поляк О. П. Вплив ризик-менеджменту на формування стратегії управління бізнес-процесами

підприємства в умовах цифрової економіки: міжнародний досвід. *Бізнес Інформ*. 2021. № 1. С. 272-278.

70. Гедз М. Й., Вишневська В. А., Науменко С. Д. Маркетингові стратегії та економічні ризики цифровізації інтеграційно-диверсифікаційних процесів в корпоративному менеджменті. *Вісник економічної науки України*. 2024. № 1. С. 131-138.

71. Хаустова К. М., Мельник Я. В. Індикатори стратегічного контролю як складова цифрового менеджменту підприємства. *Бізнес Інформ*. 2021. № 10. С. 351-357.

72. Дергачова В. В., Колешня Я. О., Голюк В. Я. Цифрова термінологія у стратегіях: сутність, місце та роль діджитал менеджменту. *Економічний вісник Національного технічного університету України "Київський політехнічний інститут"*. 2022. № 22. С. 114-117.

73. Грінка Т. І., Немченко Т. А. Нові стратегії менеджменту при цифровій трансформації бізнесу в Україні. *Центральноукраїнський науковий вісник. Економічні науки*. 2023. Вип. 9. С. 49-57.

74. Scopus. https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=953f5db8aba259ddb59b418e2b45b594&sot=a&sdt=a&sl=24&s=TITLE%28economic+security%29&origin=resultslist&count=10&analyzeResults=Analyze+results (дата звернення: 10.03.2026).

75. Адлер О. О., Кавецький В. В. Стратегічне управління бізнес-процесами підприємства на основі рівня його економічної безпеки. *Innovation and Sustainability*. 2024. Iss. 1. С. 73-82.

76. Живко З. Б., Овєчкіна О. А., Родченко С. С., Сакун Л. М. Інноваційна модель стратегічного розвитку в управлінні безпековою економікою в умовах посилення зовнішньоекономічних зв’язків та діджиталізації. *Формування ринкових відносин в Україні*. 2022. № 4. С. 44-51.

77. Живко З. Б., Писаренко В. В., Савенко О. А., Шпортюк Н. Л. Моделювання системи безпекового стратегічного управління інноваційно

орієнтованих підприємств агропродовольчої сфери в глобалізаційних умовах економіки знань. *Формування ринкових відносин в Україні*. 2022. № 11. С. 37-45.

78. Зачосова Н. В., Коваль О. В., Сафонов Д. В. Активні та пасивні стратегії управління економічною безпекою суб'єктів господарювання в умовах традиційних та інноваційних загроз. *Економіка, управління та адміністрування*. 2023. № 1. С. 43-48.

79. Зачосова Н. В., Коваль О. В., Шевченко В. В. Стратегічне управління ризиками в системі економічної безпеки суб'єктів господарювання в умовах Індустрії 4.0. Проблеми системного підходу в економіці. 2020. Вип. 5. С. 47-51.

80. Зачосова Н. В., Коваль О. В., Байкер М. В. Розвиток персоналу та кадрового потенціалу як елементи стратегічного управління фінансово-економічною безпекою суб'єкта господарювання. *Науковий погляд: економіка та управління*. 2022. № 1. С. 61-66.

81. Копча Ю. Ю. Науковий підхід до формування стратегічних орієнтирів управління потенціалом економічної безпеки підприємств. *Бізнес Інформ*. 2019. № 7. С. 330-336.

82. Корчевська Л. О. Адаптаційні та біфуркаційні стратегії управління економічною безпекою підприємства. *Академічний огляд*. 2020. № 1. С. 26-37.

83. Латишева О. В., Касьянюк С. В., Мілявський М. Ю. Визначення особливостей управління витратами в системі формування стратегії економічної безпеки та сталого розвитку вітчизняних підприємств. *Економіка. Фінанси. Право*. 2018. № 7. С. 15-20.

84. Лізут Р. А. Загальні та деталізовані стратегії управління організаційно-економічною безпекою підприємств. *Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка*. 2019. Вип. 202. С. 265-274.

85. Олійник А., Іщейкін Т., Карташов Р., Невкритий М. Стратегічне управління економічною безпекою аграрного підприємства у бізнес-середовищі. *Вісник Хмельницького національного університету. Економічні науки*. 2024. № 6. С. 234-238.

86. Онищенко О. В., Яценко Н. М., Гончаренко Н. О. Роль економічної безпеки у стратегічному управлінні промисловим підприємством. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2022. № 4. С. 119-127.

87. Приймак Н. С., Дев'яткова О. В. Стратегічне управління економічною безпекою підприємства: теоретичні основи та інструментарій. *Вісник Донецького національного університету економіки і торгівлі імені Михайла Туган-Барановського. Серія : Економічні науки*. 2022. № 1. С. 37-45.

88. Сидорчук І. Систематизація теоретико-методологічних підходів до формування, реалізації та моделювання стратегій управління інноваційним розвитком та фінансово-економічною безпекою підприємницьких структур. *Modeling the development of the economic systems*. 2021. № 2. С. 33-39.

89. Сімкова Т. О. Управління розвитком автотранспортних підприємств у контексті визначення складових механізму формування стратегічних напрямків в умовах гарантування економічної безпеки. *Економічний вісник Дніпровської політехніки*. 2025. № 1. С. 137-147.

90. Толпежніков Р. О., Толпежнікова Т. Г., Балашов М. І. Методологічні підходи до управління змінами в стратегії забезпечення потенціалу економічної безпеки промислових підприємств. *Менеджер*. 2019. № 4. С. 56-63.

91. Топоркова О. В., Акімова Н. С., Наумова Т. А. Стратегічні аспекти управління ризиками для забезпечення економічної безпеки підприємства. *Бізнес Інформ*. 2019. № 8. С. 237-243.

92. Турило А. М., Турило А. А., Короленко Р. В., Короленко С. М. Стратегія розвитку, корпоративне управління і людський капітал відносно економічної стратагеми, економічної девіації і фінансово-економічної безпеки в діяльності підприємства. *Вісник Криворізького національного університету*. 2022. Вип. 54. С. 109-114.

93. Яремко І. І. Сучасні інструменти стратегічного управління як засіб підвищення економічної безпеки підприємства. *Публічне адміністрування та національна безпека*. 2023. № 10. С. 51-56.

94. Google Trends. https://trends.google.com.ua/explore?q=%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0&date=today%205-y&geo=UA (дата звернення: 10.03.2026).

95. Костюк Ж. С. Поняття ризику, небезпеки та загрози як базових категорій розкриття сутності економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2013. Вип. 43. С. 142-149.

96. Цікановська Н. А. Інтерпретація понять "виклик", "небезпека", "загроза" та "ризик" у теорії фінансової безпеки. *Фінансовий простір*. 2013. № 3. С. 110-114.

97. Новіков А. О. Взаємозв'язок понять ризику, небезпеки і загрози у контексті забезпечення фінансово-економічної безпеки. *International scientific journal*. 2015. № 8. С. 136-138.

98. Рудніченко Є. М. Загроза, ризик, небезпека: сутність та взаємозв'язок із системою економічної безпеки підприємства. *Економіка. Менеджмент. Підприємництво*. 2013. № 25(1). С. 188-195.

99. Лубенець І. О. Трактування сутності категорій невизначеність, загроза та ризик у контексті економічної безпеки підприємства. *Вісник Запорізького національного університету. Економічні науки*. 2017. № 1. С. 158-165.

100. Данкевич А. Є., Ткачук Г. Ю. Теоретична сутність ризиків, небезпек та загроз у контексті забезпечення економічної безпеки підприємства. *Економічний вісник університету*. 2018. Вип. 38. С. 118-125.

101. Нікітіна А. В. Поняття загрози, ризику, небезпеки та їх взаємозв'язок в системі економічної безпеки підприємств за умов висококонкурентних ринків. *Проблеми і перспективи розвитку підприємництва*. 2017. № 3(1). С. 64-69.

102. Колісніченко П. Т. Загрози, ризики та небезпеки в системі економічної безпеки підприємства. *Науковий вісник Херсонського державного університету. Сер. : Економічні науки*. 2017. Вип. 24(1). С. 56-59.

103. Мельник С. І. Дослідження викликів, ризиків, загроз та небезпеки в системі забезпечення фінансової безпеки підприємства. *Проблеми системного підходу в економіці*. 2019. Вип. 4(1). С. 172-177.

104. Зачосова Н. В. Поняття фінансової безпеки як наукової та управлінської категорії у взаємозв'язку з дефініціями виклику, небезпеки, загрози і ризику. *Вісник Черкаського національного університету імені Богдана Хмельницького. Серія : Економічні науки*. 2019. Вип. 2. С. 34-40.

105. Корнієнко Т. О. Вплив загроз та ризиків на формування системи економічної безпеки підприємства. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2022. № 4. С. 43-48.

106. Капелюшна Т. В. Формування площини безпеки підприємства під дією ризиків і загроз. *Бізнес Інформ*. 2024. № 3. С. 255-262.

107. Чернега О. М., Левченко В. М. Операційні ризики в управлінні підприємством: аналіз та шляхи мінімізації. *Вісник економічних наук України*. 2021. № 1 (40). С. 13-19.

108. Бойчук Т., Даньков А. Управління ризиками в контексті забезпечення фінансово-економічної безпеки транспортних і промислових компаній. *Науковий вісник Полісся*. 2023. № 2. С. 143-160.

109. Буданов М. П. Управління ризиками в системі організаційно-економічного забезпечення енергетичної безпеки підприємств. *Економічний вісник Дніпровської політехніки*. 2024. № 3. С. 150-160.

110. Нестеренко В. Ю., Прокопенко М. В., Коваль І. Б. Антикризове управління в системах ризик-менеджменту та управління економічною безпекою підприємства. *Проблеми і перспективи розвитку підприємництва*. 2024. № 1. С. 136-143.

111. Герасименко О. М., Зачосова Н. В. Оцінка рівня зрілості управління ризиками в процесі забезпечення економічної безпеки підприємства: аналітичне дослідження. *Вісник Київського національного університету технологій та дизайну. Серія : Економічні науки*. 2019. № 3. С. 66–81.

112. Герасименко О. М., Пасєка С. Р. Концептуальні основи ризик-орієнтованого підходу до управління у процесі забезпечення системи економічної безпеки підприємств різних галузей народного господарства. *Вчені запиписки університету "КРОК". Серія : Економіка*. 2019. Вип. 4. С. 148-155.

113. Данілова Е. І. Методологія ризик-орієнтованого підходу до управління економічною безпекою підприємства. *Modern economics*. 2018. № 12. С. 61-68.

114. Гриценко Л. Л., Кожушко І. О., Чепурко В. О., Перепеліцин Г. Б. Ризик-орієнтоване управління в системі економічної безпеки корпоративного підприємства. *Бізнес Інформ*. 2023. № 8. С. 281-288.

115. Лоскутова Г. А. Ризик-орієнтоване управління у транспортних технологіях: шлях до економічної безпеки. *Інформаційно-керуючі системи на залізничному транспорті*. 2025. № 3(дод.). С. 47-48.

116. Потюк В. М. Управління ризиками та інтеграція цифрових інструментів у бізнес-процеси підприємств для забезпечення їх економічної безпеки в умовах трансформації національної економіки. *Наукові інновації та передові технології*. 2025. № 12. С. 3285-3308.

117. Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. *Вісник економіки*. 2021. Вип. 1. С. 97-110.

118. Бондарчук О. В. Системи моніторингу та управління ризиками в умовах цифровізації. *Інновації в бізнес-процесах*. 2020. № 7(2). С. 13-28.

119. Гонтар І. В. Великі дані в управлінні фінансовими ризиками. *Фінансова економіка*. 2023. № 21(3). С. 112-130.

120. Гончар О. В., Сидоренко О. М. Блокчейн та його застосування для управління корпоративними ризиками. *Технології блокчейн в бізнесі*. 2022. № 5(3). С. 102-115.

121. Гребенюк В. О. Автоматизація управлінських процесів та оцінка ризиків у сучасних ІТ-системах. *Інформаційні технології в економіці*. 2024. № 19(2). С. 89-104.

122. Гринюк В. Стратегічні ризики та управління ними в умовах глобалізації. Харків: Фоліо, 2021. 315 с.

123. Іванов А. В., Петренко М. О. ІТ-системи в управлінні ризиками: концептуальні підходи та технології. *Журнал інформаційних технологій і управління*. 2021. № 12(3). С. 25-38.

124. Іванов А. О. Управління фінансовими ризиками на підприємствах металургійної промисловості: методи та інструменти. *Журнал економічних досліджень*. 2021. № 15(3). С. 44-58.

125. Коваленко А. М. Машинне навчання як інструмент прогнозування ризиків у банківському секторі. *Журнал банківської справи*. 2023. № 22(4). С. 44–59.

126. Мельник І. В. Моделювання та аналіз ризиків підприємств : монографія. Львів: Видавництво ЛНУ ім. Івана Франка, 2020. 240 с.

127. Мельник І. О. Фінансові ризики: теорія та практика управління. Львів: Сполом, 2020. 198 с.

128. Мельник І. О., Шевчук В. В. Фінансові ризики та стратегії їх мінімізації. Львів: Сполом, 2020. 224 с.

129. Мельничук Л. І. Аналіз великих даних та їх роль в управлінні ризиками. *Економіка і бізнес*. 2023. № 10(1). С. 42-59.

130. Петров В. І., Сидоров С. В. Стратегічне управління підприємствами в умовах економічної нестабільності. Харків: Видавництво ХНУ імені В. Н. Каразіна, 2021. 302 с.

131. Степаненко О. В. Цифрові технології в управлінні ризиками. Київ: Вища школа, 2022. 186 с.

132. Степаненко С. Інноваційні та технологічні ризики в управлінні підприємствами. Київ: Наукова думка, 2022. 270 с.

133. Ткаченко С. І., Левченко В. Ю. Цифрові технології в управлінні ризиками підприємств: глобальні тенденції та український досвід. *Економіка і інновації*. 2023. № 14(1). С. 34-50.

134. Чернега С. П., Левченко О. В. Використання великих даних для оцінки і моніторингу ризиків. Одеса: Астропринт, 2021. 212 с.

135. Чернявська Т. С. Інформаційні технології в управлінні бізнес-ризиками. *Науковий вісник Національного університету*. 2022. № 18(4). С. 66-72.

136. Яковенко О. П. Штучний інтелект у фінансовому аналізі та управлінні ризиками. *Вісник банківської справи*. 2021. № 15(2). С. 77-93.

137.Павлюк Є.С. Методичні підходи до розробки стратегій для сучасних підприємств: зарубіжний досвід для вітчизняних управлінців. Сучасні наукові підходи до вирішення глобальних криз: роль інтеграції наук і технологій у змінах суспільства: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 13 лютого 2026 р.). Кременчук: ЦФЕНД, 2026. С.28-31.

138. Степанова О. В., Степанова Н. С. Методичний підхід до формування та оцінки стратегії підприємства. *Бізнес Інформ*. 2025. № 4. С. 318-324.

139. Чуприна Х., Ніколайко Д., Гуляєв Д., Якимчук Т. Наукові підходи та методологічні засади розробки стратегій модернізації підприємств. *Шляхи підвищення ефективності будівництва в умовах формування ринкових відносин*. 2024. Вип. 53(3). С. 37-56.

140. Балюк Ю. С. Методичне забезпечення формування стратегії розвитку експортно-імпортної діяльності підприємств. *Журнал стратегічних економічних досліджень*. 2023. № 6. С. 38-49.

141. Петченко М. В. Методологічні підходи до стратегізації розвитку інноваційних екосистем авіатранспортних підприємств. *Соціальна економіка*. 2025. Вип. 69. С. 180-189.

142. Олешко О. В., Дзюба О. М. Методичні аспекти удосконалення формування інноваційної стратегії підприємств. *Економіка. Фінанси. Право*. 2025. № 4. С. 66-70.

143. Терещенко С. І., В’юненко О. Б. Методологічні підходи до впровадження хмарних технологій у процес розробки та реалізації антикризової

стратегії підприємства під час воєнного стану. *Наука і техніка сьогодні. Серія : Педагогіка; Право; Економіка; Фізико-математичні науки; Техніка*. 2025. № 11. С. 587-601.

144. Kim W. C., Mauborgne R. *Blue Ocean Shift: Beyond Competing - Proven Steps to Inspire Confidence and Seize New Growth*. New York: Hachette Books, 2017. 336 p.

145. Aithal S. Black ocean strategy – a probe into a new type of strategy used for organizational success. *GE-International Journal of Management Research*. 2015. Vol. 3. P. 45-65.

146. Gündüz Ş. Preventing blue ocean from turning into red ocean: A case study of a room escape game. *Journal of Human Sciences*. 2018. Vol. 15, № 1. URL: https:doi.org/10.14687/jhs.v15i1.5140.

147. Mauborgne R., Kim W. C. Red Ocean Traps: The Mental Models That Undermine Market-Creating Strategies. *Harvard Business Review*. 2015. Vol. 93, № 3. P. 80-86.

148. Broman G., Robèrt K.-H. A Framework for Strategic Sustainable Development. *Journal of Cleaner Production*. 2015. Vol. 140. URL: https:doi.org/10.1016/j.jclepro.2015.10.121.

149. Кравченко А. О., Кузнецова С. О. Методика адаптивного стратегічного управління інвестиційною діяльністю підприємств в умовах високої ринкової турбулентності. *Бізнес Інформ*. 2025. № 5. С. 197-204.

150. Коваленко О. С. Щодо ролі методів і моделей прийняття управлінських рішень у процесі розробки стратегії економічного розвитку сучасних підприємств. *Наукові праці МАУП. Сер. : Економічні науки. Психологічні науки*. 2013. Вип. 2. С. 97-100.

151. Чичун В. А. Методологічні аспекти розробки корпоративних стратегій. *Вісник Чернівецького торговельно-економічного інституту. Економічні науки*. 2013. Вип. 1. С. 215-221.

152. Науменко М. О., Луханіна К. Д. Розробка методичного забезпечення стратегічного управління підприємством. *Вісник економіки транспорту і промисловості*. 2014. Вип. 45. С. 188-191.

153. Анісімова О. М., Шикова Л. В. SWOT – аналіз підприємства як метод забезпечення розробки ефективної стратегії управління. *Проблеми і перспективи розвитку підприємництва*. 2011. № 1. С. 24-30.

154. Палига Є. М., Бурда І. Я. Методичні засади розробки та реалізації стратегії забезпечення кадрової безпеки підприємства. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2013. Вип. 1. С. 292-297.

155. Цимбал С. В. Розробка методики вибору стратегії розвитку підприємств автомобільного транспорту. *Вісник Житомирського державного технологічного університету. Серія : Технічні науки*. 2014. № 2. С. 198-203.

156. Hoshin Kanri X Matrix. URL: https://www.vertex42.com/Files/download2/themed.php?file=hoshin-kanri-x-matrix.xlsx (дата звернення: 10.03.2026).

157. Балан В. Г. Методи нечіткого багатокритерійного аналізу у формуванні нової парадигми стратегічного управління підприємствами. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2025. № 1(1). С. 132-146.

158. Балан В. Оцінювання стратегічних наборів підприємства з використанням Fuzzy CODAS-методу. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2021. Вип. 2. С. 13-22.

159. Грищенко С. І. Методичні положення формування фінансової стратегії сталого розвитку підприємства туризму. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2025. № 2(2). С. 122-130.

160. Дем'яненко Т. І., Яковенко І. С. Реінжиніринг бізнес-процесів як сучасний метод управління стратегічними змінами на підприємстві. *Адаптивне управління: теорія і практика. Серія : Економіка*. 2022. Вип. 14. URL:http://nbuv.gov.ua/UJRN/admthp_2022_14_9 (дата звернення: 10.03.2026).

161. Дикань В. Л., Кузнецов Є. М. Методичне забезпечення формування стратегії сталого розвитку підприємств залізничного транспорту. *Вісник економіки транспорту і промисловості*. 2023. № 84. С. 9-20.

162. Овсієнко Н. В., Котвицька Н. М., Овсієнко В. В. Методичні підходи до створення стратегії управління ризиками сучасних підприємств. *Економічний простір*. 2025. № 197. С. 199-203.

163. Олійник Т. І., Сапожніков Н. М. Методологічні основи у формуванні адаптивної стратегії підприємницького середовища: планування асортименту та контроль якості продукції. *Ефективна економіка*. 2024. № 11. URL: https://www.nayka.com.ua/index.php/ee/article/view/5133 (дата звернення: 10.03.2026).

164. Польова О. Л., Бігун В. С., Савицький О. А. Методичні підходи розробки економічної стратегії управління підприємством. *Ефективна економіка*. 2024. № 8. URL: http://nbuv.gov.ua/UJRN/efek_2024_8_33 (дата звернення: 10.03.2026).

165. Турило А. М., Турило А. А., Короленко Р. В. Методологія наукових досліджень в аспекті загальної і фінансової стратегії підприємства. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2025. № 3(2). С. 135-140.

166. Філіна С. В., Дрига О. В., Кужель О. В. Теоретичні та методичні аспекти стратегії розвитку підприємства. *Економічний простір*. 2024. № 192. С. 120-124.

167. Янгулов Е. П. Теоретичне обґрунтування методологічних основ моделі стратегічного управління для малих підприємств. *Економічний простір*. 2024. № 196. С. 128-136.

168. Самойленко В. В. Оцінка методів стратегічного управління бізнес-процесами підприємства в період цифровізації. *Ефективна економіка*. 2025. № 4. URL: http://nbuv.gov.ua/UJRN/efek_2025_4_70 (дата звернення: 10.03.2026).

169. Сироїд Т. І. Методологічні підходи до формування та реалізації інвестиційно-інноваційної стратегії підприємства в умовах діджиталізації. *Інвестиції: практика та досвід*. 2024. № 15. С. 188-193.

170. Pavliuk E. The place of risk management in strategies for ensuring the economic security of enterprises. *Сучасний стан та тенденції розвитку науки та освіти* : матеріали III Міжнародної науково-практичної конференції / Міжнародний гуманітарний дослідницький центр (м. Дніпро, 5 січня 2026 р.). Research Europe, 2026. С.177-181.

171. Ковернега Т. А. Особливості формування стратегії управління економічними ризиками для забезпечення економічної безпеки на вітчизняних підприємствах. *Науковий вісник Херсонського державного університету. Сер. : Економічні науки*. 2014. Вип. 8(7). С. 98-102.

172. Солодовнік О. О. Ризики стратегічних рішень у сфері фінансово-економічної безпеки публічно-приватного партнерства. *Бізнес Інформ*. 2017. № 6. С. 240-244.

173.Павлюк Є.С. Оцінка впливу цифрових ризиків на стан економічної безпеки підприємства як елемент обґрунтування досяжності його стратегічних цілей. *Науково-виробничий журнал «Бізнес-навігатор».* 2026. Випуск 1 (84). С.9-14.

174. Добровольська В. В., Ляховецький О. О. Перешкоди та ризики при впровадженні цифрових технологій у господарську діяльність. *Науковий вісник Львівського державного університету внутрішніх справ. серія юридична*. 2024. Вип. 4. С. 10-18.

175. Зачосова Н. В., Коваленко А. О., Куценко Д. М. Кадрова політика у механізмі управління економічною безпекою в умовах четвертої промислової революції. *Академічний огляд*. 2022. № 2. С. 142-157.

176. Демчишак Н. Б., Клек А. Р., Цвєткова З. М. Інституційно-організаційні основи формування фінтех-екосистеми України: вплив інвестиційних ризиків на інноваційну активність і цифровізацію підприємств.

Ефективна економіка. 2024. № 7. URL: http://nbuv.gov.ua/UJRN/efek_2024_7_33 (дата звернення: 06.03.2026).

177. Осадча О. О., Роздопченюк В. М. Ризики економічної безпеки підприємства в умовах цифровізації. *Вісник Національного університету водного господарства та природокористування. Економічні науки*. 2024. Вип. 3. С. 116-126.

178. Світовий О. М., Вилєгжанін С. В. Застосування елементів штучного інтелекту в управлінні ризиками ІТ-проєктів в контексті цифрової трансформації підприємств. *Ефективна економіка*. 2025. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2025_5_34 (дата звернення: 06.03.2026).

179. Іванова Н. В., Кононенко С. О. Ризики економічної безпеки в контексті глобальної діджиталізації аутсорсингу. *Інвестиції: практика та досвід*. 2023. № 6. С. 168-174.

180. Сазонова С. В. Оцінка ризиків стратегічного управління телекомунікаційними підприємствами в умовах цифрової економіки. *Вісник Сумського національного аграрного університету. Серія : Економіка і менеджмент*. 2021. Вип. 3. С. 31-37.

181. Левченко О. М., Ткачук О. В., Царенко І. О. Соціально-економічні передумови забезпечення національної безпеки в умовах глобалізації. *Економіка і регіон*. 2018. № 1. С. 37-46.

182. Левченко О. М., Вовк М. О., Юрченко Н. І., Гаврилюк А. Р. Діагностика системи управління фінансово-економічною безпекою конкурентоспроможних підприємств агропродовольчої сфери в умовах цифровізації. *Агросвіт*. 2024. № 4. С. 22-30.

183. Panchenko V., Rushchyshyn M., Nemchenko T., Shtets T., Kalinin A. Modeling of the Assessment System of the Main Risks of Investing in Engineering Enterprises in the Conditions of the Development of the Knowledge Economy. *International Journal of Safety and Security Engineering*. 2022. Vol. 12, No. 5. P. 623–629.

184. Панченко В. А. Методичні засади аналізу та забезпечення економічної безпеки підприємств авіаційної галузі. *Проблеми економіки*. 2024. № 2. С. 174-180.

185. Панченко В., Панченко О. Інструментарій зміцнення економічної безпеки підприємств в умовах кризи. *Modeling the development of the economic systems*. 2024. № 3. С. 291-295.

186. Панченко В. Управління життєздатністю в системі економічної безпеки підприємств. *Modeling the development of the economic systems*. 2022. № 3. С. 127-132.

187. Іванова М. І., Ткаченко А. М., Загорудько В. Л. Визначення рівня економічної безпеки, враховуючи конкурентоспроможність підприємства. *Підприємництво та інновації*. 2019. Вип. 10. С. 52-56.

188. Архипенко Т. А., Іванова М. І. Систематизація визначень поняття "економічна безпека підприємства". *Нобелівський вісник*. 2021. № 1. С. 6–14.

189. Архипенко Т., Іванова М. Оцінка економічної безпеки підприємства як підґрунтя прийняття ефективних управлінських рішень на засадах сталого розвитку. *Збірник наукових праць Черкаського державного технологічного університету. Серія : Економічні науки*. 2025. Т. 26, Вип. 1. С. 124-133.

190. Гуцалюк О. М. Роль інформаційно-аналітичних ресурсів у фінансовому забезпеченні технологій управління економічною безпекою банківських установ. *Держава та регіони. Серія : Економіка та підприємництво*. 2015. № 2. С. 9-12.

191. Гуцалюк О. М. Концептуальні засади забезпечення економічної безпеки корпоративних інтеграційних процесів. *Проблеми економіки*. 2016. № 3. С. 144-152.

192. Гуцалюк О. М., Бондар Ю. А., Коцюрба О. Ю., Пітел Н. С. Управління розвитком інноваційно-проєктної діяльності освітніх закладів в умовах взаємодії, конкурентоспроможності та забезпечення їх фінансово-економічної безпеки. *Вісник економічної науки України*. 2023. № 2. С. 90-96.

193. Шевченко А. М. Стратегічні орієнтири функціонування фінансової підсистеми механізму управління економічною безпекою підприємств. *Вісник ЧНУ ім. Б. Хмельницького. Серія «Економічні науки»*. 2025. Т. 29, № 1. С. 88-97.

194. Шевченко А. М., Чакалов Р. К. Формування механізму управління фінансово-економічною безпекою підприємства під час його стратегічного розвитку в умовах цифрових трансформацій. *Науковий погляд: економіка та управління*. 2025. № 2 (90). С. 145-150.

195. Шевченко А. М., Чакалов А. К. Фінансові та правові ризики для розвитку бізнесу в умовах цифровізації та роль механізму управління економічною безпекою підприємства у протидії їм. *Трансформаційна економіка*. 2025. № 2 (11). С. 128-133.

196. Носань Н. С., Куценко Д. М. Основи забезпечення фінансово-економічної безпеки на мікро- та макрорівнях: українські реалії. *Проблеми системного підходу в економіці*. 2019. Вип. 2(1). С. 51-56.

197. Чакалов А. К., Носань Н. С. Проблеми управління фінансово-економічною безпекою бізнесу під впливом війни: традиційні напрями досліджень і проєктний підхід. *Науковий погляд: економіка та управління*. 2023. № 1. С. 105-109.

198. Носань Н. С. Стратегічні орієнтири забезпечення фінансового складника економічної безпеки національної економіки в контексті слідування цілям сталого розвитку. *Бізнес-навігатор*. 2019. Вип. 3-1. С. 53-57.

199. Зачосова Н. В., Білоус С. П., Бичкова Д. О. Роль і значення ефективного механізму управління фінансово-економічною безпекою підприємств для їх стратегічного розвитку під впливом ризиків. *Актуальні питання економічних наук*. 2025. № 11. DOI: 10.5281/zenodo.15517465.

200. Назаренко С. А., Білоус С. П., Тітенко Н. В. Парадигмальні та концептуальні засади розвитку фінансового менеджменту у механізмі управління економічною безпекою підприємства. *Бізнес-навігатор*. 2025. Вип. 5 (82). С. 276-280. DOI: 10.32782/business-navigator.82-42.

201. Pavliuk E. Adaptation of strategic management of enterprises under the influence of digitalization to achieve a state of economic security. *Current Problems of Sustainable Development.* 2026. Vol. 3, № 1. P.83-90.

202. Navigate: Digital Risk Index 2025. URL: https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt5aac0415b1f186d8/navigate_digital_risk_index.pdf (дата звернення: 05.01.2026).

203. Share of enterprises using any business software (ERP, CRM or BI). *Eurostat.* URL: https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt5aac0415b1f186d8/navigate_digital_risk_index.pdf (дата звернення: 05.03.2026).

204. Ukraine. Digital Development Country Profile. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf (дата звернення: 05.03.2026).

205. Огляд ринку кібербезпеки в Україні. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 05.03.2026).

206. Digital 2026: Ukraine. URL: https://datareportal.com/reports/digital-2026-ukraine (дата звернення: 05.03.2026).

207. ENISA Threat Landscape 2024. *European Union Agency for Cybersecurity*. 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 21.03.2026).

208. Cost of a Data Breach Report 2024. *IBM Security*. 2024. URL: https://www.ibm.com/reports/data-breach (дата звернення: 21.03.2026).

209. Global Cybersecurity Outlook 2024. *World Economic Forum*. 2024. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2024 (дата звернення: 21.03.2026).

210. Q2 2024 - a brief overview of the main incidents in industrial cybersecurity. URL: https://ru.scribd.com/document/824779367/kaspersky-ics-cert-

q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-en (дата звернення: 21.03.2026).

211. Бурдига І. Атака на «Київстар»: історичний шатдаун та уроки з нього. URL: https://www.dw.com/uk/hakeri-proti-kiivstaru-istoricnij-obval-mobilnogo-zvazku-ta-uroki-z-nogo/a-67720041 (дата звернення: 21.03.2026).

212. Capita cyber incident: what happened and how we responded. *Capita PLC News*. 2023. URL: https://www.capita.com/about-us/responsible-business/cyber-incident-what-happened-and-how-we-responded (дата звернення: 21.03.2026).

213. MGM Resorts & Caesars cyberattack analysis. *IBM Security Intelligence*. 2023. URL: https://www.guycarp.com/content/dam/guycarp-rebrand/insights-images/2024/02/2024_2_Casino_Incident_Analysis_publish.pdf (дата звернення: 21.03.2026).

214. The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies. *arXiv.org Cornell University*. 2025. URL: https://arxiv.org/abs/2502.04303 (дата звернення: 21.03.2026).

215. Learning Lessons: British Library cyber incident report. *The British Library*. 2024. URL: https://www.bl.uk/stories/blogs/posts/learning-lessons-from-the-cyber-attack (дата звернення: 21.03.2026).

216. MOVEit Transfer and MOVEit Cloud Vulnerability. *Progress Software Security*. 2023. URL: https://digital.nhs.uk/cyber-alerts/2023/cc-4335 (дата звернення: 21.03.2026).

217. London Hospitals Face Major Disruptions After Cyberattack. *The New York Times*. 2024. URL: https://www.nytimes.com/2024/06/05/world/europe/london-hospitals-cyberattack.html (дата звернення: 21.03.2026).

218. Stryker hackers struck by FBI in domain seizure campaign. *ITPro Security*. 2024. URL: https://www.itpro.com/security/cyber-attacks/stryker-hackers-struck-by-fbi-in-domain-seizure-campaign (дата звернення: 21.03.2026).

219. Кошельок І. П., Малікова І. П. Методичні підходи до оцінки економічної безпеки підприємства. *Східна Європа: економіка, бізнес та управління*. 2021. Випуск 5 (32). С. 62-69.

220. Орлова А. А., Вишневська В. А., Бурлака В. В. Аналіз методичних підходів до оцінки економічної безпеки підприємства. *Ефективна економіка*. 2024. № 1. URL: http://nbuv.gov.ua/UJRN/efek_2024_1_64 (дата звернення: 21.03.2026).

221. Ткаченко Т. П., Гречко А. В. Узагальнення методичних підходів оцінювання економічної безпеки промислових підприємств. *Економічний вісник Національного технічного університету України "Київський політехнічний інститут"*. 2022. № 22. С. 79-82.

222. Богданюк І. В. Використання індикаторного підходу до оцінки економічної безпеки підприємств. *Економічний простір*. 2024. № 193. С. 81-86.

223. Хаванов А. В. Розробка та впровадження комплаєнс-індикаторів для оцінки рівня зрілості системи економічної безпеки підприємств. *Економічний простір*. 2025. № 201. С. 230-233.

224. Середа О. О. Оцінювання фінансової безпеки корпоративних підприємств в умовах цифрової економіки. *Часопис економічних реформ*. 2025. № 2. С. 105-112.

225. Кукоба А. В. Нефінансове оцінювання стану виробничої складової економічної безпеки підприємства. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2025. № 4(2). С. 58-62.

226. Мазіашвілі А. Р., Воловельська І. В., Кулеш В. Р. Оцінювання рівня системи економічної безпеки підприємства залізничного транспорту. *Наукові інновації та передові технології*. 2025. № 12. С. 3226-3237.

227. Вівчар О. І. Комплексне оцінювання стратегії зміцнення економічної безпеки підприємств мережевих структур України в умовах воєнного стану. *Економіка України*. 2023. № 12. С. 23-40.

228. Назаренко І. Л., Білоусова В. М. Адаптування комплексної методики визначення рівня економічної безпеки, оцінки ризиків та ймовірності банкрутства для малих підприємств. *Вісник економіки транспорту і промисловості*. 2023. № 83. С. 77-90.

229. Богданюк І. В., Мандич С. М. Багатофакторна модель оцінки ризиків та їх вплив на економічну безпеку підприємства. *Бізнес Інформ*. 2024. № 9. С. 148-153.

230. Сластяникова А., П'ятодверний М. Ризики в системі економічної безпеки підприємств: методи оцінювання. *Адаптивне управління: теорія і практика. Серія : Економіка*. 2024. Вип. 19. URL: http://nbuv.gov.ua/UJRN/admthp_2024_19_17 (дата звернення: 21.03.2026).

231. Ткаченко Т. Оцінювання ефективності системи економічної безпеки промислового підприємства в конкурентних умовах. *Проблеми і перспективи економіки та управління*. 2021. № 4. С. 163-169.

232. Копилюк О. І., Музичка О. М., Рутар Р. І. Комплексна оцінка рівня фінансово-економічної безпеки підприємства. *Інфраструктура ринку*. 2022. Вип. 63. С. 57-61.

233. Бабічев А. В., Самородов Б. В. Концептуальна модель оцінки й аналізу інформаційної компоненти економічної безпеки підприємства. *Проблеми економіки*. 2023. № 3. С. 157-167.

234. АТ «Укртелеком». URL: https://opendatabot.ua/c/21560766 (дата звернення: 15.03.2026).

235. АТ «Укрпошта». URL: https://opendatabot.ua/c/21560045 (дата звернення: 15.03.2026).

236. АТ «Укрзалізниця». URL: https://opendatabot.ua/c/40075815 (дата звернення: 15.03.2026).

237. ПрАТ «Київстар». URL: https://opendatabot.ua/c/21673832 (дата звернення: 15.03.2026).

238. НЕК «Укренерго». URL: https://opendatabot.ua/c/00100227 (дата звернення: 15.03.2026).

239. КПТМ «Черкаситеплокомуненерго». URL: https://opendatabot.ua/c/02082522 (дата звернення: 15.03.2026).

240. АТ «Черкасиобленерго». URL: https://opendatabot.ua/c/22800735 (дата звернення: 15.03.2026).

241. КП «Черкасиводоканал». URL: https://opendatabot.ua/c/03357168 (дата звернення: 15.03.2026).

242. ПрАТ «Черкаське хімволокно». (ДП «Черкаська ТЕЦ»). URL: https://opendatabot.ua/c/00204033 (дата звернення: 15.03.2026).

243. АТ «Черкаський автобус». URL: https://opendatabot.ua/c/05390419 (дата звернення: 15.03.2026).

244. Криворучко О. М., Шморгун О. А. Розроблення стратегій управління персоналом в умовах цифровізації. *Вісник економіки транспорту і промисловості*. 2025. № 90. С. 37-45.

245. Криворучко О. М., Фемяк О. А. Концептуальні аспекти стратегічного управління персоналом підприємства в умовах цифровізації. *Економіка транспортного комплексу*. 2024. Вип. 44. С. 111-131.

246. Квасницька Р. С., Скоробогата Л. В., Кульгук І. І. Інноваційні стратегії управління ринковою цінністю підприємств за умов цифровізації системи адміністрування в період дії військового стану. *Випробування та сертифікація*. 2024. № 4. С. 113-120.

247. Коритько Т. Ю. Механізм управління та формування стратегії адаптації підприємств в умовах цифровізації економіки. *Економічний вісник Донбасу*. 2025. № 1. С. 56-62.

248. Лігоненко Л. О. Вплив цифровізації на систему управління результативністю підприємств та формування стратегії їх діяльності. *Економічний простір*. 2025. № 199. С. 220-227.

249. Логінова О. Стратегічне управління підприємством в умовах цифрової економіки. *Наука. Освіта. Молодь*. 2024. № 17. С. 125-127.

250. Паламарчук О. М., Яременко Л. М., Скрипник Р. Є. Цифровізація бізнесу: нові можливості для стратегічного управління підприємствами в умовах економічної нестабільності. *Формування ринкових відносин в Україні*. 2025. № 1. С. 90-96.

251. Сазонова С. В., Новиков Д. М., Макаренко Т. Оцінка конкурентоспроможності підприємства на принципах стратегічного управління

в умовах цифрової економіки. *Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент*. 2024. Вип. 59. С. 114-121.

252. Шиманович П. О., Крілик Б. Б., Якубець М. Р., Волос М. В., Романинець О. В., Цісінський М. М. Стратегічне управління розвитком підприємств в умовах цифровізації економіки. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2023. № 12(1). С. 174-182.

253. Кирилюк І., Ломако Є., Черняк В. Стратегічний розвиток сільськогосподарського підприємства. *Економіка та суспільство*. 2025. № 79. URL: https://doi.org/10.32782/2524-0072/2025-79-192 (дата звернення: 01.02.2026).

254. Кирилюк І. М., Ільченко І. О. Теоретичні засади управління цифровізацією бізнес-процесів на підприємствах. *Здобутки економіки: перспективи та інновації*. 2025. № 23. URL: https://doi.org/10.5281/zenodo.17347525 (дата звернення: 01.02.2026).

255. Кирилюк І. М., Денисенко В. О., Ільченко І. О. Концептуальні підходи до формування системи управління цифровою трансформацією бізнес-процесів. *Актуальні питання економічних наук*. 2025. № 16. URL: https://doi.org/10.5281/zenodo.17456607 (дата звернення: 01.02.2026).

256. Денисенко В. О., Кирилюк І. М., Калач В. М. Управління цифровою трансформацією підприємства як фактор конкурентоспроможності. *Успіхи і досягнення у науці*. 2025. № 6 (16). С. 750-759.

257. Гнидюк В. С., Кирилюк І. М., Огіренко А. О. Значення «data-driven» підходу в маркетинговій діяльності та його потенціал в стратегії управління інноваційно орієнтованих аграрних підприємств. *Актуальні проблеми економіки*. 2025. № 5 (287). С. 16-31.

258. Zachosova N., Koval O. Strategic management in ensuring economic security in the digital economy and the VUCA World. *MEST Journal*. 2022. № 7/1. P. 217-224.

259.Павлюк Є. С. Адаптація стратегії управління підприємством до ризиків економічній безпеці як засіб узгодження інтересів його стейкхолдерів.

Актуальні проблеми економіки, обліку, управління і права в сучасних умовах: збірник тез доповідей міжнародної науково-практичної конференції (м. Рівне, 8 січня 2026 р.). Рівне: ЦФЕНД, 2026. С.95-98.

260.Щепка О. В., Сало С. О., Григір С. І. Напрямки підвищення рівня економічної безпеки підприємств під впливом цифровізації та адаптивного управління. *Економічний вісник Донбасу*. 2024. № 1-2. С. 98-102.

261.Поліщук О. Б. Адаптаційний потенціал як основа формування адаптивно-орієнтованої системи управління економічною безпекою підприємства. *Інфраструктура ринку*. 2022. Вип. 63. С. 82-87.

262.Василега В. Адаптивна стратегія забезпечення економічної безпеки підприємства. *Адаптивне управління: теорія і практика. Серія : Економіка*. 2024. Вип. 19. URL: http://nbuv.gov.ua/UJRN/admthp_2024_19_23 (дата звернення: 03.01.2026).

263. Бедрій Д. І. Метод інтегрованого протиризикового управління стейкхолдерами наукових проєктів в умовах невизначеності та поведінкової економіки. *Управління розвитком складних систем*. 2021. Вип. 45. С. 13-20.

264. Бєлобородова М. В., Олійник Т. І. Роль стейкхолдерів в управлінні якістю діяльності організації (на прикладі закладу охорони здоров'я). *Вісник ХНАУ. Серія : Економічні науки*. 2020. № 2. С. 124-139.

265. Власенко Т., Котельникова Ю., Городецька Т., Помогалова Н. Залучення стейкхолдерів для успішного управління проєктом. *Modeling the development of the economic systems*. 2023. № 3. С. 8-13.

266. Давидов О. І. Формування стратегії управління фундаментально-стейкхолдерською доданою вартістю підприємств. *Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки*. 2024. № 5(2). С. 151-159.

267. Кавецький В. В. Інвестиції промислових підприємств на засадах стейкхолдерської теорії: сутність, класифікації, підходи до управління ефективністю інвестицій. *Вісник Хмельницького національного університету. Економічні науки*. 2019. № 6(1). С. 78-83.

268. Казіміров М. А. Теоретичні засади управління ризиками неплатоспроможності банків з урахуванням інтересів різних груп стейкхолдерів. *Економічний простір*. 2024. № 189. С. 129-136.

269. Коваленко В., Сергєєва О., Іванова Т. Корпоративна соціальна відповідальність у забезпеченні ефективної системи управління взаємовідносинами банків зі стейкхолдерами. *Фінансово-кредитні системи: перспективи розвитку*. 2022. Вип. 1. С. 70-81.

270. Петренко В. С. Сучасне розуміння стейкхолдерської моделі управління конкурентоспроможністю ІТ-підприємства. *Ефективна економіка*. 2025. № 2. URL: http://nbuv.gov.ua/UJRN/efek_2025_2_10 (дата звернення: 02.03.2026).

271. Федичишин А. С., Ніронов Д. А. Маркетингове управління відносинами зі стейкхолдерами. *Ефективна економіка*. 2024. № 7. URL: http://nbuv.gov.ua/UJRN/efek_2024_7_100 (дата звернення: 02.03.2026).

272. Шкромида В. В., Максимів Ю. В., Гнатюк Т. М. Цифрова інтеграція фінансової та управлінської звітності в інтересах стейкхолдерів. *Актуальні проблеми розвитку економіки регіону*. 2025. Вип. 21(1). С. 359-368.

273. Кильницька Є. В., Сергієнко Ю. І. Теоретико-методичні аспекти організації управління підприємством з позиції взаємодії зі стейкхолдерами. *Бізнес Інформ*. 2021. № 3. С. 188-194.

274. Роїк О. Р. Оцінка ризиків при побудові стейкхолдерної моделі стратегічного управління туристичним бізнесом. *Причорноморські економічні студії*. 2022. Вип. 76. С. 272-278.

275. Залуцька Х. Я., Гнат І. А., Стефанцов Д. В. Процес стратегічного управління підприємством з урахуванням особливостей його взаємодії зі стейкхолдерами. *Бізнес Інформ*. 2023. № 6. С. 209-215.

276. Портна О. В., Цвар О. О. Стратегічні зміни в управлінні персоналом: світовий досвід застосування стейкхолдерно-орієнтованих підходів. *Бізнес Інформ*. 2020. № 9. С. 284-290.

277. Нор В. В. Роль інформаційної прозорості в управлінні економічною безпекою підприємств: стейкхолдер-орієнтований підхід. *Економічний вісник Національного технічного університету України "Київський політехнічний інститут"*. 2024. № 31. С. 45-50.

278. Галахов Є. М., Барабаш О. В. Стратегічні пріоритети системи інформаційної безпеки підприємства, що залучає фріланс-ресурс. *Сучасний захист інформації*. 2019. № 3. С. 30-35.

279. Нехай В., Нехай В. Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою сільськогосподарських підприємств на основі стратегії Cyber Situation Awareness. *Проблеми і перспективи економіки та управління*. 2020. № 1. С. 238-247.

280. Храпкін О. Стратегічне управління інформаційною безпекою підприємства: сучасні підходи та виклики. *Проблеми і перспективи економіки та управління*. 2023. № 4. С. 86-94.

281. Чубаєвський В. І. Стратегічні орієнтири формування корпоративної політики інформаційної безпеки. *Причорноморські економічні студії*. 2021. Вип. 72(2). С. 24-30.

282. Дімітров О. Ю. Генеза поняття «цифрова грамотність» у зарубіжній науковій думці. *Перспективи та інновації науки (Серія «Педагогіка», Серія «Психологія», Серія «Медицина»)*. 2025. № 9. С. 410-423.

283. Антонова С. Є., Сидор Н. А., Юхимець Н. С. Окремі аспекти цифрової грамотності українців. *Державне управління: удосконалення та розвиток*. 2023. № 5. URL: http://nbuv.gov.ua/UJRN/Duur_2023_5_14 (дата звернення: 11.02.2026).

284. Струтинська І. Цифрова грамотність людського капіталу бізнес-структур. *Економічний часопис Східноєвропейського національного університету імені Лесі Українки*. 2019. № 4. С. 93-100.

285. Сухомлин О. Формування системи мотивації підвищення цифрової грамотності для навчання протягом життя. *Молодь і ринок*. 2021. № 7-8. С. 141-145.

286. Царук Н. Г. Чинники розвитку та складники цифрової грамотності бухгалтера. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2021. Вип. 35. С. 69-73.

287. Зварич Р., Дудник Ю., Гомотюк В., Боднар С. Ризик-менеджмент цифрової трансформації в умовах пандемії. *Вісник економіки*. 2022. Вип. 1. С. 38-53.

288. Черелюк В. О. Організаційне забезпечення ризик-менеджменту в умовах цифровізації. *Вісник економіки транспорту і промисловості*. 2024. № 88. С. 110-118.

289. Наторіна А. О. Синкретичність менеджменту цифрових ризиків та інформаційної безпеки. *Економіка, управління та адміністрування*. 2019. № 3. С. 30-34.

290. Семенова К. Д., Тарасова К. І. Становлення нового цифрового світу та проблеми менеджменту кібер-ризиків. *Маркетинг і менеджмент інновацій*. 2017. № 3. С. 236-244.

291. Кудлай В. О. Цифрова грамотність особистості в контексті розвитку інформаційного суспільства. *Вісник Маріупольського державного університету. Серія : Філософія, культурологія, соціологія*. 2015. Вип. 10. С. 97-104.

292. Шостя С. П. Філософія освітніх проектів формування цифрової грамотності. *Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія*. 2017. Вип. 48(1). С. 189-200.

293. Гаврілова Л. Г., Топольник Я. В. Цифрова культура, цифрова грамотність, цифрова компетентність як сучасні освітні феномени. *Інформаційні технології і засоби навчання*. 2017. Т. 61, вип. 5. С. 1-14.

294. Сегол Р. І. Підвищення цифрової грамотності майбутніх фахівців із видавничої справи та редагування: досвід створення та впровадження масового відкритого онлайн-курсу. *Обрії друкарства*. 2018. № 1. С. 170-180.

295. Бречко О. Фінансова і цифрова грамотність, як базові складові розвитку сучасного інформаційного суспільства. *Регіональні аспекти розвитку продуктивних сил України*. 2019. Вип. 24. С. 129-135.

296. Струтинська І. Цифрова грамотність людського капіталу бізнес-структур. *Економічний часопис Східноєвропейського національного університету імені Лесі Українки*. 2019. № 4. С. 93-100.

297. Кулинич М., Шворак А., Жиленко Л. Впровадження цифрової грамотності в умовах майбутніх змін професії бухгалтера. *Економічний часопис Східноєвропейського національного університету імені Лесі Українки*. 2020. № 1. С. 216-224.

298. Карпова О. Теоретичний аналіз проблеми розвитку цифрової грамотності в молоді в умовах безперервного навчання. *Актуальні питання гуманітарних наук*. 2022. Вип. 47(2). С. 256-261.

299. Ільїна А., Дяк Т., Левченко О. Феномен візуальної грамотності цифрової доби: методологічний аспект. *Педагогічні інновації: ідеї, реалії, перспективи*. 2022. Вип. 2. С. 36-42.

300. Дмитренко Т. Л., Терещенко Г. М. Підвищення рівня освіти у сфері кібербезпеки, фінансової та цифрової грамотності як чинник зниження ризиків на крипторинку. *Освітня аналітика України*. 2023. Вип. 1. С. 38-50.

ДОДАТКИ

Додаток А

Довідки про впровадження результатів дослідження

УКРАЇНА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені БОГДАНА ХМЕЛЬНИЦЬКОГО
бульвар Шевченка, 81, м. Черкаси, 18031
тел./факс: (0472) 354463, 372142
e-mail: cic@cdu.edu.ua

UKRAINE
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
BOHDAN KHMELNYTSKY NATIONAL UNIVERSITY of CHERKASY
81, Shevchenko blvd., Cherkasy, Ukraine, 18031
Phone/Fax: +380(472)354463, 372142
e-mail: cic@cdu.edu.ua

25.03.2026 № 79/04

на № _____

Довідка
про впровадження результатів дослідження
Павлюка Євгенія Станіславовича
«Адаптація стратегічного управління підприємством для протидії цифровим ризикам економічній безпеці»,
поданого на здобуття ступеня доктора філософії
зі спеціальності 073 – Менеджмент

Упродовж 2022-2025 років на базі Черкаського національного університету імені Богдана Хмельницького було проведено наукове дослідження, яке стосувалось теоретико-методичних і прикладних аспектів стратегічного управління підприємством для протидії цифровим ризикам його економічній безпеці, і набуло завершеного вигляду у формі дисертаційної роботи на тему: «Адаптація стратегічного управління підприємством для протидії цифровим ризикам економічній безпеці».

Теоретичні результати дослідження використано під час викладання фахових дисциплін, які є обов'язковими у професійній підготовці майбутніх бакалаврів і магістрів менеджменту, таких як: «Стратегічний менеджмент», «Стратегічне та інноваційне управління розвитком організації», «Проєктний менеджмент».

Предметом впровадження наукового дослідження Павлюка Є.С. стало розв'язання наукового завдання, яке полягало в доповненні, розширенні та оновленні науково-методичних засад і практичних підходів до адаптивної модифікації системи стратегічного управління підприємством у напрямі спрямування її ресурсів і потенціалу на забезпечення його економічної безпеки в умовах інтенсифікації цифрових ризиків зовнішнього та внутрішнього середовищ. З цією метою було узагальнено та уточнено концептуальні засади адаптації стратегічного управління підприємствами під впливом цифровізації, запропоновано напрями оновлення механізму стратегічного управління економічною безпекою підприємства із дотриманням балансу інтересів стейкхолдерів і досліджено можливості інтеграції принципів цифрового ризик-менеджменту у стратегії безпеко орієнтованого економічного розвитку підприємств в Україні.

Результати дослідження Павлюка Є.С. обговорені на засіданні кафедри менеджменту та державної служби Черкаського національного університету імені Богдана Хмельницького (протокол № 7 від 03.03.2026 р.), отримали високу оцінку та рекомендовані до подальшого впровадження.

Відповідальний за впровадження – Павлюк Є.С.

Проректор з наукової, інноваційної та міжнародної діяльності Олександр СПРЯГАЙЛО

№ 1054 від 02.04.2026 р.

ДОВІДКА
про впровадження результатів дослідження
Павлюка Євгенія Станіславовича
на тему
«Адаптація стратегічного управління підприємством для протидії цифровим ризикам економічній безпеці»,
що подається на здобуття наукового ступеня доктора філософії
зі спеціальності 073 «Менеджмент»

У реаліях воєнного часу керівництво підприємства часто стикалося з проблемою неможливості ефективного прогнозування та якісного форсайту розвитку майбутніх подій у його фінансово-господарській діяльності, що суттєво ускладнювало планування майбутніх показників, KPI, OKR, а також розробку стратегії управління бізнесом і в цілому досягнення його довгострокових цілей та забезпечення високого рівня економічної безпеки. Завдяки дослідженню Павлюка Є.С. було переглянуто алгоритми стратеготворення, сформовано підхід щодо використання можливостей командної роботи під час встановлення стратегічних орієнтирів для масштабування впливу підприємства на ринку, а також внесено зміни до алгоритмів безпеки орієнтованої поведінки працівників, у тому числі у цифровому просторі. Особливо варто підкреслити інформаційну цінність проведеного дослідження у контексті розроблення win-win стратегій для підприємства у площинах взаємодії з постачальниками, клієнтами контрагентами та органами державної влади.

З огляду на наведені факти, дослідження Павлюка Євгенія Станіславовича має практичну цінність, і може вважатись успішно апробованим на прикладному рівні. Формалізовані автором рекомендації є такими, що мають потенціал широкого використання суб'єктам підприємницької діяльності у сучасних реаліях ведення бізнесу в Україні.

Директор ПП «Мак Тревел» Л.М. Шмітько

ТОВ «АВІА-СЕРВІС»
18029, м. Черкаси, вул. Сумгаїтська, 7, ідентифікаційний код 30921031

№ 287 від 03.04.2026 р.

Довідка
про впровадження результатів дослідження
Павлюка Євгенія Станіславовича
на тему
«Адаптація стратегічного управління підприємством для протидії цифровим ризикам економічній безпеці»,
поданого на здобуття ступеня доктора філософії
зі спеціальності 073 «Менеджмент»

Керівництвом підприємства враховані пропозиції Павлюка Євгенія Станіславовича під час формування стратегії стабілізації діяльності підприємства та його подальшого сталого розвитку в частині протидії традиційним та інноваційним ризикам, зокрема тим, які формуються у цифровому просторі ведення сучасного бізнесу.

У матеріалах проведеного дослідження, що стосується різних аспектів, проблем і особливостей стратегічного менеджменту в умовах невизначеності, менеджмент компанії віднайшов для себе дієві підказки щодо покращення стару організації роботи працівників в умовах стрімкої діджиталізації його бізнес-процесів. До прикладу, було ініційовано заходи щодо оцінювання та підвищення рівня цифрової грамотності управлінського персоналу, а також проведено інформаційну роботу у напрямку важливості започаткування резильєнтних сценаріїв реагування топ-менеджменту підприємства на форс-мажорні виклики для стану його економічної безпеки. Дисертація Павлюка Є.С. дає розуміння того, наскільки важливим елементом довгострокового успіху підприємницької діяльності є рівень захищеності бізнесу від економічних загроз і їх негативних фінансових, репутаційних, іміджевих наслідків. Тому керівництвом підприємства заплановано розшити межі використання безпеко орієнтованих заходів у структурі генерального менеджменту, зокрема, планується розробити стратегію економічної безпеки на найближчі п'ять років.

Директор ТОВ «Авіа-Сервіс» Олександр АРТЕМЕНКО

Товариство з обмеженою відповідальністю «Авіа-Сервіс» 30921031 Україна м.Запоріжжя

№ 52 від 27.03.2026 р.

ДОВІДКА

про впровадження результатів дослідження

Євгенія Станіславовича

на тему: «Адаптація стратегічного управління підприємством для протидії цифровим ризикам економічній безпеці»,

що подається на здобуття наукового ступеня доктора філософії

зі спеціальності 073 «Менеджмент»

У дослідженні Павлюка Євгенія Станіславовича представлено інформаційний матеріал, отриманий у результаті ґрунтовного аналізу стратегічних позиції і конкретизації стратегічних орієнтирів діяльності українських підприємств. Опрацьовані автором відомості, його критичний аналіз сильних, слабких сторін, ризиків і можливостей, уточнених для українських компаній, дозволили сформувати для підприємства карти актуальних ризиків, встановити стратегічні цілі з використанням технології Smart та суттєво підвищити якість процесу стратегічного планування фінансово-господарської діяльності на перспективу. Водночас, особливо цінними на прикладному рівні виявилися пропозиції щодо підвищення рівня економічної безпеки підприємства за допомогою мультисценарного планування ключових індикаторів його розвитку. Таким чином, матеріали дисертаційного дослідження Євгенія Станіславовича послугували інформаційним підґрунтям для покращення якості стратегічного управління суб'єктом господарювання і отримали впровадження у його практичній діяльності.

Директор ТОВ «Техвантаж-Сервіс» В.М. Ляш

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ ТЕХВАНТАЖ-СЕРВІС Ідентифікаційний код 36819017 УКРАЇНА м. ЧЕРКАСИ

Додаток Б

Список публікацій здобувача

Публікації у наукових фахових виданнях України:

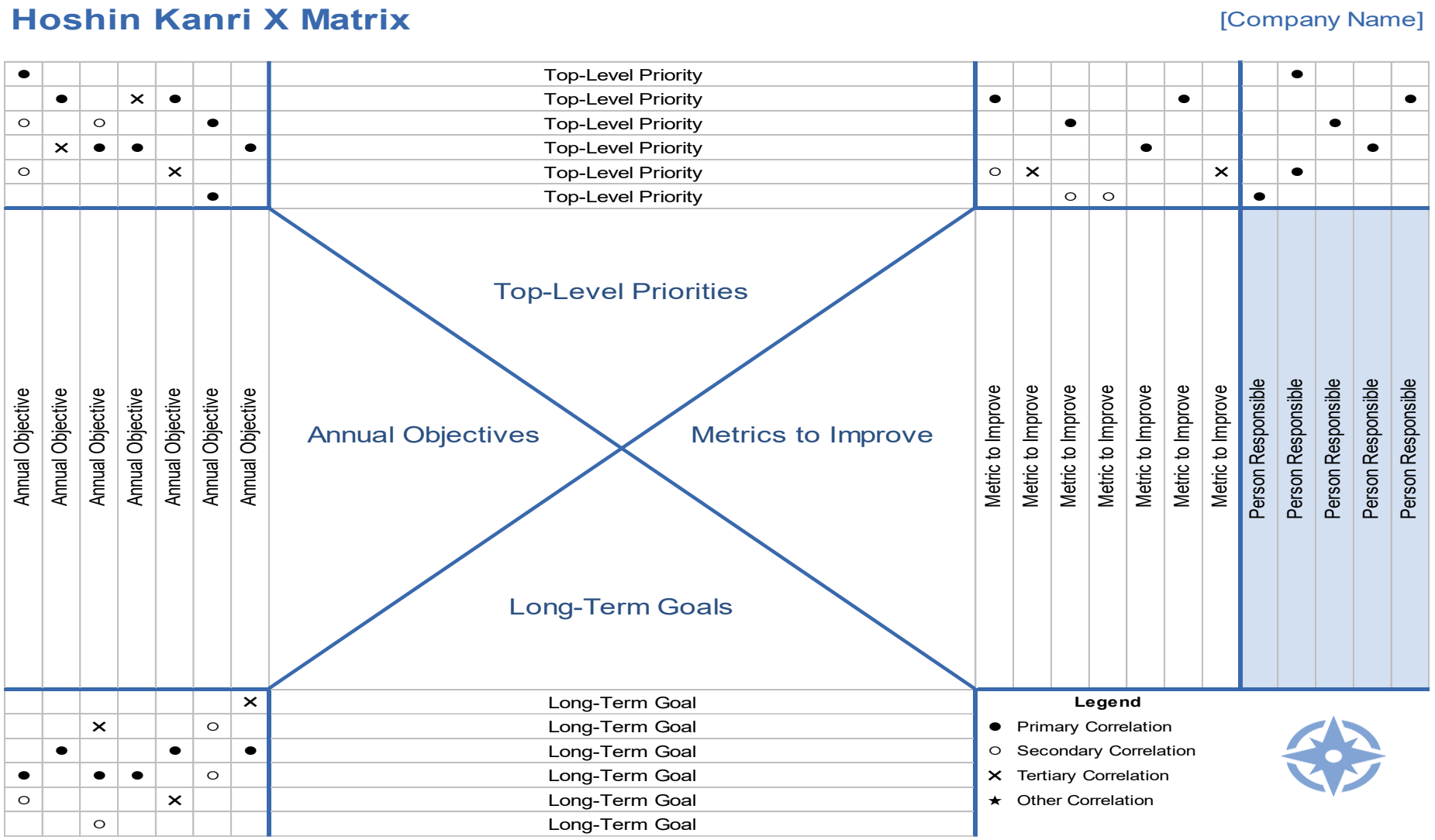
1. Шарий В.І., Павлюк Є. С. Логічний аналіз стратегічного управління в організації. *Економіка та суспільство*. 2024. №70. URL: https://economyandsociety.in.ua/index.php/journal/article/view/5342/5285 (дата звернення: 02.04.2026) https://doi.org/10.32782/2524-0072/2024-70-85.
2. Павлюк Є.С. Сучасні підходи до стратегічного управління підприємствами: зміни парадигм під впливом пермакризи та ризиків світу BANI. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут».* 2025. № 35. С.162-167. https://doi.org/10.20535/2307-5651.35.2025.352397.
3. Павлюк Є.С. Оцінка впливу цифрових ризиків на стан економічної безпеки підприємства як елемент обґрунтування досяжності його стратегічних цілей. *Науково-виробничий журнал «Бізнес-навігатор».* 2026. Випуск 1 (84). С.9-14. https://doi.org/10.32782/business-navigator.84-2.
4. Pavliuk E. Adaptation of strategic management of enterprises under the influence of digitalization to achieve a state of economic security. *Current Problems of Sustainable Development.* 2026. Vol. 3, № 1. P.83-90. https://doi.org/10.60022/3(1)-11S.

Матеріали наукових конференцій та інші видання:

1. Pavliuk E. The place of risk management in strategies for ensuring the economic security of enterprises. *Сучасний стан та тенденції розвитку науки та освіти* : матеріали III Міжнародної науково-практичної конференції / Міжнародний гуманітарний дослідницький центр (м. Дніпро, 5 січня 2026 р.). Research Europe, 2026. С.177-181. https://doi.org/10.64076/ihrc260105.
2. Павлюк Є. С. Адаптація стратегії управління підприємством до ризиків економічній безпеці як засіб узгодження інтересів його стейкхолдерів. *Актуальні проблеми економіки, обліку, управління і права в сучасних умовах*: збірник тез доповідей міжнародної науково-практичної конференції (м. Рівне, 8 січня 2026 р.). Рівне: ЦФЕНД, 2026. С.95-98.
3. Pavliuk E. Current state of development of scientific theories of strategic management of enterprises under the influence of digitalization. *Пріоритетні напрями досліджень в науковій та освітній діяльності*: матеріали XVII Міжнародної науково-практичної конференції. м. Львів, 9-10 січня 2026 року. Львів: Львівський науковий форум, 2026. С.6-10.
4. Павлюк Є.С. Методичні підходи до розробки стратегій для сучасних підприємств: зарубіжний досвід для вітчизняних управлінців. Сучасні наукові підходи до вирішення глобальних криз: роль інтеграції наук і технологій у змінах суспільства: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 13 лютого 2026 р.). Кременчук: ЦФЕНД, 2026. С.28-31.

Додаток В

Зразок Х-матриці для методу Hoshin Kanri



Джерело: [156]

Додаток Д

Таблиця Д.1. - Показники для оцінювання стану економічної безпеки АТ «Укртелеком»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	12934	10539	8112	6701	6182
Середня заробітна плата, грн	12494	12230	14851	19033	23100
Дохід на одного працівника, грн	408217	416934	513379	648180	672982
Динаміка доходу, %	-3,1	-16,78	-5,22	4,3	-4,22
Розмір чистого прибутку, тис. грн	1637165	-2992741	156376	389467	1194856
Рентабельність діяльності, %	31,01	-68,11	3,75	8,97	28,72
Розмір активів, тис. грн	16220898	12930434	12629530	13024296	13808234
Розмір зобов'язань, тис. грн.	1417017	1935628	1810868	1819269	1544009
Розмір чистих активів, тис. грн	14803881	10994806	10818662	11205027	12264225
Коефіцієнт автономії, %	91,26	85,03	85,66	86,03	88,82

Джерело: складено автором за даними [234]

Таблиця Д.2. - Показники для оцінювання стану економічної безпеки АТ «Укрпошта»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	62373	53432	34751	31739	31739
Середня заробітна плата, грн	8272	8530	14327	16743	16745
Дохід на одного працівника, грн	178699	193207	333260	408898	413322
Динаміка доходу, %	21,38	-7,38	12,18	12,06	1,08
Розмір чистого прибутку, тис. грн	162039	-1258089	-796361	-413204	1997285
Рентабельність діяльності, %	1,45	-12,19	-6,88	-3,18	15,23
Розмір активів, тис. грн	10996285	9418683	11502953	11538899	26496304
Розмір зобов'язань, тис. грн.	7194286	6869557	9633204	9952662	21348400
Розмір чистих активів, тис. грн	3801999	2549126	1869749	1586237	5147904
Коефіцієнт автономії, %	34,58	27,06	16,25	13,75	19,43

Джерело: складено автором за даними [235]

Таблиця Д.3. - Показники для оцінювання стану економічної безпеки АТ «Укрзалізниця»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	232837	210742	187620	178616	169952
Середня заробітна плата, грн	13298	13144	16521	19696	21324
Дохід на одного працівника, грн	363663	356050	493645	575933	523558
Динаміка доходу, %	13,71	-11,38	23,43	11,07	-13,5
Розмір чистого прибутку, тис. грн	154185	-8730774	4836962	-4188474	-7789332
Рентабельність діяльності, %	0,18	-11,64	5,22	-4,07	-8,75
Розмір активів, тис. грн	259373276	249569123	272360686	279038815	298892591
Розмір зобов’язань, тис. грн.	23214004	13326474	17324539	18429726	51733007
Розмір чистих активів, тис. грн	236159272	236242649	255036147	260609089	247159584
Коефіцієнт автономії, %	91,05	94,66	93,64	93,40	82,69

Джерело: складено автором за даними [236]

Таблиця Д.4. - Показники для оцінювання стану економічної безпеки ПрАТ «Київстар»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	3804	3659	3261	3296	3475
Середня заробітна плата, грн	44268	63938	47240	54407	65417
Дохід на одного працівника, грн	7507663	8445196	10170208	11116306	12605826
Динаміка доходу, %	14,23	8,2	7,33	10,48	19,56
Розмір чистого прибутку, тис. грн	11431825	9516514	10542590	11331462	12307536
Рентабельність діяльності, %	40,03	30,8	31,79	30,93	28,1
Розмір активів, тис. грн	29794175	40375619	50396195	66444188	84939977
Розмір зобов’язань, тис. грн.	6490592	10368602	9521642	12703603	15097087
Розмір чистих активів, тис. грн	23303583	30007017	40874553	53740585	69842890
Коефіцієнт автономії, %	78,22	74,32	81,11	80,88	82,23

Джерело: складено автором за даними [237]

Таблиця Д.5. - Показники для оцінювання стану економічної безпеки НЕК «Укренерго»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	7964	7729	7480	7534	7476
Середня заробітна плата, грн	31770	34141	36354	44556	50860
Дохід на одного працівника, грн	8926293	10652153	11096409	13422195	14409457
Динаміка доходу, %	22,04	15,81	0,81	21,83	6,53
Розмір чистого прибутку, тис. грн	163162	7389474	45181422	-38882968	-4597924
Рентабельність діяльності, %	0,23	-8,98	54,43	-38,45	-4,27
Розмір активів, тис. грн	92632682	99044597	176903615	173792136	179228936
Розмір зобов’язань, тис. грн.	39673600	59864489	70816851	143330671	150422970
Розмір чистих активів, тис. грн	52959082	39180108	106086764	30461465	28805966
Коефіцієнт автономії, %	57,17	39,56	59,97	17,53	16,07

Джерело: складено автором за даними [238]

Таблиця Д.6. - Показники для оцінювання стану економічної безпеки КПТМ «Черкаситеплокомуненерго»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	672	656	665	650	668
Середня заробітна плата, грн	15900	17456	18959	21789	23875
Дохід на одного працівника, грн	11234557	1144869	1035579	1186468	1283750
Динаміка доходу, %	10,3	-7,2	-8,3	11,99	11,2
Розмір чистого прибутку, тис. грн	18706	111341	10563	-106545	-65019
Рентабельність діяльності, %	4,77	14,83	1,53	-13,82%	-7,58
Розмір активів, тис. грн	586957	1138092	1166816	1454175	2210509
Розмір зобов’язань, тис. грн.	492042	587660	566403	881941	1683450
Розмір чистих активів, тис. грн	94915	550432	600413	572234	527059
Коефіцієнт автономії, %	16,17	48,36	51,46	39,35	23,84

Джерело: складено автором за даними [239]

Таблиця Д.7. - Показники для оцінювання стану економічної безпеки АТ «Черкасиобленерго»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	3926	3802	3660	3494	3281
Середня заробітна плата, грн	15774	15890	17103	21656	27601
Дохід на одного працівника, грн	540491	558436	814953	1099148	1327953
Динаміка доходу, %	25,73	0,06	40,48	28,76	13,45
Розмір чистого прибутку, тис. грн	13519	5521	4734	-119464	1497822
Рентабельність діяльності, %	0,64	0,26	0,16	-3,11	34,38
Розмір активів, тис. грн	7465609	7324021	7370531	7756205	7922437
Розмір зобов’язань, тис. грн.	2854607	3249889	4066250	5038214	3732705
Розмір чистих активів, тис. грн	4611002	4074132	3304281	2717991	4189732
Коефіцієнт автономії, %	61,76	55,63	44,83	35,04	52,88

Джерело: складено автором за даними [240]

Таблиця Д.8. - Показники для оцінювання стану економічної безпеки КП «Черкасиводоканал»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	659	645	635	619	609
Середня заробітна плата, грн	15344	16333	17734	20193	21439
Дохід на одного працівника, грн	558979	610490	640762	742519	862330
Динаміка доходу, %	27,26	6,09	3,33	12,96	14,26
Розмір чистого прибутку, тис. грн	93485	-87098	24561	-16164	62290
Рентабельність діяльності, %	25,38	-22,12	6,04	-3,52	11,86
Розмір активів, тис. грн	635261	676756	725523	779480	877145
Розмір зобов’язань, тис. грн.	108376	168726	216770	277222	191655
Розмір чистих активів, тис. грн	526885	508030	508753	502258	685490
Коефіцієнт автономії, %	82,94	75,07	70,12	64,44	78,15

Джерело: складено автором за даними [241]

Таблиця Д.9 - Показники для оцінювання стану економічної безпеки ПрАТ «Черкаське хімволокно» (ДП «Черкаська ТЕЦ»)

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	723	726	700	707	752
Середня заробітна плата, грн	16099	16226	18590	23496	30664
Дохід на одного працівника, грн	2109048	2383036	3531337	5835918	7547025
Динаміка доходу, %	5,76	13,46	42,82	66,91	37,55
Розмір чистого прибутку, тис. грн	-109990	-876423	-339903	688691	1070367
Рентабельність діяльності, %	7,21	-50,66	-13,75	16,69	18,86
Розмір активів, тис. грн	1021805	1464504	1362333	3383961	4400408
Розмір зобов’язань, тис. грн.	913170	1720392	1823968	2935425	2913888
Розмір чистих активів, тис. грн	108635	-255888	-461635	448536	1486520
Коефіцієнт автономії, %	10,63	-17,47	-33,89	13,25	33,78

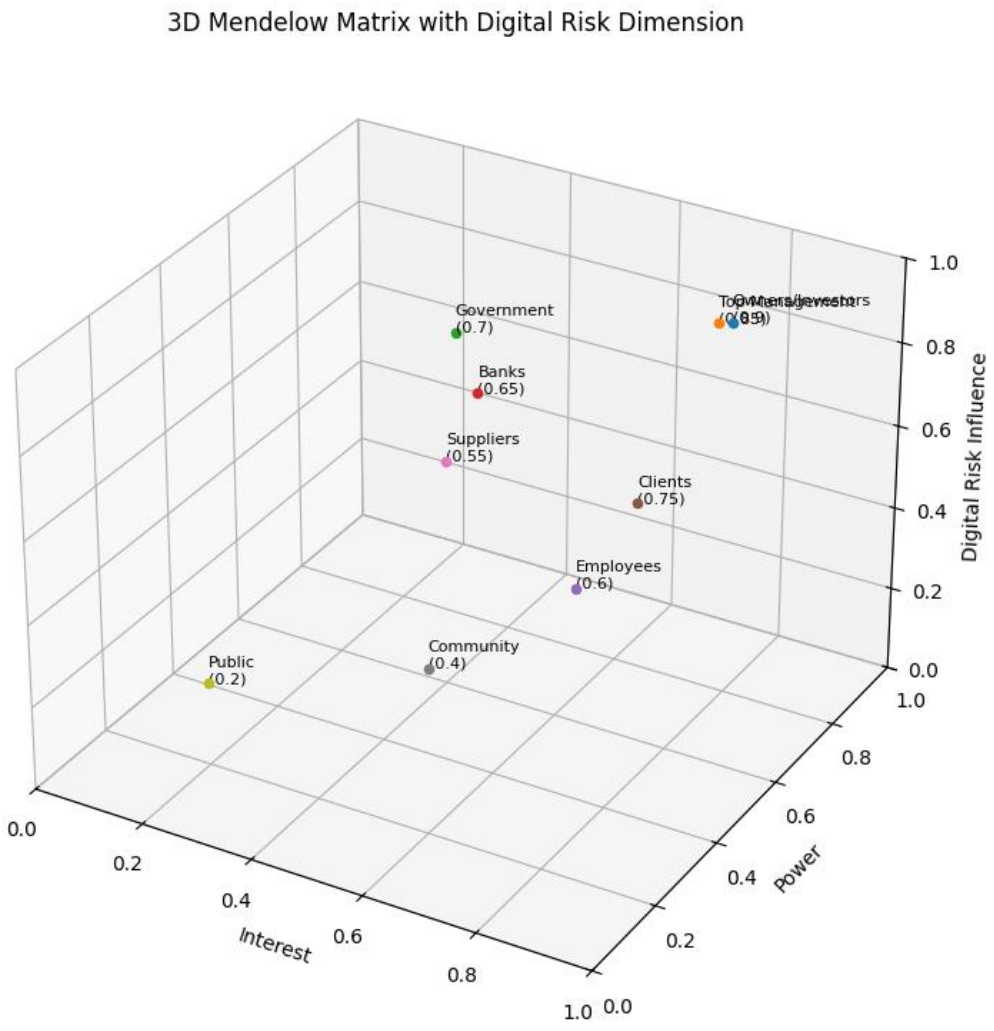
Джерело: складено автором за даними [242]

Таблиця Д.10. - Показники для оцінювання стану економічної безпеки АТ «Черкаський автобус»

Показники	2021	2022	2023	2024	2025
Кількість персоналу, осіб	403	403	412	412	379
Середня заробітна плата, грн	13740	14404	24046	26753	35838
Дохід на одного працівника, грн	1577340	2090057	4188786	4298590	4571807
Динаміка доходу, %	28,98	32,51	104,89	2,62	-2,16
Розмір чистого прибутку, тис. грн	22840	65019	182440	122088	82975
Рентабельність діяльності, %	3,59	7,72	10,57	6,89	4,79
Розмір активів, тис. грн	361038	524098	805115	1131717	1124096
Розмір зобов’язань, тис. грн.	199155	266111	358792	543057	456703
Розмір чистих активів, тис. грн	161883	257987	446323	588660	667393
Коефіцієнт автономії, %	44,84	49,22	55,44	52,01	59,37

Джерело: складено автором за даними [243]

Додаток Ж



Джерело: складено автором із використанням методів математичного моделювання та інструменту ШІ (ChatGPT)

Додаток З

Розрахунок інтегрального індексу впливу стейкхолдерів на рішення ПП «Мак Тревел»

Стейкхолдери	ImL	IL	DRI	Інтегральний індекс
Власники та інвестори	0,9	0,8	0,9	**0,87**
Управлінський персонал	0,8	0,7	0,9	**0,8**
Державні органи влади	0,9	0,6	0,8	**0,78**
Банки та фінансові донори	0,7	0,9	0,6	**0,73**
Клієнти і споживачі	0,7	0,6	0,4	**0,58**
Персонал	0,7	0,9	0,9	**0,82**
Постачальники і контрагенти	0,5	0,6	0,4	**0,5**
Громада (локальне ком'юніті)	0,1	0,2	0,1	**0,13**

Джерело: розраховано автором із використанням математичного та експертного методів

Розрахунок інтегрального індексу впливу стейкхолдерів на рішення ТОВ «Техвантаж-Сервіс»

Стейкхолдери	ImL	IL	DRI	Інтегральний індекс
Власники та інвестори	0,8	1	0,9	**0,89**
Управлінський персонал	0,8	0,8	0,9	**0,83**
Державні органи влади	0,8	0,7	0,5	**0,68**
Банки та фінансові донори	0,7	0,8	0,5	**0,67**
Клієнти і споживачі	0,7	0,7	0,3	**0,58**
Персонал	0,8	0,9	0,7	**0,8**
Постачальники і контрагенти	0,7	0,8	0,5	**0,67**
Громада (локальне ком'юніті)	0,4	0,6	0,4	**0,46**

Джерело: розраховано автором із використанням математичного та експертного методів

Розрахунок інтегрального індексу впливу стейкхолдерів на рішення ТОВ «Авіа-Сервіс»

Стейкхолдери	ImL	IL	DRI	Інтегральний індекс
Власники та інвестори	1	1	0,7	**0,91**
Управлінський персонал	1	1	0,8	**0,94**
Державні органи влади	0,8	0,8	0,6	**0,74**
Банки та фінансові донори	0,6	0,7	0,6	**0,63**
Клієнти і споживачі	0,7	0,7	0,7	**0,7**
Персонал	0,8	0,8	0,9	**0,83**
Постачальники і контрагенти	0,6	0,7	0,5	**0,6**
Громада (локальне ком'юніті)	0,5	0,5	0,4	**0,47**

Джерело: розраховано автором із використанням математичного та експертного методів